Lattices and orders in number fields

Hugo Chapdelaine

June 2024

Contents

Abstract

The goal of this note is to gather in one place some basic results on lattices and orders in number fields. Most of these results can be found in the literature but in a rather scattered way, and sometimes, such results are formulated in more general setups which may obscure the simpler aspects of lattices and orders in number fields. Some proofs are provided but for the more technical ones a reference is usually provided.

1 Introduction

In [5], the author made a detailed investigation of a special type of GL_2-real analytic Eisenstein series for which some basic results on lattices and orders in number fields, not so easily found in the literature, were required. The present paper can be viewed as a slightly updated version of Section 4 of [5] which goal, back then, was to gather in one place some of the needed results used in loc. cit. Our goal in this note is modest and we simply wish to provide a basic reference on lattices and orders in number fields that covers the required needs in [5] and also of our forthcoming papers [6] and [7]. It seemed to us better to publish this note as a separate entity so that it can, at least provisionally, provide a concise reference for the number theorists who wish to learn more about some of the theoretical intricacies involved when one replaces the maximal order of a number field by a non-maximal order. In fact, as a testimony, when the author wrote [3] and [4] he had a misconception about the two notions of $\mathcal{O}$-properness and $\mathcal{O}$-invertibility for a general order (see Section 3.7). In particular, this paper takes the opportunity to clarify the relationships between these two notions.

Let us give some quick overview of the literature on the topic considered in this note. A good reference for orders in imaginary quadratic field with interesting number theory applications is [9]. For general orders of number fields, a short introduction can be found §12 of Chapter 1 of [20], and a much more detailed presentation is given in [22]. The author found also very useful some unpublished documents from Keith Conrad, available on his personal website, as for example [8]. In the coming work [7], we give an introduction to what we call *signature lattice zeta functions*. It is possible to rephrase and extend the Stark conjectures (see [12],[13],[14] and [15]) for this special class of zeta functions and we expect that such an appropriate reformulation will involve a ray class field theory for general orders of number fields. Very recently, the nice preprint [16] has appeared on arxiv where the two authors work out a comprehensive ray class field theory for a general order of a number field. No doubt that their paper will fill a significant gap in the literature and is likely to become a standard reference for the class field theory of orders. Incidentally, the introduction of [16] provides a thorough review of the literature on orders of number fields to which we refer the reader. On the topic of class field theory, previous to the paper [16], we are aware of [18] which gave a presentation of a ring class field theory for a general order.

2 Signature of a number field and embeddings

We let $c_\infty : \mathbb{C} \to \mathbb{C}$ denote the complex conjugation. Usually for an element $a \in \mathbb{C}$ we denote its complex conjugate $c_\infty(a)$ by $\overline{a}$.

Let K be an number field of degree g over $\mathbb{Q}$. We say that K has signature (r_1, r_2) if K has r_1 real embeddings and $2r_2$ complex embeddings. If K has signature (r_1, r_2) then $g = r_1 + 2r_2$. Let $\Sigma := \mathrm{Hom}(K, \mathbb{C})$ be a complete set of embeddings of K into $\mathbb{C}$. The group $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \langle c_\infty \rangle$ acts on the left of Σ. If $\tau \in \Sigma$ then $\overline{\tau}$ means $c_\infty \circ \tau$. We choose to write Σ as the union of:

(i) its set of real embeddings:

$$\Sigma_r = \{\tau_1 = \rho_1,\, \tau_2 = \rho_2,\, \ldots,\, \tau_{r_1} = \rho_{r_1}\} \tag{2.1}$$

(ii) its set of complex embeddings labeled as

$$\Sigma_c := \{\tau_{r_1+1} := \sigma_1,\, \tau_{r_1+2} = \sigma_2,\, \ldots, \tau_{r_1+r_2} = \sigma_{r_2}, \\ \tau_{r_1+r_2+1} = \overline{\sigma}_1,\, \ldots,\, \tau_{r_1+2r_2} = \overline{\sigma}_{r_2}\} \tag{2.2}$$

So this provides a partition $\Sigma = \Sigma_r \bigsqcup \Sigma_c$. The set Σ_r can be viewed as the $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ fix point set of Σ.

As usual, for $x \in K$ one defines its trace and its norm

$$\mathrm{Tr}_{K/\mathbb{Q}}(x) = \sum_i \tau_i(x) \in \mathbb{Q} \quad \text{and} \quad \mathbf{N}_{K/\mathbb{Q}}(x) = \prod_i \tau_i(x) \in \mathbb{Q}. \tag{2.3}$$

If A is a ring we let $A^\times$ denote its group of invertible elements under the multiplication. We let $\mathcal{O}_K$ be the ring of integers of K. Recall that if $x \in \mathcal{O}_K$ then $x \in \mathcal{O}_K^\times$ if and only if $\mathbf{N}_{K/\mathbb{Q}}(x) \in \{\pm 1\}$.

A subring $\mathcal{O} \subseteq K$ is called an *order* of K if $[\mathcal{O}_K : \mathcal{O}] < \infty$. Since $\mathcal{O}_K/\mathcal{O}$ is an integral extension it follows that $\mathcal{O}^\times = \mathcal{O}_K^\times \cap \mathcal{O}$. For some basic results on the behavior of chains of prime ideals in an integral extension of rings see for example Theorem 26 on p. 694 of [10]. Note that the results in Section 3.11 provide more precise results on chain of prime ideals in the specific setting of the integral extension $\mathcal{O}_K/\mathcal{O}$.

For the rest of the paper K is a number field signature (r_1, r_2) and of degree $g = r_1 + 2r_2$. Also, unless otherwise specified, $\mathcal{O}$ will be an order in $\mathcal{O}_K$.

3 Lattices and orders in number fields

By a *lattice* $\mathcal{L} \subseteq K$ we mean a free $\mathbb{Z}$-module of rank g. For two lattices $\mathcal{L}_1, \mathcal{L}_2 \subseteq K$, we define their product as

$$\mathcal{L}_1\mathcal{L}_2 = \left\{ \sum_{i=1}^n \ell_{1,i}\ell_{2,i} : \ell_{1,i} \in \mathcal{L}_1, \ell_{2,i} \in \mathcal{L}_2, n \in \mathbb{Z}_{\geq 1} \right\}.$$

One may verify that $\mathcal{L}_1\mathcal{L}_2$ is again a lattice. Moreover, the product operation on lattices is associative. We denote the set if lattices in K by Latt_K. It is an abelian monoid for the multiplication of lattices.

Recall that

$$\begin{aligned} \mathrm{Tr}_{K/\mathbb{Q}}(\_,\_) : K \times K &\to \mathbb{Q} \\ (x,y) &\mapsto \mathrm{Tr}_{K/\mathbb{Q}}(xy) \end{aligned}$$

provides a non-degenerate symmetric bilinear pairing such that its restriction to $\mathcal{O}_K \times \mathcal{O}_K$ is $\mathbb{Z}$-valued.

Definition 3.1. *Let $\mathcal{L} \subseteq K$ be a lattice and let $(x_1, \ldots, x_g)$ be an ordered $\mathbb{Z}$-basis of $\mathcal{L}$. The discriminant of $\mathcal{L}$ is defined as*

$$\mathrm{disc}(\mathcal{L}) := \det(\mathrm{Tr}(x_i x_j)) \in \mathbb{Z}. \tag{3.1}$$

Note that $\mathrm{disc}(\mathcal{L})$ does not depend on the choice of the ordered $\mathbb{Z}$-basis of $\mathcal{L}$ and it is non-vanishing (since $K/\mathbb{Q}$ is separable). Here are some basic properties on the discriminant (see for example Chapter 4 of [19]):

(1) $\mathrm{disc}(\mathcal{L}) = (\det(\tau_i(x_j)))^2$.

(2) If $\mathcal{L} \subseteq \mathcal{M}$ is a sublattice then $\mathrm{disc}(\mathcal{L}) = [\mathcal{M} : \mathcal{L}]^2 \cdot \mathrm{disc}(\mathcal{M})$.

(3) $d_K := \mathrm{disc}(\mathcal{O}_K) \in \mathbb{Z}$ is called the *discriminant* of K. We have $d_K \equiv 0, 1 \pmod 4$ and $\mathrm{sign}(d_K) = (-1)^{r_2}$.

3.1 $\mathcal{O}$-properness

Let $\mathcal{L} \subseteq K$ be a lattice. We define

$$\mathcal{O}_{\mathcal{L}} := \{\lambda \in K : \lambda\mathcal{L} \subseteq \mathcal{L}\},$$

and call $\mathcal{O}_{\mathcal{L}}$ the *multiplier ring* of $\mathcal{L}$ (or the *endomorphism ring of* $\mathcal{L}$). One may check that $\mathcal{O}_{\mathcal{L}}$ is an order of K.

Definition 3.2. *If $\mathcal{O}$ is an order of K, such that $\mathcal{O} = \mathcal{O}_{\mathcal{L}}$, then we say that $\mathcal{L}$ is* $\mathcal{O}$**-proper**.

Remark 3.3. The property of "$\mathcal{O}$-properness" is used in [17] in the setting of lattices of imaginary quadratic fields and we have chosen here to use this terminology in the more general setting of lattices in number fields.

So, by definition, for any lattice $\mathcal{L}$, we always have that $\mathcal{L}$ is $\mathcal{O}_{\mathcal{L}}$-proper and moreover, $\mathcal{O}_{\mathcal{L}}$ is the only order $\mathcal{O}$ of K for which $\mathcal{L}$ is $\mathcal{O}$-proper. For an arbitrary lattice $\mathcal{L} \subseteq K$ we may view $\mathcal{L}$ as a finitely generated $\mathcal{O}_{\mathcal{L}}$-module. Since

$$\{\epsilon \in \mathcal{O}_{\mathcal{L}} : \epsilon\mathcal{L} = \mathcal{L}\} = \mathcal{O}_{\mathcal{L}}^{\times},$$

we may identify the group of units of $\mathcal{O}_{\mathcal{L}}$ with the group of automorphisms of $\mathcal{L}$ when $\mathcal{L}$ is viewed as an $\mathcal{O}_{\mathcal{L}}$-module.

Definition 3.4. *Given an order $\mathcal{O} \subseteq K$ and two $\mathcal{O}$-ideals $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}$ we say that $\mathfrak{a}$ and $\mathfrak{b}$ are coprime if $\mathfrak{a} + \mathfrak{b} = \mathcal{O}$. Recall that* Latt_K *denotes the set of all lattices in K. Given an order $\mathcal{O} \subseteq K$, we let* $\mathrm{Latt}_{\mathcal{O}}$ *the subset of elements in* Latt_K *which are also $\mathcal{O}$-modules. In particular, if $\mathcal{O} \subseteq \mathcal{O}'$ is an inclusion of orders then* $\mathrm{Latt}_{\mathcal{O}'} \subseteq \mathrm{Latt}_{\mathcal{O}}$*. An element $\mathcal{L} \in \mathrm{Latt}_{\mathcal{O}}$ is called a fractional $\mathcal{O}$-ideal. A lattice $\mathfrak{a}$ is said to be an $\mathcal{O}$-integral lattice if $\mathfrak{a} \in \mathrm{Latt}_{\mathcal{O}}$ and $\mathfrak{a} \subseteq \mathcal{O}$.*

3.2 The multiplicative inverse operation

Definition 3.5. *Let $\mathcal{L}$ be a lattice of K. We define the multiplicative inverse of $\mathcal{L}$ to be*

$$\mathcal{L}^{-1} := \{\lambda \in K : \lambda\mathcal{L} \subseteq \mathcal{O}_{\mathcal{L}}\}. \tag{3.2}$$

Note that, by definition, $\mathcal{L}^{-1}$ is always an $\mathcal{O}_{\mathcal{L}}$-module and that $\mathcal{L}\mathcal{L}^{-1} \subseteq \mathcal{O}_{\mathcal{L}}$. Since $\mathcal{L}^{-1}$ is an $\mathcal{O}_{\mathcal{L}}$-module, it follows that that $\mathcal{O}_{\mathcal{L}} \subseteq \mathcal{O}_{\mathcal{L}^{-1}}$. From the previous inclusion, it follows that $\mathcal{L} \subseteq (\mathcal{L}^{-1})^{-1}$. As Example 3.6 below shows, the three preceding inclusions could be strict in general. The example below is inspired from an email exchange with Keith Conrad in the year 2014, who kindly pointed out to me Exercise 18 on page 94 of [2] (cf. with Example 2.4 of [16]).

Example 3.6. Let $\theta \in \overline{\mathbb{Q}}$ be such that $\theta^3 = 2$ and consider the cubic field $K := \mathbb{Q}(\theta)$. We have that $\mathcal{O}_K = \mathbb{Z}[\theta]$. Let $\mathcal{R} := \mathbb{Z} + 2\theta\mathbb{Z} + 2\theta^2\mathbb{Z}$. One may verify that $\mathcal{R}$ is an order of index four in $\mathcal{O}_K$. Consider the lattice $\mathcal{M} := 4\mathbb{Z} + \theta\mathbb{Z} + \theta^2\mathbb{Z} \subseteq K$. Then direct computations (which we leave to the reader) show that

(i) $\mathcal{O}_{\mathcal{M}} = \mathcal{R}$,

(ii) $\mathcal{M}^2 = 2\mathbb{Z} + 2\theta\mathbb{Z} + \theta^2\mathbb{Z}$,

(iii) $\mathcal{O}_{\mathcal{M}^2} = \mathcal{O}_K$,

(iv) $\mathcal{M}^{-1} = 2\mathbb{Z} + 2\theta\mathbb{Z} + \theta^2\mathbb{Z} = 2\mathcal{O}_K + \theta^2\mathcal{O}_K$,

(v) $\mathcal{O}_{\mathcal{M}^{-1}} = \mathcal{O}_K$ and $(\mathcal{M}^{-1})^{-1} = \frac{1}{2}(2\mathcal{O}_K + \theta\mathcal{O}_K) = \frac{1}{2}(2\mathbb{Z} + \theta\mathbb{Z} + \theta^2\mathbb{Z}) \supsetneqq \mathcal{M}$,

(vi) $\mathcal{M}\mathcal{M}^{-1} \subseteq 2\mathcal{O}_K \subsetneqq \mathcal{R}$.

Example 3.6 is instructive since it shows that if $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Latt}_K$ are $\mathcal{O}$-proper, then $\mathcal{L}_1\mathcal{L}_2$ is not necessarily $\mathcal{O}$-proper (take $\mathcal{L}_1 = \mathcal{L}_2 = \mathcal{M}$ where $\mathcal{M}$ is as above). Moreover, the lattice $\mathcal{M}$ above is such that $\mathcal{O}_{\mathcal{M}} \neq \mathcal{O}_{\mathcal{M}^{-1}}$ and $\mathcal{M} \subsetneqq (\mathcal{M}^{-1})^{-1}$. In particular, the application $[-1] : Latt_K \to Latt_K$, given by $\mathcal{L} \mapsto \mathcal{L}^{-1}$ is not necessarily involutive.

Remark 3.7. Let $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Latt}_K$ and assume that $\mathcal{O} := \mathcal{O}_{\mathcal{L}_1} = \mathcal{O}_{\mathcal{L}_2}$. Then one readily sees from the definitions that the multiplicative inverse operation behaves in a contravariant way:

$$\mathcal{L}_1 \subseteq \mathcal{L}_2 \Rightarrow \mathcal{L}_2^{-1} \subseteq \mathcal{L}_1^{-1}. \tag{3.3}$$

However, without the strong assumption $\mathcal{O} = \mathcal{O}_{\mathcal{L}_1} = \mathcal{O}_{\mathcal{L}_2}$, the implication (3.3) is false in general.

3.3 $\mathcal{O}$-invertibility

Let $\mathcal{L} \in \mathrm{Latt}_{\mathcal{O}}$. By definition of $\mathcal{O}_{\mathcal{L}}$ we have that $\mathcal{O} \subseteq \mathcal{O}_{\mathcal{L}}$.

Definition 3.8. *We say that $\mathcal{L}$ is $\mathcal{O}$-**invertible**, if there exists an $\mathcal{O}$-module $\mathcal{L}' \in \mathrm{Latt}_{\mathcal{O}}$ such that $\mathcal{L}\mathcal{L}' = \mathcal{O}$. We denote the set of $\mathcal{O}$-invertible lattices in K by $\mathrm{Inv}_{\mathcal{O}}$. It is a submonoid of $\mathrm{Latt}_{\mathcal{O}}$.*

Let $\mathcal{L} \in \mathrm{Latt}_{\mathcal{O}}$ and assume that it is $\mathcal{O}$-invertible. Since $\mathcal{O}_{\mathcal{L}} \cdot \mathcal{L}\mathcal{L}' \subseteq \mathcal{L}\mathcal{L}' = \mathcal{O}$ and $1 \in \mathcal{L}\mathcal{L}' = \mathcal{O}$, this implies that $\mathcal{O}_{\mathcal{L}} \subseteq \mathcal{O}$ and therefore $\mathcal{O} = \mathcal{O}_{\mathcal{L}}$. Thus, if $\mathcal{L}$ is an $\mathcal{O}$-invertible module, it is automatically $\mathcal{O}$-proper. The converse is not true in general as will be explained in this section further down below. Now let $\mathcal{L} \in \mathrm{Latt}_{\mathcal{O}}$ and assume that there exists $\mathcal{L}' \in \mathrm{Latt}_{\mathcal{O}}$ such that $\mathcal{L}\mathcal{L}' = \mathcal{O}$. Then we claim that such a lattice $\mathcal{L}' \in \mathrm{Latt}_{\mathcal{O}}$ is necessarily unique. Indeed, let $\mathcal{L}'' \in \mathrm{Latt}_{\mathcal{O}}$ be such that $\mathcal{L}\mathcal{L}'' = \mathcal{O}$. Then multiplying the previous equality by $\mathcal{L}'$ we find that $(\mathcal{L}'' =)\ \mathcal{O}\mathcal{L}'' = \mathcal{L}'\mathcal{O}\ (= \mathcal{L}')$ so that $\mathcal{L}'' = \mathcal{L}'$. It follows from this that $\mathrm{Inv}_{\mathcal{O}}$ is a subgroup of the monoid $\mathrm{Latt}_{\mathcal{O}}$. Moreover, if $\mathcal{L}, \mathcal{L}' \in \mathrm{Latt}_{\mathcal{O}}$ and $\mathcal{L}\mathcal{L}' = \mathcal{O}$, we claim that necessarily $\mathcal{L}'$ must be equal to $\mathcal{L}^{-1}$. Indeed, we have proved earlier that $\mathcal{O} = \mathcal{O}_{\mathcal{L}}$, and from the definition of $\mathcal{L}^{-1}$ we see that $\mathcal{L}' \subseteq \mathcal{L}^{-1}$ which in particular implies that $\mathcal{O} = \mathcal{L}\mathcal{L}' \subseteq \mathcal{L}\mathcal{L}^{-1} \subseteq \mathcal{O}_{\mathcal{L}} = \mathcal{O}$ and thus $\mathcal{L}\mathcal{L}^{-1} = \mathcal{O}$. Finally, by the uniqueness of the inverse for $\mathcal{L}$ proved earlier we deduce that $\mathcal{L}^{-1} = \mathcal{L}'$.

Remark 3.9. In [16], the terminology of "potential invertibility" for a given lattice $\mathcal{L}$ is used in the following sense: a lattice $\mathcal{L} \in \mathrm{Latt}_K$ is said to be potentially invertible if $\mathcal{L}$ is $\mathcal{O}_{\mathcal{L}}$-invertible.

From the above discussion we obtain:

Proposition 3.10. *Let $\mathcal{L} \in \mathrm{Latt}_K$. Then*

$$\mathcal{L}\mathcal{L}^{-1} = \mathcal{O}_{\mathcal{L}} \iff 1 \in \mathcal{L}\mathcal{L}^{-1} \iff \mathcal{L} \text{ is } \mathcal{O}_{\mathcal{L}}\text{-invertible.}$$

Moreover, if $\mathcal{L}$ is $\mathcal{O}_{\mathcal{L}}$-invertible, one has that $(\mathcal{L}^{-1})^{-1} = \mathcal{L}$ and that $\mathcal{O}_{\mathcal{L}} = \mathcal{O}_{\mathcal{L}^{-1}}$.

Let us provide an example of a lattice $\mathcal{L}$ which is $\mathcal{O}_{\mathcal{L}}$-proper but not $\mathcal{O}_{\mathcal{L}}$-invertible. Looking at Example 3.6, we see that $\mathcal{O}_{\mathcal{M}} = \mathcal{R}$ and $\mathcal{M}\mathcal{M}^{-1} \subsetneqq \mathcal{R} = \mathcal{O}_{\mathcal{M}}$. In particular, the $\mathcal{O}_{\mathcal{M}}$-proper lattice $\mathcal{M}$ is not $\mathcal{O}_{\mathcal{M}}$-invertible. For a further discussion on the discrepancy between the $\mathcal{O}$-invertibility and $\mathcal{O}$-properness, see Section 3.7.

If the lattice $\mathcal{L} = \mathcal{O} \subseteq K$ is an order, then one may easily check that $\mathcal{O}_{\mathcal{O}} = \mathcal{O}$ and that $\mathcal{O}^{-1} = \mathcal{O}$. It is worthwhile to remind the reader of the following set of equivalences for $\mathcal{O}$-invertibility which will be used later on in the proof of Corollary 3.34.

Theorem 3.11. *Let $\mathcal{O} \subseteq \mathcal{O}_K$ be an order and let $\mathcal{L} \in \mathrm{Latt}_K$. Then the following statements are equivalent:*

(1) $\mathcal{L}$ is $\mathcal{O}$-invertible.

(2) $\mathcal{L}$ is a projective $\mathcal{O}$-module.

(3) $\mathcal{L}$ is a locally free $\mathcal{O}$-module, i.e., for each non-zero prime ideal $\mathfrak{p} \subseteq \mathcal{O}$, one has that $\mathcal{L}_{\mathfrak{p}}$ is a free $\mathcal{O}_{\mathfrak{p}}$-module (necessarily of rank 1).

Proof For a proof of these equivalences the author may consult for example Section 11.2 of [21]. See also Corollary 6.2 of [8] □

Let $\mathcal{O} \subseteq \mathcal{O}_K$ be an order and let M be a torsion free finitely generated $\mathcal{O}$-module. Then $M \hookrightarrow M \otimes_{\mathcal{O}} K \simeq K^r$ for some integer r which is called the rank of M. If M has rank one it follows from the previous injection that M is isomorphic, as an $\mathcal{O}$-module, to an ideal $\mathfrak{a}$ of $\mathcal{O}$. So it makes sense to ask the following: Given two non-zero ideals $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}$ when are these isomorphic as $\mathcal{O}$-modules ? Obviously, if there exists a $\lambda \in K^\times$ such that $\lambda\mathfrak{a} = \mathfrak{b}$ then $\mathfrak{a}$ and $\mathfrak{b}$ will be isomorphic as $\mathcal{O}$-modules. It turns out that the converse is also true namely that if $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}$ are two non-zero ideals which are isomorphic as $\mathcal{O}$-modules, then necessarily there exists a $\lambda \in K^\times$ such that $\lambda\mathfrak{a} = \mathfrak{b}$, see for example [23].

Remark 3.12. The latter converse statement can be seen directly in the special case when at least one of the two ideals, say $\mathfrak{a}$, is $\mathcal{O}$-invertible. Indeed, let $\varphi : \mathfrak{a} \to \mathfrak{b}$ be an isomorphism of $\mathcal{O}$-modules. Choose $\lambda \in \mathcal{O}\backslash\{0\}$ such that $\lambda\mathfrak{a}^{-1} \subseteq \mathcal{O}$. By $\mathcal{O}$-flatness it follows that φ induces an isomorphism of $\mathcal{O}$-modules $\widetilde{\varphi} : \lambda\mathfrak{a}^{-1}\mathfrak{a} = \lambda\mathcal{O} \to \lambda\mathfrak{a}^{-1}\mathfrak{b}$. In particular, $\lambda\mathfrak{a}^{-1}\mathfrak{b}$ is $\mathcal{O}$-cyclic and thus $\lambda\mathfrak{a}^{-1}\mathfrak{b} = \mu\mathcal{O}$ for some $\mu \in K^\times$ so that $\frac{\lambda}{\mu}\mathfrak{a} = \mathfrak{b}$.

Let $\mathfrak{a}, \mathfrak{b} \in \mathrm{Latt}_{\mathcal{O}}$. We shall write $\mathfrak{a} \sim_{\mathcal{O}} \mathfrak{b}$ whenever there exists $\lambda \in K^\times$ such that $\lambda\mathfrak{a} = \mathfrak{b}$. Note that the relation $\sim_{\mathcal{O}}$ preserves the $\mathcal{O}$-invertibility. In general, the set

$$\begin{aligned} \mathrm{Isom}_1(\mathcal{O}) &:= \{\text{isomorphism classes of torsion free } \mathcal{O}\text{-modules of rank } 1\} \\ &\simeq \mathrm{Latt}_{\mathcal{O}} / \sim_{\mathcal{O}}, \end{aligned} \tag{3.4}$$

is only a monoid which can be shown to be finite by using classical results of the geometry of numbers. If we restrict the set $\mathrm{Latt}_{\mathcal{O}}$ to $\mathrm{Inv}_{\mathcal{O}}$ in (3.4) then one gets a group which is usually called the *Picard group* and which is often denoted by $\mathrm{Pic}(\mathcal{O})$. In the special case when $\mathcal{O} = \mathcal{O}_K$ is the maximal order, the positive integer

$$h_K := \#\,\mathrm{Pic}(\mathcal{O}_K)$$

is called the *class number of K*.

Let us also mention one further result related to the notion of invertibility which we have extracted directly from [16] (see Proposition 2.22 of loc. cit.):

Proposition 3.13. *(Dade, Taussky, Zassenhaus) Fix an order $\mathcal{O}$. Given $\mathfrak{a} \in \mathrm{Latt}_{\mathcal{O}}$ there exists a positive integer $N_{\mathfrak{a}} \geq 1$ such that*

$$\mathfrak{a}^n \textit{ is } \mathcal{O}_{\mathfrak{a}^n}\textit{-invertible} \Longleftrightarrow n \geq N_{\mathfrak{a}}. \tag{3.5}$$

Furthermore, $N_{\mathfrak{a}}$ is bounded uniformly by $N_{\mathfrak{a}} \leq g - 1$.

For a more thorough discussion about the notion of invertibility we refer to [16].

3.4 The conductor of an order and the invertibility of prime ideals

Definition 3.14. *The conductor of an order $\mathcal{O} \subseteq K$ is defined as*

$$\mathrm{cond}(\mathcal{O}) := \mathfrak{c}_{\mathcal{O}} := \{x \in K : x\mathcal{O}_K \subseteq \mathcal{O}\}.$$

One may check that $\mathfrak{c}_{\mathcal{O}}$ is the largest integral $\mathcal{O}_K$-ideal which is included in $\mathcal{O}$. In particular, $\mathfrak{c}_{\mathcal{O}}$ is an integral $\mathcal{O}$-ideal. The next proposition gives a complete characterization of the invertible *prime* ideals of $\mathcal{O}$.

Theorem 3.15. *A non-zero prime ideal $\mathfrak{p} \subseteq \mathcal{O}$ is $\mathcal{O}$-invertible if and only if $\mathfrak{p}$ is relatively prime to $\mathfrak{c}_{\mathcal{O}}$, i.e., $\mathfrak{p} + \mathfrak{c}_{\mathcal{O}} = \mathcal{O}$.*

Proof See for example Theorem 6.1 of [8]. □

Remark 3.16. Note that the "only if direction" in Theorem 3.15 is no longer true if $\mathfrak{p}$ is not prime. For example, assume that $\mathfrak{c}_{\mathcal{O}} \subsetneqq \mathcal{O}_K$ and let $c > 1$ be the smallest integer inside $\mathfrak{c}_{\mathcal{O}}$. Then the $\mathcal{O}$-ideal $c\mathcal{O}$ is invertible (since it is principal) but it is not coprime to $\mathfrak{c}_{\mathcal{O}}$.

Definition 3.17. *A non-zero prime ideal $\mathfrak{p} \subseteq \mathcal{O}$ is said to regular if $\mathfrak{p} \nmid \mathfrak{c}_{\mathcal{O}}$. Otherwise it is said to be irregular.*

Example 3.18. Let us describe explicitly what the non-regular prime ideals look like for orders in the simplest nontrivial case, namely for orders in a quadratic field $K = \mathbb{Q}(\sqrt{D})$. Here we assume that D is its discriminant (positive or negative) and to fix the idea let us assume also that $D \equiv 2, 3 \pmod 4$ so that $\mathbb{Z} + \sqrt{D}\mathbb{Z} = \mathcal{O}_K$ (the same argument works if $D \equiv 1 \pmod 4$). For $f \in \mathbb{Z}_{>0}$, let $\mathcal{O}_f := \mathbb{Z} + f\mathcal{O}_K$ be the unique order of conductor f contained in $\mathcal{O}_K$. For each prime $\ell | f$, let $P_\ell := \ell\mathbb{Z} + f\sqrt{D}\mathbb{Z}$. It is an $\mathcal{O}_f$-prime ideal above $\ell\mathbb{Z}$. It can be directly checked that P_ℓ is not $\mathcal{O}_f$-invertible (which is consistent with Theorem 3.15). Moreover, one has that $P_\ell \supsetneqq \ell\mathcal{O}_f \supsetneqq P_\ell^2$ which shows that $\ell\mathcal{O}_f$ is a P_ℓ-primary ideal which is not a power of P_ℓ; compare with Remark 3.38. We claim that P_ℓ is the only prime ideal of $\mathcal{O}_f$ above $\ell\mathbb{Z}$. So let us check that this is indeed the case. Let Q be a prime ideal of $\mathcal{O}_f$ which is above $\ell\mathbb{Z}$. Since $Q \cap \mathbb{Z} = \ell\mathbb{Z}$ it follows that $Q \supseteq \ell\mathcal{O}_f$. However, $\ell\mathcal{O}_f$ is never prime (since for example $\sqrt{D}\cdot(f\sqrt{D}) \in \ell\mathcal{O}_f$ while $\sqrt{D}, f\sqrt{D} \notin \ell\mathcal{O}_f$) it follows that $Q \supsetneqq \ell\mathcal{O}_f$. Since $[\mathcal{O}_f : \ell\mathcal{O}_f] = \ell^2$ we must necessarily have $[\mathcal{O}_f : Q] = \ell$. There are $\ell + 1$ index ℓ subgroups in $\mathcal{O}_f$ which are given by $L_k := \mathbb{Z}(f\sqrt{D} + k) + \ell\mathbb{Z}$ for $0 \leq k \leq \ell - 1$ and $M := \mathbb{Z}\ell f\sqrt{D} + \mathbb{Z}$. The case $Q = M$ is impossible since $1 \in M$. The case $L_0 = Q$ does occur since $L_0 = P_\ell$. Finally the case $L_k = Q$, for some $1 \leq k \leq \ell - 1$, is impossible since L_k is not closed under the multiplication by $f\sqrt{D}$. Indeed, we have $f\sqrt{D} \cdot (f\sqrt{D} + k) - k(f\sqrt{D} + k) = f^2 D - k^2 \in \mathbb{Z}$; but if L_k were closed under the multiplication by $f\sqrt{D}$ this would mean that $f^2 D - k^2 \in \ell\mathbb{Z}$ which is absurd since $\ell | f$ and $\ell \nmid k$.

3.5 Fractional $\mathcal{O}$-ideals

Let $\mathcal{O} \subseteq \mathcal{O}_K$ be an order. Recall that a *fractional $\mathcal{O}$-ideal* is a lattice $\mathfrak{a} \subseteq K$ which is an $\mathcal{O}$-module. To learn more about fractional ideals in the setting of orders we refer to [16] which also provides a good review of the literature on the subject.

We wish now to record some basic facts on $\mathcal{O}_K$-lattices which are not necessarily true when one replaces $\mathcal{O}_K$ by a general order $\mathcal{O} \subseteq \mathcal{O}_K$, so that the reader should be cautious before applying any of the facts below in the setting of a general order.

Proposition 3.19. *Let $\mathcal{O} = \mathcal{O}_K$ be a maximal order. Then the following hold true*

(1) Let $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}$ be two nonzero ideals. Then there exists an ideal $\mathfrak{c} \subseteq \mathcal{O}$, relatively prime to both $\mathfrak{a}$ and $\mathfrak{b}$, such that $\mathfrak{c}\mathfrak{a} = \lambda\mathcal{O}$ is a principal ideal.

(2) Each fractional $\mathcal{O}$-ideal $\mathfrak{a}$ is $\mathcal{O}$-invertible. In particular, if $\mathfrak{a} \subseteq \mathcal{O}$ is a nonzero ideal then $\mathfrak{a}$ is $\mathcal{O}$-invertible.

(3) Let $\mathfrak{a} \subseteq \mathcal{O}$ be a nonzero ideal. Then the quotient ring $\mathcal{O}/\mathfrak{a}$ is a principal ring (i.e. each ideal is principal).

(4) Let $\mathfrak{a} \subseteq \mathcal{O}$ be a nonzero ideal and let $a \in \mathfrak{a}\backslash\{0\}$. Then there exists $b \in \mathfrak{a}$ such that $a\mathcal{O} + b\mathcal{O} = \mathfrak{a}$.

(5) Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \subseteq K$ be three fractional $\mathcal{O}$-ideal. Then there exists $a \in \mathfrak{a}^{-1}\mathfrak{c}$ and $b \in \mathfrak{b}^{-1}\mathfrak{c}$ such that $a\mathfrak{a} + b\mathfrak{b} = \mathfrak{c}$.

(6) Let $\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_n \subseteq K$ be fractional $\mathcal{O}$-ideals and set $\mathfrak{b} = \mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_n$. Then $\bigoplus_{k=1}^n \mathfrak{a}_k$ is isomorphic as an $\mathcal{O}$-module to $\mathcal{O}^{n-1} \oplus \mathfrak{b}$.

Proof The proofs of most of these facts can be found in Section 16.3 of [10] (if a statement is not directly proved in the text then it is to be found in the exercises at the end of the same section). □

It is not too difficult to find counter-examples to each statement above when the order $\mathcal{O}$ is no longer assumed to be maximal so that we leave this task to the interested reader.

3.5.1 On the two generator problem for the ideals of an order

It follows from (4) of Proposition 3.19 that each ideal of $\mathcal{O}_K$ can be generated by two elements. One may wonder if such a result still holds true for ideals in a general order.

Definition 3.20. *Following the terminology of [11], we say that a ring R satisfies the property* IG_2 *if every ideal in R can be generated by two elements.*

One has the following surprising and remarkably precise result

Theorem 3.21. *(Theorem 3.6 of [11]) An order $\mathcal{O}$ is an* IG_2 *ring if and only if* $\mathrm{disc}(\mathcal{O})$ *is fourth-power-free over $\mathbb{Z}$.*

Example 3.22. (Example 3.8 of [11]) Consider the order $\mathcal{O} = \mathbb{Z}[2\sqrt[3]{5}] \subseteq K = \mathbb{Q}(\sqrt[3]{5})$. Let $\mathfrak{a} := \mathbb{Z}[\sqrt[3]{5}]$ and view it as a fractional $\mathcal{O}$-ideal. Then $\mathfrak{a}$ is not 2-generated. Note that $\mathrm{disc}(\mathcal{O}) = 2^6 \cdot 3 \cdot 5^2$.

3.6 The dual operation

We would like now to recall some classical results about dual lattices with respect to the trace pairing. Recall that

$$\mathrm{Tr}_{K/\mathbb{Q}}(\_,\_) : K \times K \to \mathbb{Q}$$

is a non-degenerate symmetric bilinear pairing.

Definition 3.23. *For a lattice $\mathcal{L} \subseteq K$, we define the dual lattice of $\mathcal{L}$ by*

$$\mathcal{L}^* := \{x \in K : \mathrm{Tr}_{K/\mathbb{Q}}(x\ell) \in \mathbb{Z} \textit{ for all } \ell \in \mathcal{L}\}. \tag{3.6}$$

Note that the $*$ operation is contravariant on the partially ordered set of lattices Latt_K, i.e., if $\mathcal{L}_1 \subseteq \mathcal{L}_2$, then $\mathcal{L}_1^* \supseteq \mathcal{L}_2^*$. Using the notion of the dual $\mathbb{Z}$-basis of a given $\mathbb{Z}$-basis of $\mathcal{L}$, one easily proves that $\mathcal{L}^*$ is again a lattice and that $\mathcal{L}^{**} = \mathcal{L}$. It follows that the map $\mathcal{L} \mapsto \mathcal{L}^*$ is an involution on the set $Latt_K$.

Proposition 3.24. *For any $\mathcal{L} \in \mathrm{Latt}_K$ we always have $\mathcal{O}_{\mathcal{L}} = \mathcal{O}_{\mathcal{L}^*}$. In particular, if $\mathcal{L} \in \mathrm{Latt}_{\mathcal{O}}$ then $\mathcal{L}$ is $\mathcal{O}$-proper if and only if $\mathcal{L}^*$ is $\mathcal{O}$-proper.*

Proof From the definition of $\mathcal{L}^*$ we see that $\mathcal{O}_{\mathcal{L}} \cdot \mathcal{L}^* \subseteq \mathcal{L}^*$ and therefore $\mathcal{O}_{\mathcal{L}} \subseteq \mathcal{O}_{\mathcal{L}^*}$; conversely, substituting $\mathcal{L}$ by $\mathcal{L}^*$ in the previous inclusion, and using the identity $\mathcal{L}^{**} = \mathcal{L}$, we deduce that $\mathcal{O}_{\mathcal{L}^*} \subseteq \mathcal{O}_{\mathcal{L}}$. □

3.6.1 Dual of an order and the different ideal

Let $\mathcal{O} \subseteq \mathcal{O}_K$ be an order. By definition, we have

$$\mathcal{O}^* = \{x \in K : \mathrm{Tr}_{K/\mathbb{Q}}(xy) \in \mathbb{Z} \text{ for all } y \in \mathcal{O}\}. \tag{3.7}$$

It follows from (3.7) that $\mathcal{O}^*$ is the *largest* $\mathcal{O}$-module in $\mathrm{Latt}_{\mathcal{O}}$ such that for all $x \in \mathcal{O}^*$, $\mathrm{Tr}_{K/\mathbb{Q}}(x) \in \mathbb{Z}$. In particular we get

Proposition 3.25. *Let $\mathcal{O}$ be an order then $\mathcal{O} \subseteq \mathcal{O}^*$, $\mathcal{O}^* \in \mathrm{Latt}_{\mathcal{O}}$ and $\mathcal{O} \subseteq \mathrm{End}(\mathcal{O}^*)$.*

When $\mathcal{O} = \mathcal{O}_K$ is the maximal order, every fractional ideal of K is $\mathcal{O}_K$-invertible. In particular, it makes sense to define

$$\mathfrak{d}_K := ((\mathcal{O}_K)^*)^{-1}.$$

The $\mathcal{O}_K$-fractional ideal $\mathfrak{d}_K$ is called the *different ideal of K*. Note that for any order $\mathcal{O} \subseteq \mathcal{O}_K$, we always have $\mathfrak{d}_K^{-1} = (\mathcal{O}_K)^* \subseteq \mathcal{O}^*$.

3.7 Relationship between $\mathcal{L}^{-1}$ and $\mathcal{L}^*$

We would like now to describe some relationships between the lattices $\mathcal{L}^{-1}$ and $\mathcal{L}^*$.

Let $\mathcal{L} \in \mathrm{Latt}_K$. Then $\mathcal{M} := \mathcal{L}\mathcal{L}^*$ is an $\mathcal{O}_{\mathcal{L}}$-module such that for all $x \in \mathcal{M}$, $\mathrm{Tr}_{K/\mathbb{Q}}(x) \in \mathbb{Z}$. It thus follows that

$$\mathcal{L}\mathcal{L}^* \subseteq (\mathcal{O}_{\mathcal{L}})^*. \tag{3.8}$$

In fact, it will be shown in Proposition 3.29 that the inclusion (3.8) is always an equality.

For every $y \in \mathcal{L}$ and $x \in \mathcal{L}^{-1}(\mathcal{O}_{\mathcal{L}})^*$ we have $xy \in \mathcal{L}\mathcal{L}^{-1}(\mathcal{O}_{\mathcal{L}})^* \subseteq (\mathcal{O}_{\mathcal{L}})^*$ so that $\mathrm{Tr}_{K/\mathbb{Q}}(xy) \in \mathbb{Z}$. It thus follows from the definition of $\mathcal{L}^*$ that

$$\mathcal{L}^{-1}(\mathcal{O}_{\mathcal{L}})^* \subseteq \mathcal{L}^*. \tag{3.9}$$

Combining (3.8) and (3.9) we obtain

Proposition 3.26. *For $\mathcal{L} \in \mathrm{Inv}_{\mathcal{O}}$ we have $\mathcal{L}^* = \mathcal{L}^{-1}(\mathcal{O}_{\mathcal{L}})^*$.*

Remark 3.27. Let us point out one subtle point regarding the dual operation. In general, if $\mathcal{L}$ is $\mathcal{O}$-invertible, it does not necessarily follow that $\mathcal{L}^*$ is $\mathcal{O}$-invertible. For example, assume that $\mathcal{L}$ is $\mathcal{O}$-invertible, so that $\mathcal{O} = \mathcal{O}_{\mathcal{L}}$, but that $\mathcal{O}^*$ is not $\mathcal{O}$-invertible. We then claim that in this case, $\mathcal{L}^*$ is never $\mathcal{O}$-invertible. Indeed, since $\mathcal{L}$ is $\mathcal{O}$-invertible we have from Proposition 3.26 that

$$\mathcal{L}^* = \mathcal{L}^{-1}(\mathcal{O}_{\mathcal{L}})^*. \tag{3.10}$$

Now by way of contradiction, assume furthermore that $\mathcal{L}^*$ is $\mathcal{O}$-invertible. In that case it would follow from (3.10) that $\mathcal{O}^* = \mathcal{L}^{-1}\mathcal{L}^*$ and therefore $\mathcal{O}^*$ would be $\mathcal{O}$-invertible. But this contradicts our initial assumption that $\mathcal{O}^*$ was not $\mathcal{O}$-invertible.

3.7.1 A criterion for an equivalence between $\mathcal{O}$-properness and $\mathcal{O}$-invertibility

When we wrote the papers [3] and [4], we wrongly thought that $\mathcal{O}$-properness was equivalent to $\mathcal{O}$-invertibility. Fortunately, this does not affect any of the results of the aforementioned papers, since this fictive equivalence was only mentioned but never used in any of the proofs. However, even though these two notions are not equivalent in general, there is a criterion (may be not so well-known to the algebraic number theorists), which says exactly when they agree on the set $\mathrm{Latt}_{\mathcal{O}}$.

Theorem 3.28. *The following two statements are equivalent:*

(i) $\mathcal{L}$ is $\mathcal{O}$-proper $\Longleftrightarrow$ $\mathcal{L}$ is $\mathcal{O}$-invertible.

(ii) The $\mathbb{Z}$-dual $\mathcal{O}^*$ of $\mathcal{O}$, with respect to the trace pairing, is $\mathcal{O}$-invertible.

Proof See Theorem 4.1 of [8]. □

Let us draw one straightforward consequence from the above theorem. Let $\mathcal{L} \in \mathrm{Latt}_K$ be an arbitrary lattice and set $\mathcal{O} := \mathcal{O}_{\mathcal{L}}$; so that by definition of $\mathcal{O}$, $\mathcal{L}$ is $\mathcal{O}$-proper. Then in the fortunate outcome that $\mathcal{O}^*$ is $\mathcal{O}$-invertible it follows directly from Theorem 3.28 that $\mathcal{L}$ is $\mathcal{O}$-invertible. It can be shown that condition (ii) in Theorem 3.28 is always satisfied, if the order $\mathcal{O}$ is *monogenic*, i.e., if $\mathcal{O} = \mathbb{Z}[\mu]$ for some $\mu \in \mathcal{O}$, see Corollary 4.3 of [8]. Therefore, when $\mathcal{O}$ is monogenic, the notions of $\mathcal{O}$-invertibility and $\mathcal{O}$-properness agree. In particular, $\mathcal{O}$-properness and $\mathcal{O}$-invertibility are equivalent when K is a quadratic field, since any order of a given quadratic field is monogenic.

In the course of the proof of Theorem 4.1 of [8], the following is proved:

Proposition 3.29. *Let $\mathcal{L} \in \mathrm{Latt}_K$ then $\mathcal{L}\mathcal{L}^* = (\mathcal{O}_{\mathcal{L}})^*$.*

Proof We have already proved in (3.8) that $\mathcal{L}\mathcal{L}^* \subseteq (\mathcal{O}_{\mathcal{L}})^*$. For completeness, let us include the proof given in [8] for the reverse inclusion. Let $x \in (\mathcal{L}\mathcal{L}^*)^*$. Then $\mathrm{Tr}_{K/\mathbb{Q}}(x\mathcal{L}\mathcal{L}^*) = \mathrm{Tr}_{K/\mathbb{Q}}((x\mathcal{L}^*)\mathcal{L}) \subseteq \mathbb{Z}$ so that $x\mathcal{L}^* \subseteq \mathcal{L}^*$ by definition of $\mathcal{L}^*$. Dualizing the previous inclusion we obtain $\frac{1}{x}\mathcal{L} \supseteq \mathcal{L}$, i.e. that $x\mathcal{L} \subseteq \mathcal{L}$ and thus $x \in \mathcal{O}_{\mathcal{L}}$. This proves that $(\mathcal{L}\mathcal{L}^*)^* \subseteq \mathcal{O}_{\mathcal{L}}$ and by dualizing once more we finally get that $(\mathcal{O}_{\mathcal{L}})^* \subseteq \mathcal{L}\mathcal{L}^*$. □

3.8 Index and covolume

Let $\mathcal{L}_1, \mathcal{L}_2 \subseteq K$ be two lattices. We define the rational index

$$[\mathcal{L}_1 : \mathcal{L}_2]$$

as the absolute value of the determinant of any g-by-g matrix with rational entries which takes a $\mathbb{Z}$-basis of $\mathcal{L}_1$ to a $\mathbb{Z}$-basis of $\mathcal{L}_2$. So we always have $[\mathcal{L}_1 : \mathcal{L}_2] \in \mathbb{Q}_{>0}$. The rational index satisfies the transitivity formula $[\mathcal{L}_1 : \mathcal{L}_2][\mathcal{L}_2 : \mathcal{L}_3] = [\mathcal{L}_1 : \mathcal{L}_3]$ for all lattices $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3 \in \mathrm{Latt}_K$. We also define the *absolute norm* of $\mathcal{L}$ as

$$\mathbf{N}(\mathcal{L}) := [\mathcal{O}_K : \mathcal{L}] \in \mathbb{Q}_{>0}.$$

Let $\langle , \rangle$ be a choice of a real inner product on $W := \mathbb{R}^g$ so that $(W, \langle , \rangle)$ becomes a real euclidean space of dimension g. Let $\{w_1, \dots, w_n\}$ be linearly independent vectors. The $\langle , \rangle$-volume of the "unit box" $\mathcal{B} = \{\sum_i t_i w_i : 0 \leq t_i \leq 1\}$ is defined as

$$\mathrm{vol}_{\langle , \rangle}(\mathcal{B}) = |\det(\langle w_i, w_j \rangle)_{i,j}|^{1/2}. \tag{3.11}$$

The rule $\mathcal{B} \mapsto \mathrm{vol}_{\langle , \rangle}(\mathcal{B})$ gives rise to a (Borel) measure on W which we still denote by $\mathrm{vol}_{\langle , \rangle}$.

Let $L \subseteq W$ be a lattice of maximal rank and $\{w_1, \dots, w_n\}$ be a $\mathbb{Z}$-basis of L. Let $\mathcal{B}$ be the unit box generated by the w_i's. The $\langle , \rangle$-covolume of L is defined as

$$\mathrm{cov}_{\langle , \rangle}(L) := \mathrm{vol}_{\langle , \rangle}(\mathcal{B}). \tag{3.12}$$

We choose to embed K in $V := \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ in the following way

$$\begin{aligned} \iota : K &\to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \\ \lambda &\mapsto \iota(\lambda) := (\tau_j(\lambda))_{j=1}^{r_1+r_2} \end{aligned} \tag{3.13}$$

where the embeddings τ_j's are the embeddings of K as defined as in Section 2. Let $V := \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, it is an $\mathbb{R}$-algebra. We shall denote a typical element $v \in V$ as $v = (v_1, \dots, v_{r_1+r_2})$.

Definition 3.30. *Let $v, w \in V$.*

(1) The Minkowski metric on V (the standard euclidean metric) is defined as

$$\langle v, w \rangle_{\mathcal{M}} := \sum_{i=1}^{r_1} v_i w_i + \sum_{i=r_1+1}^{r_1+r_2} v_i \overline{w_i}.$$

(2) The canonical metric of type (r_1, r_2) on V is defined as

$$\langle v, w \rangle_c := \sum_{i=1}^{r_1} x_i y_i + 2 \sum_{i=r_1+1}^{r_1+r_2} v_i \overline{w_i}.$$

We let $\mathrm{vol}_{\mathcal{M}} := \mathrm{vol}_{\langle,\rangle_{\mathcal{M}}}$ and $\mathrm{vol}_c := \mathrm{vol}_{\langle,\rangle_c}$ be the respective volume measure on V.

Proposition 3.31. *Let $X \subseteq V$ be a measurable set. Then $\mathrm{vol}_c(X) = 2^{r_2} \mathrm{vol}_{\mathcal{M}}(X)$. Moreover, if $\mathcal{L} \in \mathrm{Latt}_K$ then*

$$\mathrm{cov}_c(\iota(\mathcal{L})) = \sqrt{|d_K|} \cdot [\mathcal{O}_K : \mathcal{L}]. \tag{3.14}$$

Proof See p. 30-31 of [20]. □

Definition 3.32. *For $\mathcal{L} \in \mathrm{Latt}_K$ we define*

$$\mathrm{cov}(\mathcal{L}) := \sqrt{|d_K|} \cdot [\mathcal{O}_K : \mathcal{L}] = \sqrt{|\operatorname{disc}(\mathcal{L})|}, \tag{3.15}$$

So by definition, $\mathrm{cov}(\mathcal{L})$ corresponds to the covolume of $\iota(\mathcal{L})$ with respect to the *canonical metric* on V. The covolume of $\iota(\mathcal{L})$ with respect to the Minkowski metric is instead equal to $2^{-r_2}\sqrt{|d_K|} \cdot [\mathcal{O}_K : \mathcal{L}]$.

Lemma 3.33. *We have $\mathrm{cov}(\mathcal{L})\,\mathrm{cov}(\mathcal{L}^*) = 1$.*

Proof This is a general result for (not necessarily symmetric) non-degenerate bilinear forms. Let (V, b) be real vector space of dimension g equipped with a non-degenerate (not necessarily symmetric) bilinear form b. Let $L \subseteq V$ be a lattice. Define $L^* := \{v^* \in V : B(L, v^*) \subseteq \mathbb{Z}\}$. Let $\mathcal{B} = (e_1, \dots, e_g)_{i=1}^{g}$ be an ordered $\mathbb{Z}$-basis of L. Given a $v \in V$ we let $[v]_{\mathcal{B}} \in \mathbb{R}^g$ denote the column vector representing v in the basis $\mathcal{B}$. Let $B := (b(e_i, e_j))_{i,j} \in M_g(\mathbb{R})$ so that the matrix B is just the matrix representation of the $\mathbb{R}$-bilinear form $b(\_, \_)$ with respect to the ordered basis $\mathcal{B}$. Mimicking the definition of the discriminant in (3.1) we let $d_L := |\det(B)|$ be the absolute value discriminant of L. It does not depend on the choice of the ordered basis $\mathcal{B}$ since already $\det(B)$ is independent of $\mathcal{B}$; and it is useful to think of $\sqrt{d_L}$ as the "covolume of L" with respect to b. Let $\mathcal{B}^* := (e_1^*, \ldots, e_g^*)$ be the dual basis of $\mathcal{B}$ with respect to b, so that for all $1 \leq i, j \leq g$, $b(e_i, e_j^*) = \delta_{ij}$. It follows from the definition of L^* that $L^* = \mathbb{Z}e_1^* + \ldots + \mathbb{Z}e_g^*$ (in particular L^* is a lattice). Note that in general $(\mathcal{B}^*)^*$ is not necessarily equal to $\mathcal{B}$ since $b(\_,\_)$ was not assumed to be symmetric. Now let $T = (t_{ij}) \in M_g(\mathbb{R})$ be such that $\sum_{j=1}^g t_{ij} e_j = e_i^*$ for $1 \leq j \leq g$. Note that $T = ([e_1^*]_{\mathcal{B}}, \ldots, [e_g^*]_{\mathcal{B}})$ (the square matrix obtained by stacking together the column vectors $[e_i^*]_{\mathcal{B}}$). Since $b(e_i, e_j^*) = \delta_{ij}$ it follows from the definition of B that $BT \overset{(a)}{=} I_g$. Similary, if we let $B^* := (b(e_i^*, e_j^*))_{i,j} \in M_g(\mathbb{R})$, then again since $b(e_i, e_j^*) = \delta_{ij}$, it follows that $(T^{-1})^t B^* \overset{(b)}{=} I_g$. Multiplying together (a) and (b) we find $I_g = BT(T^{-1})^t B^*$ and taking the determinant we finally obtain $d_L \cdot d_{L^*} = 1$. □

Corollary 3.34. *For all lattices $\mathcal{L} \in \mathrm{Latt}_K$, one has $[\mathcal{O}_K : \mathcal{L}] \cdot [\mathcal{O}_K, \mathcal{L}^*] = \mathbf{N}(\mathcal{L}) \cdot \mathbf{N}(\mathcal{L}^*) = \frac{1}{|d_K|}$.*

3.9 Bounds for the index $[\mathfrak{b} : \mathfrak{a}\mathfrak{b}]$ in a general order

Let

$$I(\mathcal{O}) := \{\mathfrak{a} \subseteq \mathcal{O} : \mathfrak{a} \text{ is a non-zero } \mathcal{O}\text{-ideal}\}. \tag{3.16}$$

In other words, $I(\mathcal{O})$ is the (abelian) monoid of integral $\mathcal{O}$-ideals. If $\mathfrak{a}, \mathfrak{b} \in I(\mathcal{O})$ and $\mathfrak{a} \neq \mathcal{O}$ then it follows from Nakayama's lemma that

$$\mathfrak{a}\mathfrak{b} \subsetneq \mathfrak{b}. \tag{3.17}$$

In particular $I(\mathcal{O})$ is always a torsion free abelian monoid in the sense that if $\mathfrak{a} \in I(\mathcal{O})$ and $\mathfrak{a}^n = \mathcal{O}$ for some $n \in \mathbb{Z}_{\geq 1}$ then necessarily $\mathfrak{a} = \mathcal{O}$. Given an $\mathfrak{a} \in I(\mathcal{O})$ let us define

$$n_{\mathfrak{a}} := \min\{n \in \mathbb{Z}_{>0} : n \in \mathfrak{a}\} \in \mathfrak{a}. \tag{3.18}$$

Let $\mathfrak{a}, \mathfrak{b} \in I(\mathcal{O})$ and set $n := n_{\mathfrak{b}}$. From the inclusions $\mathfrak{a} \supseteq \mathfrak{a}\mathfrak{b} \supseteq n\mathfrak{a}$ we deduce the following upper bound for the index $[\mathfrak{a} : \mathfrak{a}\mathfrak{b}]$:

$$[\mathfrak{a} : \mathfrak{a}\mathfrak{b}] \Big| n^g. \tag{3.19}$$

In particular, if $\mathfrak{p} \in I(\mathcal{O})$ is a prime ideal above $p\mathbb{Z}$ then necessarily we have

$$[\mathcal{O} : \mathfrak{p}] \Big| p^g. \tag{3.20}$$

When either $\mathfrak{a}$ or $\mathfrak{b}$ is $\mathcal{O}$-invertible one can say more.

Proposition 3.35. *Let $\mathcal{O} \subseteq \mathcal{O}_K$ be an order and let $\mathfrak{a}, \mathfrak{b} \in \mathrm{Latt}_{\mathcal{O}}$.*

(i) If $\mathfrak{a}$ is $\mathcal{O}$-invertible then $\mathfrak{a}/\mathfrak{a}\mathfrak{b} \simeq \mathcal{O}/\mathfrak{b}$ (where $\simeq$ is a non-canonical isomorphism of $\mathbb{Z}$-modules).

(ii) If either $\mathfrak{a}$ or $\mathfrak{b}$ is $\mathcal{O}$-invertible then $[\mathcal{O} : \mathfrak{a}] \cdot [\mathcal{O} : \mathfrak{b}] = [\mathcal{O} : \mathfrak{a}\mathfrak{b}]$.

Proof We have $[\mathcal{O} : \mathfrak{a}\mathfrak{b}] = [\mathcal{O} : \mathfrak{a}][\mathfrak{a} : \mathfrak{a}\mathfrak{b}]$ and therefore (ii) follows from (i). It remains to show (i) namely that there exists an abelian group isomorphism (non-canonical!) between the two finite $\mathbb{Z}$-modules $\mathfrak{a}/\mathfrak{a}\mathfrak{b}$ and $\mathcal{O}/\mathfrak{b}$ if $\mathfrak{a}$ is $\mathcal{O}$-invertible. Let $p \in \mathbb{Z}_{\geq 2}$ be a prime and set $S_p := \mathcal{O}\backslash(\mathfrak{p}_1 \cup \mathfrak{p}_2 \cup \ldots \cup \mathfrak{p}_e)$, where $\mathfrak{p}_i$'s are the distinct prime ideals of $\mathcal{O}$ above $p\mathbb{Z}$. The set S_p is multiplicatively closed and the localized ring $\mathcal{O}_p := S_p^{-1}\mathcal{O}$ is a semi-local ring. Since $\mathfrak{a}$ is $\mathcal{O}$-invertible, it follows that $\mathfrak{a}_p := S_p^{-1}\mathfrak{a}$ is a principal $\mathcal{O}_p$-module. Therefore, there exists $\pi_p \in \mathcal{O}_p$, such that $\mathfrak{a}_p = \pi_p\mathcal{O}_p$. Since $\mathcal{O}_p$ is a flat $\mathcal{O}$-module, we have $\mathfrak{a}_p/\mathfrak{a}_p\mathfrak{b}_p \simeq (\mathfrak{a}/\mathfrak{a}\mathfrak{b})_p$ and $\mathcal{O}_p/\mathfrak{b}_p \simeq (\mathcal{O}/\mathfrak{b})_p$. Now consider the map $\varphi_p : \mathcal{O}_p/\mathfrak{b}_p \to \mathfrak{a}_p/\mathfrak{a}_p\mathfrak{b}_p$, given by $x+\mathfrak{b}_p \mapsto x\pi_p+\mathfrak{a}_p\mathfrak{b}_p$. It follows that φ_p is an $\mathcal{O}_p$-module isomorphism. In particular, we have

$$(p\text{-primary subgroup of } \mathfrak{a}/\mathfrak{a}\mathfrak{b}) \simeq (\mathfrak{a}/\mathfrak{a}\mathfrak{b})_p \simeq (p\text{-primary subgroup of } \mathcal{O}/\mathfrak{b}\ )\simeq (\mathcal{O}/\mathfrak{b})_p$$

Finally, since p was arbitrary, it follows that $\mathfrak{a}/\mathfrak{a}\mathfrak{b}$, as a finite $\mathbb{Z}$-module, is isomorphic to $\mathcal{O}/\mathfrak{b}$. □

Remark 3.36. Working a bit more carefully, one can show that the above map φ is actually a map of $\mathcal{O}$-modules (see Proposition B.2 of [16]).

3.10 Primary factorization in orders

The primary decomposition theorem for Noetherian rings, when specialized to one dimensional Noetherian domains gives the following:

Theorem 3.37. *Let A be a Noetherian domain of dimension 1. Then every non-zero ideal $\mathfrak{a}$ in A can be uniquely written, up to ordering, as*

$$\mathfrak{a} = \mathfrak{q}_1 \ldots \mathfrak{q}_r \tag{3.21}$$

where $\mathfrak{q}_i$ are primary ideals and where the associated prime ideals $\mathfrak{p}_i = \mathrm{rad}(\mathfrak{q}_i)$ are distinct.

Proof The existence of such a factorization is a direct consequence of the primary decomposition theorem but the unicity is more subtle and uses the fact that the isolated primary components of $\mathfrak{a}$ are uniquely determined by $\mathfrak{a}$ (see Corollary 4.11 of [1]). For a complete proof of Theorem 3.37 see for example Proposition 9.1 of [1]. □

Theorem 3.37 applies in particular to orders.

Remark 3.38. One can show that a prime ideal $\mathfrak{p} \subseteq \mathcal{O}$ is regular (see Definition 3.17) if and only if each integral $\mathfrak{p}$-primary ideal of $\mathcal{O}$ is a power of $\mathfrak{p}$. When $\mathfrak{p}$ is regular we know from Theorem 3.15 that $\mathfrak{p}$ is $\mathcal{O}$-invertible. For the other direction, if all the $\mathfrak{p}$-primary ideals are powers of $\mathfrak{p}$ then the local ring $\mathcal{O}_\mathfrak{p}$ admits a discrete valuation and in particular the localization $\mathfrak{p}_\mathfrak{p}$ is free of rank 1 over $\mathcal{O}_\mathfrak{p}$. Moreover, if $\mathfrak{q} \neq \mathfrak{p}$ is prime, then the localization $\mathfrak{p}_\mathfrak{q} = \mathcal{O}_\mathfrak{q}$ is again free of rank one over $\mathcal{O}_\mathfrak{q}$. Thus, applying Theorem 3.11 we find that $\mathfrak{p}$ is $\mathcal{O}$-invertible.

It is easy to deduce some upper bound for the number of primary factors which appear in the primary decomposition of $\ell\mathcal{O}$ where $\ell \in \mathbb{Z}$ is a prime number. Let us give such upper an bound which is relevant for bounding the size of the fibers of the map $\mathrm{Spec}(\mathcal{O}) \to \mathrm{Spec}(\mathbb{Z})$.

Proposition 3.39. *Let $\ell \in \mathbb{Z}$ be a prime number and let $\ell\mathcal{O} = \mathfrak{q}_1 \cdots \mathfrak{q}_r$ be the primary factorization of $\ell\mathcal{O}$ where $\mathfrak{p}_i = \mathrm{rad}(\mathfrak{q}_i)$ are the distinct prime ideals supported on $\ell\mathcal{O}$. Then $r \leq g$.*

Proof It follows from (3.17) that we have the following chain of proper inclusions

$$\mathcal{O} \supsetneqq I_1 \supsetneqq I_2 \supsetneqq \cdots \supseteq I_r = \ell\mathcal{O} \tag{3.22}$$

where $I_k = \mathfrak{q}_1 \cdots \mathfrak{q}_k$ for $1 \leq k \leq r$. From (3.17), we know on one hand that $\ell^{f_k} \Big| [I_k : I_{k+1}]$ for some $f_k \geq 1$ whenever $1 \leq k \leq r-1$. On the other hand, we also know that $[\mathcal{O} : \ell\mathcal{O}] = \ell^g$ and therefore we must have $r \leq g$. □

3.11 The contraction and extension maps for the integral extension $\mathcal{O} \subseteq \mathcal{O}_K$

Using the notation of [16], given an order $\mathcal{O} \subseteq K$ and an $\mathcal{O}$-ideal $\mathfrak{m} \subseteq \mathcal{O}$, we let

$$I_{\mathfrak{m}}(\mathcal{O}) := \{\mathfrak{a} \subseteq \mathcal{O} : \mathfrak{a} \text{ is an } \mathcal{O}\text{-ideal and } \mathfrak{a} + \mathfrak{m} = \mathcal{O}\}. \tag{3.23}$$

So $I_{\mathfrak{m}}(\mathcal{O})$ is the (abelian) monoid of integral $\mathcal{O}$-ideals which are coprime to $\mathfrak{m}$. When $\mathfrak{m} = \mathcal{O}$ we have $I_{\mathfrak{m}}(\mathcal{O}) = I(\mathcal{O})$.

The ring homomorphism $\mathcal{O} \subseteq \mathcal{O}_K$ gives rise to the usual extension and contraction maps

$$\begin{aligned} \mathrm{ext} : I(\mathcal{O}) &\to I(\mathcal{O}_K) \\ \mathfrak{a} &\mapsto \mathrm{ext}(\mathfrak{a}) = {}^e\mathfrak{a} := \mathfrak{a}\mathcal{O}_K \end{aligned}$$

and

$$\begin{aligned} \mathrm{con} : I(\mathcal{O}_K) &\to I(\mathcal{O}) \\ \mathfrak{a} &\mapsto \mathrm{con}(\mathfrak{a}) = {}^c\mathfrak{a} := \mathfrak{a} \cap \mathcal{O} \end{aligned}$$

It straightforward to see that the extension map is always a monoid homomorphism but in general the contraction map may fail to be a monoid morphism (see [16]). However, we have the following:

Proposition 3.40. *Let $\mathfrak{f} := \mathfrak{c}_{\mathcal{O}}$ be the conductor of $\mathcal{O}$. Then the maps* $\mathrm{ext} : I_{\mathfrak{f}}(\mathcal{O}) \to I_{\mathfrak{f}}(\mathcal{O}_K)$ *and* $\mathrm{con} : I_{\mathfrak{f}}(\mathcal{O}_K) \to I_{\mathfrak{f}}(\mathcal{O})$ *are monoid bijections which are inverse to one another.*

Proof This is a special case of Lemma 3.7 of [16] which deals with an arbitrary extension of orders $\mathcal{O} \subseteq \mathcal{O}'$ and where $\mathfrak{f} = \mathfrak{f}_{\mathcal{O}'}(\mathcal{O})$ is the relative conductor ideal. The above proposition follows directly from theirs by taking $\mathcal{O}' = \mathcal{O}_K$. □

Remark 3.41. Proposition 3.40 is not so surprising in light of the following. By definition $\mathfrak{f} = \mathfrak{c}_{\mathcal{O}}$ is the largest $\mathcal{O}_K$-ideal contained in $\mathcal{O}$. In particular, if h_K denotes the class number of K then $\mathfrak{f}^{h_K} = \lambda\mathcal{O}_K$ for some $\lambda \in \mathcal{O}_K$ which is supported only on the prime ideals of $\mathcal{O}_K$ which divide $\mathfrak{f}$. Since $\lambda\mathcal{O}_K \subseteq \mathcal{O}$ it follows readily that $\mathcal{O}_K[\frac{1}{\lambda}] = \mathcal{O}[\frac{1}{\lambda}]$.

References

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra.* Addison-Wesley Series in Mathematics. Westview Press, Boulder, CO, economy edition, 2016. For the 1969 original see [MR0242802].

[2] Borevich and Shafarevich. *Number theory.* Academic Press, 1966.

[3] H. Chapdelaine. Functional equation for partial zeta functions twisted by additive characters. *Acta Arith.*, 136:213–228, 2009.

[4] H. Chapdelaine. Some arithmetic properties of partial zeta functions weighted by sign characters,. *J. Number Theory*, 130:803–814, 2010.

[5] H. Chapdelaine. GL_2 real analytic Eisenstein series twisted by parameter matrices and multiplicative integral quasi-characters. pages 1–148, 2016. https://arxiv.org/abs/1607.02910.

[6] H. Chapdelaine. Lattice zeta functions for number fields. pages 1–74, 2024. *submitted for publication.*

[7] H. Chapdelaine. Signature lattice zeta functions and Eisenstein series over totally real fields. pages 1–35, 2024. *In preparation.*

[8] K. Conrad. The conductor ideal of an order. *Expository paper available on his website*, pages 1–20, 2012.

[9] David A. Cox. *Primes of the form* x^2+ny^2. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.

[10] D. Dummit and R. Foote. *Abstract algebra.* Wiley, 3rd edition, 2003.

[11] Cornelius Greither. On the two generator problem for the ideals of a one-dimensional ring. *J. Pure Appl. Algebra*, 24(3):265–276, 1982.

[12] Stark H.M. Values of L-functions at $s = 1$, I L-functions for quadratic forms. *Advances in Math.*, 7:301–343, 1971.

[13] Stark H.M. L-functions at $s = 1$, II Artin L-functions with rational characters. *Advances in Math.*, 17:60–92, 1975.

[14] Stark H.M. L-functions at $s = 1$, III Totally real fields and hilbert's twelfth problem. *Advances in Math.*, 22:64–84, 1976.

[15] Stark H.M. L-functions at $s = 1$, IV First derivatives at $s = 0$. *Advances in Math.*, 35:197–235, 1980.

[16] Gene S. Kopp and Jeffrey C. Lagarias. Class field theory for orders of number fields. *arxiv*, pages 1–47, 2022.

[17] S. Lang. *Elliptic Functions, 2^{nd} Edition.* Springer-Verlag, New-York, 1994.

[18] Chang Lv and YingPu Deng. On orders in number fields: Picard groups, ring class fields and applications. *Sci. China Math.*, 58(8), 2015.

[19] M. Ram Murty and Jody Esmonde. *Problems in algebraic number theory*, volume 190 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 2005.

[20] J. Neukirch. *Algebraic number theory.* Springer-Verlag Berlin Heidelberg, 1999.

[21] J. Rotman. *Advanced Modern Algebra.* Prentice Hall, 2002.

[22] Peter Stevenhagen. The arithmetic of number rings. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 209–266. Cambridge Univ. Press, Cambridge, 2008.

[23] Hans Zassenhaus. Neuer Beweis der Endlichkeit der Klassenzahl bei unimodularer Äquivalenz endlicher ganzzahliger Substitutionsgruppen. *Abh. Math. Sem. Univ. Hamburg*, 12(1):276–288, 1937.