university of groningen

faculty of science and engineering

Arakelov and Minkowski Theory for S-Integers

Master Project Mathematics

October 2024

Student: N. Veltman

First supervisor: Prof. J.S. Müller

Second supervisor: Prof. J. Top

Abstract

The infrastructure is a group-like structure inside the equivalence class of the unit element of the class group of a real quadratic number field. It induces an algorithm that can compute the regulator of the real quadratic number field. Among other things, this thesis explores the potential of giving an Arakelov theoretical description of the infrastructure for so-called fake real quadratic orders; a specific type of S-integers in an imaginary quadratic number field. To see the utility of Arakelov theory, this thesis describes the Arakelov theoretical description of the original infrastructure. Moreover, it extends Arakelov theory to S-integers. This includes the study of the Arakelov S-class group. Two isomorphic groups are constructed, and the topology is examined. Furthermore, two definitions for reduced Arakelov S-divisors are suggested. To support Arakelov theory for S-integers, also Minkowski theory has been studied for these rings. Namely, this thesis shows how non-zero fractional ideals of S-integers can be viewed as lattices in the S-Minkowski space. Furthermore, it includes an analogue of Minkowski's Convex Body Theorem for the S-Minkowski space. To talk about lattices in this space, the structure of lattices in locally compact groups is examined. This includes the full description of fundamental regions and covolumes of lattices.

Contents

Introduction

Let K be a quadratic number field and Cl_K its class group. If K is imaginary, every equivalence class in Cl_K contains a unique *reduced* integral ideal. If K is real, this is no longer the case. Then every equivalence class in Cl_K contains a finite number of reduced integral ideals, called a *cycle*. In 1972, Daniel Shanks noted that the cycle corresponding to the unit element of Cl_K attains a group-like structure (see [Sha72]). This is known as the *infrastructure* of K. A possible failure of the associative law prevents the infrastructure from being an abelian group. Using a distance formula and his Baby-Step Giant-Step Algorithm on the infrastructure, Shanks was able to design an algorithm that can compute the regulator of the real quadratic number field. While Shanks described this phenomenon also using binary quadratic forms, it was Hendrik Lenstra who introduced a group on binary quadratic forms, that could be used to make Shanks' observations precise (see [Len82]). The ideas were generalized to any number field by Johannes Buchmann in 1990 (see [Buc90]). Buchmann's algorithm can compute the class group and regulator of any number field in subexponential running time, under reasonable assumptions. Now, Shanks' and Buchmann's algorithms were examined using Arakelov theory for number fields by René Schoof in 2008 (see [Sch08]).

This is one part of the historical and motivational background. On the other hand, we have the *fake real quadratic orders*. To introduce them, consider the *rings of S-integers*. These are subrings of a number field K defined by

$$\mathcal{O}_{K,S} := \{x \in K : \mathrm{ord}_{\mathfrak{p}}(x) \geq 0 \text{ for all } \mathfrak{p} \notin S\},$$

for some finite set S of non-zero prime ideals of $\mathcal{O}_K$. Now, consider an imaginary quadratic number field of discriminant $d \in \mathbb{Z}$. Furthermore, take an odd prime $q \in \mathbb{Z}$ such that d is a square modulo q. Then it follows that

$$q\mathcal{O}_K = \mathfrak{q}\overline{\mathfrak{q}},$$

for some non-zero prime ideal $\mathfrak{q} \subseteq \mathcal{O}_K$. If we take $S = \{\mathfrak{q}\}$, we obtain a subring of K by $\mathcal{O}_{d,q} := \mathcal{O}_{K,S}$. Henri Cohen observed that these subrings behave similarly to the ring of integers of a real quadratic number field. For that reason, Cohen called these types of S-integers fake real quadratic orders. They are studied in great detail by Richard Micheal Oh and Hongyan Wang (see [Oh14], [Wan17]). Oh discusses the potential of an analogue of the infrastructure for fake real quadratic orders. It was Wang that was able to describe such an infrastructure. However, it did not lead to a faster algorithm that could compute the regulator of a fake real quadratic order. In this case, the regulator is defined as $R_{d,q} := \log|\varepsilon_q|_\infty$, where ε_q is the generator of the unit group of $\mathcal{O}_{d,q}$. Equivalently, the element ε_q is the generator of the principal ideal $\mathfrak{q}^n$, where $n \in \mathbb{Z}_{>0}$ is the order of $\mathfrak{q}$ in the class group of K.

The goal of this thesis is to combine these two concepts. Schoof successfully described the infrastructure using Arakelov theory. Therefore, this might be the right setting to design the infrastructure for fake real quadratic orders. However, this thesis does not include such a description. Instead, it gives all the ingredients that are needed for a description. Moreover, it explains the obstacles that come along.

While Schoof describes the infrastructure using Arakelov theory, his paper mostly focuses on the Arakelov theoretical description of Buchmann's algorithm. Therefore, the first step is to give a full Arakelov theoretical description of the original infrastructure that is built on the ideas of Schoof. This is given in Chapter 4 of this thesis. It includes a short overview of Arakelov theory for any number field as described in Schoof's paper. Arakelov theory for number fields makes use of *Arakelov divisors*. They are an analogue of divisors on a complete projective curve. Instead of points on the curve, it uses the places of the number field. One can give an analogue of the Picard group, which is called the *Arakelov class group*. So-called *reduced* Arakelov divisors play a major role in the description of the infrastructure. They are the analogue of reduced integral ideals. One of the key outcomes of this chapter is the development of a reduction algorithm for Arakelov divisors in a real quadratic number field (see Algorithm 4.3.8). Given an Arakelov divisor, it returns a reduced Arakelov divisor that is *ideal equivalent*. This equivalence relationship is the same as saying that two Arakelov divisors lie on the same connected component of the Arakelov class group. Using the ideas of the reduction algorithm,

we can prove that any reduced Arakelov divisor induces a complete set of distinct reduced Arakelov divisors that are ideal equivalent (see Theorem 4.3.18). This is the analogue of a cycle of the class group, which we will call an *Arakelov cycle*. We describe a distance formula that gives the notion of distance between ideal equivalent Arakelov divisors. Moreover, it recovers Lenstra's distance formula (see Corollary 4.3.27). We end this chapter by constructing a group-like structure on the Arakelov cycle induced by the zero Arakelov divisor. This is the Arakelov theoretical description of the infrastructure of a real quadratic number field. Finally, applying the ideas of the Baby-Step Giant-Step Algorithm to the infrastructure, we were able to design an algorithm that can compute the regulator of a real quadratic number field (see Algorithm 4.3.43).

We aim to give an Arakelov theoretical description of the infrastructure for fake real quadratic orders. Therefore, we first have to define Arakelov theory for these subrings. But, why not generalize it immediately to any ring of S-integers of any number field? This is what happens in Chapter 5 of this thesis. We extend the notion of Arakelov divisors to so-called *Arakelov S-divisors*. One can define *principal Arakelov S-divisors* that depend on the elements in the number field. They form a subgroup of the group of Arakelov S-divisors. They induce a quotient group, called the *Arakelov S-class group*. This is the extension of the Arakelov class group. The main part of this chapter is spent on the analysis of this last group. We show how the group is isomorphic to the group of *metrized S-line bundles* (see Theorem 5.2.18). These are projective $\mathcal{O}_{K,S}$-modules of rank 1 with some additional structure given by a $K_{\mathbb{R}}$-*metric*. Moreover, we construct a group of *ideal S-lattices* that is also isomorphic to the Arakelov S-class group (see Theorem 5.2.26). Ideal S-lattices are structures that behave like fractional ideals and lattices simultaneously. Furthermore, we investigate the topology of the Arakelov S-class group. We show how its connected components are metrizable (see Theorem 5.3.16). Lastly, we propose two generalizations of reduced Arakelov divisors. Moreover, we show how in both cases there are only a finite number of reduced Arakelov S-divisors (see Theorem 5.4.10 and 5.4.17).

While trying to generalize reduced Arakelov divisors, some problems came into play. Reduced Arakelov divisors depend on the notion of *minimal elements* in a fractional ideal. The existence of a minimal element is guaranteed since any fractional ideal of $\mathcal{O}_K$ forms a lattice in the Minkowski space $K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R}$. This was the motivation to study Minkowski theory for the rings of S-integers. We aimed to find a space where fractional ideals of $\mathcal{O}_{K,S}$ can be viewed as lattices. In contrast to the space $K_{\mathbb{R}}$, the desired space was no longer a Euclidean space. Therefore, we could not use the classical theory of lattices in Euclidean spaces. We had to extend the theory of lattices to locally compact groups. This is done in Chapter 2 of this thesis. While this theory can be found in the literature, it is often incomplete. We aim to give the full theory of lattices in locally compact groups. From the formal definition of lattices to discrete and co-compact subgroups in abelian *L-groups* (see Theorem 2.6.4), from fundamental regions to its existence, and from Haar measures to covolumes.

After the general theory of lattices in locally compact groups was examined, we could finally investigate Minkowski theory for the rings of S-integers. This is given in Chapter 3. It starts with a short overview of some results on S-integers that are important along the way. This includes their structure, prime ideals, fractional ideals, and units. Then we show that any non-zero fractional ideal of $\mathcal{O}_{K,S}$ can be viewed as a lattice in the *S-Minkowski space* K_S (see Theorem 3.4.6). This space is an extension of $K_{\mathbb{R}}$ that takes the completions of K with respect to the prime ideals (finite places) of S into account. The covolume of a lattice corresponding to a fractional ideal can be related to the covolume of the lattice implied by $\mathcal{O}_{K,S}$ itself. Therefore, we describe a fundamental region of $\mathcal{O}_{K,S}$ and compute its covolume (see Theorem 3.4.3). Furthermore, we prove an analogue of the Heine-Borel Theorem and Minkowski's Convex Body Theorem for the space K_S (see Theorem 3.3.12 and 3.3.23).

We start this thesis with some preliminaries in Chapter 1. They make sure that terminology and notation are consistent throughout this thesis, and known to the reader. We end this thesis with a more specific description of fake real quadratic orders in Chapter 6. Furthermore, we describe some ideas and obstacles of a potential Arakelov theoretical description of the infrastructure for fake real quadratic orders.

Acknowledgements

Before we dive into mathematics, I would like to take a moment to thank my first supervisor Professor Steffen Müller. First of all, he was the one who noticed that it could be interesting to combine the infrastructure, Arakelov theory, and fake real quadratic orders. It turns out, he was certainly right about this. This research has been a great journey with beautiful mathematics. Within my research, he allowed me to study the things I found interesting. This was a great pleasure. Moreover, he always gave me the feeling that I was going in the right direction. He supported this research with many suggestions to overcome certain issues. I like the way we had our meetings, and I look forward to the possibility of working together again in the future.

I also would like to thank my second supervisor Professor Jaap Top. While he was not much involved during the research, he was always approachable and ready to help. He also supported me with physical literature that could not be found on the internet. This has helped progress in several parts of this research.

I thank Professor Florian Hess and Professor René Schoof for the useful meetings that we had at the University of Groningen. Lastly, I would like to thank Professor Koen de Boer. He clarified some parts of his work, which helped me to solve some problems in the theory of ideal S-lattices.

1 Preliminaries

In this chapter, we gave a brief overview of basic definitions and results from (algebraic) number theory, commutative algebra, and measure theory. This ensures consistent notation and terminology throughout this thesis. Furthermore, it gives the reader the necessary background to understand this thesis. Except for the notation, the content of Sections 1.1, 1.2, 1.4, and 1.5 are known to those that are familiar with (algebraic) number theory and commutative algebra. Therefore, those readers are safe to skip these sections. However, we advise the reader to read Section 1.3, 1.7, and 1.8 as they are the motivation to study Chapter 2, 3, and 4.

Remark 1.0.1. Throughout this thesis, the Axiom of Choice is assumed to hold. ♦

1.1 Dedekind Domains

The definitions and results stated in this section are basics in (algebraic) number theory. Therefore, they can be found in any book or lecture notes in this area. We will mostly be using the convention from [Neu99].

Throughout this section, let $\mathcal{O}$ be a Dedekind domain and F its field of fractions.

Definition 1.1.1. An additive subgroup $J \subseteq \mathcal{O}$ is called an *integral ideal* of $\mathcal{O}$ if $ax \in J$ for all $x \in J$ and $a \in \mathcal{O}$. An $\mathcal{O}$-submodule I of F is called a *fractional ideal* of $\mathcal{O}$ if there exists some $a \in \mathcal{O}$ such that aI is an integral ideal of $\mathcal{O}$. The set of fractional ideals of $\mathcal{O}$ is denoted by $\mathrm{Id}_{\mathcal{O}}$. A *principal fractional ideal* is a fractional ideal of the form $x\mathcal{O}$ for some $x \in F$.

Any integral ideal is a fractional ideal but the converse is not true. The following definition will be used later in this thesis.

Definition 1.1.2. Let I be a fractional ideal of $\mathcal{O}$. An element $x \in I$ is called *primitive* if there does not exist an $m \in \mathbb{Z}_{>1}$ such that $x \in mI$.

Since $\mathcal{O}$ is a Dedekind domain, the set $\mathrm{Id}_{\mathcal{O}}$ forms an abelian group under multiplication. More precisely, the unit element is given by $\mathcal{O}$ itself, and for any fractional ideal I of $\mathcal{O}$ the inverse is given by

$$I^{-1} := \{x \in F : xI \subseteq \mathcal{O}\}. \tag{1}$$

One can find this result in Proposition 3.8 of Chapter I in [Neu99]. The subset of principal fractional ideals form a subgroup of this abelian group.

Definition 1.1.3. The quotient group of $\mathrm{Id}_{\mathcal{O}}$ by its subgroup of principal fractional ideals is called the *class group* of $\mathcal{O}$. Fractional ideals of $\mathcal{O}$ are said to be *equivalent* if they define the same equivalence class in the class group of $\mathcal{O}$. For $I \in \mathrm{Id}_{\mathcal{O}}$ we denote its equivalence class in the class group by $[I]$.

Fractional ideals I and J of $\mathcal{O}$ are equivalent if there exists some $x \in F^*$ such that $I = xJ$. Another consequence of $\mathcal{O}$ being a Dedekind domain is that any fractional ideal of $\mathcal{O}$ can be uniquely written as a finite product of non-zero prime ideals of $\mathcal{O}$ (see [Neu99, Corollary 3.9, Chapter I]). We denote the set of prime ideals of $\mathcal{O}$ by $\mathrm{Spec}(\mathcal{O})$. So for any $I \in \mathrm{Id}_{\mathcal{O}}$ and non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}$ there exists an $n_{\mathfrak{p}} \in \mathbb{Z}$ such that

$$I = \prod_{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}) \setminus \{(0)\}} \mathfrak{p}^{n_{\mathfrak{p}}}. \tag{2}$$

If I is an integral ideal of $\mathcal{O}$, then $n_{\mathfrak{p}} \in \mathbb{Z}_{\geq 0}$ for all non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}$ (see [Neu99, Theorem 3.3, Chapter I]).

Proposition 1.1.4. Any prime ideal of $\mathcal{O}$ is maximal.

Proof. This is a consequence from the fact that a Dedekind domain is a domain of dimension 1 (see [AM69, Theorem 9.3]). □

Remark 1.1.5. We denote the integer $n_{\mathfrak{p}}$ for I, corresponding to the non-zero prime ideal $\mathfrak{p}$, by $\mathrm{ord}_{\mathfrak{p}}(I)$. So for any non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}$ we get a group homomorphism $\mathrm{ord}_{\mathfrak{p}}\colon \mathrm{Id}_{\mathcal{O}} \to \mathbb{Z}$. ♦

Definition 1.1.6. Let S be a finite set of non-zero prime ideals of $\mathcal{O}$ and $I \in \mathrm{Id}_{\mathcal{O}}$. Then I is said to be *coprime* to S if $\mathrm{ord}_{\mathfrak{p}}(I) = 0$ for all $\mathfrak{p} \in S$.

The analogue of this definition for the rationals numbers is saying that a rational number $\frac{a}{b} \in \mathbb{Q}$ is coprime to a set S of prime numbers if $p \nmid a$ and $p \nmid b$ for all $p \in S$.

A consequence of the unique factorization of fractional ideals is that we can speak about division.

Definition 1.1.7. Let $I, J \in \mathrm{Id}_{\mathcal{O}}$. Then I is said to *divide* J if $J \subseteq I$. If I divides J, this is denoted by $I|J$.

Proposition 1.1.8. Let $I, J \in \mathrm{Id}_{\mathcal{O}}$.

i.) Then $I|J$ if and only if there exists some integral ideal A of $\mathcal{O}$ such that $IA = J$.

ii.) Then $I|J$ if and only if $\mathrm{ord}_{\mathfrak{p}}(I) \leq \mathrm{ord}_{\mathfrak{p}}(J)$ for all non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}$.

Proof. To show Statement (i.), assume that $I|J$. Then $J \subseteq I$, and so $JI^{-1} \subseteq II^{-1} = \mathcal{O}$. Then $A := JI^{-1}$ is an integral ideal and $IA = I(JI^{-1}) = J$. Conversely, suppose that there exists some integral ideal A of $\mathcal{O}$ such that $IA = J$. Then $J = IA \subseteq I\mathcal{O} \subseteq I$, and so $I|J$.

Now, for any non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}$, we have the group homomorphism $\mathrm{ord}_{\mathfrak{p}}$. Then $IA = J$ if and only if $\mathrm{ord}_{\mathfrak{p}}(J) = \mathrm{ord}_{\mathfrak{p}}(IA) = \mathrm{ord}_{\mathfrak{p}}(I) + \mathrm{ord}_{\mathfrak{p}}(A) \geq \mathrm{ord}_{\mathfrak{p}}(I)$, using the fact that A is an integral ideal. Therefore, Statement (ii.) follows directly from Statement (i.). □

Definition 1.1.9. For any integral ideal I of $\mathcal{O}$, the *(absolute) norm* of I is defined by

$$N_{\mathcal{O}}(I) := \#(\mathcal{O}/I) \in \mathbb{Z}_{>0} \cup \{\infty\}.$$

Proposition 1.1.10. Let I, J be integral ideals of $\mathcal{O}$.

i.) Then $N_{\mathcal{O}}(IJ) = N_{\mathcal{O}}(I)N_{\mathcal{O}}(J)$.

ii.) Let $k \in \mathbb{Z}_{>0}$. Then the number of integral ideals I of $\mathcal{O}$ such that $N_{\mathcal{O}}(I) < k$ is finite.

This result can be found in Theorem 3.29 of [Kha22]. Due to Proposition 1.1.10 (i.), we can extend the notion of the norm to any fractional ideal of $\mathcal{O}$.

Definition 1.1.11. For any $I \in \mathrm{Id}_{\mathcal{O}}$ with unique factorization as in (2), we define the *(absolute) norm* of I by $N_{\mathcal{O}}(I) := \prod_{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}) \setminus \{(0)\}} N_{\mathcal{O}}(\mathfrak{p})^{n_{\mathfrak{p}}}$.

The norm defines a group homomorphism $N_{\mathcal{O}}\colon \mathrm{Id}_{\mathcal{O}} \to \mathbb{Q}^*$.

Let $L|F$ be a finite field extension. Moreover, we assume that this extension is separable.

Definition 1.1.12. For any $x \in L$, the *trace*, denoted by $\mathrm{Tr}_{L|F}(x)$, and *norm*, denoted by $\mathrm{N}_{L|F}(x)$, are respectively defined by the trace and determinant of the F-linear transformation $T_x\colon L \to L$ given by $y \mapsto xy$.

Remark 1.1.13. Notice that $\mathrm{Tr}_{L|F}(x), \mathrm{N}_{L|F}(x) \in F$ for all $x \in L$, since the trace and determinant of an F-linear transformation is always in F. ♦

Let $\overline{F}$ denote an algebraic closure of F.

Definition 1.1.14. A map $f : L \to \overline{F}$ is called an *F-embedding* of L if it is an injective ring homomorphism and the identity map on $F \subseteq L$.

The following result is Proposition 2.6 of Chapter I in [Neu99].

Proposition 1.1.15. For any $x \in L$, one has

$$\mathrm{Tr}_{L|F}(x) = \sum_{\sigma} \sigma(x), \qquad \mathrm{N}_{L|F}(x) = \prod_{\sigma} \sigma(x),$$

where the sum (resp. product) runs over all F-embeddings σ of L.

Until now, we have considered a Dedekind domain $\mathcal{O}$ and its field of fractions F. Now, suppose that $L|F$ is a separable finite field extension and $\mathfrak{O}$ the integral closure of $\mathcal{O}$ in L. Then by Proposition 8.1 in Chapter I of [Neu99], the ring $\mathfrak{O}$ is also a Dedekind domain. We denote this construction of Dedekind domains by $\mathfrak{O}|\mathcal{O}$.

Definition 1.1.16. The fractional ideal

$$\mathfrak{C}_{\mathfrak{O}|\mathcal{O}} := \{x \in L : \mathrm{Tr}_{L|F}(x\mathfrak{O}) \subseteq \mathcal{O}\}$$

of $\mathfrak{O}$ is called the *inverse different* of $\mathfrak{O}|\mathcal{O}$. Its inverse $\mathfrak{D}_{\mathfrak{O}|\mathcal{O}} := \mathfrak{C}_{\mathfrak{O}|\mathcal{O}}^{-1}$ is called the *different* of $\mathfrak{O}|\mathcal{O}$.

For any $x \in \mathfrak{O}$, one has $\mathrm{Tr}_{L|F}(x) \in \mathcal{O}$ (see [Neu99, Page 12]). Therefore, we have $\mathfrak{O} \subseteq \mathfrak{C}_{\mathfrak{O}|\mathcal{O}}$. Consequently, the different of $\mathfrak{O}|\mathcal{O}$ is an integral ideal of $\mathfrak{O}$. By Remark 1.1.13, we know that the image of the norm of any element in L is in F. Therefore, the following definition makes sense.

Definition 1.1.17. For any fractional ideal I of $\mathfrak{O}$, the *relative norm* of I is defined by the fractional ideal $N_{\mathfrak{O}|\mathcal{O}}(I)$ of $\mathcal{O}$ generated by the images of the norm of the elements in I. More precisely, one has $N_{\mathfrak{O}|\mathcal{O}}(I) := \{N_{L|F}(x) : x \in I\}\mathcal{O}$.

One can show that the relative norm is a group homomorphism $N_{\mathfrak{O}|\mathcal{O}} \colon \mathrm{Id}_{\mathfrak{O}} \to \mathrm{Id}_{\mathcal{O}}$ (see [Sut24, Proposition 6.7]). The lecture notes [Sut24] also study some equivalent representations of the relative norm. Since we are not interested in them, we refer to these lecture notes.

Definition 1.1.18. The fractional ideal $N_{\mathfrak{O}|\mathcal{O}}(\mathfrak{D}_{\mathfrak{O}|\mathcal{O}})$ of $\mathcal{O}$ is called the *relative discriminant* of $\mathfrak{O}|\mathcal{O}$.

1.2 Number Fields

Like the previous section, the definitions and results stated in this section are basics in (algebraic) number theory. We will mostly be using the convention from [Neu99].

Throughout this section, consider the field extension $K|\mathbb{Q}$, that is, the field K is an (algebraic) number field. Throughout this thesis, let the degree of K be denoted by $n \in \mathbb{Z}_{>0}$, unless stated otherwise. By applying the Primitive Element Theorem, we know that there exists some $\gamma \in K$ such that $K = K_0(\gamma)$ (see [Kha22, Theorem A.28]). Let $f \in \mathbb{Q}[t]$ be the minimal polynomial of γ. One can show that $\deg(f) = n$ (see [Kha22, Proposition A.2]). The minimal polynomial f is a product of linear polynomials over $\overline{\mathbb{Q}}$. Hence, there exists $\gamma_i \in \mathbb{C}$ for all $0 \leq i \leq n-1$ such that $f(t) = \prod_{i=0}^{n-1}(t - \gamma_i)$. Equivalently, the elements $\gamma_i \in \overline{\mathbb{Q}}$ for integer $0 \leq i \leq n-1$, are all the roots of polynomial f. We denote by r_1 the number of roots that are real and by r_2 the number of roots that are complex. As complex roots come in pairs, with their complex conjugate, we have $n = r_1 + 2r_2$. Every root of f defines a $\mathbb{Q}$-embedding into $\overline{\mathbb{Q}}$. Namely, we have the $\mathbb{Q}$-embedding defined by $\gamma \mapsto \gamma_i$ for all integers $0 \leq i \leq n-1$. It can be shown that these are all the $\mathbb{Q}$-embeddings of K (see [Xia16, Theorem 1, Section 1.3]). From now on, we will call a $\mathbb{Q}$-embedding of K simply a field embedding of K. It follows that the field embeddings of K are in bijection with the roots of f. Therefore, throughout this thesis, we will refer to field embeddings of K instead of roots of the minimal polynomial f. If γ_i is real, the image of K, under the corresponding field embedding, is in $\mathbb{R}$. If γ_i is complex, this is not the case.

Definition 1.2.1. The field embeddings coming from a real (resp. complex) root are called *real* (resp. *complex*) field embeddings. The set of all field embeddings of the number field K is denoted by Σ_K.

Remark 1.2.2. Throughout this thesis, let the complex conjugation of $z \in \mathbb{C}$ be denoted by $\overline{z}$. Furthermore, we denote the real part of a complex number by $\Re$ and the imaginary part by $\Im$. Lastly, the absolute value on $\mathbb{C}$ (or on $\mathbb{R}$) will be denoted by $|.|_\infty$. ♦

Just like roots, the complex field embeddings come in pairs. Namely, for any complex field embedding $\sigma\colon K \to \overline{\mathbb{Q}}$, we also have the complex field embedding $\overline{\sigma}\colon K \to \overline{\mathbb{Q}}$. It comes with the relation that $\overline{\sigma}(x) = \overline{\sigma(x)}$ for any $x \in K$.

Definition 1.2.3. Let σ, σ' be two field embeddings of K. Then σ and σ' are called *conjugate* field embeddings if $\sigma(x) = \overline{\sigma'(x)}$ for all $x \in K$. Otherwise, the field embeddings are called *non-conjugate*.

The following definition will be used throughout this thesis.

Definition 1.2.4. The *degree* of a field embedding $\sigma \in \Sigma_K$ is defined by

$$\deg(\sigma) := \begin{cases} 1, & \text{if } \sigma \text{ is a real field embedding,} \\ 2, & \text{if } \sigma \text{ is a complex field embedding.} \end{cases}$$

We move on to the ring of integers of K, denoted by $\mathcal{O}_K$. The ring $\mathcal{O}_K$ contains all elements of K that are roots of a monic polynomial with integer coefficients. It is known that $\mathcal{O}_K$ is a Dedekind domain (see [Neu99, Theorem 3.1, Chapter I]). The set of non-zero prime ideals of $\mathcal{O}_K$ will be denoted by $\mathfrak{P}_K^0 := \mathrm{Spec}(\mathcal{O}_K)\backslash\{(0)\}$. The group of fractional ideals will be denoted by $\mathrm{Id}_K := \mathrm{Id}_{\mathcal{O}_K}$ and the subgroup of principal fractional ideals by P_K. The class group of $\mathcal{O}_K$, defined in Definition 1.1.3, is denoted by Cl_K. The order of the class group Cl_K is known to be finite and will be denoted by the $h_k \in \mathbb{Z}_{>0}$ (see [Neu99, Theorem 6.3, Chapter I]).

Definition 1.2.5. The integer h_K is called the *class number* of the number field K.

In the ring of integers of K, the norm of an element in $\mathcal{O}_K$ can be related to the norm of fractional ideals.

Proposition 1.2.6. Let $x \in K^*$, then $|N_{K|\mathbb{Q}}(x)|_\infty = N_{\mathcal{O}_K}(x\mathcal{O}_K)$.

Proof. We know that $N_{\mathcal{O}_K}\colon \mathrm{Id}_K \to \mathbb{Q}^*$ is a group homomorphism and $N_{K|\mathbb{Q}}(xy) = N_{K|\mathbb{Q}}(x)N_{K|\mathbb{Q}}(y)$ for any $x, y \in K$. The latter is a consequence of Proposition 1.1.15. Since K is the field of fractions of $\mathcal{O}_K$, the result is true if it holds for a non-zero element in $\mathcal{O}_K$. This was proven on page 35 in [Neu99]. □

The ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n. Moreover, any finitely generated $\mathcal{O}_K$-submodule of K is a free $\mathbb{Z}$-module of rank n (see [Neu99, Proposition 2.10, Chapter I]). Let $\{a_1, \ldots, a_n\}$ be any $\mathbb{Z}$-basis of $\mathcal{O}_K$. Furthermore, let $\sigma_1, \ldots, \sigma_n$ denote all field embeddings of K. Then the quantity

$$\det((\sigma_i(a_j))_{1\leq i,j\leq n})^2 \tag{3}$$

is independent of the choice of basis (see [Neu99, Page 15]).

Definition 1.2.7. The quantity (3) is called the *(absolute) discriminant* of the number field K and is denoted by d_K.

The following result relates the discriminant of K to the different of $\mathcal{O}_K|\mathbb{Z}$.

Proposition 1.2.8. The absolute value of the discriminant d_K of K equals $N_{\mathcal{O}_K}(\mathfrak{D}_{\mathcal{O}_K|\mathbb{Z}})$.

Proof. The relative discriminant $N_{\mathcal{O}_K|\mathbb{Z}}(\mathfrak{D}_{\mathcal{O}_K|\mathbb{Z}})$ of $\mathcal{O}_K|\mathbb{Z}$ equals the fractional ideal of $\mathbb{Z}$ generated by d_K (see [Kha22, Theorem 7.8]). Furthermore, one has $N_{\mathcal{O}_K|\mathbb{Z}}(\mathfrak{D}_{\mathcal{O}_K|\mathbb{Z}}) = N_{\mathcal{O}_K}(\mathfrak{D}_{\mathcal{O}_K|\mathbb{Z}})\mathbb{Z}$. This result is Proposition 6.11 in [Kha22]. Combining these results, we obtain that

$$d_K\mathbb{Z} = N_{\mathcal{O}_K|\mathbb{Z}}(\mathfrak{D}_{\mathcal{O}_K|\mathbb{Z}}) = N_{\mathcal{O}_K}(\mathfrak{D}_{\mathcal{O}_K|\mathbb{Z}})\mathbb{Z}.$$

Since $\mathbb{Z}^* = \{\pm 1\}$, we obtain that $\pm d_K = N_{\mathcal{O}_K}(\mathfrak{D}_{\mathcal{O}_K|\mathbb{Z}})$, and so $|d_K|_\infty = N_{\mathcal{O}_K}(\mathfrak{D}_{\mathcal{O}_K|\mathbb{Z}})$. □

Now, let $\mathcal{O}_K^*$ denote the group of units of $\mathcal{O}_K$. Let μ_K denote the subgroup of $\mathcal{O}_K^*$ containing the elements of finite order, i.e. the roots of unity of K. By Dirichlet's Unit Theorem, the group $\mathcal{O}_K^*$ is a direct product of μ_K and a free abelian group of rank $r_1 + r_2 - 1$ (see [Neu99, Theorem 7.4, Chapter I]). Let $\{\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1}\}$

be any set of generators of the free group of $\mathcal{O}_K^*$. Furthermore, let $\sigma_1, \ldots, \sigma_{r_1+r_2}$ denote all field embeddings of K that are pairwise distinct and non-conjugate. Then the quantity

$$\left|\det\left((\deg(\sigma_i)\log|\sigma_i(\varepsilon_j)|_\infty)_{1\leq i,j\leq r_1+r_2-1}\right)\right|_\infty \tag{4}$$

is independent of the choice of basis. Furthermore, note that $\sigma_{r_1+r_2}$ is not used in this quantity. But it turns out that this quantity is also independent of the choice of the order of the pairwise distinct and non-conjugate field embeddings. This is explained in Proposition 7.5 of [Neu99].

Definition 1.2.9. The quantity (4) is called the *regulator* of the number field K and is denoted by R_K.

1.3 Infrastructure

In this section, we will look into some specific number fields.

Definition 1.3.1. An integer $d \in \mathbb{Z}$ is called a *fundamental discriminant* if $d \neq 1$ is square-free and $d \equiv 1 \bmod 4$, or $d = 4D$, where $D \in \mathbb{Z}$ is square-free and $D \equiv 2, 3 \bmod 4$.

Throughout this section, we consider the quadratic number field $K = \mathbb{Q}(\sqrt{d})$ for some fundamental discriminant $d \in \mathbb{Z}$. The element $\sqrt{d}$ has minimal polynomial $t^2 - d \in \mathbb{Q}[t]$. The roots of this polynomial are given by $\sqrt{d}$ and $-\sqrt{d}$. This implies that $r_1 = 2$ and $r_2 = 0$ if $d > 0$. Furthermore, if $d < 0$, we have $r_1 = 0$ and $r_2 = 1$.

Definition 1.3.2. If $d > 0$, the number field K is called a *real quadratic number field*. If $d < 0$, the number field K is called a *imaginary quadratic number field*.

In the previous section, we saw that the roots of the minimal polynomial are in bijection with the field embeddings of K. Consequently, the number field K has 2 field embeddings. One trivial field embedding that is given by $\sqrt{d} \mapsto \sqrt{d}$ and one non-trivial field embedding, denoted by σ, given by $\sqrt{d} \mapsto -\sqrt{d}$. Using Proposition 1.1.15, we know that the norm of $x \in K$ is given by $N_{K|\mathbb{Q}}(x) = x\sigma(x)$. Set $\omega = \frac{d+\sqrt{d}}{2}$, then the ring of integers is given by $\mathcal{O}_K = \mathbb{Z}[\omega]$. Moreover, the discriminant of K equals d. These results are found in [Coh93, Section 5.1]. For the units of $\mathcal{O}_K$, one has

$$\mathcal{O}_K^* = \begin{cases} \{\pm 1\} \times \langle \varepsilon_K \rangle, & \text{if } d > 0, \\ \{\pm 1, \pm\zeta, \pm\zeta^2 : 1 + \zeta + \zeta^2 = 0\}, & \text{if } d = -3, \\ \{\pm 1, \pm i : 1 + i^2 = 0\}, & \text{if } d = -4, \\ \{\pm 1\}, & \text{if } d < -4, \end{cases} \tag{5}$$

where ε_K denotes a fundamental unit of $\mathcal{O}_K$ if $d > 0$. One can find this result in [JW09, Section 4.3].

Remark 1.3.3. There are certain choices for the fundamental unit. Throughout this paper, we restrict to the fundamental unit such that $\varepsilon_K \in \mathbb{R}_{>1}$. The fundamental unit is related to the fundamental solution of the Pell equation. For more information on the fundamental solution and the fundamental unit, we refer to [JW09]. ♦

If $d > 0$, the regulator of K is given by $R_K = \log|\varepsilon_K|_\infty$. We have $R_K = \log(\varepsilon_K)$ since $\varepsilon_K > 1$. The regulator of an imaginary quadratic number field is defined to be 1 by convention. This convention makes sure that the Class Number Formula holds (see [Neu99, Page 467]).

Now, the infrastructure is a group-like structure inside the equivalence class of the unit element of Cl_K. It induces an algorithm that computes the regulator for a real quadratic number field. In this section, we will give a short recap of the construction of this algorithm. We use the description of this as described in [JW09]. Firstly, we focus on any quadratic number field and recall some extra results on these number fields. This consists of some information on the ring of integers and the representation of its integral ideals. Thereafter, we describe a reduction algorithm and explain how this can be used to study the infrastructure.

Proposition 1.3.4. Any integral ideal I of $\mathcal{O}_K$ can be written as

$$I = a\left(\frac{b}{r}\mathbb{Z} + \left(\frac{c+\sqrt{d}}{r}\right)\mathbb{Z}\right),$$

where $a, b, c \in \mathbb{Z}$ and

$$r = \begin{cases} 2, & \text{if } d \equiv 1 \bmod 4, \\ 1, & \text{otherwise,} \end{cases}$$

such that $r|b$ and $rb|d - c^2$. Vice versa, any such representation must be an integral ideal of $\mathcal{O}_K$. Such representation is denoted by $I = (a)[b, c]$.

This result is Equation (4.9) in [JW09].

Definition 1.3.5. An integral ideal I of $\mathcal{O}_K$ is called *primitive* if it cannot be written as $I = mJ$ for some other integral ideal J of $\mathcal{O}_K$ and $m \in \mathbb{Z}$ with $|m|_\infty > 1$.

In terms of the representation of Proposition 1.3.4, this means that we can take $a = 1$. In this case, we write $I = [b, c]$.

Definition 1.3.6. An integral ideal I of $\mathcal{O}_K$ is called *reduced* if it is primitive and there does not exist a non-zero $a \in I$ such that $|a|_\infty < N_{\mathcal{O}_K}(I)$ and $|\sigma(a)|_\infty < N_{\mathcal{O}_K}(I)$.

Example 1.3.7. We can view $\mathcal{O}_K$ as an integral ideal. For any integral ideal J of $\mathcal{O}_K$ and $m \in \mathbb{Z}$ with $|m|_\infty > 1$, the integral ideal mJ is strictly contained in $\mathcal{O}_K$. Thus, we see that $\mathcal{O}_K$ is primitive. Furthermore, we have $N_{\mathcal{O}_K}(\mathcal{O}_K) = 1$. Suppose that there exists a non-zero $a \in \mathcal{O}_K$ such that $|a|_\infty < 1$ and $|\sigma(a)|_\infty < 1$. Then using Proposition 1.1.15 and 1.2.6 we have

$$N_{\mathcal{O}_K}(a\mathcal{O}_K) = |N_{K|\mathbb{Q}}(a)|_\infty = |a\sigma(a)|_\infty < 1.$$

This contradicts the fact that $N_{\mathcal{O}_K}(a\mathcal{O}_K) \in \mathbb{Z}_{>0}$. Hence, we know that $\mathcal{O}_K$ is also reduced. ■

Corollary 5.5.1 and Corollary 5.8.1 in [JW09] tell us that if I is a reduced integral ideal, its norm is bounded by $\sqrt{|d|_\infty}$. Therefore, by Proposition 1.1.10 (ii.), there can only exist finitely many reduced integral ideals in $\mathcal{O}_K$.

Given any fractional ideal I of $\mathcal{O}_K$, it is possible to find a reduced integral ideal equivalent to I.

Algorithm 1.3.8. (Reduction Algorithm for Fractional Ideals)
Input: Any fractional ideal I of $\mathcal{O}_K$.
Output: A reduced integral ideal J of $\mathcal{O}_K$ such that I and J are equivalent.

i.) Compute $\alpha \in \mathcal{O}_K$ such that αI is an integral ideal of $\mathcal{O}_K$.

ii.) Find the integral ideal representation of Proposition 1.3.4 for αI, i.e. $I = (a)[b, c]$ for some $a, b, c \in \mathbb{Z}$.

iii.) If $[b, c]$ is reduced, then return $J = [b, c]$. Else, set $b_0 := b$, $c_0 := c$, and $i = 0$.

iv.) Set $i = i + 1$ and compute the integral ideal $[b_i, c_i]$, where

$$s_i := \begin{cases} \left\lfloor \frac{c_{i-1}}{b_{i-1}} \right\rceil, & \text{if } d < 0, \\ \left\lfloor \frac{c_{i-1}+\sqrt{d}}{b_{i-1}} \right\rfloor, & \text{if } d > 0, \end{cases} \qquad c_i := s_i b_{i-1} - c_{i-1}, \qquad b_i := \frac{d - c_i^2}{b_{i-1}}.$$

vi.) If $[b_i, c_i]$ is reduced, then return $J = [b_i, c_i]$. Else, return to step (iv.).

The algorithm is investigated in Section 5.1 of [JW09]. More explicitly, on pages 100 and 103 of that book, one can find the reason why the algorithm terminates in a finite number of steps. One should notice that this book uses a different representation of integral ideals. Therefore, the algorithm is a little bit different. However, by transforming to the representation of Proposition 1.3.4, one finds Algorithm 4.3.8. The description of this algorithm using this transformation was also used on pages 15 and 16 in [Wan17].

Algorithm 1.3.8 is not deterministic. This means that the output might differ when one uses the same input several times. Namely, the α computed in step (i.) is not unique. Therefore, the integral αI might differ. However, if we focus on integral ideals, we can always take $\alpha = 1$ in step (i.). Hence, the algorithm is deterministic when integral ideals are the input.

Remark 1.3.9. If $d < 0$, it can be proven that any equivalence class in Cl_K contains a unique reduced integral ideal, up to conjugation. This result is [JW09, Theorem 5.17]. ♦

In the remainder of this section, we will restrict to $d > 0$. Let $I = [b, c]$ be a primitive integral ideal in $\mathcal{O}_K$. Let ρ denote the operator that sends $[b, c]$ to $I' := [b', c']$, where

$$s := \left\lfloor \frac{c + \sqrt{d}}{b} \right\rfloor, \qquad c' := sb - c, \qquad b' := \frac{d - c'^2}{b}.$$

Note that this is the same as step (iv.) in Algorithm 1.3.8. Then these integral ideals are equivalent by the relation

$$I' = \xi I, \qquad \xi := \frac{c' + \sqrt{d}}{b}. \tag{6}$$

It can be shown that if I is reduced, then so is $\rho(I)$ (see [JW09, Theorem 5.12]). Now, we would like to apply ρ recursively. So for any $i \in \mathbb{Z}_{>0}$, denote $I_i := \rho^i(I)$, where ρ^i denote i compositions of ρ. We use the convention that $I_0 := I$. There exists a minimal $m \in \mathbb{Z}_{>0}$ such that $I_m = I_0$. Moreover, the set $\{I_0, I_1, \ldots, I_{m-1}\}$ is a complete set of distinct reduced integral ideals equivalent to I. This result is proven in Section 5.3 of [JW09].

Definition 1.3.10. Let I be a reduced integral ideal of $\mathcal{O}_K$. The complete set of distinct reduced integral ideals equivalent to I is called the *cycle* of I. The cycle of $\mathcal{O}_K$ is called the *principal cycle* of K.

Consider the representation $I_i = [b_i, c_i]$ for $b_i, c_i \in \mathbb{Z}$ for all $i \in \mathbb{Z}_{\geq 0}$. In Equation (6), we saw that $I_{i+1} = \xi_i I_i$, where $\xi_i := \frac{c_{i+1} + \sqrt{d}}{b_i}$. Set $\theta_i := \prod_{j=0}^{i-1} \xi_j$, then

$$I_i = \xi_{i-1} I_{i-1} = \xi_{i-1}\xi_{i-2} I_{i-2} = \ldots = \left(\prod_{j=0}^{i-1} \xi_j \right) I_0 = \theta_i I_0.$$

We use the convention that $\theta_0 := 1$. One can show that $\theta_m = \varepsilon_K$ (see [JW09, page 113].

The main discovery of Shanks was a group-like structure inside the principal cycle of K. So let $I = \mathcal{O}_K$. With the same notation, we have $I_i = \theta_i I_0 = \theta_i \mathcal{O}_K$. Hence, the principal cycle is given by

$$\mathcal{C} := \{I_0, I_1, \ldots, I_{m-1}\} = \{\theta_0 \mathcal{O}_K, \theta_1 \mathcal{O}_K, \ldots, \theta_{m-1} \mathcal{O}_K\}.$$

Definition 1.3.11. For any $i \in \mathbb{Z}_{\geq 0}$, the *distance* of I_i is defined by $\delta(I_i) := \log(\theta_i)$.

The distance of I_m is given by

$$\delta(I_m) = \log(\theta_m) = \log(\varepsilon_K) = R_K.$$

Since $I_m = I_0$, the value of $\delta(I_m)$ can be seen as the 'entire distance' of the principal cycle $\mathcal{C}$. Thus, the entire distance equals the regulator of K. Therefore, if there exists some $k \in \mathbb{Z}$ such that $\delta(I_i) = \delta(I_j) + kR_K$

for some $i, j \in \mathbb{Z}_{\geq 0}$, then $I_i = I_j$. Furthermore, one can show that $\delta(I_i) \approx i$ (see [JW09, Theorem 3.17]). It follows that $R_K = \delta(I_m) \approx m$. Hence, the regulator estimates the number of reduced integral ideals equivalent to $\mathcal{O}_K$.

Take I_i, I_j in the principal cycle $\mathcal{C}$. Then these integral ideals are principal, and so is their product $I_i I_j = \theta_i \theta_j \mathcal{O}_K$. We can apply Algorithm 1.3.8 to this product. This gives us a reduced integral ideal equivalent to $I_i I_j$. Consequently, this reduced integral ideal must be contained in the principle cycle. Let $I_k \in \mathcal{C}$ be this reduced integral ideal. Because the algorithm is deterministic on integral ideals, the reduced integral ideal I_k is uniquely determined from I_i and I_j. We define this operation by $*\colon \mathcal{C} \times \mathcal{C} \to \mathcal{C}$, i.e. $I_i * I_j := I_k$. Since I_k and $I_i I_j$ are equivalent, there exists some $\theta \in K^*$ such that $I_k = \theta I_i I_j$. Notice that this θ is determined from Algorithm 1.3.8. Then we also have $\theta_k \mathcal{O}_K = \theta \theta_i \theta_j \mathcal{O}_K$. Hence, there exists some $a \in \mathcal{O}_K^*$ such that $\theta_k = a\theta\theta_i\theta_j$. One can take $a = \pm 1$ such that $\theta_k = |\theta|_\infty \theta_i \theta_j$ (see [JW09, Page 174]). Set

$$\kappa(I_i; I_j) := \log |\theta|_\infty, \tag{7}$$

then

$$\delta(I_i * I_j) = \delta(I_k) = \log(\theta_k) = \log(x\theta_i\theta_j) = \log(x) + \log(\theta_i) + \log(\theta_j) = \kappa(I_i; I_j) + \delta(I_i) + \delta(I_j).$$

It can be shown that

$$-\log(d) < \kappa(I_i; I_j) < \log(2) \tag{8}$$

for all $0 \leq i, j \leq m - 1$ (see [JW09, Page 175]).

Definition 1.3.12. The principal cycle $\mathcal{C}$, together with the operation $*$, is called the *infrastructure* of K.

The operation $*$ is closed in $\mathcal{C}$. Furthermore, it is also commutative since the product of ideals is commutative. Moreover, for any $I \in \mathcal{C}$, we have $\mathcal{O}_K * I = I$. This follows from the fact that $\mathcal{O}_K I = I$ and I is reduced. Thus, we see that $\mathcal{O}_K \in \mathcal{C}$ plays the role of the unit element in $\mathcal{C}$. Furthermore, it is possible to define an inverse for any element in $\mathcal{C}$. Now, for any $I_i, I_j, I_k \in \mathcal{C}$ we get

$$\delta((I_i * I_j) * I_k) = \delta(I_i) + \delta(I_j) + \delta(I_k) + \kappa(I_i * I_j; I_k) + \kappa(I_i; I_j),$$

and

$$\delta(I_i * (I_j * I_k)) = \delta(I_i) + \delta(I_j) + \delta(I_k) + \kappa(I_i; I_j * I_k) + \kappa(I_j; I_k).$$

If $\kappa(I_i * I_j; I_k) + \kappa(I_i; I_j) \neq \kappa(I_i; I_j * I_k) + \kappa(I_j; I_k)$, then $\delta((I_i * I_j) * I_k) \neq \delta(I_i * (I_j * I_k))$. By injectivity of δ on $\mathcal{C}$, this would imply that $(I_i * I_j) * I_k \neq I_i * (I_j * I_k)$. This means that the associative law does not need to hold for $*$. This prevents $\mathcal{C}$ from being an abelian group.

However, due to its group-like structure, Shanks was able to apply some ideas of his Baby-Step Giant-Step Algorithm on $\mathcal{C}$. This helped to compute the entire distance of the principal cycle, i.e. the regulator. The Baby-Step Giant-Step Algorithm is used to compute the order of an element in a finite abelian group. For an explanation of the Baby-Step Giant-Step Algorithm we refer to Section 5.4.1 in [Coh93]. But shortly, for a finite abelian group G and an element $g \in G$, the baby-steps consist of multiplication (under the group operation) by g. In the principal cycle $\mathcal{C}$, this can be seen as applying the operator ρ. Furthermore, in the cyclic group G, the giant-steps consist of multiplication by g^i for some $i \in \mathbb{Z}_{i>1}$. This is where the operation $*$ comes into play for $\mathcal{C}$. Namely, one can multiply by I_i for some $i \in \mathbb{Z}_{\geq 0}$ to take 'bigger' steps in the principal cycle. This can be worked out in an algorithm that computes the regulator of K.

Algorithm 1.3.13. (Infrastructure Algorithm)
Input: Any fundamental discriminant $d \in \mathbb{Z}_{>0}$.
Output: The regulator R_K of the number field $K = \mathbb{Q}(\sqrt{d})$.

i.) **Baby-Steps**
Set $I_0 := \mathcal{O}_K$, and compute $\mathcal{A} := \{I_0, I_1, \ldots, I_i, I_{j+1}, I_{j+2}\}$, where $I_k = \rho^k(I_0)$ for all $0 \leq k \leq j + 2$. Furthermore, take $j \in \mathbb{Z}_{>0}$ such that $\delta(I_j) > \sqrt[4]{d} > \delta(I_{j-1})$.

ii.) Set $i = 0$ and $J_i := I_j$.

iii.) **Giant-Steps**
Set $i = i + 1$ and compute $J_i := J_{i-1} * I_j$.

iv.) If $J_i \in \mathcal{A}$, find $I_k \in \mathcal{A}$ such that $J_i = I_k$. Then return $R_K = \delta(J_i) - \delta(I_k)$. Else, return to step (iii.).

For investigation and the correctness of this algorithm we refer to Section 7.4 in [JW09]. It even gives a more explicit description of the infrastructure. However, the results used in that book rely on the theory of continued fractions. Namely, the principal cycle can be related to the continued fraction of $\frac{(r-1)+\sqrt{d}}{r}$. Continued fractions are not needed in this thesis and the ideas of the infrastructure can be explained without them. Therefore, we choose to not discuss them. For a more expansive treatment of the infrastructure we refer to Chapter 3, 6, and Section 7.4 of [JW09].

Remark 1.3.14. After Shanks had discovered the infrastructure, Lenstra gave another way to describe this phenomenon (see [Len82]). Lenstra used reduced binary quadratic forms of discriminant d rather than reduced integral ideals of $\mathcal{O}_K$. This construction is closely related to the description of the infrastructure using Arakelov theory. The latter will be seen in Section 4.3. That is why we do not dive into the theory developed by Lenstra. See also Remark 4.3.5. ♦

1.4 Valuations and Absolute Values

In this section, we will introduce valuations and absolute values. This section is mostly based on the first four sections of Chapter II in [Neu99]. However, to prevent confusion, in this book absolute values are called valuations, and valuations are called exponential valuations.

For now, let K be any field.

Definition 1.4.1. A *valuation* of field K is a function $v\colon K \to \mathbb{R} \cup \{\infty\}$ such that for all $x, y \in K$

i.) $v(x) = \infty$ if and only if $x = 0$,

ii.) $v(xy) = v(x) + v(y)$,

iii.) $v(x + y) \geq \min\{v(x), v(y)\}$.

An element $x \in K$ is said to have *valuation* $v(x)$. A valuation is called *discrete* if there exists some $t \in \mathbb{R}_{>0}$ such that $v(K^*) = t\mathbb{Z}$. Moreover, a discrete valuation is *normalized* if $t = 1$.

One can always transfer a discrete valuation into a normalized one, by dividing by the element t. So we will always assume that our discrete valuations are normalized. Let v be any valuation of field K. As shown in Proposition 3.8 of Chapter II in [Neu99], the elements of K with a non-negative valuation form a subring of K.

Definition 1.4.2. Let v be a valuation of field K. The set of elements of K with a non-negative valuation is called the *valuation ring* of K with respect to v. If v is discrete, the valuation ring is called a *discrete valuation ring* (abbreviated as DVR).

Proposition 3.8 of Chapter II in [Neu99] shows some other facts as well. The units of a valuation ring are given by the elements of K with a zero valuation. Furthermore, the ring has a unique maximal ideal given by the elements of K with a positive valuation. Consequently, any valuation ring is a local ring.

Remark 1.4.3. Some special properties of DVRs are listed in Proposition 9.2 in [AM69]. We list the properties that will be important throughout this thesis.

i.) Any DVR is a principal ideal domain and therefore a Dedekind domain.

ii.) Every non-zero fractional ideal is a power of the maximal ideal.

iii.) Let K be any field that attains a discrete valuation ring $\mathcal{O}$. Then any element x of K can be written as $x = t^k a$, for some $a \in \mathcal{O}^*$, generator t of the maximal ideal of $\mathcal{O}$ (called a *uniformizer* of $\mathcal{O}$), and $k \in \mathbb{Z}$.

♦

Definition 1.4.4. An *absolute value* of field K is a function $|.| \colon K \to \mathbb{R}$ such that for all $x, y \in K$

i.) $|x| \geq 0$, and $|x| = 0$ if and only if $x = 0$,

ii.) $|xy| = |x||y|$,

iii.) $|x + y| \leq |x| + |y|$ (*triangle inequality*).

An absolute value is called *non-Archimedean* if $|x + y| \leq \max\{|x|, |y|\}$ (*strong triangle inequality*). Otherwise, the absolute value is called *Archimedean*.

For any valuation v of K, a non-Archimedean absolute value $|.|$ of K is created by setting $|x| = r^{-v(x)}$, for some $r \in \mathbb{R}_{>1}$. This is a direct verification of the conditions from the definitions. For the rest of this section, let K be a number field.

Example 1.4.5. In Remark 1.1.5, we have seen the group homomorphism $\mathrm{ord}_{\mathfrak{p}} \colon \mathrm{Id}_K \to \mathbb{Z}$ for any $\mathfrak{p} \in \mathfrak{P}_K^0$. We can define a discrete valuation on K by setting $\mathrm{ord}_{\mathfrak{p}}(x) := \mathrm{ord}_{\mathfrak{p}}(x\mathcal{O}_K)$ for any $x \in K^*$ and $\mathrm{ord}_{\mathfrak{p}}(0) = \infty$. This discrete valuation is called the $\mathfrak{p}$-*adic valuation*. Since $N_{\mathcal{O}_K}(\mathfrak{p}) \in \mathbb{R}_{>1}$, we have a non-Archimedean absolute value, which we denote by $|.|_{\mathfrak{p}}$, given by $|x|_{\mathfrak{p}} = N_{\mathcal{O}_K}(\mathfrak{p})^{-\mathrm{ord}_{\mathfrak{p}}(x)}$. This is called the $\mathfrak{p}$-*adic absolute value*.

For any field embedding $\sigma \in \Sigma_K$, we can define an absolute value $|x|_\sigma := |\sigma(x)|_\infty$. This defines an Archimedean absolute value. There are only $r_1 + r_2$ such absolute values on K as $|.|_\sigma = |.|_{\overline{\sigma}}$. ■

Due to the notion of absolute values, we can speak about convergence.

Definition 1.4.6. Let $|.|$ be an absolute value of K. Then K is called *complete* with respect to the absolute value $|.|$, if all Cauchy sequences in K converge.

Definition 1.4.7. Let $|.|$ be an absolute value of K. A field L with absolute value $|.|'$ is called a *completion* of K with respect to $|.|$ if

i.) K is a subfield of L and the absolute value $|.|'$ restricted to K gives $|.|$,

ii.) L is complete with respect to $|.|'$,

iii.) K is dense in L.

Completions of K with respect to any absolute value $|.|$ are unique up to isomorphism of fields (see [Neu99, Section 4, Chapter II]). To find one, we can proceed as follows. Consider the ring R of all Cauchy sequences on K, and its maximal ideal m containing all Cauchy sequences converging to zero. The absolute value $|.|$ can be extended to the field R/m. Namely, for any $x \in R/m$, which is represented by Cauchy sequence $(x_i)_{i \geq 1}$, we define the absolute value of x by $|x| := \lim_{i \to \infty} |x_i|$. Then the field R/m is complete with respect to $|.|$. The field K can be embedded into R/m by sending every $x \in K$ to the equivalence class of the Cauchy sequence given by $(x)_{i \geq 1}$.

Consider the absolute value $|.|_\sigma$ for any $\sigma \in \Sigma_K$. The completion of K with respect to $|.|_\sigma$ is denoted by K_σ.

Theorem 1.4.8. Let $\sigma \in \Sigma_K$. Then the completion K_σ is topologically isomorphic as field to $\mathbb{R}$ or $\mathbb{C}$. Given such an isomorphism f, one has $|x|_\sigma = |f(x)|_\infty^t$ for all $x \in K_\sigma$, and some $t \in (0, 1]$. More precisely, the completion is isomorphic to $\mathbb{R}$ if σ is a real field embedding. Otherwise, the completion is isomorphic to $\mathbb{C}$.

Proof. Since $|.|_\sigma$ is an Archimedean absolute value, Ostrowski's Theorem tells that K_σ is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$ (see [Neu99, Theorem 4.2, Chapter II]). Moreover, the theorem tells us that given such isomorphism f, one has $|x|_\sigma = |f(x)|_\infty^t$ for all $x \in K_\sigma$, and some $t \in (0, 1]$. Suppose that σ corresponds to a real field embedding of K. We know that σ induces an isomorphism between K and a subfield L of $\mathbb{R}$. Since σ is a field embedding, it fixes $\mathbb{Q}$. Hence, we know that L contains the subfield $\mathbb{Q}$. Moreover, the absolute value $|.|_\sigma$ on K is transferred to the absolute value $|.|_\infty$ on L. Since $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to $|.|_\infty$, and $\mathbb{Q} \subseteq L \subseteq \mathbb{R}$, the completion of L with respect to $|.|_\infty$ must be $\mathbb{R}$. Then the completion K_σ must be isomorphic to $\mathbb{R}$. If σ corresponds to a complex field embedding, then σ induces an isomorphism between K and a subfield of $\mathbb{C}$ containing a non-real number. It follows that the completion of this subfield cannot equal $\mathbb{R}$. By Ostrowski's Theorem, it must be isomorphic to $\mathbb{C}$. Consequently, the completion K_σ is isomorphic to $\mathbb{C}$. □

Now, consider the absolute value $|.|_\mathfrak{p}$ for any $\mathfrak{p} \in \mathfrak{P}_K^0$. The completion of K with respect to $|.|_\mathfrak{p}$ is denoted by $K_\mathfrak{p}$. We can also extend the discrete valuation $\mathrm{ord}_\mathfrak{p}$ from K to $K_\mathfrak{p}$. Namely, for any $x \in K_\mathfrak{p}$, which is represented by Cauchy sequence $(x_i)_{i\geq 1}$, we define the valuation of x by $v(x) := \lim_{i\to\infty} v(x_i)$. By verifying the conditions of Definition 1.4.1, we get a discrete valuation on $K_\mathfrak{p}$. The DVR of K with respect to $\mathrm{ord}_\mathfrak{p}$ is given by

$$\mathcal{O}_{K,\mathfrak{p}} := \{x \in K : \mathrm{ord}_\mathfrak{p}(x) \geq 0\}, \tag{9}$$

and has unique maximal ideal $\mathfrak{m}_{K,\mathfrak{p}} := \{x \in K : \mathrm{ord}_\mathfrak{p}(x) > 0\}$. The ring $\mathcal{O}_{K,\mathfrak{p}}$ is also known as the localization of $\mathcal{O}_K$ with respect to $\mathfrak{p}$. Now, the DVR of $K_\mathfrak{p}$ with respect to $\mathrm{ord}_\mathfrak{p}$ is given by

$$\mathcal{O}_\mathfrak{p} := \{x \in K_\mathfrak{p} : \mathrm{ord}_\mathfrak{p}(x) \geq 0\},$$

and has unique maximal ideal $\mathfrak{m}_\mathfrak{p} := \{x \in K_\mathfrak{p} : \mathrm{ord}_\mathfrak{p}(x) > 0\}$. By Remark 1.4.3, we know that $\mathcal{O}_{K,\mathfrak{p}}$ and $\mathcal{O}_\mathfrak{p}$ are Dedekind domains. So we can use the norm that we saw in Definition 1.1.11.

Lemma 1.4.9. For any $k \in \mathbb{Z}_{>0}$ one has

$$\mathcal{O}_K/\mathfrak{p}^k \cong \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{m}_{K,\mathfrak{p}}^k \cong \mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^k.$$

Consequently, one has $N_{\mathcal{O}_K}(\mathfrak{p}^k) = N_{\mathcal{O}_{K,p}}(\mathfrak{m}_{K,\mathfrak{p}}^k) = N_{\mathcal{O}_\mathfrak{p}}(\mathfrak{m}_\mathfrak{p}^k)$.

This result is a combined consequence of Corollary 11.2 of Chapter I and Proposition 4.3 of Chapter II in [Neu99].

Take any $\mathfrak{p} \in \mathfrak{P}_K^0$. It follows directly from the definition of a prime ideal that $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. Hence, there exists a prime number p such that $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. So we have the $\mathfrak{p}$-adic absolute value for K and the p-adic absolute value for $\mathbb{Q}$. One can show that the completion $K_\mathfrak{p}$ of K with respect to the $\mathfrak{p}$-adic absolute value is a field extension of $\mathbb{Q}_p$, the completion of $\mathbb{Q}$ with respect to the p-adic absolute value. This fact is proven in a more general setting in Section 8 of Chapter II in [Neu99]. Moreover, by Proposition 5.2 in Chapter II of [Neu99] this extension is finite. Since the characteristic of $\mathbb{Q}_p$ equals zero, it is even a separable finite field extension. Now, the DVR $\mathcal{O}_\mathfrak{p}$ is the integral closure of $\mathbb{Z}_p$ (the DVR of $\mathbb{Q}_p$ with respect to ord_p) in $K_\mathfrak{p}$. This fact is proven inside the proof of Theorem 4.8 in Chapter II in [Neu99]. Moreover, the field of fractions of $\mathcal{O}_\mathfrak{p}$ (resp. $\mathbb{Z}_p$) equals $K_\mathfrak{p}$ (resp. $\mathbb{Q}_p$).

So in summary, we have the Dedekind domain $\mathbb{Z}_p$ with its field of fractions $\mathbb{Q}_p$. Moreover, we have a finite separable field extension $K_\mathfrak{p}|\mathbb{Q}_p$, with the integral closure $\mathcal{O}_\mathfrak{p}$ of $\mathbb{Z}_p$ in $K_\mathfrak{p}$. Thus, by the construction of the different in Definition 1.1.16, we can speak of the different of $\mathcal{O}_\mathfrak{p}|\mathbb{Z}_p$ for any $\mathfrak{p} \in \mathfrak{P}_K^0$.

Proposition 1.4.10. For any number field K, one has $|d_K|_\infty = \prod_{\mathfrak{p}\in\mathfrak{P}_K^0} N_{\mathcal{O}_\mathfrak{p}}(\mathfrak{D}_{\mathcal{O}_\mathfrak{p}|Z_p})$.

Proof. In Proposition 1.2.8, we saw that $|d_K|_\infty = N_{\mathcal{O}_K}(\mathfrak{D}_{\mathcal{O}_K|\mathbb{Z}})$. Corollary 2.3 in Chapter III of [Neu99] states that

$$\mathfrak{D}_{\mathcal{O}_K|\mathbb{Z}} = \prod_{\mathfrak{p}\in\mathfrak{P}_K^0} (\mathfrak{D}_{\mathcal{O}_\mathfrak{p}|Z_p} \cap \mathcal{O}_K).$$

Hence, we obtain that

$$|d_K|_\infty = N_{\mathcal{O}_K}\left(\prod_{\mathfrak{p}\in\mathfrak{P}_K^0}(\mathfrak{D}_{\mathcal{O}_\mathfrak{p}|Z_p}\cap\mathcal{O}_K)\right) = \prod_{\mathfrak{p}\in\mathfrak{P}_K^0} N_{\mathcal{O}_K}(\mathfrak{D}_{\mathcal{O}_\mathfrak{p}|Z_p}\cap\mathcal{O}_K),$$

using that $N_{\mathcal{O}_K}$ is a group homomorphism. So it remains to show that $N_{\mathcal{O}_K}(\mathfrak{D}_{\mathcal{O}_\mathfrak{p}|Z_p}\cap\mathcal{O}_K) = N_{\mathcal{O}_\mathfrak{p}}(\mathfrak{D}_{\mathcal{O}_\mathfrak{p}|Z_p})$ for any $\mathfrak{p}\in\mathfrak{P}_K^0$. By definition of the different, we have that $\mathfrak{D}_{\mathcal{O}_\mathfrak{p}|Z_p}$ is an integral ideal of $\mathcal{O}_\mathfrak{p}$. Thus, by Remark 1.4.3, we know that there exists some $k\in\mathbb{Z}_{\geq 0}$ such that $\mathfrak{D}_{\mathcal{O}_\mathfrak{p}|Z_p} = \mathfrak{m}_\mathfrak{p}^k$. By definition, we have

$$\mathfrak{m}_\mathfrak{p}^k = \{x\in K_\mathfrak{p} : \mathrm{ord}_\mathfrak{p}(x)\geq k\}.$$

Then

$$\mathfrak{m}_\mathfrak{p}^k\cap\mathcal{O}_K = \{x\in\mathcal{O}_K : \mathrm{ord}_\mathfrak{p}(x)\geq k\} = \mathfrak{p}^k.$$

So we see that

$$N_{\mathcal{O}_K}(\mathfrak{D}_{\mathcal{O}_\mathfrak{p}|Z_p}\cap\mathcal{O}_K) = N_{\mathcal{O}_K}(\mathfrak{m}_\mathfrak{p}^k\cap\mathcal{O}_K) = N_{\mathcal{O}_K}(\mathfrak{p}^k) = N_{\mathcal{O}_\mathfrak{p}}(\mathfrak{m}_\mathfrak{p}^k) = N_{\mathcal{O}_\mathfrak{p}}(\mathfrak{D}_{\mathcal{O}_\mathfrak{p}|Z_p}),$$

where we made use of Lemma 1.4.9. □

1.5 Places of Number Fields

This section builds on the previous section. Throughout this section let K be a number field.

Let $|.|$ be an absolute value of K. Then $|.|$ determines a metric of K by $d(x,y) := |x-y|$. This metric determines a topology on K.

Definition 1.5.1. Two absolute values of K are called *equivalent* when they define the same topology on K.

It can be shown that two absolute values $|.|_1$ and $|.|_2$ of K are equivalent if and only if there exists some $t\in\mathbb{R}_{\geq 0}$ such that $|x|_1 = |x|_2^t$ for all $x\in K$ (see [Neu99, Proposition 3.3, Chapter II]). It follows that an Archimedean absolute value cannot be equivalent to a non-Archimedean absolute value, and vice versa.

Definition 1.5.2. A *place* for K is a class of equivalent absolute values. Equivalence classes of non-Archimedean absolute values are called *finite places*, and equivalence classes of Archimedean absolute values are *infinite places*. The set of all places of K is denoted by $\mathcal{V}_K$.

These places can be related to the absolute values that we have seen in Example 1.4.5. The following result is given by Theorem 3.3 in [Con24c].

Theorem 1.5.3. Each non-Archimedean absolute value of K is equivalent to a $\mathfrak{p}$-adic absolute value for a unique non-zero prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$. Each Archimedean absolute value of K is equivalent to an absolute value induced from a real or complex field embedding of K.

It follows from uniqueness that the finite places are in bijection with the non-zero prime ideals of $\mathcal{O}_K$. Therefore, we will use finite places and non-zero prime ideals of $\mathcal{O}_K$ interchangeably. Moreover, the set of non-zero prime ideals of $\mathcal{O}_K$ and the set of finite places of K are both denoted by $\mathfrak{P}_K^0$. For any $x\in K$, we have $|x|_\sigma = |x|_{\overline{\sigma}}$ for some complex field embedding $\sigma\in\Sigma_K$. Therefore, a complex pair of field embeddings defines the same infinite place. Furthermore, non-conjugate field embeddings define non-equivalent absolute values. Hence, we see that the infinite places are in bijection with the field embeddings of K that are pairwise distinct and non-conjugate. Consequently, we have in total r_1+r_2 infinite places. Because of this bijection, we will use infinite places and field embeddings of K interchangeably. The set of infinite places will be denoted by Σ_K^∞. Set theoretically we have

$$\mathcal{V}_K = \mathfrak{P}_K^0\cup\Sigma_K^\infty.$$

Whenever we take an arbitrary place from $\mathcal{V}_K$, we will denote this by ν. Moreover, it makes sense to talk about $|.|_\nu$, using the absolute value we have seen in Example 1.4.5. If we specifically talk about finite places, we will denote a place by $\mathfrak{p}$. If we specifically talk about infinite places, we will denote a place by σ.

There is an interesting result relating the roots of unity with the absolute values corresponding to the infinite places of K. This result is stated in [Xia16, Corollary 1, Section 6.5].

Proposition 1.5.4. Let $a \in \mathcal{O}_K^*$. Then $a \in \mu_K$ if and only if $|a|_\sigma = 1$ for all $\sigma \in \Sigma_K^\infty$.

Definition 1.5.5. For any $\nu \in V_K$, the function $\|.\|_\nu \colon K_\nu \to \mathbb{R}$ defined by

$$\|x\|_\nu := \begin{cases} |x|_\nu, & \text{if } \nu \text{ is finite or corresponds to a real field embedding of } K, \\ |x|_\nu^2, & \text{if } \nu \text{ corresponds to a complex field embedding of } K, \end{cases}$$

is called the *normalized absolute value*.

So the only difference between normalized absolute values and the absolute values we have seen in Example 1.4.5, is that we take the square if ν corresponds to a complex field embedding of K. In this case, the normalized absolute value $\|.\|_\nu$ is not an absolute value as defined in Definition 1.4.4. Namely, it fails to satisfy the triangle inequality. We will see that for notation it is sufficiently great to make this distinction. The importance of considering places is seen through Proposition 1.3 of Chapter III in [Neu99].

Theorem 1.5.6 (Product Formula)**.** Let $x \in K^*$. Then $\|x\|_\nu = 1$ for almost all $\nu \in V_K$ and $\prod_{\nu \in \mathcal{V}_K} \|x\|_\nu = 1$.

1.6 Measure Theory

Throughout this thesis, we will need some measure theory. In this section, we will recall the basics of measure theory. We want to keep it as short as possible but still include all theory needed throughout this thesis. Someone familiar with measure theory is safe to skip this section. This section is based on [Coh13] and [Bog07].

Throughout this thesis, let $\bigsqcup$ denote the disjoint union. Let us now recall the most important structures in measure theory.

Definition 1.6.1. Let $\mathfrak{A}$ be any set. A collection $\mathcal{A}$ of subsets of $\mathfrak{A}$ is called a *σ-algebra* on $\mathfrak{A}$ if

i.) $\mathfrak{A} \in \mathcal{A}$,

ii.) if $A \in \mathcal{A}$, then $A^c := \mathfrak{A} \backslash A \in \mathcal{A}$,

iii.) if $A_i \in \mathcal{A}$ for all $i \in \mathbb{Z}_{>0}$, then $\bigcup_{i \geq 1} A_i \in \mathcal{A}$.

The elements of $\mathcal{A}$ are called *measurable sets*.

Definition 1.6.2. Let $\mathcal{A}$ be a *σ-algebra* on set $\mathfrak{A}$. A function $\mu \colon \mathcal{A} \to [0, \infty]$ is called a *measure* on $\mathcal{A}$ if

i.) $\mu(\emptyset) = 0$,

ii.) $\mu\left(\bigsqcup_{i \geq 1} A_i\right) = \sum_{i \geq 1} \mu(A_i)$ (*countable additive*).

An element $A \in \mathcal{A}$ is said to have *measure* $\mu(A)$. The measure μ is called *finite* if $\mu(\mathfrak{A}) < \infty$. If there exist measurable sets A_i such that $\mathfrak{A} = \bigcup_{i \geq 1} A_i$ and $\mu(A_i) < \infty$ for all $i \in \mathbb{Z}_{>0}$, then μ is called *σ-finite*.

Definition 1.6.3. A triple $(\mathfrak{A}, \mathcal{A}, \mu)$ is called a *measure space* if $\mathcal{A}$ is a σ-algebra on set $\mathfrak{A}$ and μ is a measure on $\mathcal{A}$. If μ is σ-finite, then the measure space is called *σ-finite*.

The following result will be used several times throughout this thesis.

Proposition 1.6.4. Let $(\mathfrak{A}, \mathcal{A}, \mu)$ be a measure space. Let $A, B \in \mathcal{A}$ such that $A \subseteq B$, then $\mu(A) \leq \mu(B)$. Moreover, if $\mu(A) < \infty$, then $\mu(B \backslash A) = \mu(B) - \mu(A)$.

For a proof of this result see the proof of Proposition 1.2.2 in [Coh13].

Let $\mathfrak{A}$ be any set. One can show that the intersection of any collection of σ-algebras on $\mathfrak{A}$ forms a σ-algebra on $\mathfrak{A}$ itself. Consequently, for any collection $\mathcal{E}$ of subsets of $\mathfrak{A}$, there exists a smallest (with respect to the inclusion of sets) σ-algebra containing $\mathcal{E}$. The proof of these results can be found in the proofs of [Coh13, Proposition 1.1.2 and Corollary 1.1.3].

Definition 1.6.5. Let $\mathcal{E}$ be a collection of subsets of set $\mathfrak{A}$. The smallest σ-algebra containing $\mathcal{E}$ is called the σ-algebra *generated* by $\mathcal{E}$ and is denoted by $\sigma(\mathcal{E})$.

We use the notion of generating σ-algebras in a special case.

Definition 1.6.6. Let X be a topological space, and $\mathcal{E}$ be the collection of open sets with respect to the topology. Then the σ-algebra generated by $\mathcal{E}$ is called the *Borel* σ-algebra on X and is denoted by $\mathcal{B}(X)$. The elements of $\mathcal{B}(X)$ are called *Borel measurable sets*. Furthermore, any measure on $\mathcal{B}(X)$ is called a *Borel measure* on $\mathcal{B}(X)$.

Proposition 1.6.7. Let X be a Hausdorff topological space. Then any compact subset of X is a Borel measurable set.

Proof. Let $C \subseteq X$ be a compact subset. Since X is Hausdorff, we know that C must be closed (see [Sin19, Theorem 5.1.8]). Therefore, we know that C^c is open, and so $C^c \in \mathcal{B}(X)$. Since $\mathcal{B}(X)$ is a σ-algebra, we have $C = (C^c)^c \in \mathcal{B}(X)$. □

Definition 1.6.8. Let X be a Hausdorff topological space and $\mu \colon \mathcal{B}(X) \to [0, \infty]$ a Borel measure on $\mathcal{B}(X)$. Then μ is called a *regular Borel measure* on $\mathcal{B}(X)$ if

i.) $\mu(A) < \infty$ for all compact $A \in \mathcal{B}(X)$,

ii.) $\mu(A) = \inf\{\mu(B) : A \subseteq B, B \text{ open}\}$ for all $A \in \mathcal{B}(X)$,

iii.) $\mu(A) = \sup\{\mu(B) : B \subseteq A, B \text{ compact}\}$, for all open sets $A \subseteq X$.

Remark 1.6.9. If we have everything the same as in Definition 1.6.8, but we require that the third condition holds for all Borel measurable sets, the measure is called a *Radon measure*. So any Radon measure is a regular Borel measure. However, it has to be said that sometimes this distinction between Radon measures and regular Borel measures fades away in the literature. This is due to its small difference in conditions, which in certain cases are equivalent. Therefore, in some literature, regular Borel measures are called Radon measures and vice versa. So to make things precise in this thesis, we will work with the convention as described in Section 7.2 of [Coh13]. So we only work with regular Borel measures as defined in Definition 1.6.8. We will ignore the notion of Radon measures. ♦

Example 1.6.10. Consider $\mathbb{R}^m$ for some $m \in \mathbb{Z}_{>0}$. We endow $\mathbb{R}^m$ with the Euclidean topology. The σ-algebra $\mathcal{B}(\mathbb{R}^m)$ admits a special measure, called the *Lebesgue measure*. This measure is constructed as follows. We define an *m-dimensional interval* to be an open and bounded set $B \subseteq \mathbb{R}^m$ of the form

$$B = I_1 \times \ldots \times I_m,$$

for some interval I_i in $\mathbb{R}$ for $1 \leq i \leq m$. The *volume* of an m-dimensional interval B is the product of the lengths of the interval I_i for $1 \leq i \leq m$ and is denoted by $\text{vol}(B)$. For any $A \in \mathcal{B}(\mathbb{R}^m)$, let $\mathcal{C}_A$ denote all sequences $(B_i)_{i \geq 1}$ of m-dimensional intervals such that $A \subseteq \bigcup_{i \geq 1} B_i$. Then the Lebesgue measure, denoted by μ_m, is given by

$$\mu_m(A) := \inf \left\{ \sum_{i \geq 1} \text{vol}(B_i) : (B_i)_{i \geq 1} \in \mathcal{C}_A \right\}.$$

Now, the Lebesgue measure is a regular Borel measure on $\mathcal{B}(\mathbb{R})$. Namely, the measure μ_m is finite on compact sets by construction. Furthermore, Proposition 1.4.1 of [Coh13] proves condition (ii.) and (iii.) of Definition 1.6.8. ■

Proposition 1.6.11. Let $T\colon \mathbb{R}^m \to \mathbb{R}^m$ be a linear transformation. Then for any $A \in \mathcal{B}(\mathbb{R}^m)$ the set $T(A)$ is Borel measurable. Moreover, the equality $\mu_m(T(A)) = |\det(T)|_\infty \mu_m(A)$ holds.

This result can be found in [Bog07, Corollary 3.6.4].

Enough on the Lebesgue measure. For the rest of this section, let $(\mathfrak{A}_i, \mathcal{A}_i, \mu_i)$ be a measure space for $i = 1, 2$. Furthermore, we endow $\mathbb{R}$ with the Euclidean topology and let $\overline{\mathbb{R}}$ denote the extended real line, i.e. the real line together with $\pm\infty$.

Definition 1.6.12. A map $f\colon \mathfrak{A}_1 \to \mathfrak{A}_2$ is called $(\mathcal{A}_1, \mathcal{A}_2)$-*measurable* if $f^{-1}(A) \in \mathcal{A}_1$ for all $A \in \mathcal{A}_2$. Moreover, a function $g\colon \mathfrak{A}_1 \to \overline{\mathbb{R}}$ is called $\mathcal{A}_1$-*measurable* if $f^{-1}(A) \in \mathcal{A}_1$ for all $A \in \mathcal{B}(\mathbb{R})$.

Proposition 1.6.13. Let $\mathcal{A}_2$ be the σ-algebra generated by $\mathcal{E}$. Then $f\colon \mathfrak{A}_1 \to \mathfrak{A}_2$ is $(\mathcal{A}_1, \mathcal{A}_2)$-measurable if $f^{-1}(E) \in \mathcal{A}_1$ for all $E \in \mathcal{E}$.

This result is Proposition 2.6.2 of [Coh13].

Definition 1.6.14. Let $f\colon \mathfrak{A}_1 \to \overline{\mathbb{R}}$ be an $\mathcal{A}_1$-measurable function. The *integral* of f over $\mathfrak{A}_1$ with respect to μ is formally defined by

$$\int_{\mathfrak{A}_1} f(a)\mu(da).$$

Whenever this integral is finite, the function f is called *integrable* with respect to μ.

The definition and construction of this integral relies on simple and non-negative functions. Because this is quite expensive to write down, we refer to Section 2.3 of [Coh13]. Next, we look at the Change of Variables analogue for these measure integrals.

Theorem 1.6.15. Let $f\colon \mathfrak{A}_1 \to \mathfrak{A}_2$ be an $(\mathcal{A}_1, \mathcal{A}_2)$-measurable map, and $g\colon \mathfrak{A}_2 \to \overline{\mathbb{R}}$ an $\mathcal{A}_2$-measurable function. Suppose that μ_1 is non-zero. Then $f^*\mu_1 := \mu_1 \circ f^{-1}$ is a measure on $\mathcal{A}_2$. Furthermore, the function $g \circ f$ is integrable with respect to μ_1 if and only if g is integrable with respect to $f^*\mu_1$. Moreover, one has

$$\int_{\mathfrak{A}_2} g(b)(f^*\mu_1)(db) = \int_{\mathfrak{A}_1} g(f(a))\mu_1(da).$$

Proof. See the proof of Theorem 3.6.1 in [Bog07]. □

Suppose that $(\mathfrak{A}_i, \mathcal{A}_i, \mu_i)$ are σ-finite measure spaces for $i = 1, 2$. Then there is a way to create a σ-algebra on the Cartesian product $\mathfrak{A}_1 \times \mathfrak{A}_2$.

Definition 1.6.16. The σ-algebra on $\mathfrak{A}_1 \times \mathfrak{A}_2$, generated by $\mathcal{E} := \{A_1 \times A_2 | A_1 \in \mathcal{A}_1, A_2 \in \mathcal{A}_2\}$, is called the *product σ-algebra* on $\mathfrak{A}_1$ and $\mathfrak{A}_2$ and is denoted by $\mathcal{A}_1 \otimes \mathcal{A}_2$.

We have $\sigma(\mathcal{E}) = \mathcal{A}_1 \otimes \mathcal{A}_2$. Now, let A be a subset of $\mathfrak{A}_1 \times \mathfrak{A}_2$. For $a \in \mathfrak{A}_1$ we define

$$A_a := \{b \in \mathfrak{A}_2 : (a, b) \in A\}. \tag{10}$$

Similarly, for $b \in \mathfrak{A}_2$ we define

$$A^b := \{a \in \mathfrak{A}_1 : (a, b) \in A\}.$$

Proposition 1.6.17. For all $a \in \mathfrak{A}_1$ one has $A_a \in \mathcal{A}_2$, and the function $a \mapsto \mu_2(A_a)$ is $\mathcal{A}_1$-measurable. Likewise, for all $b \in \mathfrak{A}_2$ one has $A^b \in \mathcal{A}_1$ and the function $b \mapsto \mu_1(A^b)$ is $\mathcal{A}_2$-measurable.

These results can be found in Lemma 5.1.2 and Proposition 5.1.3 of [Coh13]. Now, as stated in Theorem 5.1.4 in [Coh13], there is a unique measure on $\mathcal{A}_1 \otimes \mathcal{A}_2$, denoted by $\mu_1 \otimes \mu_2$, that satisfies

$$(\mu_1 \otimes \mu_2)(A_1 \times A_2) = \mu_1(A_1)\mu_2(A_2),$$

for any $A_1 \in \mathcal{A}_1$ and $A_2 \in \mathcal{A}_2$. For any set $A \in \mathcal{A}_1 \otimes \mathcal{A}_2$ the measure is given by

$$(\mu_1 \otimes \mu_2)(A) = \int_{\mathfrak{A}_1} \mu_2(A_a)\mu_1(da) = \int_{\mathfrak{A}_2} \mu_1(A^b)\mu_2(db). \tag{11}$$

Definition 1.6.18. The unique measure $\mu_1 \otimes \mu_2$ is called the *product measure* of μ_1 and μ_2.

Definition 1.6.19. The measure space $(\mathfrak{A}_1 \times \mathfrak{A}_2, \mathcal{A}_1 \otimes \mathcal{A}_2, \mu_1 \otimes \mu_2)$ is called the *product measure space* of $(\mathfrak{A}_1, \mathcal{A}_1, \mu_1)$ and $(\mathfrak{A}_2, \mathcal{A}_2, \mu_2)$.

1.7 Classical Theory of Lattices

In this section, we will introduce lattices in Euclidean spaces and see Minkowski's Convex Body Theorem. This section is based on Section 4 of Chapter I in [Neu99].

Let V be a Euclidean space, that is, a finite-dimensional $\mathbb{R}$-vector space equipped with a positive definite, symmetric, and bilinear map, i.e. an inner product. Throughout this section we set $\dim_{\mathbb{R}} V = m$, and denote the inner product by $\langle \cdot, \cdot \rangle \colon V \times V \to \mathbb{R}$. We endow V with the topology induced from the inner product. Therefore, the space V induces the Borel σ-algebra $\mathcal{B}(V)$.

Definition 1.7.1. A *lattice* in V is a subgroup of the form

$$\Gamma = u_1\mathbb{Z} + \ldots + u_k\mathbb{Z},$$

for linearly independent vectors $u_1, \ldots, u_k \in V$. Whenever k equals m, the lattice Γ is called *complete*.

Remark 1.7.2. A subgroup Γ in V is a lattice if and only if Γ is discrete. That is to say that for all $u \in \Gamma$ there exists some open set A in V such that $u \in A$ and $\Gamma \cap A = \{u\}$ (see [Neu99, Proposition 4.2, Chapter I]). We will see a generalization of this notion in Definition 2.3.1. ♦

Let Γ be a lattice in V. Consider the quotient group V/Γ. We endow this space with the quotient topology (see [Sin19, Definition 6.1.1]).

Proposition 1.7.3. Let Γ be a lattice in V. Then the following statements are equivalent.

i.) Γ is complete.

ii.) There exists a bounded subset $B \subseteq V$ such that $V = \bigcup_{u \in \Gamma}(u + B)$.

iii.) V/Γ is compact with respect to the quotient topology.

Proof. The fact that Statement (i.) is equivalent to Statement (ii.) is given by Lemma 4.3 of Chapter I in [Neu99]. So we only need to show that Statement (ii.) and (iii.) are equivalent. Now, suppose that there exists a bounded subset $B \subseteq V$ such that $V = \bigcup_{u \in \Gamma}(u + B)$. Then the closure of B, denoted by $\overline{B}$, is closed and bounded. By the Heine-Borel Theorem (see [Sut09, Theorem 13.22]) it follows that $\overline{B}$ is compact in V. Consider the canonical map $\phi \colon V \to V/\Gamma$. This map is continuous and an open mapping (see [Sin19, Proposition 12.3.1]). Then ϕ is surjective once restricted to $\overline{B}$. Hence, we see that V/Γ is the image of a compact space under a continuous map. Therefore, it is compact itself (see [Sin19, Theorem 5.1.11]).

Conversely, suppose that $\mathcal{V}/\Gamma$ is compact. Let I be an index set and $\{A_i\}_{i\in I}$ an open cover of bounded subsets of V. Since ϕ is an open mapping, the set $\{\phi(A_i)\}_{i\in I}$ forms an open covering of V/Γ. By compactness, there exists a finite index set $J \subseteq I$ such that $\{\phi(A_j)\}_{j\in J}$ forms an open covering of V/Γ. Thus

$$\begin{aligned} V/\Gamma = \bigcup_{j\in J} \phi(A_j) &\implies \phi^{-1}(V/\Gamma) = \phi^{-1}\left(\bigcup_{j\in J} \phi(A_j)\right) \\ &\implies V = \bigcup_{j\in J} \phi^{-1}(\phi(A_j)) \\ &\implies V = \left(\bigcup_{j\in J} A_j\right) + \Gamma. \end{aligned}$$

Since each A_j is bounded, we have that $B := \left(\bigcup_{j\in J} A_j\right)$ is bounded. So we get

$$V = B + \Gamma = \bigcup_{u\in\Gamma} (B + u),$$

with a bounded subset B of V. □

Definition 1.7.4. Let Γ be a complete lattice in V. A *fundamental region* of the lattice Γ is a Borel measurable set $\Lambda \subseteq V$ such that $V = \bigsqcup_{u\in\Gamma}(\Lambda + u)$.

For a complete lattice Γ we can explicitly describe a fundamental region of the lattice Γ. Namely, let Γ be of the form $u_1\mathbb{Z} + \ldots + u_m\mathbb{Z}$, for linearly independent vectors $u_1, \ldots, u_m \in V$. Then a fundamental region is given by

$$\Lambda := \left\{ \sum_{i=1}^{m} t_i u_i : 0 \le t_i < 1, \text{ for all } i \right\}. \tag{12}$$

For Euclidean spaces, the inner product gives us a notion of volume. More generally, it gives us a Haar measure. But this will only be introduced later on (see Definition 2.2.3). For any set of the form

$$\left\{ \sum_{i=1}^{m} t_i u_i : 0 \le t_i < 1, \text{ for all } i \right\},$$

for linearly independent vectors $v_1, \ldots, v_m \in V$, we set the volume to be

$$\sqrt{|\det([\langle v_i, v_j\rangle]_{1\le i,j\le k})|_\infty}.$$

The set

$$\left\{ \sum_{i=1}^{m} t_i e_i : 0 \le t_i < 1, \text{ for all } i \right\},$$

for an orthonormal basis $e_1, \ldots, e_m \in V$ has volume 1.

Definition 1.7.5. Let Γ be a complete lattice in V and Λ a fundamental region of Γ. The *covolume* of Γ, denoted by covol(Γ), is defined to be the volume of the fundamental region (12).

One of the main results of complete lattices in Euclidean spaces is Minkowski's Convex Body Theorem. The proof of this theorem can be found in the proof of Theorem 4.4 of Chapter I in [Neu99].

Definition 1.7.6. Let A be a subset of V. The set A is said to be *symmetric* if for all $u \in A$ also $-u \in A$.

Definition 1.7.7. Let A be a subset of V. The set A is said to be *convex* if $tu+(1-t)v \in A$ for all $u, v \in A$ and $t \in [0,1]$.

Theorem 1.7.8 (Minkowski's Convex Body Theorem)**.** Let Γ be a complete lattice in V, and $A \subseteq V$ a symmetric and convex Borel measurable set. If the volume of A is strictly bigger than $2^m \operatorname{covol}(\Gamma)$, then A contains at least one non-zero lattice point of Γ.

Remark 1.7.9. If one analyzes the proof of Minkowski's Convex Body Theorem, one notices that the assumption of convexity can be weakened. One only has to assume that $\frac{1}{2}u + \frac{1}{2}v \in A$ for all $u, v \in A$. So that is to say that Definition 1.7.7 only needs to hold for $t = \frac{1}{2}$. This observation will be useful later on. ♦

1.8 Minkowski Theory

In this section, we will construct the Minkowski space. This is an example of a Euclidean space. Therefore, we can use the theory from the last section. It can be shown that the fractional ideals of $\mathcal{O}_K$ are complete lattices in this space. This section is based on Section 5 of Chapter I in [Neu99].

The following results on tensor products will be used throughout this thesis.

Proposition 1.8.1. Let R be a domain and M a free R-module of rank r. For any ring R', that can be viewed as an R-module, the R'-module $R' \otimes_R M$ is free of rank r.

Proof. Use bilinearity over R to show that $\{1 \otimes m_i\}_{1 \leq i \leq r}$ is a basis of $R' \otimes_R M$, for a given basis $\{m_i\}_{1 \leq i \leq r}$ of R-module M. □

Proposition 1.8.2. Let R be a domain and F its field of fractions. Moreover, let V be an F-vector space. For any non-zero R-module M inside F we have $M \otimes_R V \cong V$, as R-modules. In particular, for any non-zero fractional ideal I of R, we have $I \otimes_R V \cong V$.

Proof. The R-module isomorphism is given by the linear extension of the map $M \otimes_R V \to V$ defined by $m \otimes v \mapsto mv$. □

Let K be a number field of degree $n = r_1 + 2r_2$, and set $K_{\mathbb{C}} := \prod_{\sigma \in \Sigma_K} \mathbb{C} = C^n$. We can embed K into $K_{\mathbb{C}}$ through the embedding $\Psi \colon K \to K_{\mathbb{C}}$ defined by $x \mapsto (\sigma(x))_{\sigma \in \Sigma_K}$.

Definition 1.8.3. The embedding Ψ is called the *Minkowski embedding* of K.

The Minkowski embedding is not surjective. Therefore, it is common to take a different codomain for it. Recall that Σ_K contains real and complex field embeddings (see Definition 1.2.1). Denote any real field embedding by $\rho \colon K \to \mathbb{R}$ (in total r_1 field embeddings), and the set of all real field embeddings by $\Sigma_K^{\mathbb{R}}$. Any pair of complex field embeddings that are conjugate is denoted by $\tau, \overline{\tau} \colon K \to \mathbb{C}$ (in total r_2 pairs). Take one choice of every pair and put them together in the set $\Sigma_K^{\mathbb{C}}$. Recall that the infinite places of K are in bijection with the field embeddings of K that are pairwise distinct and non-conjugate. Therefore, we have

$$\Sigma_K^{\infty} = \Sigma_K^{\mathbb{R}} \cup \Sigma_K^{\mathbb{C}}.$$

For any $\tau \in \Sigma_K^{\mathbb{C}}$, we have $\overline{\tau}(x) = \overline{\tau(x)}$ for all $x \in K$. Therefore, the codomain of Ψ is commonly restricted to

$$K_{\mathbb{R}} := \left\{ (u_\sigma)_{\sigma \in \Sigma_K} \in \prod_{\sigma \in \Sigma_K} \mathbb{C} : u_\rho \in \mathbb{R} \text{ for all } \rho \in \Sigma_K^{\mathbb{R}}, \overline{u_\tau} = u_{\overline{\tau}} \in \mathbb{C} \text{ for all } \tau \in \Sigma_K^{\mathbb{C}} \right\} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}. \tag{13}$$

There are various ways to describe $K_{\mathbb{R}}$. We have the $\mathbb{R}$-vector space isomorphisms given by

$$K_{\mathbb{R}} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2} \cong \mathbb{R}^n.$$

It follows that $K_\mathbb{R}$ is an n-dimensional $\mathbb{R}$-vector space. Recall that $K = \mathbb{Q}(\gamma)$ for some primitive element $\gamma \in K$. Let f be the minimal polynomial of γ. Then $K \cong \mathbb{Q}[t]/f(t)$. So $K_\mathbb{R}$ is also isomorphic as $\mathbb{R}$-vector space to $K \otimes_\mathbb{Q} \mathbb{R}$.

$$K \otimes_\mathbb{Q} \mathbb{R} \cong \mathbb{Q}[t]/f(t) \otimes_\mathbb{Q} \mathbb{R} \cong \mathbb{R}[t]/f(t) \cong \mathbb{R}^n,$$

where the last ring isomorphism follows from the fact that $\deg(f) = n$. Furthermore, we also have the isomorphism of $\mathbb{R}$-vector space given by $K_\mathbb{R} \cong \mathcal{O}_K \otimes_\mathbb{Z} \mathbb{R}$. Namely, we know that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n. So using Proposition 1.8.1, we have that $\mathcal{O}_K \otimes_\mathbb{Z} \mathbb{R}$ is an n-dimensional $\mathbb{R}$-vector space. Lastly, and maybe the most convenient one, we have by Theorem 1.4.8 that $K_\rho \cong \mathbb{R}$ for any $\rho \in \Sigma_K^\mathbb{R}$, and $K_\tau \cong \mathbb{C}$ for any $\tau \in \Sigma_K^\mathbb{C}$. Hence, we obtain

$$K_\mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \prod_{\rho \in \Sigma_K^\mathbb{R}} K_\rho \times \prod_{\tau \in \Sigma_K^\mathbb{C}} K_\tau = \prod_{\sigma \in \Sigma_K^\infty} K_\sigma.$$

We change between the different representations of $K_\mathbb{R}$ whenever one is more convenient to work within a given setting.

Remark 1.8.4. Since $K_\mathbb{R} = \prod_{\sigma \in \Sigma_K^\infty} K_\sigma$, we have the inclusion $\prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}_{>0} \subseteq K_\mathbb{R}$. Furthermore, for any $u \in K_\mathbb{R}$, there exists some $u_\sigma \in K_\sigma$ for all $\sigma \in \Sigma_K$ such that $u = (u_\sigma)_{\sigma \in \Sigma_K}$. Moreover, we set $\overline{u} := (\overline{u_\sigma})_{\sigma \in \Sigma_K}$. We use these conventions throughout this thesis. ♦

The $\mathbb{C}$-vector space $K_\mathbb{C}$ comes with a Hermitian inner product given by

$$\langle u, v \rangle_\mathbb{C} := \sum_{\sigma \in \Sigma_K} u_\sigma \overline{v_\sigma},$$

for any $u, v \in K_\mathbb{C}$. Now, view $K_\mathbb{R}$ as in (13). Then we can restrict $\langle \cdot, \cdot \rangle_\mathbb{C}$ to $K_\mathbb{R}$. Take any $u, v \in K_\mathbb{R}$. If $\rho \in \Sigma_K^\mathbb{R}$, we have $u_\rho, v_\rho \in \mathbb{R}$. It follows that $u_\rho \overline{v_\rho} = u_\rho v_\rho = \Re(u_\rho \overline{v_\rho})$. If we take $\tau \in \Sigma_K^\mathbb{C}$, then $\overline{u_\tau} = u_{\overline{\tau}}$ and $\overline{v_\tau} = v_{\overline{\tau}}$. Hence

$$u_\tau \overline{v_\tau} + u_{\overline{\tau}} \overline{v_{\overline{\tau}}} = u_\tau \overline{v_\tau} + \overline{u_\tau} v_\tau = u_\tau \overline{v_\tau} + \overline{u_\tau \overline{v_\tau}} = 2\Re(u_\tau \overline{v_\tau}),$$

using that in general $z + \overline{z} = 2\Re(z)$ for any $z \in \mathbb{C}$. So using Definition 1.2.4, we have

$$\langle u, v \rangle_\mathbb{R} := \langle u, v \rangle_\mathbb{C} = \sum_{\sigma \in \Sigma_K} u_\sigma \overline{v_\sigma} = \sum_{\sigma \in \Sigma_K^\infty} \deg(\sigma) \Re(u_\sigma \overline{v_\sigma}).$$

Notice, in the last summation we run over Σ_K^∞ instead of Σ_K. This is because we combined the conjugate complex field embeddings. Since this is a real-valued map, we see that $\langle u, v \rangle_\mathbb{R} = \langle v, u \rangle_\mathbb{R}$. Consequently, we obtain an inner product on $K_\mathbb{R}$. Since $K_\mathbb{R}$ is a finite-dimensional $\mathbb{R}$-vector space, it is a Euclidean space.

Remark 1.8.5. The Minkowski space is an n-dimensional $\mathbb{R}$-vector space, and therefore isomorphic as $\mathbb{R}$-vector space to $\mathbb{R}^n$. Viewing $K_\mathbb{R}$ as $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, one can define an isomorphism $f \colon K_\mathbb{R} \to \mathbb{R}^n$ given by

$$(u_1, \ldots, u_{r_1}, u_{r_1+1}, \ldots, u_{r_2}) \mapsto (u_1, \ldots, u_{r_1}, \Re(u_{r_1+1}), \Im(u_{r_1+1}), \Re(u_{r_1+2}), \Im(u_{r_1+2}), \ldots, \Re(u_{r_2}), \Im(u_{r_2})).$$

Due to this isomorphism, one can transform the inner product $\langle \cdot, \cdot \rangle_\mathbb{R}$ to an inner product on $\mathbb{R}^n$. For $(u_\sigma)_{\sigma \in \Sigma_K}, (v_\sigma)_{\sigma \in \Sigma_K} \in \prod_{\sigma \in \Sigma_K} \mathbb{R} = \mathbb{R}^n$, this inner product is given by

$$\langle u, v \rangle = \sum_{\sigma \in \Sigma_K} \deg(\sigma) u_\sigma v_\sigma. \tag{14}$$

If $r_2 > 0$, this transformation is different from the dot product on $\mathbb{R}^n$. In Section 1.7, we saw that the inner product on Euclidean spaces gives us a notion of volume. Therefore, we can induce a volume on $\mathbb{R}^n$ using the dot product. This equals the Lebesgue measure as seen in Example 1.6.10. On the other hand, we can induce a volume on $\mathbb{R}^n$ using the inner product (14). Set the later to be $\mathrm{vol}_\mathbb{R}$, then for any Borel measurable set A, we have

$$\mathrm{vol}_\mathbb{R}(A) = 2^{r_2} \mu_n(A),$$

where μ_n is the Lebesgue measure on $\mathcal{B}(\mathbb{R}^n)$. For more information, see Proposition 5.1 in Chapter I of [Neu99]. ♦

Theorem 1.8.6. Let I be a non-zero fractional ideal of $\mathcal{O}_K$. Then $\Psi(I)$ is a complete lattice in $K_{\mathbb{R}}$. Moreover, the covolume of $\Psi(I)$ is given by

$$\mathrm{covol}(\Psi(I)) = N_{\mathcal{O}_K}(I)\sqrt{|d_K|_\infty},$$

where d_K is the discriminant of K.

The proof for non-zero integral ideals is given by the proof of Proposition 5.2 of Chapter I in [Neu99]. For any fractional ideal I of $\mathcal{O}_K$ there exists some $a \in \mathcal{O}_K$ such that aI is an integral ideal. Using this fact, one can extend this theorem to any fractional ideal. We will not prove this explicitly, because in Theorem 3.4.6 and Proposition 3.4.8 we will prove a generalization.

2 General Theory of Lattices

In Section 1.7, we have seen the construction of lattices in Euclidean spaces. A Euclidean space is locally compact and Hausdorff as topological space. Moreover, a Euclidean space has an underlying additive group structure. Therefore, a Euclidean space is an example of what we will define to be a locally compact group (see Definition 2.2.1). We will define a generalization of lattices in these types of groups. This construction is not new and can be found in the literature. However, it happens many times that the literature is incomplete. Often, the literature defines lattices for locally compact groups but does not examine the existence of fundamental regions and the notion of covolumes. This is because one needs some extra structure on locally compact groups to show existence. These groups will be called L-groups. On the other hand, sometimes lattices are considered in L-groups in the literature. But in that case, the general notion of lattices in locally compact groups is often avoided. In this chapter, we want to derive the complete story. All the proofs of the results obtained in this chapter are self-written.

2.1 Topological Groups

In this section, we give a brief summary of the theory of topological groups. Throughout this thesis, we will write the group operation of any arbitrary group (not necessarily abelian) additively and denote its unit element by 0.

Let G be a group (not necessarily abelian) and endow G with any topology. In the following definition, we take the product topology on $G \times G$. For the definition of the product topology, see Section 2.2 in [Sin19].

Definition 2.1.1. The group G is called a *topological group* if the maps $G \to G$ given by $g \mapsto -g$ and $G \times G \to G$ given by $(g, h) \mapsto g + h$ are continuous with respect to the respective topologies.

Recall that a map $f\colon X \to Y$ of topological spaces X, Y is called a *homeomorphism* if it is bijective and f and its inverse is continuous. In that case, we say that X and Y are *homeomorphic*.

Proposition 2.1.2. Let G be a topological group and $h \in G$. Then the maps defined by $g \mapsto h+g$, $g \mapsto g+h$, and $g \mapsto -g$ are homeomorphisms of G onto G.

This result is Proposition 9.1.2 of [Coh13].

Corollary 2.1.3. Let G be a topological group and $h \in G$. Then the maps defined by $g \mapsto h + g$, $g \mapsto g + h$, and $g \mapsto -g$ are $(\mathcal{B}(G), \mathcal{B}(G))$-measurable.

Proof. By Proposition 2.1.2, the maps are homeomorphisms. Hence, for any open subset in G, the pre-images of these maps are open in G. Since $\mathcal{B}(G)$ is generated by the open sets of G, it follows from Proposition 1.6.13 that these maps are $(\mathcal{B}(G), \mathcal{B}(G))$-measurable. □

Corollary 2.1.4. Let G be a topological group, $h \in G$, and A any subset of G. If A is open (resp. measurable), then the sets $h + A$, $A + h$, and $-A$ are open (resp. measurable).

Proof. The set $h + A$ is the pre-image of A under the map given by $g \mapsto g - h$. If A is open, it follows from Proposition 2.1.2 that $h + A$ is open. If A is measurable, it follows by Corollary 2.1.3 that $h + A$ is measurable. By symmetry, we can show that the same argument works for $A + h$. Moreover, a similar argument, with the map given by $g \mapsto -g$, works for the set $-A$. □

Proposition 2.1.5. Let G be a topological group. Every open neighborhood A of 0 contains an open neighborhood B such that $B = -B$ and $B + B \subseteq A$.

For a proof of this result see the proof of [Sin19, Lemma 12.1.5].

2.2 Locally Compact Groups and Haar Measures

In this section, we introduce a specific type of measure on topological groups, so-called left/right Haar measures. There is a fundamental result for these left/right Haar measures on locally compact groups.

All properties of topological spaces, e.g. Hausdorff, compact, complete, locally compact, second-countable, etc. carry over to a topological group.

Definition 2.2.1. A topological group is called a *locally compact group* if it is locally compact and Hausdorff.

Let G be a topological group and H a subgroup of G. Denote the set of all left cosets $g + H$ for $g \in G$ by G/H. Let $\phi : G \to G/H$ be the canonical map given by $g \mapsto g + H$. We endow the set G/H with the quotient topology, that is, a set $A \subseteq G/H$ is open if $\phi^{-1}(A)$ is open in G. Therefore, the map ϕ is also continuous. Similarly, one can create a topology on the set of right cosets $H + g$ for $g \in G$, denoted by $H\backslash G$. One can show that the map $f : G/H \to H\backslash G$ defined by $g + H \mapsto H - g$ is a homeomorphism. We will mostly be focused on G/H, but because of this homeomorphism, everything can be carried over to $H\backslash G$. If the subgroup H is normal then the set G/H forms a group. Since G is a topological group, the map $f\colon G \to G$ defined by $g \mapsto -g$ is continuous. The map $f'\colon G/H \to G/H$ defined by $g + H \to -g + H$ is the composition of ϕ and f. Since ϕ and f are continuous, so is f'. A similar argument shows that the map $G/H \times G/H \to G/H$ defined by $(g + H, h + H) \to (g + h) + H$ is continuous. Hence, by Definition 2.1.1, the group G/H is a topological group. But remember this is only the case if H is normal.

Proposition 2.2.2. Let H be a closed subgroup of locally compact group G. Then G/H is a locally compact Hausdorff space. Moreover, if H is normal, then G/H is a locally compact group.

Proof. Proposition 12.3.2 of [Sin19] tells us that G/H must be Hausdorff since H is closed. Take any $g + H \in G/H$ for some $g \in G$. Since G is locally compact, there exists a compact subset $C \subseteq G$ such that $g \in C$. Consider the canonical map $\phi\colon G \to G/H$. Since ϕ is continuous, Theorem 15.1.11 in [Sin19] tells us that $\phi(C) \subseteq G/H$ is compact. Hence, the set $\pi(C)$ is a compact neighborhood of $g + H$. This says precisely that G/H must be locally compact as well. As a result of this, we know that G/H is a locally compact Hausdorff space. If H is normal, then G/H becomes a topological group. In that case, the group G/H is a locally compact group. □

The following definition is an important type of measure on Hausdorff topological groups.

Definition 2.2.3. Let G be a Hausdorff topological group and $\mu\colon \mathcal{B}(G) \to [0, \infty]$ a non-zero regular Borel measure on $\mathcal{B}(G)$. Then μ is called a *left Haar measure* on $\mathcal{B}(G)$ if for any $g \in G$ and $A \in \mathcal{B}(G)$ one has $\mu(g + A) = \mu(A)$.

The Euclidean space $\mathbb{R}^m$ is a locally compact group for any $m \in \mathbb{Z}_{>0}$. In Example 1.6.10, we have seen that the Lebesgue measure on $\mathcal{B}(\mathbb{R}^m)$ is a regular Borel measure. It turns out that the Lebesgue measure is even a left Haar measure. This is shown in Proposition 1.4.4 of [Coh13]. The following theorem is a fundamental result of locally compact groups.

Theorem 2.2.4. Let G be a locally compact group. Then $\mathcal{B}(G)$ attains a unique left Haar measure up to scalar multiple.

Theorem 9.2.2 in [Coh13] proves the existence, and Theorem 9.2.6 in [Coh13] proves the uniqueness.

Remark 2.2.5. We conclude that a locally compact group G induces a measure space $(G, \mathcal{B}(G), \mu_G)$, where μ_G is a left Haar measure on $\mathcal{B}(G)$. ♦

By symmetry, one can define right Haar measures.

Definition 2.2.6. Let G be a Hausdorff topological group and $\mu\colon \mathcal{B}(G) \to [0, \infty]$ a non-zero regular Borel measure on $\mathcal{B}(G)$. Then μ is called a *right Haar measure* on $\mathcal{B}(G)$ if for any $g \in G$ and $A \in \mathcal{B}(G)$ one has $\mu(A + g) = \mu(A)$.

Theorem 2.2.4 holds for right Haar measures (see [Coh13, Corollary 9.3.2]). We want to study when the collection of left Haar measures coincides with the collection of right Haar measures.

Let G be a locally compact group and μ a left Haar measure on $\mathcal{B}(G)$. In Proposition 2.1.2, we saw that the map $f_g\colon G \to G$ defined by $h \mapsto h + g$ is a homeomorphism for any $g \in G$. By verifying the conditions of Definition 1.6.8 we have that $\mu_g := \mu \circ f_g$ is a regular Borel measure on $\mathcal{B}(G)$. Furthermore, for any $h \in G$ and $A \in \mathcal{B}(G)$, we have

$$\mu_g(h + A) = \mu(f_g(h + A)) = \mu(h + A + g) = \mu(A + g) = \mu_g(A),$$

using that μ is a left Haar measure. Hence, also μ_g is a left Haar measure on $\mathcal{B}(G)$. We will use the construction of this left Haar measure throughout this section. By Theorem 2.2.4, this means that there exists a $\Delta(g) \in \mathbb{R}_{>0}$, depending on $g \in G$, such that $\mu_g = \Delta(g)\mu$. In this way, we create a map $\Delta\colon G \to \mathbb{R}_{>0}$. Notice, the map Δ is defined from the choice of left Haar measure μ on $\mathcal{B}(G)$. However, it turns out that this is independent of this choice.

Proposition 2.2.7. Let G be a locally compact group. The map $\Delta\colon G \to \mathbb{R}_{>0}$ is independent of the choice of left Haar measure on $\mathcal{B}(G)$.

Proof. Let $\Delta\colon G \to \mathbb{R}_{>0}$ be the map such that $\mu_g = \Delta(g)\mu$ for some left Haar measure μ on $\mathcal{B}(G)$. Now, let χ be another left Haar measure on $\mathcal{B}(G)$. Then by Theorem 2.2.4, there exists some $\lambda \in \mathbb{R}_{>0}$ such that $\chi = \lambda\mu$. Set $\chi_g = \chi \circ f_g$, then for any $A \in \mathcal{B}(G)$, we have

$$\chi_g(A) = \chi(f_g(A)) = \lambda\mu(f_g(A)) = \lambda\mu_g(A) = \Delta(g)\lambda\mu(A) = \Delta(g)\chi(A).$$

Hence, we see that $\chi_g = \Delta(g)\chi$. □

By Proposition 2.2.7, we see that the map $\Delta : G \to \mathbb{R}_{>0}$ depends only on the group G. Therefore, the following definition makes sense.

Definition 2.2.8. Let G be a locally compact group. The map $\Delta : G \to \mathbb{R}_{>0}$ is called the *modular map* of G.

Definition 2.2.9. A locally compact group G is called *unimodular* if $\Delta(g) = 1$ for all $g \in G$.

Proposition 2.2.10. Let G be a locally compact group. The group G is unimodular if and only if the collection of left Haar measure on $\mathcal{B}(G)$ coincides with the collection of right Haar measures on $\mathcal{B}(G)$.

Proof. Suppose that G is unimodular. Let μ be a left Haar measure on $\mathcal{B}(G)$. Since G is unimodular, we have $\Delta(g) = 1$ for all $g \in G$. Thus, for any $g \in G$ and $A \in \mathcal{B}(G)$, we have

$$\mu(A + g) = \mu(f_g(A)) = \mu_g(A) = \Delta(g)\mu(A) = \mu(A).$$

Hence, the measure μ is a right Haar measure on $\mathcal{B}(G)$. Conversely, let μ be a right Haar measure on $\mathcal{B}(G)$. For any $A \in \mathcal{B}(G)$, we have seen in Corollary 2.1.4 that $-A \in \mathcal{B}(G)$. Define $\chi(A) := \mu(-A)$. Then Proposition 9.3.1 in [Coh13] shows that $\chi\colon \mathcal{B}(G) \to [0, \infty]$ is a left Haar measure on $\mathcal{B}(G)$. As a result of our earlier observation, we have that χ is also a right Haar measure on $\mathcal{B}(G)$. Since $\mu(A) = \chi(-A)$, Proposition 9.3.1 in [Coh13] says as well that μ is a left Haar measure.

Conversely, suppose that the collection of left Haar measure on $\mathcal{B}(G)$ coincides with the collection of right Haar measures on $\mathcal{B}(G)$. Suppose that μ is a left and right Haar measure on $\mathcal{B}(G)$. Then for any $g \in G$ and $A \in \mathcal{B}(G)$, we have

$$\mu_g(A) = \mu(f_g(A)) = \mu(A + g) = \mu(A) = \mu(A).$$

It follows that $\Delta(g) = 1$ for all $g \in G$. Consequently, the group G is unimodular by definition. □

If we consider unimodular groups, we will simply speak about Haar measures, rather than left or right Haar measures. We can look into a few examples of unimodular locally compact groups.

Proposition 2.2.11. Let G be a locally compact group. If G is abelian or has the discrete topology, then it is unimodular.

Proof. Suppose that G is abelian. Then any left Haar measure on $\mathcal{B}(G)$ is a right Haar measure on $\mathcal{B}(G)$ and vice versa. One simply uses the fact that G is abelian. It follows from Proposition 2.2.10 that G is unimodular.

Suppose that the topology on G is discrete. Example 9.2.1 in [Coh13] tells us that the counting measure is a left Haar measure on $\mathcal{B}(G)$. For any $A \in \mathcal{B}(G)$, the counting measure is given by

$$\mu(A) := \begin{cases} \#A, & \text{if } \#A < \infty, \\ \infty, & \text{otherwise.} \end{cases}$$

For any $g \in G$ and $A \in \mathcal{B}(G)$, we have $\#(A + g) = \#A$. Then

$$\mu_g(A) = \mu(f_g(A)) = \mu(A + g) = \mu(A).$$

So we see that $\Delta(g) = 1$ for all $g \in G$. Consequently, the group G is unimodular by definition. □

2.3 Discrete Subgroups

In Remark 1.7.2, we saw that a subgroup in a Euclidean space is a lattice if and only if it is discrete. It turns out that this notion is also important if we want to define lattices in locally compact groups. So in this section, we will introduce this notion. Throughout this section, let G be a topological group.

Definition 2.3.1. A subset A of G is called *discrete* if for all $a \in A$ there exists some open set B in G such that $a \in B$ and $A \cap B = \{a\}$.

We provide some useful results on discrete subsets in G.

Proposition 2.3.2. Let A be a subset in G.

i.) The subset A is discrete if and only if the subspace topology of A is discrete.

ii.) If A is discrete, then so is any subset $B \subseteq A$.

iii.) If A is discrete and compact, then A is a finite set.

Proof. To show Statement (i.), let A be a discrete subset of G. Then for all $a \in A$ there exists some open set B in G such that $a \in B$ and $A \cap B = \{a\}$. By the subspace topology, this means that all singletons are open in A. Since any subset of A is an arbitrary union of singletons, any subset of A is open. It follows that the subspace topology of A is discrete. Conversely, suppose that the subspace topology of A is discrete. Then for any $a \in A$ the singleton $\{a\}$ is open. By the subspace topology, this means that there exists some open subset $B \subseteq G$ such that $A \cap B = \{a\}$. In other words, the subset A is discrete.

To show Statement (ii.), take any subset B in A. Then for any $b \in B$ one has $b \in A$. Since A is discrete, there exists some open set C in G such that $b \in C$ and $A \cap C = \{b\}$. Then also $B \cap C = \{b\}$, since $B \subseteq A$. Hence, the subset B is discrete by definition.

To show Statement (iii.), let A be a discrete and compact subset of G. By Statement (i.), it follows that the subspace topology on A is discrete. As a result of this, all singletons in A are open. Moreover, the singletons form an open cover of A. By compactness of A, this open cover has a finite subcover. Thus, the subset A can be covered by a finite number of singletons. It follows that A must be a finite set. □

The following result is Proposition 3.1.17 of [ADGB22].

Proposition 2.3.3. If G is Hausdorff and H is a discrete subgroup in G, then H is closed in G.

2.4 Definition of Lattices

In this section, we will define lattices in locally compact groups. This section is based on Chapter I in [Rag72]. However, the definition of lattices is used in many other literature, in particular, when one looks into the theory of Lie groups. For example, see Chapter 4 in [Mor15]. Throughout this section, let G be a locally compact group and H a closed subgroup of G.

Consider the set of left cosets G/H. In Section 2.2, we have seen that we can endow the set G/H with the quotient topology. Furthermore, the group G acts on G/H by $(g, h+H) \mapsto (g+h)+H$. So whenever we write $g + A$ for any $g \in G$ and $A \subseteq G/H$, we use this group action.

Definition 2.4.1. Let μ be a Borel measure on $\mathcal{B}(G/H)$. Then μ is called *G-invariant* if $\mu(A) = \mu(g + A)$ for all $g \in G$ and $A \in \mathcal{B}(G/H)$.

Let Δ_G denote the modular map of G, and Δ_H the modular map of H that we have seen in Definition 2.2.8.

Proposition 2.4.2. There exists a G-invariant Borel measure on $\mathcal{B}(G/H)$ if and only if $\Delta_G(h) = \Delta_H(h)$ for all $h \in H$. Moreover, if such a Borel measure exists, it is unique up to scalar multiple.

These results can be found on pages 18 and 19 in [Rag72]. The subgroup H is assumed to be closed. By Proposition 2.3.3, we know that any discrete subgroup of G is closed. Hence, from now on, we can assume H to be discrete.

Corollary 2.4.3. Let H be a discrete subgroup of G. Then there exists a G-invariant Borel measure on $\mathcal{B}(G/H)$ if and only if $\Delta_G(h) = 1$ for all $h \in H$.

Proof. Since H is discrete it has the discrete topology (see Proposition 2.3.2 (i.)). It follows from Proposition 2.2.11 that H is unimodular. Thus, we know that $\Delta_H(h) = 1$ for all $h \in H$. Now, apply Proposition 2.4.2 to obtain the desired result. □

In Definition 1.6.2 we have seen the definition of a finite measure. Now, we have all the ingredients to define a lattice in a locally compact group.

Definition 2.4.4. A subset Γ of G is called a *lattice* if it is a discrete subgroup and there exists a G-invariant finite Borel measure on $\mathcal{B}(G/\Gamma)$.

Proposition 2.4.5. If G contains a lattice, then it is unimodular.

This result is stated by Remark 1.9 on page 21 in [Rag72], and depends on the classification of the subgroups of the multiplicative group $\mathbb{R}_{>0}$.

It is hard to see that Definition 2.4.4 generalizes Definition 1.7.1. Besides this problem, the next step is to generalize the notions of a fundamental region (Definition 1.7.4) and the covolume (Definition 1.7.5) of a lattice. If G contains a lattice, we know that it is unimodular, and we speak about Haar measures, rather than left or right Haar measures. The unique Haar measure on a locally compact group can be used to define the covolume. It remains to attach a fundamental region to a lattice. The natural generalization of Definition 1.7.4 is given as follows.

Definition 2.4.6. Let Γ be a lattice in locally compact group G. A *fundamental region* of the lattice Γ is a Borel measurable set $\Lambda \subseteq G$ such that $G = \bigsqcup_{\gamma \in \Gamma} (\Lambda + \gamma)$.

In the classical setting, we have constructed an explicit fundamental region for a lattice (see (12)). Therefore, the existence of a fundamental region is guaranteed. However, to show existence in this setting, one must assume that the locally compact group is second-countable. Because locally compact groups that are second-countable will be used throughout this thesis, we will study them in the next section. Once we assume that these groups are abelian, it becomes easier to see why Definition 2.4.4 generalizes Definition 1.7.1. We will study this at the end of this chapter.

2.5 L-groups

In this section, we investigate a smaller class of locally compact groups. We study some properties and the behavior of lattices in these groups. We can fully extend the notion of a fundamental region and the covolume of a lattice in these groups.

To avoid lengthy terminology, we propose the following definition.

Definition 2.5.1. A group G is called a *L-group* if it is a locally compact group that is second-countable.

We define these types of groups, as they have the required conditions to build up the rest of the theory for lattices. This is also the reason why we call them L-groups. Namely, the 'L' refers to lattices. In the rest of this thesis, we will mostly be using L-groups. However, whenever it is possible, we will try to prove results as general as possible.

Before we dive into lattices in L-groups, we provide some useful results on these groups. By Remark 2.2.5, any L-group G induces a measure space $(G, \mathcal{B}(G), \mu_G)$, where μ_G is a left Haar measure on $\mathcal{B}(G)$.

Proposition 2.5.2. Let $(G, \mathcal{B}(G), \mu_G)$ be a measure space induced by an L-group G, where μ_G is a left Haar measure on $\mathcal{B}(G)$. Then $(G, \mathcal{B}(G), \mu_G)$ is a σ-finite measure space.

Proof. By Definition 1.6.3, it is enough to show that the left Haar measure on $\mathcal{B}(G)$ is σ-finite. Proposition 7.1.6 in [Coh13] tells us that any locally compact Hausdorff space that is second-countable is a countable union of compact sets. In particular, this is true for an L-group. Hence, there exists compact subset $C_i \subseteq G$ for all $i \in \mathbb{Z}_{>0}$ such that $G = \bigcup_{i \geq 1} C_i$. By Proposition 1.6.7, we have $C_i \in \mathcal{B}(G)$ for all $i \in \mathbb{Z}_{>0}$. Since μ_G is a left Haar measure, so in particular a regular Borel measure, we have $\mu_G(C_i) < \infty$ for all $i \in \mathbb{Z}_{>0}$. It follows from Definition 1.6.2 that the left Haar measure μ_G is σ-finite. □

In Definition 1.6.19, we have seen the product measure space. For the construction, we needed σ-finite measure spaces. Hence, the proposition allows us to investigate the product measure space of the measure spaces induced by some abelian L-groups.

Proposition 2.5.3. Let G_i be an abelian L-group for $i = 1, 2$. Furthermore, let $(G_i, \mathcal{B}(G_i), \mu_i)$ be the measure space induced by G_i, where μ_i is a Haar measure on $\mathcal{B}(G_i)$. Then $G_1 \times G_2$ is an abelian L-group. Furthermore, the Borel σ-algebra on the topological group $G_1 \times G_2$ equals the product σ-algebra on G_1 and G_2. In other words, one has $\mathcal{B}(G_1 \times G_2) = \mathcal{B}(G_1) \otimes \mathcal{B}(G_2)$. Moreover, the product measure $\mu_1 \otimes \mu_2$ is a Haar measure on $\mathcal{B}(G_1 \times G_2)$.

Proof. We endow $G_1 \times G_2$ with the product topology. In that way, we turn it into a topological group (see [Sin19, Section 12.4]). Abelianness, locally compactness (see [Sin19, Theorem 5.4.6]), Hausdorffness (see [Sin19, Theorem 4.4.4]), and second-countability (see [Sin19, Theorem 7.1.7]) are preserved under finite products of groups. Therefore, the group $G_1 \times G_2$ is an abelian L-group as well.

Since G_1 and G_2 are locally compact groups that have a countable base with respect to their respective typologies, Proposition 7.6.2 in [Coh13] tells us that $\mathcal{B}(G_1 \times G_2) = \mathcal{B}(G_1) \otimes \mathcal{B}(G_2)$. Moreover, it tells us that $\mu_1 \otimes \mu_2$ is a regular Borel measure on $\mathcal{B}(G_1 \times G_2)$.

It remains to show that $\mu_1 \otimes \mu_2$ is a Haar measure on $\mathcal{B}(G_1 \times G_2)$. Take any $(g_1, g_2) \in G_1 \times G_2$ and any $A \in \mathcal{B}(G_1 \times G_2)$. Using the construction of Equation (10), for any $g \in G_1$ one has

$$\begin{aligned}
((g_1, g_2) + A)_g &= \{h \in G_2 : (g, h) \in (g_1, g_2) + A\} \\
&= \{h \in G_2 : (g - g_1, h - g_2) \in A\} \\
&= g_2 + \{h \in G_2 : (g - g_1, h) \in A\} \\
&= g_2 + A_{(g - g_1)}.
\end{aligned}$$

Now, using Equation (11), we have

$$\begin{aligned}(\mu_1 \otimes \mu_2)((g_1, g_2) + A) &= \int_{G_1} \mu_2 \left(((g_1, g_2) + A)_g\right) \mu_1(dg) \\ &= \int_{G_1} \mu_2 \left(g_2 + A_{(g-g_1)}\right) \mu_1(dg) \\ &= \int_{G_1} \mu_2 \left(A_{(g-g_1)}\right) \mu_1(dg),\end{aligned}$$

where in the last step we used that μ_2 is a Haar measure. Next, let $f\colon G_1 \to \overline{\mathbb{R}}$ be the function given by $g \mapsto \mu_2(A_g)$. In Proposition 1.6.17, we saw that this is $\mathcal{B}(G_1)$-measurable. Furthermore, let $k\colon G_1 \to G_1$ be the map given by $g \mapsto g - g_1$. By Corollary 2.1.3, the map k is $(\mathcal{B}(G_1), \mathcal{B}(G_1))$-measurable. Moreover, we can write

$$\int_{G_1} \mu_2 \left(A_{(g-g_1)}\right) \mu_1(dg) = \int_{G_1} f(k(g))\mu_1(dg).$$

Now, applying Theorem 1.6.15 we get

$$\int_{G_1} f(k(g))\mu_1(dg) = \int_{G_1} f(g)(k * \mu_1)(dg).$$

Now, for any $B \in \mathcal{B}(G_1)$, we have

$$k * \mu_1(B) = \mu_1(k^{-1}(B)) = \mu_1(B + g_1) = \mu_1(B),$$

where in the last step we used that μ_1 is a Haar measure. Hence, we have $k * \mu_1 = \mu_1$. Therefore

$$\int_{G_1} f(g)(k * \mu_1)(dg) = \int_{G_1} f(g)\mu_1(dg) = \int_{G_1} \mu_2(A_g)\mu_1(dg) = (\mu_1 \otimes \mu_2)(A).$$

Combining all equalities, we obtain that

$$(\mu_1 \otimes \mu_2)((g_1, g_2) + A) = (\mu_1 \otimes \mu_2)(A).$$

This shows that $\mu_1 \otimes \mu_2$ is a Haar measure on $\mathcal{B}(G_1 \times G_1)$. □

Now that we have studied L-groups a little bit, we can go back to lattices. Since L-groups are locally compact groups, we can use Definition 2.4.4. In Definition 2.4.6, we have seen the definition of a fundamental region of a lattice. In an L-group we can prove its existence.

Proposition 2.5.4. Let Γ be a lattice in an L-group G. Then there exists a fundamental region for Γ. Moreover, it has non-zero measure with respect to any Haar measure on $\mathcal{B}(G)$.

Proof. Consider the canonical map $\phi\colon G \to G/\Gamma$. Since Γ is a subgroup, it contains the unit element 0 of G. As Γ is discrete, there exists some open subset $A \subseteq G$ such that $\Gamma \cap A = \{0\}$. Then by Proposition 2.1.5, there exists an open neighborhood B of 0 such that $B = -B$ and $B + B \subseteq A$. Hence, we know that

$$\Gamma \cap (B + B) \subseteq \Gamma \cap A = \{0\}.$$

Now, consider the left cosets $g + B$ for any $g \in G$. We claim that ϕ is injective on any such left coset. Therefore, take any $b, b' \in B$ such that $\phi(g + b) = \phi(g + b')$. This means that there exist $\gamma, \gamma' \in \Gamma$ such that $g + b + \gamma = g + b' + \gamma'$. This implies that $b' - b = \gamma' - \gamma$. We have $b' - b \in B - B = B + B$. On the other hand, since Γ is a subgroup, we have $\gamma' - \gamma \in \Gamma$. So $b' - b \in (B + B) \cap \Gamma \subseteq \{0\}$. We may conclude that $b = b'$. This shows that ϕ is injective on the left coset $g + B$ for all $g \in G$.

By Corollary 2.1.4, we know that $g + B$ is open for any $g \in G$. Therefore, the set $\{g + B\}_{g \in G}$ is an open cover for G. Since G is second-countable there exists a countable subcovering (see [Sin19, Theorem 7.2.6]),

which we denote by $\{A_i\}_{i\geq 1}$. Any Haar measure on $\mathcal{B}(G)$ is a non-zero measure, and so the group G has non-zero measure. Therefore, without loss of generality, we can assume that A_1 has non-zero measure. We know that ϕ is injective on any A_i. Set $B_1 := A_1$, and define

$$B_i := A_i \backslash \left(A_i \cap \phi^{-1}(\phi(A_1 \cup \ldots \cup A_{i-1}))\right),$$

for $i \in \mathbb{Z}_{\geq 2}$. Then $B_i \subseteq A_i$ for all $i \in \mathbb{Z}_{>0}$. Hence, the map ϕ is also injective on any B_i. We have

$$\phi(B_i) = \phi(A_i) \backslash \left(\phi(A_i) \cap \phi(A_1 \cup \ldots \cup A_{i-1})\right),$$

where we used that $\phi(\phi^{-1}(A)) = A$ for any $A \subseteq G/\Gamma$, as ϕ is surjective. We can see from the construction of $\phi(B_i)$ that $\phi(B_i) \cap \phi(B_j) = \emptyset$ for all $i, j \in \mathbb{Z}_{>0}$. Hence, the map ϕ is also injective on the set $\Lambda := \bigcup_{i\geq 1} B_i$. We have $\Lambda \subseteq \bigcup_{i\geq 1} A_i$, and therefore

$$\phi(\Lambda) \subseteq \phi\left(\bigcup_{i\geq 1} A_i\right).$$

We will also show the other inclusion. So take any $a \in \bigcup_{i\geq 1} A_i$. Then $a \in A_i$ for some $i \in \mathbb{Z}_{>0}$. If $a \in B_i$, then $\phi(a) \in \phi(\Lambda)$. If $a \notin B_i$, then by construction of B_i, we have $a \in A_i \cap \phi^{-1}(\phi(A_1 \cup \ldots \cup A_{i-1}))$. Thus, we know $a \in \phi^{-1}(\phi(A_1 \cup \ldots \cup A_{i-1}))$, and so $\phi(a) \in \phi(A_1 \cup \ldots \cup A_{i-1})$. Consequently, there exists a minimal integer $1 \leq j \leq i-1$ such that $\phi(a) \in \phi(A_j)$. Then

$$\phi(a) \in \phi(A_j) \backslash \left(\phi(A_j) \cap \phi(A_1 \cup \ldots \cup A_{j-1}))\right) = \phi(B_j).$$

Therefore, we know that $\phi(a) \in \phi(\Lambda)$. So in all cases, we have $\phi(a) \in \phi(\Lambda)$. We obtain that

$$\phi(\Lambda) \supseteq \phi\left(\bigcup_{i\geq 1} A_i\right).$$

Since $\{A_i\}_{i\geq 1}$ is an open covering of G, we conclude that

$$\phi(\Lambda) = \phi\left(\bigcup_{i\geq 1} A_i\right) = \phi(G).$$

As a result of this, the map ϕ is surjective and injective if it is restricted to Λ. Therefore, the subset Λ of G satisfies $G = \bigsqcup_{\gamma\in\Gamma}(\Lambda + \gamma)$.

All the sets A_i are open. This means that for any $i \in \mathbb{Z}_{>0}$, the union $A := A_1 \cup \ldots \cup A_{i-1}$ is open. Then

$$\phi^{-1}(\phi(A)) = A + \Gamma = \bigcup_{\gamma\in\Gamma}(A + \gamma).$$

By Corollary 2.1.4, the sets $\gamma + A$ are open for all $\gamma \in \Gamma$. It follows that $\phi^{-1}(\phi(A))$ is open since it is the union of open sets. Then $A_i \cap \phi^{-1}(\phi(A))$ is open, and so it is Borel measurable. Then also $(A_i \cap \phi^{-1}(\phi(A)))^c$ is Borel measurable. Since A_i is Borel measurable, we get that

$$B_i = A_i \cap (A_i \cap \phi^{-1}(\phi(A)))^c$$

is Borel measurable. Then Λ is Borel measurable since it is the union of Borel measurable sets. Therefore, we conclude that Λ is a fundamental region of Γ as defined in Definition 2.4.6.

We saw that the Borel measurable set Λ contains the set $A_1 = B_1$ with non-zero measure with respect to any Haar measure. Hence, by Proposition 1.6.4, the measure of Λ must be non-zero with respect to any Haar measure on $\mathcal{B}(G)$. □

In principle, the proof of Proposition 2.5.4 gives a way to construct a fundamental region. Moreover, the proof does not use that there exists a G-invariant finite Borel measure on $\mathcal{B}(G/\Gamma)$. This means that the proposition would hold for any discrete subgroup rather than a lattice. However, this condition is used in the following result.

Proposition 2.5.5. Let Γ be a lattice in an L-group G and Λ a fundamental region of Γ. Then Λ has finite measure with respect to any Haar measure on $\mathcal{B}(G)$.

Proof. Let μ_G be any Haar measure on $\mathcal{B}(G)$ and $\phi\colon G \to G/\Gamma$ the canonical map. Since Γ is a lattice, there exists a G-invariant finite Borel measure χ on $\mathcal{B}(G/H)$. For any $A \in \mathcal{B}(G/\Gamma)$ set $\mu(A) := \mu_G(\Lambda \cap \phi^{-1}(A))$. We claim that μ is also a G-invariant Borel measure on $\mathcal{B}(G/\Gamma)$. If so, by Proposition 2.4.2 there exists some $\lambda \in \mathbb{R}_{>0}$ such that $\mu = \lambda\chi$. Since χ is a finite measure, we would get that $\mu(G/H) = \lambda\chi(G/\Gamma) < \infty$. So $\mu(G/H) = \mu_G(\Lambda \cap \phi^{-1}(G/\Gamma)) = \mu_G(\Lambda \cap G) = \mu_G(\Lambda)$ has finite measure.

So we must show the claim. Firstly, we will show that μ is a Borel measure on $\mathcal{B}(G/\Gamma)$. We have $\mu(\emptyset) = \mu_G(\emptyset) = 0$, using that μ_G is a measure. Using that μ_G is countable additive we can prove that μ is countable additive. Namely, let $A_i \in \mathcal{B}(G/\Gamma)$ be pairwise disjoint sets for all $i \in \mathbb{Z}_{\geq 0}$, then

$$\begin{aligned}
\mu\left(\bigsqcup_{i\geq 1} A_i\right) &= \mu_G\left(\Lambda \cap \phi^{-1}\left(\bigsqcup_{i\geq 1} A_i\right)\right) \\
&= \mu_G\left(\bigsqcup_{i\geq 1} (\Lambda \cap \phi^{-1}(A_i)),\right) \\
&= \sum_{i\geq 1} \mu_G(\Lambda \cap \phi^{-1}(A_i)) \\
&= \sum_{i\geq 1} \mu(A_i).
\end{aligned}$$

Hence, we get that μ is a Borel measure on $\mathcal{B}(G/\Gamma)$. Let us show that it is also G-invariant. Take any $g \in G$ and $A \in \mathcal{B}(G/\Gamma)$, then

$$\mu(g + A) = \mu_G(\Lambda \cap \phi^{-1}(g + A)) = \mu_G\left(\Lambda \cap (g + \phi^{-1}(A))\right) = \mu_G\left(((-g) + \Lambda) \cap \phi^{-1}(A)\right),$$

where in the last step we used that μ_G is a Haar measure. Specifically, we used that μ_G is translation invariant. Now, since Λ is a fundamental region of Γ, we have

$$\begin{aligned}
\mu_G\left(((-g) + \Lambda) \cap \phi^{-1}(A)\right) &= \mu_G\left(G \cap ((-g) + \Lambda) \cap \phi^{-1}(A)\right) \\
&= \mu_G\left(\left(\bigsqcup_{\gamma\in\Gamma} (\Lambda + \gamma)\right) \cap ((-g) + \Lambda) \cap \phi^{-1}(A)\right) \\
&= \mu_G\left(\bigsqcup_{\gamma\in\Gamma} \left((\Lambda + \gamma) \cap ((-g) + \Lambda) \cap \phi^{-1}(A)\right)\right) \\
&= \sum_{\gamma\in\Gamma} \mu_G\left((\Lambda + \gamma) \cap ((-g) + \Lambda) \cap \phi^{-1}(A)\right),
\end{aligned}$$

where we used that μ_G is countable additive. Now, set $\Lambda' := (-g) + \Lambda$. Then Λ' is also a fundamental region of Γ. Since Γ is a subgroup, we also have $G = \bigsqcup_{\gamma\in\Gamma}(\Lambda' - \gamma)$. Furthermore, since $\gamma \in \Gamma$, we have $\phi^{-1}(A) - \gamma = \phi^{-1}(A)$.

So using that μ_G is translation invariant, we get that

$$\begin{aligned}\sum_{\gamma\in\Gamma}\mu_G\left((\Lambda+\gamma)\cap((-g)+\Lambda)\cap\phi^{-1}(A)\right) &= \sum_{\gamma\in\Gamma}\mu_G\left(\Lambda\cap(\Lambda'-\gamma)\cap(\phi^{-1}(A)-\gamma)\right)\\ &= \mu_G\left(\Lambda\cap\left(\bigsqcup_{\gamma\in\Gamma}(\Lambda'-\gamma)\right)\cap\phi^{-1}(A)\right)\\ &= \mu_G(\Lambda\cap G\cap\phi^{-1}(A))\\ &= \mu_G(\Lambda\cap\phi^{-1}(A))\\ &= \mu(A).\end{aligned}$$

Combining all the results, we obtain that $\mu(g+A)=\mu(A)$. Consequently, the measure μ is G-invariant. □

Combining Proposition 2.5.4 and 2.5.5 we know that any fundamental region of a lattice has non-zero and finite measure. However, there can exist more than one fundamental region. We have the following result.

Proposition 2.5.6. Let Γ be a lattice in an L-group G. Then all fundamental regions of Γ have the same measure with respect to any Haar measure on $\mathcal{B}(G)$.

Proof. Let Λ,Λ' be two fundamental regions of Γ and μ_G a Haar measure on $\mathcal{B}(G)$. Then

$$\begin{aligned}\mu_G(\Lambda) &= \mu_G(\Lambda\cap G)\\ &= \mu_G\left(\Lambda\cap\bigsqcup_{\gamma\in\Gamma}(\Lambda'+\gamma)\right) &(15)\\ &= \mu_G\left(\bigsqcup_{\gamma\in\Gamma}(\Lambda\cap(\Lambda'+\gamma))\right)\\ &= \sum_{\gamma\in\Gamma}\mu_G\left(\Lambda\cap(\Lambda'+\gamma)\right) &(16)\\ &= \sum_{\gamma\in\Gamma}\mu_G\left((\Lambda-\gamma)\cap\Lambda'\right) &(17)\\ &= \mu_G\left(\bigsqcup_{\gamma\in\Gamma}(\Lambda'\cap(\Lambda-\gamma))\right) &(18)\\ &= \mu_G\left(\Lambda'\cap\bigsqcup_{\gamma\in\Gamma}(\Lambda+\gamma)\right) &(19)\\ &= \mu_G\left(\Lambda'\cap G\right) &(20)\\ &= \mu_G\left(\Lambda'\right),\end{aligned}$$

where in Equation (15) and (20) we used that Λ,Λ' are fundamental regions, in Equation (16) and (18) the fact that μ_G is countable additive, in Equation (17) that μ_G is a Haar measure, and in Equation (19) that Γ is closed under inverses. □

Definition 2.5.7. Let Γ be a lattice in an L-group G and Λ a fundamental region of Γ. Moreover, let μ_G be any Haar measure on $\mathcal{B}(G)$. The *covolume* of Γ is defined by $\mathrm{covol}(\Gamma):=\mu_G(\Lambda)$.

By Proposition 2.5.6, the covolume is well-defined and does not depend on the choice of fundamental region. However, the covolume depends on the normalization of the Haar measure μ_G. In contrast, ratios of covolumes are independent of the normalization.

Proposition 2.5.8. Let $\Gamma' \subseteq \Gamma$ be lattices in an L-group G. Then $[\Gamma\colon \Gamma'] := \#\Gamma/\Gamma' < \infty$ and

$$\operatorname{covol}(\Gamma') = [\Gamma\colon \Gamma']\operatorname{covol}(\Gamma).$$

Proof. Consider the set of left cosets Γ/Γ' and the canonical map $\phi : \Gamma \to \Gamma/\Gamma'$. We endow Γ/Γ' with the quotient topology. Now, take any subset $A \subseteq \Gamma/\Gamma'$. Then $\phi^{-1}(A) \subseteq \Gamma$ is open, since Γ has the discrete topology (see Proposition 2.3.2 (i.)). The quotient topology implies that A is open in Γ/Γ'. Since we took A arbitrarily, this shows that all subsets of Γ/Γ' are open. Hence, the group Γ/Γ' has the discrete topology and is therefore a discrete subset of G/Γ' (see Proposition 2.3.2 (i.)). Moreover, we that Γ/Γ' a subgroup of G/Γ', since Γ is a subgroup of G. By Proposition 2.3.3, we know that the discrete subgroup Γ' is closed in the locally compact group G. By Proposition 2.2.2, it follows that G/Γ' is a Hausdorff space. By Proposition 2.3.3, we see that Γ/Γ' must be closed in G/Γ'. We know, since Γ' is a lattice, that G/Γ' is compact with respect to the quotient topology. Closed subsets in compact spaces are compact itself (see [Sin19, Theorem 5.1.7]). Therefore, we have shown that Γ/Γ' is compact and discrete. It follows from Proposition 2.3.2 (iii.) that Γ/Γ' must be a finite set.

Let Λ be a fundamental domain of Γ. Set A to be a set of representatives of the left cosets in Γ/Γ'. By the previous result we have that A is a finite set and equals $[\Gamma\colon \Gamma']$. We know $A \subseteq \Gamma$, and since Λ is a fundamental region of Γ, it follows that the sets $\Lambda + a$ are pairwise disjoint for all $a \in A$. So consider the disjoint union $\Lambda' := \bigsqcup_{a\in A}(\Lambda + a)$. Now, consider the map $f\colon G \to G$ defined by $g \mapsto g - a$ for any $a \in A$. By Corollary 2.1.4, the set $f^{-1}(\Lambda) = a + \Lambda$ is Borel measurable, since Λ is. Hence, the set Λ' is Borel measurable since it is the union of Borel measurable sets. Furthermore, the sets $\Lambda' + \gamma$ for $\gamma \in \Gamma'$ are pairwise disjoint. Otherwise, the sets $\Lambda + \gamma$ for $\gamma \in \Gamma$ would not be pairwise disjoint, contradicting the fact that Λ is a fundamental region of Γ. Moreover, we have

$$\bigsqcup_{\gamma\in\Gamma'}(\Lambda' + \gamma) = \bigsqcup_{\gamma\in\Gamma'}\left(\left(\bigsqcup_{a\in A}(\Lambda + a)\right) + \gamma\right) = \bigsqcup_{\gamma\in\Gamma}(\Lambda + \gamma) = G,$$

using that A is a set of representatives of the left cosets in Γ/Γ', and that Λ is a fundamental region of Γ. It follows from Definition 2.4.6 that Λ' is a fundamental region of Γ'. Now, let μ_G be any Haar measure on $\mathcal{B}(G)$. Since μ_G is countable additive, we get

$$\operatorname{covol}(\Gamma') = \mu_G(\Lambda') = \mu_G\left(\bigsqcup_{a\in A}(\Lambda + a)\right) = \sum_{a\in A}\mu_G(\Lambda + a) = \sum_{a\in A}\mu_G(\Lambda) = \#A \cdot \operatorname{covol}(\Gamma) = [\Gamma\colon \Gamma']\operatorname{covol}(\Gamma),$$

where we used that μ_G is a Haar measure. □

2.6 Co-compact Subgroups

In Proposition 1.7.3, we saw that a lattice in a Euclidean space is complete if and only if the quotient space is compact. If we assume that an L-group is abelian, any lattice satisfies this characterization as well. Therefore, we will start by defining a general notion for this property.

Throughout this section, let G be a topological group.

Definition 2.6.1. A subgroup H in G is called *co-compact* if the set of left cosets G/H is compact with respect to the quotient topology.

We provide some useful results on co-compact subgroups in G.

Proposition 2.6.2. Let H be a subgroup in G. If H is co-compact in G, then so is any subgroup $H' \supseteq H$.

Proof. Take any normal subgroup H' such that $H \subseteq H'$. Consider the map $f\colon G/H \to G/H'$ defined by $g + H \mapsto g + H'$. Since $H \subseteq H'$, this map is well-defined and surjective. Take any open set A in G/H'. The quotient topology implies that the set $\{g \in G : g + H' \in A\}$ is open in G. Now, the pre-image of A under f is given by

$$f^{-1}(A) = \{g + H : g + H' \in A\} \subseteq G/H.$$

With respect to the quotient topology, this is open since $\{g \in G : g + H' \in A\}$ is open in G. This shows that f is continuous. Since f is continuous and G/H is compact, then also the image of f is compact (see [Sin19, Theorem 5.1.11]). Since f is surjective, this means that G/H' is compact. Hence, the subgroup H' is co-compact. □

Proposition 2.6.3. Let G_1, G_2 be topological groups and $f\colon G_1 \to G_2$ a homeomorphism of topological groups and a group homomorphism. If $H \subseteq G$ is co-compact, then $f(H)$ is co-compact.

Proof. Since H is co-compact, it is a subgroup of G_1. Since f is a group homomorphism, the set $f(H)$ is a subgroup of G_2. It remains to show that $G_2/f(H)$ is compact with respect to the quotient topology. Therefore, consider the map $k\colon G_1/H \to G_2/f(H)$ defined by $g + H \mapsto f(g) + f(H)$. Since f is a group homomorphism, the map k is well-defined. Furthermore, the map k is surjective since f is. Now, consider an open subset $A \subseteq G_2/f(H)$. The quotient topology implies that the set $B := \{g \in G_2 : g + f(H) \in A\}$ is open in G_2. Since f is a homeomorphism, it is continuous. Therefore, the set $f^{-1}(B)$ is open in G_1. This set is given by

$$f^{-1}(B) = \{g \in G_1 : f(g) \in B\} = \{g \in G_1 : f(g) + f(H) \in A\}.$$

Now, the pre-image of A under k is given by

$$k^{-1}(A) = \{g + H : k(g + H) \in A\} = \{g + H : f(g) + f(H) \in A\}.$$

With respect to the quotient topology, this is open since $\{g \in G_1 : f(g) + f(H) \in A\}$ is open in G. This shows that k is continuous. Since k is continuous and G_1/H is compact, then also the image of k is compact (see [Sin19, Theorem 5.1.11]). Since k is surjective, this means that $G_2/f(H)$ is compact. We conclude that $f(H)$ is co-compact. □

We will use these results later in this thesis. However, for now, we give an equivalent characterization of lattices in an abelian L-group.

Theorem 2.6.4. Let G be an abelian L-group. A subset Γ in G is a lattice if and only if Γ is a discrete and co-compact subgroup of G.

Proof. Suppose that Γ is a discrete and co-compact subgroup of G. Then Γ is a lattice if there exists a G-invariant finite Borel measure on $\mathcal{B}(G/H)$. We assumed G to be abelian. Hence, by Proposition 2.2.11, we know that G is unimodular, i.e. $\Delta_G(g) = 1$ for all $g \in G$. Then by Corollary 2.4.3, there exists a G-invariant Borel measure μ on $\mathcal{B}(G/\Gamma)$. It remains to show that $\mu(G/\Gamma) < \infty$. By Proposition 2.3.3, we know that Γ is closed in G. Since G is abelian, we know that Γ is a normal subgroup. It follows from Proposition 2.2.2 that G/Γ is a locally compact group. Therefore, there exists a unique, up to scalar multiple, Haar measure χ on $\mathcal{B}(G/\Gamma)$ (see Theorem 2.2.4). Since χ is a Haar measure, it is also G-invariant as defined in Definition 2.4.1. Thus, by Proposition 2.4.2, there exists a $\lambda \in \mathbb{R}_{>0}$ such that $\mu = \lambda\chi$. Since χ is a regular Borel measure on $\mathcal{B}(G/\Gamma)$, it is finite on compact sets. The subgroup Γ is co-compact, and thus is G/Γ compact. It implies that $\chi(G/\Gamma) < \infty$. We get that $\mu(G/\Gamma) = \lambda\chi(G/\Gamma) < \infty$.

Conversely, let Γ be a lattice in G. Then by Definition 2.4.4, it is a discrete subgroup and there exists a G-invariant finite Borel measure μ on $\mathcal{B}(G/\Gamma)$. In particular, the measure μ is finite on any compact set in G/Γ. For the same reason as above, we know that G/Γ is a locally compact group. Moreover, the group G is second-countable, since it is an L-group. These conditions imply that μ is a regular Borel measure (see [Coh13, Proposition 7.2.3]). Together with the fact that μ is G-invariant and finite, we know that μ is a finite Haar measure on $\mathcal{B}(G/\Gamma)$. Proposition 9.3.3 in [Coh13] tells us that G/Γ is compact since μ is finite. Consequently, the subset Γ is co-compact. □

Remark 2.6.5. Due to this result, we see that the notion of lattices in an abelian L-group is a generalization of complete lattices in a Euclidean space. Therefore, we can reason that Definition 2.4.4 generalizes complete lattices. This means that we have found a reasonable theory of lattices in locally compact groups that extends the classical theory of lattices in Euclidean spaces. In the rest of this thesis, we will only consider abelian L-groups. So we are safe to define a lattice in such a group to be a discrete and co-compact subgroup. ⧫

3 Rings of S-Integers

In this chapter, we will study the rings of S-integers of a number field. In Chapter 6, we will see that this generalizes fake real quadratic orders. Section 3.1 and 3.2 are known to the literature. However, in the literature, either the proofs of these results are skipped or it cannot be found in one place. Therefore, we include this in the thesis. The proofs within these sections are self-written. Furthermore, we derive some new results for the rings of S-integers. This includes an analogue of Minkowski's Convex Body Theorem (see Theorem 1.7.8) and an extension of Theorem 1.8.6. We will study this in the last two sections of this chapter. Throughout this chapter, let K be a number field.

3.1 Structure

From now on, unless stated otherwise, we assume S to be a finite subset of $\mathfrak{P}_K^0$. Moreover, whenever we write $\mathfrak{p} \notin S$, we mean $\mathfrak{p} \in \mathfrak{P}_K^0 \backslash S$. Consider the subset of K given by

$$\mathcal{O}_{K,S} := \{x \in K : |x|_\mathfrak{p} \leq 1 \text{ for all } \mathfrak{p} \notin S\}.$$

Recall that for any $x \in K$, the $\mathfrak{p}$-adic valuation and $\mathfrak{p}$-adic absolute value are related by $|x|_\mathfrak{p} = N_{\mathcal{O}_K}(\mathfrak{p})^{-\operatorname{ord}_\mathfrak{p}(x)}$. Therefore, saying that $|x|_\mathfrak{p} \leq 1$ is equivalent to saying $\operatorname{ord}_\mathfrak{p}(x) \geq 0$. Therefore, we also have

$$\mathcal{O}_{K,S} = \{x \in K : \operatorname{ord}_\mathfrak{p}(x) \geq 0 \text{ for all } \mathfrak{p} \notin S\}. \tag{21}$$

By properties of the $\mathfrak{p}$-adic absolute value, the set $\mathcal{O}_{K,S}$ is a subring of K.

Definition 3.1.1. The ring $\mathcal{O}_{K,S}$ is called the *ring of S-integers* of K.

This notation is different from the notation of the valuation ring $\mathcal{O}_{K,\mathfrak{p}}$ we have seen in (9). Actually, one has to consider $S = \mathfrak{P}_K^0 \backslash \{\mathfrak{p}\}$ to receive $\mathcal{O}_{K,\mathfrak{p}}$. But since we only allow S to be a finite set, there should be no confusion.

Proposition 3.1.2. If $S = \emptyset$, then $\mathcal{O}_{K,S} = \mathcal{O}_K$. Furthermore, if $S \subseteq S'$ are finite sets of $\mathfrak{P}_K^0$, then $\mathcal{O}_{K,S} \subseteq \mathcal{O}_{K,S'}$.

Proof. These two facts are consequences of the definition. □

Lemma 3.1.3. One has $\mathfrak{p}^m \mathcal{O}_{K,S} = \mathcal{O}_{K,S}$ for all $\mathfrak{p} \in S$ and non-zero $m \in \mathbb{Z}$.

Proof. Throughout this proof, take $\mathfrak{p} \in S$ arbitrarily. Suppose that $m \in \mathbb{Z}_{>0}$. Then it suffices to prove it for $m = 1$. The general case follows by applying it inductively. We know that $\mathcal{O}_K \subseteq \mathcal{O}_{K,S}$ by Proposition 3.1.2. Thus, we see that $\mathfrak{p}\mathcal{O}_{K,S} \subseteq \mathcal{O}_{K,S}$. For the converse, take any $x \in \mathcal{O}_{K,S}$. Since the class group Cl_K is finite, there exists some $k \in \mathbb{Z}_{>0}$ such that $\mathfrak{p}^k$ is principal. Let ε be a choice of generator of $\mathfrak{p}^k$. Then $\varepsilon^{-1}\mathcal{O}_K = \mathfrak{p}^{-k}$. This means that $\operatorname{ord}_\mathfrak{q}(\varepsilon^{-1}) = 0$ for all non-zero prime ideals $\mathfrak{q} \neq \mathfrak{p}$, and $\operatorname{ord}_\mathfrak{p}(\varepsilon^{-1}) = -k$. Since $\mathfrak{p} \in S$, we have that $\varepsilon^{-1} \in \mathcal{O}_{K,S}$. Consequently, we get that $\varepsilon^{-1}x \in \mathcal{O}_{K,S}$. Then $x = \varepsilon(\varepsilon^{-1}x) \in \mathfrak{p}\mathcal{O}_{K,S}$. Consequently, we have $\mathcal{O}_{K,S} \subseteq \mathfrak{p}\mathcal{O}_{K,S}$. Inclusion from both sides gives us the desired result.

So we have $\mathfrak{p}^m \mathcal{O}_{K,S} = \mathcal{O}_{K,S}$ for all $m \in \mathbb{Z}_{>0}$. So we have $\mathcal{O}_{K,S} = \mathfrak{p}^{-m}\mathcal{O}_{K,S}$. We see that the case in which m is negative follows directly. □

There are several alternatives to view the rings of S-integers. We will treat two of them.

Proposition 3.1.4. For $a \in \mathcal{O}_K \backslash \{0\}$, one has $\mathcal{O}_{K,S} = \mathcal{O}_K\left[a^{-1}\right]$ if and only if the finite places $\mathfrak{p}$ for which $\left|a^{-1}\right|_\mathfrak{p} > 1$ are exactly equal to S. Equivalently, the prime ideals in the unique factorization of $a\mathcal{O}_K$ are exactly the prime ideals from S.

For the proof, we refer to the proof of Lemma 1.1 in [Con24b]. Such a can always be found. Namely, since the class number h_k is finite, we have that $\mathfrak{p}^{h_k}$ is principal for all $\mathfrak{p} \in S$. Also, the product of these principal ideals is principal. Therefore,

$$\left(\prod_{\mathfrak{p}\in S} \mathfrak{p}\right)^{h_K} = a\mathcal{O}_K$$

for some $a \in \mathcal{O}_K$. We have that $\mathfrak{p}|a\mathcal{O}_K$ if and only if $\mathfrak{p} \in S$. It follows by the lemma that $\mathcal{O}_{K,S} = \mathcal{O}_K\left[a^{-1}\right]$. An alternative way of defining S-integers, is to view them as a ring of fractions of $\mathcal{O}_K$.

Proposition 3.1.5. Let $\mathcal{P} := \mathcal{O}_K \setminus \bigcup_{\mathfrak{p}\notin S} \mathfrak{p}$. Then $\mathcal{P}$ is a multiplicatively closed set. Furthermore, the ring of fractions of $\mathcal{O}_K$ with respect to $\mathcal{P}$ equals $\mathcal{O}_{K,S}$.

Proof. In this proof, we will repeatedly use Definition 1.1.7 and Proposition 1.1.8. Firstly, the set $\mathcal{P}$ is multiplicatively closed if $1 \in \mathcal{P}$ and $x, y \in \mathcal{P}$ imply that $xy \in \mathcal{P}$. If $1 \in \bigcup_{\mathfrak{p}\notin S} \mathfrak{p}$, then there exists some $\mathfrak{p} \notin S$ such that $1 \in \mathfrak{p}$. This contradicts the fact that $\mathfrak{p}$ is a prime ideal, and so $1 \in \mathcal{P}$. Now, take $x, y \in \mathcal{P}$. Suppose that $xy \in \bigcup_{\mathfrak{p}\notin S} \mathfrak{p}$, then there exists some $\mathfrak{p} \notin S$ such that $xy \in \mathfrak{p}$. Using that $\mathfrak{p}$ is a prime ideal we have $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. Hence, at least one of x, y is contained in $\bigcup_{\mathfrak{p}\notin S} \mathfrak{p}$. This contradicts the fact that $x, y \in \mathcal{P}$. Thus, we must have $xy \notin \bigcup_{\mathfrak{p}\notin S} \mathfrak{p}$, which implies that $xy \in \mathcal{P}$.

Next, we have to show that $\mathcal{O}_K\mathcal{P}^{-1} = \mathcal{O}_{K,S}$. We have

$$\mathcal{O}_K\mathcal{P}^{-1} = \left\{\frac{a}{x} : a \in \mathcal{O}_K, x \in \mathcal{P}\right\}.$$

So take any $\frac{a}{x} \in \mathcal{O}_K\mathcal{P}^{-1}$. Then $x \notin \bigcup_{\mathfrak{p}\notin S} \mathfrak{p}$, and so $x \notin \mathfrak{p}$ for all $\mathfrak{p} \notin S$. Since $x \in \mathcal{O}_K$, this implies that $\mathrm{ord}_{\mathfrak{p}}(x) = 0$ for all $\mathfrak{p} \notin S$. As $a \in \mathcal{O}_K$, we have that $\mathrm{ord}_{\mathfrak{p}}(a) \geq 0$ for all $\mathfrak{p} \in \mathfrak{P}_K^0$. Hence, for any $\mathfrak{p} \notin S$, we have

$$\mathrm{ord}_{\mathfrak{p}}\left(\frac{a}{x}\right) = \mathrm{ord}_{\mathfrak{p}}(a) - \mathrm{ord}_{\mathfrak{p}}(x) = \mathrm{ord}_{\mathfrak{p}}(a) \geq 0.$$

By construction (21) one has $\frac{a}{x} \in \mathcal{O}_{K,S}$. Conversely, take $x \in \mathcal{O}_{K,S}$. Then $\mathrm{ord}_{\mathfrak{p}}(x) \geq 0$ for all $\mathfrak{p} \notin S$. If there exists some $y \in \mathcal{P}$ such that $xy \in \mathcal{O}_K$, then there exists some $a \in \mathcal{O}_K$ such that $xy = a$. This would imply that $x = \frac{a}{y} \in \mathcal{O}_K\mathcal{P}^{-1}$. It follows from inclusion on both sides that $\mathcal{O}_K\mathcal{P}^{-1} = \mathcal{O}_{K,S}$. Such $y \in \mathcal{P}$ can always be constructed. Let $S' \subseteq S$ contain exactly the prime ideals $\mathfrak{p} \in S$ such that $\mathrm{ord}_{\mathfrak{p}}(x) < 0$. Since Cl_K is a finite group, there exists some $k_{\mathfrak{p}} \in \mathbb{Z}_{>0}$ such that $\mathfrak{p}^{k_{\mathfrak{p}}}$ is principal for all $\mathfrak{p} \in S'$. Denote a choice of generator by $\varepsilon_{\mathfrak{p}}$. Then, we can find an $m_{\mathfrak{p}} \in \mathbb{Z}_{>0}$ such that $\mathrm{ord}_{\mathfrak{p}}(\varepsilon_{\mathfrak{p}}^{m_{\mathfrak{p}}} x) \geq 0$. We just need to take $m_{\mathfrak{p}}$ sufficiently large. Then for $y = \prod_{\mathfrak{p}\in S'} \varepsilon_{\mathfrak{p}}^{m_{\mathfrak{p}}}$ one has $\mathrm{ord}_{\mathfrak{p}}(xy) \geq 0$ for all $\mathfrak{p} \in \mathfrak{P}_K^0$. We get that $xy \in \mathcal{O}_K$. It remains to show that $y \in \mathcal{P}$. We know that $y \in \mathcal{O}_K$ since it is a product of integral ideals of $\mathcal{O}_K$. Suppose $y \in \bigcup_{\mathfrak{p}\notin S} \mathfrak{p}$, then $y \in \mathfrak{p}$ for some $\mathfrak{p} \notin S$. This means that $\mathfrak{p}|y\mathcal{O}_K = \prod_{\mathfrak{q}\in S'} \mathfrak{q}^{k_{\mathfrak{q}} m_{\mathfrak{q}}}$. This contradicts the unique factorization of fractional ideals in $\mathcal{O}_K$. We conclude that $y \in \mathcal{P}$. □

Corollary 3.1.6. The ring of S-integer $\mathcal{O}_{K,S}$ of K is a Dedekind domain

Proof. We know that $\mathcal{O}_K$ is a Dedekind domain. This property is preserved under any ring of fractions (see [Neu99, Proposition 11.4, Chapter I]). It follows from Proposition 3.1.5 that $\mathcal{O}_{K,S}$ is a Dedekind domain. □

This Corollary allows us to apply the theory from Section 1.1 to $\mathcal{O}_{K,S}$. We will study this a little bit more precisely in the next section.

3.2 Fractional Ideals and Class Group

We know that $\mathcal{O}_{K,S}$ is a Dedekind domain. Let $\mathrm{Id}_{K,S} := \mathrm{Id}_{\mathcal{O}_{K,S}}$ denote the abelian group formed by the fractional ideals of $\mathcal{O}_{K,S}$. Furthermore, we denote its subgroup of principal fractional ideals by $\mathrm{P}_{K,S}$. The class group of $\mathcal{O}_{K,S}$ (see Definition 1.1.3) is denoted by $\mathrm{Cl}_{K,S}$. The order of the class group is denoted by the $h_{K,S} \in \mathbb{Z}_{>0} \cup \{\infty\}$. We will see at the end of this section that this order is finite.

In Section 1.1, we saw that any fractional ideal of $\mathcal{O}_{K,S}$ can be uniquely written as a finite product of non-zero prime ideals of $\mathcal{O}_{K,S}$. Let us study the prime ideals of $\mathcal{O}_{K,S}$.

Proposition 3.2.1. The prime ideals of $\mathcal{O}_{K,S}$ are in bijection with the prime ideals of $\mathcal{O}_K$ not contained in S. This map is given by

$$\mathfrak{p} \mapsto \mathfrak{p}\mathcal{O}_{K,S}, \qquad \mathfrak{P} \mapsto \mathfrak{P} \cap \mathcal{O}_K, \tag{22}$$

for prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ and prime ideal $\mathfrak{P} \subseteq \mathcal{O}_{K,S}$. The set of prime ideals of $\mathcal{O}_{K,S}$ is denoted by $\mathrm{Spec}(\mathcal{O}_{K,S})$.

Proof. In Proposition 3.1.5, we have seen that $\mathcal{O}_{K,S} = \mathcal{O}_K\mathcal{P}^{-1}$ for $\mathcal{P} = \mathcal{O}_K \setminus \bigcup_{\mathfrak{p}\notin S} \mathfrak{p}$. Then Proposition 11.1 in [Neu99] tells us that the prime ideals of $\mathcal{O}_{K,S}$ are in bijection with the prime ideals of $\mathcal{O}_K$ contained in $\mathcal{O}_K \setminus \mathcal{P} = \bigcup_{\mathfrak{p}\notin S} \mathfrak{p}$. Moreover, the proposition gives us the corresponding maps (22). So it remains to show that $\mathfrak{p} \subseteq \bigcup_{\mathfrak{p}\notin S} \mathfrak{p}$ if and only if $\mathfrak{p} \notin S$. Any $\mathfrak{p} \notin S$ is contained in $\bigcup_{\mathfrak{p}\notin S} \mathfrak{p}$.

For the converse, we use that Corollary 2.4 in [RV70] states that $\mathcal{O}_K$ is compactly packed. This property states that for any set $A \subseteq \mathfrak{P}_K^0$ and integral ideal $I \subseteq \mathcal{O}_K$ such that $I \subseteq \bigcup_{\mathfrak{p}\in A} \mathfrak{p}$ implies that $I \subseteq \mathfrak{p}$ for some $\mathfrak{p} \in A$. So suppose that $\mathfrak{q} \subseteq \bigcup_{\mathfrak{p}\notin S} \mathfrak{p}$, for any $\mathfrak{q} \in S$. Then by compactly compactness of $\mathcal{O}_K$, we have that $\mathfrak{q} \subseteq \mathfrak{p}$ for some $\mathfrak{p} \notin S$. Hence, $\mathfrak{p}|\mathfrak{q}$, which contradicts the fact that $\mathfrak{q}$ is a prime ideal and every integral ideal has a unique factorization of non-zero prime ideals. Consequently, the converse is also true. □

From this proposition, we see that $\mathrm{Spec}(\mathcal{O}_{K,S}) = \{\mathfrak{p}\mathcal{O}_{K,S} : \mathfrak{p} \notin S\} \cup \{(0)\}$. Hence, any $I \in \mathrm{Id}_{K,S}$ can be written as

$$I = \prod_{\mathfrak{p}\notin S} (\mathfrak{p}\mathcal{O}_{K,S})^{n_\mathfrak{p}},$$

for some $n_\mathfrak{p} \in \mathbb{Z}$ for all $\mathfrak{p} \notin S$. Moreover, we get the group homomorphism $\mathrm{ord}_{\mathfrak{p}\mathcal{O}_{K,S}} \colon \mathrm{Id}_{K,S} \to \mathbb{Z}$ for any $\mathfrak{p} \in S$, that we have seen in Remark 1.1.5. If $S = \emptyset$, we transferred this map to a valuation of K (see Example 1.4.5). We can do this here as well. For any $x \in K^*$, we set $\mathrm{ord}_{\mathfrak{p}\mathcal{O}_{K,S}}(x) := \mathrm{ord}_{\mathfrak{p}\mathcal{O}_{K,S}}(x\mathcal{O}_{K,S})$. By convention, we set $\mathrm{ord}_{\mathfrak{p}\mathcal{O}_{K,S}}(0) = \infty$. One can show by verification of Definition 1.4.1, that this is a discrete valuation of K. Next, we can show that the discrete valuations $\mathrm{ord}_\mathfrak{p}$ and $\mathrm{ord}_{\mathfrak{p}\mathcal{O}_{K,S}}$ are equal for any $\mathfrak{p} \notin S$.

Proposition 3.2.2. Let $x \in K^*$, then

$$x\mathcal{O}_{K,S} = \prod_{\mathfrak{p}\notin S} (\mathfrak{p}\mathcal{O}_{K,S})^{\mathrm{ord}_\mathfrak{p}(x)}.$$

Consequently, one has $\mathrm{ord}_{\mathfrak{p}\mathcal{O}_{K,S}}(x) = \mathrm{ord}_\mathfrak{p}(x)$ for all $\mathfrak{p} \notin S$.

Proof. We have $x\mathcal{O}_K = \prod_{\mathfrak{p}\in\mathfrak{P}_K^0} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(x)}$, for any $x \in K^*$. So

$$x\mathcal{O}_{K,S} = (x\mathcal{O}_K)\mathcal{O}_{K,S} = \left(\prod_{\mathfrak{p}\in\mathfrak{P}_K^0} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(x)}\right)\mathcal{O}_{K,S} = \left(\prod_{\mathfrak{p}\notin S} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(x)}\right)\prod_{\mathfrak{p}\in S} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(x)}\mathcal{O}_{K,S},$$

where we used the fact that $\mathcal{O}_K\mathcal{O}_{K,S} = \mathcal{O}_{K,S}$. Using Lemma 3.1.3, we have that $\prod_{\mathfrak{p}\in S} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(x)}\mathcal{O}_{K,S} = \mathcal{O}_{K,S}$. Then

$$x\mathcal{O}_{K,S} = \left(\prod_{\mathfrak{p}\notin S} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(x)}\right)\prod_{\mathfrak{p}\in S} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(x)}\mathcal{O}_{K,S} = \left(\prod_{\mathfrak{p}\notin S} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(x)}\right)\mathcal{O}_{K,S} = \prod_{\mathfrak{p}\notin S} (\mathfrak{p}\mathcal{O}_{K,S})^{\mathrm{ord}_\mathfrak{p}(x)}.$$

Therefore, we have $\mathrm{ord}_{\mathfrak{p}\mathcal{O}_{K,S}}(x) = \mathrm{ord}_{\mathfrak{p}\mathcal{O}_{K,S}}(x\mathcal{O}_{K,S}) = \mathrm{ord}_\mathfrak{p}(x)$ for all $\mathfrak{p} \notin S$. □

Recall Definition 1.1.6 for the definition of coprime fractional ideals. We know that the fractional ideals of $\mathcal{O}_K$ (resp. $\mathcal{O}_{K,S}$) have a unique factorization of non-zero prime ideals of $\mathcal{O}_K$ (resp. $\mathcal{O}_{K,S}$). Therefore, by the bijection given in Proposition 3.2.1, we have that the fractional ideals of $\mathcal{O}_{K,S}$ are in bijection with the

fractional ideals of $\mathcal{O}_K$ that are coprime to S. Let $\mathrm{Id}_K^{\mathrm{co}}$ denote the fractional ideals of $\mathcal{O}_K$ that are coprime to S. Then this bijection is given by

$$\iota : \mathrm{Id}_{K,S} \to \mathrm{Id}_K^{\mathrm{co}}, \qquad \prod_{\mathfrak{p}\notin S} (\mathfrak{p}\mathcal{O}_{K,S})^{n_\mathfrak{p}} \mapsto \prod_{\mathfrak{p}\notin S} \mathfrak{p}^{n_\mathfrak{p}}. \tag{23}$$

Let $\langle S\rangle$ (resp. $\langle [S]\rangle$) denote the subgroup of Id_K (resp. Cl_K) generated by the prime ideals in S.

Proposition 3.2.3. There exist group isomorphisms $\mathrm{Id}_{K,S} \cong \mathrm{Id}_K/\langle S\rangle$ and $\mathrm{Cl}_{K,S} \cong \mathrm{Cl}_K/\langle [S]\rangle$.

Proof. Consider the map $\varphi : \mathrm{Id}_K \to \mathrm{Id}_{K,S}$ defined by $I \mapsto I\mathcal{O}_{K,S}$. Note that the image of φ is in $\mathrm{Id}_{K,S}$. Namely, if $I \in \mathrm{Id}_K$ has some $\mathfrak{p} \in S$ in its factorization, then it is canceled by multiplication with $\mathcal{O}_{K,S}$ (see Lemma 3.1.3). As a result of this, the fractional ideal $I\mathcal{O}_{K,S}$ is precisely given by a product of prime ideals of $\mathcal{O}_{K,S}$. It follows that $I\mathcal{O}_{K,S} \in \mathrm{Id}_{K,S}$. Since we have that the fractional ideals of $\mathcal{O}_{K,S}$ are in bijection with the fractional ideals of $\mathcal{O}_K$ that are coprime to S, the map φ defines a surjective group homomorphism. Moreover, we have $I \in \ker(\varphi)$ if and only if $n_\mathfrak{p} = 0$ for all $\mathfrak{p} \notin S$. Equivalently, we know $I \in \ker(\varphi)$ if and only if $I \in \langle S\rangle$. It follows that φ induces a group isomorphism $\mathrm{Id}_{K,S} \cong \mathrm{Id}_K/\langle S\rangle$.

Consider the map $\psi : \mathrm{Cl}_K \to \mathrm{Cl}_{K,S}$ defined by $[I] \mapsto [I\mathcal{O}_{K,S}]$. Notice that for any $x \in K^*$, we have $(x\mathcal{O}_K)\mathcal{O}_{K,S} = x\mathcal{O}_{K,S}$. Thus, the map ψ is a well-defined group homomorphism. Since φ is surjective, so is ψ. If $[I] \in \ker(\psi)$ then $[I\mathcal{O}_{K,S}] = [\mathcal{O}_{K,S}]$. Then there exists some $x \in K^*$ such that $I\mathcal{O}_{K,S} = x\mathcal{O}_{K,S}$. Then for any $\mathfrak{p} \notin S$

$$\mathrm{ord}_\mathfrak{p}(I) = \mathrm{ord}_{\mathfrak{p}\mathcal{O}_{K,S}}(I\mathcal{O}_{K,S}) = \mathrm{ord}_{\mathfrak{p}\mathcal{O}_{K,S}}(x\mathcal{O}_{K,S}) = \mathrm{ord}_{\mathfrak{p}\mathcal{O}_{K,S}}(x) = \mathrm{ord}_\mathfrak{p}(x),$$

where we used Proposition 3.2.2. We see that $I = xJ$, with $J \in \langle S\rangle$. It follows that

$$[I] = [xJ] = [J] \in \langle [S]\rangle.$$

Conversely, for any $[I] \in \langle [S]\rangle$, we have $\psi([I]) = [I\mathcal{O}_{K,S}] = [\mathcal{O}_{K,S}]$, using Lemma 3.1.3, and so $[I] \in \ker(\psi)$. This shows that $\ker(\psi) = \langle [S]\rangle$. Consequently, the group homomorphism ψ induces a group isomorphism $\mathrm{Cl}_{K,S} \cong \mathrm{Cl}_K/\langle [S]\rangle$. □

The following convention is used throughout this thesis.

Definition 3.2.4. Let $I \in \mathrm{Id}_{K,S}$. We denote the fractional ideal $\iota(I)$ of $\mathcal{O}_K$ by I_S. Equivalently, let C be the equivalence class in $\mathrm{Id}_K/\langle S\rangle$ that corresponds to I under the isomorphism from Proposition 3.2.3. Then the fractional ideal I_S is the unique representative of C that is coprime to S.

One has $I = I_S\mathcal{O}_{K,S}$ for any $I \in \mathrm{Id}_{K,S}$.

Lemma 3.2.5. Let $I \in \mathrm{Id}_{K,S}$ and $x \in I$. Then $x \in I_S$ if and only if $|x|_\mathfrak{p} \leq 1$ for all $\mathfrak{p} \in S$.

Proof. In this proof, we will repeatedly use Definition 1.1.7 and Proposition 1.1.8. Suppose that $x \in I_S$. Then $I_S | x\mathcal{O}_K$, and so $\mathrm{ord}_\mathfrak{p}(I_S) \leq \mathrm{ord}_\mathfrak{p}(x)$ for all $\mathfrak{p} \in \mathfrak{P}_K^0$. Since I_S is coprime to S, we have $\mathrm{ord}_\mathfrak{p}(I_S) = 0$ for all $\mathfrak{p} \in S$. Hence, we see that $\mathrm{ord}_\mathfrak{p}(x) \geq 0$ for all $\mathfrak{p} \in S$. Or equivalently, we have $|x|_\mathfrak{p} \leq 1$ for all $\mathfrak{p} \in S$.

Conversely, suppose that $|x|_\mathfrak{p} \leq 1$ for all $\mathfrak{p} \in S$. Since $x \in I$ we have $x\mathcal{O}_{K,S} \subseteq I$, and so $I | x\mathcal{O}_{K,S}$. This means that $\mathrm{ord}_{\mathfrak{p}\mathcal{O}_{K,S}}(I) \leq \mathrm{ord}_{\mathfrak{p}\mathcal{O}_{K,S}}(x)$ for all $\mathfrak{p} \notin S$. By the definition of I_S, we have $\mathrm{ord}_{\mathfrak{p}\mathcal{O}_{K,S}}(I) = \mathrm{ord}_\mathfrak{p}(I_S)$ for all $\mathfrak{p} \notin S$, and $\mathrm{ord}_\mathfrak{p}(I_S) = 0$ for all $\mathfrak{p} \in S$. In Proposition 3.2.2, we have seen that $\mathrm{ord}_{\mathfrak{p}\mathcal{O}_{K,S}}(x) = \mathrm{ord}_\mathfrak{p}(x)$ for all $\mathfrak{p} \notin S$. Since $|x|_\mathfrak{p} \leq 1$, we have $\mathrm{ord}_\mathfrak{p}(x) \geq 0$ for all $\mathfrak{p} \in S$. Thus, we have $\mathrm{ord}_\mathfrak{p}(I_S) \leq \mathrm{ord}_\mathfrak{p}(x)$ for all $\mathfrak{p} \in \mathfrak{P}_K^0$. Thus, we get that $I_S | x\mathcal{O}_K$, and so $x\mathcal{O}_K \subseteq I_S$. Since $1 \in \mathcal{O}_K$, we get $x \in I_S$. □

In Definition 1.1.11, we have seen the construction of the norm for any fractional ideal of $\mathcal{O}_{K,S}$. It induced a group homomorphism $N_{\mathcal{O}_{K,S}} \colon \mathrm{Id}_{K,S} \to \mathbb{Q}^*$. The norm of a fractional ideal I of $\mathcal{O}_{K,S}$ can be related to the norm of the fractional ideal I_S of $\mathcal{O}_K$.

Proposition 3.2.6. Let $\mathfrak{p} \notin S$, then $N_{\mathcal{O}_K}(\mathfrak{p}) = N_{\mathcal{O}_{K,S}}(\mathfrak{p}\mathcal{O}_{K,S})$. Moreover, the equality $N_{\mathcal{O}_{K,S}}(I) = N_{\mathcal{O}_K}(I_S)$ holds for any $I \in \mathrm{Id}_{K,S}$.

Proof. Throughout this proof, take $\mathfrak{p} \notin S$ arbitrarily. Consider the ring homomorphism $f\colon \mathcal{O}_K \to \mathcal{O}_{K,S}/\mathfrak{p}\mathcal{O}_{K,S}$ given by $a \mapsto [a]$ (where [.] denotes the equivalence classes in the quotient ring). Now, for any $y \in \mathcal{O}_K \setminus \bigcup_{\mathfrak{p} \notin S} \mathfrak{p}$ we have the equality $\mathcal{O}_K = \mathfrak{p} + y\mathcal{O}_K$. This can be seen as follows. We know that $\mathfrak{p} + y\mathcal{O}_K$ is an integral ideal containing $\mathfrak{p}$. In a Dedekind domain, all prime ideals are maximal (see Proposition 1.1.4). Therefore, we either have $\mathfrak{p} = \mathfrak{p} + y\mathcal{O}_K$ or $\mathcal{O}_K = \mathfrak{p} + y\mathcal{O}_K$. The former is impossible as it would imply that $y \in \mathfrak{p} \subseteq \bigcup_{\mathfrak{p} \notin S} \mathfrak{p}$. This contradicts the choice of y.

Take any $x \in \mathcal{O}_{K,S}$. It follows from Proposition 3.1.5 that there exist some $a \in \mathcal{O}_K$ and $y \in \mathcal{P} = \mathcal{O}_K \setminus \bigcup_{\mathfrak{p} \notin S} \mathfrak{p}$ such that $x = \frac{a}{y}$. Since $y \in \mathcal{P}$, we know, by the above reasoning, that $\mathcal{O}_K = \mathfrak{p} + y\mathcal{O}_K$. Then there exist some $b \in \mathcal{O}_K$ and $c \in \mathfrak{p}$ such that $a = c + yb$, and so $x = \frac{a}{y} = \frac{c}{y} + b$. Since $c \in \mathfrak{p}$ and $\frac{1}{y} \in \mathcal{O}_{K,S}$, we have $\frac{c}{y} \in \mathfrak{p}\mathcal{O}_{K,S}$. It follows that $[b] = [x]$. So there exists some $b \in \mathcal{O}_K$ such that $f(b) = [b] = [x]$. It allows us to conclude that f is surjective.

We claim that $\ker(f) = \mathfrak{p}$. Take any $a \in \mathfrak{p}$, then $a \in \mathfrak{p}\mathcal{O}_{K,S}$. Equivalently, we have $f(a) = [a] = [0]$, so $\mathfrak{p} \subseteq \ker(f)$. For the converse, take any $a \in \ker(f)$. This means that $[a] = f(a) = [0]$, and so $a \in \mathfrak{p}\mathcal{O}_{K,S}$. Therefore, we know that $a \in \mathcal{O}_K \cap \mathfrak{p}\mathcal{O}_{K,S} = \mathfrak{p}$, where the last equality follows from the bijection given in Proposition 3.2.1. It follows that $\ker(f) \subseteq \mathfrak{p}$. Thus, we showed the claim. Therefore, the ring homomorphism f induces a ring isomorphism $\mathcal{O}_K/\mathfrak{p} \cong \mathcal{O}_{K,S}/\mathfrak{p}\mathcal{O}_{K,S}$. We conclude that both rings have the same order. By Definition 1.1.9, we deduce that $N_{\mathcal{O}_K}(\mathfrak{p}) = N_{\mathcal{O}_{K,S}}(\mathfrak{p}\mathcal{O}_{K,S})$.

Take any $I \in \mathrm{Id}_{K,S}$ written as $\prod_{\mathfrak{p} \notin S}(\mathfrak{p}\mathcal{O}_{K,S})^{n_\mathfrak{p}}$ for some $n_\mathfrak{p} \in \mathbb{Z}$ for all $\mathfrak{p} \notin S$. Then by definition, we have the fractional ideal $I_S = \prod_{\mathfrak{p} \notin S} \mathfrak{p}^{n_\mathfrak{p}}$. In Proposition 1.1.10 (i.), we have seen that $N_{\mathcal{O}_K}$ and $N_{\mathcal{O}_{K,S}}$ are group homomorphisms. Then

$$N_{\mathcal{O}_{K,S}}\left(\prod_{\mathfrak{p} \notin S}(\mathfrak{p}\mathcal{O}_{K,S})^{n_\mathfrak{p}}\right) = \prod_{\mathfrak{p} \notin S} N_{\mathcal{O}_{K,S}}(\mathfrak{p}\mathcal{O}_{K,S})^{n_\mathfrak{p}} = \prod_{\mathfrak{p} \notin S} N_{\mathcal{O}_K}(\mathfrak{p})^{n_\mathfrak{p}} = N_{\mathcal{O}_K}\left(\prod_{\mathfrak{p} \notin S} \mathfrak{p}^{n_\mathfrak{p}}\right),$$

where we used the result obtained earlier in this proof. Consequently, we get that $N_{\mathcal{O}_{K,S}}(I) = N_{\mathcal{O}_K}(I_S)$. □

The units of ring $\mathcal{O}_{K,S}$ is denoted by $\mathcal{O}_{K,S}^*$. An element $x \in \mathcal{O}_{K,S}$ is a unit if and only if $x^{-1} \in \mathcal{O}_{K,S}$. Hence, we have that $|x|_\mathfrak{p} \leq 1$ and $|x^{-1}|_\mathfrak{p} \leq 1$ for all $\mathfrak{p} \notin S$. Therefore

$$\mathcal{O}_{K,S}^* = \{x \in K : |x|_\mathfrak{p} = 1 \text{ for all } \mathfrak{p} \notin S\},$$

or equivalently

$$\mathcal{O}_{K,S}^* = \{x \in K : \mathrm{ord}_\mathfrak{p}(x) = 0 \text{ for all } \mathfrak{p} \notin S\}. \tag{24}$$

We can obtain the following results.

Proposition 3.2.7. There exists an exact sequence

$$0 \to \mathcal{O}_K^* \to \mathcal{O}_{K,S}^* \to \bigoplus_{\mathfrak{p} \in S} \mathbb{Z} \to \mathrm{Cl}_K \to \mathrm{Cl}_{K,S} \to 0.$$

Consequently, there exists an isomorphism $\mathcal{O}_{K,S}^* \cong \mu_K \times \mathbb{Z}^{\#S + r_1 + r_2 - 1}$, and the order $h_{K,S}$ of the class group is finite.

These results are given in [Neu99, Section 11, Chapter I].

3.3 S-Minkowski Space

The next step is to see if it is possible to generalize Theorem 1.8.6. In other words, we aim to view non-zero fractional ideals of $\mathcal{O}_{K,S}$ as lattices in a certain topological space. In this section, we will construct this space. Moreover, we study some properties of this space. Among other things, this includes the analogue of the Heine-Borel Theorem and Minkowski's Convex Body Theorem (see Theorem 1.7.8).

3.3.1 Components: Completions of Number Fields

The space we want to construct is a product of completions of our number field K. Therefore, we first investigate these completions a little bit. This is not new and can be found in the literature. However, the proofs of the results are self-written.

Throughout this thesis, for a metric space (M, d), let $B^d(u, \varepsilon) := \{v \in M : d(u, v) < \varepsilon\}$ denote the open ball of radius $\varepsilon \in \mathbb{R}_{>0}$ with center u in M. Furthermore, let $B^d[u, \varepsilon] := \{v \in M : d(u, v) \leq \varepsilon\}$ denote the closed ball of radius $\varepsilon \in \mathbb{R}_{>0}$ with center u in M.

Consider the completion K_ν, for any $\nu \in \mathcal{V}_K$. We have seen its construction in Section 1.4. The absolute value $|.|_\nu$ induces a metric $d_\nu(x, y) := |x - y|_\nu$ for $x, y \in K$. We denote this metric space by (K_ν, d_ν).

Lemma 3.3.1. Let $\mathfrak{p} \in \mathfrak{P}^0_K$, $x \in K_\mathfrak{p}$, and $\varepsilon \in \mathbb{R}_{>0}$. If $y \in B^{d_\mathfrak{p}}(x, \varepsilon)$, then $B^{d_\mathfrak{p}}(x, \varepsilon) = B^{d_\mathfrak{p}}(y, \varepsilon)$. Similarly, if $y \in B^{d_\mathfrak{p}}[x, \varepsilon]$, then $B^{d_\mathfrak{p}}[x, \varepsilon] = B^{d_\mathfrak{p}}_\varepsilon[y, \varepsilon]$.

Proof. Suppose that $y \in B^{d_\mathfrak{p}}(x, \varepsilon)$, and take any $z \in B^{d_\mathfrak{p}}(y, \varepsilon)$. Then both the values $|z - y|_\mathfrak{p}, |y - x|_\mathfrak{p}$ are strictly less than ε. So the strong triangle inequality implies that

$$|z - x|_\mathfrak{p} = |(z - y) + (y - x)|_\mathfrak{p} \leq \max\{|z - y|_\mathfrak{p}, |y - x|_\mathfrak{p}\} < \varepsilon.$$

This means that $z \in B^{d_\mathfrak{p}}(x, \varepsilon)$, and so we get $B^{d_\mathfrak{p}}(y, \varepsilon) \subseteq B^{d_\mathfrak{p}}(x, \varepsilon)$. The other inclusion has a similar argument. We conclude that $B^{d_\mathfrak{p}}(x, \varepsilon) = B^{d_\mathfrak{p}}(y, \varepsilon)$. In this proof, the strict inequality $<$ could easily be replaced by $\leq$. Consequently, the statement for closed balls follows as well. □

For any $\nu \in \mathcal{V}_K$, the metric space (K_ν, d_ν) induces a topological structure on K_ν. Furthermore, we know that K_ν is endowed with an abelian additive group structure since it is a field. The topology is compatible with these additive operations. Hence, for any $\nu \in \mathcal{V}_K$, the additive group K_ν is a topological group.

Proposition 3.3.2. Let $\nu \in \mathcal{V}_K$. Then K_ν is an abelian L-group.

Proof. Since K_ν is a field, the additive group structure is abelian for any $\nu \in \mathcal{V}_K$. By Theorem 1.4.8, we know that the topology on K_σ is equivalent to the Euclidean topology on $\mathbb{R}$ and $\mathbb{C}$ for any $\sigma \in \Sigma^\infty_K$. Since these are locally compact, Hausdorff, and second-countable topological spaces, so is K_σ. Hence, we see that K_σ is an abelian L-group for any $\sigma \in \Sigma^\infty_K$. Now, consider $K_\mathfrak{p}$ for any $\mathfrak{p} \in \mathfrak{P}^0_K$. This is locally compact as well. This is stated in Proposition 5.1 in Chapter II of [Neu99]. The group $K_\mathfrak{p}$ is Hausdorff since its topology is induced from a metric (see [Sut09, Proposition 11.5]). It remains to show that the topological group $K_\mathfrak{p}$ is second-countable for any $\mathfrak{p} \in \mathfrak{P}^0_K$. For the rest of the proof, consider any $\mathfrak{p} \in \mathfrak{P}^0_K$ arbitrarily. We have to find a countable collection of open subsets of $K_\mathfrak{p}$ such that any other open subset of $K_\mathfrak{p}$ is a union of a subcollection. We claim that the collection

$$\mathcal{B} := \left\{B^{d_\mathfrak{p}}(x, N_{\mathcal{O}_K}(\mathfrak{p})^k) : x \in K, k \in \mathbb{Z}\right\}$$

does the job. Let A be an open subset of $K_\mathfrak{p}$, and take any $a \in A$. Since A is open, there exists some $\varepsilon_a \in \mathbb{R}_{>0}$, depending on $a \in A$, such that $B^{d_\mathfrak{p}}(a, \varepsilon_a) \subseteq A$. Now, there exists a $k_a \in \mathbb{Z}$, depending on $a \in A$, such that $N_{\mathcal{O}_K}(\mathfrak{p})^{k_a} < \varepsilon_a$. Consequently, we get the inclusions given by $\{a\} \subseteq B^{d_\mathfrak{p}}(a, N_{\mathcal{O}_K}(\mathfrak{p})^{k_a}) \subseteq B^{d_\mathfrak{p}}(a, \varepsilon_a) \subseteq A$ for any $a \in A$. Then

$$A = \bigcup_{a \in A} \{a\} \subseteq \bigcup_{a \in A} B^{d_\mathfrak{p}}(a, N_{\mathcal{O}_K}(\mathfrak{p})^{k_a}) \subseteq \bigcup_{a \in A} B^{d_\mathfrak{p}}(a, \varepsilon_a) \subseteq A.$$

It follows that

$$A = \bigcup_{a \in A} B^{d_{\mathfrak{p}}}(a, N_{\mathcal{O}_K}(\mathfrak{p})^{k_a}).$$

Now, Theorem 4.2 of Chapter 2 in [Cas86] tells us that K is dense in $K_{\mathfrak{p}}$. Therefore, for any $a \in A$, there exists some $x_a \in K$, such that $x_a \in B^{d_{\mathfrak{p}}}(a, N_{\mathcal{O}_K}(\mathfrak{p})^{k_a})$. Note that x_a depends on k_a, and therefore depends on a. By Lemma 3.3.1, we have

$$B^{d_{\mathfrak{p}}}(a, N_{\mathcal{O}_K}(\mathfrak{p})^{k_a}) = B^{d_{\mathfrak{p}}}(x_a, N_{\mathcal{O}_K}(\mathfrak{p})^{k_a}).$$

As a result of this, we get

$$A = \bigcup_{a \in A} B^{d_{\mathfrak{p}}}(a, N_{\mathcal{O}_K}(\mathfrak{p})^{k_a}) = \bigcup_{a \in A} B^{d_{\mathfrak{p}}}(x_a, N_{\mathcal{O}_K}(\mathfrak{p})^{k_a}).$$

Note that $B^{d_{\mathfrak{p}}}(x_a, N_{\mathcal{O}_K}(\mathfrak{p})^{k_a}) \in \mathcal{B}$ for all $a \in A$. This means that A can be written as a union of a subcollection of $\mathcal{B}$. It remains to show that $\mathcal{B}$ is countable. We can write

$$\mathcal{B} = \bigcup_{x \in K} \bigcup_{k \in \mathbb{Z}} \left\{ B^{d_{\mathfrak{p}}}(x, N_{\mathcal{O}_K}(\mathfrak{p})^{k}) \right\}.$$

We see that $\mathcal{B}$ is a union of singletons over K and $\mathbb{Z}$. Number fields are countable and $\mathbb{Z}$ is countable. Thus, the collection $\mathcal{B}$ is countable. □

As stated in Remark 2.2.5, any locally compact group induces a measure space. Hence, for any $\nu \in \mathcal{V}_K$, the locally compact group K_ν induces a measure space $(K_\nu, \mathcal{B}(K_\nu), \mu_\nu)$, where μ_ν is some Haar measure on $\mathcal{B}(K_\nu)$. Notice that we can consider Haar measures rather than left or right Haar measures since the group is abelian. We can make appropriate choices for the normalization of this Haar measure. For any infinite place $\sigma \in \Sigma_K^\infty$, corresponding to a real field embedding, we know $K_\sigma \cong \mathbb{R}$ by Theorem 1.4.8. We have seen that the Lebesgue measure μ_1 is a Haar measure on $\mathcal{B}(\mathbb{R})$ (see Example 1.6.10). Therefore, we can take the Lebesgue measure as the Haar measure on $\mathcal{B}(K_\sigma)$. We denote this choice by μ_σ. For any infinite place $\sigma \in \Sigma_K^\infty$, corresponding to a complex field embedding, we know $K_\sigma \cong \mathbb{C}$ by Theorem 1.4.8. Furthermore, we have $\mathbb{C} \cong \mathbb{R}^2$, and therefore, we can take the Lebesgue measure μ_2 on $\mathcal{B}(\mathbb{R}^2)$ as the Haar measure on $\mathcal{B}(K_\sigma)$. However, we chose a different normalization. Namely, we take twice the Lebesgue measure. We denote this choice by μ_σ.

For a finite place $\mathfrak{p} \in \mathfrak{P}_K^0$, we have to reason a bit different. By Proposition 1.6.7, we know that compact subsets are Borel measurable. Moreover, we know that compact subsets have finite measure for any Haar measure. By Theorem 2.2.4, we know that Haar measures are unique up to scalar multiple. Therefore, if we chose the measure for a certain compact subset, the Haar measure is uniquely determined. Proposition 5.1 of Chapter II of [Neu99] tells us that the DVR $\mathcal{O}_{\mathfrak{p}}$ is compact for any $\mathfrak{p} \in \mathfrak{P}_K^0$. Therefore, we can make a unique choice for the measure on $\mathcal{O}_{\mathfrak{p}}$. For any $\mathfrak{p} \in \mathfrak{P}_K^0$, we choose $\mu_{\mathfrak{p}}(\mathcal{O}_{\mathfrak{p}}) := N_{\mathcal{O}_{\mathfrak{p}}}(\mathfrak{D}_{\mathcal{O}_{\mathfrak{p}}|\mathbb{Z}_p})^{-1/2}$, where $\mathfrak{D}_{\mathcal{O}_{\mathfrak{p}}|\mathbb{Z}_p}$ is the different of $\mathcal{O}_{\mathfrak{p}}|\mathbb{Z}_p$. The different of $\mathcal{O}_{\mathfrak{p}}|\mathbb{Z}_p$ was treated at the end of Section 1.4. We denote this Haar measure by $\mu_{\mathfrak{p}}$ for any $\mathfrak{p} \in \mathfrak{P}_K^0$.

Remark 3.3.3. The choices of μ_ν for any $\nu \in \mathcal{V}_K$, will be used throughout the rest of this thesis. The choice of these Haar measures is not arbitrary. They agree with the choices described in Tate's thesis. They make sure that the Haar measures are *self-dual*. Since this notion is not part of this thesis, we refer to Tate's thesis for an explanation. For example, this thesis can be found in Chapter XV of [CF67]. ♦

Since K_ν is a field for any $\nu \in \mathcal{V}_K$, we have a multiplicative operation $K_\nu \times K_\nu \to K_\nu$, which we will denote by $(x, y) \mapsto xy$.

Lemma 3.3.4. Let $\nu \in \mathcal{V}_K$ and $x \in K_\nu^*$.

i.) If $A \subseteq K_\nu$ is an open subset, then so is xA.

ii.) If $A \subseteq K_\nu$ is a Borel measurable subset, then so is xA.

Proof. To show Statement (i.), take any open subset $A \subseteq K_\nu$ and any $y \in xA$. Then there exists some $a \in A$ such that $y = xa$. Since A is open, there exists some $\varepsilon \in \mathbb{R}_{>0}$ such that $B^{d_\nu}(a, \varepsilon) \subseteq A$. Let $\lambda := |x|_\nu \varepsilon$, and take any $z \in B^{d_\nu}(y, \lambda)$. Note that

$$d_\nu(z, xa) = |z - xa|_\nu = |x|_\nu \left| \frac{z}{x} - a \right|_\nu = |x|_\nu d_\nu \left(\frac{z}{x}, a \right).$$

This means that

$$d_\nu(z, y) < \lambda \implies d_\nu(z, xa) < \lambda \implies |x|_\nu d_\nu \left(\frac{z}{x}, a \right) < \lambda \implies d_\nu \left(\frac{z}{x}, a \right) < \frac{\lambda}{|x|_\nu} = \varepsilon.$$

We get $\frac{z}{x} \in B^{d_\nu}(a, \varepsilon) \subseteq A$, and so $z \in xA$. This implies that $B^{d_\nu}(y, \lambda) \subseteq xA$, and therefore xA is open.

To show Statement (ii.), consider the map $f \colon K_\nu \to K_\nu$ given by $y \mapsto x^{-1}y$. For any open subset $A \subseteq K_\nu$, we know by Statement (i.) that $f^{-1}(A) = xA$ is open. It follows that $f^{-1}(A) \in \mathcal{B}(K_\nu)$. Since $\mathcal{B}(K_\nu)$ is generated by the open sets of K_ν, it follows from Proposition 1.6.13 that f is (K_ν, K_ν)-measurable. This means that for any $A \in \mathcal{B}(K_\nu)$ the set $f^{-1}(A) = xA$ is Borel measurable. □

Lemma 3.3.5. Let $\mathfrak{p} \in \mathfrak{P}_K^0$ and $a \in \mathcal{O}_\mathfrak{p}$. Then $N_{\mathcal{O}_\mathfrak{p}}(a\mathcal{O}_\mathfrak{p}) = N_{\mathcal{O}_K}(\mathfrak{p})^{\mathrm{ord}_\mathfrak{p}(a)}$.

Proof. Since $\mathcal{O}_\mathfrak{p}$ is a DVR, every non-zero ideal of $\mathcal{O}_\mathfrak{p}$ is a power of $\mathfrak{m}_\mathfrak{p}$ (see Remark 1.4.3). In fact, for any $a \in \mathcal{O}_\mathfrak{p}$, we have $a\mathcal{O}_\mathfrak{p} = \mathfrak{m}_\mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(a)}$ (see page 69 in [Neu99]). Therefore, using Lemma 1.4.9, we have

$$\mathcal{O}_\mathfrak{p}/a\mathcal{O}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(a)} \cong \mathcal{O}_K/\mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(a)}.$$

This means that $N_{\mathcal{O}_\mathfrak{p}}(a\mathcal{O}_\mathfrak{p}) = N_{\mathcal{O}_K}(\mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(a)}) = N_{\mathcal{O}_K}(\mathfrak{p})^{\mathrm{ord}_\mathfrak{p}(a)}$. □

Now, there is an interesting result if we compare the measure of $A \in \mathcal{B}(K_\nu)$ with xA for any $x \in K_\nu^*$ and $\nu \in \mathcal{V}_K$.

Proposition 3.3.6. Let $\nu \in \mathcal{V}_K$. For any $x \in K_\nu^*$ and $A \in \mathcal{B}(K_\nu)$ one has $\mu_\nu(xA) = \|x\|_\nu \mu_\nu(A)$.

Proof. Firstly, note that by Lemma 3.3.4 (ii.), it makes sense to take the measure of xA. Now, let ν be an infinite place $\sigma \in \Sigma_K^\infty$. If σ corresponds to a real field embedding, then μ_σ is the Lebesgue measure on $\mathcal{B}(\mathbb{R})$, and $\|.\|_\sigma$ is the absolute value of $\mathbb{R}$. If σ corresponds to a complex field embedding, then μ_σ is twice the Lebesgue measure of $\mathcal{B}(\mathbb{R}^2)$, and $\|.\|_\sigma$ is the square of the absolute value on $\mathbb{C}$. Therefore, the property follows directly from Proposition 1.6.11.

Now, let ν be a finite place $\mathfrak{p} \in \mathfrak{P}_K^0$. Consider the map $f_x \colon K_\mathfrak{p} \to K_\mathfrak{p}$ given by $y \mapsto xy$. It is not hard to verify that f_x is an automorphism of the additive group $K_\mathfrak{p}$ for all $x \in K_\mathfrak{p}^*$. For any $A \in \mathcal{B}(K_\mathfrak{p})$, we have that $f_x^{-1}(A) = x^{-1}A$. By Lemma 3.3.4 (ii.), we know that this is contained in $\mathcal{B}(K_\mathfrak{p})$. It follows that f_x is also $(B(K_\mathfrak{p}), B(K_\mathfrak{p}))$-measurable. Theorem 1.6.15 tells us that $\mu_x := \mu_\mathfrak{p} \circ f_x$ is a measure on $\mathcal{B}(K_\mathfrak{p})$. Moreover, since it is an automorphism, the conditions of Definition 1.6.8 are preserved. Thus, it is also a Borel regular measure. For $A \in \mathcal{B}(K_\mathfrak{p})$ and $y \in K_\mathfrak{p}^*$, we have

$$\mu_x(y + A) = \mu_\mathfrak{p}(f_x(y + A)) = \mu_\mathfrak{p}(xy + xA) = \mu_\mathfrak{p}(xA) = \mu_x(A),$$

using that $\mu_\mathfrak{p}$ is a Haar measure on $\mathcal{B}(K_\mathfrak{p})$. Hence, also μ_x is a Haar measure on $\mathcal{B}(K_\mathfrak{p})$. So by Theorem 2.2.4, there must exists some $\lambda_x \in \mathbb{R}$, depending on x, such that $\mu_x = \lambda_x \mu_\mathfrak{p}$. Define the function $\lambda \colon K_\mathfrak{p}^* \to \mathbb{R}$ such that $\lambda(x) = \lambda_x$. For any $A \in \mathcal{B}(K_\mathfrak{p})$, we have

$$\mu_\mathfrak{p}(xA) = \mu_\mathfrak{p}(f_x(A)) = \mu_x(A) = \lambda_x \mu_\mathfrak{p}(A) = \lambda(x)\mu_\mathfrak{p}(A).$$

Take any $x, y \in K_{\mathfrak{p}}^*$, and $A \in \mathcal{B}(K_{\mathfrak{p}})$ that has non-zero measure with respect to $\mu_{\mathfrak{p}}$. Then we have

$$\lambda(xy) = \frac{\mu_{xy}(A)}{\mu_{\mathfrak{p}}(A)} = \frac{\mu_x(yA)}{\mu_{\mathfrak{p}}(A)} = \frac{\lambda(x)\mu_{\mathfrak{p}}(yA)}{\mu_{\mathfrak{p}}(A)} = \frac{\lambda(x)\mu_y(A)}{\mu_{\mathfrak{p}}(A)} = \frac{\lambda(x)\lambda(y)\mu_{\mathfrak{p}}(A)}{\mu_{\mathfrak{p}}(A)} = \lambda(x)\lambda(y).$$

We conclude that the function λ is multiplicative. Now, consider $a \in \mathcal{O}_{\mathfrak{p}} \backslash \{0\}$, and the quotient ring $\mathcal{O}_{\mathfrak{p}}/a\mathcal{O}_{\mathfrak{p}}$. Let R denote a set of representatives of $\mathcal{O}_{\mathfrak{p}}/a\mathcal{O}_{\mathfrak{p}}$. Using that a measure is countable additive, we get

$$\mu_{\mathfrak{p}}(\mathcal{O}_{\mathfrak{p}}) = \mu_{\mathfrak{p}}\left(\bigsqcup_{r \in R}(r + a\mathcal{O}_{\mathfrak{p}})\right) = \sum_{r \in R} \mu_{\mathfrak{p}}(r + a\mathcal{O}_{\mathfrak{p}}).$$

Now, using that $\mu_{\mathfrak{p}}$ is a Haar measure, we obtain that

$$\sum_{r \in R} \mu_{\mathfrak{p}}(r + a\mathcal{O}_{\mathfrak{p}}) = \sum_{r \in R} \mu_{\mathfrak{p}}(a\mathcal{O}_{\mathfrak{p}}) = \#R \cdot \mu_{\mathfrak{p}}(a\mathcal{O}_{\mathfrak{p}}) = \#R \cdot \lambda(a)\mu_{\mathfrak{p}}(\mathcal{O}_{\mathfrak{p}}).$$

Note that we have $\#R = N_{\mathcal{O}_K}(\mathfrak{p})^{\mathrm{ord}_{\mathfrak{p}}(a)}$. Since $\mu_p r(\mathcal{O}_{\mathfrak{p}})$ is finite and non-zero, we get that $\lambda(a) = \#R^{-1}$. By Lemma 3.3.5, we have that $\#R = N_{\mathcal{O}_{\mathfrak{p}}}(a\mathcal{O}_{\mathfrak{p}}) = N_{\mathcal{O}_K}(\mathfrak{p})^{\mathrm{ord}_{\mathfrak{p}}(a)}$. We obtain that $\lambda(a) = N_{\mathcal{O}_K}(\mathfrak{p})^{-\mathrm{ord}_{\mathfrak{p}}(a)} = \|a\|_{\mathfrak{p}}$ for all $a \in \mathcal{O}_{\mathfrak{p}} \backslash \{0\}$. Now, take a uniformizer $t \in \mathfrak{m}_{\mathfrak{p}}$ (see Remark 1.4.3). Then for any $x \in K_{\mathfrak{p}}^*$, there exists a $k \in \mathbb{Z}$ and $a \in \mathcal{O}_{\mathfrak{p}}^*$ such that $x = at^k$. Since $a, t \in \mathcal{O}_{\mathfrak{p}} \backslash \{0\}$, we have $\lambda(a) = \|a\|_{\mathfrak{p}}$ and $\lambda(t) = \|t\|_{\mathfrak{p}}$. Since λ is multiplicative, it follows that

$$\mu_{\mathfrak{p}}(xA) = \mu_{\mathfrak{p}}(at^kA) = \lambda(t^ka)\mu_{\mathfrak{p}}(A) = \lambda(t)^k\lambda(a)\mu_{\mathfrak{p}}(A) = \|t\|_{\mathfrak{p}}^k\|a\|_{\mathfrak{p}}\mu_{\mathfrak{p}}(A) = \|t^ka\|_{\mathfrak{p}}\mu_{\mathfrak{p}}(A) = \|x\|_{\mathfrak{p}}\mu_{\mathfrak{p}}(A). \quad \square$$

In the next section, we are interested in the product of completions of a number field. Now, we briefly discuss what happens if we only consider the completions with respect to the infinite places of K. In Section 1.8, we constructed the space $K_{\mathbb{R}}$, and saw that $K_{\mathbb{R}} = \prod_{\sigma \in \Sigma_K^\infty} K_\sigma$. Now, by Proposition 3.3.2, we know that K_σ is an abelian L-group, for any $\sigma \in \Sigma_K^\infty$. By applying Proposition 2.5.3 recursively, we get that $K_{\mathbb{R}}$ is an abelian L-group as well. Moreover, a Haar measure on $K_{\mathbb{R}}$ is given by the product measure of the Haar measures μ_σ on $\mathcal{B}(K_\sigma)$ for $\sigma \in \Sigma_K^\infty$. Because we have unique choices for μ_σ, we get a unique Haar measure on $\mathcal{B}(K_{\mathbb{R}})$, which we denote by $\mu_{\mathbb{R}}$.

Definition 3.3.7. The measure space $(K_{\mathbb{R}}, \mathcal{B}(K_{\mathbb{R}}), \mu_{\mathbb{R}})$ is called the *Minkowski space* of K.

Remark 3.3.8. We have $\mu_{\mathbb{R}} = \bigotimes_{\sigma \in \Sigma_K^\infty} \mu_\sigma$. For any infinite place $\sigma \in \Sigma_K^\infty$, corresponding to a real field embedding, we took the Lebesgue measure on $\mathcal{B}(\mathbb{R})$. For any infinite place $\sigma \in \Sigma_K^\infty$, corresponding to a complex field embedding, we took twice the Lebesgue measure on $\mathcal{B}(\mathbb{R}^2)$. It follows that for any $A \in \mathcal{B}(K_{\mathbb{R}})$, we have

$$\mu_{\mathbb{R}}(A) = 2^{r_2}\mu_n(A),$$

using that we have r_2 complex field embeddings and μ_n is the Lebesgue measure on $\mathcal{B}(\mathbb{R}^n)$. We see that the normalization of $\mu_{\mathbb{R}}$ is the same as the volume $\mathrm{vol}_{\mathbb{R}}$ that we introduced in Remark 1.8.5. So we see that $\mathrm{vol}_{\mathbb{R}}$ equals the Haar measure $\mu_{\mathbb{R}}$. Using Theorem 1.8.6, we see that the covolume of the lattice $\Psi(\mathcal{O}_K)$ equals $\sqrt{|d_K|_\infty}$ with respect to $\mu_{\mathbb{R}}$. ♦

In the next section, we add completions with respect to finite places into the product of $K_{\mathbb{R}}$.

3.3.2 Structure

Set

$$S^\infty := S \cup \Sigma_K^\infty,$$

and consider

$$K_S := \prod_{\nu \in S^\infty} K_\nu = \prod_{\sigma \in \Sigma_K^\infty} K_\sigma \times \prod_{\mathfrak{p} \in S} K_{\mathfrak{p}}.$$

For any $u \in K_S$, there exists some $u_\nu \in K_\nu$ for all $\nu \in S^\infty$ such that $u = (u_\nu)_{\nu \in S^\infty}$. Sometimes we consider the infinite and finite places separately. In that case, we always consider the infinite places first. Moreover, we write $u = ((u_\sigma)_{\sigma \in \Sigma_K^\infty}, (u_\mathfrak{p})_{\mathfrak{p} \in S})$. We will use this convention throughout this thesis.

The set K_S attains a commutative ring structure by entry-wise addition and multiplication.

Proposition 3.3.9. The additive group K_S is an abelian L-group with respect to the product topology.

Proof. By Proposition 3.3.2, we know that K_ν is an abelian L-group for any $\nu \in \mathcal{V}_K$. By applying Proposition 2.5.3 recursively, we get that K_S is an abelian L-group as well. From its proof, we can see that the topology on K_S is induced from the product topology. □

Recall that for any $\nu \in \mathcal{V}_K$, the topology on K_ν is induced from the metric d_ν. We can take the product metric

$$d_S(u, v) := \sum_{\nu \in S^\infty} d_\nu(u_\nu, v_\nu) \tag{25}$$

with $u, v \in K_S$.

Proposition 3.3.10. The product topology on K_S is induced from the metric $d_S \colon K_S \times K_S \to \mathbb{R}$.

Proof. Proposition 10.17 [Sut09] tells us that the product topology is compatible with the product metric (25). □

So we have obtained a metric space (K_S, d_S). Let us investigate some properties of this metric space.

Let (M, d) be a metric space. At the beginning of Section 3.3.1, we defined the open and closed balls. Note that $B^d(u, \varepsilon) \subseteq B^d[u, \varepsilon]$ for any $u \in M$ and $\varepsilon \in \mathbb{R}_{>0}$. Since $B^d[u, \varepsilon]$ is closed, the closure of the open ball $B^d(u, \varepsilon)$, denoted by $\overline{B^d(u, \varepsilon)}$, is also contained in $B^d[u, \varepsilon]$. It is not always true that

$$\overline{B^d(u, \varepsilon)} = B^d[u, \varepsilon]. \tag{26}$$

Namely, let M be any set, and consider the metric

$$d(u, v) = \begin{cases} 0, & \text{if } u = v, \\ 1, & \text{otherwise,} \end{cases}$$

for $u, v \in M$. Then for any $u \in M$, we have $B^d(u, 1) = \{u\}$, $\overline{B^d(u, 1)} = \{u\}$, and $B^d[u, 1] = M$. Hence, the equality (26) is not true. However, the equality is true in a Euclidean space. It follows from Theorem 1.4.8 that it is true in the metric space (K_σ, d_σ) for any $\sigma \in \Sigma_K^\infty$. It turns out to be true in the metric space (K_S, d_S) as well.

Proposition 3.3.11. For any $u \in K_S$ and $\varepsilon \in \mathbb{R}_{>0}$ one has $\overline{B^{d_S}(u, \varepsilon)} = B^{d_S}[u, \varepsilon]$.

Proof. It remains to show that $\mathcal{B}^{d_S}[u, \varepsilon] \subseteq \overline{B^{d_S}(u, \varepsilon)}$. Take any $v \in \mathcal{B}^{d_S}[u, \varepsilon]$, and any $\lambda \in \mathbb{R}_{>0}$. Set $\alpha_\nu := d_\nu(u_\nu, v_\nu)$ for any $\nu \in S^\infty$. Then for any $\sigma \in \Sigma_K^\infty$, one has $v_\sigma \in B^{d_\sigma}[u_\sigma, \alpha_\sigma] = \overline{B^{d_\sigma}(u_\sigma, \alpha_\sigma)}$, where we used that equality (26) is true in Euclidean spaces. Equivalently, the element v_σ is a point of closure of $B^{d_\sigma}(u_\sigma, \alpha_\sigma)$. Therefore, for $s := \frac{\lambda}{\#\Sigma_K^\infty} \in \mathbb{R}_{>0}$, there exists some w_σ such that $w_\sigma \in B^{d_\sigma}(v_\sigma, s) \cap B^{d_\sigma}(u_\sigma, \alpha_\sigma)$

for all $\sigma \in \Sigma_K^\infty$. Set $w_\mathfrak{p} := v_\mathfrak{p}$ for all $\mathfrak{p} \in \mathfrak{P}_K^0$ and $w := (w_\nu)_{\nu \in S^\infty} \in K_S$. Then

$$\begin{aligned} d_S(w,v) &= \sum_{\nu \in S^\infty} d_\nu(w_\nu, v_\nu) \\ &= \sum_{\sigma \in \Sigma_K^\infty} d_\nu(w_\sigma, v_\sigma) + \sum_{\mathfrak{p} \in S} d_\nu(w_\mathfrak{p}, v_\mathfrak{p}) \\ &= \sum_{\sigma \in \Sigma_K^\infty} d_\nu(w_\sigma, v_\sigma) + \sum_{\mathfrak{p} \in S} d_\nu(v_\mathfrak{p}, v_\mathfrak{p}) \\ &= \sum_{\sigma \in \Sigma_K^\infty} d_\nu(w_\sigma, v_\sigma) \\ &< \#\Sigma_K^\infty \cdot s = \lambda, \end{aligned}$$

and

$$d_S(u,w) = \sum_{\nu \in S^\infty} d_\nu(u_\nu, w_\nu) = \sum_{\sigma \in \Sigma_K^\infty} d_\nu(u_\sigma, w_\sigma) + \sum_{\mathfrak{p} \in \mathfrak{P}_K^0} d_\mathfrak{p}(u_\mathfrak{p}, v_\mathfrak{p}) < \sum_{\nu \in S^\infty} \alpha_\nu = d_S(u,v) < \varepsilon.$$

This allows us to conclude that $w \in B^{d_S}(v,\lambda) \cap B^{d_S}(u,\varepsilon)$. Hence, since $\lambda \in \mathbb{R}_{>0}$ was taken arbitrary, it follows that v is a point of closure of $B^{d_S}(u,\varepsilon)$, i.e. $v \in \overline{B^{d_S}(u,\varepsilon)}$. We conclude that $\mathcal{B}^{d_S}[u,\varepsilon] \subseteq \overline{B^{d_S}(u,\varepsilon)}$. □

Since K_S is Hausdorff, we have that a compact subset $A \subseteq K_S$ is closed in K_S (see [Sin19, Theorem 5.1.8]). Furthermore, Proposition 13.10 in [Sut09] tells us that a compact subset $A \subseteq K_S$ is bounded. In a Euclidean space, the converse is also true, i.e. a closed and bounded subset is compact. This result is known as the Heine-Borel Theorem (see [Sut09, Theorem 13.22]). In general, the converse is not true. However, there is an analogue of the Heine-Borel Theorem for the space K_S.

Theorem 3.3.12. Let $A \subseteq K_S$. Then A is compact if and only if A is closed and bounded.

Proof. It suffices to show that a closed and bounded subset is compact since we already saw the converse. So let A be a closed and bounded subset in K_S. Since A is bounded, there exist some $u \in A$ and $\varepsilon \in \mathbb{R}_{>0}$ such that $A \subseteq B^{d_S}[u,\varepsilon]$. For any $v \in B^{d_S}[u,\varepsilon]$ we have $d_S(u,v) \leq \varepsilon$. By construction of d_S, we also have $d_\nu(u_\nu, v_\nu) \leq \varepsilon$ for any $\nu \in S^\infty$. Hence, wee see that $v_\nu \in B^{d_\nu}[u_\nu,\varepsilon]$ for all $\nu \in S^\infty$. Therefore, we see that $B^{d_S}[u,\varepsilon] \subseteq \prod_{\nu \in S^\infty} B^{d_\nu}[u_\nu,\varepsilon]$. We claim that $B^{d_\nu}[u_\nu,\varepsilon]$ is compact in K_ν for all $\nu \in S^\infty$. Since the product of compact sets is compact, it would follow that $\prod_{\nu \in S^\infty} B^{d_\nu}[u_\nu,\varepsilon]$ is compact. Theorem 5.1.7 in [Sin19] tells us that closed sets in compact sets are compact itself. Since $B^{d_S}[u,\varepsilon]$ is closed, it follows that it is compact. In its turn A is closed and contained in compact set $B^{d_S}[u,\varepsilon]$, so it must be compact itself.

So it remains to show the claim. For any $\sigma \in \Sigma_K^\infty$, by Theorem 1.4.8, the completion K_σ is isomorphic to $\mathbb{R}$ or $\mathbb{C}$. It follows that $B^{d_\sigma}[u_\sigma,\varepsilon]$ is compact in K_σ by the Heine-Borel Theorem for $\mathbb{R}^m$ (take $m = 1, 2$). So take any $\mathfrak{p} \in S$. We know that the image of the absolute value $|.|_\mathfrak{p}$ consists only of powers of $N_{\mathcal{O}_K}(\mathfrak{p})$. So there exists some $k \in \mathbb{Z}$ such that $B^{d_\mathfrak{p}}[u_\mathfrak{p},\varepsilon] = B^{d_\mathfrak{p}}[u_\mathfrak{p}, N_{\mathcal{O}_K}(\mathfrak{p})^{-k}]$. Let $B_0 := B^{d_\mathfrak{p}}[u_\mathfrak{p}, N_{\mathcal{O}_K}(\mathfrak{p})^{-k}]$, and take any $x \in B_0$. Then

$$|x - u_\mathfrak{p}|_\mathfrak{p} = d_\mathfrak{p}(x, u_\mathfrak{p}) \leq N_{\mathcal{O}_K}(\mathfrak{p})^{-k}.$$

Take any $a \in \mathfrak{p}^k \backslash \mathfrak{p}^{k+1}$. We know that $\mathrm{ord}_\mathfrak{p}(a) = k$, or equivalently $|a|_\mathfrak{p} = N_{\mathcal{O}_K}(\mathfrak{p})^{-k}$. So with this result, we can reason that

$$\begin{aligned} |x - u_\mathfrak{p}|_\mathfrak{p} \leq N_{\mathcal{O}_K}(\mathfrak{p})^{-k} &\implies N_{\mathcal{O}_K}(\mathfrak{p})^k |x - u_\mathfrak{p}|_\mathfrak{p} \leq 1 \\ &\implies |a^{-1}|_\mathfrak{p} |x - u_\mathfrak{p}|_\mathfrak{p} \leq 1 \\ &\implies |a^{-1}(x - u_\mathfrak{p})|_\mathfrak{p} \leq 1. \end{aligned}$$

By definition, we have $a^{-1}(x-u_\mathfrak{p}) \in \mathcal{O}_\mathfrak{p}$. Let R be a set of representatives of $\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$. Then there exists some $r \in R$ such that $a^{-1}(x-u_\mathfrak{p}) - r \in \mathfrak{m}_\mathfrak{p}$. Therefore, we have $\mathrm{ord}_\mathfrak{p}(a^{-1}(x-u_\mathfrak{p})-r) > 0$. Then

$$\begin{aligned} |a^{-1}(x-u_\mathfrak{p}) - r|_\mathfrak{p} \leq N_{\mathcal{O}_K}(\mathfrak{p})^{-1} &\implies |a^{-1}|_\mathfrak{p}|x-u_\mathfrak{p}-ar|_\mathfrak{p} \leq N_{\mathcal{O}_K}(\mathfrak{p})^{-1} \\ &\implies |x-u_\mathfrak{p}-ar|_\mathfrak{p} \leq N_{\mathcal{O}_K}(\mathfrak{p})^{-k-1}. \end{aligned}$$

We see that $x \in B^{d_\mathfrak{p}}[u_\mathfrak{p}+ar, N_{\mathcal{O}_K}(\mathfrak{p})^{-k-1}]$. Since we took $x \in B_0$ arbitrarily, we can say that

$$B_0 \subseteq \bigcup_{r\in R} B^{d_\mathfrak{p}}[u_\mathfrak{p}+ar, N_{\mathcal{O}_K}(\mathfrak{p})^{-k-1}].$$

We will show the other inclusion as well. Take any $x \in \bigcup_{r\in R} B^{d_\mathfrak{p}}[u_\mathfrak{p}+ar, N_{\mathcal{O}_K}(\mathfrak{p})^{-k-1}]$. Then there exists an $r \in R$ such that $|x-u_\mathfrak{p}+ar|_\mathfrak{p} \leq N_{\mathcal{O}_K}(\mathfrak{p})^{-k-1}$. We have that $r \in \mathcal{O}_\mathfrak{p}$, so $|r|_\mathfrak{p} \leq 1$. Therefore, we get that $|ar|_\mathfrak{p} \leq N_{\mathcal{O}_K}(\mathfrak{p})^{-k}$. Using the strong triangle inequality, we get

$$|x-u_\mathfrak{p}|_\mathfrak{p} = |x-u_\mathfrak{p}+ar-ar|_\mathfrak{p} \leq \max\{|x-u_\mathfrak{p}+ar|_\mathfrak{p}, |ar|_\mathfrak{p}\} \leq N_{\mathcal{O}_K}(\mathfrak{p})^{-k}.$$

It follows that $x \in B_0$. So by inclusion from both sides, we can say that

$$B_0 = \bigcup_{r\in R} B^{d_\mathfrak{p}}[u_\mathfrak{p}+ar, N_{\mathcal{O}_K}(\mathfrak{p})^{-k-1}].$$

Now, suppose that B_0 is not compact in $K_\mathfrak{p}$. Then there exists an open cover $\{A_i\}_{i\in I}$ of B_0 that has no finite subcover, where I is some index set. Since R is a finite set, there exists some $r \in R$ such that

$$B_1 := B^{d_\mathfrak{p}}[u_\mathfrak{p}+ar, N_{\mathcal{O}_K}(\mathfrak{p})^{-k-1}]$$

cannot be covered by finitely many open sets from the open cover. Now, replace B_0 by B_1, to find a closed ball B_2 in B_1 of radius $N_{\mathcal{O}_K}(\mathfrak{p})^{-k-2}$ that cannot be covered by finitely many open sets from the open cover. Continuing this argument, we find an infinite sequence of closed balls $(B_j)_{j\geq 0}$ such that $B_j \subseteq B_{j-1}$, B_j has radius $N_{\mathcal{O}_K}(\mathfrak{p})^{-k-j}$, and B_j cannot be covered by finitely many open sets from the open cover. For $j \in \mathbb{Z}_{\geq 0}$ chose any $x_j \in B_j$. In this way, we create a sequence $(x_j)_{j\geq 0}$. By Lemma 3.3.1, we have $B_j = B^{d_\mathfrak{p}}[x_j, N_{\mathcal{O}_K}(\mathfrak{p})^{-k-j}]$. For $j,l \in \mathbb{Z}_{\geq 0}$ we have $B_j \subseteq B_l$ or vice versa. This implies that

$$|x_j - x_l|_\mathfrak{p} \leq N_{\mathcal{O}_K}(\mathfrak{p})^{-k-\min\{j,l\}} \to 0, \qquad \text{if } j,l \to \infty.$$

Since $K_\mathfrak{p}$ is complete, there exists a limit $x \in K_\mathfrak{p}$ of the sequence $(x_j)_{j\geq 0}$. Moreover, for any $j \in \mathbb{Z}_{\geq 0}$ we have

$$|x-x_j|_\mathfrak{p} = \lim_{l\to\infty} |x_l - x_j|_\mathfrak{p} \leq N_{\mathcal{O}_K}(\mathfrak{p})^{-k-j}.$$

Therefore, we have $x \in B^{d_\mathfrak{p}}[x_j, N_{\mathcal{O}_K}(\mathfrak{p})^{-k-j}] = B_j$ for all $j \in \mathbb{Z}_{\geq 0}$. By Lemma 3.3.1 it follows that $B_j = B^{d_\mathfrak{p}}[x, N_{\mathcal{O}_K}(\mathfrak{p})^{-k-j}]$. Now, since $\{A_i\}_{i\in I}$ covers B_0, there exists some $m \in I$ such that $x \in A_m$. Since A_m is open, there exists some $j \in \mathbb{Z}_{\geq 0}$ such that $x \in B_j$ and $B_j \subseteq A_m$. But then B_j can be covered by finitely many open sets from the open cover. Thus, we reach a contradiction. From our assumptions, we conclude that B_0 must be compact. □

Remark 3.3.13. If $K = \mathbb{Q}$, then this result is Theorem 4.1 of [Eve11]. We used the ideas of the proof in these lecture notes to generalize it to any number field. ♦

The topology on K_S, induced from the metric d_S, allows us to create the Borel σ-algebra $\mathcal{B}(K_S)$. Besides stating that K_S is an abelian L-group, Proposition 2.5.3 constructs a Haar measure on $\mathcal{B}(K_S)$. Specifically, it is the product measure of the Haar measures μ_ν on $\mathcal{B}(K_\nu)$ for $\nu \in S^\infty$. We denote this Haar measure on $\mathcal{B}(K_S)$ by d_S, and notation wise we have $\mu_S = \bigotimes_{\nu\in S^\infty} \mu_\nu$.

Definition 3.3.14. The measure space $(K_S, \mathcal{B}(K_S), \mu_S)$ is called the *S-Minkowski space* of K.

The S-Minkowski space of K can be seen as an extension of the Minkowski space as described in Definition 3.3.7. Namely, if we take $S = \emptyset$, we recover the Minkowski space. In the rest of this thesis, we will use $K_{\mathbb{R}}$ to denote the Minkowski space, rather than $K_\emptyset$. Furthermore, we can embed K into K_S. For any $\nu \in \mathcal{V}_K$, the completion K_ν comes with a field embedding $K \to K_\nu$. Using these field embeddings diagonally, we get a way to embed K into K_S. We denote this field embedding by $\Psi_S \colon K \to K_S$.

Definition 3.3.15. The field embedding $\Psi_S \colon K \to K_S$ is called the *S-Minkowski embedding* of K.

If we take $S = \emptyset$, we recover the Minkowski embedding Ψ (see Definition 1.8.3). We rather denote the Minkowski embedding by Ψ than $\Psi_\emptyset$.

Proposition 3.3.16. The S-Minkowski field embedding Ψ_S is a ring homomorphism and $\Psi_S(K)$ is dense in K_S.

Proof. The map Ψ_S is a ring homomorphism since all the field embeddings at all places are ring homomorphisms. Theorem 4.2 in Chapter 2 of [Cas86] states that $\Psi_S(K)$ is dense in K_S. □

Remark 3.3.17. Whenever we take $x \in K$, and consider the element $\Psi_S(x) \in K_S$, we use the convention that $\Psi_S(x) = (x)_{\nu \in S^\infty}$. So we ignore the embeddings from K into a completion K_ν for $\nu \in S^\infty$. ♦

3.3.3 Analogue of Minkowski's Convex Body Theorem

The space K_S contains completions with respect to finite places if $S \neq \emptyset$. In that case, it is not a Euclidean space. Namely, it is not an $\mathbb{R}$-vector space. This is different from $K_{\mathbb{R}}$, as we saw in Section 1.8. We know that Minkowski's Convex Body Theorem only holds for Euclidean spaces. We were interested to see if it is possible to extend this theorem to K_S. Namely, we have a notion of volume and lattices on K_S. So all ingredients are available. In this section, we will show that there is a way to get an analogue of Minkowski's Convex Body Theorem for K_S.

The first step is to generalize Lemma 3.3.4 and Proposition 3.3.6.

Remark 3.3.18. Throughout this thesis, we denote the multiplicative units of the ring K_S by K_S^*. They are given by all the elements in K_S with non-zero entries. ♦

Lemma 3.3.19. Let $u \in K_S^*$.

i.) If $A \subseteq K_S$ is an open subset, then so is uA.

ii.) If $A \subseteq K_S$ is a Borel measurable subset, then so is uA.

Proof. To show Statement (i.), let $A \subseteq K_S$ be open, and take any $v \in uA$. Then there exists some $a \in A$ such that $v = ua$. Since A is open, there exists some $\varepsilon \in \mathbb{R}_{>0}$ such that $B^{d_S}(a, \varepsilon) \subseteq A$. Set $\alpha := \min_{\nu \in S^\infty}\{|u_\nu|_\nu\}$, $\lambda := \alpha\varepsilon$, and take any $w \in B^{d_S}(v, \lambda)$. Note that

$$d_S(w, ua) = \sum_{\nu \in S^\infty} |w_\nu - u_\nu a_\nu|_\nu = \sum_{\nu \in S^\infty} |u_\nu|_\nu \left|\frac{w_\nu}{u_\nu} - a_\nu\right|_\nu \geq \alpha \sum_{\nu \in S^\infty} \left|\frac{w_\nu}{u_\nu} - a_\nu\right|_\nu = \alpha d_S\left(\frac{w}{u}, a\right).$$

So

$$d_S(w, v) < \lambda \implies d_S(w, ua) < \lambda \implies \alpha d_S\left(\frac{w}{u}, a\right) < \lambda \implies d_S\left(\frac{w}{u}, a\right) < \frac{\lambda}{\alpha} = \varepsilon.$$

We obtain that $\frac{w}{u} \in B^{d_S}(a, \varepsilon) \subseteq A$, and so $w \in uA$. This implies that $B^{d_S}(v, \lambda) \subseteq uA$, and therefore uA is open.

To show Statement (ii.), consider the map $f \colon K_S \to K_S$ given by $v \mapsto u^{-1}v$. For any open subset $A \subseteq K_S$, we know from Statement (i.) that $f^{-1}(A) = uA$ is open. It follows that $uA \in \mathcal{B}(K_S)$. Since $\mathcal{B}(K_S)$ is generated by the open sets of K_S, it follows from Proposition 1.6.13 that f is (K_S, K_S)-measurable. This means that for any $A \in \mathcal{B}(K_S)$ the set $f^{-1}(A) = uA$ is Borel measurable. □

Take any $A \in \mathcal{B}(K_S)$ such that $A = \prod_{\nu \in S^\infty} A_\nu$ for some and $A_\nu \in \mathcal{B}(K_\nu)$. For any $u \in K_S^*$, Lemma 3.3.19 (ii.) tells us that $uA \in \mathcal{B}(K_S)$. So we can take the measure of this set. We get

$$\mu_S(uA) = \mu_S\left(\prod_{\nu \in S^\infty} u_\nu A_\nu\right) = \left(\bigotimes_{\nu \in S^\infty} \mu_\nu\right)\left(\prod_{\nu \in S^\infty} u_\nu A_\nu\right) = \prod_{\nu \in S^\infty} \mu_\nu(u_\nu A_\nu),$$

where we used the construction of the product measure. Using Proposition 3.3.6, we obtain that

$$\prod_{\nu \in S^\infty} \mu_\nu(u_\nu A_\nu) = \prod_{\nu \in S^\infty} \|u_\nu\|_\nu \mu_\nu(A_\nu) = \left(\prod_{\nu \in S^\infty} \|u_\nu\|_\nu\right) \mu_S\left(\prod_{\nu \in S^\infty} A_\nu\right) = \left(\prod_{\nu \in S^\infty} \|u_\nu\|_\nu\right) \mu_S(A).$$

So we obtain that $\mu_S(uA) = \left(\prod_{\nu \in S^\infty} \|u_\nu\|_\nu\right) \mu_S(A)$. This result can be extended to any $A \in \mathcal{B}(K_S)$. The proof of this result is self-written.

Proposition 3.3.20. For any $u \in K_S^*$ and $A \in \mathcal{B}(K_S)$ one has

$$\mu_S(uA) = \left(\prod_{\nu \in S^\infty} \|u_\nu\|_\nu\right) \mu_S(A).$$

Proof. Take any $\nu, \eta \in S^\infty$, any $A \in \mathcal{B}(K_\nu \times K_\eta)$ and $u = (u_\nu, u_\eta) \in K_\nu \times K_\eta$. Consider the product measure $\mu := \mu_\nu \otimes \mu_\eta$ on $\mathcal{B}(K_\nu \times K_\eta)$. We will show that

$$\mu(uA) = \|u_\eta\|_\eta \|u_\nu\|_\nu \mu(A).$$

Using Equation (11) we know that

$$\mu(uA) = \int_{K_\nu} \mu_\eta((uA)_x) \mu_\nu(dx).$$

Using the construction of Equation (10), for any $x \in K_\nu$ one has

$$\begin{aligned}(uA)_x &= \{y \in K_\eta : (x, y) \in uA\} \\ &= \{y \in K_\eta : (xu_\nu^{-1}, yu_\eta^{-1}) \in A\} \\ &= u_\eta\{y \in K_\eta : (xu_\nu^{-1}, y) \in A\} \\ &= u_\eta A_{(xu_\nu^{-1})}.\end{aligned}$$

So we get

$$\mu(uA) = \int_{K_\nu} \mu_\eta((uA)_x) \mu_\nu(dx) = \int_{K_\nu} \mu_\eta\left(u_\eta A_{(xu_\nu^{-1})}\right) \mu_\nu(dx) = \|u_\eta\|_\eta \int_{K_\nu} \mu_\eta\left(A_{(xu_\nu^{-1})}\right) \mu_\nu(dx),$$

where in the last step we used Proposition 3.3.6 for μ_η. Next, let $f \colon K_\nu \to \overline{\mathbb{R}}$ be the function given by $x \mapsto \mu_\eta(A_x)$. In Proposition 1.6.17, we saw that this is $\mathcal{B}(K_\nu)$-measurable. Furthermore, let $g \colon K_\nu \to K_\nu$ be the map given by $x \mapsto xu_\nu^{-1}$. For any $B \in \mathcal{B}(K_\nu)$, we have $g^{-1}(B) = u_\nu B$. This pre-image is in $\mathcal{B}(K_\nu)$ by Lemma 3.3.4 (ii.). Hence, the map g is $(\mathcal{B}(K_\nu), \mathcal{B}(K_\nu))$-measurable. Moreover, we can write

$$\int_{K_\nu} \mu_\eta\left(A_{(xu_\nu^{-1})}\right) \mu_\nu(dx) = \int_{K_\nu} f(g(x)) \mu_\nu(dx).$$

Now, applying Theorem 1.6.15 we get

$$\int_{K_\nu} f(g(x)) \mu_\nu(dx) = \int_{K_\nu} f(x)(g^* \mu_\nu)(dx).$$

Now, for any $B \in \mathcal{B}(K_\nu)$, we have

$$g^*\mu_\nu(B) = \mu_\nu(g^{-1}(B)) = \mu_\nu(u_\nu B) = \|u_\nu\|_\nu \mu_\nu(B),$$

using Proposition 3.3.6 for μ_ν. Thus, we have $g^*\mu_1 = \|u_\nu\|_\nu \mu_1$. Therefore

$$\int_{K_\nu} f(x)(g^*\mu_\nu)(dx) = \|u_\nu\|_\nu \int_{K_\nu} f(x)\mu_\nu(dx) = \|u_\nu\|_\nu \int_{K_\nu} \mu_\eta(A_x)\mu_\nu(dx) = \|u_\nu\|_\nu \mu(A).$$

Combining all equalities, we obtain that $\mu(uA) = \|u_\eta\|_\eta \|u_\nu\|_\nu \mu(A)$. Now, applying the argument recursively, gives the desired result. □

Minkowski's Convex Body Theorem makes use of symmetric and convex subsets of a Euclidean space (see Definition 1.7.6 and Definition 1.7.7). We have to extend these notions to K_S.

Definition 3.3.21. Let A be a subset of K_S. The set A is said to be *symmetric* if for all $u \in A$ also $-u \in A$.

Definition 3.3.22. Let A be a subset of K_S and $w \in K_S^*$. The set A is said to be *w-convex* if $w(u+v) \in A$ for all $u, v \in A$.

Definition 3.3.21 is a natural extension of Definition 1.7.6. It is not immediately clear why w-convexity is an extension of convexity in Euclidean spaces. Therefore, we will explain the reasoning behind the definition. In Remark 1.7.9, we saw that one does not need convexity in Minkowski's Convex Body Theorem. One needs that

$$\frac{1}{2}u + \frac{1}{2}v \in A, \qquad u, v \in A, \tag{27}$$

for some symmetric Borel measurable set A of the Euclidean space. We know that $\Psi_S(\frac{1}{2}) \in K_S^*$. Therefore, we see that $\Psi_S(\frac{1}{2})$-convexity, as described in Definition 3.3.22, is an extension of condition (27). So the first idea was to use $\Psi_S(\frac{1}{2})$-convexity in the analogue of Minkowski's Convex Body Theorem. But we noticed that it could be generalized to w-convexity for any $w \in K_S^*$.

The following result is an analogue of Minkowski's Convex Body Theorem.

Theorem 3.3.23. Let Γ be a lattice in K_S and A a symmetric Borel measurable set of K_S. Moreover, let A be w-convex for some $w \in K_S^*$. If $\mu_S(A) > \left(\prod_{\nu \in S^\infty} \|w_\nu^{-1}\|_\nu\right) \mathrm{covol}(\Gamma)$, then A contains at least one non-zero lattice point of Γ.

Proof. Suppose that the sets $wA + u$, for $u \in \Gamma$ are pairwise disjoint. Let Λ be a fundamental region of Γ, as described in Definition 2.4.6. Then also the sets $\Lambda \cap (wA + u)$, for $u \in \Gamma$ are pairwise disjoint. Moreover, by Corollary 2.1.4 and Lemma 3.3.19 (ii.), the sets $\Lambda \cap (wA + u)$, for $u \in \Gamma$ are Borel measurable. We have

$$\bigsqcup_{u \in \Gamma} \Lambda \cap (wA + u) \subseteq \Lambda.$$

Therefore, by Proposition 1.6.4 and, we have

$$\mu_S(\Lambda) \geq \mu_S\left(\bigsqcup_{u \in \Gamma} \Lambda \cap (wA + u)\right) = \sum_{u \in \Gamma} \mu_S\left(\Lambda \cap (wA + u)\right), \tag{28}$$

where we used that μ_S is countable additive. We know by Definition 2.2.3 that μ_S is invariant under translations. Therefore

$$\mu_S\left(\Lambda \cap (wA + u)\right) = \mu_S\left((\Lambda \cap (wA + u)) - u\right) = \mu_S\left((\Lambda - u) \cap wA\right). \tag{29}$$

Since Λ is a fundamental region of Γ, we know that $K_S = \bigsqcup_{u\in\Gamma}(\Lambda - u)$. Therefore, we have

$$wA = K_S \cap wA = \left(\bigsqcup_{u\in\Gamma}(\Lambda - u)\right) \cap wA = \bigsqcup_{u\in\Gamma}(\Lambda - u) \cap wA. \tag{30}$$

Combining equations (28),(29) and (30) we obtain

$$\mu_S(\Lambda) \geq \sum_{u\in\Gamma} \mu_S\left(\Lambda \cap (wA + u)\right) = \sum_{u\in\Gamma} \mu_S\left((\Lambda - u) \cap wA\right) = \mu_S\left(\bigsqcup_{u\in\Gamma}(\Lambda - u) \cap wA\right) = \mu_S\left(wA\right).$$

By Proposition 3.3.20, we get that

$$\mu_S\left(wA\right) = \left(\prod_{\nu\in S^\infty} \|w_\nu\|_\nu\right) \mu_S(A).$$

So we have

$$\operatorname{covol}(\Gamma) = \mu_S(\Lambda) \geq \mu_S\left(wA\right) = \left(\prod_{\nu\in S^\infty} \|w\|_\nu\right) \mu_S(A),$$

contradicting the hypothesis. So by contradiction, the sets $wA + u$, for $u \in \Gamma$ are not pairwise disjoint. In particular, there exist distinct $u, v \in \Gamma$ such that

$$(wA + u) \cap (wA + v) \neq \emptyset.$$

Hence, there exist $a, b \in A$ such that $wa + u = wb + v$. Set $\alpha := u - v = wb - wa$. Since A is symmetric we have $-a \in A$. Moreover, the set A is w-convex, so we have $\alpha = wb - wa \in A$. Since Γ is a subgroup of K_S, we also have $\alpha = a - b \in \Gamma$. As a result of this, we know $\alpha \in \Gamma \cap A$. Since u, v were distinct, the element α is non-zero. □

While this proof is new to the literature, it is very much based on the proof of Minkowski's Convex Body Theorem in [Neu99, Theorem 4.4, Chapter I].

Remark 3.3.24. Theorem 3.3.23 could be generalized to any abelian L-group. Let G be an abelian L-group, and consider the measure space $(G, \mathcal{B}(G), \mu_G)$, where μ_G is some Haar measure on $\mathcal{B}(G)$. Moreover, let G be an R-module for some ring R (in the case of K_S, we could view K_S as a K_S-module). Suppose that $A \in \mathcal{B}(G)$ is a set such that

i.) $-u \in A$ for all $u \in A$ (analogue of Definition 3.3.21),

ii.) there exists an $r \in R$ such that $rA \in \mathcal{B}(G)$ (analogue of Lemma 3.3.19 (ii.)),

iii.) and for all $a, b \in A$ we have $r(a + b) \in A$ (analogue of Definition 3.3.22).

Let Γ be a lattice in G. If

$$\mu_G(rA) > \operatorname{covol}(\Gamma), \tag{31}$$

then A contains at least one non-zero lattice point of Γ. The proof is similar to the one we saw for K_S. In the case of K_S, condition (31) could be simplified with the use of Proposition 3.3.20. ♦

3.4 Minkowski Theory for the Ring of S-Integers

As stated before, we constructed K_S to be able to generalize Theorem 1.8.6. We will do this in this section. All proofs are self-written. Throughout this section, we use Theorem 2.6.4. Namely, a subset in K_S is a lattice if and only if it is a discrete and co-compact subgroup. Moreover, consider the real number

$$\mathfrak{D}_S := \prod_{\mathfrak{p}\in S} \left(N_{\mathcal{O}_\mathfrak{p}}(\mathfrak{D}_{\mathcal{O}_\mathfrak{p}|\mathbb{Z}_p})\right). \tag{32}$$

To embed fractional ideals of $\mathcal{O}_{K,S}$ into K_S, we use the S-Minkowski embedding Ψ_S (see Definition 3.3.15). Now, the first part of the extension of Theorem 1.8.6 was proved by [Con24b] in Theorem 2.1.

Proposition 3.4.1. The image of $\mathcal{O}_{K,S}$ under Ψ_S is a lattice in K_S.

If we take $S = \emptyset$, we recover the fact that $\Psi(\mathcal{O}_K)$ is a lattice in $K_\mathbb{R}$. We saw that the covolume of $\Psi(\mathcal{O}_K)$ equals $\sqrt{|d_K|_\infty}$ with respect to $\mu_\mathbb{R}$ (see Remark 3.3.8). A natural question is to ask for the covolume of the lattice $\Psi_S(\mathcal{O}_{K,S})$ in K_S.

Lemma 3.4.2. Let $\mathfrak{p} \in \mathfrak{P}_K^0$ and $k \in \mathbb{Z}$. For any $x \in \mathfrak{m}_\mathfrak{p}^k$ there exists an $a \in \mathfrak{p}^k$ such that $|x-a|_\mathfrak{p} \leq 1$.

Proof. Since $x \in \mathfrak{m}_\mathfrak{p}^k$, we have $\mathrm{ord}_\mathfrak{p}(x) \geq k$. So, if $k \geq 0$, we have $\mathrm{ord}_\mathfrak{p}(x) \geq 0$. Then we can take any $a \in \mathfrak{p}^k$. Namely, one has $\mathrm{ord}_\mathfrak{p}(a) \geq 0$, and so $\mathrm{ord}_\mathfrak{p}(x-a) \geq \min\{\mathrm{ord}_\mathfrak{p}(x), \mathrm{ord}_\mathfrak{p}(a)\} \geq 0$. This is equivalent to saying $|x-a|_\mathfrak{p} \leq 1$. Suppose that $k < 0$. From Theorem 4.1 in Chapter 10 of [Cas86] we can deduce that for any $x \in K_\mathfrak{p}$, there exists an $a \in K$ such that

$$|x-a|_\mathfrak{p} < 1, \qquad |a|_\mathfrak{q} \leq 1, \text{ for all } \mathfrak{q} \in \mathfrak{P}_K^0 \backslash \{\mathfrak{p}\}.$$

So there exists also such $a \in K$ for $x \in \mathfrak{m}_\mathfrak{p}^k$. It remains to show that such a lives in $\mathfrak{p}^k$. This is the case if $\mathfrak{p}^k | a\mathcal{O}_K$, or equivalently $\mathrm{ord}_\mathfrak{p}(a) \geq k$ and $\mathrm{ord}_\mathfrak{q}(a) \geq 0$ for all $\mathfrak{q} \in \mathfrak{P}_K^0 \backslash \{\mathfrak{p}\}$. Suppose that $\mathrm{ord}_\mathfrak{p}(a) < k$. Then

$$\mathrm{ord}_\mathfrak{p}(x-a) \geq \min\{\mathrm{ord}_\mathfrak{p}(x), \mathrm{ord}_\mathfrak{p}(a)\} = \mathrm{ord}_\mathfrak{p}(a).$$

Suppose, for the matter of contradiction, that $\mathrm{ord}_\mathfrak{p}(x-a) > \mathrm{ord}_\mathfrak{p}(a)$, then

$$\mathrm{ord}_\mathfrak{p}(a) = \mathrm{ord}_\mathfrak{p}(-a) = \mathrm{ord}_\mathfrak{p}((x-a)-x) \geq \min\{\mathrm{ord}_\mathfrak{p}(x-a), \mathrm{ord}_\mathfrak{p}(x)\} > \mathrm{ord}_\mathfrak{p}(a).$$

We reach a contradiction. Therefore, we have $\mathrm{ord}_\mathfrak{p}(x-a) = \mathrm{ord}_\mathfrak{p}(a)$. Equivalently, we have

$$|x-a|_\mathfrak{p} = |a|_\mathfrak{p} = N_{\mathcal{O}_K}(\mathfrak{p})^{-k} \geq 1,$$

using that $k < 0$. But we had $|x-a|_\mathfrak{p} \leq 1$. So we have again a contradiction. Therefore, we obtain $\mathrm{ord}_\mathfrak{p}(a) \geq k$. □

Theorem 3.4.3. Let Λ be a fundamental region of $\Psi(\mathcal{O}_K)$ in $K_\mathbb{R}$. The set

$$\Pi := \Lambda \times \prod_{\mathfrak{p}\in S^\infty} \mathcal{O}_\mathfrak{p} \subseteq K_S$$

is a fundamental region of $\Psi_S(\mathcal{O}_{K,S})$ in K_S. Consequently, the covolume, with respect to the Haar measure μ_S on $\mathcal{B}(K_S)$, of the lattice $\Psi_S(\mathcal{O}_{K,S})$ in K_S equals $\sqrt{|d_K|_\infty \mathfrak{D}_S^{-1}}$.

Proof. In Remark 3.3.8, we have seen the Haar measure $\mu_\mathbb{R}$ on $\mathcal{B}(K_\mathbb{R})$. By the same remark, we obtained $\mathrm{covol}(\Psi(\mathcal{O}_K)) = \mu_\mathbb{R}(\Lambda) = \sqrt{|d_K|_\infty}$. Since $\mu_S = \bigotimes_{\nu\in S^\infty} \mu_\nu$, we have

$$\mu_S = \left(\bigotimes_{\sigma\in\Sigma_K^\infty} \mu_\sigma\right) \otimes \left(\bigotimes_{\mathfrak{p}\in S} \mu_\mathfrak{p}\right) = \mu_\mathbb{R} \otimes \left(\bigotimes_{\mathfrak{p}\in S} \mu_\mathfrak{p}\right). \tag{33}$$

If Π is a fundamental region of $\Psi_S(\mathcal{O}_{K,S})$, then using (33) we have that

$$\operatorname{covol}(\Psi_S(\mathcal{O}_{K,S})) = \mu_S(\Pi) = \mu_{\mathbb{R}}(\Lambda)\prod_{\mathfrak{p}\in S}\mu_{\mathfrak{p}}(\mathcal{O}_{\mathfrak{p}}) = \sqrt{|d_K|_\infty \mathfrak{D}_S^{-1}},$$

where we used that $\mu_{\mathfrak{p}}(\mathcal{O}_{\mathfrak{p}}) = N_{\mathcal{O}_{\mathfrak{p}}}(\mathfrak{D}_{\mathcal{O}_{\mathfrak{p}}|\mathbb{Z}_p})^{-1/2}$ for all $\mathfrak{p}\in\mathfrak{P}_K^0$.

So it remains to show that Π is a fundamental region of $\Psi_S(\mathcal{O}_{K,S})$. First notice that Π is Borel measurable since it is the product of Borel measurable sets. Suppose that the union $\bigcup_{u\in\Psi_S(\mathcal{O}_{K,S})}(u+\Pi)$ is not disjoint. Then there exist distinct $\Psi_S(x),\Psi_S(y)\in\Psi_S(\mathcal{O}_{K,S})$ and distinct $u,v\in\Pi$ such that $\Psi_S(x)+u=\Psi_S(y)+v$. Looking at the entries, this means that $x+u_\nu = y+v_\nu$ for all $\nu\in S^\infty$, where we used the convention of Remark 3.3.17. Set $\alpha := x-y$, then $\alpha = v_\nu - u_\nu$ for all $\nu\in S^\infty$. Note that α is non-zero since x,y are distinct. Since $x,y\in\mathcal{O}_{K,S}$, we have $\alpha\in\mathcal{O}_{K,S}$. This means that $\operatorname{ord}_{\mathfrak{p}}(\alpha)\geq 0$ for all $\mathfrak{p}\notin S$. On the other hand, we have $u_{\mathfrak{p}},v_{\mathfrak{p}}\in\mathcal{O}_{\mathfrak{p}}$ for all $\mathfrak{p}\in S$. Therefore, we have $\alpha\in\mathcal{O}_{\mathfrak{p}}$, i.e. $\operatorname{ord}_{\mathfrak{p}}(\alpha)\geq 0$ for all $\mathfrak{p}\in S$. In particular, we see that $\operatorname{ord}_{\mathfrak{p}}(\alpha)\geq 0$ for all $\mathfrak{p}\in\mathfrak{P}_K^0$. Hence, we have that $\alpha\in\mathcal{O}_K$. Then for all $\sigma\in\Sigma_K^\infty$, we have $v_\sigma - u_\sigma = \alpha\in\mathcal{O}_K$. We obtain that $(v_\sigma)_{\sigma\in\Sigma_K^\infty} = (u_\sigma)_{\sigma\in\Sigma_K^\infty} + \Psi(\alpha)$, and so the sets $0+\Lambda = \Psi(\alpha)+\Lambda$ are not disjoint since α is non-zero. This contradicts the fact that Λ is a fundamental region of $\Psi(\mathcal{O}_K)$, i.e. it satisfies the disjoint union

$$K_{\mathbb{R}} = \bigsqcup_{u\in\Psi_S(\mathcal{O}_K)}(u+\Lambda).$$

Consequently, the union $\bigsqcup_{u\in\Psi_S(\mathcal{O}_{K,S})}(u+\Pi)$ is a disjoint union.

Now, take any $u\in K_S$. For any $\mathfrak{p}\in S$, we have $u_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}} = \mathfrak{m}_{\mathfrak{p}}^{\operatorname{ord}_{\mathfrak{p}}(u_{\mathfrak{p}})}$ (see [Neu99, Page 69]). Thus, we also have $u_{\mathfrak{p}}\in\mathfrak{m}_{\mathfrak{p}}^{\operatorname{ord}_{\mathfrak{p}}(u_{\mathfrak{p}})}$. By Lemma 3.4.2, we know that there exists an $a_{\mathfrak{p}}\in\mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}(u_{\mathfrak{p}})}$ such that $|u_{\mathfrak{p}}-a_{\mathfrak{p}}|_{\mathfrak{p}}\leq 1$. Since $a_{\mathfrak{p}}\in\mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}(u_{\mathfrak{p}})}$, we know that there exists some integral ideal $I\subseteq\mathcal{O}_K$ such that $a_{\mathfrak{p}}\mathcal{O}_K = \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}(u_{\mathfrak{p}})}I$. Hence, we obtain that $\operatorname{ord}_{\mathfrak{q}}(a_{\mathfrak{p}})\geq 0$ for all $\mathfrak{q}\neq\mathfrak{p}$. Equivalently, we have $|a_{\mathfrak{p}}|_{\mathfrak{q}}\leq 1$ for all $\mathfrak{q}\neq\mathfrak{p}$. We do this for all $\mathfrak{p}\in S$, and so we can set $a := \sum_{\mathfrak{p}\in S}a_{\mathfrak{p}}\in K$. Then for any $\mathfrak{q}\in S$, we get

$$|u_{\mathfrak{q}}-a|_{\mathfrak{q}} = \left|u_{\mathfrak{q}} - \sum_{\mathfrak{p}\in S}a_{\mathfrak{p}}\right|_{\mathfrak{q}} \leq \max_{\mathfrak{p}\in S\setminus\{\mathfrak{q}\}}\{|u_{\mathfrak{q}}-a_{\mathfrak{q}}|_{\mathfrak{q}}, |a_{\mathfrak{p}}|_{\mathfrak{q}}\}\leq 1.$$

Equivalently, we know $u_{\mathfrak{p}}-a\in\mathcal{O}_{\mathfrak{p}}$ for all $\mathfrak{p}\in S$. This means that

$$u-\Psi_S(a)\in\prod_{\sigma\in\Sigma_K^\infty}K_\sigma\times\prod_{\mathfrak{p}\in S}\mathcal{O}_{\mathfrak{p}}.$$

Now, by subtracting another element of the form $\Psi_S(b)$ for some $b\in\mathcal{O}_K$, we can bring the infinite entries into Λ. Since $b\in\mathcal{O}_{\mathfrak{p}}$, for all $\mathfrak{p}\in S$, this subtraction does not do anything to the finite places. Then we see that

$$u-\Psi_S(a)-\Psi_S(b)\in\Lambda\times\prod_{\mathfrak{p}\in S}\mathcal{O}_{\mathfrak{p}} = \Pi.$$

It follows that $u\in\Psi_S(a-b)+\Pi$. For any $\mathfrak{p}\in S$, we know that $\operatorname{ord}_{\mathfrak{q}}(a_{\mathfrak{p}})\geq 0$ for all $\mathfrak{q}\notin S$. Therefore, we have $\operatorname{ord}_{\mathfrak{q}}(a)\geq 0$ for all $\mathfrak{q}\notin S$. In particular, we have $a\in\mathcal{O}_{K,S}$. Since $b\in\mathcal{O}_K$, we get $a-b\in\mathcal{O}_{K,S}$. So $u\in\Psi_S(x)+\Pi$ for some $x\in\mathcal{O}_{K,S}$. Since u was taken arbitrary from K_S, it follows that

$$K_S = \bigsqcup_{v\in\Psi_S(\mathcal{O}_{K,S})}(v+\Pi).$$

According to Definition 2.4.6, the subset Π is a fundamental region of the lattice $\Psi_S(\mathcal{O}_{K,S})$. □

Remark 3.4.4. The covolume depends on the normalization of the Haar measure on $\mathcal{B}(K_S)$. We took the covolume with respect to the Haar measure μ_S on $\mathcal{B}(K_S)$. The Haar measure μ_S is taken to be the product measure of the Haar measures μ_ν for $\nu \in \mathcal{V}_K$. In Section 3.3.1, we made choices for these Haar measures on $\mathcal{B}(K_\nu)$. They were also used in Tate's thesis (see Remark 3.3.3). If one were to set $\mu_{\mathfrak{p}}(\mathcal{O}_{\mathfrak{p}}) = 1$ for all $\mathfrak{p} \in \mathfrak{P}_K^0$, one would get that $\operatorname{covol}(\Psi_S(\mathcal{O}_{K,S})) = \sqrt{|d_K|_\infty}$ with respect to μ_S. ♦

To fully extend Theorem 1.8.6, we extend Proposition 3.4.1 to non-zero fractional ideals of $\mathcal{O}_{K,S}$.

Lemma 3.4.5. Let Γ be a lattice in K_S and take $u \in K_S^*$. Then $u\Gamma$ is a lattice in K_S. Moreover, its covolume is given by $\operatorname{covol}(u\Gamma) = \left(\prod_{\nu \in S^\infty} \|u_\nu\|_\nu\right) \operatorname{covol}(\Gamma)$.

Proof. Since Γ is an additive subgroup of K_S, also $u\Gamma$ is an additive subgroup of K_S. Now, take any $v \in u\Gamma$. Then there exists some $\gamma \in \Gamma$ such that $v = u\gamma$. Since Γ is a lattice, it is also discrete. Therefore, there exists some open neighborhood A of γ such that $\Gamma \cap A = \{\gamma\}$. Since $u \in K_S^*$ has no non-zero entries, we have $u\Gamma \cap uA = \{u\gamma\} = \{v\}$. Note that $v \in uA$, and by Lemma 3.3.19 (i.) uA is open. It follows that for any $v \in u\Gamma$ there exists an open neighborhood for v containing no other point from $u\Gamma$ than v itself. Hence, we can say that $u\Gamma$ is discrete. It remains to show that $u\Gamma$ is co-compact. Consider the map $f\colon K_S \to K_S$ defined by $v \mapsto uv$. This map is injective since $u \in K_S^*$ has no non-zero entries. For any $v \in K_S$ we can take $u^{-1}v \in K_S$ such that $f(u^{-1}v) = v$. This means that f is surjective. This means that f is bijective, and its inverse is given by multiplication by u^{-1}. In Lemma 3.3.19 (i.), we saw that open sets are preserved under multiplication. Therefore, the map f and its inverse are continuous. In particular, the map f is a homeomorphism of topological groups. Furthermore, the map f is a group homomorphism. Since Γ is a lattice, it is also co-compact. By Proposition 2.6.3, it follows that $f(\Gamma) = u\Gamma$ is co-compact as well. Consequently, we see that $u\Gamma$ is a discrete and co-compact subgroup of K_S, i.e. a lattice.

Now, let Λ be a fundamental region of Γ. Then by Lemma 3.3.19 (ii.), we know that $u\Lambda$ is Borel measurable. Furthermore, the sets $v + u\Lambda$ for $v \in u\Gamma$ are pairwise disjoint. Otherwise, the sets $v + \Lambda$ for $v \in \Gamma$ would not be pairwise disjoint, contradicting the fact that Λ is a fundamental region of Γ. Furthermore, we have

$$\bigsqcup_{v \in u\Gamma} (v + u\Lambda) = \bigsqcup_{v \in \Gamma} (uv + u\Lambda) = u\left(\bigsqcup_{v \in \Gamma} (v + \Lambda)\right) = uK_S.$$

Since $u \in K_S^*$, we get that $uK_S = K_S$. It follows by Definition 2.4.6 that $u\Lambda$ is a fundamental region of $u\Gamma$. Then

$$\operatorname{covol}(u\Gamma) = \mu_S(u\Lambda) = \left(\prod_{\nu \in S^\infty} \|u_\nu\|_\nu\right) \mu_S(\Lambda) = \left(\prod_{\nu \in S^\infty} \|u_\nu\|_\nu\right) \operatorname{covol}(\Gamma),$$

where we used Proposition 3.3.20. □

Theorem 3.4.6. The image of any non-zero fractional ideal I of $\mathcal{O}_{K,S}$ under Ψ_S is a lattice in K_S.

Proof. First, we show that it is true for some principal fractional ideal. So let $x\mathcal{O}_{K,S} \in \mathrm{P}_{K,S}$ for some $x \in K^*$. By Proposition 3.4.1, we know that $\Psi_S(\mathcal{O}_{K,S})$ is a lattice. Since $x \in K^*$, we know that $\Psi_S(x) \in K_S^*$. By applying Lemma 3.4.5, we get that $\Psi_S(x)\Psi_S(\mathcal{O}_{K,S}) = \Psi_S(x\mathcal{O}_{K,S})$ is a lattice in K_S.

Now, let I be any fractional ideal of $\mathcal{O}_{K,S}$. Since I is an additive subgroup in K, and Ψ_S is a ring homomorphism (see Proposition 3.3.16), its image under Ψ_S is also an additive subgroup in K_S. Now, there exists some non-zero $x \in \mathcal{O}_{K,S}$ such that xI is an integral ideal of $\mathcal{O}_{K,S}$. Dividing by x we obtain $I \subseteq \frac{1}{x}\mathcal{O}_{K,S}$. Furthermore, take any non-zero $y \in xI$. Since xI is an integral ideal, we have $y\mathcal{O}_{K,S} \subseteq xI$, and so $\frac{y}{x}\mathcal{O}_{K,S} \subseteq I$. We obtain

$$\frac{y}{x}\mathcal{O}_{K,S} \subseteq I \subseteq \frac{1}{x}\mathcal{O}_{K,S}.$$

This implies that

$$\Psi_S\left(\frac{y}{x}\mathcal{O}_{K,S}\right) \subseteq \Psi_S(I) \subseteq \Psi_S\left(\frac{1}{x}\mathcal{O}_{K,S}\right).$$

By the first result of this proof, we have that $\Psi_S\left(\frac{y}{x}\mathcal{O}_{K,S}\right)$ and $\Psi_S\left(\frac{1}{x}\mathcal{O}_{K,S}\right)$ are lattices. This means that $\Psi_S\left(\frac{1}{x}\mathcal{O}_{K,S}\right)$ is discrete, and so by Proposition 2.3.2 (ii.) $\Psi_S(I)$ is also discrete. Furthermore, we have that $\Psi_S\left(\frac{y}{x}\mathcal{O}_{K,S}\right)$ is co-compact, and so by Proposition 2.6.2 $\Psi_S(I)$ is also co-compact. We see that $\Psi_S(I)$ is a discrete and co-compact subgroup of K_S, i.e. a lattice. □

So we have shown that the image of any fractional ideal I of $\mathcal{O}_{K,S}$ under Ψ_S in K_S is a lattice. This means that we can speak about the covolume for such lattices. Just like Theorem 1.8.6, we can say something explicit about its value.

Lemma 3.4.7. Let $x \in K^*$, then $N_{\mathcal{O}_{K,S}}(x\mathcal{O}_{K,S}) = N_{\mathcal{O}_K}(x\mathcal{O}_K)\prod_{\mathfrak{p}\in S}\|x\|_{\mathfrak{p}}$.

Proof. In Lemma 3.2.2, we have seen that $x\mathcal{O}_{K,S} = \prod_{\mathfrak{p}\notin S}(\mathfrak{p}\mathcal{O}_{K,S})^{\mathrm{ord}_{\mathfrak{p}}(x)}$. By Proposition 3.2.6, it follows that

$$\begin{aligned}
N_{\mathcal{O}_{K,S}}(x\mathcal{O}_{K,S}) &= N_{\mathcal{O}_{K,S}}\left(\prod_{\mathfrak{p}\notin S}(\mathfrak{p}\mathcal{O}_{K,S})^{\mathrm{ord}_{\mathfrak{p}}(x)}\right)\\
&= \prod_{\mathfrak{p}\notin S} N_{\mathcal{O}_{K,S}}(\mathfrak{p}\mathcal{O}_{K,S})^{\mathrm{ord}_{\mathfrak{p}}(x)}\\
&= \prod_{\mathfrak{p}\notin S} N_{\mathcal{O}_K}(\mathfrak{p})^{\mathrm{ord}_{\mathfrak{p}}(x)}\\
&= \frac{\prod_{\mathfrak{p}} N_{\mathcal{O}_K}(\mathfrak{p})^{\mathrm{ord}_{\mathfrak{p}}(x)}}{\prod_{\mathfrak{p}\in S} N_{\mathcal{O}_K}(\mathfrak{p})^{\mathrm{ord}_{\mathfrak{p}}(x)}}\\
&= N_{\mathcal{O}_K}(x\mathcal{O}_K)\prod_{\mathfrak{p}\in S}\|x\|_{\mathfrak{p}},
\end{aligned}$$

where we used that $\|x\|_{\mathfrak{p}} = |x|_{\mathfrak{p}} = N_{\mathcal{O}_K}(\mathfrak{p})^{-\mathrm{ord}_{\mathfrak{p}}(x)}$ for all $\mathfrak{p} \in \mathfrak{P}_K^0$. □

Proposition 3.4.8. Let I be a non-zero fractional ideal of $\mathcal{O}_{K,S}$. Then the covolume, with respect to the Haar measure μ_S on $\mathcal{B}(K_S)$, of the lattice $\Psi_S(I)$ in K_S equals

$$\mathrm{covol}(\Psi_S(I)) = N_{\mathcal{O}_{K,S}}(I)\sqrt{|d_K|_\infty \mathfrak{D}_S^{-1}}.$$

Proof. Let I be a non-zero integral ideal of $\mathcal{O}_{K,S}$. By Theorem 3.4.6, we know that $\Psi_S(I)$ and $\Psi_S(\mathcal{O}_{K,S})$ are lattices in K_S. Furthermore, since $I \subseteq \mathcal{O}_{K,S}$, we also have the inclusion $\Psi_S(I) \subseteq \Psi_S(\mathcal{O}_{K,S})$ of lattices. It follows from Proposition 2.5.8 that $\mathrm{covol}(\Psi_S(I)) = [\Psi_S(\mathcal{O}_{K,S}) : \Psi_S(I)]\,\mathrm{covol}(\Psi_S(\mathcal{O}_{K,S}))$. By injectivity of Ψ_S, we can create a ring isomorphism $\mathcal{O}_{K,S}/I \cong \Psi_S(\mathcal{O}_{K,S})/\Psi_S(I)$. It follows that

$$[\Psi_S(\mathcal{O}_{K,S}) : \Psi_S(I)] = \#\Psi_S(\mathcal{O}_{K,S})/\Psi_S(I) = \#\mathcal{O}_{K,S}/I = N_{\mathcal{O}_{K,S}}(I).$$

We obtain

$$\mathrm{covol}(\Psi_S(I)) = N_{\mathcal{O}_{K,S}}(I)\,\mathrm{covol}(\Psi_S(\mathcal{O}_{K,S})).$$

Now, let I be any fractional ideal of $\mathcal{O}_{K,S}$. Then there exists some non-zero $x \in \mathcal{O}_{K,S}$ such that xI is an integral ideal of $\mathcal{O}_{K,S}$. Thus, by the previous result, we have

$$\mathrm{covol}(\Psi_S(xI)) = N_{\mathcal{O}_{K,S}}(xI)\,\mathrm{covol}(\Psi_S(\mathcal{O}_{K,S})). \tag{34}$$

Since $\Psi_S(xI) = \Psi_S(x)\Psi_S(I)$, and $\Psi_S(x) \in K_S^*$, it follows by Lemma 3.4.5 that

$$\mathrm{covol}(\Psi_S(xI)) = \left(\prod_{\nu\in S^\infty}\|x\|_\nu\right)\mathrm{covol}(\Psi_S(I)).$$

Using Propositions 1.1.15 and 1.2.6, we get that $\prod_{\sigma\in\Sigma_K^\infty}\|x\|_\sigma = N_{\mathcal{O}_K}(x\mathcal{O}_K)$, and so we find

$$\operatorname{covol}(\Psi_S(xI)) = N_{\mathcal{O}_K}(x\mathcal{O}_K)\left(\prod_{\mathfrak{p}\in S}\|x\|_\mathfrak{p}\right)\operatorname{covol}(\Psi_S(I)). \tag{35}$$

Since $N_{\mathcal{O}_{K,S}}$ is a group homomorphism, we have $N_{\mathcal{O}_{K,S}}(xI) = N_{\mathcal{O}_{K,S}}(x\mathcal{O}_{K,S})N_{\mathcal{O}_{K,S}}(I)$. So using Lemma 3.4.7, we get

$$N_{\mathcal{O}_{K,S}}(xI)\operatorname{covol}(\Psi_S(\mathcal{O}_{K,S})) = N_{\mathcal{O}_K}(x\mathcal{O}_K)\left(\prod_{\mathfrak{p}\in S}\|x\|_\mathfrak{p}\right)N_{\mathcal{O}_{K,S}}(I)\operatorname{covol}(\Psi_S(\mathcal{O}_{K,S})). \tag{36}$$

Substituting Equation (35) and (36) into Equation (34) gives us

$$N_{\mathcal{O}_K}(x\mathcal{O}_K)\left(\prod_{\mathfrak{p}\in S}\|x\|_\mathfrak{p}\right)\operatorname{covol}(\Psi_S(I)) = N_{\mathcal{O}_K}(x\mathcal{O}_K)\left(\prod_{\mathfrak{p}\in S}\|x\|_\mathfrak{p}\right)N_{\mathcal{O}_{K,S}}(I)\operatorname{covol}(\Psi_S(\mathcal{O}_{K,S}).$$

This implies that

$$\operatorname{covol}(\Psi_S(I)) = N_{\mathcal{O}_{K,S}}(I)\operatorname{covol}(\Psi_S(\mathcal{O}_{K,S})).$$

Using Theorem 3.4.3, we obtain that

$$\operatorname{covol}(\Psi_S(I)) = N_{\mathcal{O}_{K,S}}(I)\sqrt{|d_K|_\infty\mathfrak{D}_S^{-1}}.$$ □

3.5 Discussion on the Results

At the end of this chapter, we relate the results from the previous section to the existing literature. For this, we have to introduce the adele ring of K. Moreover, we give a conjecture to extend the results from the previous section.

We have seen the completion K_ν for all $\nu\in\mathcal{V}_K$. Furthermore, for any $\mathfrak{p}\in\mathfrak{P}_K^0$, we have the DVR $\mathcal{O}_\mathfrak{p}$. For any $\sigma\in\Sigma_K^\infty$, we set $\mathcal{O}_\sigma := K_\sigma$.

Definition 3.5.1. The ring

$$\mathbb{A}_K := \left\{(x_\nu)_{\nu\in\mathcal{V}_K}\in\prod_{\nu\in\mathcal{V}_K}K_\nu : x_\nu\in\mathcal{O}_\nu \text{ for all but finitely many } \nu\in\mathcal{V}_K\right\}$$

is called the *adele ring* of K.

The adele ring is a commutative ring by entry-wise addition and multiplication. The adele ring of K is endowed with a topology. Namely, we give $\mathbb{A}_K$ the topology where the basis is given by the open sets in the collection

$$\mathcal{B} := \left\{\prod_{\nu\in\mathcal{V}_K}A_\nu : A_\nu\subseteq K_\nu \text{ is open for all } \nu\in\mathcal{V}_K, \text{ and } A_\nu=\mathcal{O}_\nu \text{ for all but finitely many } \nu\in\mathcal{V}_K\right\}.$$

In this way, one can show that we create a locally compact group (see [CF67, Section 13 & 14, Chapter II]). By Proposition 3.3.2, we know that K_ν is second-countable for every $\nu\in\mathcal{V}_K$. Moreover, the set of places $\mathcal{V}_K$ is countable. It follows that $\mathcal{B}$ is a countable set. Therefore, the adele ring is also second-countable. By definition, we get that $\mathbb{A}_K$ is an abelian L-group. Then we know by Theorem 2.2.4, that $\mathcal{A}_K$ attains a unique Haar measure on $\mathcal{B}(\mathbb{A}_K)$, up to scalar multiple. In Section 3.3 in Chapter XV of [CF67], a certain

Haar measure is constructed. We denote this Haar measure by μ_K. It satisfies the following property. Let T be a finite subset of $\mathcal{V}_K$. Consider any Borel measurable set of the form $B := A \times \left(\prod_{\nu \in \mathcal{V}_K \setminus T} \mathcal{O}_\nu\right)$, where $A \subseteq \prod_{\nu \in T} K_\nu$ is Borel measurable. For such a set, we have

$$\mu_K(B) = \mu_T(A) \prod_{\nu \in \mathcal{V}_K \setminus T} \mu_\nu(\mathcal{O}_\mathfrak{p}),$$

where $\mu_T = \bigotimes_{\nu \in T} \mu_\nu$.

For any $\nu \in \mathcal{V}_K$, the completion K_ν comes with a field embedding $K \to K_\nu$. Using these field embeddings diagonally, we get a way to embed K in $\mathbb{A}_K$. We denote this field embedding by $\Psi_K \colon K \to \mathbb{A}_K$. This is well-defined since for any $x \in K$, there are only finitely many $\mathfrak{p} \in \mathfrak{P}_K^0$ such that $x \notin \mathcal{O}_\mathfrak{p}$.

Theorem 3.5.2. The image of K under Ψ_K is a lattice in $\mathbb{A}_K$.

Remark 3.5.3. Notice that it does not make sense to extend this result to non-zero fractional ideals of K. Namely, viewing K as a Dedekind domain, the only non-zero fractional ideal of K is K itself. ♦

This result was proven in Tate's thesis (see [CF67, Corollary 4.1.1, Chapter XV]). A natural question is to ask for the covolume of the lattice $\Psi_K(K)$ in $\mathbb{A}_K$. This was also proven in Tate's thesis (see [CF67, Theorem 4.1.3, Chapter XV]). Namely, let Λ be a fundamental region of $\Psi(\mathcal{O}_K)$ in $K_\mathbb{R}$. Then with a similar argument as in the proof of Theorem 3.4.3, one can show that

$$\Pi := \Lambda \times \prod_{\mathfrak{p} \in \mathfrak{P}_K^0} \mathcal{O}_\mathfrak{p} \subseteq \mathbb{A}_K$$

is a fundamental region of $\Psi_K(K)$ in $\mathbb{A}_K$. In the construction of the Haar measure μ_K above, we set $T = \Sigma_K^\infty$. Then we get

$$\operatorname{covol}(\Psi_K(K)) = \mu_K(\Pi) = \mu_\mathbb{R}(\Lambda) \prod_{\mathfrak{p} \in \mathfrak{P}_K^0} \mu_\mathfrak{p}(\mathcal{O}_\mathfrak{p}) = \sqrt{|d_K|_\infty} \prod_{\mathfrak{p} \in \mathfrak{P}_K^0} \left(N_{\mathcal{O}_\mathfrak{p}}(\mathfrak{D}_{\mathcal{O}_\mathfrak{p}|\mathbb{Z}_p})\right)^{-1/2},$$

where we used that $\mu_\mathfrak{p}(\mathcal{O}_\mathfrak{p}) = N_{\mathcal{O}_\mathfrak{p}}(\mathfrak{D}_{\mathcal{O}_\mathfrak{p}|\mathbb{Z}_p})^{-1/2}$ for all $\mathfrak{p} \in \mathfrak{P}_K^0$. Using Proposition 1.4.10, we see that $|d_K|_\infty = \prod_{\mathfrak{p} \in \mathfrak{P}_K^0} N_{\mathcal{O}_\mathfrak{p}}(\mathfrak{D}_{\mathcal{O}_\mathfrak{p}|Z_p})$. Hence, we get that $\operatorname{covol}(\Psi_K(K)) = 1$, with respect to the Haar measure μ_K on $\mathcal{B}(\mathbb{A}_K)$.

Let us summarize what we have. Let K be any number field and S be a finite set of finite places. Then we have $\mathcal{O}_K \subseteq \mathcal{O}_{K,S} \subseteq K$.

i.) Any non-zero fractional ideal I of the ring of integers $\mathcal{O}_K$ forms a lattice in $K_\mathbb{R}$ and has covolume $N_{\mathcal{O}_K}(I)\sqrt{|d_K|_\infty}$, with respect to the Haar measure $\mu_\mathbb{R}$ on $\mathcal{B}(K_\mathbb{R})$.

ii.) Any non-zero fractional ideal I of the ring of S-integers $\mathcal{O}_{K,S}$ forms a lattice in K_S and has covolume $N_{\mathcal{O}_{K,S}}(I)\sqrt{|d_K|_\infty \mathfrak{D}_S^{-1}}$, with respect to the Haar measure μ_S on $\mathcal{B}(K_S)$.

iii.) The number field K forms a lattice in $\mathbb{A}_K$ and has covolume 1, with respect to the Haar measure μ_K on $\mathcal{B}(\mathbb{A}_K)$.

We can therefore conclude that we have been building the 'bridge' from Minkowski theory, as described in Section 1.8, to the theory of adeles, as described in Tate's thesis. But we have to notice that the bridge is incomplete. Namely, we always assumed S to be a finite set. But if we allow S to be an infinite set, the set $\mathcal{O}_{K,S}$ is still a subring of K. For example, if we take $S = \mathfrak{P}_K^0 \setminus \{\mathfrak{p}\}$ for some $\mathfrak{p} \in \mathfrak{P}_K^0$, we get $\mathcal{O}_{K,S} = \mathcal{O}_{K,\mathfrak{p}}$

(see (9)). However, we cannot determine the rank of the unit group $\mathcal{O}_{K,S}^*$ if S is infinite. Therefore, it is usually of less interest. However, one can copy the proof of Proposition 3.1.5 to show that

$$\mathcal{O}_K\mathcal{P}^{-1} = \mathcal{O}_{K,S}, \qquad \mathcal{P} := \mathcal{O}_K \setminus \bigcup_{\mathfrak{p}\notin S} \mathfrak{p},$$

even if S is infinite. The proof of Corollary 3.1.6 implies that $\mathcal{O}_{K,S}$ is a Dedekind domain. Therefore, the theory of Section 1.1 applies to $\mathcal{O}_{K,S}$ even if S is infinite. Therefore, one may still ask in what space the non-zero fractional ideals of these subrings form a lattice. While this thesis has not studied this problem, we can make a reasonable guess.

Conjecture 3.5.4. Let K be a number field and S be a set of finite places (possibly infinite), and set $S^\infty = \Sigma_K^\infty \cup S$. Any non-zero fractional ideal of the ring

$$\mathcal{O}_{K,S} := \{x \in K : |x|_\mathfrak{p} \leq 1 \text{ for all } \mathfrak{p} \notin S\}$$

forms a lattice in the abelian L-group

$$\mathbb{A}_K^S := \left\{ (x_\nu)_{\nu\in S^\infty} \in \prod_{\nu\in S^\infty} K_\nu : x_\nu \in \mathcal{O}_\nu \text{ for all but finitely many } \nu \in \mathcal{V}_K \right\}.$$

Moreover, its covolume equals

$$N_{\mathcal{O}_{K,S}}(I)\sqrt{|d_K|_\infty \mathfrak{D}_S^{-1}},$$

with respect to a unique Haar measure on $\mathcal{B}(\mathbb{A}_K^S)$ that is constructed in a similar way as μ_K on $\mathcal{B}(\mathbb{A}_K)$.

This conjecture covers all the results. Namely, if $S = \emptyset$, we have $\mathcal{O}_{K,S} = \mathcal{O}_K$ and $\mathbb{A}_K^S = K_\mathbb{R}$. If S is a finite set, we have $\mathbb{A}_K^S = K_S$, since we have a finite product. If $S = \mathfrak{P}_K^0$, it would recover the theory of adeles.

Remark 3.5.5. In Section 3.3.3, we gave an analogue of Minkowski's Convex Body Theorem for K_S. Theorem 2.1 in [Con24a] states an analogue for the adele ring of K. Except, this theorem considered a specific symmetric and convex subset of $\mathbb{A}_K$ and the lattice K. Using Remark 3.3.24, one might be able to extend Theorem 3.3.23 to the adele ring of K. But this has to be studied in more detail to give a conclusive answer. ♦

4 Arakelov Theory for Rings of Integers

As we have seen in the introduction, we are interested in the infrastructure for fake real quadratic orders. In particular, we want to use Arakelov theory to describe it. But what is Arakelov theory for number fields in the first place, and how can it be used to describe the original infrastructure? These questions will be answered in this chapter.

4.1 Definitions and Results

In this section, we give an overview of the definitions and results of Arakelov theory for number fields as described in [Sch08]. We will not be specific and detailed as most of the theory will be covered in a generalization in Chapter 5. Throughout this section, let K be a number field.

Definition 4.1.1. An *Arakelov divisor* D of K is given by a finite formal sum of the form

$$D = \sum_{\mathfrak{p} \in \mathfrak{P}_K^0} n_\mathfrak{p} \mathfrak{p} + \sum_{\sigma \in \Sigma_K^\infty} x_\sigma \sigma, \qquad n_\mathfrak{p} \in \mathbb{Z}, x_\sigma \in \mathbb{R}. \tag{37}$$

The set of Arakelov divisors of K is denoted by Div_K.

Note that Div_K attains an additive group structure. The unit element of Div_K is the zero Arakelov divisor. It is the Arakelov divisor where all coefficients are zero.

Definition 4.1.2. A *principal Arakelov divisor* of K is defined by

$$\mathrm{div}(x) := \sum_{\mathfrak{p} \in \mathfrak{P}_K^0} n_\mathfrak{p} \mathfrak{p} + \sum_{\sigma \in \Sigma_K^\infty} x_\sigma \sigma, \qquad n_\mathfrak{p} = \mathrm{ord}_\mathfrak{p}(x), x_\sigma = -\log |x|_\sigma,$$

for some $x \in K^*$. The set of principal Arakelov divisors of K is denoted by Prin_K.

One can verify that Prin_K forms a subgroup of Div_K.

Definition 4.1.3. The quotient group $\mathrm{Div}_K / \mathrm{Prin}_K$ is called the *Arakelov class group* of K and is denoted by Pic_K.

Throughout this thesis, for $D \in \mathrm{Div}_K$ we denote its equivalence class in Pic_K by $[D]$.

Definition 4.1.4. Two Arakelov S-divisors $D, D' \in \mathrm{Div}_K$ are called *equivalent* if $[D] = [D']$ in Pic_K. Equivalently, there exists an $x \in K^*$ such that $D - D' = \mathrm{div}(x)$.

The group Pic_K is an analogue of the Picard group of a complete projective curve. Just like for divisors on such a curve, we can talk about the degree of an Arakelov divisor.

Definition 4.1.5. The *degree* of a finite place $\mathfrak{p} \in \mathfrak{P}_K^0$ is defined by $\deg(\mathfrak{p}) := \log(N_{\mathcal{O}_K}(\mathfrak{p}))$.

Recall the degree of a field embedding from Definition 1.2.4. We can extend the degree of places linearly, to get the degree of an Arakelov divisor.

Definition 4.1.6. For any Arakelov divisor D of K written as (37), the *degree* of D is defined by

$$\deg(D) := \sum_{\mathfrak{p} \in \mathfrak{P}_K^0} n_\mathfrak{p} \deg(\mathfrak{p}) + \sum_{\sigma \in \Sigma_K^\infty} x_\sigma \deg(\sigma).$$

The subgroup of Arakelov divisors with degree zero is denoted by Div_K^0.

We obtain a group homomorphism $\deg\colon \mathrm{Div}_K \to \mathbb{R}$. A consequence of the product formula (see Theorem 1.5.6) is that $\deg(\mathrm{div}(x)) = 0$ for all $x \in K^*$, i.e. $\mathrm{Prin}_K \subseteq \mathrm{Div}_K^0$.

Definition 4.1.7. The quotient group $\mathrm{Div}_K^0 / \mathrm{Prin}_K$ is called the *degree-zero-Arakelov class group* of K and is denoted by Pic_K^0.

The group Pic_K^0 is an analogue of the subgroup of the Picard group of a complete projective curve consisting of divisors with degree 0.

Let us study the structure of the Arakelov class group a little bit. The principal Arakelov divisors come with a group homomorphism $\mathrm{div}\colon K^* \to \mathrm{Div}_K$. For any $a \in \mathcal{O}_K^*$, we have $\mathrm{ord}_{\mathfrak{p}}(a) = 0$ for all $\mathfrak{p} \in \mathfrak{P}_K^0$. It follows from Proposition 1.5.4 that $\mathrm{div}(a) = 0$ if and only if $a \in \mu_K$. Thus, group homomorphism div induces an injective group homomorphism $\mathrm{div}\colon K^*/\mu_K \to \mathrm{Div}_K$. Besides this, it makes sense to view Arakelov divisors, for which the finite places have coefficients equal to zero, inside $\prod_{\sigma\in\Sigma_K^\infty} \mathbb{R}$. If we restrict div to $\mathcal{O}_K^*$, we can restrict its codomain to $\prod_{\sigma\in\Sigma_K^\infty} \mathbb{R}$. Therefore, the group homomorphism div induces an injective group homomorphism $\tau : \mathcal{O}_K^*/\mu_K \to \prod_{\sigma\in\Sigma_K^\infty} \mathbb{R}$ given by $a \mapsto (-\log|a|_\sigma)_{\sigma\in\Sigma_K^\infty}$. The cokernel of this group homomorphism is denoted by T_K, and is given by

$$T_K := \prod_{\sigma\in\Sigma_K^\infty} \mathbb{R}/\{(\log|a|_\sigma)_{\sigma\in\Sigma_K^\infty} : a \in \mathcal{O}_K^*\}.$$

Define the group homomorphism $\zeta\colon T_K \to \mathrm{Pic}_K$ by $[(x_\sigma)_{\sigma\in\Sigma_K^\infty}] \mapsto [\sum_{\sigma\in\Sigma_K^\infty} x_\sigma\sigma]$. Furthermore, define group homomorphism $\chi\colon \mathrm{Pic}_K \to \mathrm{Cl}_K$ by $[D] \to [\prod_{\mathfrak{p}\in\mathfrak{P}_K^0} \mathfrak{p}^{-n_{\mathfrak{p}}}]$, where D is given as in (37). Then we have a short exact sequence

$$0 \longrightarrow T_K \xrightarrow{\zeta} \mathrm{Pic}_K \xrightarrow{\chi} \mathrm{Cl}_K \longrightarrow 0\ . \tag{38}$$

We will not prove this fact. However, we prove a commutative diagram of short exact sequences, containing this short exact sequence (see Theorem 5.1.16). Since principal Arakelov divisors have degree zero, we can also restrict the codomain of τ to $\left(\prod_{\sigma\in\Sigma_K^\infty} \mathbb{R}\right)^0$, the subgroup of $\prod_{\sigma\in\Sigma_K^\infty} \mathbb{R}$ containing Arakelov divisors of degree zero. We can also obtain a short exact sequence given by

$$0 \longrightarrow T_K^0 \longrightarrow \mathrm{Pic}_K^0 \longrightarrow \mathrm{Cl}_K \longrightarrow 0\ ,$$

where

$$T_K^0 := \left(\prod_{\sigma\in\Sigma_K^\infty} \mathbb{R}\right)^0 /\{(\log|a|_\sigma)_{\sigma\in\Sigma_K^\infty} : a \in \mathcal{O}_K^*\}.$$

For a proof of this result, we refer to the proof of Proposition 2.2 in [Sch08].

Example 4.1.8. Let us take $K = \mathbb{Q}(\sqrt{d})$ for some fundamental discriminant $d \in \mathbb{Z}_{>0}$. For terminology and notation of this number field, we refer to the beginning of Section 1.3. It is conjectured that there are infinitely many values for d such that the class number h_K equals 1 (see [Neu99, Page 37]). If this is the case, the group Cl_K is trivial. Hence, by short exact sequence (38), we have $\mathrm{Pic}_K \cong T_K$. Furthermore, if we look in this case at T_K^0, we have

$$\begin{aligned} T_K^0 &= \{(t,t') \in \mathbb{R}^2 : t + t' = 0\}/\{(\log|\varepsilon_K^k|_\infty, \log|\sigma(\varepsilon_K^k)|_\infty) : k \in \mathbb{Z}\} \\ &= \{(t,-t) | t \in \mathbb{R}\}/\{(k\log|\varepsilon_K|_\infty, -k\log|\varepsilon_K|_\infty) : k \in \mathbb{Z}\} \\ &\cong \mathbb{R}/\log|\varepsilon_K|_\infty\mathbb{Z} \\ &= \mathbb{R}/R_K\mathbb{Z}. \end{aligned}$$

It follows that $\mathrm{Pic}_K^0 \cong \mathbb{R}/R_K\mathbb{Z}$. ■

Example 4.1.9. Let us take $K = \mathbb{Q}(\sqrt{d})$ for some fundamental discriminant $d \in \mathbb{Z}_{<0}$. In this case, we have two complex field embeddings, which are conjugate to each other. Therefore, we have exactly one infinite place. We get that $(\prod_{\sigma\in\Sigma_K^\infty} \mathbb{R})^0 = \mathbb{R}^0 = \{0\}$. So, we obtain $T_K^0 = 0$. It follows that $\mathrm{Pic}_K^0 \cong \mathrm{Cl}_K$. ■

There is a shorter way to encode Arakelov divisors. Namely, any Arakelov divisor given by (37), can be mapped to

$$\left(\prod_{\mathfrak{p}\in\mathfrak{P}_K^0}\mathfrak{p}^{-n_\mathfrak{p}}, (e^{-x_\sigma})_{\sigma\in\Sigma_K^\infty}\right).$$

That is, the Arakelov divisor D is mapped to a pair (I,u), where I is a non-zero fractional ideal of $\mathcal{O}_K$ and $u\in\prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}_{>0}\subseteq K_\mathbb{R}$ (see Remark 1.8.4). Conversely, any such pair is mapped to an Arakelov divisor by

$$\left(\prod_{\mathfrak{p}\in\mathfrak{P}_K^0}\mathfrak{p}^{n_\mathfrak{p}}, (u_\sigma)_{\sigma\in\Sigma_K^\infty}\right)\mapsto\sum_{\mathfrak{p}\in\mathfrak{P}_K^0}(-n_\mathfrak{p})\mathfrak{p}+\sum_{\sigma\in\Sigma_K^\infty}(-\log(u_\sigma))\sigma. \tag{39}$$

It is not hard to see that these maps create a bijection. Because of this bijection, we interchange the notations freely.

Definition 4.1.10. Let $D\in\mathrm{Div}_K$. The notation (37) is called the *additive notation* of the Arakelov divisor D. The notation $D=(I,u)$ for some non-zero $I\in\mathrm{Id}_K$ and $u\in\prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}_{>0}$, is called the *multiplicative notation* of the Arakelov divisor D.

The group operation of the group $\mathrm{Div}_{K,S}$ in the multiplicative notation is given by

$$(I,u)+(J,v)=(IJ,uv),\qquad (I,u),(J,v)\in\mathrm{Div}_K\,.$$

The zero Arakelov divisor in the multiplicative notation is given by $(\mathcal{O}_K,(1)_{\sigma\in\Sigma_K^\infty})$. Any principal Arakelov divisor $\mathrm{div}_S(x)$ for some $x\in K^*$, is given by $(x^{-1}\mathcal{O}_K,(|x|_\sigma)_{\sigma\in\Sigma_K^\infty})$ in the multiplicative notation.

Remark 4.1.11. In [Sch08] the multiplicative notation is introduced in Chapter 4. However, a pair (I,u), where I is a non-zero fractional ideal of $\mathcal{O}_K$ and $u\in\prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}_{>0}\subseteq K_\mathbb{R}$, is called a *Hermitian line bundle*. In Section 5.2.2, we will introduce metrized S-line bundles, which have nothing to do with Hermitian line bundles. Therefore, to prevent confusion, we avoid the name of Hermitian line bundles. ♦

We can construct a set that is in bijection with the Arakelov class group.

Definition 4.1.12. An *ideal lattice* of K is a pair $(L,\langle\cdot,\cdot\rangle_L)$, where L is a projective $\mathcal{O}_K$-module of rank 1 and $\langle\cdot,\cdot\rangle_L$ is an inner product on the $\mathbb{R}$-vector space $L\otimes_\mathbb{Z}\mathbb{R}$ satisfying

$$\langle\alpha x,y\rangle_L=\langle x,\overline{\alpha}y\rangle_L,$$

for $x,y\in L\otimes_\mathbb{Z}\mathbb{R}$ and $\alpha\in K_\mathbb{R}$. Two ideal lattices $(L,\langle\cdot,\cdot\rangle_L),(L',\langle\cdot,\cdot\rangle_{L'})$ are called *isometric* if there exists an $\mathcal{O}_K$-module isomorphism $\varphi\colon L\mapsto L'$ such that

$$\langle x,y\rangle_L=\langle\psi(x),\psi(y)\rangle_{L'},\qquad x,y\in L\otimes_\mathbb{Z}\mathbb{R},$$

where $\psi\colon L\otimes_\mathbb{Z}\mathbb{R}\to L'\otimes_\mathbb{Z}\mathbb{R}$ is given by the tensor map $\varphi\otimes\mathrm{id}_\mathbb{R}$.

The notion of rank for a projective module might be unfamiliar. In Section 5.2.2, we introduce metrized S-line bundles, which can be seen as a generalization of ideal lattices. However, this section starts with a brief overview of the rank of projective modules. We refer to the first part of this section if one wants to understand this notion right now.

Remark 4.1.13. In Definition 4.1.12, we take an inner product on $\mathbb{R}$-vector space $L\otimes_\mathbb{Z}\mathbb{R}$. However, this is equivalent to taking an inner product on the $\mathbb{R}$-vector space $L\otimes_{\mathcal{O}_K}K_\mathbb{R}$. Namely,

$$L\otimes_\mathbb{Z}\mathbb{R}\cong(L\otimes_{\mathcal{O}_K}\mathcal{O}_K)\otimes_\mathbb{Z}\mathbb{R}\cong L\otimes_{\mathcal{O}_K}(\mathcal{O}_K\otimes_\mathbb{Z}\mathbb{R})\cong L\otimes_{\mathcal{O}_K}K_\mathbb{R}.$$ ♦

There is a natural way to associate an ideal lattice to an Arakelov divisor $D = (I, u)$. Namely, one can show that $u\Psi(I) \subseteq K_{\mathbb{R}}$ is a projective $\mathcal{O}_K$ module of rank 1, where Ψ denotes the Minkowski embedding (see Definition 1.8.3). We will prove this in a generalization in Section 5.2.2. Furthermore, we have $u\Psi(I) \otimes_{\mathcal{O}_K} K_{\mathbb{R}} \cong K_{\mathbb{R}}$ as $\mathcal{O}_K$-modules by Proposition 1.8.2. But this can also be seen as isomorphism of $K_{\mathbb{R}}$-modules. Therefore, the inner product $\langle \cdot, \cdot \rangle_{\mathbb{R}}$ from the Minkowski space $K_{\mathbb{R}}$, gives $u\Psi(I)$ the structure of an ideal lattice. Furthermore, in Theorem 1.8.6 we have seen that $\Psi(I)$ is a lattice in $K_{\mathbb{R}}$ with covolume $\operatorname{covol}(\Psi(I)) = N_{\mathcal{O}_K}(I)\sqrt{|d_K|_\infty}$. Since $u \in K_{\mathbb{R}}^*$, it follows by Lemma 3.4.5 that $u\Psi(I)$ is also a lattice in $K_{\mathbb{R}}$. Moreover, its covolume is given by

$$\operatorname{covol}(u\Psi(I)) = \left(\prod_{\sigma \in \Sigma_K^\infty} \|u_\sigma\|_\sigma \right) \operatorname{covol}(\Psi(I)) = \left(\prod_{\sigma \in \Sigma_K^\infty} \|u_\sigma\|_\sigma \right) N_{\mathcal{O}_K}(I)\sqrt{|d_K|_\infty}.$$

Proposition 4.1.14. Let K be a number field with discriminant d_K.

i.) The map that associates the ideal lattice $(u\Psi(I), \langle \cdot, \cdot \rangle_{\mathbb{R}})$ to an Arakelov divisor $D = (I, u)$ induces a bijection between Pic_K and the isometry classes of ideal lattices.

ii.) The map that associates the ideal lattice $(u\Psi(I), \langle \cdot, \cdot \rangle_{\mathbb{R}})$ to an Arakelov divisor $D = (I, u)$ induces a bijection between Pic_K^0 and the isometry classes of ideal lattices of covolume $\sqrt{|d_K|_\infty}$.

Proof. See the proof of [Sch08, Proposition 4.3]. □

4.2 Reduced Arakelov Divisors

In this section, we introduce minimal elements and reduced Arakelov divisors. They play a major role in the infrastructure description, which we will see in the next section. This section is based on Chapter 7 of [Sch08]. Throughout this section, let K be a number field.

Definition 4.2.1. Let $I \in \operatorname{Id}_K$. An element $x \in I$ is called *minimal* in I if it is non-zero and if the only element $y \in I$ for which $|y|_\sigma < |x|_\sigma$ for all $\sigma \in \Sigma_K^\infty$ is $y = 0$.

In Section 5.4, we will see a generalization of minimal elements. The existence of a minimal element in a fractional ideal is guaranteed from the fact that any fractional ideal of $\mathcal{O}_K$ forms a lattice in $K_{\mathbb{R}}$. In Proposition 5.4.4, one can find a proof of this for the generalization of minimal elements.

Lemma 4.2.2. Let $I \in \operatorname{Id}_K$. If $x \in I$ is minimal, then 1 is minimal in $x^{-1}I$.

Proof. One has $1 \in x^{-1}I$. So it remains to check whether it is minimal. Suppose that there exists $y \in x^{-1}I$ such that $|y|_\sigma < 1$ for all $\sigma \in \Sigma_K^\infty$. Then y can be written as $x^{-1}z$ for some $z \in I$. This implies that

$$|x^{-1}z|_\sigma < 1 \quad \Longrightarrow \ |x|_\sigma^{-1}|z|_\sigma < 1 \quad \Longrightarrow \ |z|_\sigma < |x|_\sigma,$$

for all $\sigma \in \Sigma_K^\infty$. By the minimality of $x \in I$, this implies that $z = 0$, and so $y = 0$. □

Consider the map $\pi \colon \operatorname{Id}_K \to \operatorname{Div}_K^0$ defined by

$$\pi(I) := \sum_{\mathfrak{p} \in \mathfrak{P}_K^0} (-\operatorname{ord}_{\mathfrak{p}}(I))\mathfrak{p} + \sum_{\sigma \in \Sigma_K^\infty} \left(\frac{1}{n} \log(N_{\mathcal{O}_K}(I)) \right) \sigma. \tag{40}$$

One can restrict the codomain of π to Div_K^0 because one can show that $\deg(\pi(I)) = 0$ for all $I \in \operatorname{Id}_K$. In terms of the multiplicative notation of Arakelov divisors, we have that $\pi(I) = (I, (N_{\mathcal{O}_K}(I)^{-1/n})_{\sigma \in \Sigma_K^\infty})$ for any $I \in \operatorname{Id}_K$. Note that for $I, J \in \operatorname{Id}_K$ we have $IJ \in \operatorname{Id}_K$ and

$$(IJ, (N_{\mathcal{O}_K}(IJ)^{-1/n})_{\sigma \in \Sigma_K^\infty}) = (I, (N_{\mathcal{O}_K}(I)^{-1/n})_{\sigma \in \Sigma_K^\infty}) + (J, (N_{\mathcal{O}_K}(J)^{-1/n})_{\sigma \in \Sigma_K^\infty}),$$

where we used that $N_{\mathcal{O}_K} \colon \operatorname{Id}_K \to \mathbb{Q}$ is a group homomorphism. Hence

$$\pi(IJ) = \pi(I) + \pi(J). \tag{41}$$

In other words, the map π is a group homomorphism.

Definition 4.2.3. An Arakelov divisor $D \in \mathrm{Div}_K$ is called *reduced* if it is of the form $D = \pi(I)$ for some $I \in \mathrm{Id}_K$ such that $1 \in I$ is minimal. The set of reduced Arakelov divisors is denoted by Red_K.

Since $\deg(\pi(I)) = 0$ for all $I \in \mathrm{Id}_K$, we have $\mathrm{Red}_K \subseteq \mathrm{Div}_K^0$. It can be shown that Red_K is a finite set. This result can be found in Proposition 7.2 in [Sch08], or a generalization of this result in Theorem 5.4.17 of this thesis.

Example 4.2.4. Note that the zero Arakelov divisor is given by $(\mathcal{O}_K, (1)_{\sigma \in \Sigma_K^\infty}) = \pi(\mathcal{O}_K)$. So the zero Arakelov divisor is reduced if $1 \in \mathcal{O}_K$ is minimal. Suppose that there exists a non-zero $a \in \mathcal{O}_K$ such that $|a|_\sigma < 1$ for all $\sigma \in \Sigma_K^\infty$. Then using Proposition 1.1.15 and 1.2.6 we have

$$N_{\mathcal{O}_K}(a\mathcal{O}_K) = |N_{K|\mathbb{Q}}(a)|_\infty = \left| \prod_{\sigma \in \Sigma_K^\infty} \sigma(a) \right|_\infty = \prod_{\sigma \in \Sigma_K^\infty} |a|_\sigma < 1.$$

This contradicts the fact that $N_{\mathcal{O}_K}(a\mathcal{O}_K) \in \mathbb{Z}_{>0}$. Consequently, the element $1 \in \mathcal{O}_K$ is minimal, and so the zero Arakelov divisor is reduced. ■

Similar to Algorithm 1.3.8, we would like to describe a reduction algorithm that given an Arakelov divisor in Div_K returns a reduced Arakelov divisor. Algorithm 1.3.8 returns an equivalent reduced integral ideal in Cl_K. Therefore, one could reason that the reduction algorithm in Div_K should return an equivalent reduced Arakelov divisor (see Definition 4.1.4). However, from the short exact sequence (38), we know that Pic_K has infinite order since T_K has infinite order. Thus, there are infinitely many equivalence classes in Pic_K. This means, since Red_K is finite, that we cannot always find a reduced Arakelov divisor equivalent to an arbitrary Arakelov divisor from Div_K. Therefore, we propose the following definition.

Definition 4.2.5. Two Arakelov divisors $D = (I, u)$ and $D' = (I', u')$ are called *ideal equivalent* if $[I] = [I']$ in Cl_K.

Remark 4.2.6. If Pic_K is equipped with the common topological structure, the definition of ideal equivalent Arakelov divisors coincides with lying on the same connected component of the topological space Pic_K. We do not discuss this any further at this point, but return to this once we introduce the topology on the Arakelov class group for the rings of S-integers in Section 5.3. More precisely, see Remark 5.3.9. ♦

Now, the number of equivalence classes of this equivalence relation equals $h_k < \infty$. Contrary to the earlier observation, we can find a reduced Arakelov divisor ideal equivalent to any Arakelov divisor $D \in \mathrm{Div}_K$.

Algorithm 4.2.7. (Reduction Algorithm for Arakelov Divisors)
Input: Any Arakelov Divisor D of K.
Output: A reduced Arakelov divisor D' such that D and D' are ideal equivalent.

i.) Find $I \in \mathrm{Id}_K$ and $u \in \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}_{>0}$ such that $D = (I, u)$.

ii.) If $1 \in I$ is minimal, then return $D' = \pi(I)$. Else find a minimal element $x \in I$.

iii.) Return $D' = \pi(x^{-1}I)$.

The correctness of this algorithm is an immediate consequence of Lemma 4.2.2. Notice that the element $x \in I$ in step (ii.) is not unique. Namely, there might exist more than one minimal element in I. Therefore, the algorithm is not deterministic. This means that given the same input, the output might differ. To find a minimal element, and check whether $1 \in I$ is minimal, one can use Algorithm 10.3 of [Sch08]. However, this algorithm takes divisors on Div_K^0, rather than Div_K. But this can probably be extended to Div_K. We will not do this here since we will describe an explicit reduction algorithm for real quadratic number fields in the next section. Often, it also suffices to only consider Arakelov divisors of degree zero. This can be seen in the next example.

Remark 4.2.8. If $K = \mathbb{Q}(\sqrt{d})$ for some fundamental discriminant $d \in \mathbb{Z}_{<0}$, we have that $\mathrm{Pic}_K^0 \cong \mathrm{Cl}_K$ (see Example 4.1.9). This means that Arakelov divisors are equivalent in Pic_K^0 if and only if they are ideal equivalent. Hence, using Algorithm 4.2.7, we can find a reduced Arakelov divisor equivalent to any Arakelov divisor in Pic_K^0. Contrary to Remark 1.3.9, there is no uniqueness statement about reduced Arakelov divisors in an equivalence class. This is made more precise in Example 9.3 in [Sch08]. ♦

4.3 Arakelov Theoretical Description of the Infrastructure

In Section 1.3, we have seen the infrastructure. The infrastructure yields an algorithm to compute the regulator of a real quadratic number field. [Sch08] gives in Chapter 8 a short description of the infrastructure using Arakelov theory. In this section, we work this out in more detail. Throughout this section, let K denote a real quadratic number field, i.e. $K = \mathbb{Q}(\sqrt{d})$ for some fundamental discriminant $d \in \mathbb{Z}_{>0}$. We use the same convention about these types of number fields as explained at the beginning of Section 1.3.

4.3.1 Reduction Algorithm for Arakelov Divisors in Real Quadratic Number Fields

To investigate the infrastructure using Arakelov theory, we first want to make Algorithm 4.2.7 more explicit and less non-deterministic. Therefore, we have to dive into some ideal theory.

It is known that any fractional ideal I of $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank 2 (see [Neu99, Proposition 2.10, Chapter I]). This means that $I = x\mathbb{Z} + y\mathbb{Z}$ for some $x, y \in I$. Recall Definition 1.1.2 of primitive elements in a fractional ideal.

Lemma 4.3.1. Let $I \in \mathrm{Id}_K$.

i.) An element $x \in I$ is primitive if and only if it is part of a $\mathbb{Z}$-basis.

ii.) The fractional ideal I contains a primitive element.

iii.) If $x \in I$ is primitive, then 1 is primitive in $x^{-1}I$.

iv.) If $x \in I$ is minimal, then x is primitive in I.

Proof. To show Statement (i.), let $x \in I$ be part of a $\mathbb{Z}$-basis. Say this $\mathbb{Z}$-basis is given by the elements $x, y \in I$. Suppose that there exists some $m \in \mathbb{Z}_{>1}$ such that $x \in mI$. Then $\frac{x}{m} \in I$. Since $I = x\mathbb{Z} + y\mathbb{Z}$, there exist $k, l \in \mathbb{Z}$ such that $\frac{x}{m} = kx + ly$. Since x, y form a basis of I, we can compare coefficients, i.e. $k = \frac{1}{m}$. Since k, m are integers, we must have $m = \pm 1$, reaching a contradiction with the choice of m. Therefore, the element $x \in I$ must be primitive. Conversely, let $x \in I$ be primitive. Since I is a free $\mathbb{Z}$-module of rank 2, there exist $y, z \in I$ such that $I = y\mathbb{Z} + z\mathbb{Z}$. Then there exist $k, l \in \mathbb{Z}$ such that $x = ky + lz$. If $\gcd(k, l) > 1$, then there exist $a \in \mathbb{Z}_{>1}$ and $b, c \in \mathbb{Z}$ such that $x = a(by + cz)$. Then $x \in aI$, contradicting the assumption that x is primitive. Therefore, we have $\gcd(k, l) = 1$. By Bezout's Identity, this means that there exist $a, b \in \mathbb{Z}$ such that $ak + bl = 1$. Consequently, one can verify that x and $-by + az$ are linearly independent and generate I. Consequently, they form a $\mathbb{Z}$-basis for I. Hence, the element $x \in I$ is part of a $\mathbb{Z}$-basis.

Statement (ii.) follows from Statement (i.) since a $\mathbb{Z}$-basis can always be found.

To show Statement (iii.), let $x \in I$ be primitive. Then by Statement (i.), we have that x is part of a $\mathbb{Z}$-basis. Let this $\mathbb{Z}$-basis be given by $x, y \in I$. Then

$$I = x\mathbb{Z} + y\mathbb{Z} \quad \Longrightarrow \; x^{-1}I = x^{-1}\left(x\mathbb{Z} + y\mathbb{Z}\right) = \mathbb{Z} + x^{-1}y\mathbb{Z}.$$

Hence, the element 1 is part of a $\mathbb{Z}$-basis of $x^{-1}I$. So by Statement (i.), we have that $1 \in x^{-1}I$ is primitive.

To show Statement (iv.), assume that there exists $m \in \mathbb{Z}_{>1}$ such that $x \in mI$. Then $\frac{x}{m} \in I$ is non-zero, and we have that $\left|\frac{x}{m}\right|_\infty < |x|_\infty$ and $\left|\sigma\left(\frac{x}{m}\right)\right|_\infty = \left|\frac{\sigma(x)}{m}\right|_\infty < |\sigma(x)|_\infty$. We reach a contradiction by the minimality of $x \in I$. Hence, the element x is primitive. □

Now, Section 2 in [Len82] states that any fractional ideal $\mathcal{O}_K$ can be written in a specific form.

Proposition 4.3.2. Let $I \in \mathrm{Id}_K$. Then I can be written as

$$I = \alpha \left(\mathbb{Z} + \left(\frac{b + \sqrt{d}}{2a} \right) \mathbb{Z} \right),$$

where $\alpha \in K^*$, $a, b \in \mathbb{Z}$ with $c = \frac{b^2 - d}{4a} \in \mathbb{Z}$ are such that $\gcd(a, b, c) = 1$, and $N_{K|\mathbb{Q}}(\alpha)/a \in \mathbb{Z}_{>0}$ which equals $N_{\mathcal{O}_K}(I)$.

In Proposition 1.3.4, we saw a representation for integral ideals of $\mathcal{O}_K$. The representation of Proposition 4.3.2 is for any fractional ideal of $\mathcal{O}_K$. For a given I, the element $\alpha \in K^*$ and the integers a, b inside the representation of Proposition 4.3.2 are not guaranteed to be unique. One can take α as any primitive element of I. Given I and α, the element a is uniquely determined due to the equality $a = \frac{N_{K|\mathbb{Q}}(\alpha)}{N_{\mathcal{O}_K}(I)}$. Moreover, the integer b is unique modulo $2a$. It is known how the representation changes when taking the product of fractional ideals.

Proposition 4.3.3. Let $I_i \in \mathrm{Id}_K$ for $i = 1, 2$. Write

$$I_i = \alpha_i \left(\mathbb{Z} + \left(\frac{b_i + \sqrt{d}}{2a_i} \right) \mathbb{Z} \right),$$

where $\alpha_i \in K^*$ and $a_i, b_i \in \mathbb{Z}$ with $c_i = \frac{b_i^2 - d}{4a_i} \in \mathbb{Z}$ are such that $\gcd(a_i, b_i, c_i) = 1$. Then

$$I_1 I_2 = \alpha \left(\mathbb{Z} + \left(\frac{b + \sqrt{d}}{2a} \right) \mathbb{Z} \right),$$

where $t = \gcd(a_1, a_2, \frac{1}{2}(b_1 + b_2))$, $\alpha = \frac{\alpha_1 \alpha_2}{t}$, $a = \frac{a_1 a_2}{t^2}$, and if $k, l, m \in \mathbb{Z}$ are such that

$$t = k a_1 + l a_2 + \frac{m}{2}(b_1 + b_2),$$

then

$$b \equiv \frac{1}{t} \left(k a_1 b_2 + l a_2 b_1 + \frac{m}{2}(b_1 b_2 + d) \right) \bmod 2a.$$

For a proof of this result, we refer to Section 2 in [Len82].

Suppose that 1 is primitive in I. Then in the representation of Proposition 4.3.2, we can take $\alpha = 1$. In this case, we have $a = N_{\mathcal{O}_K}(I^{-1})$. Since the norm of a fractional ideal is strictly positive, we have $a \in \mathbb{Z}_{>0}$. Thereafter, we can take b uniquely in the interval

$$\mathcal{A}_a := \begin{cases} \{t \in \mathbb{R} : -a \leq t \leq a\}, & \text{if } a \geq \sqrt{d}, \\ \{t \in \mathbb{R} : \sqrt{d} - 2a \leq t \leq \sqrt{d}\}, & \text{if } a < \sqrt{d}. \end{cases} \tag{42}$$

It follows that the integers a, b, c are uniquely determined. We set $x_{(I,1)} := \frac{b + \sqrt{d}}{2a}$ with these choices. So when 1 is a primitive element of I, the element $x_{(I,1)}$ forms a $\mathbb{Z}$-basis with 1.

Proposition 4.3.4. Let $I \in \mathrm{Id}_K$ such that $1 \in I$ is primitive. Write $x_{(I,1)} = \frac{b + \sqrt{d}}{2a}$, where $a = N_{\mathcal{O}_K}(I^{-1})$ and $b \in \mathcal{A}_a$. Then the following statements are equivalent.

i.) The Arakelov divisor $\pi(I)$ is reduced.

ii.) The element 1 in I is minimal.

iii.) $-1 < \sigma\left(x_{(I,1)}\right) < 0$ and $x_{(I,1)} > 1$.

iv.) $|\sqrt{d} - 2a|_\infty < b < \sqrt{d}$.

Proof. Definition 4.2.3 implies that Statement (i.) and (ii.) are equivalent.

Set $x := x_{(I,1)}$ and assume that $1 \in I$ is minimal. Then $\pi(I)$ is reduced. Hence, by Proposition 7.2 in [Sch08], we have that $N_{\mathcal{O}_K}(I^{-1}) < \sqrt{d}$. So we have $a < \sqrt{d}$, which means that $b \in [\sqrt{d} - 2a, \sqrt{d}]$. Since a, b are integers and $\sqrt{d}$ is non-rational, the integer b cannot equal the bounds of this interval. Equivalently, we have

$$\sqrt{d} - 2a < b < \sqrt{d} \quad \Longrightarrow \; -2a < b - \sqrt{d} < 0 \quad \Longrightarrow \; -1 < \frac{b - \sqrt{d}}{2a} < 0.$$

Then these inequalities say that $-1 < \sigma(x) < 0$. If $x = 0$, then $b = -\sqrt{d}$. This leads to a contradiction as b is an integer. Hence, the element $x \in I$ is non-zero and satisfies $|\sigma(x)|_\infty < 1$. By the minimality of $1 \in I$, this means that we have $|x|_\infty > 1$. Furthermore, we can write $\sigma(x) = x - \frac{\sqrt{d}}{a}$. This implies that $\sigma(x) < x$. Therefore, the element x cannot be smaller than -1, so we must have $x > 1$. This shows that Statement (ii.) implies Statement (iii.).

Conversely, assume that $-1 < \sigma(x) < 0$ and $x > 1$. Suppose that there exists some non-zero $y \in I$ such that $|y|_\infty < 1$ and $|\sigma(y)|_\infty < 1$. Since $y \in I = \mathbb{Z} + x\mathbb{Z}$, there exist $k, l \in \mathbb{Z}$ such that $y = k + lx$. Then the conditions say that

$$|k + lx|_\infty < 1, \qquad |k + l\sigma(x)|_\infty < 1.$$

Suppose that $k = 0$, then $y = lx$. But there is no non-zero integer l such that $|lx|_\infty < 1$, since $x > 1$. So we can assume k to be non-zero. Suppose now that $k > 0$, then the first condition holds only if $lx \leq 0$. Since $x > 1$, this precisely says that $l \leq 0$. The second condition holds only if $l\sigma(x) \leq 0$. Since $\sigma(x) < 0$, this precisely says that $l \geq 0$. We conclude that $l = 0$. Suppose now that $k < 0$. Then the first condition holds only if $lx \geq 0$. Since $x > 1$, this precisely says that $l \geq 0$. The second condition holds only if $l\sigma(x) \geq 0$. Since $\sigma(x) < 0$, this precisely says that $l \leq 0$. We see that $l = 0$. So from both cases, we get that $l = 0$. This means that $y = k \in \mathbb{Z}$. But there is no non-zero integer such that $|k|_\infty < 1$. We conclude that such $y \in I$ cannot exist. Consequently, the element 1 is minimal in I. This shows that Statement (iii.) implies Statement (ii.).

One has

$$-1 < \sigma(x) < 0 \quad \Longleftrightarrow \quad -1 < \frac{b - \sqrt{d}}{2a} < 0 \quad \Longleftrightarrow \quad \sqrt{d} - 2a < b < \sqrt{d}.$$

Moreover, we have

$$x > 1 \quad \Longleftrightarrow \quad \frac{b + \sqrt{d}}{2a} > 1 \quad \Longleftrightarrow \quad b > 2a - \sqrt{d}.$$

Combining these results, we see that

$$-1 < \sigma(x) < 0, \;\; x > 1 \quad \Longleftrightarrow \quad |\sqrt{d} - 2a|_\infty < b < \sqrt{d}.$$

Hence, Statement (iii.) and Statement (iv.) are equivalent. □

Remark 4.3.5. We want to show the relation between Lenstra's work in [Len82] and the Arakelov theoretical setting. Therefore, we have to introduce quadratic forms.

Definition 4.3.6. A *(primitive integral binary) quadratic form* of discriminant d is a polynomial

$$aX^2 + bXY + cY^2 \in \mathbb{Z}[X, Y]$$

such that $\gcd(a, b, c) = 1$ and $b^2 - 4ac = d$. A quadratic form of discriminant d is denoted by (a, b, c), and the set of quadratic forms of discriminant d by $\mathcal{F}_d$.

Now, using the representation from Proposition 4.3.2, we can construct a map $f\colon \mathrm{Id}_K \to \mathcal{F}_d$. Namely, say we have $I \in \mathrm{Id}_K$ represented as

$$I = \alpha\left(\mathbb{Z} + \left(\frac{b+\sqrt{d}}{2a}\right)\mathbb{Z}\right),$$

where $\alpha \in K^*$ and $a, b \in \mathbb{Z}$ with $c = \frac{b^2-d}{4a} \in \mathbb{Z}$ are such that $\gcd(a,b,c) = 1$. Then we set

$$f(I) := (a,b,c).$$

Note that this map is not injective since the mapping is independent of $\alpha \in K^*$. However, the map f induces a bijection $\mathrm{Cl}_K \cong \mathcal{F}_d/\operatorname{SL}_2(\mathbb{Z})$, where the last set is given by the orbits induced by the group action of $\operatorname{SL}_2(\mathbb{Z})$ on $\mathcal{F}_d$ given by

$$\begin{pmatrix} u & v \\ s & t \end{pmatrix} \cdot (a,b,c) = (au^2 + bus + cs^2, 2auv + but + bvs + 2cst, av^2 + bvt + ct^2),$$

for $\begin{pmatrix} u & v \\ s & t \end{pmatrix} \in SL_2(\mathbb{Z}), (a,b,c) \in \mathcal{F}_d$.

Definition 4.3.7. A quadratic form $(a,b,c) \in \mathcal{F}_d$ is *reduced* if $|\sqrt{d} - 2|a|_\infty|_\infty < b < \sqrt{d}$.

Given a reduced quadratic form $(a,b,c) \in \mathcal{F}_d$, we also have the reduced quadratic form $(-a,b,-c)$. If $a = 0$, then we would need that $b^2 = d$, contradicting the fact that d is square-free. Hence, the reduced quadratic forms of discriminant d can be split into two sets of equal size. One set such that $a \in \mathbb{Z}_{>0}$ and one set such that $a \in \mathbb{Z}_{<0}$. Proposition 4.3.4 implies that Red_K is in bijection with the reduced quadratic forms of discriminant d with $a \in \mathbb{Z}_{>0}$. We conclude that the Arakelov theoretical setting is closely related to the work of Lenstra. This was also stated in Example 8.2 in [Sch08].

For the rest of this chapter, we will not deal with Lenstra's work and focus on the Arakelov theoretical setting. But, many aspects of his work will show up as these settings are closely related. This relation also gave us the ideas to translate the reduction algorithm described in [Len82, Section 4] to the Arakelov setting. Moreover, for the proof of Theorem 4.3.9 we were inspired by the proof of Theorem 4.1 in [Lag80]. However, all proofs in this chapter are self-written. ♦

Now, we describe a reduction algorithm that is a little bit more explicit than Algorithm 4.2.7. This algorithm is still non-deterministic. However, rather than depending on the choice of minimal element, it depends on the choice of primitive element. It turns out that this is easier to control.

Algorithm 4.3.8. (Reduction Algorithm for Arakelov Divisors in Real Quadratic Number Fields)
Input: Any Arakelov Divisor D of K.
Output: A reduced Arakelov divisor D' such that D and D' are ideal equivalent.

i.) Find $I \in \mathrm{Id}_K$ and $u \in \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}_{>0}$ such that $D = (I,u)$.

ii.) Find a primitive element $\alpha \in I$.

iii.) If $\alpha = 1$, set $I' := I$. Else, set $I' := \alpha^{-1}I$.

iv.) If $1 \in I'$ is minimal, then return $D' = \pi(I')$. Else, set $I_0 := I'$.

v.) Set $i = 0$.

vi.) Set $i = i + 1$ and compute $I_i = x_{(I_{i-1},1)}^{-1} I_{i-1}$.

vii.) If $1 \in I_i$ is minimal, then return $D' = \pi(I_i)$. Else, return to step (vi.).

Theorem 4.3.9. Algorithm 4.3.8 is correct and terminates in a finite number of steps.

Proof. If the Arakelov divisor is given in the multiplicative notation, step (i.) can be skipped. If the Arakelov divisor is given in the additive notation, one can use bijection (39) to complete step (i.). Either way, one will end up with I given in its unique factorization of non-zero prime ideals of $\mathcal{O}_K$. Then we can find the representation of Proposition 4.3.2 for I. This can be done by finding the representation for the prime ideals in the factorization of I, followed by Proposition 4.3.32. For the representation of the prime ideals, one can always take the norm of the prime ideal as the primitive element. We obtain a $\mathbb{Z}$-basis of I in this way. Then Lemma (4.3.1) (i.) states that we found a primitive element. Hence step (ii.) is solvable in a finite number of steps.

In step (iii.), we create a fractional ideal I' such that $1 \in I'$ is primitive. Namely, either $1 \in I$ is primitive, or we make it primitive by dividing the fractional ideal I by α. The latter is true by Lemma 4.3.1 (iii.). Now, using the equivalent statements of Proposition 4.3.4, one can verify whether $1 \in I'$ is minimal. If so, then $\pi(I')$ is reduced and ideal equivalent to $D = (I, u)$ since $I' = I$ or $I' = \alpha^{-1}I$. Hence, the correctness of step (iv.) follows. Otherwise, the element $1 \in I' = I_0$ is just primitive and not minimal. So we divide by $x_{(I_0,1)}$ to create a new fractional ideal I_1 for which $1 \in I_1$ is primitive. We can again check whether this is minimal using the equivalent statements of Proposition 4.3.4. If so, we can return $\pi(I_1)$ since this is reduced and ideal equivalent to $D = (I, u)$. It is ideal equivalent to I since we only divided I by elements of K to obtain I_1. If not, we proceed by dividing by $x_{(I_1,1)}$.

It remains to show that in the sequence $(I_i)_{i\geq 0}$ of fractional ideals, there exists some $j \in \mathbb{Z}_{\geq 0}$ such that $1 \in I_j$ is minimal. This will show that the algorithm is correct and terminates in a finite number of steps. We will show this now. Set $x_i := x_{(I_i,1)}$ for all $i \in \mathbb{Z}_{\geq 0}$. By construction of the element $x_{(I_i,1)}$ in I_i, we have

$$I_i = \mathbb{Z} + x_i\mathbb{Z}, \qquad x_i = \frac{b_i + \sqrt{d}}{2a_i},$$

where $a_i = N_{\mathcal{O}_K}(I_i^{-1})$ and $b_i \in \mathcal{A}_{a_i}$ are integers. Furthermore, we have the relation $c_i := \frac{b_i^2 - d}{4a_i}$ such that $\gcd(a_i, b_i, c_i) = 1$. We claim that $a_{i+1} = |c_i|_\infty$ and $b_{i+1} \equiv -b_i \bmod 2a_{i+1}$ for all $i \in \mathbb{Z}_{\geq 0}$. This can be seen as follows. Note that we have

$$N_{K|\mathbb{Q}}(x_i) = x_i\sigma(x_i) = \left(\frac{b_i + \sqrt{d}}{2a_i}\right)\left(\frac{b_i - \sqrt{d}}{2a_i}\right) = \frac{b_i^2 - d}{4a_i^2} = \frac{c_i}{a_i}.$$

Now

$$a_{i+1} = N_{\mathcal{O}_K}(I_{i+1}^{-1}) = N_{\mathcal{O}_K}(x_i I_i^{-1}) = N_{\mathcal{O}_K}(x_i\mathcal{O}_K)N_{\mathcal{O}_K}(I_i^{-1}) = |N_{K|\mathbb{Q}}(x_i)|_\infty a_i = |c_i|_\infty,$$

where we used that $N_{\mathcal{O}_K}$ is a group homomorphism and Proposition 1.2.6. Next, we have

$$x_i^{-1} = \frac{2a_i}{b_i + \sqrt{d}} = \frac{2a_i(b_i - \sqrt{d})}{(b_i + \sqrt{d})(b_i - \sqrt{d})} = \frac{2a_i(b_i - \sqrt{d})}{b_i^2 - d} = \frac{b_i - \sqrt{d}}{2c_i}.$$

So

$$I_{i+1} = x_i^{-1}I_i = x_i^{-1}(\mathbb{Z} + x_i\mathbb{Z}) = \mathbb{Z} + x_i^{-1}\mathbb{Z} = \mathbb{Z} + \left(\frac{b_i - \sqrt{d}}{2c_i}\right)\mathbb{Z}.$$

By multiplying by $\pm 1 \in \mathbb{Z}^*$, we get

$$I_{i+1} = \mathbb{Z} + \left(\frac{-b_i + \sqrt{d}}{2|c_i|_\infty}\right)\mathbb{Z} = \mathbb{Z} + \left(\frac{-b_i + \sqrt{d}}{2a_{i+1}}\right)\mathbb{Z},$$

where we used that $a_{i+1} = |c_i|_\infty$. On the other hand, we have

$$I_{i+1} = \mathbb{Z} + x_{i+1}\mathbb{Z} = \mathbb{Z} + \left(\frac{b_{i+1} + \sqrt{d}}{2a_{i+1}}\right)\mathbb{Z}.$$

The representation of Proposition 4.3.2 tells us that the b_i and b_{i+1} are uniquely determined modulo $2a_{i+1}$. So we have $b_{i+1} \equiv -b_i \bmod 2a_{i+1}$. Hence, the claim follows.

If $|c_i|_\infty \geq \sqrt{d}$, then we claim that $|c_{i+1}|_\infty \leq \frac{|c_i|_\infty}{4}$. Namely, we have $b_{i+1} \in \mathcal{A}_{a_{i+1}} = \mathcal{A}_{|c_i|_\infty}$, and so $b_{i+1} \leq |c_i|_\infty$. We obtain that $0 \leq b_{i+1}^2 \leq c_i^2$ and $0 < d \leq c_i^2$. Consequently, the value of $|b_{i+1}^2 - d|_\infty$ is less than c_i^2. So

$$|c_{i+1}|_\infty = \frac{|b_{i+1}^2 - d|_\infty}{|4a_{i+1}|_\infty} \leq \frac{c_i^2}{|4c_i|_\infty} = \frac{|c_i|_\infty}{4}.$$

So after finitely many iterations, we will end up with $|c_j|_\infty \leq \sqrt{d}$ for some $j \in \mathbb{Z}_{\geq 0}$. Suppose that $|c_j|_\infty \leq |c_{j+1}|_\infty$. Then we have

$$4|c_j|_\infty^2 < 4|c_{j+1}|_\infty |c_j|_\infty = 4\left|\frac{b_{j+1}^2 - d}{4a_{j+1}}\right|_\infty |c_j|_\infty = \left|\frac{b_{j+1}^2 - d}{c_j}\right|_\infty |c_j|_\infty = |b_{j+1}^2 - d|_\infty.$$

We know that $b_{j+1} \in \mathcal{A}_{a_{j+1}} = \mathcal{A}_{|c_j|_\infty}$. Since $|c_j|_\infty \leq \sqrt{d}$, we have $b_{j+1} \in [\sqrt{d} - 2|c_j|_\infty, \sqrt{d}]$. We see that $0 \leq b_{j+1}^2 \leq d$, and so $|b_{j+1}^2 - d|_\infty = d - b_{j+1}^2 \leq d$. Thus, we get

$$4|c_j|_\infty^2 < d \quad \Longrightarrow\ 2|c_j|_\infty < \sqrt{d}. \tag{43}$$

This implies that $b_{j+1} \geq \sqrt{d} - 2|c_j|_\infty > 0$. Therefore

$$2a_{j+1} = 2|c_j|_\infty < \sqrt{d} < \sqrt{d} + b_{j+1} \quad \Longrightarrow\ 2a_{j+1} - \sqrt{d} < b_{j+1}.$$

Hence, since $b_{j+1} \in [\sqrt{d} - 2a_{i+1}, \sqrt{d}]$, we get

$$|\sqrt{d} - 2a_{j+1}|_\infty < b_{j+1} < \sqrt{d}.$$

In this case, set $m := j + 1$. On the other hand, if $|c_{j+1}|_\infty < |c_j|_\infty$, then we have $|c_{j+1}|_\infty < \sqrt{d}$. Since $b_{j+2} \in \mathcal{A}_{a_{j+2}} = \mathcal{A}_{|c_{j+1}|_\infty}$, we get $b_{j+2} \in [\sqrt{d} - 2|c_{j+1}|_\infty, \sqrt{d}]$. Furthermore

$$4|c_{j+1}|_\infty^2 < 4|c_{j+1}|_\infty |c_j|_\infty = 4\left|\frac{b_{j+1}^2 - d}{4a_{j+1}}\right|_\infty |c_j|_\infty = \left|\frac{b_{j+1}^2 - d}{c_j}\right|_\infty |c_j|_\infty = |b_{j+1}^2 - d|_\infty \leq d.$$

Then

$$4|c_{j+1}|_\infty^2 < d \quad \Longrightarrow\ 2|c_{j+1}|_\infty < \sqrt{d}.$$

Now, repeat the argument starting from Equation (43), by replacing j by $j+1$. Consequently, we obtain that

$$|\sqrt{d} - 2a_{j+2}|_\infty < b_{j+2} < \sqrt{d}.$$

In this case, set $m := j + 2$. From case distinction, we obtain

$$|\sqrt{d} - 2a_m|_\infty < b_m < \sqrt{d}$$

for some $m \in \mathbb{Z}_{\geq 0}$. Proposition 4.3.4 tells us that this is equivalent to saying that 1 is minimal in $I_m = \mathbb{Z} + x_m\mathbb{Z}$. □

Remark 4.3.10. Notice that the element $\alpha \in I$ in step (ii.) is not unique. Namely, there might exist more than one primitive element in I. Therefore, the algorithm is not deterministic. ♦

Remark 4.3.11. Given an Arakelov divisor $D = (I, u)$, the Algorithm 4.3.8 returns a reduced Arakelov divisor $D' = \pi(J)$ such that D and D' are ideal equivalent. This means that there exists some $x \in K^*$ such that $J = xI$. Analyzing the proof of Theorem 4.3.9, we have constructed such x. Namely, with the same notation as in the proof, we have $J = (\alpha \prod_{i=0}^{m-1} x_i)^{-1} I$. The element $\prod_{i=0}^{m-1} x_i$ is uniquely determined from D and α. So, we set $x_D^{\alpha} := \prod_{i=0}^{m-1} x_i$. Then we can say that $J = (\alpha x_D^{\alpha})^{-1} I$. ♦

4.3.2 The Infrastructure Operator and Arakelov Cycles

In Section 1.3, we saw that a crucial step was to apply the ideas of the reduction algorithm to integral ideals that were already reduced (see Equation (6)). By doing this inductively, we obtained a complete set of reduced integral ideals that are equivalent. We called such a set a cycle (see Definition 1.3.10). We would like to get this situation in the Arakelov theoretical setting.

Let $\mathrm{Red}_K^1 \subseteq \mathrm{Div}_K$ denote all Arakelov divisors of the form $\pi(I)$, where $I \in \mathrm{Id}_K$ such that $1 \in I$ is primitive.

Definition 4.3.12. The operator $\rho\colon \mathrm{Red}_K^1 \to \mathrm{Red}_K^1$ defined by $\pi(I) \mapsto \pi\left(x_{(I,1)}^{-1} I\right)$ is called the *infrastructure operator* of K.

If $1 \in I$ is minimal, then by Lemma 4.3.1 (iv.), it is also primitive. Therefore, we have $\mathrm{Red}_K \subseteq \mathrm{Red}_K^1$.

Proposition 4.3.13. Let $\pi(I) \in \mathrm{Red}_K$, then we have $\rho(\pi(I)) \in \mathrm{Red}_K$.

Proof. Since $\pi(I) \in \mathrm{Red}_K$, we know that $1 \in I$ is minimal. Set $x := x_{(I,1)}$. We claim that x is also minimal in I. By Lemma 4.2.2, this would mean that 1 is minimal in $x^{-1}I$. Consequently, we have $\rho(\pi(I)) = \pi(x^{-1}I) \in \mathrm{Red}_K$. So it remains to show the claim.

Since $1 \in I$ is minimal, Proposition 4.3.4 tells us that $-1 < \sigma(x) < 0$ and $x > 1$. Suppose now that there exists some non-zero $y \in I$ such that $|y|_\infty < |x|_\infty$ and $|\sigma(y)|_\infty < |\sigma(x)|_\infty$. Since $y \in I = \mathbb{Z} + x\mathbb{Z}$, there exist $k, l \in \mathbb{Z}$ such that $y = k + lx$. Then the conditions say that

$$|k + lx|_\infty < |x|_\infty = x, \qquad |k + l\sigma(x)|_\infty < |\sigma(x)|_\infty,$$

where we used in the first condition that $x > 1$. Suppose that $l > 0$. Since $x > 1$, we have that $lx \geq x > 0$. Then the first condition holds only if $k < 0$. Since $\sigma(x) < 0$, we have $l\sigma(x) \leq \sigma(x) < 0$. Thus, the second condition holds only if $k > 0$, reaching a contradiction, and so $l \notin \mathbb{Z}_{>0}$. Suppose that $l < 0$. Since $x > 1$, we have that $lx \leq -x < 0$. Hence, the first condition holds only if $k > 0$. Since $\sigma(x) < 0$, we have $l\sigma(x) \geq -\sigma(x) > 0$. Therefore, the second condition holds only if $k < 0$, reaching a contradiction, and so $l \notin \mathbb{Z}_{<0}$. So we have that $l = 0$ and $y = k \in \mathbb{Z}$. But there is no non-zero integer such that $|k|_\infty < |\sigma(x)|_\infty < 1$ (looking at the second condition). We may conclude that such $y \in I$ cannot exist. This says that x is minimal in I. □

Proposition 4.3.4 tells us that if $1 \in I$ is minimal, then the element $x_{(I,1)}$ forms a $\mathbb{Z}$-basis with 1 and satisfies $-1 < \sigma\left(x_{(I,1)}\right) < 0$ and $x_{(I,1)} > 1$. While the choice of $x_{(I,1)}$ is unique, we never claimed that it is the unique element with these properties. However, it turns out to be true. Moreover, we can also find the 'opposite' of $x_{(I,1)}$.

Lemma 4.3.14. Let $I \in \mathrm{Id}_K$ such that $1 \in I$ is minimal. Then $x_{(I,1)}$ is the unique element of I satisfying $x_{(I,1)} > 1$ and $-1 < \sigma\left(x_{(I,1)}\right) < 0$ such that $1, x_{(I,1)}$ form a $\mathbb{Z}$-basis for I. Furthermore, there exists a unique element y in I satisfying $\sigma(y) < -1$ and $0 < y < 1$ such that $1, y$ form a $\mathbb{Z}$-basis for I. We denote this unique element y by $y_{(I,1)}$. Moreover, the element $y_{(I,1)}$ is minimal.

Proof. Let x, x' be two elements of I satisfying $x, x' > 1$ and $-1 < \sigma(x), \sigma(x') < 0$ such that $1, x$ and $1, x'$ form a $\mathbb{Z}$-basis for I. There exist $j, k, l, m \in \mathbb{Z}$ such that $x = j + kx'$, and $x' = l + mx$. Substitution gives

$$x = j + k(l + mx) = (j + kl) + kmx.$$

Since $1, x$ form a basis of I, we can compare coefficients, implying $km = 1$. Since k, m are integers, we must have $k = m = \pm 1$. Say $k = m = 1$, then we have

$$x = j + x' \implies \sigma(x) = j + \sigma(x').$$

Then

$$-1 < \sigma(x') < 0 \implies -1 + j < \sigma(x) < j.$$

If $j < 0$, we have $\sigma(x) < j \leq -1$, reaching a contradiction. If $j > 0$, we have $0 \leq -1 + j < \sigma(x)$, reaching a contradiction. Hence, we have that $j = 0$, i.e. $x = x'$. So if $k = m = 1$, we have uniqueness. Say $k = m = -1$, then we have

$$x = j - x' \implies \sigma(x) = j - \sigma(x').$$

Then

$$-1 < \sigma(x') < 0 \implies 0 < -\sigma(x') < 1 \implies j < \sigma(x) < j + 1.$$

If $j \geq 0$, we have $\sigma(x) > j \geq 0$, reaching a contradiction. If $j < 0$, then

$$x' > 1 \implies -x' < -1 \implies x < -1 + j < -1,$$

reaching a contradiction. So if $k = m = -1$, it is impossible to have two such elements. By covering all cases, we have shown uniqueness.

Now, let us look at the existence of $y_{(I,1)}$. Since $1 \in I$ is minimal, we know by Lemma 4.3.1 (iv.) that it is also primitive. So using the representation of Proposition 4.3.2, we can write

$$I = \mathbb{Z} + \frac{b + \sqrt{d}}{2a}\mathbb{Z},$$

where $a = N_{\mathcal{O}_K}(I^{-1})$, and b is uniquely determined modulo $2a$. So we can take b uniquely in the interval $[-\sqrt{d}, 2a - \sqrt{d}]$. Since a, b are integers and $\sqrt{d}$ is non-rational, the integer b cannot equal the bounds of this interval. Equivalently, we have

$$-\sqrt{d} < b < 2a - \sqrt{d} \implies 0 < b + \sqrt{d} < 2a \implies 0 < \frac{b + \sqrt{d}}{2a} < 1.$$

So set $y_{(I,1)} := \frac{b+\sqrt{d}}{2a}$. Then these inequalities say that $0 < y_{(I,1)} < 1$. Therefore, the element $y_{(I,1)} \in I$ is non-zero and satisfies $|y_{(I,1)}|_\infty < 1$. Minimality of $1 \in I$ implies that $|\sigma(y_{(I,1)})| > 1$. Furthermore, we can write $\sigma(y_{(I,1)}) = y_{(I,1)} - \frac{\sqrt{d}}{a}$, and so $\sigma(y_{(I,1)}) < y_{(I,1)}$. Therefore, the element $\sigma(y_{(I,1)})$ cannot be bigger than 1. So we have that $\sigma(y_{(I,1)}) < -1$. Thus, this choice of $y_{(I,1)}$ satisfies $\sigma(y_{(I,1)}) < -1$, $0 < y_{(I,1)} < 1$ and forms a $\mathbb{Z}$-basis with 1.

The proof that $y_{(I,1)}$ is the unique element with the claimed properties, is similar to the uniqueness proof of $x_{(I,1)}$ that we saw at the beginning of this proof. Likewise, the fact that $y_{(I,1)}$ is minimal in I is similar to the proof that $x_{(I,1)}$ is minimal in Proposition 4.3.13. □

In what follows, the bounds on $x_{(I,1)}$ and $y_{(I,1)}$ will be used a lot. We will use them without reference.

Proposition 4.3.13 implies that the infrastructure operator induces a map $\rho\colon \mathrm{Red}_K \to \mathrm{Red}_K$.

Proposition 4.3.15. The infrastructure operator ρ is a bijection on Red_K.

Proof. We will prove this by constructing an inverse of $\rho\colon \mathrm{Red}_K \to \mathrm{Red}_K$. Take $\pi(I) \in \mathrm{Red}_K$. Then $1 \in I$ is minimal. By Lemma 4.3.14 it follows that $y_{(I,1)}$ is also minimal in I. By Lemma 4.2.2, this means that 1 is minimal in $y_{(I,1)}^{-1}I$. Consequently, we have $\pi(y_{(I,1)}^{-1}I) \in \mathrm{Red}_K$. So consider the map $\rho' : \mathrm{Red}_K \to \mathrm{Red}_K$ defined by $\pi(I) \mapsto \pi(y_{(I,1)}^{-1}I)$. We now show that the map ρ' is the inverse of ρ. Namely, take any $\pi(I) \in \mathrm{Red}_K$. Then $1 \in I$ is minimal, and set $x := x_{(I,1)}$. Since $-1 < \sigma(x) < 0$ and $x > 1$, we have $\sigma(x^{-1}) < -1$ and $0 < x^{-1} < 1$. Furthermore, we have

$$I = \mathbb{Z} + x\mathbb{Z} \quad \implies x^{-1}I = x^{-1}(\mathbb{Z} + x\mathbb{Z}) = \mathbb{Z} + x^{-1}\mathbb{Z}.$$

By Lemma 4.3.14, we have seen that $y := y_{(x^{-1}I,1)}$ is the unique element of $x^{-1}I$ satisfying $\sigma(y) < -1$ and $0 < y < 1$ such that $1, y$ form a $\mathbb{Z}$-basis for $x^{-1}I$. We obtain that $y = x^{-1}$. So then

$$\rho'(\rho(\pi(I))) = \rho^{-1}(\pi(x^{-1}I)) = \pi\left(y^{-1}(x^{-1}I)\right) = \pi(I).$$

Since Red_K is a finite set, we have that ρ and ρ' are each other's inverses. In particular, the infrastructure operator $\rho\colon \mathrm{Red}_K \to \mathrm{Red}_K$ is a bijection. □

Now that we have investigated the infrastructure operator, we are interested to see what happens if we apply it inductively. Take any $\pi(I) \in \mathrm{Red}_K$. We can apply ρ inductively and have $\rho^k(\pi(I)) \in \mathrm{Red}_K$ for all $k \in \mathbb{Z}_{\geq 0}$. We use the convention that $\rho^0 = \mathrm{id}_{\mathrm{Red}_K}$. Set $\xi_0 := x_{(I,1)}$ and $I_0 := I$. Define recursively the fractional ideals and elements

$$I_i := \xi_{i-1}^{-1} I_{i-1}, \qquad \xi_i := x_{(I_i,1)},$$

for $i \in \mathbb{Z}_{>0}$. We obtain $\rho(\pi(I_{k-1})) = \pi(I_k)$ or more generally $\rho^k(\pi(I_0)) = \pi(I_k)$ for any $k \in \mathbb{Z}_{\geq 0}$. Furthermore, set $\theta_0 := 1$ and for $i \in \mathbb{Z}_{>0}$ define the element

$$\theta_i := \prod_{j=0}^{i-1} \xi_j.$$

Then we have

$$I_i = \xi_{i-1}^{-1} I_{i-1} = \xi_{i-1}^{-1}\xi_{i-2}^{-1} I_{i-2} = \ldots = \left(\prod_{j=0}^{i-1} \xi_j^{-1}\right) I_0 = \theta_i^{-1} I_0.$$

Then for any $k \in \mathbb{Z}_{\geq 0}$, we have the relation

$$\rho^k(\pi(I_0)) = \pi(I_k) = \pi(\theta_k^{-1} I). \tag{44}$$

We have $I_k = \mathbb{Z} + \xi_k\mathbb{Z}$ for any $k \in \mathbb{Z}_{k\geq 0}$. So

$$I = I_0 = \theta_k I_k = \theta_k(\mathbb{Z} + \xi_k\mathbb{Z}) = \theta_k\mathbb{Z} + \theta_{k+1}\mathbb{Z}. \tag{45}$$

As a result of this, we can say that θ_k, θ_{k+1} form a $\mathbb{Z}$-basis for I for all $k \in \mathbb{Z}_{\geq 0}$. Note that the sequence $(\theta_i)_{i\geq 0}$ is uniquely determined from the reduced Arakelov divisor $\pi(I)$.

Definition 4.3.16. Let $\pi(I) \in \mathrm{Red}_K$. The sequence $(\theta_i)_{i\geq 0}$ is called the *θ-sequence* of $\pi(I)$.

Lemma 4.3.17. Let $\pi(I), \pi(J) \in \mathrm{Red}_K$. If there exists some $\gamma \in \mathbb{R}_{>1}$ such that $I = \gamma J$, then there exists some θ_k in the θ-sequence of $\pi(I)$ such that $\gamma = \theta_k$.

Proof. Consider the θ-sequence $(\theta_i)_{i\geq 0}$ of $\pi(I)$. Since $\xi_j > 1$ for all $j \in \mathbb{Z}_{\geq 0}$, we have $\theta_i > 1$ for all $i \in \mathbb{Z}_{>0}$. Consequently, the sequence $(\theta_i)_{i\geq 0}$ is monotone increasing and bounded from below by $\theta_0 = 1$. Since $\gamma > 1$, there exists some $m \in \mathbb{Z}_{\geq 0}$ such that

$$\theta_m < \gamma \leq \theta_{m+1}. \tag{46}$$

Assume, for the matter of contradiction, that $\gamma \neq \theta_{m+1}$. Equivalently, we assume that we have strict inequalities in (46). Since $\pi(J)$ is reduced, we have $1 \in J$, so $\gamma \in I$. Then using (45), there exist $k, l \in \mathbb{Z}$ such that

$$\gamma = k\theta_m + l\theta_{m+1}. \tag{47}$$

Using (46), we obtain

$$\theta_m < k\theta_m + l\theta_{m+1} < \theta_{m+1}. \tag{48}$$

Since γ is non-zero, not both k and l are zero. Assume that $k = 0$. Then $\gamma = l\theta_{m+1}$. If $l > 0$, then γ exceeds the upper bound, since $\theta_m > 0$. If $l < 0$, then γ exceeds the lower bound. Therefore, we reach a contradiction. So k must be non-zero. Furthermore, we know that $\theta_i > 1$ for all $i \in \mathbb{Z}_{>0}$. This means that not both k, l can be negative, because then γ will exceed the lower bound of (48). Furthermore, not both can be positive because then γ will exceed the upper bound of (48). So we can say that if $k > 0$, we need $l \leq 0$. Moreover, if $k < 0$, then we need $l \geq 0$.

From (45), we also have $\theta_m \in I = \gamma J$. Hence, there exists some non-zero $x \in J$ such that $\theta_m = \gamma x$. Substituting this into (46) gives $\gamma x < \gamma$. Since $\gamma > 1$, we have $x < 1$. So in particular $|x|_\infty < 1$. Since $\pi(J)$ is reduced, we have that $1 \in J$ is minimal. So, we have that $|\sigma(x)|_\infty > 1$. Then

$$|\sigma(\theta_m)|_\infty = |\sigma(\gamma x)|_\infty = |\sigma(\gamma)|_\infty |\sigma(x)|_\infty > |\sigma(\gamma)|_\infty.$$

Using expression (47) of γ, we obtain

$$|\sigma(\theta_m)|_\infty > |k\sigma(\theta_m) + l\sigma(\theta_{m+1})|_\infty. \tag{49}$$

Now, we know that $-1 < \sigma(\xi_j) < 0$ for all $j \in \mathbb{Z}_{\geq 0}$, so $|\sigma(\theta_i)|_\infty < 1$ for all $i \in \mathbb{Z}_{>0}$. Moreover, exactly one out of $\sigma(\theta_m), \sigma(\theta_{m+1})$ can be positive. We saw that if $k > 0$, we need $l \leq 0$. Moreover, if $k < 0$, then we need $l \geq 0$. We will use these facts in the following case distinction.

i.) If $k > 0$ and $\sigma(\theta_m) > 0$, then we must have $l\sigma(\theta_{m+1}) < 0$ for (49) to hold. However, we know that $l \leq 0$ and $\sigma(\theta_{m+1}) < 0$, reaching a contradiction.

ii.) If $k > 0$ and $\sigma(\theta_m) < 0$, then we must have $l\sigma(\theta_{m+1}) > 0$ for (49) to hold. However, we know that $l \leq 0$ and $\sigma(\theta_{m+1}) > 0$, reaching a contradiction.

iii.) If $k < 0$ and $\sigma(\theta_m) > 0$, then we must have $l\sigma(\theta_{m+1}) > 0$ for (49) to hold. However, we know that $l \geq 0$ and $\sigma(\theta_{m+1}) < 0$, reaching a contradiction.

iv.) If $k < 0$ and $\sigma(\theta_m) < 0$, then we must have $l\sigma(\theta_{m+1}) < 0$ for (49) to hold. However, we know that $l \geq 0$ and $\sigma(\theta_{m+1}) > 0$, reaching a contradiction.

Since k and $\sigma(\theta_{m+1})$ are non-zero, we have covered all cases. Thus, inequalities (48) and (49) are not solvable at the same time for $k, l \in \mathbb{Z}$. Consequently, we reach a contradiction. Therefore, by our assumption, we must have $\gamma = \theta_{m+1}$. Now, set $k = m + 1$. □

Theorem 4.3.18. Let $\pi(I) \in \mathrm{Red}_K$. Then there exists a minimal $m \in \mathbb{Z}_{>0}$ such that $\rho^m(\pi(I)) = \pi(I)$, and the set

$$\{\pi(I), \rho(\pi(I)), \ldots, \rho^{m-1}(\pi(I))\}$$

is a complete set of distinct reduced Arakelov divisors ideal equivalent to $\pi(I)$.

Proof. Let $\pi(J)$ be reduced for some $J \in \mathrm{Id}_K$ that is ideal equivalent to $\pi(I)$. Hence, there exists some $\gamma \in K^*$ such that $I = \gamma J$. We can assume γ to be positive, otherwise, we can multiply by $-1 \in \mathcal{O}_K^*$. Then there exists some $l \in \mathbb{Z}$ such that $\gamma\varepsilon_K^l > 1$ (see Remark 1.3.3). Since $\varepsilon_K^l J = J$, we have $\gamma\varepsilon_K^l J = \gamma J = I$. Thus, we can assume that $I = \gamma J$ for some $\gamma > 1$. It follows from Lemma 4.3.17 that there exists some θ_k in the θ-sequence of $\pi(I)$ such that $\gamma = \theta_k$. Then

$$I = \theta_k J \quad \Longrightarrow \theta_k^{-1} I = J.$$

It follows that

$$\pi(J) = \pi(\theta_k^{-1} I) = \rho^k(\pi(I)). \tag{50}$$

Therefore, the reduced Arakelov divisor $\pi(J)$ is contained in the set

$$\mathcal{B} := \{\pi(I), \rho(\pi(I)), \rho^2(\pi(i)), \dots, \rho^k(\pi(I)), \dots\}.$$

Now, the $\mathcal{B}$ contains only reduced Arakelov divisors. Since Red_K is a finite set, there must exist integers $0 < j < l$ such that $\rho^j(\pi(I)) = \rho^l(\pi(I))$. By Proposition 4.3.15, we obtain that $\rho^{l-j}(\pi(I)) = \pi(I)$. Hence, there exists an $m \in \mathbb{Z}_{>0}$ such that $\rho^m(\pi(I)) = \pi(I)$. Then there exists a minimal such integer m. So

$$\{\pi(I), \rho(\pi(I)), \dots, \rho^{m-1}(\pi(I))\} \tag{51}$$

is a complete set of distinct reduced Arakelov divisors ideal equivalent to $\pi(I)$. Namely, by construction of ρ, they are ideal equivalent to $\pi(I)$. Furthermore, they are distinct, because if there existed integers $0 < k < l < m$ such that $\rho^k(\pi(I)) = \rho^l(\pi(I))$, then we would have $\rho^{l-k}(\pi(I)) = \pi(I)$ for $l - k < m$, contradicting the minimality of m. Now, if any reduced Arakelov divisor is ideal equivalent to $\pi(I)$ and is not contained in the set (51), we reach a contradiction with our earlier observation. Namely, any such Arakelov divisor is the image of ρ^k for some $k \in \mathbb{Z}_{\geq 0}$ (see Equation (50)). We conclude that the set (51) is also complete. □

This result allows us to define the following things.

Definition 4.3.19. Let $\pi(I)$ be a reduced Arakelov divisor of K. The smallest integers $m \in \mathbb{Z}_{\geq 0}$ such that $\rho^m(\pi(I)) = \pi(I)$ is called the *period* of $\pi(I)$, and is denoted by $\mathrm{ord}(\pi(I))$. Moreover, the complete set

$$\left\{\rho^k(\pi(I)) : 1 \leq k \leq \mathrm{ord}(\pi(I)) - 1\right\}$$

of distinct reduced Arakelov divisors ideal equivalent to $\pi(I)$ is called the *Arakelov cycle* of $\pi(I)$. The Arakelov cycle of $\pi(\mathcal{O}_K)$ is called the *principal Arakelov cycle* of K.

The Arakelov cycle of a reduced Arakelov divisor of K is an analogue of the cycle of a reduced integral ideal of $\mathcal{O}_K$ defined in Definition 1.3.10.

Proposition 4.3.20. Let $\pi(I) \in \mathrm{Red}_K$ and $(\theta_i)_{i \geq 0}$ the θ-sequence of $\pi(I)$. Then $\theta_{\mathrm{ord}(\pi(I))} = \varepsilon_K$.

Proof. Since $I = \varepsilon_K I$ with $\varepsilon_K > 1$ (see Remark 1.3.3), we know by Lemma 4.3.17 that there exists some $k \in \mathbb{Z}_{\geq 0}$ such that $\varepsilon_K = \theta_k$. Therefore, we have

$$\rho^k(\pi(I)) = \pi(\theta_k^{-1} I) = \pi(\varepsilon_K^{-1} I)) = \pi(I).$$

Since $\mathrm{ord}(\pi(I)) \in \mathbb{Z}_{>0}$ is minimal such that $\rho^{\mathrm{ord}(\pi(I))}(\pi(I)) = \pi(I)$, we must have $k \geq \mathrm{ord}(\pi(I))$. Since $(\theta_i)_{i \geq 1}$ is a monotone increasing sequence, we have $\theta_k \geq \theta_{\mathrm{ord}(\pi(I))}$. We also have

$$\pi(I) = \rho^{\mathrm{ord}(\pi(I))}(\pi(I)) = \pi(\theta_{\mathrm{ord}(\pi(I))}^{-1} I) = \pi(\theta_{\mathrm{ord}(\pi(I))}^{-1} \mathcal{O}_K) + \pi(I),$$

using Equation (41). It follows that $\pi(\theta_{\mathrm{ord}(\pi(I))}^{-1} \mathcal{O}_K)$ is the zero Arakelov divisor. So by definition of π, we have that $\mathrm{ord}_{\mathfrak{p}}(\theta_{\mathrm{ord}(\pi(I))}) = 0$ for all $\mathfrak{p} \in \mathfrak{P}_K^0$. We obtain that $\theta_{\mathrm{ord}(\pi(I))} \in \mathcal{O}_K^*$. Together with the fact that $\theta_{\mathrm{ord}(\pi(I))} > 1$, there must exists some $l \in \mathbb{Z}_{>0}$ such that $\theta_{\mathrm{ord}(\pi(I))} = \varepsilon_K^l$. So we get that

$$\varepsilon_K = \theta_k \geq \theta_{\mathrm{ord}(\pi(I))} = \varepsilon_K^l.$$

Since $\varepsilon_K > 1$ and $l \in \mathbb{Z}_{>0}$, this only holds if $l = 1$. So we obtain that $\varepsilon_K = \theta_{\mathrm{ord}(\pi(I))}$. □

This result gives us a way to determine the fundamental unit of $\mathcal{O}_K$ and the regulator of K.

Example 4.3.21. Let $d = 12$. Consider the reduced Arakelov divisor $\pi(\mathcal{O}_K)$. We want to determine the period of $\pi(\mathcal{O}_K)$. Along the way, we keep track of the θ-sequence. This data allows us to find the fundamental unit by Proposition 4.3.20. So let us start by computing $\rho(\pi(\mathcal{O}_K))$. This means that we have to divide $\mathcal{O}_K$ by $\xi_0 = x_{(\mathcal{O}_K,1)}$. So let us first determine ξ_0. We have

$$\xi_0 = \frac{b + \sqrt{d}}{2a},$$

where we have integers $a = N_{\mathcal{O}_K}(\mathcal{O}_K^{-1})$ and $b \in \mathcal{A}_a$. Since $a = 1$, we get $b \in [\sqrt{12} - 2, \sqrt{12}]$. The only integers in this interval are $2, 3$. In Section 1.3, we saw that $\mathcal{O}_K = \mathbb{Z}[\omega]$ with $\omega = \frac{12+\sqrt{12}}{2}$. Now, if we take $b = 3$, we cannot have $\omega \in \mathbb{Z} + \xi_0\mathbb{Z} = \mathcal{O}_K$. Hence, we must have $b = 2$. So we get

$$\mathcal{O}_K = \mathbb{Z} + \xi_0\mathbb{Z} = \mathbb{Z} + \left(\frac{2 + \sqrt{12}}{2}\right)\mathbb{Z}.$$

Now, we divide by ξ_0 to obtain

$$\xi_0^{-1}\mathcal{O}_K = \mathbb{Z} + \left(\frac{2}{2 + \sqrt{12}}\right)\mathbb{Z} = \mathbb{Z} + \left(\frac{2 + \sqrt{12}}{4}\right)\mathbb{Z}. \tag{52}$$

Thus, we have

$$\rho(\pi(\mathcal{O}_K)) = \pi(\xi_0^{-1}\mathcal{O}_K) = \pi\left(\mathbb{Z} + \left(\frac{2 + \sqrt{12}}{4}\right)\mathbb{Z}\right).$$

Since this is not equal to $\pi(\mathcal{O}_K)$, we need to compute $\rho^2(\pi(\mathcal{O}_K))$. Therefore, we have to divide by the element $\xi_1 := x_{(\xi_0^{-1}\mathcal{O}_K,1)}$. We have

$$\xi_1 = \frac{b + \sqrt{d}}{2a},$$

where we have integers $a = N_{\mathcal{O}_K}(\xi_0\mathcal{O}_K^{-1})$ and $b \in \mathcal{A}_a$. Using Proposition 1.1.15 and 1.2.6, we have that $N_{\mathcal{O}_K}(\xi_0\mathcal{O}_K^{-1}) = |N_{K|\mathbb{Q}}(\xi_0)|_\infty = |\xi_0\sigma(\xi_0)|_\infty$. So we have

$$a = \left|\left(\frac{2 + \sqrt{12}}{2}\right)\left(\frac{2 - \sqrt{12}}{2}\right)\right|_\infty = 2.$$

It follows that $b \in [\sqrt{12} - 2, \sqrt{12}]$. Since b is uniquely determined in this interval, and we already had representation (52), we can conclude that $b = 2$. So we get

$$\xi_0^{-1}\mathcal{O}_K = \mathbb{Z} + \xi_1\mathbb{Z} = \mathbb{Z} + \left(\frac{2 + \sqrt{12}}{4}\right)\mathbb{Z}.$$

Now, we divide $\xi_0^{-1}\mathcal{O}_K$ by ξ_1 to obtain

$$\xi_1^{-1}\xi_0^{-1}\mathcal{O}_K = \mathbb{Z} + \left(\frac{4}{2 + \sqrt{12}}\right)\mathbb{Z} = \mathbb{Z} + \left(\frac{2 + \sqrt{12}}{2}\right)\mathbb{Z} = \mathcal{O}_K.$$

So we get

$$\rho^2(\pi(\mathcal{O}_K)) = \rho(\pi(\xi_0^{-1}\mathcal{O}_K)) = \pi(\xi_1^{-1}\xi_0^{-1}\mathcal{O}_K) = \pi(\mathcal{O}_K).$$

Thus, the period of $\pi(\mathcal{O}_K)$ equals 2. By Theorem 4.3.20, we have that $\varepsilon_K = \theta_{\mathrm{ord}(\pi(\mathcal{O}_K))} = \xi_0\xi_1$. Hence, we get

$$\varepsilon_K = \left(\frac{2 + \sqrt{12}}{4}\right)\left(\frac{2 + \sqrt{12}}{2}\right) = 2 + \sqrt{3},$$

which is known to be the fundamental unit of $\mathcal{O}_K$ for $d = 12$. Furthermore, the regulator is given by

$$R_K = \log(\varepsilon_K) = \log(2 + \sqrt{3}) \approx 0.57194754753.$$ ■

From this example, one may wonder what the importance is of the second entry of $\pi(I) = (I, (\mathrm{N}_{\mathcal{O}_K}(I))_{\sigma\in\Sigma_K^\infty})$, for some $I \in \mathrm{Id}_K$, because we did not consider it at all. We simply divide by the elements ξ_i, and continue until we get back to the original fractional ideal. So these ideas can purely happen ideal theoretically. There is no need to consider Arakelov divisors. But if d is much larger, the number of divisions may grow. Therefore, the method we saw in this example may be expensive. To solve this issue, we can define a distance between two reduced Arakelov divisors that are ideal equivalent. This distance is dependent on the second entry of $\pi(I)$. With this distance, we still have a way to find the regulator, but not the fundamental unit. But in certain situations, it is enough to compute the regulator. This is much more manageable since it is the log of the 'size' of the fundamental unit. The latter can grow rapidly if the fundamental discriminant $d \in \mathbb{Z}_{\geq 0}$ grows.

4.3.3 Distance Formula

In Section 1.3, the next step was to define the distance between reduced integral ideals in the principal cycle of K (see Definition 1.3.11). We can do the same thing for the principal Arakelov cycle of K. However, we can even define the distance between Arakelov divisors that are ideal equivalent.

Recall the group

$$T_K = \mathbb{R}^2/\{(\log|a|_\infty, \log|\sigma(a)|_\infty) : a \in \mathcal{O}_K^*\}$$

that we have seen in the short exact sequence (38). Moreover, we had the injective group homomorphism $\zeta\colon T_K \to \mathrm{Pic}_K$ defined by $[(x_\sigma)_{\sigma\in\Sigma_K^\infty}] \mapsto [\sum_{\sigma\in\Sigma_K^\infty} x_\sigma\sigma]$. Using the group isomorphism $\log : \mathbb{R}_{>0} \to \mathbb{R}$, we also have

$$T_K \cong \mathbb{R}^2_{>0}/\{(|a|_\infty, |\sigma(a)|_\infty) : a \in \mathcal{O}_K^*\}. \tag{53}$$

We will use this representation for T_K throughout this section. Whenever we take an arbitrary $u \in \mathbb{R}^2_{>0}$, we use the convention that $u = (u_1, u_2)$. Moreover, for $u \in \mathbb{R}^2_{>0}$, we denote its equivalence class in T_K by $[u]$. The group homomorphism ζ is given by $[u] \mapsto [(\mathcal{O}_K, u)]$, using the representation of T_K from (53). Consider the function $\delta^1_{\mathrm{Pic}}\colon T_K \to \mathbb{R}/R_K\mathbb{Z}$ defined by

$$\delta^1_{\mathrm{Pic}}([u]) := \frac{1}{2}\log\left(\frac{u_1}{u_2}\right) \bmod R_K.$$

Throughout this chapter, we will commonly ignore the notation of '$\bmod R_K$'. But one has to keep in mind that the image of $\delta^1_{\mathrm{Pic}}([u])$ is only uniquely determined modulo R_K.

Proposition 4.3.22. The function δ^1_{Pic} is well-defined.

Proof. Suppose that $[u] = [v]$ in T_K. Then there exists some $a \in \mathcal{O}_K^*$ such that $(u_1, u_2) = (|a|_\infty v_1, |\sigma(a)|_\infty v_2)$ and

$$\delta^1_{\mathrm{Pic}}([u]) = \frac{1}{2}\log\left(\frac{u_1}{u_2}\right) = \frac{1}{2}\log\left(\frac{|a|_\infty v_1}{|\sigma(a)|_\infty v_2}\right).$$

As $a \in \mathcal{O}_K^*$, we have $|N_{K|\mathbb{Q}}(a)|_\infty = 1$. Proposition 1.1.15 implies that $|a\sigma(a)|_\infty = 1$. Equivalently, we have $|a|_\infty = |\sigma(a)|_\infty^{-1}$. Therefore, we get

$$\delta^1_{\mathrm{Pic}}([u]) = \frac{1}{2}\log\left(\frac{|a|_\infty^2 v_1}{v_2}\right) = \frac{1}{2}\log|a|_\infty^2 + \frac{1}{2}\log\left(\frac{v_1}{v_2}\right) = \log|a|_\infty + \delta^1_{\mathrm{Pic}}([v]).$$

Since $a \in \mathcal{O}_K^*$, there exists some $k \in \mathbb{Z}$ such that $a = \pm\varepsilon_K^k$. It follows that $\log|a|_\infty = k\log|\varepsilon_K|_\infty = kR_K$, and so $\delta^1_{\mathrm{Pic}}([u]) \equiv \delta^1_{\mathrm{Pic}}([v]) \bmod R_K$. This shows that δ^1_{Pic} is well-defined. □

Let $D, D' \in \mathrm{Div}_K$ be two Arakelov divisors that are ideal equivalent. Write them in multiplicative notation $D = (I, u)$ and $D' = (J, v)$. Then there exists some $x \in K^*$ such that $I = xJ$. We obtain that

$$D - D' + \mathrm{div}(x) = (\mathcal{O}_K, w),$$

where $w = (u_1 v_1^{-1}|x|_\infty, u_2 v_2^{-1}|\sigma(x)|_\infty)$. This means that $[D - D'] = [(\mathcal{O}_K, w)]$ in the Arakelov class group Pic_K. Note that $[(\mathcal{O}_K, w)]$ is the image of $[w] \in T_K$ under the group homomorphism ζ. We claim that $[w]$ is the unique class in T_K such that its image under ζ equals $[D - D']$. Suppose that there exists some other $w' \in \mathbb{R}^2_{>0}$ such that $[D - D'] = [(\mathcal{O}_K, w')]$. Then $[(\mathcal{O}_K, w)] = [(\mathcal{O}_K, w')]$ in Pic_K. Hence, there exists some $y \in K^*$ such that

$$(\mathcal{O}_K, w) + \mathrm{div}(y) = (\mathcal{O}_K, w').$$

This means that $\mathcal{O}_K = y\mathcal{O}_K$ and $w' = (|y|_\infty, |\sigma(y)|_\infty)w$. We get that $y \in \mathcal{O}_K^*$, and so $[w] = [w']$ in T_K. Consequently, the class $[w]$ in T_K is uniquely determined by $[D - D']$. Therefore, the following definition is well-defined.

Definition 4.3.23. The *distance* between two Arakelov divisors $D, D' \in \mathrm{Div}_K$ that are ideal equivalent is defined by

$$\delta_{\mathrm{Pic}}(D, D') := \delta^1_{\mathrm{Pic}}([w]),$$

such that $[D - D'] = [(\mathcal{O}_K, w)]$.

Note that the distance is only defined for Arakelov divisors that are ideal equivalent. Furthermore, we will always view the distance in $\mathbb{R}$. But we have to keep in mind that the distance is only uniquely determined modulo R_K (see Proposition 4.3.22).

Suppose that $[D - D'] = [(\mathcal{O}_K, w)]$ for ideal equivalent Arakelov divisors $D, D' \in \mathrm{Div}_K$ and $w \in \mathbb{R}^2_{>0}$. Then

$$[D' - D] = -[(\mathcal{O}_K, w)] = [(\mathcal{O}_K, w^{-1})].$$

This means that

$$\delta_{\mathrm{Pic}}(D, D') = \delta^1_{\mathrm{Pic}}([w]) = \frac{1}{2}\log\left(\frac{w_1}{w_2}\right) = -\frac{1}{2}\log\left(\frac{w_1^{-1}}{w_2^{-1}}\right) = -\delta^1_{\mathrm{Pic}}([w^{-1}]) = -\delta_{\mathrm{Pic}}(D', D).$$

This means that the distance is not symmetric. More precisely, the distance has a positive and negative orientation.

The following result tells us that the distance is uniquely determined by the equivalence classes in Pic_K.

Proposition 4.3.24. Let $D_1, D_2, D_3 \in \mathrm{Div}_K$ be ideal equivalent.

i.) If $[D_1] = [D_2]$ in Pic_K, then $\delta_{\mathrm{Pic}}(D_1, D_2) = 0$.

ii.) If $[D_1] = [D_2]$ in Pic_K, then $\delta_{\mathrm{Pic}}(D_1, D_3) = \delta_{\mathrm{Pic}}(D_2, D_3)$.

Proof. To show Statement (i.), suppose that $[D_1] = [D_2]$. Then $[D_1 - D_2]$ equals the equivalence class of the zero Arakelov divisor $(\mathcal{O}_K, (1, 1))$. So we get that

$$\delta_{\mathrm{Pic}}(D_1, D_2) = \delta^1_{\mathrm{Pic}}([(1, 1)]) = \frac{1}{2}\log(1) = 0.$$

To show Statement (ii.), notice that $[D_1 - D_3] = [D_2 - D_3]$, since $[D_1] = [D_2]$ in Pic_K. Hence, it follows by construction of δ_{Pic} that $\delta_{\mathrm{Pic}}(D_1, D_3) = \delta_{\mathrm{Pic}}(D_2, D_3)$. □

Proposition 4.3.25. Let $I \in \mathrm{Id}_K$. Then the Arakelov divisors $\pi(x^{-1}I)$ and $\pi(y^{-1}I)$ are ideal equivalent for any $x, y \in K^*$. Moreover, the distance between them is given by

$$\delta_{\mathrm{Pic}}(\pi(x^{-1}I), \pi(y^{-1}I)) = \frac{1}{2}\log\left|\frac{\sigma(x)y}{x\sigma(y)}\right|_\infty.$$

Proof. We have $[x^{-1}I] = [y^{-1}I]$ in Cl_K. Thus, the Arakelov divisors $\pi(x^{-1}I)$ and $\pi(y^{-1}I)$ are ideal equivalent. So we can compute $\delta_{\mathrm{Pic}}(\pi(x^{-1}I), \pi(y^{-1}I))$. We have

$$\pi(x^{-1}I) - \pi(y^{-1}I) + \mathrm{div}(x^{-1}y) = (\mathcal{O}_K, u), \qquad u = \left(\frac{\sqrt{N_{\mathcal{O}_K}(y^{-1}I)}|y|_\infty}{\sqrt{N_{\mathcal{O}_K}(x^{-1}I)|x|_\infty}}, \frac{\sqrt{N_{\mathcal{O}_K}(y^{-1}I)}|\sigma(y)|_\infty}{\sqrt{N_{\mathcal{O}_K}(x^{-1}I)}|\sigma(x)|_\infty} \right).$$

We see that $[\pi(x^{-1}I) - \pi(y^{-1}I)] = [(\mathcal{O}_K, u)]$, and so $\delta_{\mathrm{Pic}}(\pi(x^{-1}I), \pi(y^{-1}I)) = \delta^1_{\mathrm{Pic}}([u])$. Using Proposition 1.1.15 and 1.2.6, we have for any $z \in K^*$ that

$$N_{\mathcal{O}_K}(z^{-1}I) = N_{\mathcal{O}_K}(z^{-1}\mathcal{O}_K)N_{\mathcal{O}_K}(I) = |z^{-1}|_\infty |\sigma(z^{-1})|_\infty N_{\mathcal{O}_K}(I).$$

Consequently, we have

$$u = \left(\sqrt{\left| \frac{\sigma(x)y}{x\sigma(y)} \right|_\infty}, \sqrt{\left| \frac{\sigma(y)x}{y\sigma(x)} \right|_\infty} \right).$$

We obtain that

$$\delta_{\mathrm{Pic}}(\pi(x^{-1}I), \pi(y^{-1}I)) = \frac{1}{2}\log\left(\left(\sqrt{\left| \frac{\sigma(x)y}{x\sigma(y)} \right|_\infty} \right) \left(\sqrt{\left| \frac{\sigma(y)x}{y\sigma(x)} \right|_\infty} \right)^{-1} \right) = \frac{1}{2}\log\left| \frac{\sigma(x)y}{x\sigma(y)} \right|_\infty. \qquad \square$$

Corollary 4.3.26. Let $\pi(I) \in \mathrm{Red}_K$ and $(\theta_i)_{i\geq 0}$ be the θ-sequence of $\pi(I)$. Then for any $k, l \in \mathbb{Z}_{\geq 0}$ one has

$$\delta_{\mathrm{Pic}}\left(\rho^k(\pi(I)), \rho^l(\pi(I))\right) = \frac{1}{2}\log\left| \frac{\sigma(\theta_k)\theta_l}{\theta_k\sigma(\theta_l)} \right|_\infty.$$

If $0 \leq k < l < \mathrm{ord}(\pi(I))$, then this formula gives the representative in the interval $[0, R_K)$.

Proof. With the notation introduced in (44), we have $\rho^k(\pi(I)) = \pi(\theta_k^{-1}I)$ for all $k \in \mathbb{Z}_{\geq 0}$, where ρ is the infrastructure operator defined in Definition 4.3.12. It follows from Proposition 4.3.25 that

$$\delta_{\mathrm{Pic}}\left(\rho^k(\pi(I)), \rho^l(\pi(I))\right) = \delta_{\mathrm{Pic}}(\pi(\theta_k^{-1}I), \pi(\theta_l^{-1}I)) = \frac{1}{2}\log\left| \frac{\sigma(\theta_k)\theta_l}{\theta_k\sigma(\theta_l)} \right|_\infty.$$

Now, let $0 \leq k < l < \mathrm{ord}(\pi(I))$. For any $i \in \mathbb{Z}_{>0}$, we have the formula

$$\theta_i = \prod_{j=0}^{i-1} \xi_j,$$

with $0 < \sigma(\xi_j) < -1$ and $\xi_j > 1$ for all integers $0 \leq j \leq i-1$. Moreover, we had the convention that $\theta_0 = 1$. In Proposition 4.3.20, we saw that $\theta_{\mathrm{ord}(\pi(I))} = \varepsilon_K$. So we conclude that

$$1 \leq \theta_k < \theta_l < \theta_{\mathrm{ord}(\pi(I))} = \varepsilon_K, \qquad |\sigma(\varepsilon_K)|_\infty = |\sigma(\theta_{\mathrm{ord}(\pi(I))})|_\infty < |\sigma(\theta_l)|_\infty < |\sigma(\theta_k)|_\infty \leq 1.$$

We see that

$$0 \leq \frac{1}{2}\log\left| \frac{\sigma(\theta_k)\theta_l}{\theta_k\sigma(\theta_l)} \right|_\infty < \frac{1}{2}\log\left| \frac{\varepsilon_K}{\sigma(\varepsilon_K)} \right|_\infty. \tag{54}$$

Since $\varepsilon_K \in \mathcal{O}_K^*$, we have $|N_{K|\mathbb{Q}}(\varepsilon_K)|_\infty = 1$. It follows from Proposition 1.1.15 that $|\varepsilon_K\sigma(\varepsilon_K)|_\infty = 1$. Equivalently, we have $|\varepsilon_K|_\infty = |\sigma(\varepsilon_K)|_\infty^{-1}$. Therefore

$$\frac{1}{2}\log\left| \frac{\varepsilon_K}{\sigma(\varepsilon_K)} \right|_\infty = \frac{1}{2}\log|\varepsilon_K|_\infty^2 = \log|\varepsilon_K|_\infty = R_K.$$

Thus, inequalities (54) tell us that $\delta_{\mathrm{Pic}}\left(\rho^k(\pi(I)), \rho^l(\pi(I))\right) \in [0, R_K)$ using the formula

$$\frac{1}{2}\log\left| \frac{\sigma(\theta_k)\theta_l}{\theta_k\sigma(\theta_l)} \right|_\infty. \qquad \square$$

Recall the interval $\mathcal{A}_a$ for some $a \in \mathbb{Z}_{>0}$ from (42).

Corollary 4.3.27. Let $\pi(I) \in \mathrm{Red}_K$, and write $x_{(I,1)} = \frac{b+\sqrt{d}}{2a}$, where $a = N_{\mathcal{O}_K}(I^{-1})$ and $b \in \mathcal{A}_a$. Then

$$\delta_{\mathrm{Pic}}\left(\pi(I), \rho(\pi(I))\right) = \frac{1}{2}\log\left|\frac{b+\sqrt{d}}{b-\sqrt{d}}\right|_\infty .$$

Proof. Let $(\theta_i)_{i\geq 0}$ be the θ-sequence of $\pi(I)$. We have $\theta_0 = 1$ by convention, and $\theta_1 = \xi_0 = x_{(I,1)}$ by construction. Take $k = 0$ and $l = 1$ in Corollary 4.3.26. Then we get

$$\delta_{\mathrm{Pic}}\left(\pi(I), \rho(\pi(I))\right) = \frac{1}{2}\log\left|\frac{\sigma(\theta_0)\theta_1}{\theta_0\sigma(\theta_1)}\right|_\infty = \frac{1}{2}\log\left|\frac{x_{(I,1)}}{\sigma\left(x_{(I,1)}\right)}\right|_\infty = \frac{1}{2}\log\left|\frac{b+\sqrt{d}}{b-\sqrt{d}}\right|_\infty . \qquad \square$$

The distance formula from Corollary 4.3.27 coincides with the distance formula introduced by Lenstra for the infrastructure using binary quadratic forms (see [Len82, Chapter 11]). Furthermore, Equation (11.2) of [Len82] states that the distance, when ρ is applied twice, is bounded from below by $\log(2)$. We can recover this as well.

Corollary 4.3.28. Let $\pi(I) \in \mathrm{Red}_K$. Suppose that the Arakelov cycle induced by $\pi(I)$ contains at least three elements. If $\delta_{\mathrm{Pic}}\left(\pi(I), \rho^2(\pi(I))\right)$ is given by its representative in $[0, R_K)$, then

$$\delta_{\mathrm{Pic}}\left(\pi(I), \rho^2(\pi(I))\right) > \log(2).$$

Proof. Let $(\theta_i)_{i\geq 0}$ be the θ-sequence of $\pi(I)$. We have $\theta_0 = 1$ by convention, and $\theta_2 = \xi_0\xi_1$ by construction. Take $k = 0$ and $l = 2$ in Corollary 4.3.26. Then we get

$$\delta_{\mathrm{Pic}}\left(\pi(I), \rho^2(\pi(I))\right) = \frac{1}{2}\log\left|\frac{\sigma(\theta_0)\theta_2}{\theta_0\sigma(\theta_2)}\right|_\infty = \frac{1}{2}\log\left|\frac{\xi_0\xi_1}{\sigma(\xi_0\xi_1)}\right|_\infty \in [0, R_K), \tag{55}$$

where the interval inclusion follows from Corollary 4.3.26 as well. So it suffices to show that

$$\frac{1}{2}\log\left|\frac{\xi_0\xi_1}{\sigma(\xi_0\xi_1)}\right|_\infty > \log(2).$$

By construction, we have $I_0 = I$, $\xi_0 = x_{(I_0,1)}$, $I_1 = \xi_0^{-1}I_0$, and $\xi_1 = x_{(I_1,1)}$. Hence, by Lemma 4.3.14, we have $\xi_i > 1$ and $-1 < \sigma(\xi_i) < 0$ for $i = 1, 2$. We know

$$\xi_i = \frac{b_i + \sqrt{d}}{2a_i},$$

where $a_i = N_{\mathcal{O}_K}(I_i^{-1})$ and $b_i \in \mathcal{A}_{a_i}$. The Arakelov divisor $\pi(I_i)$ is reduced. It follows from Proposition 7.2 in [Sch08] that $N_{\mathcal{O}_K}(I_i^{-1}) < \sqrt{d}$. So we have $a_i < \sqrt{d}$, which means that $b_i \in [\sqrt{d} - 2a_i, \sqrt{d}]$. Since $\xi_i > 1$, we have $b_i + \sqrt{d} > 2a_i$, so $b_i > 2a_i - \sqrt{d}$. Consequently, we get

$$b_i > |\sqrt{d} - 2a_i|_\infty > 0, \qquad a_i < \sqrt{d},$$

for $i = 1, 2$. So

$$0 > \sigma(\xi_i) = \frac{b_i - \sqrt{d}}{2a_i} > -\frac{\sqrt{d}}{2a_i} > -\frac{1}{2}.$$

This implies that

$$|\sigma(\xi_i)|_\infty < \frac{1}{2} \implies |\sigma(\xi_0)\sigma(\xi_1)|_\infty < \frac{1}{4} \implies \frac{1}{|\sigma(\xi_0)\sigma(\xi_1)|_\infty} > 4.$$

Using $\xi_i > 1$ for $i = 1, 2$, we get

$$\left|\frac{\xi_0\xi_1}{\sigma(\xi_0\xi_1)}\right|_\infty > \frac{1}{|\sigma(\xi_0)\sigma(\xi_1)|_\infty} > 4.$$

Hence, substituting this into Equation (55), and using that log is an increasing function, we get

$$\frac{1}{2}\log\left|\frac{\xi_0\xi_1}{\sigma(\xi_0\xi_1)}\right|_\infty > \frac{1}{2}\log(4) = \log(2). \qquad \square$$

Remark 4.3.29. Let $\pi(I)$ be a reduced Arakelov divisor and $(\theta_i)_{i\geq 0}$ the θ-sequence of $\pi(I)$. Consider the Arakelov cycle of $\pi(I)$ given by

$$\left\{\rho^k(\pi(I)) : 1 \leq k \leq \operatorname{ord}(\pi(I)) - 1\right\} = \left\{\pi(\theta_k^{-1}I) : 1 \leq k \leq \operatorname{ord}(\pi(I)) - 1\right\}.$$

For the rest of this section, put $m := \operatorname{ord}(\pi(I))$. We know that $\rho^m(\pi(I)) = \pi(I)$. Therefore, Proposition 4.3.24 (i.) implies that

$$\delta_{\mathrm{Pic}}\left(\pi(I), \rho^m(\pi(I))\right) = 0. \tag{56}$$

We have $\theta_0 = 1$ by convention, and $\theta_m = \varepsilon_K$ by Proposition 4.3.20. Take $k = 0$ and $l = m$, then by Corollary 4.3.26, we have

$$\delta_{\mathrm{Pic}}\left(\pi(I), \rho^m(\pi(I))\right) = \frac{1}{2}\log\left|\frac{\sigma(\theta_0)\theta_m}{\theta_0\sigma(\theta_m)}\right|_\infty = \frac{1}{2}\log\left|\frac{\varepsilon_K}{\sigma(\varepsilon_K)}\right|_\infty.$$

Since $\varepsilon_K \in \mathcal{O}_K^*$, we have $|N_{K|\mathbb{Q}}(\varepsilon_K)|_\infty = 1$. Hence, by Proposition 1.1.15, we have $|\varepsilon_K\sigma(\varepsilon_K)|_\infty = 1$. Equivalently, we have $|\varepsilon_K|_\infty = |\sigma(\varepsilon_K)|_\infty^{-1}$. Therefore

$$\delta_{\mathrm{Pic}}\left(\pi(I), \rho^m(\pi(I))\right) = \frac{1}{2}\log\left|\frac{\varepsilon_K}{\sigma(\varepsilon_K)}\right|_\infty = \frac{1}{2}\log|\varepsilon_K|_\infty^2 = \log|\varepsilon_K|_\infty = R_K. \tag{57}$$

Comparing (56) and (57) we see that the distance is inconsistent as a real number. However, recall that by Proposition 4.3.22 the distance was only well-defined modulo R_K. Therefore, the distances are actually the same. From this reasoning, we can visualize that the 'entire distance' of the Arakelov cycle of $\pi(I)$ equals the regulator. So if we do not take the distances modulo R_K, we get a way to determine the regulator. This is exactly what we will do in the next section. ♦

Remark 4.3.30. Schoof introduced a different distance function than δ_{Pic} in [Sch08, Chapter 6]. In Chapter 8 of the same paper, he states that its distance function recovers Lenstra's distance formula as well. This distance function is given through a different δ^1_{Pic} function. We will denote this one by $\delta^2_{\mathrm{Pic}} : T_K \to \mathbb{R}$. Only for this remark, set $\hat{a} := (|a|_\infty, |\sigma(a)|_\infty)$ for any $a \in \mathcal{O}_K^*$. Then this function is defined by

$$\delta^2_{\mathrm{Pic}}([u]) := \min_{a\in\mathcal{O}_K^*} \|\log(\hat{a}u)\|_{\mathbb{R}},$$

where $\|.\|_{\mathbb{R}} := \sqrt{\langle\cdot,\cdot\rangle_{\mathbb{R}}}$ is the norm on the Minkowski space $K_{\mathbb{R}}$ induced from the inner product $\langle\cdot,\cdot\rangle_{\mathbb{R}}$ that we have seen in Section 1.8. This function is well-defined. Namely, for $[u] = [v]$ in T_K, there exists some $a \in \mathcal{O}_K^*$ such that $u = \hat{a}v$. Then

$$\delta^2_{\mathrm{Pic}}([u]) = \min_{b\in\mathcal{O}_K^*} \|\log(\hat{b}u)\|_{\mathbb{R}} = \min_{b\in\mathcal{O}_K^*} \|\log(\hat{b}\hat{a}v)\|_{\mathbb{R}} = \min_{c\in\mathcal{O}_K^*} \|\log(\hat{c}v)\|_{\mathbb{R}} = \delta^2_{\mathrm{Pic}}([v]),$$

where we had set $c = ab$. Now, one can define an alternative distance between two Arakelov divisors $D, D' \in \mathrm{Div}_K$ that are ideal equivalent given by

$$\Delta_{\mathrm{Pic}}(D, D') := \delta^2_{\mathrm{Pic}}([w]),$$

such that $[D - D'] = [(\mathcal{O}_K, w)]$.

There are a few reasons why we chose to introduce the δ^1_{Pic} function, and not to copy Schoof's work. Firstly, while Schoof's distance can recover Lenstra's distance formula, it cannot obtain Corollary 4.3.26. Namely, the analogue of Proposition 4.3.25 would be given by

$$\Delta_{\mathrm{Pic}}(\pi(x^{-1}I), \pi(y^{-1}I)) = \sqrt{2} \min_{a \in \mathcal{O}_K^*} \left| \log \left(|a|_\infty \sqrt{\left| \frac{\sigma(x)y}{x\sigma(y)} \right|_\infty} \right) \right|_\infty$$

for any $x, y \in K^*$. So given any $\pi(I) \in \mathrm{Red}_K$, its θ-sequence $(\theta_i)_{i \geq 0}$, and any $k, l \in \mathbb{Z}_{\geq 0}$ one has

$$\Delta_{\mathrm{Pic}}\left(\rho^k(\pi(I)), \rho^l(\pi(I))\right) = \Delta_{\mathrm{Pic}}(\pi(\theta_k^{-1}I), \pi(\theta_l^{-1}I)) = \sqrt{2} \min_{a \in \mathcal{O}_K^*} \left| \log \left(|a|_\infty \sqrt{\left| \frac{\sigma(\theta_k)\theta_l}{\theta_k \sigma(\theta_l)} \right|_\infty} \right) \right|_\infty .$$

Using that $\log |a|_\infty = kR_K$ for some $k \in \mathbb{Z}$, this also equals

$$\Delta_{\mathrm{Pic}}\left(\rho^k(\pi(I)), \rho^l(\pi(I))\right) = \sqrt{2} \min_{k \in \mathbb{Z}} \left| kR_K + \frac{1}{2} \log \left(\left| \frac{\sigma(\theta_k)\theta_l}{\theta_k \sigma(\theta_l)} \right|_\infty \right) \right|_\infty .$$

Now, the absolute value, and a possible translation by R_K, force this value to be in $[0, R_K/2)$. Furthermore, to compute $\Delta_{\mathrm{Pic}}\left(\rho^k(\pi(I)), \rho^l(\pi(I))\right)$ one constantly needs to keep track of the minimum. This is different from Corollary 4.3.26. There we have an explicit formula for the distance. Since this Corollary will play a major role in the next section, we noticed that the distance Δ_{Pic} is less practical.

Another reason is that in the next section, we want to design an algorithm, using the distance function, that can compute the regulator of K. This value is unknown if the fundamental unit ε_K is unknown. Hence, it does not make sense to use δ^2_{Pic} in this algorithm as it relies on ε_K.

However, there was another reason for Schoof to introduce the function Δ_{Pic}. Namely, this function induces the topology on Pic_K. Moreover, it does so for any number field. Therefore, the function δ_{Pic} cannot be used for this, as it is only defined for a real quadratic number field. We do not discuss this any further at this point, but return to this once we introduce the topology on the Arakelov class group for the rings of S-integers in Section 5.3. ♦

4.3.4 Arakelov Infrastructure

In Definition 1.3.12, we saw the infrastructure $\mathcal{C}$ of K with operation $*$. A possible failure of the associative law prevented $\mathcal{C}$ from being an abelian group. However, due to its group-like structure, Shanks could still apply some ideas of his Baby-Step Giant-Step Algorithm on $\mathcal{C}$. In that way, he designed Algorithm 1.3.13 to compute the regulator of K. Let us try to recover this in the Arakelov setting.

Let $(\theta_i)_{i \geq 0}$ be the θ-sequence of $\pi(\mathcal{O}_K)$. Set $I_k := \theta_k^{-1}\mathcal{O}_K$ for all $k \in \mathbb{Z}_{\geq 0}$. Then we have

$$\rho^k(\pi(\mathcal{O}_K)) = \pi(\theta_k^{-1}\mathcal{O}_K) = \pi(I_k)$$

for all $k \in \mathbb{Z}_{\geq 0}$. Thus, the principal Arakelov cycle of K is given by

$$\mathcal{C}_{\mathrm{Pic}} := \left\{ \rho^k(\pi(I)) : 1 \leq k \leq \mathrm{ord}(\pi(\mathcal{O}_K)) - 1 \right\} = \left\{ \pi(I_k) : 1 \leq k \leq \mathrm{ord}(\pi(\mathcal{O}_K)) - 1 \right\}. \tag{58}$$

We use this notation throughout this section.

Remark 4.3.31. Set $x_k := x_{(I_k,1)}$ for all $k \in \mathbb{Z}_{\geq 0}$. By construction of the element $x_{(I_k,1)}$ in I_k, we have

$$I_k = \mathbb{Z} + x_k\mathbb{Z}, \qquad x_k = \frac{b_k + \sqrt{d}}{2a_k},$$

where $a_k = N_{\mathcal{O}_K}(I_k^{-1})$ and $b_k \in \mathcal{A}_{a_k}$ are integers. Furthermore, we have the relation $c_k := \frac{b_k^2 - d}{4a_k}$ such that $\gcd(a_k, b_k, c_k) = 1$. With a similar argument as in the proof of Theorem 4.3.9 one shows that $a_{k+1} = |c_k|_\infty$ and $b_{k+1} \equiv -b_k \bmod 2a_{k+1}$ for all $k \in \mathbb{Z}_{\geq 0}$. We conclude that if b_0 is even, then so is b_k for all $k \in \mathbb{Z}_{\geq 0}$. Similarly, if b_0 is odd, then so is b_k for all $k \in \mathbb{Z}_{\geq 0}$. Note that

$$x_{(I_0,1)} = \frac{b_0 + \sqrt{d}}{2},$$

where b_0 is 0 or 1 depending on the fundamental discriminant $d \in \mathbb{Z}_{>0}$. We will use this observation later on. ⧫

Now, we can use Proposition 4.3.3 to compose reduced Arakelov divisors from the principal Arakelov cycle of K. Recall the interval $\mathcal{A}_a$ for some $a \in \mathbb{Z}_{>0}$ from (42).

Algorithm 4.3.32. (Composition Algorithm for reduced Arakelov Divisors in Principal Arakelov Cycles)
Input: Any reduced Arakelov Divisors $\pi(I_i), \pi(I_j) \in \mathcal{C}_{\mathrm{Pic}}$.
Output: A reduced Arakelov divisor $\pi(I_k) \in \mathcal{C}_{\mathrm{Pic}}$.

i.) Write

$$I_l = \mathbb{Z} + x_{(I_l,1)}\mathbb{Z}, \qquad x_{(I_l,1)} = \frac{b_l + \sqrt{d}}{2a_l},$$

with $a_l = N_{\mathcal{O}_K}(I_l^{-1})$ and $b_l \in \mathcal{A}_{a_l}$ for $l = i, j$.

ii.) Compute

$$I_i I_j = \frac{1}{t}\left(\mathbb{Z} + \left(\frac{b + \sqrt{d}}{2a}\right)\mathbb{Z}\right),$$

as described in Proposition 4.3.3.

iii.) Apply Algorithm 4.3.8 to $\pi(I_i) + \pi(I_j) = \pi(I_i I_j)$. Use $\alpha = t^{-1}$ in step (ii.) of Algorithm 4.3.8. Return the output.

Proposition 4.3.33. Algorithm 4.3.32 is correct and deterministic.

Proof. We need to verify that the algorithm returns a unique element $\pi(I_k) \in \mathcal{C}_{\mathrm{Pic}}$. We apply Algorithm 4.3.8 to $\pi(I_i I_j)$ in step (iii.). In Remark 4.3.10, we have seen that the algorithm is non-deterministic since it depends on the choice of the primitive element in step (ii.). However, the element t^{-1} is uniquely determined from I_i and I_j, and is part of a $\mathbb{Z}$-basis of $I_1 I_2$. It follows from Lemma 4.3.1 (i.) that the element t^{-1} is primitive. So in step (ii.) of Algorithm 4.3.8, we can take $\alpha = t^{-1}$ uniquely. Consequently, the algorithm becomes deterministic. So let $\pi(J)$ be the output of Algorithm 4.3.8 with this choice in step (ii.). Then $\pi(J)$ is the reduced Arakelov divisor ideal equivalent to the sum of $\pi(I_i)$ and $\pi(I_j)$. Note that $I_i I_j$ is a principal fractional ideal since I_i and I_j are principal. So J must be principal as well. Since $\pi(J)$ is reduced, and $\mathcal{C}_{\mathrm{Pic}}$ is a complete list of reduced Arakelov divisors ideal equivalent to $\pi(\mathcal{O}_K)$, we must have $\pi(J) \in \mathcal{C}_{\mathrm{Pic}}$. So there exists some integer $0 \leq k \leq m-1$ such that $\pi(J) = \pi(I_k)$. So from $\pi(I_i)$ and $\pi(I_j)$ we went uniquely to $\pi(I_k)$. □

Remark 4.3.34. Let $\pi(I_k) \in \mathcal{C}_{\mathrm{Pic}}$ be the output of Algorithm 4.3.32 with input $\pi(I_i), \pi(I_j) \in \mathcal{C}_{\mathrm{Pic}}$. Precisely, we know that $\pi(I_k)$ is the output of $\pi(I_i I_j)$ from Algorithm 4.3.8. Thus, they are ideal equivalent, and so we can compute their distance. So let us examine this distance. We know that there exists some $y \in K^*$ such that $I_k = y I_i I_j$. Then

$$\pi(I_i I_j) - \pi(I_k) + \mathrm{div}(y^{-1}) = (\mathcal{O}_K, w),$$

where

$$w = \left(|y|_\infty^{-1}\sqrt{\frac{N_{\mathcal{O}_K}(I_k)}{N_{\mathcal{O}_K}(I_i I_j)}}, |\sigma(y)|_\infty^{-1}\sqrt{\frac{N_{\mathcal{O}_K}(I_k)}{N_{\mathcal{O}_K}(I_i I_j)}}\right).$$

So $[\pi(I_iI_j) - \pi(I_k)] = [(\mathcal{O}_K, w)]$ in Pic_K, and therefore

$$\begin{aligned}\delta_{\mathrm{Pic}}(\pi(I_iI_j), \pi(I_k)) &= \delta^1_{\mathrm{Pic}}([w]) \\ &= \frac{1}{2}\log\left(\left(|y|_\infty^{-1}\sqrt{\frac{N_{\mathcal{O}_K}(I_k)}{N_{\mathcal{O}_K}(I_iI_j)}}\right)\left(|\sigma(y)|_\infty^{-1}\sqrt{\frac{N_{\mathcal{O}_K}(I_k)}{N_{\mathcal{O}_K}(I_iI_j)}}\right)^{-1}\right) \\ &= \frac{1}{2}\log\left|\frac{\sigma(y)}{y}\right|_\infty.\end{aligned}$$

Set $D = \pi(I_iI_j)$, then using Remark 4.3.11 we can take $y = (\alpha x_D^{\alpha})^{-1}$. In Algorithm 4.3.32 we took $\alpha = t^{-1}$. So set $x_D := x_D^{t^{-1}}$, then we have $y = tx_D^{-1}$. Hence, we obtain that

$$\delta_{\mathrm{Pic}}(\pi(I_iI_j), \pi(I_k)) = \frac{1}{2}\log\left|\frac{tx_D}{\sigma(tx_D)}\right|_\infty = \frac{1}{2}\log\left|\frac{x_D}{\sigma(x_D)}\right|_\infty,$$

where we used that $\sigma(t) = t$ as $t \in \mathbb{Z}$. So we conclude that the distance between $\pi(I_iI_j)$ and $\pi(I_k)$ depends on x_D, which is determined by Algorithm 4.3.8. ⧫

The distance examined in this remark will be of interest at the end of this chapter. Namely, a bound of this distance ensures Algorithm 4.3.43 to terminate.

Conjecture 4.3.35. Let $\pi(I_k) \in \mathcal{C}_{\mathrm{Pic}}$ be the output of Algorithm 4.3.32 with input $\pi(I_i), \pi(I_j) \in \mathcal{C}_{\mathrm{Pic}}$. Then the formula

$$\frac{1}{2}\log\left|\frac{x_D}{\sigma(x_D)}\right|_\infty$$

gives the representative in the interval $\left[-\frac{R_K}{2}, \frac{R_K}{2}\right)$ for $\delta_{\mathrm{Pic}}(\pi(I_iI_j), \pi(I_k))$. Moreover, the absolute value of this value is bounded by $\log(d)$.

Remark 4.3.36. The analogue of this distance from Section 1.3, is the distance $\kappa(I_i; I_j)$ given in Equation (7). We saw in inequalities (8) that $-\log(d) < \kappa(I_i; I_j) < \log(2)$. So in particular $|\kappa(I_i; I_j)|_\infty < \log(d)$.

The analogue of this distance in Lenstra's work is the distance given in Equation (12.1) of [Len82]. It states that the distance is bounded by $\log(d)$. A more detailed analysis would even give the bound $\log(1 + \gamma\sqrt{d})$, where $\gamma = \frac{1+\sqrt{5}}{2}$.

An Arakelov theoretical bound does not exist in the literature. We have tried to prove the conjecture but failed to do so. However, future work is in progress to verify the bound. ⧫

Due to Algorithm 4.3.32, we can define an operator on $\mathcal{C}_{\mathrm{Pic}}$, as we now explain. Let $\pi(I_k) \in \mathcal{C}_{\mathrm{Pic}}$ be the output of Algorithm 4.3.32 with input $\pi(I_i), \pi(I_j) \in \mathcal{C}_{\mathrm{Pic}}$. Define the operation

$$\circledast \colon \mathcal{C}_{\mathrm{Pic}} \times \mathcal{C}_{\mathrm{Pic}} \to \mathcal{C}_{\mathrm{Pic}}, \qquad \pi(I_i) \circledast \pi(I_j) := \pi(I_k).$$

Definition 4.3.37. The principal Arakelov cycle $\mathcal{C}_{\mathrm{Pic}}$, together with the operation $\circledast$, is called the *Arakelov infrastructure* of K.

Proposition 4.3.38. The operation $\circledast$ on $\mathcal{C}_{\mathrm{Pic}}$ is closed and commutative. Furthermore, take any $\pi(I_i) \in \mathcal{C}_{\mathrm{Pic}}$. Then $\pi(I_i) \circledast \pi(\mathcal{O}_K) = \pi(I_i)$. Moreover, write $x_{(I_i,1)} = \frac{b_i+\sqrt{d}}{2a_i}$, where $a_i = N_{\mathcal{O}_K}(I_i^{-1})$ and $b_i \in \mathcal{A}_a$. Set

$$J := \mathbb{Z} + x\mathbb{Z}, \qquad x := \frac{b + \sqrt{d}}{2a_i},$$

where $b \equiv -b_i \bmod 2a_i$ and $b \in \mathcal{A}_{a_i}$. Then $\pi(J) \in \mathcal{C}_{\mathrm{Pic}}$ and $\pi(I_i) \circledast \pi(J) = \pi(\mathcal{O}_K)$.

Proof. The operation $\circledast$ is closed on $\mathcal{C}_{\mathrm{Pic}}$ by construction. It is also commutative since the product of ideals is commutative. Let $\pi(I_i) \in \mathcal{C}_{\mathrm{Pic}}$. Then $\pi(I_i)$ is reduced, and $\mathcal{O}_K I_i = I_i$. Therefore, the reduced Arakelov divisor $\pi(I_i)$ is the output of Algorithm 4.3.8 with input $\pi(I_i\mathcal{O}_K)$. This means that $\pi(I_i)$ is the output of Algorithm 4.3.32 with input $\pi(I_i), \pi(\mathcal{O}_K)$. Thus, we get

$$\pi(I_i) \circledast \pi(\mathcal{O}_K) = \pi(I_i).$$

Next, we have the integers $a_i = N_{\mathcal{O}_K}(I_i^{-1})$ and $b \in \mathcal{A}_{a_i}$. We know that $\pi(I_i)$ is reduced. Hence, by Proposition 7.2 in [Sch08], we have that $N_{\mathcal{O}_K}(I_i^{-1}) < \sqrt{d}$. So we have $a_i < \sqrt{d}$, which means that $b \in [\sqrt{d}-2a_i, \sqrt{d}]$. Since a_i, b are integers and $\sqrt{d}$ is non-rational, the integer b cannot equal the bounds of this interval. Equivalently, we have

$$\sqrt{d} - 2a_i < b < \sqrt{d} \quad \Longrightarrow\ -2a_i < b - \sqrt{d} < 0 \quad \Longrightarrow\ -1 < \frac{b-\sqrt{d}}{2a_i} < 0.$$

Then these inequalities say that $-1 < \sigma(x) < 0$. We also have $b_i \in \mathcal{A}_{a-i}$, and so

$$2a_i - \sqrt{d} < b_i < \sqrt{d} \quad \Longrightarrow\ -\sqrt{d} < -b_i < \sqrt{d} - 2a_i.$$

Since $b \equiv -b_i \bmod 2a$ and $b > \sqrt{d} - 2a_i$, we have $b \geq -b_i + 2_i a$. Since $-b_> - \sqrt{d}$, this also says that $b > 2a_i - \sqrt{d}$. This is equivalent to saying that $x > 1$.

So we have $J = \mathbb{Z} + x\mathbb{Z}$ such that $-1 < \sigma(x) < 0$ and $x > 1$. Proposition 4.3.4 (rather its proof for Statement (iii.) implies Statement (ii.)) shows that these conditions are sufficient to show that $1 \in J$ is minimal. Hence, the Arakelov divisor $\pi(J)$ is reduced.

We know that $\frac{1}{2}(b_i + b) = ka_i$ for some $k \in \mathbb{Z}$. Therefore, we have $\gcd(a_i, \frac{1}{2}(b_i + b)) = a_i$. Using Proposition 4.3.3, we get

$$I_i J = \frac{1}{a_i}\left(\mathbb{Z} + \left(\frac{b' + \sqrt{d}}{2}\right)\mathbb{Z}\right)$$

with $b' \equiv b_i \bmod 2$. Using Remark 4.3.31, we know that if $b_0 = 0$, then $b_i \equiv 0 \bmod 2$, and if $b_0 = 1$, then $b_i \equiv 1 \bmod 2$. So the same holds for b'. Hence, we see that $I_i J = \frac{1}{a}\mathcal{O}_K$. Therefore, the fractional ideal J is principal since I_i is principal. Since $\pi(J)$ is reduced, and $\mathcal{C}_{\mathrm{Pic}}$ is a complete list of reduced Arakelov divisors ideal equivalent to $\pi(\mathcal{O}_K)$, we must have $\pi(J) \in \mathcal{C}_{\mathrm{Pic}}$.

Now we can apply $\circledast$ to $\pi(I_i)$ and $\pi(J)$. To this end, we use Algorithm 4.3.32. Steps (i.) and (ii.) of this algorithm are already done. So we only have to apply Algorithm 4.3.8 to $\pi(I_i I)$. In step (ii.) of Algorithm 4.3.8, we need to take $\alpha = a_i^{-1}$. Thus, we obtain $I' = a_i I_i J = \mathcal{O}_K$ in step (iii.). Since $1 \in \mathcal{O}_K$ is minimal, we return $\pi(\mathcal{O}_K)$ in step (iv.). As a result of this, we get that $\pi(I_i) \circledast \pi(J) = \pi(\mathcal{O}_K)$. □

Remark 4.3.39. Throughout this section, we will denote the inverse of $\pi(I_i) \in \mathcal{C}_{\mathrm{Pic}}$ with respect to $\circledast$ by $\pi(I_i)^{-1}$. Note that this is not necessarily equal to the additive inverse $-\pi(I_i)$ in Div_K.

Note that with the notation of Remark 4.3.34 and the proof of Proposition 4.3.38, we have $\mathcal{O}_K = (a_i x_D)^{-1} I_i J$. In this case, we have $x_D = 1$. Using the same remark, we see that

$$\delta_{\mathrm{Pic}}(\pi(I_i J), \pi(\mathcal{O}_K)) = \frac{1}{2}\log\left|\frac{x_D}{\sigma(x_D)}\right|_\infty = 0.$$

This essentially comes down to saying

$$\delta_{\mathrm{Pic}}(\pi(I_i) + \pi(I_i)^{-1}, \pi(\mathcal{O}_K)) = 0. \qquad \blacklozenge$$

Proposition 4.3.38 tells us that if the associative law holds, the Arakelov infrastructure is an abelian group. So let us investigate the associative law.

Take $\pi(I) = \pi(\mathcal{O}_K)$, $k = 0$, and $l = i$ in Corollary 4.3.26. We have $\theta_0 = 1$, so for any $\pi(I_i) \in \mathcal{C}_{\mathrm{Pic}}$ we get

$$\delta_{\mathrm{Pic}}\left(\pi(\mathcal{O}_K), \pi(I_i)\right) = \delta_{\mathrm{Pic}}\left(\pi(\mathcal{O}_K), \rho^i(\pi(\mathcal{O}_K))\right) = \frac{1}{2}\log\left|\frac{\sigma(\theta_0)\theta_i}{\theta_0\sigma(\theta_i)}\right|_\infty = \frac{1}{2}\log\left|\frac{\theta_i}{\sigma(\theta_i)}\right|_\infty \in [0, R_K),$$

where the interval inclusion follows from Corollary 4.3.26 as well. It allows us to define the following function.

Definition 4.3.40. Consider the function $\delta^0_{\mathrm{Pic}} \colon \mathcal{C}_{\mathrm{Pic}} \to [0, R_K)$ given by

$$\delta^0_{\mathrm{Pic}}(\pi(I_i)) := \frac{1}{2}\log\left|\frac{\theta_i}{\sigma(\theta_i)}\right|_\infty.$$

Proposition 4.3.41. The function δ^0_{Pic} is injective.

Proof. If $\#\mathcal{C}_{\mathrm{Pic}} = 1$, the statement is true. So we can assume that $\#\mathcal{C}_{\mathrm{Pic}} \in \mathbb{Z}_{>1}$. Equivalently, we can assume that $\mathrm{ord}(\pi(\mathcal{O}_K)) \in \mathbb{Z}_{>1}$. Suppose that for $\pi(I_i), \pi(I_j) \in \mathcal{C}_{\mathrm{Pic}}$, we have $\delta^0_{\mathrm{Pic}}(\pi(I_i)) = \delta^0_{\mathrm{Pic}}(\pi(I_j))$. Without loss of generality, we can assume that $i > j$. By Definition 4.3.40, we have

$$\frac{1}{2}\log\left|\frac{\theta_i}{\sigma(\theta_i)}\right|_\infty = \frac{1}{2}\log\left|\frac{\theta_j}{\sigma(\theta_j)}\right|_\infty.$$

Set $x := \theta_i\theta_j^{-1}$. Then we get

$$\log\left|\frac{x}{\sigma(x)}\right|_\infty = 0 \quad \Longrightarrow \quad \left|\frac{x}{\sigma(x)}\right|_\infty = 1 \quad \Longrightarrow \ |x|_\infty = |\sigma(x)|_\infty.$$

For any $k \in \mathbb{Z}_{>0}$, we have the formula

$$\theta_k = \prod_{l=0}^{k-1} \xi_l,$$

with $0 < \sigma(\xi_l) < -1$ and $\xi_l > 1$ for all integers $0 \leq l \leq k-1$. Since $i > j$, we have

$$x = \theta_i\theta_j^{-1} = \prod_{l=j}^{i-1} \xi_l.$$

So we get $|x|_\infty > 1$. Moreover, we have $0 < \sigma(\xi_l) < -1$, so $|\sigma(x)|_\infty < 1$. Consequently, it is impossible to have $|x|_\infty = |\sigma(x)|_\infty$. We reach a contradiction. Therefore, we have shown the injectivity of the function δ^0_{Pic}. □

Proposition 4.3.42. Let $\pi(I_i), \pi(I_j) \in \mathcal{C}_{\mathrm{Pic}}$, and set $\pi(I_k) := \pi(I_i) \circledast \pi(I_j)$. Then

$$\delta^0_{\mathrm{Pic}}(\pi(I_k)) \equiv \delta^0_{\mathrm{Pic}}(\pi(I_i)) + \delta^0_{\mathrm{Pic}}(\pi(I_j)) + \delta_{\mathrm{Pic}}(\pi(I_iI_j), \pi(I_k)) \bmod R_K.$$

In particular, one has $\delta^0_{\mathrm{Pic}}(\pi(I_i)^{-1}) \equiv -\delta^0_{\mathrm{Pic}}(\pi(I_i)) \bmod R_K$.

Proof. In Remark 4.3.34, we saw that $I_k = tx_D^{-1}I_iI_j$. Equivalently, we obtain

$$\theta_k^{-1}\mathcal{O}_K = tx_D^{-1}\theta_i^{-1}\theta_j^{-1}\mathcal{O}_K.$$

Consequently, there exists some $a \in \mathcal{O}_K^*$ such that $\theta_k = at^{-1}x_D\theta_i\theta_j$. Now, using Definition 4.3.40, we have

$$\begin{aligned}
\delta^0_{\mathrm{Pic}}(\pi(I_k)) &= \frac{1}{2}\log\left|\frac{\theta_k}{\sigma(\theta_k)}\right|_\infty \\
&= \frac{1}{2}\log\left|\frac{at^{-1}x_D\theta_i\theta_j}{\sigma(at^{-1}x_D\theta_i\theta_j)}\right|_\infty \\
&= \frac{1}{2}\log\left|\frac{\theta_i}{\sigma(\theta_i)}\right|_\infty + \frac{1}{2}\log\left|\frac{\theta_j}{\sigma(\theta_j)}\right|_\infty + \frac{1}{2}\log\left|\frac{x_D}{\sigma(x_D)}\right|_\infty + \frac{1}{2}\log\left|\frac{a}{\sigma(a)}\right|_\infty \\
&= \delta^0_{\mathrm{Pic}}(\pi(I_i)) + \delta^0_{\mathrm{Pic}}(\pi(I_j)) + \delta_{\mathrm{Pic}}(\pi(I_iI_j), \pi(I_k)) + \frac{1}{2}\log\left|\frac{a}{\sigma(a)}\right|_\infty,
\end{aligned}$$

where we used Remark 4.3.34 for the distance $\delta_{\mathrm{Pic}}(\pi(I_iI_j), \pi(I_k))$. Since $a \in \mathcal{O}_K^*$, we know that $a = \pm\varepsilon_K^l$ for some $l \in \mathbb{Z}$. We obtain that $\frac{1}{2}\log\left|\frac{a}{\sigma(a)}\right|_\infty = lR_K$. We conclude that

$$\delta^0_{\mathrm{Pic}}(\pi(I_k)) \equiv \delta^0_{\mathrm{Pic}}(\pi(I_i)) + \delta^0_{\mathrm{Pic}}(\pi(I_j)) + \delta_{\mathrm{Pic}}(\pi(I_iI_j), \pi(I_k)) \bmod R_K.$$

For any $\pi(I_i) \in \mathcal{C}_{\mathrm{Pic}}$, we have $\pi(I_i) \circledast \pi(I_i)^{-1} = \pi(\mathcal{O}_K)$. Then

$$\delta^0_{\mathrm{Pic}}(\pi(\mathcal{O}_K)) \equiv \delta^0_{\mathrm{Pic}}(\pi(I_i)) + \delta^0_{\mathrm{Pic}}(\pi(I_i)^{-1}) + \delta_{\mathrm{Pic}}(\pi(I_i) + \pi(I_i)^{-1}, \pi(\mathcal{O}_K)) \bmod R_K.$$

We know $\delta^0_{\mathrm{Pic}}(\pi(\mathcal{O}_K)) = 0$ by Proposition 4.3.24 (i.). By Remark 4.3.39, we have

$$\delta_{\mathrm{Pic}}(\pi(I_i) + \pi(I_i)^{-1}, \pi(\mathcal{O}_K)) = 0.$$

Hence, we obtain that

$$\delta^0_{\mathrm{Pic}}(\pi(I_i)^{-1}) \equiv -\delta^0_{\mathrm{Pic}}(\pi(I_i)) \bmod R_K. \qquad \square$$

Proposition 4.3.42 tells us that δ^0_{Pic} is not additive with respect to the operation $\circledast$. This prevents $\circledast$ from being associative. Namely, for any arbitrary $\pi(I_i), \pi(I_j), \pi(I_k) \in \mathcal{C}_{\mathrm{Pic}}$ we have

$$\delta^0_{\mathrm{Pic}}((\pi(I_i) \circledast \pi(I_j)) \circledast \pi(I_k)) \equiv \delta^0_{\mathrm{Pic}}(\pi(I_i)) + \delta^0_{\mathrm{Pic}}(\pi(I_j)) + \delta^0_{\mathrm{Pic}}(\pi(I_i)) + \kappa_1 \bmod R_K,$$

and

$$\delta^0_{\mathrm{Pic}}(\pi(I_i) \circledast (\pi(I_j) \circledast \pi(I_k))) \equiv \delta^0_{\mathrm{Pic}}(\pi(I_i)) + \delta^0_{\mathrm{Pic}}(\pi(I_j)) + \delta^0_{\mathrm{Pic}}(\pi(I_i)) + \kappa_2 \bmod R_K,$$

for some error terms $\kappa_1, \kappa_2 \in \mathbb{R}$. The error terms depend on the distance treated in Conjecture 4.3.35. This distance is difficult to control and behaves differently among the elements in $\mathcal{C}_{\mathrm{Pic}}$. So it might happen that $\kappa_1 \not\equiv \kappa_2 \bmod R_K$. In that case, one has $\delta^0_{\mathrm{Pic}}((\pi(I_i) \circledast \pi(I_j)) \circledast \pi(I_k)) \neq \delta^0_{\mathrm{Pic}}(\pi(I_i) \circledast (\pi(I_j) \circledast \pi(I_k)))$. By Proposition 4.3.41, we know that δ^0_{Pic} is injective. Thus, this would imply that

$$(\pi(I_i) \circledast \pi(I_j)) \circledast \pi(I_k) \neq \pi(I_i) \circledast (\pi(I_j) \circledast \pi(I_k)).$$

This means that the associative law does not need to hold for $\circledast$. This prevents $\mathcal{C}_{\mathrm{Pic}}$ from being an abelian group.

In conclusion, the Arakelov infrastructure $\mathcal{C}_{\mathrm{Pic}}$ is not an abelian group with respect to the operation $\circledast$. However, since only the associative law fails to hold, we can say that it has a group-like structure. This is also what we saw in Section 1.3 for the infrastructure $\mathcal{C}$ with the operation $*$. In that case, we could use the Baby-Step Giant-Step Algorithm to obtain Algorithm 1.3.13. Can we do this here as well?

Before we dive into such an algorithm, let us summarize and visualize what we have done in this section. We started by investigating the principal Arakelov cycle $\mathcal{C}_{\mathrm{Pic}}$ of K (see 58). Thereafter, we defined the operation $\circledast$ on $\mathcal{C}_{\mathrm{Pic}}$ induced from Algorithm 4.3.32. We saw that $\circledast$ satisfies all group properties on $\mathcal{C}_{\mathrm{Pic}}$ except for

the associative law. To show this, we made use of a distance function $\delta^0_{\mathrm{Pic}}\colon \mathcal{C}_{\mathrm{Pic}} \to [0, R_K)$ (see Definition 4.3.40). Moreover, this function is injective (see Proposition 4.3.41). In Remark 4.3.29, we saw that the 'entire distance' of the principal Arakelov cycle equals the regulator. Together with the function δ^0_{Pic} it makes therefore sense to visualize $\mathcal{C}_{\mathrm{Pic}}$ on a circle of circumference R_K. Then any point of $\pi(I_i) \in \mathcal{C}_{\mathrm{Pic}}$ is visualized on the circle by its distance $\delta^0_{\mathrm{Pic}}(\pi(I_i)) \in [0, R_K)$. We place the unit element $\pi(\mathcal{O}_K) = \pi(I_0)$ of $\mathcal{C}_{\mathrm{Pic}}$ at the top of the circle and move clockwise along the circle (see Figure 1).

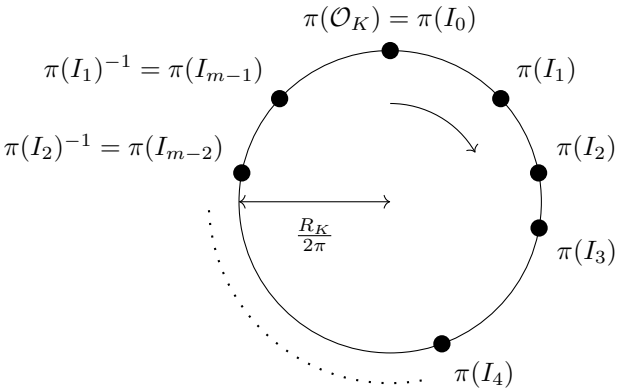

Figure 1: *A visualization of $\mathcal{C}_{\mathrm{Pic}}$ on a circle of circumference R_K.*

From Proposition 4.3.42, we concluded that for any $\pi(I_i) \in \mathcal{C}_{\mathrm{Pic}}$ we have

$$\delta^0_{\mathrm{Pic}}(\pi(I_i)^{-1}) \equiv -\delta^0_{\mathrm{Pic}}(\pi(I_i)) \bmod R_K.$$

With the visualization of $\mathcal{C}_{\mathrm{Pic}}$ on a circle of circumference R_K, we may conclude that the inverse of an element is always depicted on the opposite on the circle with respect to a vertical line splitting the circle into two equal semicircles. Specifically, we have $\pi(I_i)^{-1} = \pi(I_{m-i})$ for all $0 \leq i \leq m-1$. This is also visualized in Figure 1.

Now, let us look into the analogue of Algorithm 1.3.13.

Algorithm 4.3.43. (Infrastructure Algorithm using Arakelov Theory)
Input: Any fundamental discriminant $d \in \mathbb{Z}_{>0}$.
Output: The regulator R_K of the number field $K = \mathbb{Q}(\sqrt{d})$.

i.) **Baby-Steps**
Set $I_0 := \mathcal{O}_K$, and compute

$$\mathcal{A} := \left\{ \left(\pi(I_k), \delta^0_{\mathrm{Pic}}(\pi(I_k)\right) : 0 \leq k \leq j+1 \right\},$$

where $\pi(I_k) = \pi(\theta_k^{-1}\mathcal{O}_K) = \rho^k(\pi(I_0))$ for all $0 \leq k \leq j+1$. Take $j \in \mathbb{Z}_{\geq 0}$ such that

$$\delta^0_{\mathrm{Pic}}(\pi(I_j)) < \log(d) \leq \delta^0_{\mathrm{Pic}}(\pi(I_{j+1})). \tag{59}$$

ii.) Compute

$$\mathcal{A}' := \left\{ \left(\pi(I_k)^{-1}, -\delta^0_{\mathrm{Pic}}(\pi(I_k)\right) : \pi(I_k) \in \mathcal{A} \right\}.$$

Equivalently, compute the inverses of the reduced Arakelov divisors from $\mathcal{A}$ with respect to $\circledast$. Set $\mathcal{B} := \mathcal{A} \cup \mathcal{A}'$.

iii.) If there exists a $\left(\pi(I_k), \delta^0_{\mathrm{Pic}}(\pi(I_k)\right) \in \mathcal{A}$ such that $\pi(I_k) = \pi(I_k)^{-1}$, then return $R_K = 2\delta^0_{\mathrm{Pic}}(\pi(I_k))$.

iv.) Set $i = 0$ and $J_i := I_j$.

v.) **Giant-Steps**
Set $i = i + 1$ and compute $\big(\pi(J_i), \delta^0_{\mathrm{Pic}}(\pi(J_i)\big)$, where $\pi(J_i) := \pi(J_{i-1}) \circledast \pi(I_j)$. To compute $\delta^0_{\mathrm{Pic}}(\pi(J_i))$ do not use Definition 4.3.42, but use the formula

$$\delta^0_{\mathrm{Pic}}(\pi(J_i)) := \delta^0_{\mathrm{Pic}}(\pi(J_{i-1})) + \delta^0_{\mathrm{Pic}}(\pi(I_j)) + \delta_{\mathrm{Pic}}(\pi(J_{i-1}I_j), \pi(J_i)), \tag{60}$$

where $\delta_{\mathrm{Pic}}(\pi(J_{i-1}I_j), \pi(J_i))$ is computed by the formula of Remark 4.3.34.

vi.) If $\big(\pi(J_i), \delta^0_{\mathrm{Pic}}(\pi(J_i)\big) \in \mathcal{B}$, find $\big(\pi(I_k), \delta^0_{\mathrm{Pic}}(\pi(I_k)\big) \in \mathcal{B}$ such that $\pi(J_i) = \pi(I_k)$. Then return

$$R_K = \delta^0_{\mathrm{Pic}}(\pi(J_i)) - \delta^0_{\mathrm{Pic}}(\pi(I_k)).$$

Else, return to step (v.).

Theorem 4.3.44. Under the assumptions of Conjecture 4.3.35, Algorithm 4.3.43 is correct and terminates in a finite number of steps.

Proof. Step (i.) and (ii.) are just finitely many computations. Moreover, one can use Definition 4.3.40 to compute $\delta^0_{\mathrm{Pic}}(\pi(I_k))$ in step (i.), and Proposition 4.3.38 to compute the inverses in step (ii.). If there exists a $\big(\pi(I_k), \delta^0_{\mathrm{Pic}}(\pi(I_k)\big) \in \mathcal{A}$ such that $\pi(I_k) = \pi(I_k)^{-1}$, then by Proposition 4.3.42, we find

$$-\delta^0_{\mathrm{Pic}}(\pi(I_k)) \equiv \delta^0_{\mathrm{Pic}}(\pi(I_k)^{-1}) \equiv \delta^0_{\mathrm{Pic}}(\pi(I_k)) \bmod R_K.$$

It follows that $2\delta^0_{\mathrm{Pic}}(\pi(I_k)) = lR_K$ for some $l \in \mathbb{Z}$. Since Definition 4.3.42 tells us that $\delta^0_{\mathrm{Pic}}(\pi(I_k)) \in [0, R_K)$, we actually must have $2\delta^0_{\mathrm{Pic}}(\pi(I_k)) = R_K$. Hence, the correctness of step (iii.) has been proven. It remains to show that there exists some $i \in \mathbb{Z}_{>0}$ such that the giant-step $\big(\pi(J_i), \delta^0_{\mathrm{Pic}}(\pi(J_i)\big)$ is included in $\mathcal{B}$. The distance traveled by a single giant-step is given by

$$\delta^0_{\mathrm{Pic}}(\pi(J_i)) - \delta^0_{\mathrm{Pic}}(\pi(J_{i-1})) \tag{61}$$

for some $i \in \mathbb{Z}_{\geq 0}$. Using Equation (60), we can see that the value of (61) equals

$$\delta^0_{\mathrm{Pic}}(\pi(I_j)) + \delta_{\mathrm{Pic}}(\pi(J_{i-1}I_j), \pi(J_i)).$$

By the choice of $j \in \mathbb{Z}_{\geq 0}$, we know that $\delta^0_{\mathrm{Pic}}(\pi(I_j)) < \log(d)$. By Conjecture 4.3.35, we know that

$$|\delta_{\mathrm{Pic}}(\pi(J_{i-1}I_j), \pi(J_i))|_\infty < \log(d),$$

where the formula of Remark 4.3.34 is used to calculate $\delta_{\mathrm{Pic}}(\pi(J_{i-1}I_j), \pi(J_i))$. Consequently, we get that

$$\delta^0_{\mathrm{Pic}}(\pi(I_j)) + \delta_{\mathrm{Pic}}(\pi(J_{i-1}I_j), \pi(J_i)) < 2\log(d). \tag{62}$$

This means that the distance traveled by a single giant-step is less than $2\log(d)$. The entire distance covered by $\mathcal{A}$ is bigger than $\log(d)$ (see step (i.)). Thus, the same is true for $\mathcal{A}'$. So the set $\mathcal{B}$ covers a complete distance of at least $2\log(d)$. Hence, a single giant-step cannot cross $\mathcal{B}$ completely. As R_K is a finite number, eventually we must find a giant-step in $\mathcal{B}$. Therefore, the algorithm terminates in a finite number of steps. Given such a collision, we have two equal reduced Arakelov divisors, with different distances. They are different by the values of δ^0_{Pic} assigned in this algorithm. Specifically, the values from step (v.). Since the distances are unique modulo R_K, this means that their distance is a multiple of the regulator. But we do hit $\mathcal{B}$ with the first rotation, so we have the regulator itself. This shows the correctness of step (vi.). We conclude that the algorithm is correct and terminates in a finite number of steps. □

Remark 4.3.45. The choice of $j \in \mathbb{Z}_{\geq 0}$ in inequalities (59) depends on the bound $\log(d)$ in Conjecture 4.3.35. It ensures that the baby-steps set $\mathcal{A}$ is big enough for a collision with a giant-step (see inequality (62)). Say, the conjecture is verified with a different bound $C \in \mathbb{R}_{>0}$. Then one can replace $\log(d)$ by C in inequalities (59), and the algorithm would still terminate. ♦

The algorithm is rather abstract, so let us try to visualize it. In step (i.) of the algorithm, we create a set $\mathcal{A}$ by baby-steps. We cover at least a distance more than $\log(d)$. This is visualized in the left circle of Figure 2. Thereafter, the inverses of the reduced Arakelov divisors in $\mathcal{A}$ are computed. In that way, we cover the same distance on the other side of the circle. This is visualized in the right circle of Figure 2.

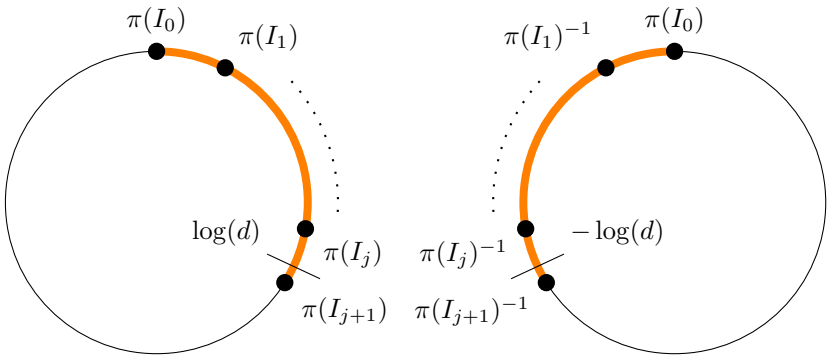

Figure 2: *A visualization of the baby-steps (left picture) together with its inverses (right picture) of Algorithm 4.3.43, covering a total distance (orange arcs) of at least* $2\log(d)$.

Now, step (iii.) of the algorithm occurs when the baby-steps cover half of the circle and there exists a reduced Arakelov divisor at the bottom of the circle. This is visualized in Figure 3. Lastly, the visualization of the giant-steps and a collision is given in Figure 4.

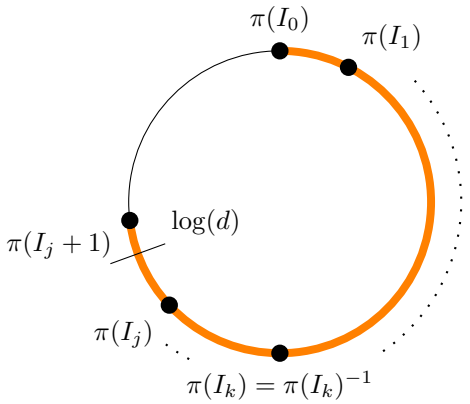

Figure 3: *A visualization of the occurrence of step (iii.) of Algorithm 4.3.43*

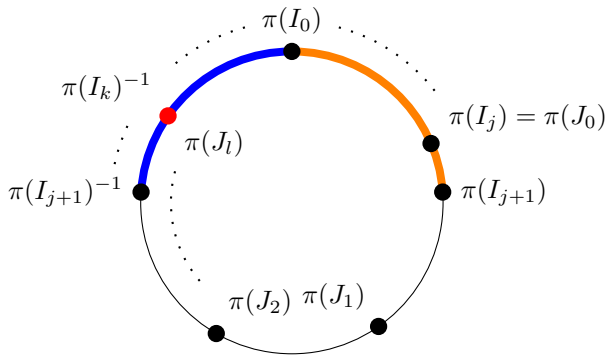

Figure 4: *A visualization of the baby-steps covering a certain distance (orange arc) together with their inverses (blue arc). Furthermore, two giant-steps $\pi(J_1), \pi(J_2)$ are depicted. Moreover, a collision between the giant-step $\pi(J_l)$ and the inverse of baby-step $\pi(I_k)$ for some $k, l \in \mathbb{Z}_{>0}$ is shown with a red bullet.*

5 Arakelov Theory for Rings of S-Integers

The goal of this chapter is to create a framework for Arakelov theory for the rings of S-integers. We do this by transferring the definitions of Chapter 4 in a reasonable way to the rings of S-integers. Furthermore, we will examine some properties of this theory. All results in this chapter are self-written. However, the ones from Section 5.2.3 are heavily based on ideas from existing literature. But we will come back to this in this section. Throughout this section, let K denote any number field and S a finite set of finite places.

5.1 Arakelov S-Divisors

In Definition 4.1.1, we have seen the definition of an Arakelov divisor of K. Simply said, an Arakelov divisor is a finite formal sum over the places of K. The finite places of K are in bijection with the non-zero prime ideals of $\mathcal{O}_K$. In Proposition 3.2.1, we have seen that the prime ideals of $\mathcal{O}_{K,S}$ are in bijection with the prime ideals of $\mathcal{O}_K$ that are not contained in S. Hence, we propose the following definition.

Definition 5.1.1. An *Arakelov S-divisor* D of K is given by a finite formal sum

$$D = \sum_{\mathfrak{p} \notin S} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\sigma \in \Sigma_K^\infty} x_\sigma \sigma, \qquad n_{\mathfrak{p}} \in \mathbb{Z}, x_\sigma \in \mathbb{R}.$$

The set of Arakelov S-divisors of K is denoted by $\mathrm{Div}_{K,S}$.

Notice that the set $\mathrm{Div}_{K,S}$ attains an abelian group structure, where the group operation is given by the addition of formal sums. The unit element is given by the zero Arakelov S-divisor, that is, the Arakelov S-divisor for which all coefficients are zero. If we take $S = \emptyset$, we recover Definition 4.1.1. In this original setting, we call them Arakelov divisors, instead of Arakelov $\emptyset$-divisors. Moreover, the set of Arakelov divisors is denoted by Div_K instead of $\mathrm{Div}_{K,\emptyset}$. The following result is an immediate consequence of the definition.

Proposition 5.1.2. If $S \subseteq S'$ are finite sets of $\mathfrak{P}_K^0$, then $\mathrm{Div}_{K,S'} \subseteq \mathrm{Div}_{K,S}$. Moreover, the set $\mathrm{Div}_{K,S'}$ is a subgroup of $\mathrm{Div}_{K,S}$.

Let $\langle S \rangle$ denote the subgroup of Div_K generated by the Arakelov divisors $\mathfrak{p}$ for $\mathfrak{p} \in S$.

Proposition 5.1.3. There exists a group isomorphism $\mathrm{Div}_{K,S} \cong \mathrm{Div}_K / \langle S \rangle$.

Proof. Consider the map $\varphi_S \colon \mathrm{Div}_K \to \mathrm{Div}_{K,S}$ that given an Arakelov divisor D written as

$$D = \sum_{\mathfrak{p} \in \mathfrak{P}_K^0} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\sigma \in \Sigma_K^\infty} x_\sigma \sigma,$$

sends it to

$$\varphi_S(D) := \sum_{\mathfrak{p} \notin S} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\sigma \in \Sigma_K^\infty} x_\sigma \sigma.$$

By the definition we have $\varphi_S(D) \in \mathrm{Div}_{K,S}$. Since Div_K and $\mathrm{Div}_{K,S}$ have the same group structure, it follows that φ_S is a group homomorphism. Surjectivity of φ_S follows from the fact that $\mathrm{Div}_{K,S} \subseteq \mathrm{Div}_K$ (see Proposition 5.1.2). Finally, we have $D \in \ker(\varphi_S)$ if and only if $n_{\mathfrak{p}} = 0$ for all $\mathfrak{p} \notin S$ and $x_\sigma = 0$ for all $\sigma \in \Sigma_K^\infty$. Therefore, we know $D \in \ker(\varphi_S)$ if and only if D is of the form $D = \sum_{\mathfrak{p} \in S} n_{\mathfrak{p}} \mathfrak{p}$. This shows that $\ker(\varphi_S) = \langle S \rangle$. Therefore, the group homomorphism φ_S induces a group isomorphism $\mathrm{Div}_{K,S} \cong \mathrm{Div}_K / \langle S \rangle$. □

In Definition 4.1.2, we have seen principal Arakelov divisors. Specifically, for a principal Arakelov divisor $\mathrm{div}(x)$ for $x \in K^*$, we take the coefficients at $\mathfrak{p} \in \mathfrak{P}_K^0$ to be $\mathrm{ord}_{\mathfrak{p}}(x)$. So, if we would like to define a principal Arakelov S-divisor for $x \in K^*$, it is reasonable to say we take the coefficients at $\mathfrak{p} \notin S$ to be $\mathrm{ord}_{\mathfrak{p}\mathcal{O}_{K,S}}(x)$. However, in Proposition 3.2.2 we saw that for any $x \in K^*$ one has $\mathrm{ord}_{\mathfrak{p}}(x) = \mathrm{ord}_{\mathfrak{p}\mathcal{O}_{K,S}}(x)$ for all $\mathfrak{p} \notin S$. Therefore, we propose the following definition.

Definition 5.1.4. A *principal Arakelov S-divisor* of K is defined by

$$\operatorname{div}_S(x) := \sum_{\mathfrak{p} \notin S} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\sigma \in \Sigma_K^\infty} x_\sigma \sigma, \qquad n_{\mathfrak{p}} = \operatorname{ord}_{\mathfrak{p}}(x), x_\sigma = -\log |x|_\sigma,$$

for some $x \in K^*$. The set of principal Arakelov S-divisors of K is denoted by $\operatorname{Prin}_{K,S}$.

If $S = \emptyset$, we recover Definition 4.1.2. In this original setting, we just call them principal Arakelov divisors, instead of principal Arakelov $\emptyset$-divisors. Moreover, the set of principal Arakelov divisors is denoted by Prin_K instead of $\operatorname{Prin}_{K,\emptyset}$. Furthermore, we simply write div instead of $\operatorname{div}_\emptyset$. Notice using the group homomorphism φ_S of the proof of Proposition 5.1.3, we have

$$\varphi_S(\operatorname{div}(x)) = \operatorname{div}_S(x). \tag{63}$$

Proposition 5.1.5. The set $\operatorname{Prin}_{K,S}$ forms a subgroup of $\operatorname{Div}_{K,S}$.

Proof. For any $x \in K^*$, we know that $\operatorname{ord}_{\mathfrak{p}}(x)$ can only be non-zero at finitely many $\mathfrak{p} \in \mathfrak{P}_K^0$. Otherwise, the fractional ideal $x\mathcal{O}_K$ has infinitely many prime ideals in its factorization, which is impossible. Together with the fact that there are only finitely many infinite places, we have that $\operatorname{div}_S(x)$ must be a finite sum. Therefore, we have that $\operatorname{Prin}_{K,S} \subseteq \operatorname{Div}_{K,S}$.

The zero Arakelov S-divisor is contained in $\operatorname{Prin}_{K,S}$ by $\operatorname{div}_S(1) = 0$. Now, for any $x \in K^*$, we have $\operatorname{ord}_{\mathfrak{p}}(x^{-1}) = -\operatorname{ord}_{\mathfrak{p}}(x)$ and $\log |x^{-1}|_\sigma = -\log |x|_\sigma$. Therefore, for any $\operatorname{div}_S(x) \in \operatorname{Prin}_{K,S}$, we have the inverse $\operatorname{div}_S(x^{-1}) \in \operatorname{Prin}_{K,S}$, since their sum equals zero. For any $x, y \in K^*$, we have $\operatorname{ord}_{\mathfrak{p}}(xy) = \operatorname{ord}_{\mathfrak{p}}(x) + \operatorname{ord}_{\mathfrak{p}}(y)$ and $\log |xy|_\sigma = \log |x|_\sigma + \log |y|_\sigma$. Then we have

$$\operatorname{div}_S(xy) = \operatorname{div}_S(x) + \operatorname{div}_S(y).$$

Therefore, for any $\operatorname{div}_S(x), \operatorname{div}_S(y) \in \operatorname{Prin}_{K,S}$, we have $\operatorname{div}_S(x) + \operatorname{div}_S(y) = \operatorname{div}_S(xy) \in \operatorname{Prin}_{K,S}$. It follows that $\operatorname{Prin}_{K,S} \subseteq \operatorname{Div}_{K,S}$ forms a subgroup of $\operatorname{Div}_{K,S}$. □

By Proposition 5.1.5, it makes sense to take the quotient group of $\operatorname{Div}_{K,S}$ by its subgroup of principal Arakelov S-divisors.

Definition 5.1.6. The quotient group $\operatorname{Div}_{K,S} / \operatorname{Prin}_{K,S}$ is called the *Arakelov S-class group* of K and is denoted by $\operatorname{Pic}_{K,S}$.

If $S = \emptyset$, we recover Pic_K from Definition 4.1.3. In this case, we write Pic_K instead of $\operatorname{Pic}_{K,\emptyset}$ and call it the Arakelov class group instead of the Arakelov $\emptyset$-class group. Throughout this thesis, for $D \in \operatorname{Div}_{K,S}$ we denote its equivalence class in $\operatorname{Pic}_{K,S}$ by $[D]$.

Definition 5.1.7. Two Arakelov S-divisors $D, D' \in \operatorname{Div}_{K,S}$ are called *equivalent* if $[D] = [D']$ in $\operatorname{Pic}_{K,S}$. Equivalently, there exists an $x \in K^*$ such that $D - D' = \operatorname{div}_S(x)$.

Remark 5.1.8. In Definition 4.1.7, we have seen the degree-zero-Arakelov class group Pic_K^0. However, there is no natural way of translating the notion of degree to Arakelov S-divisors. With natural we mean that there is not a clear translation to obtain $\operatorname{Prin}_{K,S} \subseteq \operatorname{Div}_{K,S}^0$, if $\operatorname{Div}_{K,S}^0$ would denote the set of Arakelov S-divisors of degree zero.

Looking at the geometric analogue, this becomes maybe more clear. We stated that Pic_K^0 is an analogue of the subgroup of the Picard group of a complete projective curve consisting of divisors with degree zero. What we are doing here, deleting finite places of the number field K, can be seen as deleting points on the projective curve. Deleting points on a projective curve is the same as restricting to an affine subset of the projective curve, i.e. an affine curve. There is no natural notion of the degree of divisors on an affine curve such that the principal divisors have degree zero. Namely, we might be deleting poles or zeroes from a rational function. ♦

Let $\langle [S] \rangle$ denote the subgroup of Pic_K generated by the elements $[\mathfrak{p}] \in \mathrm{Pic}_K$ for $\mathfrak{p} \in S$.

Proposition 5.1.9. There exists a group isomorphism $\mathrm{Pic}_{K,S} \cong \mathrm{Pic}_K / \langle [S] \rangle$.

Proof. Consider the map $\psi_S \colon \mathrm{Pic}_K \to \mathrm{Pic}_{K,S}$ defined by $[D] \mapsto [\varphi_S(D)]$, where φ_S is the group homomorphism from the proof of Proposition 5.1.3. Take $[D], [D'] \in \mathrm{Pic}_K$ such that $[D] = [D']$. This means that there exists some $x \in K^*$ such that $D - D' = \mathrm{div}(x)$. Then using φ_S on both sides, we get

$$\varphi_S(D - D') = \varphi_S(\mathrm{div}(x)) \quad \implies \varphi_S(D) - \varphi_S(D') = \mathrm{div}_S(x),$$

where we used that φ_S is a group homomorphism and Equation (63). This means that $[\varphi_S(D)] = [\varphi_S(D')]$ in $\mathrm{Pic}_{K,S}$. This shows that ψ_S is well-defined. Furthermore, Equation (63) says that ψ_S maps any $[\mathrm{div}(x)]$ to $[\mathrm{div}_S(x)]$. We see that ψ_S sends the unit element of Pic_K to the unit element of $\mathrm{Pic}_{K,S}$. Moreover, since φ_S is a group homomorphism, the map ψ_S is also a group homomorphism. The map ψ_S is surjective since $\mathrm{Div}_{K,S} \subseteq \mathrm{Div}_K$ (see Proposition 5.1.2). If $[D] \in \ker(\psi_S)$ then $[\varphi_S(D)] = [0]$. This says that $\varphi_S(D) \in \mathrm{Prin}_{K,S}$, i.e. there exists an $x \in K^*$ such that

$$\varphi_S(D) = \mathrm{div}_S(x). \tag{64}$$

So write

$$D = \sum_{\mathfrak{p} \in \mathfrak{P}_K^0} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\sigma \in \Sigma_K^\infty} x_\sigma \sigma.$$

Then Equation (64) says that

$$\sum_{\mathfrak{p} \notin S} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\sigma \in \Sigma_K^\infty} x_\sigma \sigma = \mathrm{div}_S(x). \tag{65}$$

Notice that

$$\mathrm{div}_S(x) = \mathrm{div}(x) - \sum_{\mathfrak{p} \in S} \mathrm{ord}_{\mathfrak{p}}(x) \mathfrak{p}. \tag{66}$$

So using Equation (65) and (66), we get

$$\begin{aligned} D &= \sum_{\mathfrak{p} \in \mathfrak{P}_K^0} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\sigma \in \Sigma_K^\infty} x_\sigma \sigma \\ &= \sum_{\mathfrak{p} \in S} n_{\mathfrak{p}} \mathfrak{p} + \left(\sum_{\mathfrak{p} \notin S} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\sigma \in \Sigma_K^\infty} x_\sigma \sigma \right) \\ &= \sum_{\mathfrak{p} \in S} n_{\mathfrak{p}} \mathfrak{p} + \mathrm{div}_S(x) \\ &= \sum_{\mathfrak{p} \in S} n_{\mathfrak{p}} \mathfrak{p} + \mathrm{div}(x) - \sum_{\mathfrak{p} \in S} \mathrm{ord}_{\mathfrak{p}}(x) \mathfrak{p} \\ &= \sum_{\mathfrak{p} \in S} (n_{\mathfrak{p}} - \mathrm{ord}_{\mathfrak{p}}(x)) \mathfrak{p} + \mathrm{div}(x). \end{aligned}$$

Then

$$D - \sum_{\mathfrak{p} \in S} (n_{\mathfrak{p}} - \mathrm{ord}_{\mathfrak{p}}(x)) \mathfrak{p} = \mathrm{div}(x).$$

This shows that $[D] = [\sum_{\mathfrak{p} \in S} (n_{\mathfrak{p}} - \mathrm{ord}_{\mathfrak{p}}(x)) \mathfrak{p}]$ in Pic_K, and so $[D] \in \langle [S] \rangle$. Therefore, we have $\ker(\psi_S) \subseteq \langle [S] \rangle$. Conversely, if $[D] \in \langle [S] \rangle$, then $\psi_S([D]) = [\varphi_S(D)] = [0]$. Hence, we also have that $\langle [S] \rangle \subseteq \ker(\psi_S)$. We obtain $\ker(\psi_S) = \langle [S] \rangle$. Therefore, we conclude that the group homomorphism ψ_S induces a group isomorphism $\mathrm{Pic}_{K,S} \cong \mathrm{Pic}_K / \langle [S] \rangle$. □

Next, we study the structure of $\mathrm{Pic}_{K,S}$ a little bit closer. More precisely, we extend the commutative diagram on page 450 in [Sch08] to the rings of S-integers. Firstly, we can associate a fractional ideal to an Arakelov S-divisor.

Definition 5.1.10. The fractional ideal $I(D)$ of $\mathcal{O}_{K,S}$ *associated* to the Arakelov S-divisor

$$D = \sum_{\mathfrak{p} \notin S} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\sigma \in \Sigma_K^\infty} x_\sigma \sigma, \qquad n_{\mathfrak{p}} \in \mathbb{Z}, x_\sigma \in \mathbb{R},$$

is defined by $I(D) := \prod_{\mathfrak{p} \notin S} (\mathfrak{p}\mathcal{O}_{K,S})^{-n_{\mathfrak{p}}}$.

The map

$$\iota \colon \mathrm{Div}_{K,S} \to \mathrm{Id}_{K,S}, \qquad D \mapsto I(D), \tag{67}$$

is a group homomorphism, i.e. for $D, D' \in \mathrm{Div}_K$ we have

$$I(D + D') = I(D)I(D'). \tag{68}$$

Definition 5.1.11. Consider the map $\pi_S \colon \mathrm{Id}_{K,S} \to \mathrm{Div}_{K,S}$ given by

$$\pi_S(I) := \sum_{\mathfrak{p} \notin S} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\sigma \in \Sigma_K^\infty} \left(\frac{1}{n} \log(N_{\mathcal{O}_{K,S}}(I)) \right) \sigma.$$

for some $I \in \mathrm{Id}_{K,S}$ written as $I = \prod_{\mathfrak{p} \notin S} (\mathfrak{p}\mathcal{O}_{K,S})^{-n_{\mathfrak{p}}}$.

The map π_S is a group homomorphism and a section of ι. If $S = \emptyset$, we recover the group homomorphism π that we have seen in (40). Throughout this thesis, we will use the notation π rather than $\pi_\emptyset$.

In Proposition 1.5.4, we saw that the subgroup $\mu_K \subseteq \mathcal{O}_K^*$, consisting roots of unity of K, is characterized by the elements $a \in \mathcal{O}_K^*$ such that $|a|_\sigma = 1$ for all $\sigma \in \Sigma_K^\infty$. One has $\mathcal{O}_K^* \subseteq \mathcal{O}_{K,S}^*$, and so $\mu_K \subseteq \mathcal{O}_{K,S}^*$. In this case, we do not have such characterization. There might exists $a \in \mathcal{O}_{K,S}^*$ such that $|a|_\sigma = 1$ for all $\sigma \in \Sigma_K^\infty$, but $a \notin \mu_K$.

Example 5.1.12. Let $K = \mathbb{Q}(\sqrt{-7})$. By Equation (5), we know that $\mu_K = \mathcal{O}_K^* = \{\pm 1\}$. Now, consider the element $x := \frac{3+\sqrt{-7}}{4}$ in K. Then

$$|x|_\sigma = \left| \frac{3 + \sqrt{-7}}{4} \right|_\infty = 1.$$

Now, let the factorization of $x\mathcal{O}_K$ of non-zero prime ideals of $\mathcal{O}_K$ be given by

$$x\mathcal{O}_K = \prod_{i=1}^{k} \mathfrak{p}_i^{n_{\mathfrak{p}}}$$

for distinct prime ideals $\mathfrak{p}_i \subseteq \mathcal{O}_K$, $n_{\mathfrak{p}} \in \mathbb{Z}$, and some $k \in \mathbb{Z}_{>0}$. Set $S = \{\mathfrak{p}_i : 1 \leq i \leq k\}$. Then $\mathrm{ord}_{\mathfrak{p}}(x) = 0$ for all $\mathfrak{p} \notin S$. Hence, (24) tells us that $x \in \mathcal{O}_{K,S}^*$. Thus, the element x is a unit of $\mathcal{O}_{K,S}$ and satisfies $|x|_\sigma = 1$ for all $\sigma \in \Sigma_K^\infty$, but is not contained in the group μ_K. ■

Define

$$\mu_{K,S} := \{a \in \mathcal{O}_{K,S}^* : |a|_\sigma = 1 \text{ for all } \sigma \in \Sigma_K^\infty\}.$$

If we take $S = \emptyset$, we recover μ_K. We rather denote this by μ_K than $\mu_{K,\emptyset}$.

In Definition 5.1.4, we have seen the definition of a principal Arakelov S-divisor. This definition induces a map $\mathrm{div}_S \colon K^* \to \mathrm{Div}_{K,S}$ defined by $x \mapsto \mathrm{div}_S(x)$.

Lemma 5.1.13. The map div_S is a group homomorphism, and induces a group isomorphism $K^*/\mu_{K,S} \cong \mathrm{Prin}_{K,S}$.

Proof. By the proof of Proposition 5.1.5, we know that div_S is a group homomorphism. By construction, we know that div_S is surjective if its codomain is restricted to $\mathrm{Prin}_{K,S}$. We know that $\mathrm{ord}_{\mathfrak{p}}(a) = 0$ for all $\mathfrak{p} \notin S$ if and only if $a \in \mathcal{O}_{K,S}^*$ (see (24)). By construction of $\mu_{K,S}$, this means that $\mathrm{div}_S(a) = 0$ if and only if $a \in \mu_{K,S}$. We obtain that $\ker(\mathrm{div}_S) = \mu_{K,S}$. Consequently, the group homomorphism div_S induces a group isomorphism $K^*/\mu_{K,S} \cong \mathrm{Prin}_{K,S}$. □

Definition 5.1.14. For $x \in K^*$, define the tuple $\hat{x} \in \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}_{>0}$ by $\hat{x} := (|x|_\sigma)_{\sigma \in \Sigma_K^\infty}$. Furthermore, for $u = (u_\sigma)_{\sigma \in \Sigma_K^\infty} \in \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}_{>0}$ define $\log(u) := (\log(u_\sigma))_{\sigma \in \Sigma_K^\infty}$.

Let us view $\prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}$ in $\mathrm{Div}_{K,S}$ by being related to the Arakelov S-divisors with zero coefficients at the finite places. The property that $\mathrm{ord}_{\mathfrak{p}}(a) = 0$ for all $\mathfrak{p} \notin S$ and $a \in \mathcal{O}_{K,S}^*$ (see (24)), implies that if we restrict div_S to $\mathcal{O}_{K,S}^*$, the codomain can be restricted to $\prod_{\sigma \in \Sigma_K^\infty} \mathbb{R} \subseteq \mathrm{Div}_{K,S}$. Explicitly, the group homomorphism div_S induces the group homomorphism

$$\tau : \mathcal{O}_{K,S}^* \to \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}, \qquad a \mapsto -\log(\hat{a}).$$

Lemma 5.1.15. The group homomorphism τ has kernel $\mu_{K,S}$.

Proof. Take any $a \in \mathcal{O}_{K,S}^*$. By construction of $\mu_{K,S}$, we know that $\log(\hat{a}) = 0$ if and only if $a \in \mu_{K,S}$. We see that $\ker(\tau) = \mu_K$. □

The cokernel of the group homomorphism τ will be denoted by $T_{K,S}$. Specifically, we have

$$T_{K,S} = \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R} / \{\log(\hat{a}) : a \in \mathcal{O}_{K,S}^*\}. \tag{69}$$

If $S = \emptyset$, we recover T_K from the short exact sequence (38). We will denote it simply by T_K rather than $T_{K,\emptyset}$. Throughout this thesis, for $u \in \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}$ we denote its equivalence class in $T_{K,S}$ by $[u]$.

Next to the group homomorphisms $\iota, \mathrm{div}_S, \tau$ introduced above, we need to construct some more group homomorphisms. Consider the group homomorphisms

$$\lambda \colon K^*/\mu_{K,S} \to \mathrm{P}_{K,S}, \qquad [x] \mapsto x^{-1}\mathcal{O}_{K,S},$$

$$\zeta_S \colon T_{K,S} \to \mathrm{Pic}_{K,S}, \qquad [(x_\sigma)_{\sigma \in \Sigma_K^\infty}] \mapsto [\sum_{\sigma \in \Sigma_K^\infty} x_\sigma \sigma],$$

and

$$\chi \colon \mathrm{Pic}_{K,S} \to \mathrm{Cl}_{K,S}, \qquad [D] \mapsto [I(D)].$$

The reason to take the inverse of x in λ has to do with the communicativeness of the diagram in the next theorem. Furthermore, let

$$\phi_1 \colon \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R} \to T_{K,S}, \qquad \phi_2 \colon \mathrm{Div}_{K,S} \to \mathrm{Pic}_{K,S}, \qquad \phi_3 \colon \mathrm{Id}_{K,S} \to \mathrm{Cl}_{K,S}$$

be the canonical maps. Lastly, let

$$\mathrm{id} \colon \mathcal{O}_{K,S}^*/\mu_{K,S} \to K^*/\mu_{K,S}, \qquad \mathrm{id}_{\mathbb{R}} \colon \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R} \to \mathrm{Div}_K, \qquad \mathrm{id}_{\mathrm{P}} \colon \mathrm{P}_{K,S} \to \mathrm{Id}_{K,S}$$

be the inclusion maps. The fact that these maps are really well-defined group homomorphisms, is either easy to verify or will be proved in the next theorem.

Theorem 5.1.16. The diagram given by

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{O}_{K,S}^*/\mu_{K,S} & \xrightarrow{\mathrm{id}} & K^*/\mu_{K,S} & \xrightarrow{\lambda} & \mathrm{P}_{K,S} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \mathrm{div}_S} & & \downarrow{\scriptstyle \mathrm{id}_{\mathrm{P}}} & & \\
0 & \longrightarrow & \prod_{\sigma\in\Sigma_K^\infty}\mathbb{R} & \xrightarrow{\mathrm{id}_{\mathbb{R}}} & \mathrm{Div}_{K,S} & \xrightarrow{\iota} & \mathrm{Id}_{K,S} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle \phi_2} & & \downarrow{\scriptstyle \phi_3} & & \\
0 & \longrightarrow & T_{K,S} & \xrightarrow{\zeta_S} & \mathrm{Pic}_{K,S} & \xrightarrow{\chi} & \mathrm{Cl}_{K,S} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

is commutative and consists of short exact sequences.

Proof. The exactness of the first column is given by Lemma 5.1.15 and the definition of $T_{K,S}$. The exactness of the second column is given by Lemma 5.1.13, and the definition of the Arakelov S-class group $\mathrm{Pic}_{K,S}$. The exactness of the third column is given by the definition of the class group $\mathrm{Cl}_{K,S}$.

To show exactness for the first row, assume that $[x] = [y]$. Then there exists some $z \in \mu_{K,S}$ such that $xz = y$. Then $y^{-1}\mathcal{O}_{K,S} = x^{-1}z^{-1}\mathcal{O}_{K,S} = x^{-1}\mathcal{O}_{K,S}$ as $z \in \mathcal{O}_{K,S}^*$. Hence, the group homomorphism λ is well-defined. The map is surjective by construction. Its kernel is given by the elements $x \in K^*$ such that $x^{-1}\mathcal{O}_{K,S} = \mathcal{O}_{K,S}$. These are precisely the elements of $\mathcal{O}_{K,S}^*$. Thus, the exactness of the first row follows. To show exactness for the second row, notice that ι is surjective since it admits the section π_S. Furthermore, its kernel is given by the Arakelov S-divisors D such that $I(D) = \mathcal{O}_{K,S}$. Therefore, the coefficients of the finite places for D must equal zero. It follows that $\prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}$ must be its kernel. So the exactness of the second row follows.

We will explain the exactness of the last row a bit more explicitly since this will be used in some other parts of this thesis. So focus on the sequence

$$0 \longrightarrow T_{K,S} \xrightarrow{\zeta_S} \mathrm{Pic}_{K,S} \xrightarrow{\chi} \mathrm{Cl}_{K,S} \longrightarrow 0 \ .$$

Note that this generalizes the short exact sequence (38) of Section 4.1. We have

$$\begin{aligned}
[(x_\sigma)_{\sigma\in\Sigma_K^\infty}] = [(y_\sigma)_{\sigma\in\Sigma_K^\infty}] &\iff (x_\sigma)_{\sigma\in\Sigma_K^\infty} = (y_\sigma - \log|a|_\sigma)_{\sigma\in\Sigma_K^\infty} \text{ for some } a \in \mathcal{O}_{K,S}^* \\
&\iff x_\sigma = y_\sigma - \log|a|_\sigma \text{ for all } \sigma \in \Sigma_K^\infty \text{ and some } a \in \mathcal{O}_{K,S}^* \\
&\iff \sum_{\sigma\in\Sigma_K^\infty} x_\sigma\sigma = \sum_{\sigma\in\Sigma_K^\infty} y_\sigma\sigma - \sum_{\sigma\in\Sigma_K^\infty} \log|a|_\sigma\sigma \text{ for some } a \in \mathcal{O}_{K,S}^* \\
&\iff \sum_{\sigma\in\Sigma_K^\infty} x_\sigma\sigma = \sum_{\sigma\in\Sigma_K^\infty} y_\sigma\sigma + \mathrm{div}_S(a) \text{ for some } a \in \mathcal{O}_{K,S}^* \\
&\iff \left[\sum_{\sigma\in\Sigma_K^\infty} x_\sigma\sigma\right] = \left[\sum_{\sigma\in\Sigma_K^\infty} y_\sigma\sigma\right] .
\end{aligned}$$

Therefore, the map ζ_S is a well-defined injective map. Furthermore, it is a group homomorphism as it respects addition. Consequently, the sequence is exact at $T_{K,S}$.

If $[D] = [D']$ for some $D, D' \in \mathrm{Div}_{K,S}$, then $D = D' + \mathrm{div}_S(x)$ for some $x \in K^*$. Denote the coefficients of the finite places of D, D' by $n_{\mathfrak{p}}, n'_{\mathfrak{p}}$ for all $\mathfrak{p} \notin S$, respectively. Then the equality implies that $n_{\mathfrak{p}} = n'_{\mathfrak{p}} + \mathrm{ord}_{\mathfrak{p}}(x)$

for all $\mathfrak{p} \notin S$. Then we have

$$I(D) = \prod_{\mathfrak{p} \notin S} (\mathfrak{p}\mathcal{O}_{K,S})^{-n_\mathfrak{p}} = \prod_{\mathfrak{p} \notin S} (\mathfrak{p}\mathcal{O}_{K,S})^{-n'_\mathfrak{p} - \operatorname{ord}_\mathfrak{p}(x)} = \prod_{\mathfrak{p} \notin S} (\mathfrak{p}\mathcal{O}_{K,S})^{-n'_\mathfrak{p}} \prod_{\mathfrak{p} \notin S} (\mathfrak{p}\mathcal{O}_{K,S})^{-\operatorname{ord}_\mathfrak{p}(x)} = I(D')(x^{-1}\mathcal{O}_{K,S}).$$

Hence, this means that $[I(D)] = [I(D)']$ in Cl_K. So the map χ is well-defined. Furthermore, for any fractional ideal $[I] \in \mathrm{Cl}_{K,S}$ written as $I = \prod_{\mathfrak{p} \notin S} (\mathfrak{p}\mathcal{O}_{K,S})^{n_\mathfrak{p}}$, we can take the Arakelov S-divisor

$$D = \sum_{\mathfrak{p} \notin S} (-n_\mathfrak{p})\mathfrak{p},$$

such that $\chi([D]) = [I(D)] = [I]$. This means that the map χ is surjective. Furthermore, for $[D], [D'] \in \mathrm{Pic}_{K,S}$

$$\chi([D] + [D']) = \chi([D + D']) = [I(D + D')] = [I(D)][I(D')] = \chi([D])\chi([D']),$$

where we used Equation (68). As a result of this, we see that χ is also a group homomorphism. Therefore, exactness at $\mathrm{Cl}_{K,S}$ follows.

It remains to show that $\mathrm{im}(\zeta_S) = \ker(\chi)$. Take any $[D] \in \mathrm{im}(\zeta_S)$. Then $[D]$ is of the form $[\sum_{\sigma \in \Sigma_K^\infty} x_\sigma \sigma]$. We get that $\chi([D]) = \chi([\sum_{\sigma \in \Sigma_K^\infty} x_\sigma \sigma]) = [\mathcal{O}_{K,S}]$, i.e. $[D] \in \ker(\chi)$. Conversely, take $[D] \in \ker(\chi)$. Then $[\mathcal{O}_{K,S}] = \chi([D])$, and so $[\mathcal{O}_{K,S}] = [I(D)]$. Hence, there exists some $x \in K^*$ such that $I(D) = x\mathcal{O}_{K,S}$. If we denote the coefficients of the finite places of D by $n_\mathfrak{p}$ for all $\mathfrak{p} \notin S$, then we get that $n_\mathfrak{p} = -\operatorname{ord}_\mathfrak{p}(x)$ for all $\mathfrak{p} \notin S$. So

$$D = \operatorname{div}_S(x^{-1}) + \sum_{\sigma \in \Sigma_K^\infty} x_\sigma \sigma,$$

for some $x_\sigma \in \mathbb{R}$. We obtain that $[D] = [\sum_{\sigma \in \Sigma_K^\infty} x_\sigma \sigma] \in \mathrm{im}(\zeta_S)$. By inclusion of both sides, we obtain $\mathrm{im}(\zeta_S) = \ker(\chi)$. This proves the exactness at $\mathrm{Pic}_{K,S}$.

A careful check can verify, with the group homomorphism constructed above, that the diagram is commutative. □

5.2 Alternative Structure of the Arakelov S-Class Group

In this section, we will introduce alternative structures of the Arakelov S-class group. This will contain a different notation for Arakelov S-divisors, and two groups that are isomorphic to $\mathrm{Pic}_{K,S}$.

5.2.1 Multiplicative Notation

To work with Arakelov S-divisors, it is not always convenient to work with the current definition. In Definition 4.1.10, we introduced the multiplicative notation of an Arakelov divisor. In this section, we will generalize this notation to Arakelov S-divisors.

Take I to be a non-zero fractional ideal of $\mathcal{O}_{K,S}$ and $u \in K_\mathbb{R}$ whose elements are all real and positive. Equivalently, we can take $u \in \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}_{>0}$ (see Remark 1.8.4). We combine these two elements into a pair written by $(I, u)_S$. Now, any Arakelov S-divisor, given by

$$D = \sum_{\mathfrak{p} \notin S} n_\mathfrak{p}\mathfrak{p} + \sum_{\sigma \in \Sigma_K^\infty} x_\sigma \sigma, \qquad n_\mathfrak{p} \in \mathbb{Z}, x_\sigma \in \mathbb{R},$$

can be mapped to such a pair. Namely, we map D to $(I(D), (e^{-x_\sigma})_{\sigma \in \Sigma_K^\infty})_S$, where $I(D)$ is the associated fractional ideal to D (see Definition 5.1.10). This mapping is injective. Namely, consider another Arakelov S-divisor defined as

$$D' = \sum_{\mathfrak{p} \notin S} m_\mathfrak{p}\mathfrak{p} + \sum_{\sigma \in \Sigma_K^\infty} y_\sigma \sigma, \qquad m_\mathfrak{p} \in \mathbb{Z}, y_\sigma \in \mathbb{R}.$$

If $D, D' \in \mathrm{Div}_{K,S}$ map both to the same pair $(I,u)_S$, then

$$I = I(D) = I(D), \qquad u = (e^{-x_\sigma})_{\sigma\in\Sigma_K^\infty} = (e^{-y_\sigma})_{\sigma\in\Sigma_K^\infty}.$$

By uniqueness of factorization of fractional ideals in non-zero prime ideals of $\mathcal{O}_{K,S}$, we have that $n_\mathfrak{p} = m_\mathfrak{p}$ for all $\mathfrak{p} \notin S$. Furthermore, since the exponential function is injective and $e^{-x_\sigma} = e^{-y_\sigma}$, we have that $x_\sigma = y_\sigma$ for all $\sigma \in \Sigma_K^\infty$. Hence, we see that D and D' have the same coefficients, i.e. $D = D'$. Moreover, this mapping is surjective. Namely, take any $(I,u)_S$, for some non-zero $I \in \mathrm{Id}_{K,S}$ and $u \in \prod_{\sigma\in\Sigma_K^\infty} \mathbb{R}_{>0}$. More specifically, write

$$I = \prod_{\mathfrak{p}\notin S} (\mathfrak{p}\mathcal{O}_{K,S})^{n_\mathfrak{p}}, \qquad u = (u_\sigma)_{\sigma\in\Sigma_K^\infty}.$$

We have that $n_\mathfrak{p} \in \mathbb{Z}$ for all $\mathfrak{p} \notin S$. Since $u \in \prod_{\sigma\in\Sigma_K^\infty} \mathbb{R}_{>0}$, we have $\log(u_\sigma) \in \mathbb{R}$ for all $\sigma \in \Sigma_K^\infty$. Then the Arakelov S-divisor of the form

$$D = -\sum_{\mathfrak{p}\notin S} n_\mathfrak{p}\mathfrak{p} - \sum_{\sigma\in\Sigma_K^\infty} \log(u_\sigma)\sigma,$$

is mapped to $(I,u)_S$. In conclusion, we have a bijection between $\mathrm{Div}_{K,S}$ and the set of pairs $(I,u)_S$, for some non-zero $I \in \mathrm{Id}_{K,S}$ and $u \in \prod_{\sigma\in\Sigma_K^\infty} \mathbb{R}_{>0}$. By this bijection, we interchange the notions of Arakelov S-divisors and these pairs freely.

Definition 5.2.1. Let $D \in \mathrm{Div}_{K,S}$. The notation

$$D = \sum_{\mathfrak{p}\notin S} n_\mathfrak{p}\mathfrak{p} + \sum_{\sigma\in\Sigma_K^\infty} x_\sigma\sigma, \qquad n_\mathfrak{p} \in \mathbb{Z}, x_\sigma \in \mathbb{R},$$

is called the *additive notation* of the Arakelov S-divisor D. The notation $D = (I,u)_S$ for some non-zero $I \in \mathrm{Id}_{K,S}$ and $u \in \prod_{\sigma\in\Sigma_K^\infty} \mathbb{R}_{>0}$, is called the *multiplicative notation* of the Arakelov S-divisor D.

If we take $S = \emptyset$, this is just the multiplicative notation we introduced in Definition 4.1.10. In this case, we denote an Arakelov divisor by (I,u) rather than $(I,u)_\emptyset$. The group operation of the group $\mathrm{Div}_{K,S}$, in the multiplicative notation, is given by

$$(I,u)_S + (J,v)_S = (IJ, uv)_S, \qquad (I,u)_S, (J,v)_S \in \mathrm{Div}_{K,S}\,.$$

Namely, the coefficients of D are mapped to powers of prime ideals and the exponential. Therefore, addition turns into multiplication. The zero Arakelov S-divisor is given by $(\mathcal{O}_{K,S}, (1)_{\sigma\in\Sigma_K^\infty})$ in the multiplicative notation. Any principal Arakelov S-divisors $\mathrm{div}_S(x)$ for some $x \in K^*$, is given by

$$(x^{-1}\mathcal{O}_{K,S}, \hat{x})_S \tag{70}$$

in the multiplicative notation. Lastly, for some $I \in \mathrm{Id}_{K,S}$, the Arakelov S-divisor $\pi_S(I)$ is given by

$$(I, (N_{\mathcal{O}_{K,S}}(I)^{-1/n})_{\sigma\in\Sigma_K^\infty})_S.$$

5.2.2 Metrized S-Line Bundles

In Definition 4.1.12, we have seen the definition of an ideal lattice of K. There was a natural way to associate an ideal lattice with an Arakelov divisor (I,u). Namely, we considered the projective $\mathcal{O}_K$-module $u\Psi(I)$ of rank 1 and took the inner product from $K_\mathbb{R}$. Here $\Psi\colon K \to K_\mathbb{R}$ denotes the Minkowski embedding. So, at first sight, a natural extension would be given as follows. Given an Arakelov S-divisor $(J,v)_S$, we create the projective $\mathcal{O}_{K,S}$-module $v\Psi(J)$ of rank 1 (these module properties will be shown in this section). Moreover, we use the Euclidean structure of $K_\mathbb{R}$ to give some additional structure to this $\mathcal{O}_{K,S}$-module. However, in comparison to $u\Psi(I)$, the subgroup $v\Psi(J)$ no longer forms a lattice in $K_\mathbb{R}$. Instead, in Theorem 3.4.6, we have seen that the non-zero fractional ideals of $\mathcal{O}_{K,S}$ form a lattice in K_S, under the image of the S-Minkowski

embedding $\Psi_S \colon K \to K_S$, rather than in $K_{\mathbb{R}}$. So either the name of ideal lattice would be inconvenient in this case, or we should consider Ψ_S rather than Ψ. However, the S-Minkowski space K_S is not a Euclidean space. Therefore, we cannot consider an inner product on K_S. This would complicate the extension of the definition of an ideal lattice. So to conclude, on one hand, we can map fractional ideals of $\mathcal{O}_{K,S}$ to $K_{\mathbb{R}}$. They no longer form lattices in $K_{\mathbb{R}}$ but we can use the inner product on $K_{\mathbb{R}}$. On the other hand, we can map fractional ideals of $\mathcal{O}_{K,S}$ to K_S. They form lattices in K_S, but we cannot use an inner product. So we have to choose between these two options. However, it turns out that we can also study them separately. This is exactly what we will do. In this section, we will consider the case where we embed everything into $K_{\mathbb{R}}$, and use the Euclidean structure of it. In the next section, we embed everything into K_S, where we use the lattice properties.

More specifically, in this section, we will consider projective $\mathcal{O}_{K,S}$-modules of rank 1. To understand the notion of rank of projective modules, we start with a short overview of this theory. Thereafter, we introduce the notion of a metrized S-line bundle. This is a projective $\mathcal{O}_{K,S}$-modules L of rank 1 supported by a $K_{\mathbb{R}}$-metric on the $K_{\mathbb{R}}$-module $L \otimes_{\mathcal{O}_{K,S}} K_{\mathbb{R}}$. We show how the set of metrized S-line bundles attains an abelian group structure. This group structure uses the tensor product of modules. Therefore, throughout this section, we will use standard tensor product rules for modules without reference. But one can find these in Chapter 2 in [AM69] or Chapter 8 in [AK21] for example. Once the group structure is given, we show how this group is isomorphic to $\mathrm{Pic}_{K,S}$.

Let R be a commutative ring. Let $\mathrm{Spec}(R)$ denote the set of all prime ideals of R. We endow $\mathrm{Spec}(R)$ with the Zariski topology. The closed sets of this topology are given by

$$V(A) := \{\mathfrak{p} \in \mathrm{Spec}(R) : A \subseteq \mathfrak{p}\},$$

for some subset $A \subseteq R$. Recall that an R-module M is projective if there exists an R-module N such that $M \bigoplus N \cong R^k$ for some $k \in \mathbb{Z}_{\geq 0}$. From now on, assume that M is a projective R-module. We know that the localization $R_{\mathfrak{p}}$ for any $\mathfrak{p} \in \mathrm{Spec}(R)$ is a local ring (see [AM69, Example 1, Page 38]). Furthermore, the projective property is a local property. So we have the projective $R_{\mathfrak{p}}$-module $M_{\mathfrak{p}}$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$. Kaplansky's Theorem for projective modules says that any projective module over a local ring is free (see [Kap58, Theorem 2]). Hence, we conclude that $M_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$-module for all $\mathfrak{p} \in \mathrm{Spec}(R)$.

Definition 5.2.2. Let M be a projective R-module. The *rank* of M at $\mathfrak{p} \in \mathrm{Spec}(R)$, denoted by $\mathrm{rank}_{\mathfrak{p}}(M)$, is defined to be the rank of the free $R_{\mathfrak{p}}$-module $M_{\mathfrak{p}}$. The module M has *constant rank* if the rank of M at $\mathfrak{p}$ is equal for all $\mathfrak{p} \in \mathrm{Spec}(R)$. In this case, the constant rank of M is denoted by $\mathrm{rank}(M)$.

Lemma 5.2.3. Let M be a projective R-module. For any $\mathfrak{p} \in \mathrm{Spec}(R)$ one has

$$\mathrm{rank}_{\mathfrak{p}}(M) = \dim_{\kappa(\mathfrak{p})} M \otimes_R \kappa(\mathfrak{p}),$$

where $\kappa(\mathfrak{p}) = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$.

Proof. One can view $\kappa(\mathfrak{p})$ as $R_{\mathfrak{p}}$-module. It follows that $\kappa(\mathfrak{p}) \otimes_{R_{\mathfrak{p}}} M_{\mathfrak{p}}$ is a free $\kappa(\mathfrak{p})$-module of rank $\mathrm{rank}_{\mathfrak{p}}(M)$, by Proposition 1.8.1. One has $M_{\mathfrak{p}} \cong R_{\mathfrak{p}} \otimes_R M$ by Proposition 3.5 in [AM69]. So by associativeness of the tensor product, we have that

$$\kappa(\mathfrak{p}) \otimes_{R_{\mathfrak{p}}} M_{\mathfrak{p}} \cong \kappa(\mathfrak{p}) \otimes_{R_{\mathfrak{p}}} (R_{\mathfrak{p}} \otimes_R M) \cong \big(\kappa(\mathfrak{p}) \otimes_{R_{\mathfrak{p}}} R_{\mathfrak{p}}\big) \otimes_R M \cong \kappa(\mathfrak{p}) \otimes_R M$$

is a free $\kappa(\mathfrak{p})$-module of rank $\mathrm{rank}_{\mathfrak{p}}(M)$. Since $\kappa(\mathfrak{p})$ is a field, we have $\mathrm{rank}_{\mathfrak{p}}(M) = \dim_{\kappa(\mathfrak{p})} M \otimes_R \kappa(\mathfrak{p})$. □

There is a way to find a relation between projective modules, finitely generated modules, and the rank.

Proposition 5.2.4. If a projective R-module has a constant rank, then it is finitely generated. Conversely, if a projective R-module is finitely generated and $\mathrm{Spec}(R)$ is connected, then it has a constant rank.

The first statement is proved by the proof of [Vas69, Proposition 1.3]. The second statement is derived in Section 2 of Chapter 1 in [Wei13].

Corollary 5.2.5. Let M be a projective module over a domain R. Moreover, let F be the field of fractions of R. Then M is finitely generated if and only if it has a constant rank. Moreover, if M is finitely generated, then the constant rank is given by $\operatorname{rank}(M) = \dim_F M \otimes_R F$.

Proof. Since R is a domain, we know that the integral ideal (0) is a prime ideal. This prime ideal can only be contained in the closed subset of $\operatorname{Spec}(R)$ given by

$$V(\{0\}) = \{\mathfrak{p} \in \operatorname{Spec}(R) : \{0\} \subseteq \mathfrak{p}\}.$$

On the other hand, we have $V(\{0\}) = \operatorname{Spec}(R)$. Therefore, if two disjoint closed subsets of $\operatorname{Spec}(R)$ cover $\operatorname{Spec}(R)$, one of them must contain the prime ideal (0). This immediately implies that one of them must be the whole space. This means that the topological space $\operatorname{Spec}(R)$ does not admit a partition, i.e. it is connected. So, if M is a projective R-module, we know by Proposition 5.2.4 that M is finitely generated if and only if it has a constant rank. In case M is finitely generated, the constant rank is given by $\operatorname{rank}(M) = \dim_F M \otimes_R F$. This is obtained by using the prime ideal (0) in Lemma 5.2.3. □

This will most commonly be used in the rest of this thesis since we will work with modules over domains. Therefore, assume for the rest of the section that R is a domain.

Denote the set of projective R-modules of constant rank 1 by P_R^1. Consequently, if we take any $M \in P_R^1$ it is automatically finitely generated by Corollary 5.2.5. For any R-module M, the set of R-module homomorphisms from M to R is denoted by $M^* := \operatorname{Hom}_R(M, R)$.

Proposition 5.2.6. The set P_R^1 contains the R-module R, and for any $M \in P_R^1$, one has $M^* \in P_R^1$. Moreover, for any $M_1, M_2 \in P_R^1$, one has $M_1 \otimes_R M_2 \in P_R^1$.

Proof. We know that R can be viewed as a free R-module itself. In particular, it is finitely generated and projective. Therefore, by Corollary 5.2.5, it has a constant rank. Moreover, the corollary tells us that its constant rank is given by

$$\operatorname{rank}(R) = \dim_F R \otimes_R F = \dim_F F = 1.$$

We get that $R \in P_R^1$. Now, take any $M \in P_R^1$. Since M is finitely generated and projective, so is M^* (see [CR15, Proposition 1.10]). In that case, Corollary 5.2.5 tells us that it has a constant rank. Proposition 1.31 in [CR15] tells us that

$$\operatorname{rank}(M^*) = \operatorname{rank}(M) \operatorname{rank}(R).$$

Therefore, we have $\operatorname{rank}(M^*) = 1$, and so $M^* \in P_R^1$. Take any $M_1, M_2 \in P_R^1$. Then $M_1 \otimes_R M_2$ is a finitely generated and projective R-module since this is preserved under tensor products (see for projectiveness Proposition 1.7 in [CR15]). It follows, by Corollary 5.2.5, that it has a constant rank. Proposition 1.31 in [CR15] tells us that

$$\operatorname{rank}(M_1 \otimes_R M_2) = \operatorname{rank}(M_1) \operatorname{rank}(M_2).$$

Therefore, we have $\operatorname{rank}(M_1 \otimes_R M_2) = 1$. We see that $M_1 \otimes_R M_2 \in P_R^1$. □

From now on, let $\mathcal{O}$ be a Dedekind domain and F its field of fractions.

Lemma 5.2.7. One has $I \in P_{\mathcal{O}}^1$ for any fractional ideal I of $\mathcal{O}$. Moreover, for any $M \in P_{\mathcal{O}}^1$ there exists a fractional ideal I of $\mathcal{O}$ that is isomorphic to M as $\mathcal{O}$-module.

Proof. Recall that an $\mathcal{O}$-module M is called torsion-free, if for any $m \in M$ there does not exist a non-zero $r \in \mathcal{O}$ such that $rm = 0$. Proposition 4.3 in Chapter III of [Neu99] states that M is projective if and only if M is torsion-free. Any fractional ideal of $\mathcal{O}$ is torsion-free as an $\mathcal{O}$-module, as it lives in the field F. In particular, any fractional ideal is projective. Now, since $\mathcal{O}$ is a Dedekind domain, we have that all fractional ideals of $\mathcal{O}$ are finitely generated as $\mathcal{O}$-module. Hence, any fractional ideal of $\mathcal{O}$ is a finitely generated and

projective $\mathcal{O}$-module. It follows from Corollary 5.2.5 that it has a constant rank. Moreover, the corollary tells us that the constant rank of $I \in \mathrm{Id}_{\mathcal{O}}$ is given by

$$\dim_F(I \otimes_{\mathcal{O}_{K,S}} F) = \dim_F F = 1,$$

where we used Proposition 1.8.2. Thus, any fractional ideal of $\mathcal{O}$ is contained in $P^1_{\mathcal{O}}$.

Now, let $M \in P^1_{\mathcal{O}}$. Since M has constant rank 1, we have that

$$1 = \mathrm{rank}(M) = \dim_F(M \otimes_{\mathcal{O}} F),$$

using Corollary 5.2.5. Consequently, there exists a non-zero $\alpha \in M \otimes_{\mathcal{O}} F$ that forms an F-basis of $M \otimes_{\mathcal{O}} F$. Then for any $u \in M$, there is a unique $x_u \in F$ such that $u \otimes 1 = x_u\alpha$. For $u \in M$ and $a \in \mathcal{O}$, we have

$$x_{au}\alpha = au \otimes 1 = a(u \otimes 1) = ax_u\alpha,$$

where we used bilinearity over $\mathcal{O}$. We get that $x_{au} = ax_u$. Moreover, for $u, v \in M$, we have

$$x_{u+v}\alpha = (u+v) \otimes 1 = u \otimes 1 + v \otimes 1 = x_u\alpha + x_v\alpha = (x_u + x_v)\alpha.$$

We see that $x_{u+v} = x_u + x_v$. Therefore, the map $f : M \to F$ given by $u \mapsto x_u$ is an $\mathcal{O}$-module homomorphism. Moreover, the map f is injective by the uniqueness of x_u for any $u \in M$. The $\mathcal{O}$-module M is finitely generated. The image of a finitely generated $\mathcal{O}$-module under an $\mathcal{O}$-module homomorphism is a finitely generated $\mathcal{O}$-module. This means that $f(M) \subseteq F$ is a finitely generated $\mathcal{O}$-module. In particular, we know that $f(M)$ is a fractional ideal of $\mathcal{O}$. By injectivity of f, it follows that M is isomorphic as $\mathcal{O}$-module to a fractional ideal of $\mathcal{O}$. □

We are done investigating the rank of projective modules. Therefore, we are ready to look into the extension of ideal lattices by embedding everything into $K_{\mathbb{R}}$. For any $\sigma \in \Sigma_K^\infty$, we have $K \subseteq K_\sigma$. Hence, we can view K_σ as a K-module. Therefore, we can also view $K_{\mathbb{R}} = \prod_{\sigma \in \Sigma_K^\infty} K_\sigma$ as a K-module. So in particular, we can view $K_{\mathbb{R}}$ as an $\mathcal{O}_{K,S}$-module. Hence, we can consider the tensor product

$$L_{\mathbb{R}} := L \otimes_{\mathcal{O}_{K,S}} K_{\mathbb{R}}$$

for some $L \in P^1_{\mathcal{O}_{K,S}}$. Notice that we can view $L_{\mathbb{R}}$ as a $K_{\mathbb{R}}$-module. Since $K_{\mathbb{R}} = \prod_{\sigma \in \Sigma_K^\infty} K_\sigma$, we also have

$$L_{\mathbb{R}} = L \otimes_{\mathcal{O}_{K,S}} K_{\mathbb{R}} = L \otimes_{\mathcal{O}_{K,S}} \left(\prod_{\sigma \in \Sigma_K^\infty} K_\sigma \right) = \prod_{\sigma \in \Sigma_K^\infty} L \otimes_{\mathcal{O}_{K,S}} K_\sigma.$$

So setting $L_\sigma := L \otimes_{\mathcal{O}_{K,S}} K_\sigma$ for any $\sigma \in \Sigma_K^\infty$, we get

$$L_{\mathbb{R}} = \prod_{\sigma \in \Sigma_K^\infty} L_\sigma. \tag{71}$$

Definition 5.2.8. Let $L \in P^1_{\mathcal{O}_{K,S}}$. A map $\langle \cdot, \cdot \rangle \colon L_{\mathbb{R}} \times L_{\mathbb{R}} \to K_{\mathbb{R}}$ is called an $K_{\mathbb{R}}$-*metric* on $L_{\mathbb{R}}$ if

i.) $\langle u, u \rangle \in \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}_{\geq 0}$ for all $u \in L_{\mathbb{R}}$ and $\langle u, u \rangle = 0$ if and only if $u = 0$.

ii.) Let the decomposition through (71) of u be given by $(u_\sigma)_{\sigma \in \Sigma_K^\infty}$. If $u_\sigma \neq 0$ for all $\sigma \in \Sigma_K^\infty$, then $\langle u, u \rangle \in \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}_{>0}$.

iii.) $\langle u, v \rangle = \overline{\langle v, u \rangle}$ for all $u, v \in L_{\mathbb{R}}$.

iv.) $\langle \alpha u + \beta v, w \rangle = \alpha \langle u, w \rangle + \beta \langle v, w \rangle$ for all $u, v, w \in L_{\mathbb{R}}$ and $\alpha, \beta \in K_{\mathbb{R}}$.

Definition 5.2.9. A *metrized S-line bundle* of K is a pair $(L, \langle\cdot,\cdot\rangle_L)$, where $L \in P^1_{\mathcal{O}_{K,S}}$ and $\langle\cdot,\cdot\rangle_L$ is a $K_\mathbb{R}$-metric on $L_\mathbb{R}$. The set of metrized S-line bundles is denoted by $\mathrm{ML}_{K,S}$.

Remark 5.2.10. The notion of metrized S-line bundles is the extension of ideal lattices for this section. Until now, we have always extended notions in such a way that if we take $S = \emptyset$, we recover the original situation. So, in this case, we expect a metrized $\emptyset$-line bundle of K to be an ideal lattice of K. However, while we still have a projective $\mathcal{O}_K$-module L of rank 1, we see that there is a difference. Namely, for metrized $\emptyset$-line bundles we consider a $K_\mathbb{R}$-metric on $L \otimes_{\mathcal{O}_K} K_\mathbb{R}$, while for an ideal lattice, we consider an inner product on $L \otimes_{\mathcal{O}_K} K_\mathbb{R}$. So the notion of metrized S-line bundles is not a full extension of ideal lattices. However, there is a reason why we take a $K_\mathbb{R}$-metric. In Proposition 4.1.14 (i.), we have seen that Pic_K and the set of isometry classes of ideal lattices are in bijection. Therefore, the set of isometry classes of ideal lattices attains an abelian group structure induced from Pic_K. We would like to obtain such a result for metrized S-line bundles. However, we would like to give a group structure on the set of metrized S-line bundles before the bijection. It would mean that we can construct a group isomorphism rather than a bijection. It turns out, by trying to accomplish this, that it is easier to work with a $K_\mathbb{R}$-metric than an inner product.

The ideas for a $K_\mathbb{R}$-metric are inspired by Section 4 of Chapter III of [Neu99], where metrized $\mathcal{O}_K$-modules are studied. ♦

In Proposition 5.2.6, we have seen that $\mathcal{O}_{K,S} \in P^1_{\mathcal{O}_{K,S}}$. Now, we can transform $\mathcal{O}_{K,S}$ into a metrized S-line bundle. Therefore, we have to endow $(\mathcal{O}_{K,S})_\mathbb{R}$ with a $K_\mathbb{R}$-metric. Notice that we have a $K_\mathbb{R}$-module isomorphism

$$(\mathcal{O}_{K,S})_\mathbb{R} = \mathcal{O}_{K,S} \otimes_{\mathcal{O}_{K,S}} K_\mathbb{R} \cong K_\mathbb{R}. \tag{72}$$

So endowing $(\mathcal{O}_{K,S})_\mathbb{R}$ with a $K_\mathbb{R}$-metric is equivalent to endowing $K_\mathbb{R}$ with a $K_\mathbb{R}$-metric.

Proposition 5.2.11. Take any $\alpha \in \prod_{\sigma\in\Sigma_K^\infty} \mathbb{R}_{>0}$. The map $\langle\cdot,\cdot\rangle_\alpha \colon K_\mathbb{R} \times K_\mathbb{R} \to K_\mathbb{R}$ defined by

$$\langle u, v\rangle_\alpha := \alpha^2 u\overline{v}$$

is a $K_\mathbb{R}$-metric on $K_\mathbb{R}$. Moreover, any $K_\mathbb{R}$-metric on $K_\mathbb{R}$ is of the form $\langle\cdot,\cdot\rangle_\alpha$ for some $\alpha \in \prod_{\sigma\in\Sigma_K^\infty} \mathbb{R}_{>0}$.

Proof. The fact that $\langle\cdot,\cdot\rangle_\alpha$ is a $K_\mathbb{R}$-metric on $K_\mathbb{R}$ is a direct verification of the conditions from Definition 5.2.8.

Now, let $\langle\cdot,\cdot\rangle$ be any $K_\mathbb{R}$-metric on $K_\mathbb{R}$. Then $\langle 1,1\rangle \in \prod_{\sigma\in\Sigma_K^\infty} \mathbb{R}_{>0}$. Therefore, we can define $\alpha := \sqrt{\langle 1,1\rangle}$, where we take the square root entry-wise. In its turn, we have $\alpha \in \prod_{\sigma\in\Sigma_K^\infty} \mathbb{R}_{>0}$. Then for any $u, v \in K_\mathbb{R}$, using conditions (iii.) and (iv.) of Definition 5.2.8, we have that

$$\langle u, v\rangle = u\langle 1, v\rangle = u\overline{\langle v, 1\rangle} = u\overline{v}\langle 1,1\rangle = \alpha^2 u\overline{v} = \langle u, v\rangle_\alpha.$$

We see that $\langle\cdot,\cdot\rangle = \langle\cdot,\cdot\rangle_\alpha$. □

So we can take any $K_\mathbb{R}$-metric on $K_\mathbb{R}$ from Proposition 5.2.11 to make $\mathcal{O}_{K,S}$ a metrized S-line bundle. Specifically, we choose $\alpha = 1$. We conclude that $(\mathcal{O}_{K,S}, \langle\cdot,\cdot\rangle_1) \in \mathrm{ML}_{K,S}$.

Given $(L, \langle\cdot,\cdot\rangle_L), (L', \langle\cdot,\cdot\rangle_{L'}) \in \mathrm{ML}_{K,S}$, there is a way to create a new metrized S-line bundle. Namely, since $L, L' \in P^1_{\mathcal{O}_{K,S}}$, we have seen in Proposition 5.2.6 that $L \otimes_{\mathcal{O}_{K,S}} L' \in P^1_{\mathcal{O}_{K,S}}$. So it remains to endow $(L \otimes_{\mathcal{O}_{K,S}} L')_\mathbb{R}$ with a $K_\mathbb{R}$-metric. Notice that

$$\begin{aligned}
(L \otimes_{\mathcal{O}_{K,S}} L')_\mathbb{R} &= (L \otimes_{\mathcal{O}_{K,S}} L') \otimes_{\mathcal{O}_{K,S}} K_\mathbb{R} \\
&\cong L \otimes_{\mathcal{O}_{K,S}} (L' \otimes_{\mathcal{O}_{K,S}} K_\mathbb{R}) \\
&\cong L \otimes_{\mathcal{O}_{K,S}} (K_\mathbb{R} \otimes_{K_\mathbb{R}} (L' \otimes_{\mathcal{O}_{K,S}} K_\mathbb{R})) \\
&\cong (L \otimes_{\mathcal{O}_{K,S}} K_\mathbb{R}) \otimes_{K_\mathbb{R}} (L' \otimes_{\mathcal{O}_{K,S}} K_\mathbb{R}) \\
&= L_\mathbb{R} \otimes_{K_\mathbb{R}} L'_\mathbb{R}.
\end{aligned}$$

Thus, we have a $K_{\mathbb{R}}$-module isomorphism

$$(L \otimes_{\mathcal{O}_{K,S}} L')_{\mathbb{R}} \cong L_{\mathbb{R}} \otimes_{K_{\mathbb{R}}} L'_{\mathbb{R}}. \tag{73}$$

So endowing $(L \otimes_{\mathcal{O}_{K,S}} L')_{\mathbb{R}}$ with a $K_{\mathbb{R}}$-metric is equivalent to endowing $L_{\mathbb{R}} \otimes_{K_{\mathbb{R}}} L'_{\mathbb{R}}$ with a $K_{\mathbb{R}}$-metric. For $u \otimes u', v \otimes v' \in L_{\mathbb{R}} \otimes_{K_{\mathbb{R}}} L'_{\mathbb{R}}$, we define

$$\langle u \otimes u', v \otimes v' \rangle_{L \otimes L'} := \langle u, v \rangle_L \langle u', v' \rangle_{L'}, \tag{74}$$

and extend this by linearity over $K_{\mathbb{R}}$. Recall that a tensor product $M \otimes_R M'$, for two R-modules M, M' and commutative ring R, is spanned by the symbols $u \otimes u'$ for $u \in M$ and $u' \in M'$. These symbols satisfy the rules

$$(u+v) \otimes u' = u \otimes u' + v \otimes u', \qquad u \otimes (u'+v') = u \otimes u' + u \otimes v',$$
$$r(u \otimes u') = (ru) \otimes u' = u \otimes (ru'),$$

for $u, v \in M$, $u', v' \in M'$, and $r \in R$. Hence, it needs to be checked that the $K_{\mathbb{R}}$-metric (74) is well-defined on the tensor product. But this follows directly from the fact that we extend it by $K_{\mathbb{R}}$-linearity. Furthermore, since $\langle \cdot, \cdot \rangle_L$ and $\langle \cdot, \cdot \rangle_{L'}$ satisfy the conditions of Definition 5.2.8, it follows that $\langle \cdot, \cdot \rangle_{L \otimes L'}$ does too. As a result of this, we know that $\langle \cdot, \cdot \rangle_{L \otimes L'}$ is a $K_{\mathbb{R}}$-metric on $L_{\mathbb{R}} \otimes_{K_{\mathbb{R}}} L'_{\mathbb{R}}$ (or equivalently $(L \otimes_{\mathcal{O}_{K,S}} L')_{\mathbb{R}}$). In conclusion, we can define the operation $\mathrm{ML}_{K,S} \times \mathrm{ML}_{K,S} \to \mathrm{ML}_{K,S}$, which we denote by $\circ$, given by

$$(L, \langle \cdot, \cdot \rangle_L) \circ (L', \langle \cdot, \cdot \rangle_{L'}) = (L \otimes_{\mathcal{O}_{K,S}} L', \langle \cdot, \cdot \rangle_{L \otimes L'}).$$

Remark 5.2.12. To complement Remark 5.2.10, if we had taken an inner product on $L_{\mathbb{R}}$ and $L'_{\mathbb{R}}$, we would run into trouble by checking that an inner product on $(L \otimes_{\mathcal{O}_{K,S}} L')_{\mathbb{R}}$ is well-defined. Namely, the rule

$$r(u \otimes u') = (ru) \otimes u' = u \otimes (ru')$$

is easier to verify for a $K_{\mathbb{R}}$-metric (because this is extended by $K_{\mathbb{R}}$-linearity), than for an inner product (because that would be extended by $\mathbb{R}$-linearity). ♦

Given a single $(L, \langle \cdot, \cdot \rangle_L) \in \mathrm{ML}_{K,S}$, there is also a way to create a new metrized S-line bundle. Namely, if $L \in P^1_{\mathcal{O}_{K,S}}$, we have seen in Proposition 5.2.6 that $L^* \in P^1_{\mathcal{O}_{K,S}}$. So it remains to endow $(L^*)_{\mathbb{R}}$ with a $K_{\mathbb{R}}$-metric. Since $L \in P^1_{\mathcal{O}_{K,S}}$, it is a projective $\mathcal{O}_{K,S}$-module of constant rank 1. It follows from Corollary 5.2.5 that it is finitely generated. Proposition 10.12 in [AK21] tells us that a projective and finitely generated $\mathcal{O}_{K,S}$-module is finitely presented. This means that there exists an exact sequence

$$M \longrightarrow N \longrightarrow L \longrightarrow 0 \ ,$$

where M, N are free $\mathcal{O}_{K,S}$-modules of finite rank. The notion is not that important, but we can apply Proposition 9.10 in [AK21]. It states, since L is finitely presented, that there exists an $\mathcal{O}_{K,S}$-module isomorphism given by

$$(L^*)_{\mathbb{R}} = \mathrm{Hom}_{\mathcal{O}_{K,S}}(L, \mathcal{O}_{K,S}) \otimes_{\mathcal{O}_{K,S}} K_{\mathbb{R}} \cong \mathrm{Hom}_{\mathcal{O}_{K,S}}(L, \mathcal{O}_{K,S} \otimes_{\mathcal{O}_{K,S}} K_{\mathbb{R}}).$$

Then we also have the $K_{\mathbb{R}}$-module isomorphism $(L^*)_{\mathbb{R}} \cong \mathrm{Hom}_{\mathcal{O}_{K,S}}(L, K_{\mathbb{R}})$, viewing $\mathrm{Hom}_{\mathcal{O}_{K,S}}(L, K_{\mathbb{R}})$ as $K_{\mathbb{R}}$-module by value-wise multiplication (see [AK21, Bimodules 8.6]). On the other hand, we have $K_{\mathbb{R}}$-module isomorphisms

$$\mathrm{Hom}_{K_{\mathbb{R}}}(L_{\mathbb{R}}, K_{\mathbb{R}}) = \mathrm{Hom}_{K_{\mathbb{R}}}(L \otimes_{\mathcal{O}_{K,S}} K_{\mathbb{R}}, K_{\mathbb{R}}) \cong \mathrm{Hom}_{\mathcal{O}_{K,S}}(L, \mathrm{Hom}_{K_{\mathbb{R}}}(K_{\mathbb{R}}, K_{\mathbb{R}})) \cong \mathrm{Hom}_{\mathcal{O}_{K,S}}(L, K_{\mathbb{R}}),$$

where the first $K_{\mathbb{R}}$-module isomorphism can be found in [AK21, Theorem 8.8]. These results can be combined to a $K_{\mathbb{R}}$-module isomorphism

$$(L^*)_{\mathbb{R}} \cong \mathrm{Hom}_{K_{\mathbb{R}}}(L_{\mathbb{R}}, K_{\mathbb{R}}) = L^*_{\mathbb{R}}. \tag{75}$$

So endowing $(L^*)_{\mathbb{R}}$ with a $K_{\mathbb{R}}$-metric is equivalent to endowing $L^*_{\mathbb{R}}$ with a $K_{\mathbb{R}}$-metric. We will do this in a bit. But we first need some analysis on $L^*_{\mathbb{R}}$.

For $u \in L_{\mathbb{R}}$, set

$$u^*(v) := \langle v, u\rangle_L$$

for any $v \in L^*_{\mathbb{R}}$. Then $u^* \in L^*_{\mathbb{R}}$.

Proposition 5.2.13. Let $(L, \langle\cdot,\cdot\rangle_L) \in \mathrm{ML}_{K,S}$. For any $f \in L^*_{\mathbb{R}}$ there exists a unique $u \in L_{\mathbb{R}}$ such that $f = u^*$.

Proof. Let us start by showing the existence. If $f = 0$, we can take $u = 0$. Namely, by condition (iv.) of Definition 5.2.8, one can conclude that $\langle v, 0\rangle_L = 0$ for all $v \in L_{\mathbb{R}}$. Now, suppose that $f \neq 0$. Then $\ker(f)$ is strictly contained in $L_{\mathbb{R}}$. Define

$$(\ker(f))^\perp := \{u \in L_{\mathbb{R}} : \langle u, v\rangle_L = 0 \text{ for all } v \in \ker(f)\}.$$

By Lemma 5.2.7, we know that there exists some $I \in \mathrm{Id}_{K,S}$ such that $I \cong L$ as $\mathcal{O}_{K,S}$-modules. Then also

$$L_{\mathbb{R}} = L \otimes_{\mathcal{O}_{K,S}} K_{\mathbb{R}} \cong I \otimes_{\mathcal{O}_{K,S}} K_{\mathbb{R}} \cong K_{\mathbb{R}},$$

where last $\mathcal{O}_{K,S}$-module isomorphism follows from Proposition 1.8.2. We conclude that $L_{\mathbb{R}}$ is always a finite dimensional $\mathbb{R}$-vector space. Now, take any basis for the subspace $\ker(f)$. Then using the Gram-Schmidt Process, we can extend it to a basis of $L_{\mathbb{R}}$ that is orthonormal with respect to the $K_{\mathbb{R}}$-metric $\langle\cdot,\cdot\rangle_L$. Normally, the Gram-Schmidt Process holds for inner products, but this can be extended to $K_{\mathbb{R}}$-metrics. Then the basis vectors not contained in $\ker(f)$, form a basis for $(\ker(f))^\perp$. Consequently, there exists a non-zero $w \in (\ker(f))^\perp$. Then $f(w)v - f(v)w \in \ker(f)$ for any $v \in L_{\mathbb{R}}$. Namely, by linearity one has

$$f(f(w)v - f(v)w) = f(w)f(v) - f(v)f(w) = 0.$$

We obtain that $\langle f(w)v - f(v)w, w\rangle_L = 0$. By linearity of the map $\langle\cdot,\cdot\rangle_L$ we have

$$f(w)\langle v, w\rangle_L - f(v)\langle w, w\rangle_L = 0 \quad \implies f(v) = \frac{f(w)\langle v, w\rangle_L}{\langle w, w\rangle_L},$$

where we used that $\langle w, w\rangle_L \in \prod_{\sigma\in\Sigma^\infty_K} \mathbb{R}_{>0}$, i.e. a unit of $K_{\mathbb{R}}$. So setting $u = \frac{\overline{f(w)}w}{\langle w,w\rangle_L} \in L_{\mathbb{R}}$, we obtain that $f(v) = \langle v, u\rangle_L$ for all $v \in L_{\mathbb{R}}$. We see that $f = u^*$.

To show uniqueness, suppose that $f = u^* = v^*$ for some $u, v \in L_{\mathbb{R}}$. Then for any $w \in L_{\mathbb{R}}$, one has $f(w) = \langle w, u\rangle_L = \langle w, v\rangle_L$. Hence, we get that $\langle w, u - v\rangle_L = 0$ for all $w \in L_{\mathbb{R}}$. In particular, we have $\langle u - v, u - v\rangle_L = 0$. By condition (i.) of Definition 5.2.8, we get that $u - v = 0$. So $u = v$, which shows uniqueness. □

Proposition 5.2.13 implies that we can identity $L^*_{\mathbb{R}}$ with the set $\{u^* | u \in L_{\mathbb{R}}\}$. Now, for $u^*, v^* \in L^*_{\mathbb{R}}$, we define

$$\langle u^*, v^*\rangle_{L^*} := \overline{\langle u, v\rangle_L}.$$

For any $\alpha \in K_{\mathbb{R}}$ and $u \in L_{\mathbb{R}}$, we have $(\alpha u)^* = \overline{\alpha}u^*$. Namely, for any $v \in L_{\mathbb{R}}$, we have

$$(\alpha u)^*(v) = \langle v, \alpha u\rangle_L = \overline{\alpha}\langle v, u\rangle_L = \overline{\alpha}u^*(v).$$

With this rule and since $\langle\cdot,\cdot\rangle_L$ satisfies the conditions of Definition 5.2.8, it follows that $\langle\cdot,\cdot\rangle_{L^*}$ does too. This means that $\langle\cdot,\cdot\rangle_{L^*}$ is a $K_{\mathbb{R}}$-metric on $L^*_{\mathbb{R}}$ (or equivalently $(L^*)_{\mathbb{R}}$). In conclusion, for any $(L, \langle\cdot,\cdot\rangle_L) \in \mathrm{ML}_{K,S}$ we have the metrized S-line bundle $(L^*, \langle\cdot,\cdot\rangle_{L^*})$.

Definition 5.2.14. Let $(L, \langle\cdot,\cdot\rangle_L), (L', \langle\cdot,\cdot\rangle_{L'}) \in \mathrm{ML}_{K,S}$. An $\mathcal{O}_{K,S}$-module isomorphism $\varphi\colon L \mapsto L'$ is said to be an *isometry* if

$$\langle u, v\rangle_L = \langle \psi(u), \psi(v)\rangle_{L'}, \qquad u, v \in L_{\mathbb{R}},$$

where $\psi\colon L_{\mathbb{R}} \to L'_{\mathbb{R}}$ is given by the tensor map $\varphi \otimes \mathrm{id}_{K_{\mathbb{R}}}$. The metrized S-line bundles $(L, \langle\cdot,\cdot\rangle_L), (L', \langle\cdot,\cdot\rangle_{L'})$ are called *isometric* if there exists an $\mathcal{O}_{K,S}$-module isomorphism $\varphi\colon L \mapsto L'$ that is also an isometry.

The notion of isometric metrized S-line bundles defines an equivalence relation on the set of metrized S-line bundles. The set of equivalence classes of metrized S-line bundles of K is denoted by $\mathcal{ML}_{K,S}$. Throughout this thesis, for $(L, \langle\cdot,\cdot\rangle_L) \in \mathrm{ML}_{K,S}$ we denote its equivalence class in $\mathcal{ML}_{K,S}$ by $[(L, \langle\cdot,\cdot\rangle_L)]$.

Proposition 5.2.15. The set $\mathcal{ML}_{K,S}$ attains an abelian group structure.

Proof. We have seen that the operation $\circ$ is closed on the set $\mathrm{ML}_{K,S}$. Take $[(L, \langle\cdot,\cdot\rangle_L)], [(L', \langle\cdot,\cdot\rangle_{L'})] \in \mathcal{ML}_{K,S}$, then the operation $\bullet$, given by

$$[(L, \langle\cdot,\cdot\rangle_L)] \bullet [(L', \langle\cdot,\cdot\rangle_{L'})] := [(L, \langle\cdot,\cdot\rangle_L) \circ (L', \langle\cdot,\cdot\rangle_{L'})] = [(L \otimes_{\mathcal{O}_{K,S}} L', \langle\cdot,\cdot\rangle_{L\otimes L'})],$$

is closed on $\mathcal{ML}_{K,S}$. However, since we deal with equivalence classes on $\mathcal{ML}_{K,S}$, it needs to be checked that $\bullet$ is well-defined on $\mathcal{ML}_{K,S}$. So let $[(L, \langle\cdot,\cdot\rangle_L)] = [(L', \langle\cdot,\cdot\rangle_{L'})]$ in $\mathcal{ML}_{K,S}$. Then there exists an $\mathcal{O}_{K,S}$-module isomorphism $\varphi\colon L \mapsto L'$ such that it is also an isometry, i.e.

$$\langle u, v\rangle_L = \langle \psi(u), \psi(v)\rangle_{L'}, \qquad u, v \in L_{\mathbb{R}}, \tag{76}$$

where $\psi\colon L_{\mathbb{R}} \to L'_{\mathbb{R}}$ is given by the tensor map $\varphi \otimes \mathrm{id}_{K_{\mathbb{R}}}$. Take any $[(M, \langle\cdot,\cdot\rangle_M)] \in \mathcal{ML}_{K,S}$. Then $\bullet$ is well-defined if

$$[(L, \langle\cdot,\cdot\rangle_L)] \bullet [(M, \langle\cdot,\cdot\rangle_M)] = [(L', \langle\cdot,\cdot\rangle_{L'})] \bullet [(M, \langle\cdot,\cdot\rangle_M)].$$

Or equivalently

$$[(L \otimes_{\mathcal{O}_{K,S}} M, \langle\cdot,\cdot\rangle_{L\otimes M})] = [(L' \otimes_{\mathcal{O}_{K,S}} M, \langle\cdot,\cdot\rangle_{L'\otimes M})]. \tag{77}$$

So we need to construct an $\mathcal{O}_{K,S}$-module isomorphism from $L \otimes_{\mathcal{O}_{K,S}} M$ to $L' \otimes_{\mathcal{O}_{K,S}} M$ that is an isometry. Consider the map $\varphi'\colon L \otimes_{\mathcal{O}_{K,S}} M \to L' \otimes_{\mathcal{O}_{K,S}} M$ given by $\varphi' := \varphi \otimes \mathrm{id}_M$. Since φ and id_M are $\mathcal{O}_{K,S}$-module isomorphisms, so is φ' (see [Con24d, Theorem 2.11]). So it remains to show that φ' is an isometry. So consider the tensor map $\psi'\colon (L \otimes_{\mathcal{O}_{K,S}} M)_{\mathbb{R}} \to (L' \otimes_{\mathcal{O}_{K,S}} M)_{\mathbb{R}}$ given by $\psi' := \varphi' \otimes \mathrm{id}_{K_{\mathbb{R}}}$. This is under the isomorphism (73) transferred to $\psi'\colon L_{\mathbb{R}} \otimes_{K_{\mathbb{R}}} M_{\mathbb{R}} \to L'_{\mathbb{R}} \otimes_{K_{\mathbb{R}}} M_{\mathbb{R}}$ given by $\psi' = \psi \otimes \mathrm{id}_{M_{\mathbb{R}}}$. Now, for $u \otimes x, v \otimes y \in L_{\mathbb{R}} \otimes_{K_{\mathbb{R}}} M_{\mathbb{R}}$, we have using the $K_{\mathbb{R}}$-metric on $L_{\mathbb{R}} \otimes_{K_{\mathbb{R}}} M_{\mathbb{R}}$ that

$$\langle u \otimes x, v \otimes y\rangle_{L\otimes M} = \langle u, v\rangle_L \langle x, y\rangle_M = \langle \psi(u), \psi(v)\rangle_{L'} \langle x, y\rangle_M,$$

where we used Equation (76). Hence, using the $K_{\mathbb{R}}$-metric on $L'_{\mathbb{R}} \otimes_{K_{\mathbb{R}}} M_{\mathbb{R}}$, we have that

$$\langle \psi(u), \psi(v)\rangle_{L'} \langle x, y\rangle_M = \langle \psi(u) \otimes x, \psi(v) \otimes y\rangle_{L'\otimes M} = \langle \psi'(u \otimes x), \psi'(v \otimes y)\rangle_{L'\otimes M}.$$

So we see that

$$\langle u \otimes x, v \otimes y\rangle_{L\otimes M} = \langle \psi'(u \otimes x), \psi'(v \otimes y)\rangle_{L'\otimes M}.$$

By extending this over $K_{\mathbb{R}}$, we can say that φ' is an isometry. This means that $(L \otimes_{\mathcal{O}_{K,S}} M, \langle\cdot,\cdot\rangle_{L\otimes M})$ and $(L' \otimes_{\mathcal{O}_{K,S}} M, \langle\cdot,\cdot\rangle_{L'\otimes M})$ are isometric. Thus, Equation (77) holds.

Next, we will show that $[(\mathcal{O}_{K,S}, \langle\cdot,\cdot\rangle_1)] \in \mathcal{ML}_{K,S}$ plays the role of the unit element. Take any metrized S-line bundle $[(L, \langle\cdot,\cdot\rangle_L)]$. We have to show that

$$[(L, \langle\cdot,\cdot\rangle_L)] \bullet [(\mathcal{O}_{K,S}, \langle\cdot,\cdot\rangle_1)] = [(L, \langle\cdot,\cdot\rangle_L)].$$

Or equivalently

$$[(L \otimes_{\mathcal{O}_{K,S}} \mathcal{O}_{K,S}, \langle\cdot,\cdot\rangle_{L\otimes\mathcal{O}_{K,S}})] = [(L, \langle\cdot,\cdot\rangle_L)]. \tag{78}$$

So we need to construct an $\mathcal{O}_{K,S}$-module isomorphism from $L \otimes_{\mathcal{O}_{K,S}} \mathcal{O}_{K,S}$ to L that is an isometry. We know that there exists an $\mathcal{O}_{K,S}$-module isomorphism $\varphi\colon L \otimes_{\mathcal{O}_{K,S}} \mathcal{O}_{K,S} \to L$ given by $a \otimes x \mapsto ax$, and is extended by $\mathcal{O}_{K,S}$-linearity. So it remains to show that φ is an isometry. The tensor map $\psi\colon (L \otimes_{\mathcal{O}_{K,S}} \mathcal{O}_{K,S})_{\mathbb{R}} \to L_{\mathbb{R}}$ given by $\psi := \varphi \otimes \mathrm{id}_{K_{\mathbb{R}}}$ is under the isomorphisms (72) and (73) transferred to $\psi\colon L_{\mathbb{R}} \otimes_{K_{\mathbb{R}}} K_{\mathbb{R}} \to L_{\mathbb{R}}$ given by $u \otimes \alpha \mapsto \alpha u$, and is extended by $K_{\mathbb{R}}$-linearity. Now, for $u \otimes \alpha, v \otimes \beta \in L_{\mathbb{R}} \otimes_{K_{\mathbb{R}}} K_{\mathbb{R}}$, we have using the $K_{\mathbb{R}}$-metric on $L_{\mathbb{R}} \otimes_{K_{\mathbb{R}}} K_{\mathbb{R}}$ that

$$\langle u \otimes \alpha, v \otimes \beta \rangle_{L \otimes \mathcal{O}_{K,S}} = \langle \alpha u \otimes 1, \beta v \otimes 1 \rangle_{L \otimes \mathcal{O}_{K,S}} = \langle \alpha u, \beta v \rangle_L \langle 1, 1 \rangle_1 = \langle \alpha u, \beta v \rangle_L = \langle \psi(u \otimes \alpha), \psi(v \otimes \beta) \rangle_L, \tag{79}$$

where we used bilinearity over $K_{\mathbb{R}}$ and that $\langle 1, 1 \rangle_1 = 1$. By extending Equation (79) over $K_{\mathbb{R}}$, we can say that φ is an isometry. This means that $(L \otimes_{\mathcal{O}_{K,S}} \mathcal{O}_{K,S}, \langle \cdot, \cdot \rangle_{L \otimes \mathcal{O}_{K,S}})$ and $(L, \langle \cdot, \cdot \rangle_L)$ are isometric. Hence, Equation (78) holds.

Next, we will show that $[(L^*, \langle \cdot, \cdot \rangle_{L^*})] \in \mathcal{ML}_{K,S}$ is the inverse for any $[(L, \langle \cdot, \cdot \rangle_L)] \in \mathcal{ML}_{K,S}$. So we must show that

$$[(L, \langle \cdot, \cdot \rangle_L)] \bullet [(L^*, \langle \cdot, \cdot \rangle_{L^*})] = [(\mathcal{O}_{K,S}, \langle \cdot, \cdot \rangle_1)].$$

Or equivalently

$$[(L \otimes_{\mathcal{O}_{K,S}} L^*, \langle \cdot, \cdot \rangle_{L \otimes L^*})] = [(\mathcal{O}_{K,S}, \langle \cdot, \cdot \rangle_1)]. \tag{80}$$

So we need to construct an $\mathcal{O}_{K,S}$-module isomorphism from $L \otimes_{\mathcal{O}_{K,S}} L^*$ to $\mathcal{O}_{K,S}$ that is an isometry. We know that there exists an $\mathcal{O}_{K,S}$-module isomorphism $\varphi\colon L \otimes_{\mathcal{O}_{K,S}} L^* \to \mathcal{O}_{K,S}$ given by $a \otimes f \mapsto f(a)$, and is extended by $\mathcal{O}_{K,S}$-linearity. So it remains to show that φ is an isometry. Consider the tensor map $\psi\colon (L \otimes_{\mathcal{O}_{K,S}} L^*)_{\mathbb{R}} \to (\mathcal{O}_{K,S})_{\mathbb{R}}$ given by $\psi := \varphi \otimes \mathrm{id}_{K_{\mathbb{R}}}$. This is under the isomorphisms (72), (73), and (75) transferred to $\psi\colon L_{\mathbb{R}} \otimes_{K_{\mathbb{R}}} L^*_{\mathbb{R}} \to K_{\mathbb{R}}$ given by $u \otimes x^* \mapsto x^*(u) = \langle u, x \rangle_L$, and is extended by $K_{\mathbb{R}}$-linearity. For $x, y \in K_{\mathbb{R}}$, consider the map $\langle x, y \rangle = \langle \psi^{-1}(x), \psi^{-1}(y) \rangle_{L \otimes L^*}$. Since φ and $\mathrm{id}_{K_{\mathbb{R}}}$ are $\mathcal{O}_{K,S}$-module isomorphisms, so is ψ (see [Con24d, Theorem 2.11]). It can even be extended to a $K_{\mathbb{R}}$-module isomorphism. Therefore, the map $\langle \cdot, \cdot \rangle$ is a $K_{\mathbb{R}}$-metric on $K_{\mathbb{R}}$. By Proposition 5.2.11, it must be of the form $\langle \cdot, \cdot \rangle_\alpha$ for some $\alpha \in \bigoplus_{\sigma \in \Sigma_K^\infty} \mathbb{R}_{>0}$. Then

$$\langle \psi^{-1}(x), \psi^{-1}(y) \rangle_{L \otimes L^*} = \langle x, y \rangle_\alpha = \alpha^2 x \overline{y} = \alpha^2 \langle x, y \rangle_1.$$

Now, take $x = \psi(u \otimes w^*)$ and $y = \psi(v \otimes z^*)$ for some arbitrarily $u \otimes w^*, v \otimes z^* \in L_{\mathbb{R}} \otimes_{K_{\mathbb{R}}} L^*_{\mathbb{R}}$. Then we get

$$\langle u \otimes w^*, v \otimes z^* \rangle_{L \otimes L^*} = \alpha^2 \langle \psi(u \otimes w^*), \psi(v \otimes z^*) \rangle_1. \tag{81}$$

Take $u \otimes u^* \in L_{\mathbb{R}} \otimes_{K_{\mathbb{R}}} L^*_{\mathbb{R}}$, then Equation (81) tells us that

$$\langle u \otimes u^*, u \otimes u^* \rangle_{L \otimes L^*} = \alpha^2 \langle \psi(u \otimes u^*), \psi(u \otimes u^*) \rangle_1. \tag{82}$$

Using the $K_{\mathbb{R}}$-metric on $L_{\mathbb{R}} \otimes_{K_{\mathbb{R}}} L^*_{\mathbb{R}}$ and $L^*_{\mathbb{R}}$, the left hand side is given by

$$\langle u \otimes u^*, u \otimes u^* \rangle_{L \otimes L^*} = \langle u, u \rangle_L \langle u^*, u^* \rangle_{L^*} = \langle u, u \rangle_L \overline{\langle u, u \rangle_L}.$$

Using the construction of ψ, the right hand side of Equation (82) is given by

$$\alpha^2 \langle \psi(u \otimes u^*), \psi(u \otimes u^*) \rangle_1 = \alpha^2 \langle \langle u, u \rangle_L, \langle u, u \rangle_L \rangle_1 = \alpha^2 \langle u, u \rangle_L \overline{\langle u, u \rangle_L}.$$

Comparing the left and right hand sides, we see that $\alpha^2 = 1$. Since $\alpha \in \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}_{>0}$, we must have $\alpha = 1$. Hence, Equation (81) becomes

$$\langle u \otimes w^*, v \otimes z^* \rangle_{L \otimes L^*} = \langle \psi(u \otimes w^*), \psi(v \otimes z^*) \rangle_1.$$

By extending this over $K_{\mathbb{R}}$, we can say that φ is an isometry. This means that $(L \otimes_{\mathcal{O}_{K,S}} L^*, \langle \cdot, \cdot \rangle_{L \otimes L^*})$ and $(\mathcal{O}_{K,S}, \langle \cdot, \cdot \rangle_1)$ are isometric. Thus, Equation (80) holds.

Lastly, the group operation is abelian and associative since these are properties of the tensor product and the product over $K_{\mathbb{R}}$. □

In the following arguments, we will work towards the result that $\mathrm{Pic}_{K,S}$ is isomorphic to $\mathcal{ML}_{K,S}$.

Recall the Minkowski embedding $\Psi\colon K \to K_{\mathbb{R}}$ from Definition 1.8.3. For $u \in \prod_{\sigma\in\Sigma_K^\infty} \mathbb{R}_{>0} \subseteq K_{\mathbb{R}}$ and $I \in \mathrm{Id}_{K,S}$, we define the $\mathcal{O}_{K,S}$-module $u\Psi(I)$ by $x \cdot u\Psi(a) := u\Psi(xa)$ for some $u\Psi(a) \in u\Psi(I)$ and $x \in \mathcal{O}_{K,S}$.

Lemma 5.2.16. For any $I \in \mathrm{Id}_{K,S}$ and $u \in \prod_{\sigma\in\Sigma_K^\infty} \mathbb{R}_{>0}$, there exists an $\mathcal{O}_{K,S}$-module isomorphism $I \cong u\Psi(I)$. Moreover, one has $u\Psi(I) \in P^1_{\mathcal{O}_{K,S}}$.

Proof. Consider the map $f\colon K \to K_{\mathbb{R}}$ defined by $x \mapsto u\Psi(x)$. Since u is a unit of $K_{\mathbb{R}}$ and Ψ injective, the map f is injective. Furthermore, since Ψ is a ring homomorphism, the map f is an $\mathcal{O}_{K,S}$-module homomorphism. Restricting f to I gives us the desired isomorphism.

In Lemma 5.2.7, we saw that $I \in P^1_{\mathcal{O}_{K,S}}$ for any $I \in \mathrm{Id}_{K,S}$. Equivalently, the fractional ideal I is a finitely generated and projective $\mathcal{O}_{K,S}$-module. Since these properties are preserved under isomorphism, it follows that the $\mathcal{O}_{K,S}$-module $u\Psi(I)$ has these properties as well. It follows from Corollary 5.2.5 that $u\Psi(I)$ has a constant rank given by $\mathrm{rank}(u\Psi(I)) = \dim_K u\Psi(I) \otimes_{\mathcal{O}_{K,S}} K$. Since $I \cong u\Psi(I)$, we also have $u\Psi(I) \otimes_{\mathcal{O}_{K,S}} K_{\mathbb{R}} \cong I \otimes_{\mathcal{O}_{K,S}} K_{\mathbb{R}}$. Then

$$\mathrm{rank}(u\Psi(I)) = \dim_K u\Psi(I) \otimes_{\mathcal{O}_{K,S}} K = \dim_K I \otimes_{\mathcal{O}_{K,S}} K = 1,$$

where we used that I has a constant rank equal to 1. Consequently, we also have $u\Psi(I) \in P^1_{\mathcal{O}_{K,S}}$. □

To make $u\Psi(I)$, for any $I \in \mathrm{Id}_{K,S}$ and $u \in \prod_{\sigma\in\Sigma_K^\infty} \mathbb{R}_{>0}$, a metrized S-line bundle, we need to endow $(u\Psi(I))_{\mathbb{R}}$ with a $K_{\mathbb{R}}$-metric. Note that

$$(u\Psi(I))_{\mathbb{R}} = u\Psi(I) \otimes_{\mathcal{O}_{K,S}} K_{\mathbb{R}} \cong I \otimes_{\mathcal{O}_{K,S}} K_{\mathbb{R}} \cong K_{\mathbb{R}}, \tag{83}$$

where we used Lemma 5.2.16, and the last $\mathcal{O}_{K,S}$-module isomorphism follows from Proposition 1.8.2. This is even a $K_{\mathbb{R}}$-module isomorphism. So endowing $(u\Psi(I))_{\mathbb{R}}$ with a $K_{\mathbb{R}}$-metric is equivalent to endowing $K_{\mathbb{R}}$ with a $K_{\mathbb{R}}$-metric. Hence, we can take any $K_{\mathbb{R}}$-metric that we have seen in Proposition 5.2.11. We take the $K_{\mathbb{R}}$-metric given by $\langle\cdot,\cdot\rangle_u$. Hence, we have $(u\Psi(I), \langle\cdot,\cdot\rangle_u) \in \mathrm{ML}_{K,S}$.

Lemma 5.2.17. Let $[(u\Psi(I), \langle\cdot,\cdot\rangle_u)], [(v\Psi(J), \langle\cdot,\cdot\rangle_v)] \in \mathcal{ML}_{K,S}$ for some $I, J \in \mathrm{Id}_{K,S}$ and $u, v \in \prod_{\sigma\in\Sigma_K^\infty} \mathbb{R}_{>0}$. Then

$$[(u\Psi(I), \langle\cdot,\cdot\rangle_u)] \bullet [(v\Psi(J), \langle\cdot,\cdot\rangle_v)] = [(uv\Psi(IJ), \langle\cdot,\cdot\rangle_{uv})].$$

Proof. We have

$$[(u\Psi(I), \langle\cdot,\cdot\rangle_u)] \bullet [(v\Psi(J), \langle\cdot,\cdot\rangle_v)] = [(u\Psi(I) \otimes_{\mathcal{O}_{K,S}} v\Psi(J), \langle\cdot,\cdot\rangle_{u\Psi(I)\otimes v\Psi(J)})].$$

Thus, we must show that

$$[(u\Psi(I) \otimes_{\mathcal{O}_{K,S}} v\Psi(J), \langle\cdot,\cdot\rangle_{u\Psi(I)\otimes v\Psi(J)})] = [(uv\Psi(IJ), \langle\cdot,\cdot\rangle_{uv})]. \tag{84}$$

So we need to construct an $\mathcal{O}_{K,S}$-module isomorphism from $u\Psi(I) \otimes_{\mathcal{O}_{K,S}} v\Psi(J)$ to $uv\Psi(IJ)$ that is an isometry. Extend $\varphi\colon u\Psi(I) \otimes_{\mathcal{O}_{K,S}} v\Psi(J) \to uv\Psi(IJ)$ given by $w \otimes w' \mapsto ww'$ over $\mathcal{O}_{K,S}$ to an $\mathcal{O}_{K,S}$-module homomorphism. The map φ is injective since u, v are units of $K_{\mathbb{R}}$ and Ψ is injective. Any element of IJ is of the form $\sum_{i=1}^m x_i y_i$ for some $x_i \in I$, $y_i \in J$, and $m \in \mathbb{Z}_{>0}$. For any $uv\Psi(\sum_{i=1}^m x_i y_i) \in uv\Psi(IJ)$, we can take

$$w := \sum_{i=1}^m (u\Psi(x_i)) \otimes (v\Psi(y_i)),$$

such that $\varphi(w) = uv\Psi(\sum_{i=1}^m x_i y_i)$. This means that φ is surjective. It follows that φ is an $\mathcal{O}_{K,S}$-module isomorphism. So it remains to show that φ is an isometry.

Consider the tensor map $\psi\colon (u\Psi(I)\otimes_{\mathcal{O}_{K,S}} v\Psi(J))_{\mathbb{R}} \to (\mathcal{O}_{K,S})_{\mathbb{R}}$ given by $\psi := \varphi\otimes \mathrm{id}_{K_{\mathbb{R}}}$. This is under the isomorphisms (72), (73), and (83), transferred to $\psi\colon K_{\mathbb{R}}\otimes_{K_{\mathbb{R}}} K_{\mathbb{R}} \to K_{\mathbb{R}}$ given by $x\otimes y\mapsto xy$, and is extended by $K_{\mathbb{R}}$-linearity. Now, for $w\otimes y, x\otimes z\in K_{\mathbb{R}}\otimes_{K_{\mathbb{R}}} K_{\mathbb{R}}$, we have using the $K_{\mathbb{R}}$-metric on $K_{\mathbb{R}}\otimes_{K_{\mathbb{R}}} K_{\mathbb{R}}$ that

$$\langle w\otimes y, x\otimes z\rangle_{u\Psi(I)\otimes_{\mathcal{O}_{K,S}} v\Psi(J)} = \langle w,x\rangle_u\langle y,z\rangle_v = (uv)^2 wy\overline{xz} = \langle wy, xz\rangle_{uv} = \langle \psi(w\otimes y), \psi(x\otimes z)\rangle_{uv}, \quad (85)$$

where we used the construction of $\langle\cdot,\cdot\rangle_u$ and $\langle\cdot,\cdot\rangle_v$. By extending Equation (85) over $K_{\mathbb{R}}$, we can say that φ is an isometry. This means that $(u\Psi(I)\otimes_{\mathcal{O}_{K,S}} v\Psi(J), \langle\cdot,\cdot\rangle_{u\Psi(I)\otimes v\Psi(J)})$ and $(uv\Psi(IJ), \langle\cdot,\cdot\rangle_{uv})$ are isometric. Consequently, Equation (84) holds. □

Theorem 5.2.18. The map $f\colon \mathrm{Pic}_{K,S}\to \mathcal{ML}_{K,S}$ given by $[(I,u)_S]\mapsto [(u\Psi(I), \langle\cdot,\cdot\rangle_u)]$ is a group isomorphism.

Proof. Firstly, we need to check whether f is well-defined. So suppose that $[(I,u)_S] = [(J,v)_S]$ in $\mathrm{Pic}_{K,S}$. We must show that

$$[(u\Psi(I), \langle\cdot,\cdot\rangle_u)] = [(v\Psi(J), \langle\cdot,\cdot\rangle_v)].$$

So we need to construct an $\mathcal{O}_{K,S}$-module isomorphism from $u\Psi(I)$ to $v\Psi(J)$ that is an isometry. We know that there exists some $x\in K^*$ such that

$$(I,u)_S = (J,v)_S + \mathrm{div}_S(x) = (J,v)_S + (x^{-1}\mathcal{O}_{K,S}, \hat{x})_S = (x^{-1}J, \hat{x}v)_S. \quad (86)$$

Hence, we have $I = x^{-1}J$. Since $u,v,\Psi(x)\in K_{\mathbb{R}}^*$, we have that the map $\varphi\colon u\Psi(I)\to v\Psi(J)$ given by $w\mapsto \frac{\Psi(x)v}{u}w$ is an $\mathcal{O}_{K,S}$-module isomorphism. So it remains to show that φ is an isometry. Consider the tensor map $\psi\colon (u\Psi(I))_{\mathbb{R}}\to (v\Psi(J))_{\mathbb{R}}$ given by $\psi := \varphi\otimes \mathrm{id}_{K_{\mathbb{R}}}$. Under isomorphism (83) this map is transformed to $\psi\colon K_{\mathbb{R}}\to K_{\mathbb{R}}$ given by $w\mapsto \Psi(x)w$. Note that $|x|_\sigma^2 = |\sigma(x)|_\infty^2 = \sigma(x)\overline{\sigma(x)}$ for all $\sigma\in\Sigma_K^\infty$. So we have that $(\hat{x})^2 = \Psi(x)\overline{\Psi(x)}$. Now, from Equation (86) we can also conclude that $u = \hat{x}v$. So for $w,w'\in K_{\mathbb{R}}$, we have

$$\langle w,w'\rangle_u = u^2 w\overline{w'} = (\hat{x})^2v^2w\overline{w'} = \Psi(x)\overline{\Psi(x)}v^2w\overline{w'} = \langle \Psi(x)w, \Psi(x)w'\rangle_v = \langle\psi(w),\psi(w')\rangle_v, \quad (87)$$

where we used the construction of $\langle\cdot,\cdot\rangle_u$ and $\langle\cdot,\cdot\rangle_v$. By extending Equation (87) over $K_{\mathbb{R}}$, we can say that φ is an isometry. Thus, we see that $(u\Psi(I),\langle\cdot,\cdot\rangle_u)$ and $(v\Psi(J),\langle\cdot,\cdot\rangle_v)$ are isometric. We obtain that $f([(I,u)_S]) = f([(J,v)_S])$, i.e. the map f is well-defined.

Next, we show that f is a group homomorphism. Using Lemma 5.2.16 and the strategy of the examples of isometric metrized S-line bundles that we have seen up to now, it is not hard to check that

$$[(\Psi(\mathcal{O}_{K,S}), \langle\cdot,\cdot\rangle_1)] = [(\mathcal{O}_{K,S}, \langle\cdot,\cdot\rangle_1)].$$

So

$$f([\mathcal{O}_{K,S}, (1)_{\sigma\in\Sigma_K^\infty}]) = [(\Psi(\mathcal{O}_{K,S}), \langle\cdot,\cdot\rangle_1)] = [(\mathcal{O}_{K,S}, \langle\cdot,\cdot\rangle_1)].$$

Hence, the unit element of $\mathrm{Pic}_{K,S}$ is sent to the unit element of $\mathcal{ML}_{K,S}$. Furthermore, for the elements $[(I,u)_S], [(J,v)_S]\in \mathrm{Pic}_{K,S}$, we have

$$\begin{aligned} f([(I,u)_S] + [(J,v)_S]) &= f([(IJ,uv)_S]) = [(uv\Psi(IJ), \langle\cdot,\cdot\rangle_{uv})] \\ &= [(u\Psi(I), \langle\cdot,\cdot\rangle_u)] \bullet [(v\Psi(J), \langle\cdot,\cdot\rangle_v)] \\ &= f([(I,u)_S]) \bullet f([(J,v)_S]), \end{aligned}$$

where we used Lemma 5.2.17.

Now, suppose that $f([(I,u)_S]) = f([(J,v)_S])$ for some $[(I,u)_S], [(J,v)_S]\in \mathrm{Pic}_{K,S}$. Then $(u\Psi(I),\langle\cdot,\cdot\rangle_u)$ and $(v\Psi(J),\langle\cdot,\cdot\rangle_v)$ are isometric. Thus, there exists an $\mathcal{O}_{K,S}$-module isomorphism $\varphi\colon u\Psi(I)\to v\Psi(J)$. So given $x\in I$ there exists a unique $y\in J$ such that $\varphi(u\Psi(x)) = v\Psi(y)$ and vice versa. We conclude that φ induces

an $\mathcal{O}_{K,S}$-module isomorphism $h\colon I \to J$. Now, take any non-zero $x \in I \subseteq K$. Since K is the field of fractions of $\mathcal{O}_{K,S}$, there exist non-zero $a, b \in \mathcal{O}_{K,S}$ such that $x = \frac{a}{b}$. Then $a = b\frac{a}{b} \in \mathcal{O}_{K,S}I = I$. Using that h is an $\mathcal{O}_{K,S}$-module homomorphism, we have

$$h(a) = h\left(b\frac{a}{b}\right) = bh\left(\frac{a}{b}\right) \quad \implies h(x) = \frac{h(a)}{b}.$$

Now, since I is a fractional ideal of $\mathcal{O}_{K,S}$, there exists a non-zero $\alpha \in \mathcal{O}_{K,S}$ such that $\alpha I \subseteq \mathcal{O}_{K,S} \cap I$. Hence, there is a non-zero $c \in \mathcal{O}_{K,S} \cap I$. Since both $a, c \in I$, we have

$$ch(x) = \frac{ch(a)}{b} = \frac{h(ac)}{b} = \frac{ah(c)}{b} = h(c)x \quad \implies h(x) = (c^{-1}h(c))x.$$

This means that the $\mathcal{O}_{K,S}$-module isomorphism h is given by multiplication by some $z := c^{-1}h(c) \in K^*$, and so $J = zI$. Since $(u\Psi(I), \langle\cdot,\cdot\rangle_u)$ and $(v\Psi(J), \langle\cdot,\cdot\rangle_v)$ are isometric, we also have that

$$\langle w, w'\rangle_u = \langle \psi(w), \psi(w')\rangle_v, \qquad w, w' \in (u\Psi(I))_{\mathbb{R}}, \tag{88}$$

where $\psi\colon (u\Psi(I))_{\mathbb{R}} \to (v\Psi(J))_{\mathbb{R}}$ is given by the tensor map $\varphi \otimes \mathrm{id}_{K_{\mathbb{R}}}$. Under isomorphism (83), this map is transformed to $\psi\colon K_{\mathbb{R}} \to K_{\mathbb{R}}$ given by $\psi(w) = \Psi(z)w$. For $w, w' \in K_{\mathbb{R}}^*$, we have using Equation (88) that

$$u^2 w\overline{w'} = \langle w, w'\rangle_u = \langle \psi(w), \psi(w')\rangle_v = \langle \Psi(z)w, \Psi(z)w'\rangle_v = v^2\Psi(z)\overline{\Psi(z)}w\overline{w'} = v^2(\hat{z})^2 w\overline{w'}.$$

Since $w, w' \in K_{\mathbb{R}}^*$, we have $u^2 = v^2(\hat{z})^2$. Or equivalently $u = v\hat{z}$. So we get that

$$(J, v)_S = (zI, u\hat{z}^{-1})_S = (I, u)_S + \mathrm{div}_S(z^{-1}).$$

We see that $[(I, u)_S]) = [(J, v)_S]$ in $\mathrm{Pic}_{K,S}$. In conclusion, the group homomorphism f is injective.

Take any $[(L, \langle\cdot,\cdot\rangle)] \in \mathcal{ML}_{K,S}$. Since $L \in P^1_{\mathcal{O}_{K,S}}$, there exists an $\mathcal{O}_{K,S}$-module isomorphism $\varphi\colon L \to I$ for some $I \in \mathrm{Id}_{K,S}$ (see Lemma 5.2.7). Consider the tensor map $\psi\colon L_{\mathbb{R}} \to I_{\mathbb{R}}$ given by $\psi := \varphi \otimes \mathrm{id}_{K_{\mathbb{R}}}$. By isomorphism (83), we know that $I_{\mathbb{R}} = I \otimes_{\mathcal{O}_{K,S}} K_{\mathbb{R}} \cong K_{\mathbb{R}}$ as $K_{\mathbb{R}}$-modules. Hence, we have a map $\langle\cdot,\cdot\rangle\colon K_{\mathbb{R}} \times K_{\mathbb{R}} \to K_{\mathbb{R}}$ given by $\langle x, y\rangle = \langle \psi^{-1}(x), \psi^{-1}(y)\rangle_L$. Since φ and $\mathrm{id}_{K_{\mathbb{R}}}$ are $\mathcal{O}_{K,S}$-module isomorphisms, so is ψ (see [Con24d, Theorem 2.11]). It can even be extended to a $K_{\mathbb{R}}$-module isomorphism. Consequently, the map $\langle\cdot,\cdot\rangle$ is a $K_{\mathbb{R}}$-metric on $K_{\mathbb{R}}$. By Proposition 5.2.11, it must be of the form $\langle\cdot,\cdot\rangle_u$ for some $u \in \bigoplus_{\sigma\in\Sigma_K^\infty} \mathbb{R}_{>0}$. Then we have

$$\langle \psi(x), \psi(y)\rangle_u = \langle \psi(x), \psi(y)\rangle = \langle x, y\rangle_L,$$

for $v, w \in K_{\mathbb{R}}$. By extending this over $K_{\mathbb{R}}$, we can say that φ is an isometry with metrized S-line bundles $(L, \langle\cdot,\cdot\rangle)$ and $(I, \langle\cdot,\cdot\rangle_u)$. We see that $(L, \langle\cdot,\cdot\rangle)$ and $(I, \langle\cdot,\cdot\rangle_u)$ are isometric. In its turn $(I, \langle\cdot,\cdot\rangle_u)$ is isometric to $(u\Psi(I), \langle\cdot,\cdot\rangle_u)$. This follows directly from Lemma 5.2.16. Then

$$f([(I, u)_S]) = [(u\Psi(I), \langle\cdot,\cdot\rangle_u)] = [(I, \langle\cdot,\cdot\rangle_u)] = [(L, \langle\cdot,\cdot\rangle_L)].$$

Therefore, the group homomorphism f is surjective.

It follows that the group homomorphism f induces a group isomorphism $\mathrm{Pic}_{K,S} \cong \mathcal{ML}_{K,S}$. □

5.2.3 Ideal S-Lattices

At the beginning of the previous section, we explained that in this section we will use the S-Minkowski embedding Ψ_S to view things in K_S. Just like metrized S-line bundles, the extension of ideal lattices that we will see in this section is not a complete extension. So if we take $S = \emptyset$, we do not recover ideal lattices as defined in Definition 4.1.12. However, we use the ideas of being an ideal and lattice simultaneously. When $S = \emptyset$, this was also done by [DB22] in Sections 1.2 and 2.5. Therefore, we generalize those constructions. The proof of Theorem 5.2.26 uses the ideas of the proof of [DB22, Lemma 2.21]. Furthermore, the proof of Proposition 5.2.23 is based on the proof for $S = \emptyset$ explained by De Boer in person.

Section 1.2 of [DB22] gives an alternative, more straightforward, definition of ideal lattices.

Definition 5.2.19. An *ideal lattice* of K is defined as a complete lattice $\Gamma \subseteq K_{\mathbb{R}}$ that satisfies $\Psi(\mathcal{O}_K)\Gamma \subseteq \Gamma$.

Since $K_{\mathbb{R}}$ is a Euclidean space, we can use Definition 1.7.1 for the definition of a complete lattice. There is a natural way of extending the definition of ideal lattices to the rings of S-integers.

Definition 5.2.20. An *ideal S-lattice* of K is defined as a lattice $\Gamma \subseteq K_S$ that satisfies $\Psi(\mathcal{O}_{K,S})\Gamma \subseteq \Gamma$. The set of ideal S-lattices is denoted by $\mathrm{IdLat}_{K,S}$.

Recall that K_S is an abelian L-group. Therefore, in this case, we use Theorem 2.6.4 to say that a lattice in K_S is a discrete and co-compact subgroup. Recall the notation of $\mathfrak{D}_S$ from Equation (32).

Proposition 5.2.21. Let $I \in \mathrm{Id}_{K,S}$ be non-zero and $u \in K_S^*$. Then $u\Psi_S(I)$ is an ideal S-lattice. Moreover, its covolume is given by

$$\mathrm{covol}(u\Psi_S(I)) = \left(\prod_{\nu \in S^\infty} \|u_\nu\|_\nu\right) N_{\mathcal{O}_{K,S}}(I)\sqrt{|d_K|_\infty \mathfrak{D}_S^{-1}}.$$

Proof. In Theorem 3.4.6, we have seen that $\Psi_S(I)$ is a lattice for any non-zero $I \in \mathrm{Id}_{K,S}$. Then in Lemma 3.4.5, we have seen that $u\Psi_S(I)$ is a lattice in K_S of covolume

$$\mathrm{covol}(u\Psi_S(I)) = \left(\prod_{\nu \in S^\infty} \|u_\nu\|_\nu\right) \mathrm{covol}(\Psi_S(I)).$$

In Proposition 3.4.8, we have seen that $\mathrm{covol}(\Psi_S(I)) = N_{\mathcal{O}_{K,S}}(I)\sqrt{|d_K|_\infty \mathfrak{D}_S^{-1}}$. We get

$$\mathrm{covol}(u\Psi_S(I)) = \left(\prod_{\nu \in S^\infty} \|u_\nu\|_\nu\right) N_{\mathcal{O}_{K,S}}(I)\sqrt{|d_K|_\infty \mathfrak{D}_S^{-1}}.$$

It remains to show that $\Psi(\mathcal{O}_{K,S})(u\Psi_S(I)) \subseteq u\Psi_S(I)$. Proposition 3.3.16 tells us that Ψ_S is a ring homomorphism. Hence, we have

$$\Psi_S(\mathcal{O}_{K,S})(u\Psi_S(I)) \subseteq u\Psi_S(I\mathcal{O}_{K,S}) = \Psi_S(I),$$

using that $I\mathcal{O}_{K,S} = I$. □

In the classical work of lattices, we made a distinction between complete and not complete lattices (see Definition 1.7.1). If a lattice Γ in $\mathbb{R}^m$ is not complete, then it might happen that $\Gamma \cap (\mathbb{R}^m)^* = \emptyset$. In this case, we view $\mathbb{R}^m$ as a ring by entry-wise multiplication. For example, take $m = 2$ and Γ the lattice spanned by $(0, 1)$. Then Γ is not complete as it is only spanned by one vector. Moreover, we have $\Gamma = \{(0, k) : k \in \mathbb{Z}\}$ and $(\mathbb{R}^2)* = \{(x, y) : x, y \neq 0\}$. Hence, we see that $\Gamma \cap (\mathbb{R}^2)^* = \emptyset$. If a lattice is complete in $\mathbb{R}^m$, then it will always contain a unit of $\mathbb{R}^m$. Namely, a complete lattice covers all directions of $\mathbb{R}^m$. So it must contain an element that has non-zero entries. In Remark 2.6.5, we saw that our definition of lattices in an abelian L-group is an extension of complete lattices in a Euclidean space. Therefore, we would like to obtain a similar result. Recall Remark 3.3.18 for the multiplicative units of K_S denoted by K_S^*.

Lemma 5.2.22. Let Γ be a lattice of K_S. Then $\Gamma \cap K_S^* \neq \emptyset$.

Proof. Suppose, for the matter of contradiction, that $\Gamma \cap K_S^* = \emptyset$. Consider the projections from Γ into K_ν for all $\nu \in S^\infty$. If the images of all projections are not equal to $\{0\}$, then you can construct an element with all non-zero entries in Γ, since Γ is closed under addition. This would contradict the assumption. Hence, there exists some $\nu \in S$ such that the image of the projection of Γ into K_ν equals $\{0\}$. Fix such a $\nu \in S^\infty$, and let $\rho : K_S \to K_\nu$ be the corresponding projection. If A is open in K_ν then $\rho^{-1}(A)$ is open in K_S. This follows from the fact that K_S is endowed with the product topology. Moreover, the map ρ is an open mapping (see [Sin19, Proposition 2.2.2]). For $x \in K_\nu$, let x^ν denote the element in K_S which has all zero entries except for x at the entry of ν. This notation will only be used throughout this proof. Consider the map

$f\colon K_\nu \to K_S$ defined by $f(x) = x^\nu$. This is an injective map, and hence f induces a bijection $f\colon K_\nu \to f(K_S)$. We claim that f is a homeomorphism. Therefore, it remains to show that f and its inverse, denoted by $f' : f(K_\nu) \to K_\nu$, are continuous. So take any open subset $A \subseteq f(K_\nu)$. Then $f^{-1}(A) = \rho(A)$. So this is open since ρ is an open mapping. We conclude that f is continuous. Now, take any closed subset $A \subseteq K_\nu$. Then $(f')^{-1}(A) = \{x^\nu \in K_S : x \in A\}$. This set is given by the product of A at ν and $\{0\}$ at all $\eta \in S^\infty \backslash \{\nu\}$. Since A is closed in K_ν and $\{0\}$ in K_η for all $S^\infty\backslash\{\nu\}$, we have that $(f')^{-1}(A)$ is closed in K_S. So we can see that f' is also continuous. Consequently, we know that K_ν and $f(K_\nu)$ are homeomorphic.

Now, consider the canonical map $\phi\colon K_S \to K_S/\Gamma$. Since we endow K_S/Γ with the quotient topology, this map is continuous. Take $x^\nu, y^\nu \in f(K_\nu)$ for some $x, y \in K_\nu$. If $\phi(x^\nu) = \phi(y^\nu)$, then $x^\nu - y^\nu \in \Gamma$. Since the image of the projection of Γ into K_ν equals $\{0\}$, we must have $x = y$. Therefore, also $x^\nu = y^\nu$. It follows that ϕ is injective on $f(K_\nu)$. Therefore, the map ϕ induces a bijection $\phi : f(K_\nu) \to \phi(f(K_\nu))$. We claim that this is a homeomorphism. Since ϕ is already continuous, it remains to show that the inverse, denoted by $\phi' : \phi(f(K_\nu)) \to f(K_\nu)$ is continuous. So take any open subset $A \subseteq f(K_\nu)$. Then $(\phi')^{-1}(A) = \{[a] \in K_S/\Gamma : a \in A\}$. With respect to the quotient topology, this is open in K_S/Γ if

$$\phi^{-1}(\{[a] \in K_S/\Gamma : a \in A\}) = A + \Gamma$$

is open in K_S. Write $A + \Gamma = \bigcup_{u\in\Gamma}(A + u)$. By Corollary 2.1.4, the set $A + u$ is open for all $u \in \Gamma$. Therefore, the sum $A + \Gamma$ is open in K_S since it is a union of open sets. This shows that ϕ' is continuous. Consequently, we see that $f(K_\nu)$ and $\phi(f(K_\nu))$ are homeomorphic.

In conclusion, we have that K_ν and $f(K_\nu)$ are homeomorphic, and $f(K_\nu)$ and $C := \phi(f(K_\nu))$ are homeomorphic. It follows that K_ν and C are homeomorphic. We claim that C is closed in K_S/Γ. Since Γ is a lattice, it is co-compact, i.e. K_S/Γ is compact. It would follow from the claim that C is compact (see [Sin19, Theorem 5.1.7]). This means that K_ν is compact, reaching a contradiction. Hence, the assumption that $\Gamma \cap K_S = \emptyset$ is not true.

It remains to show the claim. With respect to the quotient topology, the set C is closed in K_S/Γ if $\phi^{-1}(C)$ is closed in K_S. We have

$$\phi^{-1}(C) = \phi^{-1}(\phi(f(K_\nu))) = f(K_\nu) + \Gamma.$$

So we must show that $A := f(K_\nu) + \Gamma$ is closed in K_S. We will use the metric space (K_S, d_S), introduced in Proposition 3.3.10, to show this. Let $u \in K_S$ be a limit point of A. This means that there exists a sequence $(u_i)_{i\geq 1}$ such that $u_i \in B^{d_S}(u, i^{-1})\backslash\{u\} \cap A$ for all $i \in \mathbb{Z}_{>0}$. In particular, this sequence converges to u in K_S. Since $u_i \in A = f(K_\nu) + \Gamma$, there exist $x_i \in K_\nu$ and $v_i \in \Gamma$ such that $u_i = x_i^\nu + v_i$ for all $i \in \mathbb{Z}_{>0}$. We know that the entry of v_i at ν equals zero, and x_i^ν has only non-zero entry at ν. Hence, for any $i, j \in \mathbb{Z}_{>0}$, we have by construction of d_S that

$$d_S(u_i, u_j) = d_S(v_i, v_j) + d_S(x_i^\nu, x_j^\nu).$$

Since $u_i \in B^{d_S}(u, i^{-1})$ for all $i \in \mathbb{Z}_{>0}$, we have $d_S(u_i, u_j) < \frac{2}{\min\{i,j\}}$. So

$$d_S(v_i, v_j) = d_S(u_i, u_j) - d_S(x_i^\nu, x_j^\nu) < d_S(u_i, u_i) < \frac{2}{\min\{i, j\}}.$$

Hence, if $i, j \to \infty$, we have $d_S(v_i, v_j) \to 0$. In conclusion, the sequence $(v_i)_{i\geq 1}$ is a Cauchy sequence in Γ. In particular, the sequence $(v_i)_{i\geq 1}$ is a Cauchy sequence in K_S. The metric space (K_η, d_η) is complete for all $\eta \in S^\infty$. Proposition 17.11 in [Sut09] tells us that this property is preserved under finite products of topological spaces. Thus, the metric space (K_S, d_S) is complete. Therefore, the sequence $(v_i)_{i\geq 1}$ converges to some $v \in K_S$. Since Γ is a lattice in K_S, in particular a discrete subgroup of K_S, we know by Proposition 2.3.3 that Γ is closed in K_S. Consequently, it must contain the limit v. Since Γ is discrete in K_S, there exists some open set B in K_S such that $v \in B$ and $\Gamma \cap B = \{v\}$. For big enough $k \in \mathbb{Z}_{>0}$, we have $B^{d_S}(v, k^{-1}) \subseteq B$.

Fix such a $k \in \mathbb{Z}_{>0}$. Moreover, for big enough $m \in \mathbb{Z}_{>0}$, the set $B^{d_S}(v, k^{-1}) \cap \Gamma$ contains v_i for all integers $i \geq m$, so we see that $v_i = v$ for $i \geq m$. Then for $i, j \geq m$, we have

$$d_S(x_i^\nu, x_j^\nu) = d_S(u_i, u_j) - d_S(v_i, v_j) = d_S(u_i, u_j) < \frac{2}{\min\{i, j\}}.$$

Thus, if $i, j \to \infty$, we have $d_S(x_i^\nu, x_j^\nu) \to 0$. Using the construction of d_S, we also have $d_\nu(x_i, x_j) \to 0$. This means that the sequence $(x_i)_{i \geq 1}$ is a Cauchy sequence in K_ν. Since the metric space (K_ν, d_ν) is complete, the sequence $(x_i)_{i \geq 1}$ converges to some $x \in K_\nu$. It follows that the sequence $(x_i^\nu)_{i \geq 1}$ converges to x^ν in K_S. Note that $x^\nu \in f(K_\nu)$.

In summary, we have a sequence $(x_i^\nu)_{i \geq 1}$ converging to $x^\nu \in f(K_\nu)$ and a sequence $(v_i)_{i \geq 1}$ converging to some $v \in \Gamma$. Hence, we also have that the sequence $(u_i = x_i^\nu + v_i)_{i \geq 1}$ converges to $x^\nu + v \in A$. By the uniqueness of limits in a Hausdorff space, we know that $u = x^\nu + v \in A$. We conclude that A contains all its limit points. Thus, the set A is closed in K_S. □

We can use this result to prove that any ideal S-lattice has a specific form.

Proposition 5.2.23. Any ideal S-lattice of K is of the form $u\Psi_S(I)$, for some $u \in K_S^*$ and non-zero integral ideal $I \subseteq \mathcal{O}_{K,S}$.

Proof. Let $\Gamma \in \mathrm{IdLat}_{K,S}$. By Lemma 5.2.22, we can find some $u \in \Gamma \cap K_S^*$. Since Γ is an ideal S-lattice, we have $\Psi_S(\mathcal{O}_{K,S})\Gamma \subseteq \Gamma$. This means that $u\Psi_S(\mathcal{O}_{K,S}) \subseteq \Gamma$ since $u \in \Gamma$. By Proposition 5.2.21, we have that $u\Psi_S(\mathcal{O}_{K,S})$ is an ideal S-lattice. Therefore, we can take the quotient of lattices $\Gamma / u\Psi_S(\mathcal{O}_{K,S})$. By Proposition 2.5.8, this quotient group has a finite order. Denote this order by $k \in \mathbb{Z}_{>0}$. Then for any $v \in \Gamma$, we have $\Psi_S(k)v \in u\Psi_S(\mathcal{O}_{K,S})$. So

$$u\Psi_S(\mathcal{O}_{K,S}) \subseteq \Gamma \subseteq \frac{u}{\Psi_S(k)}\Psi_S(\mathcal{O}_{K,S}).$$

Set $w := \frac{\Psi_S(k)}{u} \in K_S^*$. Then

$$w\Gamma \subseteq \frac{\Psi_S(k)}{u}\left(\frac{u}{\Psi_S(k)}\Psi_S(\mathcal{O}_{K,S})\right) = \Psi_S(\mathcal{O}_{K,S}).$$

Since Ψ_S is injective, we have $\Psi_S^{-1}(w\Gamma) \subseteq \mathcal{O}_{K,S}$. Now, we know that $w \in K_S^*$ and Γ is a lattice. It follows from Lemma 3.4.5 that $w\Gamma$ is a lattice. Then we know that $\Psi_S^{-1}(w\Gamma)$ is a subgroup of $\mathcal{O}_{K,S}$ as Ψ_S is a ring homomorphism (see Proposition 3.3.16). We claim that $\Psi_S^{-1}(w\Gamma)$ is even an integral ideal of $\mathcal{O}_{K,S}$. In that case, since Ψ_S is surjective on $\Psi_S(\mathcal{O}_{K,S})$ and $w\Gamma \subseteq \Psi_S(\mathcal{O}_{K,S})$, we have $w\Gamma = \Psi_S(I)$, where $I = \Psi_S^{-1}(w\Gamma)$. We obtain that $\Gamma = w^{-1}\Psi_S(I)$, and the result follows.

It remains to show the claim. Take any $x \in \mathcal{O}_{K,S}$ and $y \in \Psi_S^{-1}(w\Gamma)$. We must show that $xy \in \Psi_S^{-1}(w\Gamma)$. Note that there exists some $v \in \Gamma$ such that $\Psi_S(y) = wv$. Then

$$\Psi_S(xy) = \Psi_S(x)\Psi_S(y) = \Psi_S(x)wv \in \Psi_S(x)w\Gamma. \tag{89}$$

Notice that

$$\Psi_S(\mathcal{O}_{K,S})(w\Gamma) = w\Psi_S(\mathcal{O}_{K,S})\Gamma \subseteq w\Gamma,$$

using that Γ is an ideal S-lattice. In particular, we have $\Psi_S(x)w\Gamma \subseteq w\Gamma$. So (89) tells us that $\Psi_S(xy) \in w\Gamma$. We get that $xy \in \Psi_S^{-1}(w\Gamma)$. This shows that $\Psi_S^{-1}(w\Gamma)$ is an integral ideal of $\mathcal{O}_{K,S}$. □

By Proposition 5.2.21, we know that $u\Psi_S(I)$ is an ideal S-lattice for any non-zero $I \in \mathrm{Id}_{K,S}$ and $u \in K_S^*$. This includes the ideal S-lattices $u\Psi_S(I)$ for some non-zero integral ideal $I \in \mathrm{Id}_{K,S}$ and $u \in K_S^*$. Hence, Proposition 5.2.23 states we have a set equality given by

$$\mathrm{IdLat}_{K,S} = \{u\Psi_S(I) : u \in K_S^*, I \in \mathrm{Id}_{K,S} \setminus \{(0)\}\}. \tag{90}$$

We use this convention. So whenever we take $u\Psi_S(I) \in \mathrm{IdLat}_{K,S}$, we take a non-zero $I \in \mathrm{Id}_{K,S}$ and $u \in K_S^*$.

Corollary 5.2.24. The set $\mathrm{IdLat}_{K,S}$ attains an abelian group structure.

Proof. For $u\Psi_S(I), v\Psi_S(J) \in \mathrm{IdLat}_{K,S}$, we construct an operation, denoted by $\diamond$, by

$$u\Psi_S(I) \diamond v\Psi_S(J) := uv\Psi_S(IJ).$$

This operation is closed by set equality (90). Moreover, this operation is associative and abelian, since these are properties of the multiplication in K_S^* and fractional ideals. The unit element is given by $\Psi_S(\mathcal{O}_{K,S})$. Moreover, the element $u\Psi_S(I) \in \mathrm{IdLat}_{K,S}$ has inverse $u^{-1}\Psi_S(I^{-1})$. □

We would like to find a group isomorphism between $\mathrm{Pic}_{K,S}$ and $\mathrm{IdLat}_{K,S}$. Namely, we can associate an ideal S-lattice to an Arakelov S-divisor. Let $D = (I,u)_S$ be an Arakelov S-divisor, where $I \in \mathrm{Id}_{K,S}$ is non-zero and $u \in \prod_{\sigma\in\Sigma_K^\infty} \mathbb{R}_{>0}$. Recall that $K_\mathbb{R} = \prod_{\sigma\in\Sigma_K^\infty} K_\sigma$ and

$$K_S = \prod_{\nu\in S^\infty} K_\nu = \prod_{\sigma\in\Sigma_K^\infty} K_\sigma \times \prod_{\mathfrak{p}\in S} K_\mathfrak{p} = K_\mathbb{R} \times \prod_{\mathfrak{p}\in S} K_\mathfrak{p}.$$

So we can embed u into K_S by defining

$$\widetilde{u} := (u, \underbrace{1,\ldots,1}_{\#S \text{ times}}).$$

Since u has positive real entries, we have $\widetilde{u} \in K_S^*$. Hence, to any Arakelov S-divisor $D = (I,u)_S$ we can associate the ideal S-lattice $\widetilde{u}\Psi_S(I)$. Writing $u = (u_\sigma)_{\sigma\in\Sigma_K^\infty}$, by Proposition 5.2.21, the covolume is given by

$$\begin{aligned}\mathrm{covol}(\widetilde{u}\Psi_S(I)) &= \left(\prod_{\sigma\in\Sigma_K^\infty} \|u_\sigma\|_\sigma \prod_{\mathfrak{p}\in S} \|1\|_\mathfrak{p}\right) N_{\mathcal{O}_{K,S}}(I)\sqrt{|d_K|_\infty \mathfrak{D}_S^{-1}} \\ &= \left(\prod_{\sigma\in\Sigma_K^\infty} \|u_\sigma\|_\sigma\right) N_{\mathcal{O}_{K,S}}(I)\sqrt{|d_K|_\infty \mathfrak{D}_S^{-1}}.\end{aligned}$$

However, this association is not enough for a group isomorphism.

Definition 5.2.25. Let $\Gamma, \Gamma' \in \mathrm{IdLat}_{K,S}$, then we write $\Gamma \sim \Gamma'$ if and only if there exists $u \in K_S^*$ such that $u\Gamma = \Gamma'$ and $|u_\sigma|_\sigma = 1$ for all $\sigma \in \Sigma_K^\infty$.

It is a direct verification that the rule $\sim$ defines an equivalence relation on $\mathrm{IdLat}_{K,S}$. The quotient group $\mathrm{IdLat}_{K,S} / \sim$ will be denoted by $\widetilde{\mathrm{IdLat}}_{K,S}$. For $\Gamma \in \mathrm{IdLat}_{K,S}$, we denote its equivalence class in $\widetilde{\mathrm{IdLat}}_{K,S}$ by $[\Gamma]$.

Theorem 5.2.26. The group homomorphism $f\colon \mathrm{Div}_{K,S} \to \widetilde{\mathrm{IdLat}}_{K,S}$ given by $(I,u)_S \mapsto [\widetilde{u}\Psi_S(I)]$ induces a group isomorphism $\mathrm{Pic}_{K,S} \cong \widetilde{\mathrm{IdLat}}_{K,S}$.

Proof. The map f sends $(\mathcal{O}_{K,S}, (1)_{\sigma\in\Sigma_K^\infty})_S$ to $[\Psi_S(\mathcal{O}_{K,S})]$. Equivalently, the map f sends the unit element of $\mathrm{Div}_{K,S}$ to the unit element of $\mathrm{IdLat}_{K,S}$. For $(I,u)_S, (J,v)_S \in \mathrm{Div}_{K,S}$ we have

$$f\left((I,u)_S + (J,v)_S\right) = f\left((IJ,uv)_S\right) = [\widetilde{(uv)}\Psi_S(IJ)] = [\widetilde{u}\Psi_S(I)] \diamond [\widetilde{v}\Psi_S(J)] = f\left((I,u)_S\right) \diamond f\left((J,v)_S\right).$$

This shows that f is a group homomorphism. Now, take any $[u\Psi_S(I)] \in \widetilde{\mathrm{IdLat}}_{K,S}$. We write

$$u = \left((u_\sigma)_{\sigma\in\Sigma_K^\infty}, (u_\mathfrak{p})_{\mathfrak{p}\in S}\right) \in K_S^*,$$

and define the elements $v, w \in K_S^*$ by

$$v := ((|u_\sigma|)_{\sigma\in\Sigma_K^\infty}, \underbrace{1,\ldots,1}_{\#S \text{ times}}), \qquad w = \left(\left(\frac{u_\sigma}{|u_\sigma|_\sigma}\right)_{\sigma\in\Sigma_K^\infty}, (u_\mathfrak{p})_{\mathfrak{p}\in S}\right).$$

Then $wv\Psi_S(I) = u\Psi_S(I)$. Moreover, we have

$$|w_\sigma|_\sigma = \left|\frac{u_\sigma}{|u_\sigma|_\sigma}\right|_\sigma = \frac{|u_\sigma|_\sigma}{|u_\sigma|_\sigma} = 1,$$

for all $\sigma \in \Sigma_K^\infty$. Therefore, we can conclude that $v\Psi_S(I) \sim u\Psi_S(I)$. We get that

$$f\left((I, (|u_\sigma|)_{\sigma\in\Sigma_K^\infty})_S\right) = [v\Psi_S(I)] = [u\Psi_S(I)].$$

This shows that f is surjective.

Next, we claim that $\ker(f) = \mathrm{Prin}_{K,S}$. Take any $\mathrm{div}_S(x) \in \mathrm{Prin}_{K,S}$. We can write $\mathrm{div}_S(x) = (x^{-1}\mathcal{O}_{K,S}, u)_S$, where $u = (|x|_\sigma)_{\sigma\in\Sigma_K^\infty} \in \prod_{\sigma\in\Sigma_K^\infty} \mathbb{R}_{>0}$ (see Equation (70)). Note that $\Psi_S(x^{-1}\mathcal{O}_{K,S}) = \Psi_S(x^{-1})\Psi_S(\mathcal{O}_{K,S})$. Furthermore, define $v \in K_S^*$ by

$$v := \Psi_S(x^{-1})\widetilde{u} = \left(\left(\frac{|x|_\sigma}{x}\right)_{\sigma\in\Sigma_K^\infty}, (x^{-1})_{\mathfrak{p}\in S}\right).$$

Then

$$|v_\sigma|_\sigma = \left|\frac{|x|_\sigma}{x}\right|_\sigma = \frac{|x|_\sigma}{|x|_\sigma} = 1,$$

for all $\sigma \in \Sigma_K^\infty$. We have $v\Psi_S(\mathcal{O}_{K,S}) = v\Psi_S(\mathcal{O}_{K,S})$, with $|v_\sigma|_\sigma = 1$ for all $\sigma \in \Sigma_K^\infty$. In particular, this means that $v\Psi_S(\mathcal{O}_{K,S}) \sim \Psi_S(\mathcal{O}_{K,S})$. With all these results, we obtain that

$$f\left((x^{-1}\mathcal{O}_{K,S}, u)_S\right) = [\widetilde{u}\Psi_S(x^{-1}\mathcal{O}_{K,S})] = [\widetilde{u}\Psi_S(x^{-1})\Psi_S(\mathcal{O}_{K,S})] = [v\Psi_S(\mathcal{O}_{K,S})] = [\Psi_S(\mathcal{O}_{K,S})].$$

This shows that $\mathrm{div}_S(x) \in \ker(f)$. For the converse, take any $(I, u)_S \in \ker(f)$, i.e. $f((I, u)_S) = [\widetilde{u}\Psi_S(I)]$ equals $[\Psi_S(\mathcal{O}_{K,S})]$. This means that there exists some $v = (v_\sigma)_{\sigma\in\Sigma_K^\infty} \in K_S$ such that $|v_\sigma|_\sigma = 1$ for all $\sigma \in \Sigma_K^\infty$, and $v\Psi_S(\mathcal{O}_{K,S}) = \widetilde{u}\Psi_S(I)$. Since $1 \in \mathcal{O}_{K,S}$, there exists some $x \in I$ such that $v = \widetilde{u}\Psi_S(x)$. This implies that $v(\widetilde{u})^{-1} = \Psi_S(x)$, and so

$$v\Psi_S(\mathcal{O}_{K,S}) = \widetilde{u}\Psi_S(I) \implies v\widetilde{u}^{-1}\Psi_S(\mathcal{O}_{K,S}) = \Psi_S(I) \implies \Psi_S(x\mathcal{O}_{K,S}) = \Psi_S(I) \implies x\mathcal{O}_{K,S} = I,$$

where in the last step we used that Ψ_S is injective. So

$$v\Psi_S(\mathcal{O}_{K,S}) = \widetilde{u}\Psi_S(I) = \widetilde{u}\Psi_S(x\mathcal{O}_{K,S}) = \widetilde{u}\Psi_S(x)\Psi_S(\mathcal{O}_{K,S}).$$

As $\widetilde{u}, v\Psi_S(x) \in K_S^*$, there exists some $a \in \mathcal{O}_{K,S}^*$ such that $v = \Psi_S(ax)\widetilde{u}$. Since $|v_\sigma|_\sigma = 1$ for all $\sigma \in \Sigma_K^\infty$, we also have $|axu_\sigma|_\sigma = 1$ (Here we use the convention of Remark 3.3.17). We obtain that $|u_\sigma|_\sigma = |(ax)^{-1}|_\sigma$. By definition of $(I, u)_S$, we have that u_σ is real positive for all $\sigma \in \Sigma_K^\infty$. Therefore, we have $u_\sigma = |(ax)^{-1}|_\sigma$ for all $\sigma \in \Sigma_K^\infty$. We see that

$$(I, u)_S = (x\mathcal{O}_{K,S}, (|(ax)^{-1}|_\sigma)_\sigma)_S = (xa\mathcal{O}_{K,S}, (|(ax)^{-1}|_\sigma)_\sigma)_S = \mathrm{div}_S((xa)^{-1}),$$

where we used that $a \in \mathcal{O}_{K,S}^*$, so $a\mathcal{O}_{K,S} = \mathcal{O}_{K,S}$. This implies that $(I, u)_S \in \mathrm{Prin}_{K,S}$. Consequently, we obtain that $\ker(f) = \mathrm{Prin}_{K,S}$.

We conclude that f induces a group isomorphism

$$\widetilde{\mathrm{IdLat}}_{K,S} \cong \mathrm{Div}_{K,S} / \ker(f) = \mathrm{Div}_{K,S} / \mathrm{Prin}_{K,S} = \mathrm{Pic}_{K,S}. \qquad \square$$

5.3 Topological Structure of the Arakelov S-Class Group

In this section, we endow $\mathrm{Pic}_{K,S}$ with a topological structure. This topology will be induced from the topological structure on $\mathrm{Div}_{K,S}$. Therefore, we first investigate the topology on $\mathrm{Div}_{K,S}$. We will state some general properties of these topological structures. Furthermore, we show how the topological structure on $\mathrm{Pic}_{K,S}$ can be induced from a metric.

Recall that any Arakelov S-divisor D in $\mathrm{Div}_{K,S}$ is given by a finite formal sum

$$D = \sum_{\mathfrak{p} \notin S} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\sigma \in \Sigma_K^\infty} x_\sigma \sigma, \qquad n_{\mathfrak{p}} \in \mathbb{Z}, x_\sigma \in \mathbb{R}.$$

Therefore, the Arakelov S-divisor D is determined by the coefficients

$$(n_{\mathfrak{p}})_{\mathfrak{p} \notin S} \in \bigoplus_{\mathfrak{p} \notin S} \mathbb{Z}, \qquad (x_\sigma)_{\sigma \in \Sigma_K^\infty} \in \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}.$$

Hence, we get

$$\mathrm{Div}_{K,S} \cong \bigoplus_{\mathfrak{p} \notin S} \mathbb{Z} \times \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}. \tag{91}$$

Note that we take the direct sum for the finite places since we want all entries to be zero except for a finite number of entries. Throughout this section, we often change between writing Arakelov S-divisors in the multiplicative notation and their coefficients. We give $\bigoplus_{\mathfrak{p} \notin S} \mathbb{Z}$ the discrete topology, i.e. all subsets of $\bigoplus_{\mathfrak{p} \notin S} \mathbb{Z}$ are open. Furthermore, we endow $\prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}$ with the Euclidean topology on $\mathbb{R}^{r_1+r_2}$. Now, we can endow $\mathrm{Div}_{K,S}$ with the product topology. If we take $S = \emptyset$, we also have a topology on Div_K. This topological structure for Div_K was introduced on page 189 in [Neu99]. In Proposition 5.1.2, we saw that $\mathrm{Div}_{K,S} \subseteq \mathrm{Div}_K$. The topology on $\mathrm{Div}_{K,S}$ equals the subspace topology induced from the topology on Div_K. This is a direct consequence of the fact that we take the product topology on Div_K and $\mathrm{Div}_{K,S}$, and the discrete topology on $\bigoplus_{\mathfrak{p} \notin S} \mathbb{Z}$.

Proposition 5.3.1. The product topology on $\mathrm{Div}_{K,S}$ is locally compact and Hausdorff.

Proof. Since the discrete topology is Hausdorff, and any topology induced from a metric is Hausdorff (see [Sut09, Proposition 11.5]), we know that the topological spaces $\bigoplus_{\mathfrak{p} \notin S} \mathbb{Z}, \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}$ are Hausdorff. Then the topological space $\mathrm{Div}_{K,S}$ is also Hausdorff, as the Hausdorff property is preserved under finite products of topological spaces (see [Sin19, Theorem 4.4.4]). Similarly, the discrete topology is locally compact, so $\bigoplus_{\mathfrak{p} \notin S} \mathbb{Z}$ is locally compact (it is not compact as the set is infinite). Also, as a consequence of the Heine-Borel Theorem, we know that $\prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}$ is locally compact. Hence, we conclude that $\mathrm{Div}_{K,S}$ is locally compact as this property is preserved under finite products of topological spaces (see [Sin19, Theorem 5.4.6]). □

The product topology is compatible with the group structure on $\mathrm{Div}_{K,S}$. This is a consequence of the discrete topology on $\bigoplus_{\mathfrak{p} \notin S} \mathbb{Z}$, and the Euclidean topology on $\prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}$, which are compatible with addition. Therefore, the group $\mathrm{Div}_{K,S}$ becomes a topological group. Proposition 5.3.1 implies that $\mathrm{Div}_{K,S}$ is a locally compact group. We can endow $\mathrm{Prin}_{K,S} \subseteq \mathrm{Div}_{K,S}$ with the subspace topology.

Proposition 5.3.2. The subspace $\mathrm{Prin}_{K,S}$ of $\mathrm{Div}_{K,S}$ is a discrete subgroup.

Proof. By Proposition 5.1.5, we know that $\mathrm{Prin}_{K,S}$ forms a subgroup of $\mathrm{Div}_{K,S}$. We know that

$$\mathrm{Prin}_{K,S} \subseteq \mathrm{Div}_{K,S} \subseteq \mathrm{Div}_K .$$

Therefore, we may conclude that the topology on $\mathrm{Prin}_{K,S}$ is the subspace topology induced from Div_K. Since we know that $\mathrm{Prin}_{K,S} \subseteq \mathrm{Prin}_K$, it suffices to show that Prin_K is discrete (see Proposition 2.3.2 (ii.)). This is shown in Proposition 1.9 of Chapter III in [Neu99]. □

Recall that for a topological space X, the connected component of $x \in X$ is given by the union of all the connected sets containing x. This unique component will be denoted by $\mathcal{C}(x)$. One can show that connected components of two different elements are either identical or disjoint. Therefore, the space X is a disjoint union of its connected components. These results can be found in Proposition 3.2.2 of [Sin19]. In a discrete space X, one has $\mathcal{C}(x) = \{x\}$ for all $x \in X$.

Proposition 5.3.3. Let $D \in \mathrm{Div}_{K,S}$, and denote its coefficients for $\mathfrak{p} \notin S$ by $n_{\mathfrak{p}} \in \mathbb{Z}$. Then

$$\mathcal{C}(D) = \{(n_{\mathfrak{p}})_{\mathfrak{p} \notin S}\} \times \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}.$$

Proof. This follows directly from the fact that $\bigoplus_{\mathfrak{p} \notin S} \mathbb{Z}$ has the discrete topology, and $\prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}$ the Euclidean topology. □

Now that we have explored the topological structure on $\mathrm{Div}_{K,S}$, we can move to the topological structure on $\mathrm{Pic}_{K,S}$. By definition, we have

$$\mathrm{Pic}_{K,S} = \mathrm{Div}_{K,S} \,/\, \mathrm{Prin}_{K,S}\,.$$

Therefore, we endow $\mathrm{Pic}_{K,S}$ with the quotient topology induced from the topology on $\mathrm{Div}_{K,S}$.

Definition 5.3.4. The quotient topology on $\mathrm{Pic}_{K,S}$ induced from the product topology on $\mathrm{Div}_{K,S}$ is called the *natural topology* on $\mathrm{Pic}_{K,S}$.

The natural topology on $\mathrm{Pic}_{K,S}$ is not random. If we take $S = \emptyset$, the natural topology on Pic_K coincides with the topological structure of Pic_K as introduced on page 190 in [Neu99]. Now, let us look at some properties of this topology on $\mathrm{Pic}_{K,S}$.

Proposition 5.3.5. The natural topology turns $\mathrm{Pic}_{K,S}$ into a locally compact group.

Proof. By Proposition 5.3.2, we know that $\mathrm{Prin}_{K,S}$ is a discrete subgroup of $\mathrm{Div}_{K,S}$. It follows from Proposition 2.3.3 that it is closed in the locally compact group $\mathrm{Div}_{K,S}$. It follows from Proposition 2.2.2 that $\mathrm{Pic}_{K,S}$ is a locally compact group. □

We are going to examine the connected components of $\mathrm{Pic}_{K,S}$. We took the Euclidean topology on $\prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}$. Specifically, it is induced by the metric

$$d(u,v) := \sqrt{\sum_{\sigma \in \Sigma_K^\infty} (u_\sigma - v_\sigma)^2},$$

for $u, v \in \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}$. In Section 1.8, we have seen the inner product $\langle \cdot, \cdot \rangle_{\mathbb{R}}$ on $K_{\mathbb{R}}$. We can take the norm on $K_{\mathbb{R}}$ as $\|.\|_{\mathbb{R}} := \sqrt{\langle \cdot, \cdot \rangle_{\mathbb{R}}}$. This induces a metric given by $d_{\mathbb{R}}(u,v) := \|u - v\|_{\mathbb{R}}$. Since $\prod_{\sigma \in \Sigma_K^\infty} \mathbb{R} \subseteq K_{\mathbb{R}}$, we can restrict this metric to $\prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}$. Specifically, we have

$$d_{\mathbb{R}}(u,v) := \sqrt{\sum_{\sigma \in \Sigma_K^\infty} \deg(\sigma)(u_\sigma - v_\sigma)^2},$$

for $u, v \in \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}$. Using Definition 1.2.4 of $\deg(\sigma)$ for some $\sigma \in \Sigma_K^\infty$, we have

$$d(u,v) \leq d_{\mathbb{R}}(u,v) \leq 2d(u,v),$$

for $u, v \in \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}$. Thus, the metrics d and $d_{\mathbb{R}}$ are Lipschitz equivalent (see [Sut09, Definition 6.33]). This means that d and $d_{\mathbb{R}}$ induce the same topology on $\prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}$ (see [Sut09, Proposition 6.34]). Hence, from now and onward, we assume that the Euclidean topology on $\prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}$ is induced from the metric $d_{\mathbb{R}}$.

Recall the group

$$T_{K,S} = \prod_{\sigma\in\Sigma_K^\infty} \mathbb{R}/\{\log(\hat{a}) : a \in \mathcal{O}_{K,S}^*\}$$

that we have seen in (69). Furthermore, in Theorem 5.1.16 we say that $T_{K,S}$ can be embedded into $\mathrm{Pic}_{K,S}$. This was given by the map $\zeta_S\colon T_{K,S} \to \mathrm{Pic}_{K,S}$ defined by $[(u_\sigma)_{\sigma\in\Sigma_K^\infty}] \mapsto [(\mathcal{O}_K, (e^{-u_\sigma})_{\sigma\in\Sigma_K^\infty})_S]$. We endow $T_{K,S}$ with the quotient topology induced from the topology on $\prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}$.

Lemma 5.3.6. The group homomorphism $\zeta_S\colon T_{K,S} \to \mathrm{Pic}_{K,S}$ is continuous.

Proof. Let $\phi\colon \mathrm{Div}_{K,S} \to \mathrm{Pic}_{K,S}$ denote the canonical map. Take any open subset $B \subseteq \mathrm{Pic}_{K,S}$. With respect to the natural topology, this means that $\phi^{-1}(B)$ is open in $\mathrm{Div}_{K,S}$. By the product topology on $\mathrm{Div}_{K,S}$, there exist open sets $Z_i \subseteq \bigoplus_{\mathfrak{p}\notin S}\mathbb{Z}$ and $R_i \subseteq \prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}$ for all $i \in I$ such that

$$\phi^{-1}(B) = \bigcup_{i\in I} Z_i \times R_i,$$

where I is some index set. Now, since R_i is open, it is the union of some open balls in $\prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}$. Therefore, there exist open balls $B^{d_\mathbb{R}}(\log(u_j), \varepsilon_j)$ for some $\varepsilon_j \in \mathbb{R}_{>0}$ and $u_j \in \prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}_{>0}$ such that

$$\phi^{-1}(B) = \bigcup_{i\in I} Z_i \times R_i = \bigcup_{i\in I}\left(\bigcup_{j\in J} Z_i \times B^{d_\mathbb{R}}(\log(u_j), \varepsilon_j)\right),$$

where J is some index set. Since ϕ is surjective, we have

$$\begin{aligned} B &= \phi(\phi^{-1}(B)) \\ &= \phi\left(\bigcup_{i\in I}\left(\bigcup_{j\in J} Z_i \times B^{d_\mathbb{R}}(\log(u_j), \varepsilon_j)\right)\right) \\ &= \bigcup_{i\in I}\left(\bigcup_{j\in J} \phi(Z_i \times B^{d_\mathbb{R}}(\log(u_j), \varepsilon_j))\right). \end{aligned}$$

Now to see how ϕ maps these sets, we have to notice that the sets $Z_i \times B^{d_\mathbb{R}}(\log(u_j), \varepsilon_j)$ defines a set of Arakelov S-divisors through isomorphism (91). Writing these in multiplicative notation, we get

$$\begin{aligned} B &= \bigcup_{i\in I}\left(\bigcup_{j\in J} \phi(Z_i \times B^{d_\mathbb{R}}(\log(u_j), \varepsilon_j))\right) \\ &= \bigcup_{i\in I}\left(\bigcup_{j\in J} \phi\left(\left\{(I,v)_S : (-\operatorname{ord}_\mathfrak{p}(I))_{\mathfrak{p}\notin S} \in Z_i, v \in \prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}_{>0} \text{ and } \|\log(u_j v)\|_\mathbb{R} < \varepsilon_j\right\}\right)\right) \\ &= \bigcup_{i\in I}\left(\bigcup_{j\in J}\left\{[(I,v)_S] : (-\operatorname{ord}_\mathfrak{p}(I))_{\mathfrak{p}\notin S} \in Z_i, v \in \prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}_{>0} \text{ and } \|\log(u_j v)\|_\mathbb{R} < \varepsilon_j\right\}\right). \end{aligned}$$

By construction of ζ_S, we have

$$\zeta_S(T_{K,S}) = \left\{[(\mathcal{O}_{K,S}, u)_S] : u \in \prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}_{>0}\right\}.$$

Let L contain all the elements $x \in K^*$ such that $x\mathcal{O}_{K,S}$ is represented in Z_i for some $i \in I$. Then either $B \cap \zeta_S(T_{K,S}) = \emptyset$ or

$$B \cap \zeta_S(T_{K,S}) = \bigcup_{x\in L}\left(\bigcup_{j\in J}\left\{[(x\mathcal{O}_{K,S}, v)_S] : v \in \prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}_{>0} \text{ and } \|\log(u_j v)\|_{\mathbb{R}} < \varepsilon_j\right\}\right)$$
$$= \bigcup_{x\in L}\left(\bigcup_{j\in J}\left\{[(\mathcal{O}_{K,S}, \hat{x}v)_S] : v \in \prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}_{>0} \text{ and } \|\log(u_j v)\|_{\mathbb{R}} < \varepsilon_j\right\}\right).$$

The last equality comes from the fact that $[(x\mathcal{O}_{K,S}, v)_S] = [(\mathcal{O}_{K,S}, \hat{x}v)_S]$ since

$$(\mathcal{O}_{K,S}, \hat{x}v)_S - (x\mathcal{O}_{K,S}, v)_S = (x^{-1}\mathcal{O}_{K,S}, \hat{x})_S = \mathrm{div}_S(x).$$

Since ζ_S is injective, we have $\zeta_S^{-1}(B) = \zeta_S^{-1}(B \cap \zeta_S(T_{K,S}))$. We obtain that $\zeta_S^{-1}(B) = \emptyset$ or

$$\zeta_S^{-1}(B) = \bigcup_{x\in L}\left(\bigcup_{j\in J}\{[\hat{x}v] : v \in B^{d_{\mathbb{R}}}(\log(u_j), \varepsilon_j)\}\right).$$

Now, the group homomorphism ζ_S is continuous if the latter is open with respect to the quotient topology on $T_{K,S}$. Let $f\colon \prod_{\sigma\in\Sigma_K^\infty}\mathbb{R} \to T_{K,S}$, be the canonical map. Then

$$f^{-1}(\zeta_S^{-1}(B)) = \bigcup_{x\in L}\left(\bigcup_{j\in J}\{\hat{x}v : v \in B^{d_{\mathbb{R}}}(\log(u_j), \varepsilon_j)\}\right) + \{\log(\hat{a}) : a \in \mathcal{O}_{K,S}^*\}$$
$$= \bigcup_{x\in L}\left(\bigcup_{j\in J}\hat{x}B^{d_{\mathbb{R}}}(\log(u_j), \varepsilon_j)\right) + \{\log(\hat{a}) : a \in \mathcal{O}_{K,S}^*\}.$$

This is a union of translates of multiples of open balls. Therefore, this is open in $\prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}$. □

The following result will be needed and is Theorem 3.1.5 of [Sin19].

Lemma 5.3.7. Let X, Y be topological spaces. If $f\colon X \to Y$ is a continuous map of topological spaces and X is connected, then $f(X)$ is connected with respect to the subspace topology.

Proposition 5.3.8. Let $[D] \in \mathrm{Pic}_{K,S}$, then $\mathcal{C}([D]) = [D]+\zeta_S(T_{K,S})$. Consequently, the connected components of $\mathrm{Pic}_{K,S}$ are given by the cosets of $\zeta_S(T_{K,S})$ in $\mathrm{Pic}_{K,S}$.

Proof. Since a Euclidean space is connected, we have that $\prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}$ is connected. Hence, using the continuous surjective canonical map $f\colon \prod_{\sigma\in\Sigma_K^\infty}\mathbb{R} \to T_{K,S}$ and Lemma 5.3.7, we have that $T_{K,S}$ is connected. By Lemma 5.3.6, we know that $\zeta_S\colon T_{K,S} \to \mathrm{Pic}_{K,S}$ is continuous. Again using Lemma 5.3.7, we know that $\zeta_S(T_{K,S})$ is connected with respect to the subspace topology on $\mathrm{Pic}_{K,S}$. Let $\phi\colon \mathrm{Div}_{K,S} \to \mathrm{Pic}_{K,S}$ be the canonical map. By construction of ζ_S, we know that

$$\zeta_S(T_{K,S}) = \left\{[(\mathcal{O}_{K,S}, v)_S] : v \in \prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}_{>0}\right\}.$$

Then

$$\phi^{-1}(\zeta_S(T_{K,S})) = \mathrm{Prin}_{K,S} + \left\{(\mathcal{O}_{K,S}, v)_S : v \in \prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}_{>0}\right\} = \bigcup_{x\in K^*}\left\{(x\mathcal{O}_{K,S}, v)_S : v \in \prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}_{>0}\right\}.$$

Now, we use isomorphism 91 to write the last set in terms of coefficients. We obtain that

$$\phi^{-1}(\zeta_S(T_{K,S})) = \bigcup_{x\in K^*} \left(\{(\mathrm{ord}_{\mathfrak{p}}(x))_{\mathfrak{p}\notin S}\} \times \prod_{\sigma\in\Sigma_K^\infty} \mathbb{R} \right).$$

This is open in $\mathrm{Div}_{K,S}$ with respect to the product topology. Thus, with respect to the quotient topology, the subgroup $\zeta_S(T_{K,S})$ must be open in $\mathrm{Pic}_{K,S}$. By Proposition 9.1.7 in [Coh13], we see that $\zeta_S(T_{K,S})$ must be closed as well.

Fix any $[D] \in \mathrm{Pic}_{K,S}$. The map $f\colon \mathrm{Pic}_{K,S} \to \mathrm{Pic}_{K,S}$ defined by $f([D']) = [D] + [D']$ is a homeomorphism by Proposition 2.1.2. It follows by Lemma 5.3.7 that $f(\zeta_S(T_{K,S})) = [D] + \zeta_S(T_{K,S})$ is also connected. Hence, we have

$$[D] + \zeta_S(T_{K,S}) \subseteq \mathcal{C}([D]).$$

Suppose that $[D] + \zeta_S(T_{K,S}) \neq \mathcal{C}([D])$. Then $\mathcal{C}([D])$ is a connected subset of $\mathrm{Pic}_{K,S}$ strictly containing $[D] + \zeta_S(T_{K,S})$. We endow $\mathcal{C}([D])$ with the subspace topology induced from $\mathrm{Pic}_{K,S}$. Since $\zeta_S(T_{K,S})$ is both open and closed in $\mathrm{Pic}_{K,S}$, then $[D] + \zeta_S(T_{K,S})$ is both open and closed in $\mathcal{C}([D])$. As $\mathcal{C}([D])$ contains $[D] + \zeta_S(T_{K,S})$ strictly, we have $B := \mathcal{C}([D])\backslash([D] + \zeta_S(T_{K,S})) \neq \emptyset$. Moreover, the subset B is both open and closed in $\mathcal{C}([D])$, since it is the complement of $[D] + \zeta_S(T_{K,S})$. As a result of this, we see that $\mathcal{C}([D])$ admits the partition $B, [D] + \zeta_S(T_{K,S})$. So $\mathcal{C}([D])$ must be disconnected. This is impossible by the definition of a connected component. So we actually have the equality $\mathcal{C}([D]) = [D] + \zeta_S(T_{K,S})$. □

Remark 5.3.9. In Definition 4.2.5, we have defined the notion of ideal equivalent Arakelov divisors. One could easily extend this notion to the rings of S-integers. Namely, two Arakelov S-divisors $D = (I, u)_S$ and $D = (J, u')_S$ are called *ideal equivalent* if $[I] = [I']$ in $\mathrm{Cl}_{K,S}$. We have the short exact sequence

$$0 \longrightarrow T_{K,S} \xrightarrow{\zeta_S} \mathrm{Pic}_{K,S} \xrightarrow{\chi} \mathrm{Cl}_{K,S} \longrightarrow 0\ ,$$

with $\chi\colon \mathrm{Pic}_{K,S} \to \mathrm{Cl}_{K,S}$ defined by $[D] \mapsto [I(D)]$. So, if two Arakelov S-divisors D, D' are ideal equivalent, their image under χ is the same. Then $[D - D'] \in \ker(\chi) = \mathrm{im}(\zeta_S)$, and so $[D] \in [D'] + \zeta_S(T_{K,S})$. The converse is also true, if $[D] \in [D'] + \zeta_S(T_{K,S})$ then D and D' are ideal equivalent. Hence, two Arakelov S-divisors are ideal equivalent if and only if they belong to the same coset of $\zeta_S(T_{K,S})$ in $\mathrm{Pic}_{K,S}$. By Proposition 5.3.8, this means that two Arakelov S-divisors are ideal equivalent if and only if they lie on the same connected component of $\mathrm{Pic}_{K,S}$. ⧫

We can define a distance function on the connected components of $\mathrm{Pic}_{K,S}$. It turns out that this distance function induces a metric on the connected components of $\mathrm{Pic}_{K,S}$.

Using the group isomorphism $\log : \mathbb{R}_{>0} \to \mathbb{R}$, the group $T_{K,S}$ is also given by

$$T_{K,S} = \prod_{\sigma\in\Sigma_K^\infty} \mathbb{R}_{>0}/\{\hat{a} : a \in \mathcal{O}_{K,S}^*\}.$$

We will use this representation for $T_{K,S}$ from now on. With this 'new' way of viewing $T_{K,S}$, the group homomorphism ζ_S is given by $[u] \mapsto [(\mathcal{O}_{K,S}, u)_S]$. Now, consider the function $\delta_{K,S}\colon T_{K,S} \to \mathbb{R}$ defined by

$$\delta^1_{K,S}([u]) := \inf_{a\in\mathcal{O}_{K,S}^*} \|\log(\hat{a}u)\|_{\mathbb{R}}, \tag{92}$$

where $\|.\|_{\mathbb{R}} := \sqrt{\langle\cdot,\cdot\rangle_{\mathbb{R}}}$ is the norm on the Minkowski space $K_{\mathbb{R}}$. Since the norm is bounded from below by the value zero, we know that the greatest lower bound (or infimum) exists. This follows from the Axiom of Completeness for the real line.

Proposition 5.3.10. The function $\delta_{K,S}\colon T_{K,S} \to \mathbb{R}$ is well-defined.

Proof. For $[u] = [v]$ in $T_{K,S}$, there exists some $a \in \mathcal{O}_{K,S}^*$ such that $u = \hat{a}v$. Then

$$\delta^1_{K,S}([u]) = \inf_{b \in \mathcal{O}^*_{K,S}} \|\log(\hat{b}u)\|_{\mathbb{R}} = \inf_{b \in \mathcal{O}^*_{K,S}} \|\log(\hat{b}\hat{a}v)\|_{\mathbb{R}} = \inf_{c \in \mathcal{O}^*_{K,S}} \|\log(\hat{c}v)\|_{\mathbb{R}} = \delta^1_{K,S}([v]),$$

where we had set $c = ab$. □

Let $[D], [D] \in \mathrm{Pic}_{K,S}$ be two Arakelov S-divisors that lie on the same connected component of $\mathrm{Pic}_{K,S}$. Since they lie on the same connected component in $\mathrm{Pic}_{K,S}$, we have $[D - D'] \in \zeta_S(T_{K,S})$. Hence, there exists some $[(\mathcal{O}_{K,S}, u)_S] \in \zeta_S(T_{K,S})$ such that

$$[D - D'] = [(\mathcal{O}_{K,S}, u)_S].$$

By injectivity of the group homomorphism ζ_S, we have that $[(\mathcal{O}_{K,S}, u)_S]$ corresponds to the class $[u]$ in $T_{K,S}$. Therefore, the class $[u]$ in $T_{K,S}$ is uniquely determined by $[D - D']$. Therefore, the following definition is well-defined.

Definition 5.3.11. The *distance* between two equivalence classes of Arakelov S-divisors $[D], [D'] \in \mathrm{Pic}_{K,S}$ that lie on the same connected component is defined by

$$\delta_{K,S}([D], [D']) := \delta^1_{K,S}([u]),$$

such that $[D - D'] = [(\mathcal{O}_{K,S}, u)_S]$.

Note that the distance is only defined for equivalence classes of Arakelov S-divisors that lie on the same connected component.

Remark 5.3.12. This distance function is not random. If one takes $S = \emptyset$, this distance was introduced in Chapter 6 of [Sch08]. However, rather than using the infimum, it uses the minimum. It is not proven in [Sch08] that this minimum is attained. To show this, one might be able to use the fact that $\mathcal{O}_K^*$ is a complete lattice in the $(r_1 + r_2 - 1)$-dimensional space given by

$$H := \left\{ x \in \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R} : \sum_{\sigma \in \Sigma_K^\infty} x_\sigma = 0 \right\}.$$

One can find this result in Theorem 7.3 of Chapter I in [Neu99]. But this is only a suggestion. One needs to study this to see whether this idea works. For general S, this thesis has not studied whether a minimum is attained in construction (92). However, since the theory works fine with the infimum, there is no need to check for a minimum. ♦

Proposition 5.3.13. The function $\delta_{K,S}$ restricts to a metric on every connected component of $\mathrm{Pic}_{K,S}$.

Proof. Let T be a connected component of $\mathrm{Pic}_{K,S}$. Let us check the three conditions of a metric.

The output of $\delta_{K,S}$ is determined by the norm $\|.\|_{\mathbb{R}}$ on $K_{\mathbb{R}}$. Therefore, the function $\delta_{K,S}$ is always non-negative. Note that $\delta^1_{K,S}$ is only zero at $[(1)_{\sigma \in \Sigma_K^\infty})] \in T_{K,S}$. Hence, for $[D], [D'] \in T$, we have

$$\begin{aligned}
\delta_{K,S}([D], [D']) = 0 &\iff \delta_{K,S}([D], [D']) = \delta^1_{K,S}([(1)_{\sigma \in \Sigma_K^\infty})]) \\
&\iff [D - D'] = [(\mathcal{O}_{K,S}, (1)_{\sigma \in \Sigma_K^\infty})_S] \\
&\iff [D] = [(\mathcal{O}_{K,S}, (1)_{\sigma \in \Sigma_K^\infty})_S] + [D'] \\
&\iff [D] = [D'].
\end{aligned}$$

Here we used that $(\mathcal{O}_{K,S}, (1)_{\sigma \in \Sigma_K^\infty})_S$ defines the zero Arakelov S-divisor. We conclude that $\delta_{K,S}$ satisfies the first condition of a metric.

Let $[D], [D'] \in T$. Then there exists some $[(\mathcal{O}_{K,S}, v)_S] \in \zeta_S(T_{K,S})$ such that $[D - D'] = [(\mathcal{O}_{K,S}, v)_S]$. So

$$[D' - D] = [-(\mathcal{O}_{K,S}, v)_S] = [(\mathcal{O}_{K,S}, v^{-1})_S].$$

We obtain that

$$\delta_{K,S}([D'], [D]) = \delta^1_{K,S}([v^{-1}]) = \inf_{a \in \mathcal{O}^*_{K,S}} \| \log(\hat{a}v^{-1}) \|_{\mathbb{R}} = \inf_{a \in \mathcal{O}^*_{K,S}} \| - \log(\hat{a}v) \|_{\mathbb{R}},$$

where in the last step, we can take out the -1 power since running over $a \in \mathcal{O}^*_{K,S}$ is the same as running over $a^{-1} \in \mathcal{O}^*_{K,S}$. Then

$$\delta_{K,S}([D'], [D]) = \inf_{a \in \mathcal{O}^*_{K,S}} \| \log(\hat{a}v) \|_{\mathbb{R}} = \delta^1_{K,S}([v]) = \delta_{K,S}([D], [D']).$$

So the function $\delta_{K,S}$ is symmetric.

Let $[D_1], [D_2], [D_3] \in T$. Then there exist $[(\mathcal{O}_{K,S}, u)_S], [(\mathcal{O}_{K,S}, v)_S] \in \zeta_S(T_{K,S})$ such that

$$[D_1 - D_2] = [(\mathcal{O}_{K,S}, u)_S],$$

$$[D_2 - D_3] = [(\mathcal{O}_{K,S}, v)_S].$$

Adding these two equations, we get

$$[D_1 - D_3] = [(\mathcal{O}_{K,S}, uv)_S].$$

We obtain that

$$\delta_{K,S}([D_1], [D_3]) = \delta^1_{K,S}([vw]) = \inf_{a \in \mathcal{O}^*_{K,S}} \| \log(\hat{a}vw) \|_{\mathbb{R}} = \inf_{b,c \in \mathcal{O}^*_{K,S}} \| \log(\hat{b}\hat{c}vw) \|_{\mathbb{R}},$$

where in the last step, we use that running over $a \in \mathcal{O}^*_{K,S}$ is the same as running over $b, c \in \mathcal{O}^*_{K,S}$. So

$$\begin{aligned}
\delta_{K,S}([D_1], [D_3]) &= \inf_{b,c \in \mathcal{O}^*_{K,S}} \| \log(\hat{b}v) + \log(\hat{c}w) \|_{\mathbb{R}} \\
&\leq \inf_{b \in \mathcal{O}^*_{K,S}} \| \log(\hat{b}v) \|_{\mathbb{R}} + \inf_{c \in \mathcal{O}^*_{K,S}} \| \log(\hat{c}w) \|_{\mathbb{R}} \\
&= \delta^1_{K,S}([v]) + \delta^1_{K,S}([w]) \\
&= \delta_{K,S}([D_1], [D_2]) + \delta_{K,S}([D_2], [D_3]).
\end{aligned}$$

In these calculations, we used the triangle inequality for the norm $\|.\|_{\mathbb{R}}$. Hence, the function $\delta_{K,S}$ satisfies the triangle inequality.

Since the function $\delta_{K,S} \colon T \times T \to \mathbb{R}$ satisfies all conditions, we conclude that it is a metric on T. □

Let T be a connected component of $\mathrm{Pic}_{K,S}$. Then Proposition 5.3.13 tells us that we have a metric space $(T, \delta_{K,S})$. Therefore, it makes sense to talk about the open balls.

Lemma 5.3.14. Let T be a connected component of $\mathrm{Pic}_{K,S}$. Then for any $\varepsilon \in \mathbb{R}_{>0}$ and any $[(I, u)_S] \in T$ one has

$$B^{\delta_{K,S}}([(I, u)_S], \varepsilon) = \left\{ [(I, v)_S] : v \in \prod_{\sigma \in \Sigma^\infty_K} \mathbb{R}_{>0} \text{ and } \| \log(uv^{-1}) \|_{\mathbb{R}} < \varepsilon \right\}.$$

Proof. Set

$$\mathcal{A} := \left\{ [(I,v)_S] : v \in \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}_{>0} \text{ and } \| \log(uv^{-1}) \|_{\mathbb{R}} < \varepsilon \right\}.$$

The open ball of radius $\varepsilon \in \mathbb{R}_{>0}$ with center $[(I,u)_S] \in T$ is given by

$$B^{\delta_{K,S}}([(I,u)_S], \varepsilon) = \{[(J,v)_S] \in T : \delta_{K,S}([(I,u)_S], [(J,v)_S]) < \varepsilon\}.$$

Take any $[(J,v)_S] \in B_\varepsilon^{\delta_{K,S}}([(I,u)_S])$. By Remark 5.3.9, there exists an $x \in K^*$ such that $J = xI$. We get that

$$[(J,v)_S] = [(xI,v)_S] = [(I,w)_S],$$

for some $w \in \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}_{>0}$. It follows that $[(I,w)_S] \in B^{\delta_{K,S}}([(I,u)_S], \varepsilon)$, and so

$$\varepsilon > \delta_{K,S}([(I,u)_S], [(I,w)_S]) = \delta^1_{K,S}([uw^{-1}]).$$

We obtain that

$$B^{\delta_{K,S}}([(I,u)_S], \varepsilon) = \left\{ [(I,v)_S] : v \in \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}_{>0} \text{ and } \delta^1_{K,S}([uv^{-1}]) < \varepsilon \right\}.$$

Let $[(I,v)_S] \in B^{\delta_{K,S}}([(I,u)_S], \varepsilon)$. Then

$$\varepsilon > \delta^1_{K,S}([uv^{-1}]) = \inf_{a \in \mathcal{O}^*_{K,S}} \| \log(\hat{a}uv^{-1}) \|_{\mathbb{R}}.$$

By definition of the infimum, there exists an $a_0 \in \mathcal{O}^*_{K,S}$ such that $\| \log(\hat{a_0}uv^{-1}) \|_{\mathbb{R}} < \varepsilon$. Therefore, we get that $[(I, (\hat{a_0})^{-1}v)_S] \in \mathcal{A}$. Since a_0 is a unit of $\mathcal{O}_{K,S}$, we have $[(I, (\hat{a_0})^{-1}v)_S] = [(I,v)_S]$. Hence, we have $[(I,v)_S] \in \mathcal{A}$. Conversely, take any $[(I,v)_S] \in \mathcal{A}$. Then

$$\varepsilon > \| \log(uv^{-1}) \|_{\mathbb{R}} \geq \inf_{a \in \mathcal{O}^*_{K,S}} \| \log(\hat{a}uv^{-1}) \|_{\mathbb{R}} = \delta^1_{K,S}([uv^{-1}]).$$

Thus, we see that $[(I,v)_S] \in B^{\delta_{K,S}}([(I,u)_S], \varepsilon)$. By set inclusion from both sides, we get that

$$B^{\delta_{K,S}}([(I,u)_S], \varepsilon) = \mathcal{A}. \qquad \square$$

For any $\varepsilon \in \mathbb{R}_{>0}$, the open ball $B^{\delta_{K,S}}([D], \varepsilon)$ is contained in the connected component T of $\mathrm{Pic}_{K,S}$ such that $[D] \in T$. But we can still use the group operation of $\mathrm{Pic}_{K,S}$ on the open ball. So we can add any other element of $\mathrm{Pic}_{K,S}$. We get the following result.

Lemma 5.3.15. For any $\varepsilon \in \mathbb{R}_{>0}$ and $[D], [D'] \in \mathrm{Pic}_{K,S}$ one has

$$[D'] + B^{\delta_{K,S}}([D], \varepsilon) = B^{\delta_{K,S}}([D + D'], \varepsilon).$$

Proof. Let T be a connected component of $\mathrm{Pic}_{K,S}$ and take $[D_1], [D_2] \in T$. Then for any $[D_3] \in \mathrm{Pic}_{K,S}$, we have

$$\delta_{K,S}([D_1 + D_3], [D_3 + D_2]) = \delta_{K,S}([D_1], [D_2]). \tag{93}$$

This follows from the fact that

$$[(D_1 + D_3) - (D_3 + D_2)] = [D_1 - D_2].$$

Now, take any

$$[D'] + [D''] \in [D'] + B^{\delta_{K,S}}([D], \varepsilon).$$

Then $\delta_{K,S}([D],[D'']) < \varepsilon$. So by Equation (93), we get

$$\delta_{K,S}([D+D'],[D'+D'']) = \delta_{K,S}([D],[D'']) < \varepsilon.$$

It follows that $[D'] + [D''] \in B^{\delta_{K,S}}([D+D'],\varepsilon)$.

Conversely, take any $[D''] \in B^{\delta_{K,S}}([D+D'],\varepsilon)$. Then $\delta_{K,S}([D+D'],[D'']) < \varepsilon$. Set $D''' := D'' - D'$. Then by Equation (93), we get

$$\delta_{K,S}([D],[D''']) = \delta_{K,S}([D+D'],[D'+D''']) = \delta_{K,S}([D+D'],[D'']) < \varepsilon.$$

Thus, we get that $[D'''] \in B^{\delta_{K,S}}([D],\varepsilon)$. Since, $D''' := D'' - D'$, we get that

$$D'' \in [D'] + B^{\delta_{K,S}}([D],\varepsilon). \qquad \square$$

As in Proposition 5.3.8, we endow the connected components of $\mathrm{Pic}_{K,S}$ with the subspace topology induced from the natural topology on $\mathrm{Pic}_{K,S}$.

Theorem 5.3.16. The metric $\delta_{K,S}$ induces the subspace topology on the connected components of $\mathrm{Pic}_{K,S}$.

Proof. Let T be a connected component of $\mathrm{Pic}_{K,S}$. Take any open subset $A \subseteq T$ with respect to the metric $\delta_{K,S}$ on T. Since open balls form a basis of a metrizable topology, we know that A can be written as the union of open balls. Hence, in order to show that A is open with respect to the subspace topology, it suffices to show that an open ball is open with respect to the subspace topology. By the construction of the subspace topology, it suffices to show that it is open in $\mathrm{Pic}_{K,S}$ with respect to the natural topology. So consider an open ball $B := B^{\delta_{K,S}}([(I,v)_S],\varepsilon)$ for some $\varepsilon \in \mathbb{R}_{>0}$ and $[(I,v)_S] \in T$. Now, let $\phi\colon \mathrm{Div}_{K,S} \to \mathrm{Pic}_{K,S}$ be the canonical map. Then B is open with respect to the natural topology if $\phi^{-1}(B)$ is open in $\mathrm{Div}_{K,S}$. By Lemma 5.3.14, we have

$$B = \left\{ [(I,v)_S] : v \in \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}_{>0} \text{ and } \|\log(uv^{-1})\|_{\mathbb{R}} < \varepsilon \right\}.$$

Then

$$\begin{aligned}
\phi^{-1}(B) &= \left\{ (I,v)_S : v \in \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}_{>0} \text{ and } \|\log(uv^{-1})\|_{\mathbb{R}} < \varepsilon \right\} + \mathrm{Prin}_{K,S} \\
&= \left\{ (I,v)_S : v \in \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}_{>0} \text{ and } \|\log(uv^{-1})\|_{\mathbb{R}} < \varepsilon \right\} + \bigcup_{x \in K^*} \{(x^{-1}\mathcal{O}_{K,S}, \hat{x})_S\},
\end{aligned}$$

where in the last step we Equation 70. Now, adding the two sets comes down to adding $(I,v)_S$ with $(x^{-1}\mathcal{O}_{K,S},\hat{x})_S$. We obtain that

$$\phi^{-1}(B) = \bigcup_{x \in K^*} \left\{ (x^{-1}I, \hat{x}v)_S : v \in \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}_{>0} \text{ and } \|\log(uv^{-1})\|_{\mathbb{R}} < \varepsilon \right\}.$$

Now, writing this in terms of the isomorphism (91), we have

$$\phi^{-1}(B) = \bigcup_{x \in K^*} \{(\mathrm{ord}_{\mathfrak{p}}(x) - \mathrm{ord}_{\mathfrak{p}}(I))_{\mathfrak{p} \notin S}\} \times \left(-\log(\hat{x}) + \mathcal{B}^{d_{\mathbb{R}}}(-\log(u),\varepsilon)\right).$$

We know that $\{(\mathrm{ord}_{\mathfrak{p}}(x) - \mathrm{ord}_{\mathfrak{p}}(I))_{\mathfrak{p} \notin S}\}$ is open in the discrete topological space $\bigoplus_{\mathfrak{p} \notin S} \mathbb{Z}$. Furthermore, we know that $\mathcal{B}^{d_{\mathbb{R}}}(-\log(u),\varepsilon)$ is open in $\prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}$. It follows from Corollary 2.1.4 that $-\log(\hat{x}) + \mathcal{B}^{d_{\mathbb{R}}}(-\log(u),\varepsilon)$

is open in $\prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}$. It follows by the product topology that $\phi^{-1}(B)$ is open in $\mathrm{Div}_{K,S}$. As a result of this, we see that B is open in $\mathrm{Pic}_{K,S}$ with respect to the natural topology.

Conversely, suppose that $A \subseteq T$ is open with respect to the subspace topology on T. Then by the subspace topology, there exists some open subset $B \subseteq \mathrm{Pic}_{K,S}$ such that $A = B \cap T$. With the same argument as in the proof of Lemma 5.3.6, there exist open subsets $Z_i \subseteq \bigoplus_{\mathfrak{p}\notin S}\mathbb{Z}$, $\varepsilon_j \in \mathbb{R}_{>0}$, and $u_j \in \prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}_{>0}$ such that

$$B = \bigcup_{i\in I}\left(\bigcup_{j\in J}\left\{[(I,v)_S] : (-\operatorname{ord}_{\mathfrak{p}}(I))_{\mathfrak{p}\notin S} \in Z_i, v \in \prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}_{>0} \text{ and } \|\log(u_j v)\|_{\mathbb{R}} < \varepsilon_j\right\}\right),$$

for some index sets I, J. Since T is a connected component of $\mathrm{Pic}_{K,S}$, we know by Proposition 5.3.8 that $T = [D] + \zeta_S(T_{K,S})$ for some $[D] \in \mathrm{Pic}_{K,S}$. Thus, write $D = (I,u)$, then

$$T = [D] + \left\{[(\mathcal{O}_{K,S},u)_S] : u \in \prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}_{>0}\right\} = \left\{[(I,u)_S] : u \in \prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}_{>0}\right\}.$$

Let L contain all the elements $x \in K^*$ such that xI is represented in Z_i for some $i \in I$. Then either $B \cap T = \emptyset$ or

$$B \cap T = \bigcup_{x\in L}\left(\bigcup_{j\in J}\left\{[(xI,v)_S] : v \in \prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}_{>0} \text{ and } \|\log(u_j v)\|_{\mathbb{R}} < \varepsilon_j\right\}\right).$$

This follows from the fact that $[(xI,v)_S] = [(I,\hat{x}v)_S]$, so $[(xI,v)_S] \in T$. So we also have

$$\begin{aligned} B \cap T &= \bigcup_{x\in L}\left(\bigcup_{j\in J}\left\{[(I,\hat{x}v)_S] : v \in \prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}_{>0} \text{ and } \|\log(u_j v)\|_{\mathbb{R}} < \varepsilon_j\right\}\right) \\ &= \bigcup_{x\in L}\left(\bigcup_{j\in J}[(\mathcal{O}_{K,S},\hat{x})_S] + \left\{[(I,v)_S] : v \in \prod_{\sigma\in\Sigma_K^\infty}\mathbb{R}_{>0} \text{ and } \|\log(u_j v)\|_{\mathbb{R}} < \varepsilon_j\right\}\right), \end{aligned}$$

where in the last step one splits $[(I,\hat{x}v)_S]$ into the sum $[(\mathcal{O}_{K,S},\hat{x})_S] + [(I,v)_S]$. By Lemma 5.3.14, this latter equals

$$B \cap T = \bigcup_{x\in L}\left(\bigcup_{j\in J}[(\mathcal{O}_{K,S},\hat{x})_S] + B^{\delta_{K,S}}([(I,u_j^{-1})_S],\varepsilon_j)\right).$$

By Lemma 5.3.15, we get that

$$B \cap T = \bigcup_{x\in L}\left(\bigcup_{j\in J}B^{\delta_{K,S}}([(I,\hat{x}u_j^{-1})_S],\varepsilon_j)\right).$$

It follows that $A = B \cap T$ is either empty or given by the union of open balls. It follows that A is open with respect to the metric. □

So let us summarize what we have seen in this section. We endowed $\mathrm{Pic}_{K,S}$ with the natural topology. The connected components, with respect to this topology, are given by the cosets of $\zeta_S(T_{K,S})$ in $\mathrm{Pic}_{K,S}$. Every connected component admits a metric, given by $\delta_{K,S}$. This metric induces the subspace topology on the connected components. The question remains whether we can recover the natural topology on $\mathrm{Pic}_{K,S}$ from $\delta_{K,S}$. This would mean that the natural topology is metrizable. But the function $\delta_{K,S}$ is only defined for equivalence classes of Arakelov S-divisors that lie on the same connected component. Hence, we cannot

extend $\delta_{K,S}$ to a metric on $\mathrm{Pic}_{K,S}$. However, there is still a way to recover the natural topology on $\mathrm{Pic}_{K,S}$ from $\delta_{K,S}$.

Let X be a topological space and $\{C_i\}_{i\in I}$ a partition of X, for some index set I. We refer to the topology on X as the natural topology. Suppose now that any C_i is a topological space as well (so we do not endow it necessarily with the subspace topology). Then we can create a new topology on X that is induced from the partition. We say $A \subseteq X$ is open if $A \cap C_i$ is open in C_i for all $i \in I$. It is not hard to verify that this gives a topology on X. We refer to this as the partition topology on X. So we now have two topologies on X; the natural topology and the partition topology. Are there cases in which they are equal? What if we would endow C_i with the subspace topology induced from the natural topology? In that case, is it true that the partition topology on X coincides with the natural topology on X?

Proposition 5.3.17. Endow any C_i with the subspace topology induced from the natural topology on X. Then the partition topology on X coincides with the natural topology on X.

Proof. Suppose that A is open in X with respect to the partition topology. Then $A \cap C_i$ is open in C_i for all $i \in I$. By the subspace topology on C_i, this means that there exists some open subset B_i in X, with respect to the natural topology, such that $B_i \cap C_i = A \cap C_i$ for all $i \in I$. Then using that $\{C_i\}_{i\in I}$ forms a partition of X, we have

$$A \cap X = A \cap \left(\bigsqcup_{i\in I} C_i \right) = \bigsqcup_{i\in I} (A \cap C_i) = \bigsqcup_{i\in I} (B_i \cap C_i) = \left(\bigcup_{i\in I} B_i \right) \cap \left(\bigsqcup_{i\in I} C_i \right) = \left(\bigcup_{i\in I} B_i \right) \cap X = \left(\bigcup_{i\in I} B_i \right).$$

Since $A = A \cap X$, we now know that A equals the union of open subsets with respect to the natural topology. Hence, the subset A is open in X with respect to the natural topology.

Conversely, suppose that A is open in X with respect to the natural topology. Then $A \cap C_i$ is open in C_i for all $i \in I$, by the subspace topology. This says exactly that A is also open in X with respect to the partition topology. □

The result of this proposition might feel trivial. But we wanted to specify this explicitly because we know that $\mathrm{Pic}_{K,S}$ is the disjoint union of its connected components, which are also the cosets of $\zeta_S(T_{K,S})$ in $\mathrm{Pic}_{K,S}$. Let R be a set of representatives for $\mathrm{Pic}_{K,S}/\zeta_S(T_{K,S})$. Then

$$\mathrm{Pic}_{K,S} = \bigsqcup_{[D]\in R} ([D] + \zeta_S(T_{K,S})).$$

By Theorem 5.3.16, the topology on the connected components is induced by $\delta_{K,S}$. Hence, also the partition topology on $\mathrm{Pic}_{K,S}$ is in some way induced by $\delta_{K,S}$. We endowed the connected components with the subspace topology induced from the natural topology on $\mathrm{Pic}_{K,S}$. It follows from Proposition 5.3.17 that the partition topology equals the natural topology on $\mathrm{Pic}_{K,S}$. It allows us to conclude that the natural topology on $\mathrm{Pic}_{K,S}$ is in some sense induced from $\delta_{K,S}$. This is stated in Chapter 6 of [Sch08] for $S = \emptyset$. So while the distance is only defined on the connected components (therefore $\delta_{K,S}$ is only a metric on the connected components) the natural topology on $\mathrm{Pic}_{K,S}$ is still in a certain sense metrizable.

5.4 Reduced Arakelov S-Divisors

In Definition 4.2.3, we defined reduced Arakelov divisors. We saw that they play a major role in the infrastructure. Recall that an Arakelov divisor $D \in \mathrm{Div}_K$ is called reduced if it is of the form $D = \pi(I)$ for some $I \in \mathrm{Id}_K$ such that $1 \in I$ is minimal. We can use the extension π_S of the group homomorphism π seen in Definition 5.1.11. It remains to generalize the notion of a minimal element in a fractional ideal of $\mathcal{O}_{K,S}$. We want to obtain two things in the generalization. If we take $S = \emptyset$, we should recover the original setting. Furthermore, only finitely many fractional ideals of $\mathcal{O}_{K,S}$ may have 1 as a minimal element. This ensures

that the number of reduced Arakelov S-divisors is finite. In this section, we propose two definitions that both fulfill these wishes.

Trying to describe Definition 4.2.1 in words, we get that a minimal element of a fractional ideal of $\mathcal{O}_K$ is minimal with respect to every infinite place. This can be seen as being minimal in $K_{\mathbb{R}} = \prod_{\sigma \in \Sigma_K^\infty} K_\sigma$. With the S-integers, we have seen that it is useful to consider K_S instead of $K_{\mathbb{R}}$. So, if we want to be minimal in K_S, we need to consider the finite places in S as well. Therefore, we get the following definitions.

Definition 5.4.1. Let $x, y \in K^*$, we write $x \preccurlyeq_S y$ if $|x|_\sigma < |y|_\sigma$ for all $\sigma \in \Sigma_K^\infty$ and $|x|_\mathfrak{p} \leq |y|_\mathfrak{p}$ for all $\mathfrak{p} \in S$.

Note that $\preccurlyeq_S$ is not a partial order as $x \preccurlyeq_S y$ and $y \preccurlyeq_S x$ does not imply that $x = y$.

Definition 5.4.2. Let I be a fractional ideal of $\mathcal{O}_{K,S}$. An element $x \in I$ is called *strongly S-minimal* in I if it is non-zero and if the only element $y \in I$ for which $y \preccurlyeq_S x$ is $y = 0$.

When we take $S = \emptyset$, we simply recover Definition 4.2.1. In this case, we still use the terminology of minimal elements rather than strongly $\emptyset$-minimal elements. Furthermore, we use the notation $\preccurlyeq$ rather than $\preccurlyeq_\emptyset$ from Definition 5.4.1. In the general case, let us look into the existence of strongly S-minimal elements in a fractional ideal.

Lemma 5.4.3. Let Γ be a lattice in K_S and $C \subseteq K_S$ a compact subset. Then $\Gamma \cap C$ is a finite set.

Proof. Since Γ is a lattice, it is a discrete subgroup and therefore closed in K_S (see Proposition 2.3.3). It follows by the subspace topology that $\Gamma \cap C$ is closed in C. We obtain that $\Gamma \cap C$ is also compact in C (see [Sin19, Theorem 5.1.7]). Since $\Gamma \cap C \subseteq \Gamma$, it follows from Proposition 2.3.2 (ii.) that $\Gamma \cap C$ is discrete. We see that $\Gamma \cap C$ is discrete and compact. It follows from Proposition 2.3.2 (iii.) that $\Gamma \cap C$ is a finite set. □

Proposition 5.4.4. Let $I \in \mathrm{Id}_{K,S}$ be non-zero, then I contains at least one strongly S-minimal element.

Proof. Take any arbitrary non-zero $x_0 \in I$. If x_0 is strongly S-minimal in I, then we are done. Otherwise, there exists a non-zero $x_1 \in I$ such that $x_1 \preccurlyeq_S x_0$. In its turn, either x_1 is strongly S-minimal in I, or there exists a non-zero $x_2 \in I$ such that $x_2 \preccurlyeq_S x_1$. Continuing this process, we either terminate to an S-minimal element of I, or we get an infinite sequence $(x_i)_{i \geq 0}$ of distinct non-zero elements of I such that $x_{i+1} \preccurlyeq_S x_i$, for all $i \in \mathbb{Z}_{\geq 0}$. We will show that the latter case reaches a contradiction. Hence, the existence of a strongly S-minimal element in I is guaranteed. By the monotone convergence theorem in $\mathbb{R}$, we have that the sequence $(|x_i|_\nu)_{i \geq 0}$ convergences for all $\nu \in S^\infty$. Set

$$\alpha_\nu := \lim_{i \to \infty} |x_i|_\nu,$$

for all $\nu \in S^\infty$. This means that for any $\nu \in S^\infty$ and for all $\varepsilon \in \mathbb{R}_{>0}$ there exist infinitely many i such that $|x_i|_\nu \in [\alpha_\nu, \alpha_\nu + \varepsilon]$. Let $\varepsilon \in \mathbb{R}_{>0}$ and $s := \#S^\infty$. Then this means that there exist infinitely many i such that

$$\alpha_\nu \leq |x_i|_\nu \leq \alpha_\nu + \frac{\varepsilon}{s},$$

for all $\nu \in S^\infty$. Set $\alpha := \sum_{\nu \in S^\infty} \alpha_\nu$, then for infinitely many i

$$\alpha \leq \sum_{\nu \in S\infty} |x_i|_\nu \leq \alpha + \varepsilon.$$

Using the metric d_S on K_S (see Equation (25)), we obtain that

$$\alpha \leq d_S(\Psi_S(x_i), 0) \leq \alpha + \varepsilon.$$

Thus, there are infinitely many i such that $\Psi_S(x_i) \in \{v \in K_S : \alpha \leq d_S(v, 0) \leq \alpha + \varepsilon\} =: A$. Note that

$$A = \big(K_S \backslash B^{d_S}(0, \alpha)\big) \cap B^{d_S}[0, \alpha + \varepsilon],$$

using the open and closed ball definition from the beginning of Section 3.3.1. Since A is an intersection of closed sets, we know that it is closed in K_S. Moreover, the set A is bounded by $2(\alpha+\varepsilon)$. It follows by Theorem 3.3.12 that A is compact in K_S. By Theorem 3.4.6, we know that $\Psi_S(I)$ forms a lattice in K_S. Since $x_i \in I$, we get that $\Psi_S(I) \cap A$ is an infinite set. This contradicts Lemma 5.4.3. □

Example 5.4.5. Let $K = \mathbb{Q}$, and so $\mathcal{O}_K = \mathbb{Z}$. We have, up to equivalence, one Archimedean absolute value given by the absolute value $|.|_\infty$ on $\mathbb{Q}$. The prime ideals of $\mathbb{Z}$ are given by $p\mathbb{Z}$ for some prime number $p \in \mathbb{Z}$. Since any fractional ideal of $\mathbb{Z}$ factors into the non-zero prime ideals of $\mathbb{Z}$, we know that the fractional ideals of $\mathbb{Z}$ are given by $\frac{a}{b}\mathbb{Z}$ for $a, b \in \mathbb{Z}$. In a fractional ideal, given by $\frac{a}{b}\mathbb{Z}$, the minimal elements are given by

$$\left\{\frac{a}{b}, -\frac{a}{b}\right\}.$$

Namely, any other element in this fractional ideal is an integer multiple of one of these, hence bigger in absolute value. Now, let S be the set only containing the prime ideal $2\mathbb{Z}$. By Proposition 3.1.4, the ring of S-integers is given by $\mathbb{Z}\left[\frac{1}{2}\right]$. Furthermore, in Proposition 3.2.1, we saw that the prime ideals of $\mathbb{Z}\left[\frac{1}{2}\right]$ are given by $p\mathbb{Z}\left[\frac{1}{2}\right]$ for any prime number $p \neq 2$. Consequently, the distinct fractional ideals of $\mathbb{Z}\left[\frac{1}{2}\right]$ are given by $\frac{a}{b}\mathbb{Z}\left[\frac{1}{2}\right]$ for $a, b \in \mathbb{Z}$ such that $a, b \equiv 1 \bmod 2$.

Let us determine the strongly S-minimal elements of any fractional ideal of $\mathbb{Z}\left[\frac{1}{2}\right]$. So consider the fractional ideal $I := \frac{a}{b}\mathbb{Z}\left[\frac{1}{2}\right]$ for $a, b \in \mathbb{Z}$ such that $a, b \equiv 1 \bmod 2$. We claim that the strongly S-minimal elements are given by

$$\left\{\pm 2^k \frac{a}{b} : k \in \mathbb{Z}\right\}. \tag{94}$$

To show the claim, let $x := \pm 2^k \frac{a}{b}$ for some $k \in \mathbb{Z}$. Suppose there exists some non-zero $y \in I$ such that $|y|_2 \leq |x|_2$, i.e. $\mathrm{ord}_2(y) \geq \mathrm{ord}_2(x) = k$. Since $y \in I$, there exists some $z \in \mathbb{Z}\left[\frac{1}{2}\right]$ such that $y = \frac{a}{b}z$. Moreover, we have $\mathrm{ord}_2(z) = \mathrm{ord}_2(y)$ since $a, b \equiv 1 \bmod 2$. Set this integer equal to $l \in \mathbb{Z}$. Then there exists some $m \in \mathbb{Z}$ such that $m \equiv 1 \bmod 2$ and $z = 2^l m$. We get that $y = \frac{a}{b}2^l m$, with $l \geq k$. Then

$$|y|_\infty = \left|\frac{a}{b}2^l m\right|_\infty \geq \left|\frac{a}{b}2^l\right|_\infty \geq \left|\frac{a}{b}2^k\right|_\infty = |x|_\infty.$$

This means that there cannot exist a non-zero element $y \in I$ such that $y \preccurlyeq_S x$. It follows that $x \in I$ is strongly S-minimal. Thus, all the elements of set (94) are strongly S-minimal. Any non-zero element of I that is not included in this set is of the form $\frac{a}{b}2^k m$ for some $k, m \in \mathbb{Z}$ such that $m \equiv 1 \bmod 2$ and $m \neq \pm 1$. Then this cannot be strongly S-minimal since $\frac{a}{b}2^k \preccurlyeq_S \frac{a}{b}2^k m$ with $\frac{a}{b}2^k \in I$. Hence, we showed that the set (94) contains exactly all strongly S-minimal elements of I.

Observe, if we take $a, b \equiv 1 \bmod 2$, then $\frac{a}{b}$ is minimal in $\frac{a}{b}\mathbb{Z}$ and strongly S-minimal in $\frac{a}{b}\mathbb{Z}\left[\frac{1}{2}\right]$. ■

Now, the last observation of the example can be generalized. Recall Definition 3.2.4 of the fractional ideal $I_S \in \mathrm{Id}_K$ for some $I \in \mathrm{Id}_{K,S}$.

Proposition 5.4.6. Let $I \in \mathrm{Id}_{K,S}$. If $x \in I_S$ is minimal, then it is strongly S-minimal in I.

Proof. In this proof, we will repeatedly use Definition 1.1.7 and Proposition 1.1.8. Suppose that $x \in I_S$ is minimal. Then x is also contained in $I = I_S\mathcal{O}_{K,S}$. Assume that there exists some $y \in I$ such that $y \preccurlyeq_S x$. Since $y \in I$ we have $y\mathcal{O}_{K,S} \subseteq I$, i.e. $I | y\mathcal{O}_{K,S}$. This means that $\mathrm{ord}_{\mathfrak{p}\mathcal{O}_{K,S}}(I) \leq \mathrm{ord}_{\mathfrak{p}\mathcal{O}_{K,S}}(y)$ for all $\mathfrak{p} \notin S$. By the definition of I_S, we have $\mathrm{ord}_{\mathfrak{p}}(I_S) = \mathrm{ord}_{\mathfrak{p}\mathcal{O}_{K,S}}(I)$ for all $\mathfrak{p} \notin S$. In Proposition 3.2.2, we have seen that $\mathrm{ord}_{\mathfrak{p}\mathcal{O}_{K,S}}(y) = \mathrm{ord}_{\mathfrak{p}}(y)$ for all $\mathfrak{p} \notin S$. We get that

$$\mathrm{ord}_{\mathfrak{p}}(I_S) \leq \mathrm{ord}_{\mathfrak{p}}(y), \qquad \mathfrak{p} \notin S. \tag{95}$$

Since $x \in I_S$, we have $x\mathcal{O}_K \subseteq I_S$, i.e. $I_S | x\mathcal{O}_K$. This means that $\mathrm{ord}_{\mathfrak{p}}(I_S) \leq \mathrm{ord}_{\mathfrak{p}}(x)$ for all $\mathfrak{p} \in \mathfrak{P}_K^0$. Furthermore, since $y \preccurlyeq_S x$, we have $|y|_{\mathfrak{p}} \leq |x|_{\mathfrak{p}}$. Hence, we obtain that

$$\mathrm{ord}_{\mathfrak{p}}(y) \geq \mathrm{ord}_{\mathfrak{p}}(x) \geq \mathrm{ord}_{\mathfrak{p}}(I_S) \qquad \mathfrak{p} \in S. \tag{96}$$

Combining (95) and (96), we see that $\mathrm{ord}_{\mathfrak{p}}(I_S) \leq \mathrm{ord}_{\mathfrak{p}}(y)$ for all $\mathfrak{p} \in \mathfrak{P}_K^0$. We conclude that $I_S | y\mathcal{O}_K$, and so $y\mathcal{O}_K \subseteq I_S$. Since $1 \in \mathcal{O}_K$, we get $y \in I_S$. So we get $y \in I_S$ such that $y \preccurlyeq_S x$. But then also $y \preccurlyeq x$. Thus, by the minimality of $x \in I_S$, we must have $y = 0$. This exactly shows that $x \in I$ is strongly S-minimal. □

The converse of this proposition is not true as we can see from Example 5.4.5. Namely, take $I = \frac{a}{b}\mathbb{Z}\left[\frac{1}{2}\right]$ for $a, b \equiv 1 \bmod 2$. Then $I_S = \frac{a}{b}\mathbb{Z}$. We have that $2\frac{a}{b} \in \frac{a}{b}\mathbb{Z}\left[\frac{1}{2}\right]$ is strongly S-minimal but it is not minimal in $\frac{a}{b}\mathbb{Z}$. However, notice that the only fractional ideal of $\mathbb{Z}\left[\frac{1}{2}\right]$ containing 1 as strongly S-minimal element is $\mathbb{Z}\left[\frac{1}{2}\right]$ itself. Namely, the strongly S-minimal elements of I are given by $\pm 2^k \frac{a}{b}$. Such an element equals 1 if and only if $k = 0$ and $a = b$, using that $a, b \equiv 1 \bmod 2$. Moreover, the fractional ideal $\mathbb{Z}$ contains 1 as a minimal element. Consequently, in this example, we see that 1 is strongly S-minimal in I if and only if it is minimal is I_S. This can also be generalized.

Lemma 5.4.7. Let $I \in \mathrm{Id}_{K,S}$. Then $1 \in I$ is strongly S-minimal if and only if $1 \in I_S$ is minimal.

Proof. The if-statement is given by Proposition 5.4.6. For the converse, suppose that $1 \in I$ is strongly S-minimal. First, we must show that $1 \in I_S$. We know by Equation (1) that

$$I = (I^{-1})^{-1} = \{x \in K : xI^{-1} \subseteq \mathcal{O}_{K,S}\}.$$

Since $1 \in I$, we have $I^{-1} \subseteq \mathcal{O}_{K,S}$. Therefore, we know that I^{-1} is an integral ideal. Consequently, for all $\mathfrak{p} \notin S$ there exists $n_{\mathfrak{p}} \in \mathbb{Z}_{\geq 0}$ such that $I^{-1} = \prod_{\mathfrak{p} \notin S} (\mathfrak{p}\mathcal{O}_{K,S})^{n_{\mathfrak{p}}}$. Then

$$I = \prod_{\mathfrak{p} \notin S} (\mathfrak{p}\mathcal{O}_{K,S})^{-n_{\mathfrak{p}}} \quad \Longrightarrow \; I_S = \prod_{\mathfrak{p} \notin S} \mathfrak{p}^{-n_{\mathfrak{p}}}.$$

We have $1 \in \mathfrak{p}^k$ for all $k \in \mathbb{Z}_{\leq 0}$ and $\mathfrak{p} \in \mathfrak{P}_K^0$. Since $-n_{\mathfrak{p}} \leq 0$, we obtain that $1 \in \prod_{\mathfrak{p} \notin S} \mathfrak{p}^{-n_{\mathfrak{p}}} = I_S$. Now, we can show that $1 \in I_S$ is minimal. Assume that there exists some $x \in I_S$ such that $x \preccurlyeq 1$. Since $x \in I_S$, we have by Lemma 3.2.5 that $|x|_{\mathfrak{p}} \leq 1$ for all $\mathfrak{p} \in S$. Together with the fact that $x \preccurlyeq 1$, we obtain that $x \preccurlyeq_S 1$. Since $x \in I_S$, it is also contained in $I = I_S\mathcal{O}_{K,S}$. By the strongly S-minimality of $1 \in I$, we must have $x = 0$. This exactly shows that $1 \in I_S$ is minimal. □

Now, we can generalize the notion of reduced Arakelov divisors.

Definition 5.4.8. An Arakelov S-divisor $D \in \mathrm{Div}_{K,S}$ is called *strongly reduced* if it is of the form $D = \pi_S(I)$ for some $I \in \mathrm{Id}_{K,S}$ such that $1 \in I$ is strongly S-minimal. The set of strongly reduced Arakelov S-divisors is denoted by $\mathrm{Red}_{K,S}^{\mathrm{s}}$.

If we take $S = \emptyset$, we recover Definition 4.2.3. In this case, we call an Arakelov divisor reduced instead of strongly reduced. Moreover, we still denote the set of reduced Arakelov divisors by Red_K.

Example 5.4.9. Note that the zero Arakelov S-divisor is given by $(\mathcal{O}_{K,S}, (1)_{\sigma \in \Sigma_K^\infty}) = \pi_S(\mathcal{O}_{K,S})$. So the zero Arakelov S-divisor is strongly reduced if $1 \in \mathcal{O}_{K,S}$ is strongly S-minimal. If $I = \mathcal{O}_{K,S}$, then $I_S = \mathcal{O}_K$. So by Proposition 5.4.6, it is enough to show that $1 \in \mathcal{O}_K$ is minimal. This is exactly what we showed in Example 4.2.4. Hence, we know that $1 \in \mathcal{O}_{K,S}$ is strongly S-minimal, and $\pi_S(\mathcal{O}_{K,S})$ is strongly reduced. ■

Theorem 5.4.10. The set of strongly reduced Arakelov S-divisors is finite.

Proof. Recall the bijection between fractional ideals of $\mathcal{O}_{K,S}$ with the fractional ideals of $\mathcal{O}_K$ coprime to S from (23). Together with Lemma 5.4.7, we have a bijection between

$$\{\pi_S(I) : I \in \mathrm{Id}_{K,S} \text{ and } 1 \in I \text{ is strongly } S\text{-minimal}\}$$

and

$$\{\pi(I) : I \in \mathrm{Id}_K^{\mathrm{CO}} \text{ and } 1 \in I \text{ is minimal}\}.$$

So we get

$$\begin{aligned}\#\operatorname{Red}^{s}_{K,S} &= \#\{\pi_S(I) : I \in \operatorname{Id}_{K,S} \text{ and } 1 \in I \text{ is strongly } S\text{-minimal}\}\\ &= \#\{\pi(I) : I \in \operatorname{Id}_K \text{ coprime to } S, \text{ and } 1 \in I \text{ is minimal}\}\\ &\leq \#\{\pi(I) : I \in \operatorname{Id}_K \text{ and } 1 \in I \text{ is minimal}\}\\ &= \#\operatorname{Red}_K .\end{aligned}$$

We see that $\operatorname{Red}_{K,S}$ must be a finite set since Red_K is finite (see [Sch08, Proposition 7.2]). □

Now, we propose a second extension of minimal elements and reduced Arakelov divisors. In Definition 5.4.1, we allowed equality at the finite places. But what if we remove those?

Definition 5.4.11. Let $x, y \in K$, we write $x \prec_S y$ if $|x|_\nu < |y|_\nu$ for all $\nu \in S^\infty$.

Note that $\prec_S$ is not a partial order as $x \prec_S y$ and $y \prec_S x$ does not imply that $x = y$.

Definition 5.4.12. Let I be a fractional ideal of $\mathcal{O}_{K,S}$. An element $x \in I$ is called *weakly S-minimal* in I if it is non-zero and if the only element $y \in I$ for which $y \prec_S x$ is $y = 0$.

When we take $S = \emptyset$, we simply recover Definition 4.2.1. In this case, we still use the terminology of minimal elements rather than weakly $\emptyset$-minimal elements. Now, let us look into the relation between weakly and strongly S-minimal elements.

Proposition 5.4.13. Let $I \in \operatorname{Id}_{K,S}$. If $x \in I$ is strongly S-minimal, then it is weakly S-minimal.

Proof. Assume that $x \in I$ is strongly S-minimal. Suppose that there exists some non-zero $y \in I$ such that $y \prec_S x$. Then it follows by definition that $y \preccurlyeq_S x$. Thus, by the strongly S-minimality of x, it follows that $y = 0$. Hence, the element x is weakly S-minimal. □

The result implies for any $I \in \operatorname{Id}_{K,S}$, we have

$$\{\text{strongly } S\text{-minimal elements of } I\} \subseteq \{ \text{ weakly } S\text{-minimal elements of } I\}.$$

The other set inclusion is not necessarily true.

Example 5.4.14. Let $K = \mathbb{Q}$, and use the same convention as in Example 5.4.5. Except, for this time, we take $S = \{5\mathbb{Z}\}$. By Proposition 3.1.4, the ring of S-integers is given by $\mathbb{Z}\left[\frac{1}{5}\right]$. Consider this ring as a fractional ideal of itself. We will show that $2 \in \mathbb{Z}\left[\frac{1}{5}\right]$ is weakly S-minimal but not strongly S-minimal. The latter is easy to see since $\operatorname{ord}_5(1) = \operatorname{ord}_5(2) = 0$, and so $1 \preccurlyeq_S 2$. Now, suppose that there exists some non-zero $x \in \mathbb{Z}\left[\frac{1}{5}\right]$ such that $|x|_5 < |2|_5$. Equivalently, we have $\operatorname{ord}_5(x) > \operatorname{ord}_5(2) = 0$. So we have $x \in \mathbb{Z}\left[\frac{1}{5}\right]$ and $\operatorname{ord}_5(x) > 0$. Consequently, we must have $x = 5^k a$ for some $k \in \mathbb{Z}_{>0}$ and $a \in \mathbb{Z}$. But then it is impossible to have $|x|_\sigma < |2|_\sigma$. Thus, there cannot exists a non-zero $x \in \mathbb{Z}\left[\frac{1}{5}\right]$ such that $x \preccurlyeq_S 2$. We conclude that the element 2 in $\mathbb{Z}\left[\frac{1}{5}\right]$ is weakly S-minimal but not strongly S-minimal. ■

Corollary 5.4.15. Let $I \in \operatorname{Id}_{K,S}$ be non-zero.

i.) Then I contains at least one weakly S-minimal element.

ii.) If $x \in I_S$ is minimal, then it is weakly S-minimal in I.

Proof. Statement (i.) is a direct consequence of Proposition 5.4.4 and 5.4.13. Statement (ii.) is a direct consequence of Proposition 5.4.6 and 5.4.13. □

Lemma 5.4.7 fails to hold for weakly S-minimal elements. To repeat the proof we would need that for any $I \in \operatorname{Id}_{K,S}$ and $x \in I$, one has $x \in I_S$ if and only if $|x|_{\mathfrak{p}} < 1$ for all $\mathfrak{p} \in S$. But this is not the case as we saw in Lemma 3.2.5.

Now we can generalize the notion of reduced Arakelov divisors once again.

Definition 5.4.16. An Arakelov S-divisor $D \in \mathrm{Div}_{K,S}$ is called *weakly reduced* if it is of the form $D = \pi_S(I)$ for some $I \in \mathrm{Id}_{K,S}$ such that $1 \in I$ is weakly S-minimal. The set of weakly reduced Arakelov S-divisors is denoted by $\mathrm{Red}^w_{K,S}$.

If we take $S = \emptyset$, we recover Definition 4.2.3. In this case, we call an Arakelov divisor reduced instead of weakly reduced. Moreover, we still denote the set of reduced Arakelov divisors by Red_K. A similar argument as in Example 5.4.9 shows that the zero Arakelov S-divisor is weakly reduced.

We would like to show that $\mathrm{Red}^w_{K,S}$ is finite, just like $\mathrm{Red}^s_{K,S}$. However, the proof of Theorem 5.4.10 uses Lemma 5.4.7. We just saw that this lemma does not hold for weakly S-minimal elements. Hence, we would have to reason differently. But we can use our analogue of Minkowski's Convex Body Theorem that we have seen in Theorem 3.3.23.

Theorem 5.4.17. The set of weakly reduced Arakelov S-divisors is finite.

Proof. Throughout this proof, we will use that a compact subset is Borel measurable (see Proposition 1.6.7). Thus, we can take the measure of a compact subset.

Take any $t \in [0, \frac{1}{2}]$ such that $\mathrm{ord}_{\mathfrak{p}}(t) = 0$ for all $\mathfrak{p} \in S$. This can always be found. Namely, since S is finite, you can pick any prime number $p \in \mathbb{Z}$ such that $p\mathcal{O}_K$ does not have any $\mathfrak{p} \in S$ in its factorization. Then $t = p^{-1}$ does the job. Let $D = \pi_S(I)$ be a weakly reduced Arakelov S-divisor. Set $u := (N_{\mathcal{O}_{K,S}}(I)^{-1/n})_{\sigma \in \Sigma_K^\infty} \in K_{\mathbb{R}}$, then $D = (I, u)_S$. Recall the notation

$$\widetilde{u} := (u, \underbrace{1, \ldots, 1}_{\#S \text{ times}}).$$

We have $\widetilde{u} \in K_S^*$. We know by Theorem 3.4.6 that $\Psi_S(I)$ is a lattice in K_S. Then by Lemma 3.4.5, we have seen that $\widetilde{u}\Psi_S(I)$ is a lattice in K_S. Therefore, we can consider its covolume. Recall that the DVR $\mathcal{O}_{\mathfrak{p}} = \{x \in K_{\mathfrak{p}} : |x|_{\mathfrak{p}} \leq 1\}$ is compact in $K_{\mathfrak{p}}$ for all $\mathfrak{p} \in S$ (see [Neu99, Proposition 5.1, Chapter II]). Since its maximal ideal $\mathfrak{m}_{\mathfrak{p}}$ is closed in $\mathcal{O}_{\mathfrak{p}}$, it is also compact. In Section 3.3.1, we gave $\mathcal{O}_{\mathfrak{p}}$ a finite measure with respect to $\mu_{\mathfrak{p}}$. By Proposition 1.6.4, it follows that $\mathfrak{m}_{\mathfrak{p}}$ has non-zero and finite measure with respect to $\mu_{\mathfrak{p}}$. So we can set

$$\alpha := \frac{\varepsilon}{2^{(r_1+r_2)}} \left(\frac{1}{\pi}\right)^{r_2} \frac{\left(\prod_{\mathfrak{p} \in S} \|t^{-1}\|_{\mathfrak{p}}\right) \mathrm{covol}(\widetilde{u}\Psi_S(I))}{\prod_{\mathfrak{p} \in S} \mu_{\mathfrak{p}}(\mathfrak{m}_{\mathfrak{p}})}, \in \mathbb{R}_{>0}$$

for some $\varepsilon \in \mathbb{R}_{>1}$ close to 1. Set $A_\sigma := \{x \in K_\sigma : |x|_\sigma \leq \alpha^{1/n}\}$ for any $\sigma \in \Sigma_K^\infty$. This set is closed and bounded in K_σ. By Theorem 1.4.8, we know that K_σ is isomorphic to $\mathbb{R}$ or $\mathbb{C}$. It follows by the Heine-Borel theorem that A_σ is compact in K_σ for all $\sigma \in \Sigma_K^\infty$. For a real field embedding $\sigma \in \Sigma_K^\infty$, we have that μ_σ is the Lebesgue measure on $\mathcal{B}(\mathbb{R})$. Then

$$\mu_\sigma(A_\sigma) = 2\alpha^{1/n}.$$

For a complex field embedding $\sigma \in \Sigma_K^\infty$, we have that μ_σ is twice the Lebesgue measure on $\mathcal{B}(\mathbb{R}^2)$. Then

$$\mu_\sigma(A_\sigma) = 2\alpha^{2/n}\pi.$$

Consider the set

$$A := \prod_{\sigma \in \Sigma_K^\infty} A_\sigma \times \prod_{\mathfrak{p} \in S} \mathfrak{m}_{\mathfrak{p}} = \{u \in K_S : |u_\sigma|_\sigma \leq \alpha^{1/n} \text{ for all } \sigma \in \Sigma_k^\infty, |u_{\mathfrak{p}}|_{\mathfrak{p}} < 1 \text{ for all } \mathfrak{p} \in S\}.$$

Then A is compact in K_S, since it is a product of compact sets. Recall that $\mu_S = \bigotimes_{\nu \in S^\infty} \mu_\nu$. So its measure with respect to μ_S is given by

$$\mu_S(A) = \prod_{\sigma \in \Sigma_k^\infty} \mu_\sigma(A_\sigma) \prod_{\mathfrak{p} \in S} \mu_{\mathfrak{p}}(\mathfrak{m}_{\mathfrak{p}}) = (2\alpha^{1/n})^{r_1}(2\alpha^{2/n}\pi)^{r_2} \prod_{\mathfrak{p} \in S} \mu_{\mathfrak{p}}(\mathfrak{m}_{\mathfrak{p}}) = 2^{r_1+r_2}\pi^{r_2}\alpha \prod_{\mathfrak{p} \in S} \mu_{\mathfrak{p}}(\mathfrak{m}_{\mathfrak{p}}).$$

From the definition of α, we get

$$\mu_S(A) = \varepsilon \left(\prod_{\mathfrak{p} \in S} \|t^{-1}\|_{\mathfrak{p}} \right) \operatorname{covol}(\widetilde{u}\Psi_S(I)).$$

Since $\varepsilon \in \mathbb{R}_{>1}$, we have that

$$\mu_S(A) > \left(\prod_{\mathfrak{p} \in S} \|t^{-1}\|_{\mathfrak{p}} \right) \operatorname{covol}(\widetilde{u}\Psi_S(I)).$$

For any $u \in A$, we have $-u \in A$ by the property that $|x|_\nu = |-x|_\nu$ for all $\nu \in \mathcal{V}_K$. Hence, the set A is symmetric as defined in Definition 3.3.21. Furthermore, for any $u, v \in A$, we have that $\Psi_S(t)u + \Psi_S(t)v \in A$. Namely, for any $\sigma \in \Sigma_K^\infty$, we have

$$|tu_\sigma + tv_\sigma|_\sigma \leq t(|u_\sigma|_\sigma + |v_\sigma|_\sigma) \leq \frac{|u_\sigma|_\sigma + |v_\sigma|_\sigma}{2} < \alpha^{1/n},$$

using that $t \in [0, \frac{1}{2}]$. For any $\mathfrak{p} \in S$, we have

$$|tu_\mathfrak{p} + tv_\mathfrak{p}|_\mathfrak{p} = |t|_\mathfrak{p}|u_\mathfrak{p} + v_\mathfrak{p}|_\mathfrak{p} = |u_\mathfrak{p} + v_\mathfrak{p}|_\mathfrak{p} \leq \max\{|u_\mathfrak{p}|_\mathfrak{p}, |v_\mathfrak{p}|_\mathfrak{p}\} < 1,$$

using that $\operatorname{ord}_\mathfrak{p}(t) = 0$ for all $\mathfrak{p} \in S$. Thus, the set A is $\Psi_S(t)$-convex as defined in Definition 3.3.22. Hence, we can apply Theorem 3.3.23. It states that there exists a non-zero $v \in \widetilde{u}\Psi_S(I) \cap A$. So write $v = \widetilde{u}\Psi_S(a)$ for some non-zero $a \in I$. Then $\widetilde{u}\Psi_S(a) \in A$, and so

$$|N_{\mathcal{O}_{K,S}}(I)^{-1/n} a|_\sigma < \alpha^{1/n}, \qquad |a|_\mathfrak{p} < 1,$$

using the construction of $\widetilde{u}$. Suppose that $N_{\mathcal{O}_{K,S}}(I^{-1}) > \alpha$. Then $|a|_\sigma < 1$ for all $\sigma \in \Sigma_K^\infty$. Consequently, we obtain that $a \prec_S 1$. This contradicts the fact that $1 \in I$ is weakly S-minimal. Therefore, we must have that $N_{\mathcal{O}_{K,S}}(I^{-1}) \leq \alpha$. Since I is a fractional ideal containing 1, we know that I^{-1} is an integral ideal of $\mathcal{O}_{K,S}$. By Proposition 1.1.10 (ii.), there can only exist finitely many integral ideals with bounded norm. We conclude that only finitely many weakly reduced Arakelov S-divisors exist. □

Remark 5.4.18. A consequence of Proposition 5.4.13 is that $\operatorname{Red}_{K,S}^s \subseteq \operatorname{Red}_{K,S}^w$. Hence, Theorem 5.4.10 is also a consequence of Theorem 5.4.17. Furthermore, in contrast to the proof of Theorem 5.4.10, the proof of Theorem 5.4.17 is independent of the fact that Red_K is finite. Theorem 5.4.17 is therefore also a proof for the finiteness of Red_K. One needs to take $S = \emptyset$. ♦

In conclusion, we have seen two extensions of minimal elements and reduced Arakelov divisors. In both cases, we recovered the original setting by taking $S = \emptyset$. Moreover, the number of strongly/weakly reduced Arakelov S-divisors is always finite.

Algorithm 4.2.7 describes a reduction algorithm for Arakelov divisors. Given an Arakelov divisor of K it returns a reduced Arakelov divisor that is ideal equivalent. In Remark 5.3.9, we saw that this is the same as returning a reduced Arakelov divisor that lies on the same connected component of Pic_K. This algorithm translates easily to Arakelov S-divisors in $\operatorname{Div}_{K,S}$.

Lemma 5.4.19. Let $I \in \operatorname{Id}_{K,S}$. If $x \in I$ is strongly (resp. weakly) S-minimal, then 1 is strongly (resp. weakly) S-minimal in $x^{-1}I$.

Proof. We have $1 \in x^{-1}I$, so it remains to check whether it is strongly (resp. weakly) S-minimal. Suppose that there exists $y \in x^{-1}I$ such that $y \preccurlyeq_S 1$ (resp. $y \prec_S 1$). Then y can be written as $x^{-1}z$ for some $z \in I$, which implies that $x^{-1}z \preccurlyeq_S 1$ (resp. $x^{-1}z \prec_S 1$). Using the multiplicative property of absolute values, we get $z \preccurlyeq_S x$ (resp. $z \prec_S x$). By the strongly (resp. weakly) S-minimality of $x \in I$, this implies that $z = 0$, and so $y = 0$. We see that $1 \in x^{-1}I$ is strongly (resp. weakly) S-minimal. □

Algorithm 5.4.20. (Reduction Algorithm for Arakelov S-Divisors)
Input: Any Arakelov S-divisor D of K.
Output: A strongly (resp. weakly) reduced Arakelov S-divisor D' such that D and D' lie on the same connected component of $\mathrm{Pic}_{K,S}$.

i.) Find $I \in \mathrm{Id}_{K,S}$ and $u \in \prod_{\sigma \in \Sigma_K^\infty} \mathbb{R}_{>0}$ such that $D = (I, u)_S$.

ii.) If $1 \in I$ is strongly (resp. weakly) S-minimal, then return $D' = \pi_S(I)$. Else find a strongly (resp. weakly) S-minimal element $x \in I$.

iii.) Return $D' = \pi_S(x^{-1}I)$.

The correctness of the algorithm is an immediate consequence of Lemma 5.4.19. Note that $x \in I$ in step (ii.) is not unique. Namely, there might exist more than one strongly (resp. weakly) S-minimal element in I. Therefore, the algorithm is not deterministic.

Remark 5.4.21. To finish this chapter, we would like to mention the paper titled 'Arakelovtheorie für Zahlkörper'. This German paper is written by Eduard Hübschke in 1987 (see [Hüb87]). As the German title suggests, this paper discusses Arakelov theory for number fields. It contains similar definitions and results as seen in Section 4.1. Besides this, it treats Arakelov theory for S-integers. Almost all results of Section 5.1 can be found in this paper. However, all results in this thesis have been proved independently. It has to be said that it deals Arakelov theory for S-integers in a more general matter. Namely, rather than considering S-integers over the ring of integers $\mathcal{O}_K$, it looks into the rings of S-integers of any order of K. Furthermore, it discusses Section 5.2.2 in a short manner. It shows how Theorem 5.2.18 only holds for the ring of integers (maximal order) and not for any arbitrary order. All other sections discussed in this thesis are not contained in this paper by Hübscke. ⧫

6 Fake Real Quadratic Orders

So far, we have built up Arakelov and Minkowski theory for the rings of S-integers of any number field. Now, we want to apply this theory to a specific type of S-integers in an imaginary quadratic number field: fake real quadratic orders. In particular, we want to give the Arakelov theoretical description of the infrastructure for fake real quadratic orders. In this chapter, we will introduce fake real quadratic orders. We investigate its structure and show some consequences of results that we have seen for the rings of S-integers. We end this chapter by discussing the potential of an Arakelov theoretical description of the infrastructure. Throughout this chapter, consider an imaginary quadratic number field $K = \mathbb{Q}(\sqrt{d})$ for some fundamental discriminant $d \in \mathbb{Z}_{<0}$. We use the convention about these types of number fields as described at the beginning of Section 1.3.

6.1 Structure

Let $q \in \mathbb{Z}$ be an odd prime number such that d is a square module q. Next, we want to investigate the integral ideal $q\mathcal{O}_K$. Recall that $\mathcal{O}_K = \mathbb{Z}[\omega]$, where $\omega = \frac{d+\sqrt{d}}{2}$. One can verify that ω is a root of the polynomial

$$f(t) = t^2 - dt + \frac{d^2 - d}{4}.$$

We know that d is a fundamental discriminant. So, by Definition 1.3.1, we know that $d \neq 1$ is square-free and $d \equiv 1 \bmod 4$, or $d = 4D$, where $D \in \mathbb{Z}$ is square-free and $D \equiv 2, 3 \bmod 4$. Hence, in all cases, we have that $4 | d^2 - d$. Consequently, the polynomial f is contained in $\mathbb{Z}[t]$. This lets us conclude that f is the minimal polynomial of ω. Since d is a square modulo p, there exists some $a \in \mathbb{Z}$ such that $a^2 \equiv d \bmod q$. So taking f modulo q gives rise to

$$\overline{f} = t^2 - dt + \frac{d^2 - a^2}{4} = \left(t + \frac{a-d}{2}\right)\left(t + \frac{-a-d}{2}\right).$$

If $q = 2$, we could not make this statement. That is why we restrict ourselves to odd primes. By the Dedekind-Kummer Theorem (see [Sut24, Theorem 6.14]), we obtain that

$$q\mathcal{O}_K = \left(q, \omega + \frac{a-d}{2}\right)\left(q, \omega + \frac{-a-d}{2}\right) = \left(q, \frac{a+\sqrt{d}}{2}\right)\left(q, \frac{a-\sqrt{d}}{2}\right)$$

is the unique factorization of $q\mathcal{O}_K$ in the non-zero prime ideals of $\mathcal{O}_K$. Set

$$\mathfrak{q} := \left(q, \frac{\sqrt{d}+a}{2}\right);$$

then we have shown that $q\mathcal{O}_K = \mathfrak{q}\overline{\mathfrak{q}}$. Set $S = \{\mathfrak{q}\}$ and $S' = \{\overline{\mathfrak{q}}\}$. We obtain the rings of S-integers $\mathcal{O}_{K,S}$ and $\mathcal{O}_{K,S'}$ of K. These rings are isomorphic by sending $a \in \mathcal{O}_{K,S}$ to its complex conjugate $\overline{a} \in \mathcal{O}_{K,S'}$. Therefore, up to isomorphism, it does not matter which prime ideal we take. Hence, the ring of S-integers obtained in this way is completely determined by the prime number $q \in \mathbb{Z}$.

Definition 6.1.1. Let $K = \mathbb{Q}(\sqrt{d})$ for some fundamental discriminant $d \in \mathbb{Z}_{<0}$. Let $q \in \mathbb{Z}$ be an odd prime such that d is a square module q. Take S to be the set only containing the unique, up to conjugation, non-zero prime ideal $\mathfrak{q}$ lying above q. Then the ring of S-integers $\mathcal{O}_{K,S}$, denoted by $\mathcal{O}_{d,q}$, is called a *fake real quadratic order* of K.

We denote a fake real quadratic order by $\mathcal{O}_{d,q}$, because, up to isomorphism, it is completely determined by the fundamental discriminant $d \in \mathbb{Z}_{<0}$ and an odd prime $q \in \mathbb{Z}$ such that d is a square module q.

We state some results regarding these fake real quadratic orders. Firstly, throughout this section let $n \in \mathbb{Z}_{\geq 0}$ denote the order of $\mathfrak{q}$ in Cl_K. Throughout this thesis, the integer n denoted the degree of the number field K.

But since K is fixed to be an imaginary quadratic field, there is no confusion. Using that $N_{\mathcal{O}_K}$ is a group homomorphism, Proposition 1.1.15 and 1.2.6 imply that

$$N_{\mathcal{O}_K}(\mathfrak{q})N_{\mathcal{O}_K}(\overline{\mathfrak{q}}) = N_{\mathcal{O}_K}(\mathfrak{q}\overline{\mathfrak{q}}) = N_{\mathcal{O}_K}(q\mathcal{O}_K) = |N_{K|\mathbb{Q}}(q)| = q^2 \quad \Longrightarrow \; N_{\mathcal{O}_K}(\mathfrak{q}) = N_{\mathcal{O}_K}(\overline{\mathfrak{q}}) = q.$$

The set of fractional ideals, set of principal fractional ideals, and class group of $\mathcal{O}_{d,q}$ will be denoted by $\mathrm{Id}_{d,q}, \mathrm{P}_{d,q}, \mathrm{Cl}_{d,q}$, respectively. From Proposition 3.2.3 it follows that

$$\mathrm{Id}_{d,q} \cong \mathrm{Id}_K / \langle \mathfrak{q} \rangle, \qquad \mathrm{Cl}_{d,q} \cong \mathrm{Cl}_K / \langle [\mathfrak{q}] \rangle.$$

Therefore, denoting by $h_{d,q}$ the order of $\mathrm{Cl}_{d,q}$, we $h_{d,q} = \frac{h_K}{n}$. A class number formula for fake real quadratic orders is given in Theorem 1.9 of [Oh14].

There is something to say about the structure and units of $\mathcal{O}_{d,q}$. According to Proposition 3.1.4, we can write $\mathcal{O}_{d,q} = \mathcal{O}_K\left[a^{-1}\right]$, for some $a \in \mathcal{O}_K \backslash \{0\}$. Explicitly, this element a satisfies $\mathrm{ord}_{\mathfrak{q}}(a) > 0$ and $\mathrm{ord}_{\mathfrak{p}}(a) = 0$ for all $\mathfrak{p} \neq \mathfrak{q}$. This means that a must be a generator of the principal integral ideal $\mathfrak{q}^n$. Any such generator is unique up to units of $\mathcal{O}_K^*$. We have seen in Equation (5) that $\mathcal{O}_K$ has only finitely many units. Let us denote a generator by ε_q, and keep in mind that it is unique up to units of $\mathcal{O}_K$. We obtain that $\mathcal{O}_{d,q} = \mathcal{O}_K\left[\varepsilon_q^{-1}\right]$. Since $\varepsilon_q \in \mathfrak{q}^n \subseteq \mathcal{O}_K \subseteq \mathcal{O}_{d,q}$, and $\varepsilon_q^{-1} \in \mathcal{O}_{d,q}$, we get that $\varepsilon_q \in \mathcal{O}_{d,q}^*$. More generally, we have $\varepsilon_q^k \in \mathcal{O}_{d,q}^*$ for all $k \in \mathbb{Z}$. On top of this, we know by Proposition 3.2.7 that

$$\mathcal{O}_{d,q}^* = \mu_K \times \langle \varepsilon \rangle,$$

for some unit $\varepsilon \in \mathcal{O}_{d,q}^*$. Note that in our case of an imaginary quadratic number field, we have $\mu_K = \mathcal{O}_K^*$. If $\varepsilon_q = \varepsilon^k$ for some integer $k \neq \pm 1$, then the prime ideal $\mathfrak{q}$ would have a smaller order than n. Hence, we actually have $\varepsilon_q = \varepsilon^{\pm 1}$. We get that

$$\mathcal{O}_{d,q}^* = \mathcal{O}_K^* \times \langle \varepsilon_q \rangle.$$

So a generator of the unit group $\mathcal{O}_{K,S}^*$ is equivalent to a generator of $\mathfrak{q}^n$.

Note that we only have one infinite place of K. This corresponds to a pair of conjugate complex field embeddings. Therefore, the only Archimedean absolute value on K is the absolute value $|.|_\infty$ on $\mathbb{C}$. Since $\mathcal{O}_K^* = \mu_K$, we have by Proposition 1.5.4 that $|a|_\infty = 1$ for all $a \in \mathcal{O}_K^*$. As stated before, the element ε_q is unique up to units of $\mathcal{O}_K^*$. So the value $|\varepsilon_q|_\infty$ is independent of the choice of generator of $\mathfrak{q}^n$. Hence, the following definition is well-defined.

Definition 6.1.2. The value $\log|\varepsilon_q|_\infty$ is called the *regulator* of $\mathcal{O}_{d,q}$ and is denoted by $R_{d,q}$.

The regulator of a fake real quadratic order can be seen as an analogue of the regulator of a real quadratic number field. Namely, in that case, the regulator is defined by the logarithm of the absolute value of the fundamental unit (see Section 1.3). In Section 4.3, we designed Algorithm 4.3.43 that could compute the regulator of a real quadratic number field using the Arakelov infrastructure. So we wish to extend this to the regulator of a fake real quadratic order. We will discuss the possibilities in the next section. We keep all the notation and terminology introduced in the present section.

Remark 6.1.3. Wang has designed an infrastructure for fake real quadratic orders using the ideas of Section 1.3, rather than the ideas of the Arakelov theoretical description (see [Wan17, Section 3.4]). Firstly, she gives an analogue of the principle cycle as seen in Definition 1.3.10. Thereafter, she describes a distance function that can be used, along the principle cycle, to compute $n \in \mathbb{Z}_{\geq 0}$ (the order of $\mathfrak{q}$ in Cl_K), rather than $\log|\varepsilon_q|_\infty$. However, Wang states that the designed Baby-Step Giant-Step infrastructure algorithm does not lead to any faster way to determine n (or ε_q), than just computing the order of $\mathfrak{q}$ and a generator of $\mathfrak{q}^n$ directly. ♦

6.2 Arakelov Theoretical Description of the Infrastructure: A Discussion

The first step is to develop Arakelov theory for fake real quadratic orders. But this has already been done in Chapter 5 for the rings of S-integers. So we can use those constructions. Arakelov S-divisors will be called Arakelov q-divisors. The group of Arakelov q-divisors and the subgroup of principal Arakelov q-divisors is denoted by $\mathrm{Div}_{d,q}, \mathrm{Prin}_{d,q}$, respectively. An Arakelov q-divisor D in multiplicative notation will be given by $D = (I, u)_q$ for some $I \in \mathrm{Id}_{d,q}$ and $u \in \mathbb{R}_{>0}$. The Arakelov S-class group is called the Arakelov q-class group and is denoted by $\mathrm{Pic}_{d,q}$. Concerning Section 5.4, the strongly (resp. weakly) S-minimal elements of a fractional ideal will be called strongly (resp. weakly) q-minimal. The set of strongly reduced (resp. weakly reduced) Arakelov q-divisors is denoted by $\mathrm{Red}^s_{d,q}$ (resp. $\mathrm{Red}^w_{d,q}$). Lastly, the group homomorphism π_S is denoted by π_q.

Now that we have Arakelov theory for fake real quadratic orders, we can directly dive into the analogue of Section 4.3. In this section, we will discuss the possibilities of this extension. But we also explain the obstacles.

We have a reduction algorithm for Arakelov q-divisors as described in Algorithm 5.4.20. This algorithm is similar to Algorithm 4.2.7. The first step in Section 4.3.1 was to develop a better reduction algorithm. From this, we got Algorithm 4.3.8. Therefore, the first task would be to find a similar algorithm for fake real quadratic orders. The algorithm heavily relies on the representation of fractional ideals as seen in Proposition 4.3.2. We used the fact that any fractional ideal of the ring of integers in a real quadratic number field is a free $\mathbb{Z}$-module of rank 2. We do not have such a statement for fractional ideals of $\mathcal{O}_{d,q}$. In particular, a fake real quadratic order $\mathcal{O}_{d,q}$ is not even a free $\mathbb{Z}$-module. However, we will now prove that any fractional ideal of $\mathcal{O}_{d,q}$ is a free $\mathbb{Z}\left[\varepsilon_q^{-1}\right]$-module of rank 2.

Take any $I \in \mathrm{Id}_{d,q}$. We denote by I_q the fractional ideal of $\mathcal{O}_K$ corresponding to I as described in Definition 3.2.4.

Lemma 6.2.1. For each $I \in \mathrm{Id}_{d,q}$, one has $I = I_q\left[\varepsilon_q^{-1}\right]$. Consequently, any $x \in I$ can be written as $a\varepsilon_q^k$ for some $k \in \mathbb{Z}_{<0}$ and $a \in I_q$.

Proof. We know that $I = I_q\mathcal{O}_{d,q}$. So any element $x \in I$ can be written as $x = \sum_{i=0}^{k} a_i b_i$ with $a_i \in I_q$ and $b_i \in \mathcal{O}_{d,q}$ for all $0 \le i \le k$, and some $k \in \mathbb{Z}_{\ge 0}$. In its turn, since $\mathcal{O}_{d,q} = \mathcal{O}_K\left[\varepsilon_q^{-1}\right]$, the b_i's can be written as

$$b_i = \sum_{j=0}^{l} \frac{b_{ij}}{\varepsilon_q^j}$$

for some $b_{ij} \in \mathcal{O}_K$ for all $0 \le j \le l$, and some $l \in \mathbb{Z}_{\ge 0}$. Combining these expressions, we obtain

$$x = \sum_{i=0}^{k} a_i b_i = \sum_{i=0}^{k} a_i \left(\sum_{j=0}^{l} \frac{b_{ij}}{\varepsilon_q^j} \right).$$

Since $a_i \in I_q$ and $b_{ij} \in \mathcal{O}_K$, we know that $a_i b_{ij} \in I_q$ for all i, j. Consequently, we can write

$$x = \sum_{i=0}^{m} \frac{c_i}{\varepsilon_q^i},$$

for some $c_i \in I_q$ for all $0 \le i \le m$, and some $m \in \mathbb{Z}_{\ge 0}$. Then

$$x = \frac{1}{\varepsilon_q^m} \sum_{i=0}^{m} c_i \varepsilon_q^{m-i}.$$

Since $c_i \in I_q$ and $\varepsilon_q^k \in \mathcal{O}_K$ for all $k \in \mathbb{Z}_{\geq 0}$, we know that $c_i \varepsilon_q^{m-i} \in I_q$ for all $0 \leq i \leq m$. Moreover, the element $c := \sum_{i=0}^{m} c_i \varepsilon_q^{m-i}$ is contained in I_q. Consequently, we see that $x = c\varepsilon_q^{-m}$, and so $x \in I_q\left[\varepsilon_q^{-1}\right]$. So we have $I \subseteq I_q\left[\varepsilon_q^{-1}\right]$. Conversely, since $I_q \subseteq I$ and $\varepsilon_q^{-1} \in \mathcal{O}_{d,q}$, we also have $I_q\left[\varepsilon_q^{-1}\right] \subseteq I\mathcal{O}_{d,q} \subseteq I$. So we see that $I = I_q\left[\varepsilon_q^{-1}\right]$. □

Lemma 6.2.2. Let R be a domain and M an R-module. Then $R[t] \otimes_R M \cong M[t]$.

Proof. The isomorphism is given by extending the map $f(t) \otimes m \mapsto mf(t)$ linearly over R. □

Proposition 6.2.3. Let $I \in \mathrm{Id}_{d,q}$. Then I is a free $\mathbb{Z}\left[\varepsilon_q^{-1}\right]$-module of rank 2.

Proof. We have seen that the fractional ideal I_q of $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank 2. The ring $\mathbb{Z}\left[\varepsilon_q^{-1}\right]$ can be viewed as a $\mathbb{Z}$-module. It follows from Proposition 1.8.1 that $\mathbb{Z}\left[\varepsilon_q^{-1}\right] \otimes_{\mathbb{Z}} I_q$ is a free $\mathbb{Z}\left[\varepsilon_q^{-1}\right]$-module of rank 2. Lemma 6.2.2 implies that $\mathbb{Z}\left[\varepsilon_q^{-1}\right] \otimes_{\mathbb{Z}} I_q \cong I_q\left[\varepsilon_q^{-1}\right]$. By Lemma 6.2.1, we know that $I_q\left[\varepsilon_q^{-1}\right] = I$. We conclude that I is a free $\mathbb{Z}\left[\varepsilon_q^{-1}\right]$-module of rank 2. □

From this result we conclude that for any $I \in \mathrm{Id}_{d,q}$ there exist $x, y \in I$ such that

$$I = x\mathbb{Z}\left[\varepsilon_q^{-1}\right] + y\mathbb{Z}\left[\varepsilon_q^{-1}\right].$$

Recall the definition of a primitive element from Definition 1.1.2.

Lemma 6.2.4. Let $I \in \mathrm{Id}_{d,q}$.

i.) An element $x \in I$ is primitive if and only if it is part of a $\mathbb{Z}\left[\varepsilon_q^{-1}\right]$-basis.

ii.) The fractional ideal I contains a primitive element.

iii.) If $x \in I$ is primitive, then 1 is primitive in $x^{-1}I$.

Proof. To show Statement (i.), let $x \in I$ be part of a $\mathbb{Z}\left[\varepsilon_q^{-1}\right]$-basis of I. Say this $\mathbb{Z}\left[\varepsilon_q^{-1}\right]$-basis is given by the elements $x, y \in I$. Suppose that there exists some $m \in \mathbb{Z}_{>1}$ such that $x \in mI$. Then $\frac{x}{m} \in I$. Since $I = x\mathbb{Z}\left[\varepsilon_q^{-1}\right] + y\mathbb{Z}\left[\varepsilon_q^{-1}\right]$, there exist $f, g \in \mathbb{Z}\left[\varepsilon_q^{-1}\right]$ such that $\frac{x}{m} = fx + gy$. We know that x, y form a basis of I, so we can compare coefficients, i.e. $f = \frac{1}{m}$. As m is an integer, the element f must be rational. Consequently, we get that $f \in \mathbb{Z}\left[\varepsilon_q^{-1}\right] \cap \mathbb{Q}$. Since ε_q is not an integer, and is contained in $\mathcal{O}_K$, it must be irrational. We conclude that $\mathbb{Z}\left[\varepsilon_q^{-1}\right] \cap \mathbb{Q} = \mathbb{Z}$. So we have $f, m \in \mathbb{Z}$ such that $f = \frac{1}{m}$. Therefore, we must have $m = \pm 1$, reaching a contradiction with the choice of m. Thus, the element x is primitive in I.

Conversely, let $x \in I$ be primitive. Since I is a free $\mathbb{Z}\left[\varepsilon_q^{-1}\right]$-module of rank 2, there exist $y, z \in I$ such that $I = y\mathbb{Z}\left[\varepsilon_q^{-1}\right] + z\mathbb{Z}\left[\varepsilon_q^{-1}\right]$. Hence, there exist $f, g \in \mathbb{Z}\left[\varepsilon_q^{-1}\right]$ such that $x = fy + gz$. With a similar argument as in the proof of Lemma 6.2.1 (replacing $\mathcal{O}_K$ by $\mathbb{Z}$), we find that there exist $a, b \in \mathbb{Z}$ and $k, l \in \mathbb{Z}_{<0}$ such that $f = a\varepsilon_q^k$ and $g = b\varepsilon_q^l$. If $\gcd(a, b) > 1$, then there exist $c \in \mathbb{Z}_{>1}$ and $d, e \in \mathbb{Z}$ such that $x = c(d\varepsilon_q^k y + e\varepsilon_q^l z)$. Then $x \in cI$, contradicting the assumption that x is primitive. We conclude that $\gcd(a, b) = 1$. By Bezout's Identity, this means that there exist $i, j \in \mathbb{Z}$ such that $ai + bj = 1$. Consequently, one can verify that x and $-j\varepsilon_q^{-l} y + i\varepsilon_q^{-k} z$ are linearly independent and generate I. Consequently, they form a $\mathbb{Z}\left[\varepsilon_q^{-1}\right]$-basis for I. Thus, the element $x \in I$ is part of a $\mathbb{Z}\left[\varepsilon_q^{-1}\right]$-basis.

Statement (ii.) follows from Statement (i.) since a $\mathbb{Z}\left[\varepsilon_q^{-1}\right]$-basis can always be found for I.

To show Statement (iii.), let $x \in I$ be primitive. Then by Statement (i.), we have that x is part of a $\mathbb{Z}\left[\varepsilon_q^{-1}\right]$-basis. Let this $\mathbb{Z}\left[\varepsilon_q^{-1}\right]$-basis be given by $x, y \in I$. Then

$$I = x\mathbb{Z}\left[\varepsilon_q^{-1}\right] + y\mathbb{Z}\left[\varepsilon_q^{-1}\right] \quad \Longrightarrow x^{-1}I = x^{-1}\left(x\mathbb{Z}\left[\varepsilon_q^{-1}\right] + y\mathbb{Z}\left[\varepsilon_q^{-1}\right]\right) = \mathbb{Z}\left[\varepsilon_q^{-1}\right] + x^{-1}y\mathbb{Z}\left[\varepsilon_q^{-1}\right].$$

We obtain that 1 is part of a $\mathbb{Z}\left[\varepsilon_q^{-1}\right]$-basis of $x^{-1}I$. So by Statement (i.), we have that $1 \in x^{-1}I$ is primitive. □

Note that this lemma is an extension of Lemma 4.3.1. Only Statement (iv.) of Lemma 4.3.1 is excluded, but we will return back to this. After Lemma 4.3.1, we saw the representation of fractional ideals in Proposition 4.3.2. Using this representation, we uniquely determined element the $x_{(I,1)}$, if 1 was primitive in a fractional ideal. This element was crucial in Algorithm 4.3.8. The analogue of this algorithm for fake real quadratic orders is conjectured as follows.

Conjecture 6.2.5. Let $I \in \mathrm{Id}_{d,q}$ such that $1 \in I$ is primitive and $D \in \mathrm{Div}_{d,q}$. Then there exists a unique choice $x_{(I)} \in I$ such that $1, x_{(I)}$ form a $\mathbb{Z}\left[\varepsilon_q^{-1}\right]$-basis of I. Moreover, this choice makes the following steps return a strongly (resp. weakly) reduced Arakelov q-divisor D', such that D and D' lie on the same connected component of $\mathrm{Pic}_{d,q}$.

i.) Find $I \in \mathrm{Id}_{d,q}$ and $u \in \mathbb{R}_{>0}$ such that $D = (I, u)_q$.

ii.) Find a primitive element $\alpha \in I$.

iii.) If $\alpha = 1$, set $I' := I$. Else, set $I' := \alpha^{-1} I$.

iv.) If $1 \in I'$ is strongly (resp. weakly) q-minimal, then return $D' = \pi_q(I')$. Else, set $I_0 := I'$.

v.) Set $i = 0$.

vi.) Set $i = i + 1$ and compute $I_i = x_{(I_{i-1})}^{-1} I_{i-1}$.

vii.) If $1 \in I_i$ is strongly (resp. weakly) q-minimal, then return $D' = \pi_q(I_i)$. Else, return to step (vi.).

Moreover, the steps terminate in a finite number of steps.

We have studied this conjecture as part of this thesis but failed to verify it. The first step is to study the representations for fractional ideals of $\mathcal{O}_{d,q}$ as $\mathbb{Z}\left[\varepsilon_q^{-1}\right]$-module. Because then one could make choices for $x_{(I)}$. One of the ideas was to relate it to the representation from Proposition 4.3.2. Namely, we have the following result.

Lemma 6.2.6. Let $I \in \mathrm{Id}_{K,S}$ and $x \in I_q$. Then the following statements are equivalent.

i.) The element x is primitive in I_q.

ii.) The element x is part of a $\mathbb{Z}$-basis of I_q.

iii.) The element x is part of a $\mathbb{Z}\left[\varepsilon_q^{-1}\right]$-basis of I.

iv.) The element x is primitive in I.

Proof. Statement (i.) implies Statement (ii.). This follows from Lemma 4.3.1 (i.).

Suppose that x is part of a $\mathbb{Z}$-basis of I_q. Let this $\mathbb{Z}$-basis be given by $x, y \in I_q$. Take any $z \in I$. By Lemma 6.2.1, there exist $a \in I_q$ and $m \in \mathbb{Z}_{<0}$ such that $z = a\varepsilon_q^m$. Since $a \in I_q$, there exist $k, l \in \mathbb{Z}$ such that $a = kx + ly$. Then $z = a\varepsilon_q^m = (kx + ly)\varepsilon_q^m = (k\varepsilon_q^m)x + (l\varepsilon_q^m)y$. Since $k\varepsilon_q^m, l\varepsilon_q^m \in \mathbb{Z}\left[\varepsilon_q^{-1}\right]$, we have that x, y generate the $\mathbb{Z}\left[\varepsilon_q^{-1}\right]$-module I. Since I has rank 2 as a $\mathbb{Z}\left[\varepsilon_q^{-1}\right]$-module, the element x, y must form a $\mathbb{Z}\left[\varepsilon_q^{-1}\right]$-basis of I. This shows that Statement (ii.) implies Statement (iii.).

Statement (iii.) implies Statement (iv.). This follows from Lemma 6.2.4 (i.).

Let x be primitive in I. Assume there exists $m \in \mathbb{Z}_{>1}$ such that $x \in mI_q$. We know $I_q \subseteq I$, so $mI_q \subseteq mI$. Therefore, we have $x \in mI$. This contradicts the fact that x is primitive in I. Hence, the element x is also primitive in I_q. This shows that Statement (iv.) implies Statement (i.). □

This result gives us a way to find a $\mathbb{Z}\left[\varepsilon_q^{-1}\right]$-basis for any fractional ideal of $\mathcal{O}_{d,q}$. To see this, take any $I \in \mathrm{Id}_{d,q}$. Proposition 4.3.2 tells us that

$$I_q = \alpha\left(\mathbb{Z} + \left(\frac{b+\sqrt{d}}{2a}\right)\mathbb{Z}\right),$$

where $\alpha \in K^*$, $a, b \in \mathbb{Z}$ with $c = \frac{b^2-d}{4a} \in \mathbb{Z}$ are such that $\gcd(a,b,c) = 1$, and $N_{K|\mathbb{Q}}(\alpha)/a \in \mathbb{Z}_{>0}$ which equals $N_{\mathcal{O}_K}(I)$. By Lemma 6.2.6, it follows that

$$I = \alpha\left(\mathbb{Z}\left[\varepsilon_q^{-1}\right] + \left(\frac{b+\sqrt{d}}{2a}\right)\mathbb{Z}\left[\varepsilon_q^{-1}\right]\right).$$

Now, we attempted to set $\alpha = 1$ and make unique choices for a, b to get a unique choice for $x_{(I)}$. With these choices, we have tried to verify Conjecture 6.2.5. But no choices have proven this conjecture.

We leave this problem and look into the next steps of the Arakelov theoretical description of the infrastructure. In Section 4.3.2, we defined the infrastructure operator and obtained the Arakelov cycles. Let us see what we can do here. Let $\mathrm{Red}^1_{d,q} \subseteq \mathrm{Div}_{d,q}$ denote all Arakelov q-divisors of the form $\pi_q(I)$, where $I \in \mathrm{Id}_{d,q}$ such that $1 \in I$ is primitive. Then the analogue of the infrastructure operator from Definition 4.3.12 would be given as follows. Consider the operator $\rho_q \colon \mathrm{Red}^1_{d,q} \to \mathrm{Red}^1_{d,q}$ defined by $\pi_q(I) \mapsto \pi_q\left(x_{(I)}^{-1} I\right)$, where $x_{(I)}$ is the element from Conjecture 6.2.5. One of the key points of Section 4.3.2 is that we could apply the infrastructure operator to the set of reduced Arakelov divisors. Namely, in Lemma 4.3.1 (iv.), we saw that a minimal element is also primitive. This is not the case in our setting for fake real quadratic orders. Let us explain this.

Let $I \in \mathrm{Id}_{d,q}$. Suppose that $x \in I$ is strongly q-minimal. Assume that there exists $m \in \mathbb{Z}_{>1}$ such that $x \in mI$. Then $\frac{x}{m} \in I$ is non-zero, and we have that $\left|\frac{x}{m}\right|_\infty < |x|_\infty$. So if we have that

$$\left|\frac{x}{m}\right|_{\mathfrak{q}} \leq |x|_{\mathfrak{q}}, \tag{97}$$

we would get a contradiction with the fact that x is strongly q-minimal. Hence, we could conclude that x must be primitive. But inequality (97) fails if $|m|_{\mathfrak{q}} < 1$. Equivalently, if $\mathrm{ord}_{\mathfrak{q}}(m) > 0$. This condition is true for all integers that have q in its factorization. Consequently, there are certain integers m for which inequality (97) fails. Since we have to take $m \in \mathbb{Z}_{>1}$ arbitrarily, we cannot control this. It would not even be true if x were 1. The same problem applies if we assume that $x \in I$ is weakly q-minimal.

Hence, neither $\mathrm{Red}^s_{d,q} \subseteq \mathrm{Red}^1_{d,q}$ nor $\mathrm{Red}^w_{d,q} \subseteq \mathrm{Red}^1_{d,q}$ can be verified. Therefore, we cannot apply ρ_q to the sets $\mathrm{Red}^s_{d,q}, \mathrm{Red}^w_{d,q}$. Consequently, we cannot translate Proposition 4.3.13 to the fake real quadratic order setting. However, this proposition allowed us to show that the infrastructure operator is a bijection on the set of reduced Arakelov divisors (see Proposition 4.3.15). Moreover, we could examine Theorem 4.3.18, which led to the definition of Arakelov cycles (see Definition 4.3.19). There have been no solutions to overcome this problem. It also heavily relies on the previous problem of finding $x_{(I)}$. Maybe one can come up with an operator that has the same properties as the infrastructure operator from Definition 4.3.12, but does not depend on $x_{(I)}$.

Looking at Section 4.3.3 and 4.3.4, there is not much to say for fake real quadratic orders if the above problems do not get solved. The only thing we can say for now is that we have a short exact sequence given by

$$0 \longrightarrow T_{d,q} \longrightarrow \mathrm{Pic}_{d,q} \longrightarrow \mathrm{Cl}_{d,q} \longrightarrow 0\ ,$$

where

$$T_{d,q} := \mathbb{R}/\{\log(\hat{a}) : a \in \mathcal{O}_{d,q}^*\}.$$

This is taken from the last row of the commutative diagram of Theorem 5.1.16. Since $\mathcal{O}_{d,q}^* = \mathcal{O}_K^* \times \langle \varepsilon_q \rangle$, we obtain that

$$T_{d,q} = \mathbb{R}/\{\log|\varepsilon_q^k| : k \in \mathbb{Z}\} \cong \mathbb{R}/\log|\varepsilon_q|\mathbb{Z} = \mathbb{R}/R_{d,q}\mathbb{Z},$$

using Definition 6.1.2. There is a possibility that $T_{d,q}$ could be used to define the distance between Arakelov q-divisors that lie on the same connected components of $\mathrm{Pic}_{d,q}$. Similar to the distance defined in Section 4.3.3.

In conclusion, there are several problems to overcome before an Arakelov theoretical description of the infrastructure for fake real quadratic orders can be given. The most important step would be to solve Conjecture 6.2.5. However, there is hope that with the ingredients described in this thesis, future progress can be made.

References

[ADGB22] Lydia Außenhofer, Dikran Dikranjan, and Anna Giordano Bruno. *Topological Groups and the Pontryagin-van Kampen duality: An Introduction*, volume 83 of *De Gruyter Studies in Mathematics*. De Gruyter, Berlin, 2022.

[AK21] Allen B. Altman and Steven L. Kleiman. *A Term of Commutative Algebra*. Worldwide Center of Mathematics, LLC, 2013 (Version 2021).

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley Publishing Company, 1969.

[Bog07] V. I. Bogachev. *Measure Theory.*, volume I. Springer-Verlag, Berlin, 2007.

[Buc90] Johannes Buchmann. A subexponential algorithm for the determination of class groups and regulators of algebraic number fields. In *Séminaire de Théorie des Nombres, Paris 1988–1989*, volume 91 of *Progr. Math.*, pages 27–41. Birkhäuser Boston, 1990.

[Cas86] J. W. S. Cassels. *Local Fields*, volume 3 of *London Mathematical Society Student Texts*. Cambridge University Press, 1986.

[CF67] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic Number Theory*. Academic Press INC. (London) LTD.; Thompson Book Company Inc., 1967.

[Coh93] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics, 138. Springer-Verlag, Berlin, 1993.

[Coh13] Donald L. Cohn. *Measure Theory*. Birkhäuser Advanced Texts Basler Lehrbücher. Springer, New York, second edition, 2013.

[Con24a] Brian Conrad. A Compactness Theorem for the Idele Group. Lecture Notes, Math 248a: Algebraic Number Theory. `https://virtualmath1.stanford.edu/~conrad/248APage/handouts/compactidele.pdf`, 2024. Accessed 11 October 2024.

[Con24b] Brian Conrad. The Lattice of S-Integers. Lecture Notes, Math 248a: Algebraic Number Theory. `https://virtualmath1.stanford.edu/~conrad/248APage/handouts/Sintlattice.pdf`, 2024. Accessed 15 January 2024.

[Con24c] Keith Conrad. Ostrowski for Number Fields. Expository papers: Algebraic number theory. `https://kconrad.math.uconn.edu/blurbs/gradnumthy/ostrowskinumbfield.pdf`, 2024. Accessed 29 January 2024.

[Con24d] Keith Conrad. Tensor Products II. Expository papers: Linear/Multilinear algebra. `https://kconrad.math.uconn.edu/blurbs/linmultialg/tensorprod2.pdf`, 2024. Accessed 14 October 2024.

[CR15] G.A. Chicas Reyes. Structure Theorems for Projective Modules. Master's thesis, University of Bordeaux, 2015.

[DB22] Koen De Boer. *Random Walks on Arakelov Class Groups*. PhD thesis, Leiden University, 2022.

[Eve11] Jan-Hendrik Evertse. P-Adic Numbers. Lecture Notes. `https://www.math.leidenuniv.nl/~evertsejh/dio2011-padic.pdf`, 2011. Accessed 11 November 2024.

[Hüb87] Eduard Hübschke. *Arakelovtheorie für Zahlkörper*. Fakultät für Mathematik der Universität Regensburg, 1987.

[JW09] Michael J. Jacobson, Jr. and Hugh C. Williams. *Solving the Pell Equation*. Canadian Mathematical Society. Springer, New York, 2009.

[Kap58] Irving Kaplansky. Projective modules. *Ann. of Math. (2)*, 68:372–377, 1958.

[Kha22] Sudesh Kaur Khanduja. *A Textbook of Algebraic Number Theory*, volume 135 of *UNITEXT - La Matematica per il 3+2*. Springer, Singapore, 2022.

[Lag80] J. C. Lagarias. Worst-case complexity bounds for algorithms in the theory of integral quadratic forms. *Journal of Algorithms*, 1:142–186, 1980.

[Len82] H. W. Lenstra, Jr. On the calculation of regulators and class numbers of quadratic fields. In *Number theory days, 1980 (Exeter, 1980)*, volume 56 of *London Math. Soc. Lecture Note Ser.*, pages 123–150. Cambridge Univ. Press, Cambridge, 1982.

[Mor15] Dave Witte Morris. *Introduction to Arithmetic Groups*. Deductive Press, 2015.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Oh14] Richard Michael Oh. *Fake Real Quadratic Orders*. ProQuest LLC, Ann Arbor, MI, 2014. Thesis (Ph.D.)–University of South Carolina.

[Rag72] M. S. Raghunathan. *Discrete Subgroups of Lie Groups*, volume 68 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag, Berlin, 1972.

[RV70] Clive M. Reis and T. M. Viswanathan. A compactness property for prime ideals in Noetherian rings. *Proc. Amer. Math. Soc.*, 25:353–356, 1970.

[Sch08] René Schoof. Computing Arakelov class groups. In *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*, volume 44 of *Mathematical Sciences Research Ibnstitute Publications*, pages 447–495. Cambridge Univ. Press, Cambridge, 2008.

[Sha72] Daniel Shanks. The infrastructure of a real quadratic field and its applications. In *Proceedings of the 1972 Number Theory Conference (Univ. Colorado, Boulder, Colo.)*, pages 217–224. University of Colorado, 1972.

[Sin19] Tej Bahadur Singh. *Introduction to Topology*. Springer, Singapore, 2019.

[Sut09] Wilson A. Sutherland. *Introduction to Metric and Topological Spaces*. Oxford University Press, Oxford, second edition, 2009. Companion web site: www.oup.com/uk/companion/metric.

[Sut24] Andrew V. Sutherland. Ideal norms and the Dedekind-Kummer theorem. lecture notes, 18.785 - number theory i. `https://math.mit.edu/classes/18.785/2021fa/LectureNotes6.pdf`, 2024. Accessed 8 October 2024.

[Vas69] Wolmer V. Vasconcelos. On projective modules of finite rank. *Proc. Amer. Math. Soc.*, 22:430–433, 1969.

[Wan17] Hongyan Wang. Numerical Tests of Two Conjectures in Fake Real Quadratic Orders. Master's thesis, University of Calgary, 2017.

[Wei13] Charles A. Weibel. *The K-Book*, volume 145 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2013. An introduction to algebraic K-theory.

[Xia16] Zhang Xianke. *Algebraic Number Theory*. Alpha Science International, second edition, 2016.