On the Picard group of real quadratic number fields

by

Begüm Gülşah Çaktı

A Dissertation Submitted to the
Graduate School of Sciences and Engineering
in Partial Fulfillment of the Requirements for
the Degree of

Master of Science

in

Mathematics

KOÇ ÜNİVERSİTESİ

August, 2020

On the Picard group of real quadratic number fields

Koç University

Graduate School of Sciences and Engineering

This is to certify that I have examined this copy of a master's thesis by

Begüm Gülşah Çaktı

and have found that it is complete and satisfactory in all respects,
and that any and all revisions required by the final
examining committee have been made.

Committee Members:

_____

Prof. Dr. Sinan Ünver (Advisor)

_____

Assoc. Prof. Ayberk Zeytin [Co-Advisor]

_____

Prof. Dr. Mine Çağlar

_____

Prof. Dr. Burak Özbağcı

_____

Assist. Prof. Altan Erdoğan

Date: _____

"Nullum vero dubium nobis esse videtur,
quin multa eaque egregia in hoc genere adhuc lateant
in quibus alii vires suas exercere possint."
Carl F. Gauss

ABSTRACT

On the Picard group of real quadratic number fields
Begüm Gülşah Çaktı
Master of Science in Mathematics
August, 2020

Computing the class group of a number field has always been one of the main problems of number theory. For this purpose, several algorithms have been introduced so far, and it turns out that some of the computations underlying these algorithms can be viewed as ones within the Arakelov class group (or Picard group) of the number field in question. In this thesis, we first construct the oriented Arakelov class group of a number field K, $\widetilde{\mathrm{Pic}}^0(K)$, that is analogous to the Picard group of an algebraic curve using basic notions attached to an oriented Arakelov divisor, e.g. degree, pairs consisting of fractional K-ideals and units in $K \otimes_{\mathbb{Q}} \mathbb{R}$. We then observe that $\widetilde{\mathrm{Pic}}^0(K)$ is an extension of the narrow ideal class group of K, which will be denoted by $\mathrm{Cl}^+(K)$, by a real Lie group. Afterwards, we focus on primitive integral indefinite binary quadratic forms of fixed discriminant and define an action of $\mathrm{GL}_2(\mathbb{Z})$ on the set consisting of these forms. We will notice that the integrality, primitivity, and discriminant are invariants of this action. To combine these two main notions, we restrict our attention to real quadratic number fields. We show that there is a natural bijection between $\mathrm{Cl}^+(K)$ and the set of equivalence classes of integral binary quadratic forms with fixed discriminant when K is a real quadratic field and then express $\widetilde{\mathrm{Pic}}^0(K)$ in the language of indefinite binary quadratic forms.

ÖZETÇE

Reel kuadratik sayı cisimlerinin Picard grubu hakkında
Begüm Gülşah Çaktı
Matematik, Yüksek Lisans
Ağustos 2020

Bir sayı cisminin sınıf sayısını hesaplamak her zaman sayılar kuramının başlıca problemlerinden biri olmuştur. Bu amaç doğrultusunda şu ana kadar birçok algoritma ortaya atılmıştır ve bu algoritmaların temelini oluşturan hesapların bir Arakelov sınıf grubu (veya Picard grubu) içerisinde görülebileceği fark edilmiştir. Bu tezde ilk olarak, bir cebirsel eğrinin Picard grubuna analog olan, K sayı cisminin yönlü Arakelov sınıf grubunu inşa edeceğiz ve bunu $\widetilde{\mathrm{Pic}}^0(K)$ ile göstereceğiz. Bu inşa için öncelikle K sayı cisminin yönlü Arakelov bölenlerini ve bu bölenlerin dereceleri ile bölenlere karşılık gelen ikilileri tanıtacağız. Sonrasında, $\widetilde{\mathrm{Pic}}^0(K)$ grubunun K cisminin dar sınıf grubunun, $\mathrm{Cl}^+(K)$, reel bir Lie grubuyla genişlemesi olduğunu gözlemleyeceğiz. Ardından, diskriminantı sabit tutarak katsayıları tamsayı olan primitif belirsiz ikili kuadratik formlara odaklanacağız ve $\mathrm{GL}_2(\mathbb{Z})$ grubunun bu formlara etkisini tanımlayacağız. Tamsayı katsayılı, primitif olmanın ve diskriminantın bu etki altında değişmediğini fark edeceğiz. Bu iki temel konsepti bağlantılamak için, dikkatimizi son olarak reel kuadratik sayı cisimlerine vereceğiz. K sayı cismi reel kuadratik olduğunda $\mathrm{Cl}^+(K)$ ve tamsayı katsayılı kuadratik formların denklik sınıflarından oluşan küme arasında birebir ve örten bir ilişki kuracağız ve $\widetilde{\mathrm{Pic}}^0(K)$ grubunu belirsiz ikili kuadratik formların dilinde ifade edeceğiz.

ACKNOWLEDGMENTS

First, I would like to express my gratitude to my advisor Ayberk Zeytin. This thesis would not have been possible without his support, encouragement, and constant patience. I owe him a lot for sharing his immense knowledge with me since I was a freshman at Galatasaray University.

I sincerely thank my official advisor Sinan Ünver for the opportunity to continue my research under the roof of Koç University. I also thank Mine Çağlar, Altan Erdoğan and Burak Özbağcı for their participation in my defense jury.

I am truly thankful to Serge Randriambololona, for his enthusiasm and patience in teaching mathematics. He is one of the cornerstones of my journey in mathematics, together with Ayberk Zeytin.

I am grateful to Ebru Nayir for her constant support and always being there for me whenever I needed it.

Moreover, I would like to thank my colleagues from Koç University: Berkay, Cem, Çağatay, Doğa Can, Elif, Ella, Fatih, Fırtına, İhsan, Murad, Murat Can, Oğuz, Ruhat, Serap, and Yasin for both fruitful mathematical discussions and all the fun that we had during our studies. Among them, I especially thank İhsan and Ruhat. I feel extremely lucky to be surrounded by true friends.

I am deeply grateful to my parents Serdar Çaktı and Lamia Çaktı and my brother Göksel Çaktı not only for supporting me and always believing in me during my studies but also for the harmony they provided at home during quarantine due to COVID-19.

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

The theory of binary quadratic forms can easily be traced back to antiquity; frequently in the form of the representation problem, that is integral solutions of $aX^2 + bXY + cY^2 = n$, where a, b, c and n are integers. The studies of Fermat and Euler re-popularized the study of binary quadratic forms. In his celebrated work "*Recherhes d'arithmétique*", Lagrange developed the arithmetic of binary quadratic forms. Even though the terminology is due to Gauss, he showed that equivalent forms represent the same integers. Also, he is the first mathematician in the written history that focuses on the discriminant $\Delta = b^2 - 4ac$ (in fact, on $-b^2 + 4ac$ to be more precise) of the binary quadratic form $aX^2+bXY+cY^2$. He made contributions to the reduction theory of binary quadratic forms and gave a constructive solution to the minimum problem of a form by using continued fractions. The first systematic treatment of the theory of binary quadratic forms is due to Gauss, [Gauss, 1801].

The works of Dedekind, Dirichlet, Kummer, and others established the standard notions of algebraic number theory, in which the main object of study is number fields, that is finite extensions of $\mathbb{Q}$. In this terminology, which is still in use today, the (narrow) class number of a number field, that is the cardinality of the (narrow) ideal class group stands out as one of the most important invariants of a number field. Especially after the false proof of Lamé of Fermat's last theorem, [Lamé, 1847], the importance of the class number was underlined.

There were not many algorithms developed in the direction of computation of class numbers, especially for general number fields. After establishing the one to one correspondence between the set of primitive indefinite integral binary quadratic forms and the narrow ideal class group of real quadratic number fields, many al-

gorithms in the language of binary quadratic forms were used to calculate class numbers of such number fields. Following the footprints of Lenstra, [Lenstra, 1982], in [Schoof, 2008], Schoof has given an interpretation of the algorithms for general number fields in terms of the Arakelov class group, $\widetilde{\mathrm{Pic}^0}(K)$, of the number field in question. In the case of real quadratic number fields, the group $\widetilde{\mathrm{Pic}^0}(K)$ is isomorphic to $\mathrm{Cl}^+(K) \times S^1$; where S^1 is the unit circle in $\mathbb{C}$. On the other hand, the algorithms for the general theory and the theory developed for real quadratic number fields do not seem to overlap.

In this thesis, we address this point. More precisely, we fix a fundamental discriminant $\Delta > 0$ and define a map from the set of primitive indefinite integral binary quadratic forms to $\widetilde{\mathrm{Pic}^0}(\mathbb{Q}(\sqrt{\Delta}))$. We then establish properties of this map, and in particular, show that its image is a dense subset. The thesis is organized as follows:

Chapter 2 contains standard material to define Arakelov divisors and Arakelov class groups. We first fix a number field K of degree n and define Arakelov divisors of K, which form an abelian group under componentwise addition. We then introduce degree notion on prime ideals of $\mathbb{Z}_K$ and infinite primes of K and extend the notion linearly to Arakelov divisors. Next, we focus on the divisors that have degree 0 and define the Arakelov class group. With the aim of expressing each Arakelov divisor multiplicatively, to each Arakelov divisor of K we associate a pair consisting of fractional ideal of K and a totally positive unit in $K \otimes_{\mathbb{Q}} \mathbb{R}$. We then show that this correspondence is in fact bijective. Hence these two notions can be identified. Later, we define *oriented* Arakelov divisors of K and the *oriented* Arakelov class group and relate them with important invariants of K such as its fractional ideals, narrow ideal class group and totally positive units of its ring of integers. The main reference of this chapter is [Schoof, 2008].

Chapter 3 consists of a detailed summary of the theory of indefinite integral binary quadratic forms. We start by defining basic notions about binary quadratic forms such as discriminant, content and their matrix representation. Then, we introduce the famous action of $\mathrm{GL}_2(\mathbb{Z})$ on the set of primitive integral indefinite binary quadratic forms and discuss invariants of this action. Next, we relate indefinite binary quadratic forms with two-dimensional commutative $\mathbb{R}$-algebras. We determine

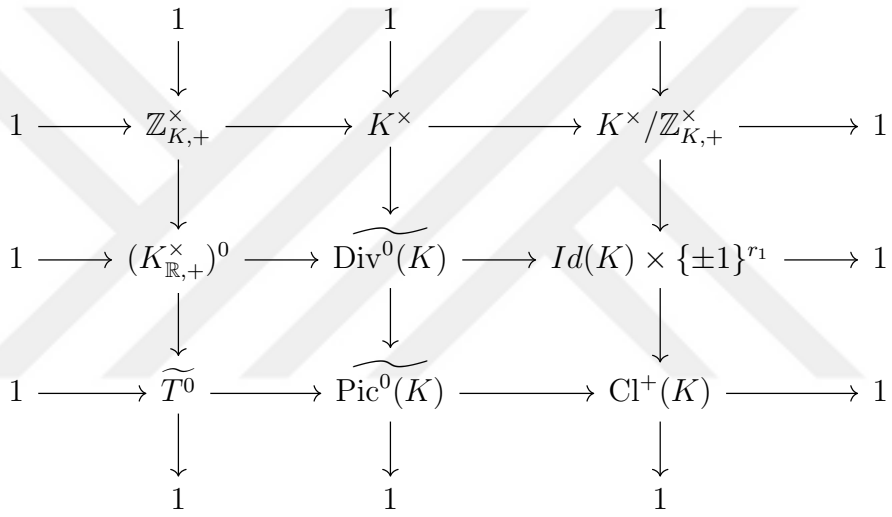
its automorphisms and algebraic properties. Later, we discuss the reduction theory of binary quadratic forms and compute the cycle of forms. Finally, we determine the automorphism group of a primitive indefinite integral binary quadratic form. The main reference of this chapter is [Buchmann and Vollmer, 2007].

In Chapter 4, we restrict our attention to real quadratic number fields. First, we study the embeddings, discriminant, and the ring of integers of a real quadratic number field and prove one of the main results that shows the one-to-one correspondence between the set of primitive integral indefinite binary quadratic forms and the narrow ideal class group of a real quadratic number field. We then define the map $\mathbf{D}$ on $\mathscr{F}(\Delta_K)$ that allows us to obtain an element of $\widetilde{\mathrm{Div}^0(K)}$. Next, we define a metric on $\widetilde{\mathrm{Pic}^0(K)}$ that is induced by the norm on $(K^{\times}_{\mathbb{R},+})^0$, which can be viewed as a 1-dimensional $\mathbb{R}$-vector space. Under this metric, we prove that the image of $\mathscr{F}(\Delta_K)$ under the map $\mathbf{D}$ is dense in $\widetilde{\mathrm{Pic}^0(K)}$.

Chapter 2

ARAKELOV DIVISORS

The main aim of this chapter is to understand the following commutative diagram with exact rows and columns:



Before we start, we fix some notations: From now on, K is a number field of degree n, r_1 is the number of real embeddings of K, r_2 is the number of complex-conjugate pairs of embeddings of K so that $n = r_1 + 2r_2$. We will denote the ring of integers of K by $\mathbb{Z}_K$. Throughout our work, we often use the important fact that the ring of integers of any number field is a Dedekind domain. The reader may refer to [Lorenzini, 1996], [Neukirch, 2013], [Jarvis, 2014] or [Milne, 2008] for a proof of this standard fact.

2.1 The Arakelov class group

Definition 2.1.1. An embedding σ of K into $\mathbb{C}$ considered up to complex conjugation is called an **infinite prime of** K. We also say that an infinite prime σ is **real** if $\sigma(K)$ is contained in $\mathbb{R}$ and **complex** otherwise.

Example 2.1.1. Consider $K = Q(\sqrt{D})$ where D is a square-free positive integer. Then the infinite primes of K are:

$$\begin{aligned} \sigma_1 : \mathbb{Q}(\sqrt{D}) &\to \mathbb{C} \\ x + y\sqrt{D} &\mapsto x + y\sqrt{D} \end{aligned}$$

and

$$\begin{aligned} \sigma_2 : \mathbb{Q}(\sqrt{D}) &\to \mathbb{C} \\ x + y\sqrt{D} &\mapsto x - y\sqrt{D} \end{aligned}$$

In this case, both infinite primes of K are real.

Remark 2.1.1. r_1 is the number of real infinite primes of the number field K and r_2 is the number of complex infinite primes.

Definition 2.1.2. A formal finite sum D of the form $\sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p} + \sum_{\sigma} x_\sigma \cdot \sigma$ where $\mathfrak{p}$ runs through all nonzero prime ideals of $\mathbb{Z}_K$, σ runs through all infinite primes of K and for integers $n_{\mathfrak{p}}$ and real numbers x_σ is called an **Arakelov divisor of** K.

Example 2.1.2. Consider the real quadratic number field $K = \mathbb{Q}(\sqrt{2})$. Then $\mathbb{Z}_K = \mathbb{Z}[\sqrt{2}]$ and $< 5 >$ is a prime ideal of $\mathbb{Z}_K$ as ${}^{\mathbb{Z}[\sqrt{2}]}\big/_{<5>} \cong \mathbb{Z}_5[\sqrt{2}]$ and $\mathbb{Z}_5[\sqrt{2}]$ is an integral domain. Let σ_1 and σ_2 denote its real infinite primes as in Example 2.1.1. Then

$$D = -\langle 5 \rangle + \frac{1}{2}\sigma_1 + \pi\sigma_2$$

is an Arakelov divisor of K.

Notation 2.1.1. The set of all Arakelov divisors of K will be denoted by $\mathrm{Div}(K)$.

Proposition 2.1.1. $\mathrm{Div}(K)$ *is an additive abelian group where the addition is defined component-wise.*

Proof. Let

$$D_i = \sum_{\mathfrak{p}} n_{\mathfrak{p}}^i \cdot \mathfrak{p} + \sum_{\sigma} x_\sigma^i \cdot \sigma \text{ for } i \in \{1, 2, 3\}$$

be Arakelov divisors of K. We show that the addition is well-defined. Indeed, we have

$$D_1 + D_2 = \left(\sum_{\mathfrak{p}} n_{\mathfrak{p}}^1 \cdot \mathfrak{p} + \sum_{\sigma} x_\sigma^1 \cdot \sigma \right) + \left(\sum_{\mathfrak{p}} n_{\mathfrak{p}}^2 \cdot \mathfrak{p} + \sum_{\sigma} x_\sigma^2 \cdot \sigma \right) = \sum_{\mathfrak{p}} (n_{\mathfrak{p}}^1 + n_{\mathfrak{p}}^2) \cdot \mathfrak{p} + \sum_{\sigma} (x_\sigma^1 + x_\sigma^2) \cdot \sigma$$

Since $n_{\mathfrak{p}}^1 + n_{\mathfrak{p}}^2 \in \mathbb{Z}$ for all prime ideals $\mathfrak{p}$ of $\mathbb{Z}_K$ and $x_\sigma^1 + x_\sigma^2 \in \mathbb{R}$ for all infinite primes σ of K, we have $D_1 + D_2 \in \mathrm{Div}(K)$. Now let us show that the addition is associative:

$$\begin{aligned}
(D_1 + D_2) + D_3 &= \left(\sum_{\mathfrak{p}} (n_{\mathfrak{p}}^1 + n_{\mathfrak{p}}^2) \cdot \mathfrak{p} + \sum_{\sigma} (x_\sigma^1 + x_\sigma^2) \cdot \sigma \right) + \left(\sum_{\mathfrak{p}} n_{\mathfrak{p}}^3 \cdot \mathfrak{p} + \sum_{\sigma} x_\sigma^3 \cdot \sigma \right) \\
&= \sum_{\mathfrak{p}} (n_{\mathfrak{p}}^1 + n_{\mathfrak{p}}^2 + n_{\mathfrak{p}}^3) \cdot \mathfrak{p} + \sum_{\sigma} (x_\sigma^1 + x_\sigma^2 + x_\sigma^3) \cdot \sigma \\
&= \left(\sum_{\mathfrak{p}} n_{\mathfrak{p}}^1 \cdot \mathfrak{p} + \sum_{\sigma} x_\sigma^1 \cdot \sigma \right) + \left(\sum_{\mathfrak{p}} (n_{\mathfrak{p}}^2 + n_{\mathfrak{p}}^3) \cdot \mathfrak{p} + \sum_{\sigma} (x_\sigma^2 + x_\sigma^3) \cdot \sigma \right) \\
&= D_1 + (D_2 + D_3)
\end{aligned}$$

The identity is the zero Arakelov divisor $D^0 = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p} + \sum_{\sigma} x_\sigma \cdot \sigma$ where $\mathfrak{p}$ where $n_{\mathfrak{p}} = 0$ for all prime ideals $\mathfrak{p}$ of $\mathbb{Z}_K$ and $x_\sigma = 0$ for all infinite primes σ of K as 0 is the identity of the additive groups $\mathbb{Z}$ and $\mathbb{R}$. The inverse of the Arakelov divisor D_1 is

$$-D_1 := \sum_{\mathfrak{p}} (-n_{\mathfrak{p}}^1) \cdot \mathfrak{p} + \sum_{\sigma} (-x_\sigma^1) \cdot \sigma$$

Indeed,

$$\begin{aligned}
D_1 + (-D_1) &= \sum_{\mathfrak{p}} (n_{\mathfrak{p}}^1 - n_{\mathfrak{p}}^1) \cdot \mathfrak{p} + \sum_{\sigma} (x_\sigma^1 - x_\sigma^1) \cdot \sigma \\
&= \sum_{\mathfrak{p}} 0 \cdot \mathfrak{p} + \sum_{\sigma} 0 \cdot \sigma \\
&= D_0
\end{aligned}$$

Lastly, we show that this is an abelian group:

$$\begin{aligned}
D_1 + D_2 &= \sum_{\mathfrak{p}} (n_{\mathfrak{p}}^1 + n_{\mathfrak{p}}^2) \cdot \mathfrak{p} + \sum_{\sigma} (x_\sigma^1 + x_\sigma^2) \cdot \sigma \\
&= \sum_{\mathfrak{p}} (n_{\mathfrak{p}}^2 + n_{\mathfrak{p}}^1) \cdot \mathfrak{p} + \sum_{\sigma} (x_\sigma^2 + x_\sigma^1) \cdot \sigma \\
&= \left(\sum_{\mathfrak{p}} n_{\mathfrak{p}}^2 \cdot \mathfrak{p} + \sum_{\sigma} x_\sigma^2 \cdot \sigma \right) + \left(\sum_{\mathfrak{p}} n_{\mathfrak{p}}^1 \cdot \mathfrak{p} + \sum_{\sigma} x_\sigma^1 \cdot \sigma \right) \\
&= D_2 + D_1
\end{aligned}$$

□

Definition 2.1.3. Let $f \in K^\times$ and consider the principal fractional ideal $f\mathbb{Z}_K$. Since $\mathbb{Z}_K$ is a Dedekind domain, we know that $f\mathbb{Z}_K$ can be uniquely represented as a product of prime ideals of $\mathbb{Z}_K$, up to the ordering of the factors. We write $f\mathbb{Z}_K = \prod_{\mathfrak{p}} \mathfrak{p}^{ord_{\mathfrak{p}}(f)}$. For a prime ideal $\mathfrak{p}$ of $\mathbb{Z}_K$, the exponent $ord_{\mathfrak{p}}(f)$ is called the **$\mathfrak{p}$-adic valuation of f on K**.

Definition 2.1.4. Let $f \in K^\times$. The Arakelov divisor

$$(f) := \sum_{\mathfrak{p}} ord_{\mathfrak{p}}(f) \cdot \mathfrak{p} + \sum_{\sigma} (-\log|\sigma(f)|) \cdot \sigma$$

is called the **principal Arakelov divisor of K associated to f**.

Example 2.1.3. For $K = \mathbb{Q}(\sqrt{2})$ and $5 \in \mathbb{Q}(\sqrt{2})^\times$, the Arakelov divisor

$$\begin{aligned}(5) &= \sum_{\mathfrak{p}} ord_{\mathfrak{p}}(5) \cdot \mathfrak{p} + [-\log|\sigma(5)| \cdot \sigma_1] + [-\log|\sigma(5)| \cdot \sigma_2] \\ &= 1 \cdot \langle 5 \rangle - \log|5| \cdot \sigma_1 - \log|5| \cdot \sigma_2\end{aligned}$$

is the principal Arakelov divisor associated to 5.

Lemma 2.1.2. *The set of all principal Arakelov divisors of K,* $\mathrm{PDiv}(K)$*, is a subgroup of* $\mathrm{Div}(K)$*.*

Proof. Note that $\mathrm{PDiv}(K)$ is a non-empty set as $K^\times = K \setminus \{0\}$ is non-empty. Let f, $g \in K^\times$. By the Subgroup Criterion we need to show that $(f) - (g) \in \mathrm{PDiv}(K)$. We know that

$$(f) = \sum_{\mathfrak{p}} ord_{\mathfrak{p}}(f) \cdot \mathfrak{p} + \sum_{\sigma} (-\log|\sigma(f)|) \cdot \sigma$$

and that

$$(g) = \sum_{\mathfrak{p}} ord_{\mathfrak{p}}(g) \cdot \mathfrak{p} + \sum_{\sigma} (-\log|\sigma(g)|) \cdot \sigma$$

which implies that

$$-(g) = \sum_{\mathfrak{p}} -ord_{\mathfrak{p}}(g) \cdot \mathfrak{p} + \sum_{\sigma} (\log|\sigma(g)|) \cdot \sigma$$

It follows that

$$\begin{aligned}(f)-(g) &= \sum_{\mathfrak{p}} ord_{\mathfrak{p}}(f)-ord_{\mathfrak{p}}(g)\cdot\mathfrak{p}+\sum_{\sigma}(-\log|\sigma(f)|+\log|\sigma(g)|)\cdot\sigma \\ &= \sum_{\mathfrak{p}} ord_{\mathfrak{p}}\Big(\frac{f}{g}\Big)\cdot\mathfrak{p}+\sum_{\sigma}\log\Big|\frac{\sigma(g)}{\sigma(f)}\Big|\cdot\sigma \text{ by a property of valuation} \\ &= \sum_{\mathfrak{p}} ord_{\mathfrak{p}}\Big(\frac{f}{g}\Big)\cdot\mathfrak{p}+\sum_{\sigma}(-\log\Big|\frac{\sigma(f)}{\sigma(g)}\Big|)\cdot\sigma \text{ by a property of logarithmic functions} \\ &= \sum_{\mathfrak{p}} ord_{\mathfrak{p}}\Big(\frac{f}{g}\Big)\cdot\mathfrak{p}+\sum_{\sigma}(-\log\Big|\sigma\Big(\frac{f}{g}\Big)\Big|)\cdot\sigma \text{ as each } \sigma \text{ is a homomorphism} \\ &= \Big(\frac{f}{g}\Big)\end{aligned}$$

Since $\frac{f}{g}\in K^{\times}$, we deduce that $(f)-(g)=\left(\frac{f}{g}\right)\in \mathrm{PDiv}(K)$. Hence $\mathrm{PDiv}(K)$ is a subgroup of $\mathrm{Div}(K)$. □

Definition 2.1.5. Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathbb{Z}_K$. The **degree of** $\mathfrak{p}$ is defined as $\log\left(\left|{}^{\mathbb{Z}_K}/_{\mathfrak{p}}\right|\right)$.

Notation 2.1.2. The degree of a non-zero prime ideal $\mathfrak{p}$ of $\mathbb{Z}_K$ will be denoted by $deg(\mathfrak{p})$.

Example 2.1.4. For $K=\mathbb{Q}(\sqrt{2})$ and $\mathfrak{p}=\langle 5\rangle$, by Example 2.1.2, we know that $deg(\langle 5\rangle)=\log(|\mathbb{Z}_5[\sqrt{2}]|)=\log(25)=2\log(5)$.

Definition 2.1.6. Let σ be an infinite prime of K. The **degree of** σ is

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

Example 2.1.5. Any real quadratic number field has two infinite primes of degree 1.

Definition 2.1.7. If $D=\sum_{\mathfrak{p}} n_{\mathfrak{p}}\cdot\mathfrak{p}+\sum_{\sigma} x_{\sigma}\cdot\sigma$ where $\mathfrak{p}$ is an Arakelov divisor of K, then the **degree of** D is defined as

$$\sum_{\mathfrak{p}} n_{\mathfrak{p}}\cdot deg(\mathfrak{p})+\sum_{\sigma} x_{\sigma}\cdot deg(\sigma)$$

Example 2.1.6. For $K=\mathbb{Q}(\sqrt{2})$, by Examples 2.1.4 and 2.1.5, the degree of the principal Arakelov divisor

$$(5)=1\cdot\langle 5\rangle-\log|5|\cdot\sigma_1-\log|5|\cdot\sigma_2$$

is:

$$deg((5)) = 2\log(5) - 2\log(5) = 0$$

Lemma 2.1.3. *Denote the set of all Arakelov divisors of K of degree 0 by $\mathrm{Div}^0(K)$. Then, $\mathrm{Div}^0(K)$ is a subgroup of $\mathrm{Div}(K)$.*

Proof. $\mathrm{Div}^0(K)$ is a non-empty set as the zero Arakelov divisor $D = 0$ have degree 0. Let

$$D_1 = \sum_{\mathfrak{p}} n^1_{\mathfrak{p}} \cdot \mathfrak{p} + \sum_{\sigma} x^1_{\sigma} \cdot \sigma \in \mathrm{Div}^0(K)$$

and

$$D_1 = \sum_{\mathfrak{p}} n^1_{\mathfrak{p}} \cdot \mathfrak{p} + \sum_{\sigma} x^1_{\sigma} \cdot \sigma \in \mathrm{Div}^0(K) \in \mathrm{Div}^0(K)$$

Then we know that

$$\sum_{\mathfrak{p}} n^1_{\mathfrak{p}} \cdot deg(\mathfrak{p}) + \sum_{\sigma} x^1_{\sigma} \cdot deg(\sigma) = \sum_{\mathfrak{p}} n^2_{\mathfrak{p}} \cdot deg(\mathfrak{p}) + \sum_{\sigma} x^2_{\sigma} \cdot deg(\sigma) = 0$$

By the Subgroup Criterion it suffices to show that $D_1 - D_2 \in \mathrm{Div}^0(K)$ so we need to prove that $deg(D_1 - D_2) = 0$. We have:

$$\begin{aligned} deg(D_1 - D_2) &= \sum_{\mathfrak{p}} (n^1_{\mathfrak{p}} - n^2_{\mathfrak{p}}) \cdot deg(\mathfrak{p}) + \sum_{\sigma} (x^1_{\sigma} - x^2_{\sigma}) \cdot deg(\sigma) \\ &= \sum_{\mathfrak{p}} n^1_{\mathfrak{p}} \cdot deg(\mathfrak{p}) + \sum_{\sigma} x^1_{\sigma} \cdot deg(\sigma) - \left(\sum_{\mathfrak{p}} n^2_{\mathfrak{p}} \cdot deg(\mathfrak{p}) + \sum_{\sigma} x^2_{\sigma} \cdot deg(\sigma) \right) \\ &= 0 \end{aligned}$$

Hence $\mathrm{Div}^0(K)$ is a subgroup of $\mathrm{Div}(K)$. □

Proposition 2.1.4. *The principal Arakelov divisors of K have degree 0.*

Proof. Let $(f) = \sum_{\mathfrak{p}} ord_{\mathfrak{p}}(f) \cdot \mathfrak{p} + \sum_{\sigma} (-\log|\sigma(f)|) \cdot \sigma \in \mathrm{PDiv}(K)$. We need to show that

$$deg((f)) = \sum_{\mathfrak{p}} ord_{\mathfrak{p}}(f) \cdot deg(\mathfrak{p}) + \sum_{\sigma} (-\log|\sigma(f)|) \cdot deg(\sigma) = 0$$

Since $f \in K^{\times}$, by the Product Formula for the valuations on K, we have :

$$\prod_{\mathfrak{p}} N(\mathfrak{p})^{-ord_{\mathfrak{p}}(f)} \cdot \prod_{\sigma\text{: real}} |\sigma(f)| \cdot \prod_{\sigma\text{: complex}} \sigma(f)\overline{\sigma(f)} = 1$$

where $N(\mathfrak{p}) := \left|\mathbb{Z}_K/_{\mathfrak{p}}\right|$. Note that $\sigma(f)\overline{\sigma(f)} = |\sigma(f)|^2$ for each complex infinite prime of K. By taking the log of both sides of the equation, we get:

$$\sum_{\mathfrak{p}} -ord_{\mathfrak{p}}(f) \cdot deg(\mathfrak{p}) + \sum_{\sigma\text{: real}} \log|\sigma(f)| + \sum_{\sigma\text{: complex}} 2\log|\sigma(f)| = 0$$

which implies that

$$0 = \sum_{\mathfrak{p}} ord_{\mathfrak{p}}(f) \cdot deg(\mathfrak{p}) + \sum_{\sigma}(-\log|\sigma(f)|) \cdot deg(\sigma) = deg((f)).$$

□

Corollary 2.1.5. $\mathrm{PDiv}(K)$ *is a subgroup of* $\mathrm{Div}^0(K)$.

Proof. This fact follows from Lemma 2.1.3 and Proposition 2.1.4. □

Definition 2.1.8. The quotient of the group $\mathrm{Div}^0(K)$ by the subgroup of principal Arakelov divisors $\mathrm{PDiv}(K)$ is called the **Arakelov class group of** K.

Notation 2.1.3. The Arakelov class group will be denoted by $\mathrm{Pic}^0(K)$.

2.2 Multiplicative notation of Arakelov divisors

Earlier we showed that $\mathrm{Div}(K)$ forms an additive group so one has an additive notation on the notion of Arakelov divisors of K. Now we would like to express each Arakelov divisor of K in multiplicative notation. This is the reason why we introduce first the following $\mathbb{R}$-algebra:

Let us concentrate on $K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R}$. We will observe that $K_{\mathbb{R}} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Since K is a number field, we know by the Primitive Element Theorem that $K = \mathbb{Q}(\alpha)$ for some algebraic number α. Let $m(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α over $\mathbb{Q}$. We know that $K \cong \mathbb{Q}[x]/\langle m(x)\rangle$, the polynomial $m(x)$ is irreducible over $\mathbb{Q}$ and of degree $deg(m(x)) = n = r_1 + 2r_2$. Note that r_1 represents the number of real roots of $m(x)$ and r_2 represents the number of pairs of complex roots of $m(x)$. We also know that $\mathbb{Q}[x] \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}[x]$ and by the compatibility property of the tensor product with quotients we get:

$$K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{Q}[x]/\langle m(x)\rangle \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}[x]/\langle m(x)\rangle$$

By definition, $m(x)$ is irreducible over rationals but it might not be an irreducible polynomial over $\mathbb{R}$. Say $m(x)$ factors in the field of real numbers as $m(x) = \prod_{i=1}^{k} m_i(x) \in \mathbb{R}[x]$ where $m_i(x) \in \mathbb{R}[x]$ is irreducible over $\mathbb{R}$ for all $i \in \{1, 2, \ldots, k\}$ and all distinct. It follows from the Chinese Remainder Theorem that:

$$K \otimes_{\mathbb{Q}} \mathbb{R} \cong \bigotimes_{i=1}^{k} \mathbb{R}[x]/ < m_i(x) >$$

Since irreducible polynomials in $\mathbb{R}[x]$ are of degree either 1 or 2 we deduce that

$$K \otimes_{\mathbb{Q}} \mathbb{R} \cong \bigotimes_{i=1}^{k} \mathbb{R}[x]/ < m_i(x) > \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

from which we also see that $K_{\mathbb{R}}$ is an $\mathbb{R}$-algebra where the addition and the multiplication are defined component-wise.

Remark 2.2.1. $K_{\mathbb{R}}$ is a ring with unit element $1 := (1, 1, \ldots, 1)$ which is not an integral domain. Indeed, $(1, 0, \ldots, 0), (0, \ldots 0, 1) \in K_{\mathbb{R}}$ are both non-zero elements of $K_{\mathbb{R}}$ but

$$(1, 0, \ldots, 0)(0, \ldots 0, 1) = (0, 0, \ldots, 0)$$

We will now determine the invertible elements of $K_{\mathbb{R}}$:

Proposition 2.2.1. *The invertible elements of $K_{\mathbb{R}}$ are those which do not have* 0 *as a component.*

Proof. Let $x = (x_1, x_2, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \in K_{\mathbb{R}}$. Then x is invertible in $K_{\mathbb{R}}$ if and only if there exists an element $x' = (x'_1, x'_2, \ldots, x'_{r_1}, z'_1, \ldots, z'_{r_2}) \in K_{\mathbb{R}}$ such that

$$\begin{aligned} x \cdot x' &= (x_1, x_2, \ldots, x_{r_1}, z_1, \ldots, z_{r_2})(x'_1, x'_2, \ldots, x'_{r_1}, z'_1, \ldots, z'_{r_2}) \\ &= (x_1 x'_1, x_2 x'_2, \ldots, x_{r_1} x'_{r_1}, z_1 z'_1, \ldots, z_{r_2} z'_{r_2}) \\ &= (1, 1, \ldots, 1) \end{aligned}$$

Now observe that

$$\begin{aligned} x \cdot x' = 1 &\iff x_i x'_i = 1 \text{ for all } i \in \{1, 2, \ldots, r_1\} \text{ and } z_j z'_j = 1 \text{ for all } j \in \{1, 2, \ldots, r_2\} \\ &\iff x_i \text{ is invertible in } \mathbb{R} \text{ for } i \in \{1, 2, \ldots, r_1\} \text{ and} \\ &\quad z_j \text{ is invertible in } \mathbb{C} \text{ for } j \in \{1, 2, \ldots, r_2\} \\ &\iff x_i \neq 0 \text{ for } i \in \{1, 2, \ldots, r_1\} \text{ and } z_j \neq 0 \text{ for } j \in \{1, 2, \ldots, r_2\} \\ &\iff \text{each component of } x \text{ is non-zero.} \end{aligned}$$

□

From the proof of the Proposition 2.2.1, we directly derive the following result:

Corollary 2.2.2. *We have* $K_{\mathbb{R}}^{\times} \cong (\mathbb{R}^{\times})^{r_1} \times (\mathbb{C}^{\times})^{r_2}$.

Definition 2.2.1. Let $x = (x_1, x_2, \ldots, x_{r_1}, z_1, \ldots, z_{r_2})$ be an element of $K_{\mathbb{R}}$. The **sign of** x is defined as the r_1-tuple $(sign(x_1), sign(x_2), \ldots sign(x_{r_1})) \in \{\pm 1\}^{r_1}$.

Definition 2.2.2. Let $x = (x_1, x_2, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \in K_{\mathbb{R}}$. The element x is called **totally positive** if $sign(x_i) = +1$ for all $i \in \{1, 2, \ldots, r_1\}$.

Notation 2.2.1. We denote the set of all totally positive elements of $K_{\mathbb{R}}$ by $K_{\mathbb{R},+}$ and the notation $K_{\mathbb{R},+}^{\times} := K_{\mathbb{R},+} \cap K_{\mathbb{R}}^{\times}$ represents the set of totally positive elements in $K_{\mathbb{R}}$ that are invertible.

Remark 2.2.2. We remark that by Proposition 2.2.1, we have $K_{\mathbb{R},+}^{\times} \cong (\mathbb{R}_+)^{r_1}$ where $\mathbb{R}_+ := \{r \in \mathbb{R} : r > 0\}$.

On $K_{\mathbb{R}}$, we define the following function:

$$\begin{aligned} \mathcal{N} : K_{\mathbb{R}} &\to \mathbb{R} \\ (x_1, x_2, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) &\mapsto \left(\prod_{i=1}^{r_1} x_i\right) \cdot \left(\prod_{j=1}^{r_2} z_j \overline{z_j}\right) \end{aligned}$$

Note that the function $\mathcal{N}$ is well-defined as $z\overline{z} = |z|^2 \in \mathbb{R}_{\geq 0}$ for any complex number z and observe that $\mathcal{N}$ is a multiplicative function:
Let $x = (x_1, x_2, \ldots, x_{r_1}, z_1, \ldots, z_{r_2})$, $y = (y_1, y_2, \ldots, y_{r_1}, z_1', \ldots, z_{r_2}') \in K_{\mathbb{R}}$ so that

$$xy = (x_1y_1, x_2y_2, \ldots, x_{r_1}y_{r_1}, z_1z_1', \ldots, z_{r_2}z_{r_2}')$$

Then,

$$\begin{aligned} \mathcal{N}(xy) &= \left(\prod_{i=1}^{r_1} x_iy_i\right) \cdot \left(\prod_{j=1}^{r_2} z_j\overline{z_j}z_j'\overline{z_j'}\right) \\ &= \left(\prod_{i=1}^{r_1} x_i\right) \cdot \left(\prod_{i=1}^{r_1} y_i\right) \cdot \left(\prod_{j=1}^{r_2} z_j\overline{z_j}\right) \cdot \left(\prod_{j=1}^{r_2} z_j'\overline{z_j'}\right) \\ &= \left[\left(\prod_{i=1}^{r_1} x_i\right) \cdot \left(\prod_{j=1}^{r_2} z_j\overline{z_j}\right)\right] \cdot \left[\left(\prod_{i=1}^{r_1} y_i\right) \cdot \left(\prod_{j=1}^{r_2} z_j'\overline{z_j'}\right)\right] \\ &= \mathcal{N}(x)\mathcal{N}(y) \end{aligned}$$

Since $\mathcal{N}$ is multiplicative, $\mathcal{N}$ induces the group homomorphism

$$\mathcal{N} : K_{\mathbb{R}}^{\times} \rightarrow \mathbb{R}^{\times}$$

We determine its kernel:

$$\begin{aligned}\ker(\mathcal{N}) &= \left\{(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \in K_{\mathbb{R}}^{\times} : \mathcal{N}((x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2})) = 1\right\} \\ &= \left\{(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \in K_{\mathbb{R}}^{\times} : \left(\prod_{i=1}^{r_1} x_i\right) \cdot \left(\prod_{j=1}^{r_2} z_j \overline{z_j}\right) = 1\right\} \\ &=: \left(K_{\mathbb{R}}^{\times}\right)^0\end{aligned}$$

We also set $\left(K_{\mathbb{R},+}^{\times}\right)^0 := \left(K_{\mathbb{R}}^{\times}\right)^0 \cap K_{\mathbb{R},+}$

2.2.1 From divisors to fractional ideals and units

We are now ready to describe each Arakelov divisor of K in multiplicative notation:

Let $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p} + \sum_{\sigma} x_{\sigma} \cdot \sigma$ be an Arakelov divisor of K. To the divisor D, we associate the ideal $I = \prod_{\mathfrak{p}} \mathfrak{p}^{-n_{\mathfrak{p}}}$ of $\mathbb{Z}_K$. Note that the description of the ideal I is well-defined as we know that each non-zero prime ideal of $\mathbb{Z}_K$ is invertible. Moreover, I is a fractional ideal of K. To D, we also associate the unit $u = (\exp(-x_{\sigma}))_{\sigma}$. Note that by Proposition 2.2.1, u is indeed a unit of $K_{\mathbb{R}}$. Also, observe that $u \in \prod_{\sigma} \mathbb{R}_+$. Hence $u \in K_{\mathbb{R},+}^{\times}$. To the Arakelov divisor D, we attach the pair (I, u) and write $D = (I, u)$.

Conversely let (I, u) be a pair such that I is a fractional ideal of K and u be a totally positive unit in $K_{\mathbb{R}}$. Since I is a fractional ideal of K, it can be uniquely written as a product of prime ideals of $\mathbb{Z}_K$. Say $I = \mathfrak{p}_1^{a_{\mathfrak{p}_1}} \ldots \mathfrak{p}_s^{a_{\mathfrak{p}_s}}$. Then set $n_{\mathfrak{p}} = -a_{\mathfrak{p}}$ if $\mathfrak{p} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ and $n_{\mathfrak{p}} = 0$ otherwise. Also, from the *totally positive* unit $u = (u_1, u_2, \ldots, u_{r_1}, u_{r_1+1}, \ldots, u_{r_1+r_2})$, we derive the coefficients $x_{\sigma_j} := -\log(u_j)$ for $j \in \{1, 2, \ldots r_1 + r_2\}$. Hence

$$D := \sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p} + \sum_{j=1}^{r_1+r_2} x_{\sigma_j} \cdot \sigma_j$$

is an Arakelov divisor of K. In fact, these maps are inverses of each other which shows that there is a bijective correspondence between $\mathrm{Div}(K)$ and the set of such pairs.

Example 2.2.1.

- The zero Arakelov divisor $D = 0$ corresponds to $(\mathbb{Z}_K, 1)$.
- If $f \in K^\times$, the principal Arakelov divisor (f) corresponds to $(f^{-1}\mathbb{Z}_K, (|\sigma(f)|)_\sigma)$.
- If $D = (I, u)$ is an Arakelov divisor of K, then $-D = (I^{-1}, u^{-1})$.

Proposition 2.2.3. *Let $D = (I, u)$ be an Arakelov divisor of K. In terms of the pair (I, u) associated to D, the degree of the Arakelov divisor D is $-\log(|\mathcal{N}(u)|N(I))$.*

Proof. Let $D = \sum_\mathfrak{p} n_\mathfrak{p} \cdot \mathfrak{p} + \sum_\sigma x_\sigma \cdot \sigma$ be an Arakelov divisor. We know that

$$D = (I, u) = (\prod_\mathfrak{p} \mathfrak{p}^{-n_\mathfrak{p}}, (\exp(-x_\sigma))_\sigma)$$

and we need to show that

$$deg(D) = \sum_\mathfrak{p} n_\mathfrak{p} \cdot deg(\mathfrak{p}) + \sum_\sigma x_\sigma \cdot deg(\sigma) = -\log(|\mathcal{N}(u)|N(I))$$

We have:

$$\begin{aligned} deg(D) &= -\sum_\mathfrak{p} -n_\mathfrak{p} \cdot deg(\mathfrak{p}) - \sum_\sigma -x_\sigma \cdot deg(\sigma) \\ &= -\sum_\mathfrak{p} -n_\mathfrak{p} \cdot \log(N(\mathfrak{p})) - \sum_\sigma -x_\sigma \cdot deg(\sigma) \\ &= -\log\Big(\prod_\mathfrak{p} N(\mathfrak{p})^{-n_\mathfrak{p}}\Big) - log\Big(\big|\prod_\sigma \exp(-x_\sigma \cdot deg(\sigma))\big|\Big) \\ &= -\log(N(I)) - log(|\mathcal{N}(u)|) \\ &= -\log(|\mathcal{N}(u)|N(I)) \end{aligned}$$

□

2.3 The oriented Arakelov class group

Definition 2.3.1. An **oriented Arakelov divisor of** K is a formal finite sum of the form $\sum_\mathfrak{p} n_\mathfrak{p} \cdot \mathfrak{p} + \sum_\sigma x_\sigma \cdot \sigma$ where $\mathfrak{p}$ runs through all nonzero prime ideals of $\mathbb{Z}_K$, σ runs through all infinite primes of K and for integers $n_\mathfrak{p}$ and $x_\sigma \in K_\sigma^\times$ where

$$K_\sigma^\times := \begin{cases} \mathbb{R}^\times & \text{if } \sigma \text{ is real} \\ \mathbb{C}^\times & \text{if } \sigma \text{ is complex} \end{cases}$$

Example 2.3.1. Consider the real quadratic field K and its infinite primes σ_1, σ_2 as in Example 2.1.1. Then $D = 1 \cdot \sigma_1 + (-1) \cdot \sigma_2$ is an oriented Arakelov divisor of K and $D' = 0 \cdot \sigma_1 + (-1)\sigma_2$ is not an oriented Arakelov divisor of K as the infinite prime σ_1 is real and $0 \notin K_\sigma^\times = \mathbb{R}^\times$.

Notation 2.3.1. The set of all oriented Arakelov divisors of K will be denoted by $\widetilde{\mathrm{Div}(K)}$.

Proposition 2.3.1. *$(\widetilde{\mathrm{Div}(K)}, \bullet)$ is an abelian group where*

$$\begin{aligned} \bullet : \widetilde{\mathrm{Div}(K)} \times \widetilde{\mathrm{Div}(K)} &\to \widetilde{\mathrm{Div}(K)} \\ \Big(\sum_{\mathfrak{p}} n_{\mathfrak{p}}^1 \cdot \mathfrak{p} + \sum_{\sigma} x_\sigma^1 \cdot \sigma, \sum_{\mathfrak{p}} n_{\mathfrak{p}}^2 \cdot \mathfrak{p} + \sum_{\sigma} x_\sigma^2 \cdot \sigma\Big) &\mapsto \sum_{\mathfrak{p}} (n_{\mathfrak{p}}^1 + n_{\mathfrak{p}}^2) \cdot \mathfrak{p} + \sum_{\sigma} (x_\sigma^1 \cdot x_\sigma^2) \cdot \sigma \end{aligned}$$

Proof. The associativity property follows from the fact that $(\mathbb{Z}, +)$ and $(K_\sigma^\times, \cdot)$ are groups. The identity element of this group is $D_{Id} := \sum_{\mathfrak{p}} 0 \cdot \mathfrak{p} + \sum_\sigma 1 \cdot \sigma$. Indeed, for any $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p} + \sum_\sigma x_\sigma \cdot \sigma \in \widetilde{\mathrm{Div}(K)}$, we have:

$$\begin{aligned} D \bullet D_{Id} &= \sum_{\mathfrak{p}} (n_{\mathfrak{p}} + 0) \cdot \mathfrak{p} + \sum_\sigma (x_\sigma \cdot 1) \cdot \sigma \\ &= \sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p} + \sum_\sigma x_\sigma \cdot \sigma \\ &= D \end{aligned}$$

Similarly, we have $D_{Id} \bullet D = D$. Now we claim that for $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p} + \sum_\sigma x_\sigma \cdot \sigma \in \widetilde{\mathrm{Div}(K)}$, its inverse is $-D := \sum_{\mathfrak{p}} (-n_{\mathfrak{p}}) \cdot \mathfrak{p} + \sum_\sigma \frac{1}{x_\sigma} \cdot \sigma$. Indeed, $-D \in \widetilde{\mathrm{Div}(K)}$ and

$$\begin{aligned} D \bullet (-D) &= \sum_{\mathfrak{p}} (n_{\mathfrak{p}} - n_{\mathfrak{p}}) \cdot \mathfrak{p} + \sum_\sigma (x_\sigma \cdot \frac{1}{x_\sigma}) \cdot \sigma \\ &= \sum_{\mathfrak{p}} 0 \cdot \mathfrak{p} + \sum_\sigma 1 \cdot \sigma \\ &= D_{Id} \end{aligned}$$

Similar arguments show that $(-D) \bullet D = D_{Id}$. This proves that $(\widetilde{\mathrm{Div}(K)}, \bullet)$ is a group. Now we prove commutativity of $(\widetilde{\mathrm{Div}(K)}, \bullet)$: For $D_1 = \sum_{\mathfrak{p}} n_{\mathfrak{p}}^1 \cdot \mathfrak{p} + \sum_\sigma x_\sigma^1 \cdot \sigma$,

$D_2 = \sum_{\mathfrak{p}} n_{\mathfrak{p}}^2 \cdot \mathfrak{p} + \sum_{\sigma} x_{\sigma}^2 \cdot \sigma \in \widetilde{\mathrm{Div}(K)}$, we have:

$$\begin{aligned} D_1 \bullet D_2 &= \sum_{\mathfrak{p}} (n_{\mathfrak{p}}^1 + n_{\mathfrak{p}}^2) \cdot \mathfrak{p} + \sum_{\sigma} (x_{\sigma}^1 \cdot x_{\sigma}^2) \cdot \sigma \\ &= \sum_{\mathfrak{p}} (n_{\mathfrak{p}}^2 + n_{\mathfrak{p}}^1) \cdot \mathfrak{p} + \sum_{\sigma} (x_{\sigma}^2 \cdot x_{\sigma}^1) \cdot \sigma \\ &= D_2 \bullet D_1 \end{aligned}$$

□

Let $\widetilde{Pairs}$ be the set of all pairs of the form (I, u) where I is a fractional ideal of K and u be a unit in $K_{\mathbb{R}}$, not necessarily totally positive. Likely to the story of "ordinary" Arakelov divisors, to represent each oriented Arakelov divisor multiplicatively, we introduce the following maps:

$$\begin{aligned} \phi_1 : \widetilde{Pairs} &\to \widetilde{\mathrm{Div}(K)} \\ (I, u) = \left(\prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}}}, (u_\sigma)_\sigma \right) &\mapsto \sum_{\mathfrak{p}} -a_{\mathfrak{p}} \cdot \mathfrak{p} + \sum_{\sigma} u_\sigma \cdot \sigma \end{aligned}$$

and

$$\begin{aligned} \phi_2 : \widetilde{\mathrm{Div}(K)} &\to \widetilde{Pairs} \\ \sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p} + \sum_{\sigma} x_\sigma \cdot \sigma &\mapsto \left(\prod_{\mathfrak{p}} \mathfrak{p}^{-n_{\mathfrak{p}}}, (x_\sigma)_\sigma \right) \end{aligned}$$

Since we have

$$\begin{aligned} \phi_1(\phi_2(D)) &= \phi_1 \left(\left(\prod_{\mathfrak{p}} \mathfrak{p}^{-n_{\mathfrak{p}}}, (x_\sigma)_\sigma \right) \right) \\ &= \sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p} + \sum_{\sigma} x_\sigma \cdot \sigma \\ &= D \end{aligned}$$

for all $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \cdot \mathfrak{p} + \sum_{\sigma} x_\sigma \cdot \sigma \in \widetilde{\mathrm{Div}(K)}$ and

$$\begin{aligned}\phi_2(\phi_1(I,u)) &= \phi_2\Big(\sum_{\mathfrak{p}} -a_{\mathfrak{p}}\cdot\mathfrak{p} + \sum_{\sigma} u_\sigma\cdot\sigma\Big)\\ &= \left(\prod_{\mathfrak{p}}\mathfrak{p}^{a_{\mathfrak{p}}}, (u_\sigma)_\sigma\right)\\ &= (I,u)\end{aligned}$$

for all $(I,u) = \left(\prod_{\mathfrak{p}}\mathfrak{p}^{a_{\mathfrak{p}}}, (u_\sigma)_\sigma\right) \in \widetilde{Pairs}$, we have a bijection between these two sets which means that we can (actually may) identify them as we did in Arakelov divisors.

Remark 2.3.1. If $\widetilde{D} = (I,u)$ is an oriented Arakelov divisor of K, then in terms of the oriented pair associated to $\widetilde{D}$, its inverse is given by $-\widetilde{D} = (I^{-1}, u^{-1})$ where $u^{-1} = (u_\sigma^{-1})_\sigma$ for $u = (u_\sigma)_\sigma$.

Remark 2.3.2. The bijection between the sets $\widetilde{Pairs}$ and $\widetilde{\mathrm{Div}(K)}$ gives rise to the following isomorphism of groups:

$$\widetilde{\mathrm{Div}(K)} \cong Id(K)\times K_{\mathbb{R}}^{\times}$$

Definition 2.3.2. Let $f\in K^{\times}$. The **principal oriented Arakelov divisor associated to** f is the oriented Arakelov divisor corresponds to $(f^{-1}\mathbb{Z}_K, (\sigma(f))_\sigma)$. In other words, the oriented Arakelov divisor

$$(\tilde{f}) := \sum_{\mathfrak{p}} ord_{\mathfrak{p}}(f)\cdot\mathfrak{p} + \sum_{\sigma}\sigma(f)\cdot\sigma$$

is called the principal oriented Arakelov divisor associated to f.

In terms of their corresponding oriented pairs, we have $\mathrm{Div}(K)\subset\widetilde{\mathrm{Div}(K)}$. The inverse of this inclusion is given by

$$\begin{aligned}\widetilde{\mathrm{Div}(K)} &\to \mathrm{Div}(K)\\ (I,(u_\sigma)_\sigma) &\mapsto (I,(|u_\sigma|)_\sigma)\end{aligned}$$

and motivates the definition of the degree of an oriented Arakelov divisor of K:

Definition 2.3.3. Let $\tilde{D} = (I, (u_\sigma)_\sigma) \in \widetilde{\mathrm{Div}(K)}$. The **degree of the oriented Arakelov divisor** D **of** K, $deg(\tilde{D})$, is given by the degree of the Arakelov divisor $D = (I, (|u_\sigma|)_\sigma)$.

Proposition 2.3.2. *Principal oriented Arakelov divisors of* K *have degree* 0.

Proof. This fact follows from the definition of the degree of an oriented Arakelov divisor of K and Proposition 2.1.4. □

Notation 2.3.2. We will denote the set of principal oriented Arakelov divisors of K by $\widetilde{\mathrm{PDiv}(K)}$ and the set of oriented Arakelov divisors of K that have degree 0 by $\widetilde{\mathrm{Div}^0(K)}$.

Notationally, Proposition 2.3.2 implies that $\widetilde{\mathrm{PDiv}(K)} \subseteq \widetilde{\mathrm{Div}^0(K)}$.

Proposition 2.3.3. $\widetilde{\mathrm{Div}^0(K)}$ *is a subgroup of* $\widetilde{\mathrm{Div}(K)}$.

Proof. By Proposition 2.3.2, we know that the set $\widetilde{\mathrm{Div}^0(K)}$ is non-empty. By the Subgroup Criterion, it suffices to show that $deg(D_1 \bullet (-D_2)) = 0$ for any D_1, $D_2 \in \widetilde{\mathrm{Div}^0(K)}$. Let $D_1 = (I_1, u)$, $D_2 = (I_2, v) \in \widetilde{\mathrm{Div}^0(K)}$. Set $u = (u_\sigma)_\sigma$, $v = (v_\sigma)_\sigma \in K_{\mathbb{R}}^\times$. We know that $-D_2 = (I_2^{-1}, (v_\sigma^{-1})_\sigma)$ and in terms of the corresponding oriented pairs, we have $D_1 \bullet (-D_2) = (I_1 I_2^{-1}, (u_\sigma v_\sigma^{-1})_\sigma)$ Define $|u| := (|u_\sigma|)_\sigma$ and $|v| := (|v_\sigma|)_\sigma$. By Proposition 2.2.3, we need to verify that

$$-\log\left(N(I_1 I_2^{-1}) \cdot |\mathcal{N}(|uv^{-1}|)|\right) = 0$$

Note that by assumption, we have:

$$-\log\left(N(I_1) \cdot |\mathcal{N}(|u|)|\right) = 0$$

and

$$-\log\left(N(I_2) \cdot |\mathcal{N}(|v|)|\right) = 0$$

Recall that $\mathcal{N}$ is a multiplicative function and we compute:

$$\begin{aligned}
-\log\left(N(I_1I_2^{-1})\cdot|\mathcal{N}(|uv^{-1}|)|\right) &= -\log\left(N(I_1)N(I_2^{-1}))\cdot|\mathcal{N}(|u|)|\mathcal{N}(|v^{-1}|)|\right)\\
&= -\log\left(N(I_1)|\mathcal{N}(|u|)|\cdot N(I_2^{-1})|\mathcal{N}(|v^{-1}|)|\right)\\
&= -\log\left(N(I_1)|\mathcal{N}(|u|)|\right)-\log\left(\frac{1}{N(I_2)}\frac{1}{|\mathcal{N}(|v|)|}\right)\\
&= -\log(1)+\log\left(N(I_2)\cdot|\mathcal{N}(|v|)|\right)\\
&= 0
\end{aligned}$$

□

Proposition 2.3.4. $\widetilde{\mathrm{PDiv}(K)}$ *is a subgroup of* $\widetilde{\mathrm{Div}^0(K)}$.

Proof. Let $f,\, g \in K^\times$ such that $(f) = (f^{-1}\mathbb{Z}_K, (\sigma(f))_\sigma)$, $(g) = (g^{-1}\mathbb{Z}_K, (\sigma(g))_\sigma) \in \widetilde{\mathrm{PDiv}(K)}$. By the Subgroup Criterion and Proposition 2.3.2, it suffices to show that $(f)\bullet(-(g))$ is a principal oriented Arakelov divisor of K. First, observe that

$$\begin{aligned}
-(g) &= (g\mathbb{Z}_K, ([\sigma(g)]^{-1})_\sigma)\\
&= (g\mathbb{Z}_K, (\sigma(g^{-1}))_\sigma) \text{ as each } \sigma \text{ is a homomorphism}\\
&= (g^{-1})
\end{aligned}$$

Then,

$$(f)\bullet(-(g)) = (f)\bullet(g^{-1}) = (f^{-1}\mathbb{Z}_K g\mathbb{Z}_K, [\sigma(f)\sigma(g^{-1})]_\sigma) = (f^{-1}g\mathbb{Z}_K, (\sigma(fg^{-1}))_\sigma)$$

Hence $(f)\bullet(-(g)) = (gf^{-1}\mathbb{Z}_K, (\sigma(fg^{-1}))_\sigma)) = (fg^{-1})$ is a principal oriented Arakelov divisor of K. □

We are now ready to define the oriented Arakelov class group of the number field K:

Definition 2.3.4. The **oriented Arakelov class group of** K (**Picard group of** K) is the quotient of $\widetilde{\mathrm{Div}^0(K)}$ by its subgroup $\widetilde{\mathrm{PDiv}(K)}$.

Notation 2.3.3. The oriented Arakelov class group of K will be denoted by $\widetilde{\mathrm{Pic}^0(K)}$.

2.4 The exactness and the commutativity of the diagram

Recall that the main aim of this chapter is to prove exactness and the commutativity of the diagram that is introduced at the beginning of this chapter. In order to understand that the sequence that is in the first row of this diagram is exact, we start with the following definition:

Definition 2.4.1. Let α be an element in $\mathbb{Z}_K$. We say that α is **totally positive** if its image under all real infinite primes of K is positive.

Example 2.4.1. Let $K = \mathbb{Q}(\sqrt{2})$ so that $\mathbb{Z}_K = \mathbb{Z}[\sqrt{2}]$. Denote the two real infinite primes of K as in Example 2.1.1. Then the element $\alpha = 2 + \sqrt{2} \in \mathbb{Z}_K$ is totally positive as $\sigma_1(\alpha) = 2 + \sqrt{2} > 0$ and $\sigma_2(\alpha) = 2 - \sqrt{2} > 0$. On the other hand the element $\alpha' = 1 + \sqrt{2} \in \mathbb{Z}_K$ is not totally positive as $\sigma_2(\alpha') = 1 - \sqrt{2} < 0$.

Remark 2.4.1. For any number field L, the set of totally positive elements in $\mathbb{Z}_L$ is non-empty as $\mathbb{Z} \subseteq \mathbb{Z}_L$ and all positive integers are totally positive because the infinite primes of L fix rational numbers. In particular, they fix integers.

Notation 2.4.1. Denote the set of all totally positive elements in $\mathbb{Z}_K$ by $\mathbb{Z}_{K,+}$ and the set of totally positive elements which are invertible in $\mathbb{Z}_K$ by $\mathbb{Z}^\times_{K,+}$.

Note that by definition we have $\mathbb{Z}^\times_{K,+} \subseteq \mathbb{Z}^\times_K$ and $\mathbb{Z}^\times_K$ is a multiplicative abelian group. The same fact holds for the set $\mathbb{Z}^\times_{K,+}$ and the usual multiplication:

Proposition 2.4.1. *$\mathbb{Z}^\times_{K,+}$ is a subgroup of $\mathbb{Z}^\times_K$ under multiplication.*

Proof. Let $\alpha, \beta \in \mathbb{Z}^\times_{K,+}$, we then have $\sigma_i(\alpha) > 0$ and $\sigma_i(\beta) > 0$ for all $i \in \{1, 2, \ldots, r_1\}$. Therefore, $\sigma_i(\alpha)\sigma_i(\beta) = \sigma_i(\alpha\beta) > 0$. Since the multiplication of two units generates another unit in $\mathbb{Z}_K$, we deduce that this set is closed under multiplication. Observe also that we have $\sigma_i(\alpha^{-1}) = \sigma_i(\alpha)^{-1} > 0$ for any $i \in \{1, 2, \ldots, r_1\}$. Combined with the fact that the inverse α^{-1} of α is again a unit in $\mathbb{Z}_K$, this set is also closed under inversion. □

Observation 2.4.1. By construction, the following sequence is exact:

$$1 \longrightarrow \mathbb{Z}^\times_{K,+} \xrightarrow{\textbf{inc}} K^\times \xrightarrow{\textbf{p}} K^\times/\mathbb{Z}^\times_{K,+} \longrightarrow 1$$

where the map **inc** denotes the natural inclusion and **p** is the natural projection.

We now introduce the following map with the aim of relating totally positive units of $\mathbb{Z}_K$ and $K_{\mathbb{R}}$:

$$\begin{aligned} \iota : \mathbb{Z}_K &\to K_{\mathbb{R}} \\ \alpha &\mapsto (\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_{r_1+r_2}(\alpha)) \end{aligned}$$

Note that the map ι is actually a group homomorphism as the infinite primes of K are homomorphisms. We will show that ι preserves units and total positivity: Let $\alpha \in \mathbb{Z}_K^{\times}$. Then we know that $N_{K/\mathbb{Q}}(\alpha) = \pm 1$ which implies that $\sigma_i(\alpha) \neq 0$ for all $i \in \{1, 2, \ldots, r_1 + r_2\}$. By Proposition 2.2.1, we have that $\iota(\alpha) \in K_{\mathbb{R}}^{\times}$. Now, let $\beta \in \mathbb{Z}_{K,+}$. Then, we know that $\sigma_i(\beta) > 0$ for all $i \in \{1, 2, \ldots, r_1\}$. It follows that $sign(\iota(\beta)) = (1, 1 \ldots, 1)$ and therefore $\iota(\beta) \in K_{\mathbb{R}}^{\times}$. This shows that the homomorphism ι induces a homomorphism

$$\mathbb{Z}_{K,+}^{\times} \to K_{\mathbb{R},+}^{\times}$$

Given any $\alpha \in \mathbb{Z}_K$, observe that:

$$\begin{aligned} \mathcal{N}(\iota(\alpha)) &= \mathcal{N}((\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_{r_1+r_2}(\alpha))) \\ &= \left(\prod_{i=1}^{r_1} \sigma_i(\alpha) \right) \cdot \left(\prod_{j=r_1+1}^{r_2} |\sigma_j(\alpha)|^2 \right) \\ &= N_{K/\mathbb{Q}}(\alpha) \end{aligned}$$

In particular, if $\alpha \in \mathbb{Z}_{K,+}^{\times}$, then we have

$$\mathcal{N}(\iota(\alpha)) = N_{K/\mathbb{Q}}(\alpha) = 1$$

and therefore $\iota(\alpha) \in (K_{\mathbb{R},+}^{\times})^0$ so ι induces the following homomorphism of abelian groups:

$$\begin{aligned} \tilde{\iota} : \mathbb{Z}_{K,+}^{\times} &\to (K_{\mathbb{R},+}^{\times})^0 \\ \alpha &\mapsto (\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_{r_1+r_2}(\alpha)) \end{aligned}$$

Clearly, $\tilde{\iota}$ is injective as each infinite prime of K is by definition an embedding of K onto either $\mathbb{R}$ or $\mathbb{C}$ and therefore an injective homomorphism.

Proposition 2.4.2. *The sequence*

$$1 \longrightarrow (K_{\mathbb{R},+}^{\times})^0 \xrightarrow{\phi} \widetilde{\mathrm{Div}^0(K)} \xrightarrow{\psi} Id(K) \times \{\pm 1\}^{r_1} \longrightarrow 1$$

is split exact where

$$\phi : (u_\sigma)_\sigma \mapsto (\mathbb{Z}_K, (u_\sigma)_\sigma)$$

and

$$\psi : D = (I, (x_\sigma)_\sigma) \mapsto (I, (sign(x_\sigma))_{\sigma:real})$$

Proof. We need to check that ϕ is well-defined: Let $(u_\sigma)_\sigma \in (K_{\mathbb{R},+}^{\times})^0$. Then for each infinite prime σ, the coefficient u_σ is non-zero which implies that $u := (u_\sigma)_\sigma \in \prod_\sigma K_\sigma^{\times}$ and therefore $(\mathbb{Z}_K, u) \in \widetilde{\mathrm{Div}(K)}$. We also know that $\mathcal{N}(u) = 1$ so

$$N(\mathbb{Z}_K)|\mathcal{N}(|u|)| = |\mathcal{N}(u)| = 1 \text{ as } N(\mathbb{Z}_K) = 1 \text{ and } u \in K_{\mathbb{R},+}$$

which shows that $(\mathbb{Z}_K, u) \in \widetilde{\mathrm{Div}^0(K)}$. Clearly, ϕ is a homomorphism as $\mathbf{1} := (1, 1, \ldots, 1) \in (K_{\mathbb{R},+}^{\times})^0$ with

$$\phi(\mathbf{1}) = (\mathbb{Z}_K, \mathbf{1}) = D_{Id}$$

and for $u = (u_\sigma)_\sigma$, $v = (v_\sigma)_\sigma$,

$$\begin{aligned}
\phi(uv) &= \phi((u_\sigma v_\sigma)_\sigma) \\
&= (\mathbb{Z}_K, (u_\sigma v_\sigma)_\sigma) \\
&= (\mathbb{Z}_K, (u_\sigma)_\sigma)(\mathbb{Z}_K, (v_\sigma)_\sigma) \\
&= \phi(u)\phi(v)
\end{aligned}$$

Now we prove that ϕ is injective. We have:

$$\begin{aligned}
u = (u_\sigma)_\sigma \in \ker\phi &\iff \phi(u) = (\mathbb{Z}_K, (u_\sigma)_\sigma) = (\mathbb{Z}_K, 1) \\
&\iff u_\sigma = 1 \text{ for each infinite prime } \sigma \\
&\iff u = 1
\end{aligned}$$

Now we determine the image of ϕ:

$$\mathrm{Im}\phi = \{(\mathbb{Z}_K, (u_\sigma)_\sigma) : (u_\sigma)_\sigma \in (K_{\mathbb{R},+}^{\times})^0\}$$

Note that since $(u_\sigma)_\sigma \in (K^\times_{\mathbb{R},+})^0$, we have $(u_\sigma)_\sigma \in K^\times_{\mathbb{R},+}$ but this holds if and only if $sign(u_\sigma) > 0$ for each real infinite prime σ of K and $u_\sigma \neq 0$ for all infinite primes σ of K. Therefore, $(u_\sigma)_\sigma \in K^\times_{\mathbb{R},+}$ if and only if $u_\sigma \in R_+$ for real infinite primes of K and $u_\sigma \in \mathbb{C}^\times$, otherwise. Combining, we deduce that $\mathrm{Im}\phi \cong (\mathbb{R}_+)^{r_1} \times (\mathbb{C}^\times)^{r_2}$. Now we concentrate on the map ψ which is clearly well-defined. We show that ψ is a homomorphism: We have $\psi(\mathbb{Z}_K, 1) = (\mathbb{Z}_K, , (1, 1, \ldots, 1)) \in Id(K) \times \{\pm 1\}^{r_1}$ and

$$\begin{aligned}
\psi((I_1, u)(I_2, v)) &= \psi((I_1 I_2, uv)) \\
&= (I_1 I_2, (sign(u_\sigma v_\sigma))_{\sigma:\text{real}}) \\
&= (I_1 I_2, (sign(u_\sigma))_{\sigma:\text{real}}(sign(v_\sigma))_{\sigma:\text{real}}) \\
&= (I_1, (sign(u_\sigma))_{\sigma:\text{real}})(I_2, (sign(v_\sigma))_{\sigma:\text{real}}) \\
&= \psi(u)\psi(v)
\end{aligned}$$

for all (I_1, u), $(I_2, v) \in \widetilde{\mathrm{Div}^0(K)}$ with $u = (u_\sigma)_\sigma$ and $v = (v_\sigma)_\sigma$. Now we prove that ψ is surjective. For $(I, (u_i)_{i=1}^{r_1}) \in Id(K) \times \{\pm 1\}^{r_1}$, we claim that $\psi(I, u) = (I, (u_i)_{i=1}^{r_1})$ where $u = \big(\frac{u_1}{\sqrt[r_1]{N(I)}}, \frac{u_2}{\sqrt[r_1]{N(I)}}, \ldots, \frac{u_{r_1}}{\sqrt[r_1]{N(I)}}, 1, 1, \ldots, 1\big)$. First, we check that $(I, u) \in \widetilde{\mathrm{Div}^0(K)}$. It suffices to show that $u \in K^\times_{\mathbb{R}}$ and $deg((I, u)) := deg((I, |u|)) = 0$. Since $(u_i)_{i=1}^{r_1} \in \{\pm 1\}^{r_1}$, we have $u_i \neq 0$ for all $i \in \{1, 2, \ldots, r_1\}$ and since $N(I) \neq 0$ we have that $u \in K^\times_{\mathbb{R}}$. Now observe that

$$|u| = \left(\frac{1}{\sqrt[r_1]{N(I)}}, \frac{1}{\sqrt[r_1]{N(I)}}, \ldots, \frac{1}{\sqrt[r_1]{N(I)}}, 1, 1, \ldots, 1\right)$$

and

$$\begin{aligned}
N(I)|\mathcal{N}(|u|)| &= N(I)\left|\left(\prod_{i=1}^{r_1} \frac{1}{\sqrt[r_1]{N(I)}}\right) \cdot \left(\prod_{j=1}^{r_2} 1\right)\right| \\
&= N(I) \cdot \frac{1}{N(I)} \\
&= 1
\end{aligned}$$

which shows that $deg(I, u) = 0$ and we have

$$\psi(I, u) = (I, (sign\Big(\frac{u_i}{\sqrt[r_1]{N(I)}}\Big))_{i=1}^{r_1}) = (I, (u_i)_{i=1}^{r_1})$$

Finally, we determine

$$\ker \psi = \{(I, u) \in \widetilde{\mathrm{Div}^0(K)} : \psi(I, u) = (\mathbb{Z}_K, sign(u)) = (\mathbb{Z}_K, 1)\}$$

Observe that $(I,u) \in \ker\psi$ if and only if $(I,u) \in \widetilde{\mathrm{Div}^0(K)}$ and $u_\sigma \in \mathbb{R}_+$ for each real infinite of K. By definition, we have $u_\sigma \in \mathbb{C}^\times$ for complex infinite primes. Therefore $\ker\psi \cong (\mathbb{R}_+)^{r_1} \times (\mathbb{C}^\times)^{r_2}$. Since ϕ is injective, ψ is surjective and

$$\mathrm{Im}\phi \cong (\mathbb{R}_+)^{r_1} \times (\mathbb{C}^\times)^{r_2} \cong \ker\psi,$$

this sequence is exact. Now we prove that this short exact sequence splits. By the Splitting Lemma, it suffices to find a homomorphism $\mathbf{s}: \ Id(K)\times\{\pm1\}^{r_1} \to \widetilde{\mathrm{Div}^0(K)}$ such that $\psi \circ \mathbf{s}$ is the identity map on $Id(K) \times \{\pm1\}^{r_1}$. We claim that the map

$$\begin{array}{rcl} \mathbf{s} : Id(K) \times \{\pm1\}^{r_1} & \to & \widetilde{\mathrm{Div}^0(K)} \\ (I,(\zeta_1,\zeta_2,\ldots,\zeta_{r_1})) & \mapsto & \left(I, \left(\frac{\zeta_1}{\sqrt[r_1]{N(I)}}, \ldots, \frac{\zeta_{r_1}}{\sqrt[r_1]{N(I)}}, 1, 1 \ldots, 1\right)\right) \end{array}$$

works. Indeed, for any $(I,(\zeta_1,\zeta_2,\ldots,\zeta_{r_1})) \in Id(K) \times \{\pm1\}^{r_1}$, we have:

$$\begin{aligned} (\psi\circ\mathbf{s})(I,(\zeta_1,\zeta_2,\ldots,\zeta_{r_1})) &= \psi\left(I, \left(\frac{\zeta_1}{\sqrt[r_1]{N(I)}}, \ldots, \frac{\zeta_{r_1}}{\sqrt[r_1]{N(I)}}, 1, 1 \ldots, 1\right)\right) \\ &= \left(I, \left(sign\left(\frac{\zeta_1}{\sqrt[r_1]{N(I)}}\right), \ldots, sign\left(\frac{\zeta_{r_1}}{\sqrt[r_1]{N(I)}}\right)\right)\right) \\ &= (I,(\zeta_1,\zeta_2,\ldots,\zeta_{r_1})) \end{aligned}$$

□

Observation 2.4.2. By Proposition 2.4.2, we now know that

$$\widetilde{\mathrm{Div}^0(K)} \cong (K^\times_{\mathbb{R},+})^0 \otimes (Id(K) \times \{\pm1\}^{r_1})$$

Below we explain a way to decompose any element of $\widetilde{\mathrm{Div}^0(K)}$ into $(K^\times_{\mathbb{R},+})^0 \otimes (Id(K) \times \{\pm1\}^{r_1})$. Let $(I,(\alpha_1,\alpha_2,\ldots,\alpha_{r_1+r_2})) \in \widetilde{\mathrm{Div}^0(K)}$. We set $\alpha := (\alpha_1,\alpha_2,\ldots,\alpha_{r_1+r_2})$. We know that $N(I)\mathcal{N}(|\alpha|) = 1$. The element

$$\beta := (|\alpha_1| \sqrt[r_1]{N(I)}, |\alpha_2| \sqrt[r_1]{N(I)}, \ldots, |\alpha_{r_1}| \sqrt[r_1]{N(I)}, \alpha_{r_1+1}, \ldots, \alpha_{r_1+r_2}) \in (K^\times_{\mathbb{R},+})^0$$

because

$$\begin{aligned}\mathcal{N}(\beta) &= \left(\prod_{i=1}^{r_1}|\alpha_i|\sqrt[r_1]{N(I)}\right)\cdot\left(\prod_{j=1}^{r_2}|\alpha_{r_1+j}|^2\right)\\ &= N(I)\cdot\left(\prod_{i=1}^{r_1}|\alpha_i|\right)\cdot\left(\prod_{j=1}^{r_2}|\alpha_{r_1+j}|^2\right)\\ &= N(I)\mathcal{N}(|\alpha|)\\ &= 1,\end{aligned}$$

$|\alpha_i| > 0$ for all $i \in \{1, 2, \ldots, r_1\}$ and $\alpha_{r_1+j} \neq 0$ for all $j \in \{1, 2, \ldots, r_2\}$. Observe also that $(I, (sign(\alpha_1), \ldots, sign(\alpha_{r_1}))) \in Id(K)\times\{\pm 1\}^{r_1}$. Therefore (I, α) is decomposed as:

$$\left[(|\alpha_1|\sqrt[r_1]{N(I)}, |\alpha_2|\sqrt[r_1]{N(I)}, \ldots, |\alpha_{r_1}|\sqrt[r_1]{N(I)}, \alpha_{r_1+1}, \ldots, \alpha_{r_1+r_2}), (I, (sign(\alpha_1), \ldots, sign(\alpha_{r_1})))\right]$$

Lemma 2.4.3. *The map*

$$\begin{aligned}\beta : K^\times &\to \widetilde{\mathrm{Div}^0(K)}\\ f &\mapsto (\tilde{f})\end{aligned}$$

is an injective group homomorphism.

Proof. The fact that β is a homomorphism is clear. We prove that β is injective. Let f, $g \in K^\times$ such that $(\tilde{f}) = (\tilde{g})$. Then $(f^{-1}\mathbb{Z}_K, (\sigma(f))_\sigma) = (g^{-1}\mathbb{Z}_K, (\sigma(g))_\sigma)$ which implies that $\sigma(f) = \sigma(g)$ for all infinite primes σ of K. Therefore $f = g$ as infinite primes are injective. Hence the map β is injective. □

Lemma 2.4.4. *The map*

$$\begin{aligned}\gamma : K^\times/\mathbb{Z}_{K,+}^\times &\to Id(K)\times\{\pm 1\}^{r_1}\\ [f] &\mapsto (f^{-1}\mathbb{Z}_K, (sign(\sigma(f)))_{\sigma:\ real})\end{aligned}$$

is an injective group homomorphism.

Proof. First we prove that γ is well-defined: Let $[f] = [g]$ in $K^\times/\mathbb{Z}_{K,+}^\times$. Then there

exists a totally positive unit $u \in \mathbb{Z}_{K,+}^{\times}$ such that $g = f \cdot u$. We have:

$$\begin{aligned}
\gamma([g]) &= \gamma([f \cdot u]) \\
&= (u^{-1} f^{-1} \mathbb{Z}_K, (sign(\sigma(fu)))_{\sigma:\text{ real}}) \\
&= (f^{-1}\mathbb{Z}_K, (sign(\sigma(fu)))_{\sigma:\text{ real}}) \text{ as } u \in \mathbb{Z}_K^{\times} \\
&= (f^{-1}\mathbb{Z}_K, (sign(\sigma(f)\sigma(u)))_{\sigma:\text{ real}}) \text{ as each } \sigma \text{ is a homomorphism} \\
&= (f^{-1}\mathbb{Z}_K, (sign(\sigma(f)))_{\sigma:\text{ real}}) \text{ as } u \text{ is totally positive} \\
&= \gamma([f])
\end{aligned}$$

Clearly, σ is a group homomorphism as:

$$\begin{aligned}
\gamma([f_1][f_2]) &= ((f_1 f_2)^{-1}\mathbb{Z}_K, (sign(\sigma(f_1 f_2)))_{\sigma:\text{ real}}) \\
&= (f_1^{-1} f_2^{-1}\mathbb{Z}_K, (sign(\sigma(f_1)))_{\sigma:\text{ real}}(sign(\sigma(f_2)))_{\sigma:\text{ real}}) \\
&= (f_1^{-1}\mathbb{Z}_K, (sign(\sigma(f_1)))_{\sigma:\text{ real}})(f_2^{-1}\mathbb{Z}_K, (sign(\sigma(f_2)))_{\sigma:\text{ real}}) \\
&= \gamma([f_1])\gamma([f_2])
\end{aligned}$$

for any $[f_1], [f_2] \in K^{\times}/\mathbb{Z}_{K,+}^{\times}$ and $\gamma([1]) = (\mathbb{Z}_K, (1, 1, \ldots, 1))$. Now we prove the injectivity of γ. Let $[f]$, $[g] \in K^{\times}/\mathbb{Z}_{K,+}^{\times}$ such that $\gamma([f]) = \gamma([g])$. Then

$$(f^{-1}\mathbb{Z}_K, (sign(\sigma(f)))_{\sigma:\text{ real}}) = (g^{-1}\mathbb{Z}_K, (sign(\sigma(g)))_{\sigma:\text{ real}}),$$

which implies that $f^{-1}\mathbb{Z}_K = g^{-1}\mathbb{Z}_K$ in $Id(K)$ and $(sign(\sigma(f)))_{\sigma} = (sign(\sigma(g)))_{\sigma}$. The first one implies that $g^{-1} = f^{-1}u$ for some $u \in \mathbb{Z}_K^{\times}$ and the latter one implies that u is a totally positive element of $\mathbb{Z}_K$. Combining, we get $f = gu$ for some $u \in \mathbb{Z}_{K,+}^{\times}$ and therefore $[f] = [g]$ in $K^{\times}/\mathbb{Z}_{K,+}^{\times}$. □

Proposition 2.4.5. *The diagram*

$$\begin{array}{ccc}
\mathbb{Z}_{K,+}^{\times} & \xrightarrow{\boldsymbol{inc}} & K^{\times} \\
\downarrow{\scriptstyle \tilde{\iota}} & & \downarrow{\scriptstyle \beta} \\
(K_{\mathbb{R},+}^{\times})^0 & \xrightarrow{\phi} & \widetilde{\mathrm{Div}^0(K)}
\end{array}$$

is commutative.

Proof. Given $\alpha \in \mathbb{Z}_{K,+}^{\times}$, we have:

$$\begin{aligned}
\phi(\tilde{\iota}(\alpha)) &= \phi((\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_{r_1+r_2}(\alpha))) \\
&= (\mathbb{Z}_K, (\sigma(\alpha))_\sigma) \\
&= (\alpha^{-1}\mathbb{Z}_K, (\sigma(\alpha))_\sigma) \text{ as } \alpha^{-1} \in \mathbb{Z}_K^{\times} \\
&= \beta(\alpha) \\
&= \beta(\mathbf{inc}(\alpha)) \text{ as } \mathbf{inc}(\alpha) = \alpha
\end{aligned}$$

□

Proposition 2.4.6. *The diagram*

$$\begin{array}{ccc}
K^{\times} & \xrightarrow{\boldsymbol{p}} & K^{\times}/\mathbb{Z}_{K,+}^{\times} \\
\downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} \\
\widetilde{\mathrm{Div}^0(K)} & \xrightarrow{\psi} & Id(K) \times \{\pm 1\}^{r_1}
\end{array}$$

is commutative.

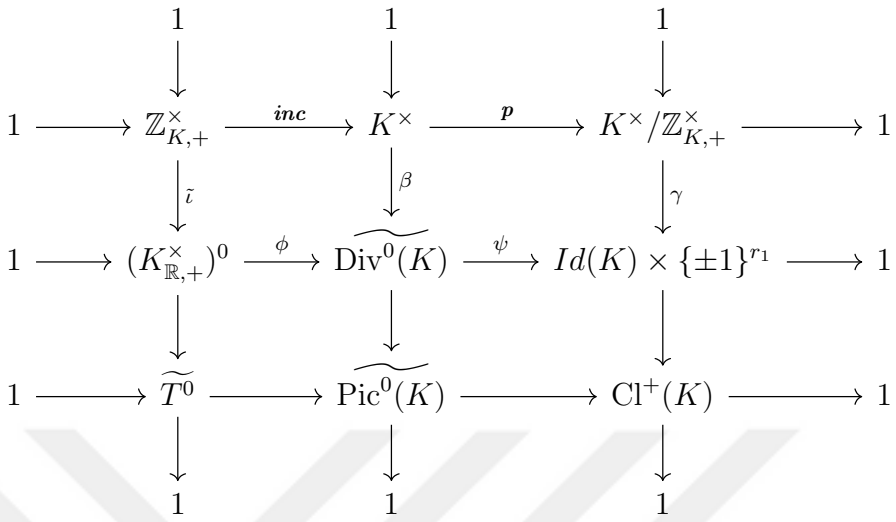
Proof. Let $f \in K^{\times}$. Then,

$$\begin{aligned}
\gamma(\mathbf{p}(f))) &= \gamma([f]) \\
&= (f^{-1}\mathbb{Z}_K, (sign(\sigma(f)))_{\sigma\text{: real}}) \\
&= \psi\big((\tilde{f})\big) \\
&= \psi(\beta(f))
\end{aligned}$$

□

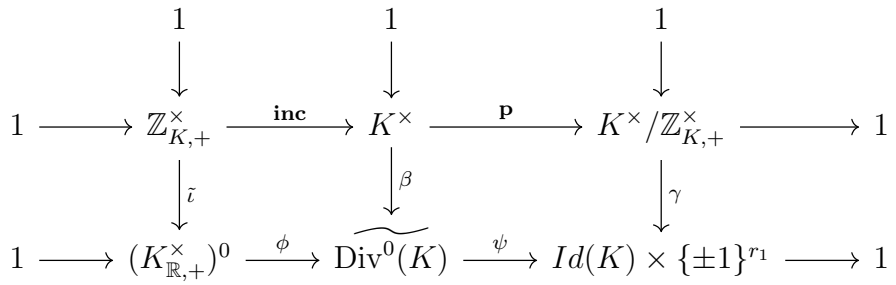
We may now state and prove our main theorem:

Theorem 2.4.7. *The following commutative diagram*



has exact rows and columns where $\widetilde{T^0} := (K^{\times}_{\mathbb{R},+})^0/\mathbb{Z}^{\times}_{K,+}$ *and* $\mathrm{Cl}^+(K)$ *denotes the narrow class group of* K*.*

Proof. By Lemma 2.4.3, Lemma 2.4.4, Observation 2.4.1, Proposition 2.4.2, Proposition 2.4.5, Proposition 2.4.6 and since we explained that $\tilde{\iota}$ is injective, we have the following commutative diagram with exact rows and columns:



Then the exactness of the main diagram follows from Snake Lemma and the commutativity of the main diagram follows from Propositions 2.4.5 and 2.4.6 combined with the fact that commutativity of the diagram is a functorial property. □

Chapter 3

BINARY QUADRATIC FORMS

In this chapter we first define the fundamental properties of an integral binary quadratic form such as its discriminant and content. We then observe that the modular group acts naturally on the set of integral binary quadratic forms, and study the invariants of the equivalence classes that arise from this action. Next, we restrict our attention to indefinite binary quadratic forms and discuss their reduction theory. Finally, we determine the automorphism group of integral primitive indefinite binary quadratic forms.

3.1 Basic Notions

Definition 3.1.1. A binary quadratic form is a degree two homogeneous polynomial in two variables and with real coefficients. In other words, **a binary quadratic form** is a polynomial of the form

$$f(X,Y) = aX^2 + bXY + cY^2$$

where a, b and c are real numbers.

Notation 3.1.1. For simplicity, the binary quadratic form $f(X,Y) = aX^2+bXY+cY^2$ will be denoted by $f = (a,b,c)$.

Remark 3.1.1. Observe that a binary quadratic form $f = (a,b,c)$ can be represented by the following manner:

$$f(X,Y) = \begin{pmatrix} X & Y \end{pmatrix} \times \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \times \begin{pmatrix} X \\ Y \end{pmatrix}$$

Notation 3.1.2. For the binary quadratic form $f = (a,b,c)$, the matrix $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ will be denoted by M_f.

Example 3.1.1. The polynomials $f(X,Y) = X^2 - XY - Y^2 = (1,-1,-1)$ and $f(X,Y) = X^2 - 5Y^2 = (1,0,-5)$ are binary quadratic forms.

Definition 3.1.2. Let $f = (a,b,c)$ be a binary quadratic form. The quantity b^2-4ac is called **the discriminant of** f which is denoted by Δ_f.

Example 3.1.2. For $f = (1,-1,-1)$, $\Delta_f = (-1)^2 - 4 \times 1 \times (-1) = 5$.

Definition 3.1.3. We say that a binary quadratic form $f = (a,b,c)$ is **indefinite** if f takes on both positive and negative values.

Example 3.1.3. The binary quadratic form $f = (1,-1,-1)$ is indefinite as $f(1,0) = 1$ is positive and $f(0,1) = -1$ is negative.

Proposition 3.1.1. *A binary quadratic form $f = (a,b,c)$ whose discriminant is not a perfect square is indefinite if and only if its discriminant Δ_f is positive.*

Proof. Let $f = (a,b,c)$ be a binary quadratic form whose discriminant is not a perfect square. Then $a \neq 0$ and f takes on both positive and negative values so there exists $(x_0,y_0) \neq (0,0) \in \mathbb{R}^2$ such that $f(x_0,y_0) = ax_0^2 + bx_0y_0 + cy_0^2 > 0$. Similary, we know that there exists a point $(x_1,y_1) \neq (0,0) \in \mathbb{R}^2$ such that $f(x_1,y_1) = ax_1^2 + bx_1y_1 + cy_1^2 < 0$. Observe that

$$ax_0^2 + bx_0y_0 + cy_0^2 = ay_0^2\left[\left(\frac{x_0}{y_0}\right)^2 + \frac{b}{a}\left(\frac{x_0}{y_0}\right) + \frac{c}{a}\right]$$

and that

$$ax_1^2 + bx_1y_1 + cy_1^2 = ay_1^2\left[\left(\frac{x_1}{y_1}\right)^2 + \frac{b}{a}\left(\frac{x_1}{y_1}\right) + \frac{c}{a}\right].$$

Set $X_0 := \frac{x_0}{y_0}$ and $X_1 := \frac{x_1}{y_1}$. Completing the square by adding $(\frac{b}{2a})^2$, we get

$$f(x_0,y_0) = ay_0^2\left[\left(X_0 + \frac{b}{2a}\right)^2 - \frac{b^2-4ac}{4a^2}\right] > 0$$

and

$$f(x_1,y_1) = ay_1^2\left[\left(X_1 + \frac{b}{2a}\right)^2 - \frac{b^2-4ac}{4a^2}\right] < 0$$

Notice that $b^2 - 4ac = \Delta_f$. If a is a positive number, then we have that

$$\left(X_1 + \frac{b}{2a}\right)^2 - \frac{\Delta_f}{4a^2} < 0$$

as y_1^2 is always non-negative which implies that $(X_1 + \frac{b}{2a})^2 < \frac{\Delta_f}{4a^2}$. Clearly, the left hand side of the latter inequality is non-negative, also so is the constant $4a^2$. Therefore, Δ_f is a positive number. Similarly if a is a negative number, then we have $(X_0 + \frac{b}{2a})^2 - \frac{\Delta_f}{4a^2} < 0$ which is the same as $(X_0 + \frac{b}{2a})^2 < \frac{\Delta_f}{4a^2}$. Again, we conclude that $\Delta_f > 0$. Now, assume that $\Delta_f = b^2 - 4ac$ is positive and not a perfect-square. Then a and c are nonzero. Observe that

$$f(1,0)\dot{f}(b,-2a) = (-a^2)\dot{(}b^2 - 4ac) = -a^2\Delta_f$$

is negative which shows that $f(1,0)$ and $f(b,-2a)$ have opposite sign. Therefore, we see that the form f is indefinite. □

Definition 3.1.4. The binary quadratic form $f = (a,b,c)$ is called **integral** if the coefficients a, b and c are integers.

Definition 3.1.5. Let $f = (a,b,c)$ be an integral binary quadratic form. The **content of** f, $cont(f)$, is defined as $\gcd(a,b,c)$.

Definition 3.1.6. Let f be an integral binary quadratic form. We say that the form f is **primitive** if $cont(f) = 1$.

Example 3.1.4. The form $f = (1,-1,-1)$ is an integral primitive binary quadratic form.

Proposition 3.1.2. *Let $f = (a,b,c)$ be an integral indefinite binary quadratic form. Then the discriminant of f, Δ_f, is a perfect square if and only if there exists a point $(x_0,y_0) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ such that $f(x_0,y_0) = 0$.*

Proof. Let $f = (a,b,c)$ be an integral indefinite binary quadratic form. First, observe that if $a = 0$, then $\Delta_f = b^2$ is a perfect square and

$$f(X,Y) = bXY + CY^2 = Y(bX + cY)$$

which implies that $f(1,0) = 0$. From now on, we assume that $a \neq 0$. Suppose that

$\Delta_f = d^2$ for some integer d. Observe that

$$\begin{aligned} 4af(X,Y) &= 4a^2X^2 + 4abXY + 4acY^2 \\ &= 4a^2X^2 + 4abXY + 4acY^2 + b^2Y^2 - b^2Y^2 \\ &= 4a^2X^2 + 4abXY + b^2Y^2 - (b^2 - 4ac)Y^2 \\ &= (2aX + bY)^2 - d^2Y^2 \end{aligned}$$

Therefore, $f(X,Y) = \frac{(2aX+Y(b-d))(2aX+Y(b+d))}{4a}$ and we have $f(b-d,-2a) = 0$. Since a, b and d are integers and $a \neq 0$, we have $(b-d,-2a) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ and we are done. Conversely, let $(x_0,y_0) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ such that $f(x_0,y_0) = 0$. Observe that $f(x_0,0) = ax_0^2 \neq 0$ as $a \neq 0$ and $x_0 \neq 0$. Then we obtain that $y_0 \neq 0$ because otherwise it would contradict the fact that $f(x_0,y_0) = f(x_0,0) = 0$. Since $4af(X,Y) = (2aX+bY)^2 - \Delta_f Y^2$ and $f(x_0,y_0) = 0$ we have that $\Delta_f = (\frac{2ax_0+by_0}{y_0})^2$. Clearly, since f is an integral form, $\Delta_f \in \mathbb{Z}$. It follows that $\frac{2ax_0+by_0}{y_0} \in \mathbb{Z}$. Thus Δ_f is a perfect square. □

3.2 Action of $\mathrm{GL}_2(\mathbb{Z})$

From now on, we restrict our attention to integral primitive binary quadratic forms whose discriminants are not perfect squares. Throughout this section, $f = (a,b,c)$ is an integral binary quadratic form such that Δ_f is not a perfect square, unless otherwise stated.

Observation 3.2.1. Let $U = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ be a matrix in $\mathrm{GL}_2(\mathbb{Z})$. By using the entries of the matrix U and the form f, we may generate a new binary quadratic form:

$$\begin{aligned} f(pX+qY, rX+sY) &= a(pX+qY)^2 + b(pX+qY)(rX+sY) + c(rX+sY)^2 \\ &= (f(p,r), 2(apq+crs) + b(ps+qr), f(q,s)) \end{aligned}$$

Notation 3.2.1. The binary quadratic form $f(pX+qY, rX+sY)$ will be denoted by $f(U(X,Y))$.

Proposition 3.2.1. *Let $\mathscr{F}$ be the set of all integral primitive binary quadratic forms. Then the map*

$$\mathscr{F} \times \mathrm{GL}_2(\mathbb{Z}) \to \mathscr{F}$$
$$(f(X,Y), U) \mapsto (fU)(X,Y) := (\det(U))f(U(X,Y))$$

defines an action of the group $\mathrm{GL}_2(\mathbb{Z})$ *on the set* $\mathscr{F}$.

Proof. Let $f = (a,b,c)$ be any integral primitive binary quadratic form. Denote the 2×2 identity matrix by I_2. By construction, we have that

$$\begin{aligned}(fI_2)(X,Y) &= \det(I_2)f(1X + 0Y, 0X + 1Y)\\ &= f(X,Y)\end{aligned}$$

Also, if $U = \begin{pmatrix} p_1 & q_1 \\ r_1 & s_2 \end{pmatrix}$ and $V = \begin{pmatrix} p_2 & q_2 \\ r_2 & s_2 \end{pmatrix}$ are two different elements of $\mathrm{GL}_2(\mathbb{Z})$, we need to show that $((fU)V)(X,Y) = (f(UV))(X,Y)$. Note that $UV = \begin{pmatrix} p_1p_2 + q_1r_2 & p_1q_2 + q_1s_2 \\ p_2r_1 + r_2s_1 & q_2r_1 + s_1s_2 \end{pmatrix}$ and $\det(UV) = \det(U)\det(V)$. We know that

$$\begin{aligned}fU &:= (a',b',c')\\ &= (\det(U))(f(p_1,r_1), 2(ap_1q_1 + cr_1s_1) + b(p_1s_1 + q_1r_1), f(q_1,s_1))\end{aligned}$$

which implies that

$$\begin{aligned}a' &= \det(U)(ap_1^2 + bp_1r_1 + cr_1^2)\\ b' &= \det(U)[2(ap_1q_1 + cr_1s_1) + b(p_1s_1 + q_1r_1)]\\ c' &= \det(U)(aq_1^2 + bq_1s_1 + cs_1^2)\end{aligned}$$

Set $(fU)V = (a'',b'',c'')$ and $f(UV) = (A,B,C)$. Then

$$\begin{aligned}a'' &= \det(V)(a'p_2^2 + b'p_2r_2 + c'r_2^2)\\ &= \det(U)\det(V)[p_2^2(ap_1^2 + bp_1r_1 + cr_1^2) + p_2r_2[2(ap_1q_1 + cr_1s_1) + b(p_1s_1 + q_1r_1)] +\\ &\quad r_2^2(aq_1^2 + bq_1s_1 + cs_1^2)]\\ &= \det(UV)f(p_1p_2 + q_1r_2, p_2r_1 + r_2s_1)\\ &= A\end{aligned}$$

$$
\begin{aligned}
b'' &= \det(V)[2(a'p_2q_2 + c'r_2s_2) + b'(p_2s_2 + q_2r_2)] \\
&= \det(U)\det(V)[2[(ap_1^2 + bp_1r_1 + cr_1^2)p_2q_2 + (aq_1^2 + bq_1s_1 + cs_1^2)r_2s_2] \\
&+ (2(ap_1q_1 + cr_1s_1) + b(p_1s_1 + q_1r_1))(p_2s_2 + q_2r_2)] \\
&= \det(UV)[2[a(p_1p_2 + q_1r_2)(p_1q_2 + q_1s_2) + c(p_2r_1 + r_2s_1)(q_2r_1 + s_1s_2)] \\
&+ b[(p_1p_2 + q_1r_2)(q_2r_1 + s_1s_2) + (p_1q_2 + q_1s_2)(p_2r_1 + r_2s_1)]] \\
&= B
\end{aligned}
$$

$$
\begin{aligned}
c'' &= \det(V)[a'q_2^2 + b'q_2s_2 + c's_2^2] \\
&= \det(U)\det(V)[q_2^2(ap_1^2 + bp_1r_1 + cr_1^2) + q_2s_2[2(ap_1q_1 + cr_1s_1) + b(p_1s_1 + q_1r_1)] \\
&+ s_2^2(aq_1^2 + bq_1s_1 + cs_1^2)] \\
&= \det(UV)f(p_1q_2 + q_1s_2, q_2r_1 + s_1s_s) \\
&= C
\end{aligned}
$$

Thus, $(fU)V = f(UV)$. □

Corollary 3.2.2. *The group $SL_2(\mathbb{Z})$ acts on integral primitive binary quadratic forms.*

Proof. The result follows from Proposition 3.2.1 and the fact that $\mathrm{SL}_2(\mathbb{Z}) \subseteq \mathrm{GL}_2(\mathbb{Z})$. □

Remark 3.2.1. Let $U = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ be a matrix in $\mathrm{SL}_2(\mathbb{Z})$ and $f = (a, b, c)$ be an integral primitive binary quadratic form. Clearly, the matrix $-U = \begin{pmatrix} -p & -q \\ -r & -s \end{pmatrix}$ is also an element of $\mathrm{SL}_2(\mathbb{Z})$. Observe that

$$
\begin{aligned}
(fU) &= (f(p, r), 2(apq + crs) + b(ps + qr), f(q, s)) \\
&= (f(-p, -r), 2(a(-p)(-q) + c(-r)(-s)) + b((-p)(-s) + (-q)(-r)), f(-q, -s)) \\
&= (f(-U))
\end{aligned}
$$

Hence the action of the matrix $-U$ on the form f is the same as the action of U which implies that we can actually identify these two matrices. Therefore, the group $PSL_2(\mathbb{Z})$ acts more naturally on the set $\mathscr{F}$ than $\mathrm{SL}_2(\mathbb{Z})$ does.

Observation 3.2.2. Let us find the relation between the matrices M_{fU} and M_f where $f = (a, b, c)$ is an integral primitive binary quadratic form and $U = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ be a matrix in $\mathrm{GL}_2(\mathbb{Z})$. We know that $(fU)(X, Y) = \det(U) f(pX + qY, rX + sY)$. So,

$$(fU)(X,Y) = \det(U) \begin{pmatrix} pX+qY & rX+sY \end{pmatrix} \times \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \times \begin{pmatrix} pX+qY \\ rX+sY \end{pmatrix}$$

which is equal to

$$\det(U) \begin{pmatrix} X & Y \end{pmatrix} \times \begin{pmatrix} p & r \\ q & s \end{pmatrix} \times \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \times \begin{pmatrix} p & q \\ r & s \end{pmatrix} \times \begin{pmatrix} X \\ Y \end{pmatrix}$$

Therefore, we have $M_{fU} = \det(U) U^T M_f U$.

Definition 3.2.1. We say that two binary quadratic forms f and g are **equivalent** if $g = fU$ for some $U \in \mathrm{GL}_2(\mathbb{Z})$. The $\mathrm{GL}_2(\mathbb{Z})$-orbit of the form f is called the **equivalence class of** f. In other words, the set

$$\{g \in \mathscr{F} : g = fU \text{ for some } U \in \mathrm{GL}_2(\mathbb{Z})\}$$

is called the **equivalence class of** f.

Definition 3.2.2. We say that two binary quadratic forms f and g are **properly equivalent** if $g = fU$ for some $U \in \mathrm{SL}_2(\mathbb{Z})$. The $\mathrm{SL}_2(\mathbb{Z})$-orbit of the form f is called the **proper equivalence class of** f. In other words, the set

$$\{g \in \mathscr{F} : g = fU \text{ for some } U \in \mathrm{SL}_2(\mathbb{Z})\}$$

is called the **proper equivalence class of** f.

Now, we will introduce some invariants of the equivalence class of an integral binary quadratic form.

Proposition 3.2.3. *The discriminant of two equivalent forms is the same.*

Proof. Let f and g be two integral forms such that $g = fU$ for some $U \in \mathrm{GL}_2(\mathbb{Z})$. Then

$$\Delta_g = -4\det(M_g) = -4\det(M_{fU}) = -4\det((\det(U))U^T M_f U) = -4\det(U)^4\det(M_f) = \Delta_f$$

as $\det(U) = \det(U^T)$ and $\det(U)^2 = 1$. □

Corollary 3.2.4. *All binary quadratic forms in the proper equivalence class of an indefinite form are indefinite.*

Proposition 3.2.5. *Two properly equivalent integral binary quadratic forms have the same content.*

Proof. Let $f = (a, b, c)$ be an integral binary quadratic form with content $d \in \mathbb{Z}$ and let g be an integral binary quadratic form such that $g = fU$ for some matrix $U = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$. We know that $g = (f(p, r), 2(apq+crs)+b(ps+qr), f(q, s))$ and $\gcd(p, q) = \gcd(p, r) = \gcd(r, s) = \gcd(q, s) = 1$ as $\det(U) = \pm 1$. So, we deduce that d divides the coefficients of the form g and there is no natural number other than 1 dividing these coefficients. Hence d divides the content of g. On the other hand, since we have $f = f(UU^{-1}) = (fU)(U^{-1}) = gU^{-1}$, we see that the content of g divides d. Thus the content of f is equal to the content of g. □

As an immediate result, we have:

Corollary 3.2.6. *All binary quadratic forms in the proper equivalence class of a primitive integral binary quadratic forms are primitive.*

Definition 3.2.3. Let $f = (a, b, c)$ be a binary quadratic form, U be a matrix in $\mathrm{GL}_2(\mathbb{Z})$. We say that the matrix U is an **automorphism of** f if $fU = f$.

Definition 3.2.4. Let $f = (a, b, c)$ be a binary quadratic form, U be a matrix in $\mathrm{SL}_2(\mathbb{Z})$. We say that the matrix U is a **proper automorphism of** f if $fU = f$.

Example 3.2.1. For any binary quadratic form f, matrices I_2 and $-I_2$ are proper automorphisms of f. Indeed, $I_2, -I_2 \in \mathrm{SL}_2(\mathbb{Z})$ and $fI_2 = f(-I_2) = f$.

Definition 3.2.5. The set consisting of all automorphisms of a form f is called the **automorphism group of** f.

Definition 3.2.6. The set consisting of all proper automorphisms of a form f is called the **proper automorphism group of** f.

Notation 3.2.2. The automorphism and the proper automorphism group of f is denoted by $Aut(f)$ and $Aut^+(f)$, respectively.

3.3 Commutative $\mathbb{R}$-algebras

Definition 3.3.1. Let A be a commutative ring with identity. We say that the ring A is a **commutative $\mathbb{R}$-algebra** if A is a vector space over $\mathbb{R}$ and if A satisfies the following condition:

$$(r_1a_1 + r_2a_2)a_3 = r_1(a_1a_3) + r_2(a_2a_3)$$

for all $a_1, a_2, a_3 \in A$ and for all $r_1, r_2 \in \mathbb{R}$.

Example 3.3.1. $\mathbb{R}^n$ and $\mathbb{C}$ are commutative $\mathbb{R}$-algebras for all $n \in \mathbb{Z}_{>0}$.

Definition 3.3.2. Let A be a commutative $\mathbb{R}$-algebra and n be a positive integer. We say that A is an **n-dimensional commutative $\mathbb{R}$-algebra** if A is an n-dimensional vector space over $\mathbb{R}$.

Example 3.3.2. For all $n \in \mathbb{Z}_{>0}$, $\mathbb{R}^n$ is an n-dimensional commutative $\mathbb{R}$-algebra and $\mathbb{C}$ is a two-dimensional commutative $\mathbb{R}$-algebra.

In order to understand primitive integral indefinite binary quadratic forms, we will now construct a specific two-dimensional commutative $\mathbb{R}$-algebra that has an $\mathbb{R}$-basis of the form $\{(1,1),(\alpha_1,\alpha_2)\}$ such that $(\alpha_1,\alpha_2)^2 = (1,1)$. Let $a = (a_1, a_2)$ and $b = (b_1, b_2)$ be two points in $\mathbb{R}^2$. If we define the multiplication ab component-wise, $\mathbb{R}^2$ becomes a two-dimensional commutative $\mathbb{R}$-algebra with identity $(1,1)$. Let us choose $(\alpha_1,\alpha_2) = (1,-1)$. Then $(\alpha_1,\alpha_2)^2 = (1,1)$.

Notation 3.3.1. The two dimensional commutative $\mathbb{R}$-algebra which satisfies the conditions above will be denoted by A_1.

Let us explicitly determine the units and zero-divisors of A_1:

Proposition 3.3.1. *The units in A_1 are exactly the elements of A_1 whose components are non-zero.*

Proof. Let (α_1, α_2) be a unit in A_1. We then know that there exists an element $(\beta_1, \beta_2) \in A_1$ such that $(\alpha_1, \alpha_2)(\beta_1, \beta_2) = (1, 1)$. Since the multiplication in A_1 is componentwise, we have $\alpha_1\beta_1 = 1$ and $\alpha_2\beta_2 = 1$ which shows that α_1 and α_2 are units of $\mathbb{R}$ so they are non-zero. Conversely, let $(\alpha_1, \alpha_2) \in A_1$ such that $\alpha_1\alpha_2 \neq 0$. We show that (α_1, α_2) is a unit of A_1. Since α_1 and α_2 are both non-zero, the elements $\frac{1}{\alpha_1}$ and $\frac{1}{\alpha_2}$ exist and by construction of A_1, the element $\left(\frac{1}{\alpha_1}, \frac{1}{\alpha_2}\right)$ is in A_1. Now,

$$(\alpha_1, \alpha_2)\left(\frac{1}{\alpha_1}, \frac{1}{\alpha_2}\right) = (1, 1)$$

and hence (α_1, α_2) is a unit. □

Proposition 3.3.2. *The zero divisors in A_1 are the non-zero elements of A_1 whose exactly one component is 0.*

Proof. Let (α_1, α_2) be a zero divisor in A_1. We then know that there exists a non-zero element $(\beta_1, \beta_2) \in A_1$ such that $(\alpha_1, \alpha_2)(\beta_1, \beta_2) = (0, 0)$ so we have $\alpha_1\beta_1 = 0$ and $\alpha_2\beta_2 = 0$. Combining with the fact the the elements (α_1, α_2) and (β_1, β_2) are both non-zero, we deduce that exactly one of α_1 and α_2 is zero. Conversely, let (α_1, α_2) be a non-zero element of A_1 such that $\alpha_1\alpha_2 = 0$. Without loss of generality, we assume that $\alpha_1 = 0$ and show that the element $(0, \alpha_2)$ is a zero divisor in A_1. We observe that $(\alpha_2, 0)$ is a non-zero element of A_1 and

$$(0, \alpha_2)(\alpha_2, 0) = (0, 0).$$

Thus the element $(0, \alpha_2)$ is a zero divisor.

□

Corollary 3.3.3. *A non-zero element of A_1 is either a unit or a zero divisor of A_1.*

Proof. Let α be a non-zero element of A_1. Two possibilities then arise: Either both of the components of α are non-zero which implies that α is a unit in A_1 by

Proposition 3.3.1 or exactly one of the components of α is 0 which shows that α is a zero divisor of A_1 by Proposition 3.3.2. □

Our next aim is to determine the automorphisms of the commutative $\mathbb{R}$-algebra A_1.

Definition 3.3.3. Let A and B be commutative $\mathbb{R}$-algebras. A map $\sigma : A \to B$ is said to be

- a **homomorphism between A and B** if $\sigma(1_A) = 1_B$ and

$$\sigma(r(\alpha\beta + \gamma)) = r(\sigma(\alpha)\sigma(\beta) + \sigma(\gamma))$$

  for all real numbers r and for all elements $\alpha,\ \beta,\ \gamma \in A$.

- an **isomorphism between A and B** if σ is a bijective homomorphism.

Definition 3.3.4. An isomorphism from a commutative $\mathbb{R}$-algebra A onto itself is called an **automorphism of** A.

Proposition 3.3.4. *The only automorphisms of the commutative $\mathbb{R}$-algebra A_1 are the identity map and*

$$\begin{aligned} \sigma : A_1 &\to A_1 \\ (\alpha_1, \alpha_2) &\mapsto (\alpha_2, \alpha_1) \end{aligned}$$

Proof. Clearly, the identity map is an automorphism of A_1. Now observe that σ is the reflection map with respect to x-axis, hence a bijection. We show that the map σ is a homomorphism from A_1 to itself: For any real number r and any (α_1, α_2), (β_1, β_2), $(\gamma_1, \gamma_2) \in A_1$, we have:

$$\begin{aligned} \sigma(r(\alpha_1, \alpha_2)(\beta_1, \beta_2) + (\gamma_1, \gamma_2)) &= \sigma(r(\alpha_1\beta_1 + \gamma_1, \alpha_2\beta_2 + \gamma_2)) \\ &= \sigma((r\alpha_1\beta_1 + r\gamma_1, r\alpha_2\beta_2 + r\gamma_2)) \\ &= (r\alpha_2\beta_2 + r\gamma_2, r\alpha_1\beta_1 + r\gamma_1) \\ &= r[(\alpha_2\beta_2, \alpha_1\beta_1) + (\gamma_2, \gamma_1)] \\ &= r[(\alpha_2, \alpha_1)(\beta_2, \beta_1) + (\gamma_2, \gamma_1)] \\ &= r[\sigma((\alpha_1, \alpha_2))\sigma((\beta_1, \beta_2)) + \sigma((\gamma_1, \gamma_2))] \end{aligned}$$

Let ϕ be any automorphism of A_1, $\gamma \in A_1$. Since the set $\{(1,1),\ (1,-1)\}$ is an $\mathbb{R}$-basis of A_1, we know that there exist real numbers α, β such that

$$\gamma = \alpha(1,1) + \beta(1,-1)$$

. Since ϕ is an automorphism of A_1, we have:

$$\phi(\gamma) = \alpha\phi((1,1)) + \beta\phi((1,-1)) = \alpha(1,1) + \beta\phi((1,-1))$$

and

$$\phi((1,-1))^2 = \phi((1,-1)^2) = \phi((1,1)) = (1,1)$$

We now prove that $\phi((1,-1)) = \pm(1,-1)$ which will imply that ϕ is either the identity map or the automorphism σ. Write $\phi((1,-1)) = a(1,1) + b(1,-1)$ where $a,\ b \in \mathbb{R}$. Then

$$(1,1) = \phi((1,-1))^2 = (a+b, a-b)^2 = ((a+b)^2, (a-b)^2)$$

We have that $(a+b)^2 = 1$ and $(a-b)^2 = 1$ which implies that $a^2 + b^2 = 1$ so either $(a,b) = \pm(1,0)$ or $(a,b) = \pm(0,1)$ but the case where $(a,b) = \pm(1,0)$ is impossible since ϕ is injective and $\phi((1,1)) = (1,1)$. Hence $(a,b) = (0,\pm 1)$, which implies that $\phi((1,-1)) = \pm(1,-1)$. □

Remark 3.3.1. Observe that an element $(\alpha_1, \alpha_2) \in A_1$ is fixed by the automorphism σ if and only if $\alpha_1 = \alpha_2$. Indeed, for any element $(\alpha_1, \alpha_2) \in A_1$,

$$\sigma((\alpha_1, \alpha_2)) = (\alpha_2, \alpha_1) = (\alpha_1, \alpha_2)$$

holds if and only if $\alpha_1 = \alpha_2$.

Definition 3.3.5. For $\alpha \in A_1$, the functions

$$N(\alpha) = \alpha\sigma(\alpha)$$

and

$$Tr(\alpha) = \alpha + \sigma(\alpha)$$

are called the **norm** and the **trace of** α, respectively.

Example 3.3.3. The norm of the element $(1,-1) \in A_1$ is

$$N((1,-1)) = (1,-1)(-1,1) = (-1,-1)$$

and the trace of the same element is

$$Tr((1,-1)) = (1,-1) + (-1,1) = (0,0).$$

Now, let us observe that the norm function is multiplicative and the trace is an additive function: Let $(\alpha_1, \alpha_2),\ (\beta_1, \beta_2) \in A_1$. We compute:

$$\begin{aligned} N((\alpha_1,\alpha_2)(\beta_1,\beta_2)) &= N((\alpha_1\beta_1, \alpha_2\beta_2)) \\ &= (\alpha_1\beta_1, \alpha_2\beta_2)(\alpha_2\beta_2, \alpha_1\beta_1) \\ &= (\alpha_1,\alpha_2)(\alpha_2,\alpha_1)(\beta_1,\beta_2)(\beta_2,\beta_1) \\ &= N((\alpha_1,\alpha_2))N((\beta_1,\beta_2)) \end{aligned}$$

and

$$\begin{aligned} Tr((\alpha_1,\alpha_2) + (\beta_1,\beta_2)) &= Tr((\alpha_1+\beta_1, \alpha_2+\beta_2)) \\ &= (\alpha_1+\beta_1, \alpha_2+\beta_2) + (\alpha_2+\beta_2, \alpha_1+\beta_1) \\ &= (\alpha_1,\alpha_2) + (\alpha_2,\alpha_1) + (\beta_1,\beta_2) + (\beta_2,\beta_1) \\ &= Tr((\alpha_1,\alpha_2)) + Tr((\beta_1,\beta_2)) \end{aligned}$$

Remark 3.3.2. The norm and the trace of any element in A_1 are fixed by the automorphism σ. Indeed, for $(\alpha_1, \alpha_2) \in A_1$, we have

$$N((\alpha_1,\alpha_2)) = (\alpha_1\alpha_2, \alpha_1\alpha_2)$$

and

$$Tr((\alpha_1,\alpha_2)) = (\alpha_1+\alpha_2, \alpha_1+\alpha_2)$$

so these vectors are fixed by σ by Remark 3.3.1

Definition 3.3.6. Let $B = \{(\alpha_1, \alpha_2), (\beta_1, \beta_2)\}$ be an $\mathbb{R}$-basis of the commutative $\mathbb{R}$-algebra A_1.The **orientation of the basis** B, which will be denoted by $o(B)$, is the sign of the real number $\alpha_2\beta_1 - \alpha_1\beta_2$. If this quantity is positive, we will say that the basis B is **positively oriented** and denote it by $o(B) = +1$. Otherwise, the basis B will be called **negatively oriented** and denoted by $o(B) = -1$. If $\theta = (\theta_1, \theta_2)$ is a point in A_1 with $\theta_1 \neq \theta_2$, then the **orientation of** θ, denoted by $o(\theta)$, is defined as the orientation of the basis $\{(1, 1), (\theta_1, \theta_2)\}$.

Example 3.3.4. The basis $B = \{(1, 1), (1, -1)\}$ is positively oriented as

$$1 \cdot 1 - 1 \cdot (-1) = 2 > 0$$

Thus, $o(B) = +1$. From the latter computation, we get $o((1, -1)) = +1$ which shows that the point $(1, -1)$ of A_1 is positively oriented.

Observation 3.3.1. For any matrix $M \in \mathrm{GL}_2(\mathbb{R})$ and any $\mathbb{R}$-basis B of A_1, we have $o(BM) = sign(\det(M))o(B)$. Indeed, let $B = (\alpha, \beta) = ((\alpha_1, \alpha_2), (\beta_1, \beta_2))$ and let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$. Observe that

$$BM = \begin{pmatrix} a\alpha + c\beta & b\alpha + d\beta \end{pmatrix} = \begin{pmatrix} (a\alpha_1 + c\beta_1, a\alpha_2 + c\beta_2) & (b\alpha_1 + d\beta_1, b\alpha_2 + d\beta_2) \end{pmatrix}$$

We have

$$\begin{aligned} o(BM) &= sign((a\alpha_2 + c\beta_2)(b\alpha_1 + d\beta_1) - (a\alpha_1 + c\beta_1)(b\alpha_2 + d\beta_2)) \\ &= sign(ad(\alpha_2\beta_1 - \alpha_1\beta_2) - bc(\alpha_2\beta_1 - \alpha_1\beta_2)) \\ &= sign((ad - bc)(\alpha_2\beta_1 - \alpha_1\beta_2)) \\ &= sign(ad - bc)sign(\alpha_2\beta_1 - \alpha_1\beta_2) \\ &= sign(\det(M))o(B) \end{aligned}$$

Lemma 3.3.5. *Let ϵ be a unit in A_1, and B be any $\mathbb{R}$-basis of A_1. Then,*

$$o(\epsilon B) = sign(N(\epsilon))o(B)$$

Proof. Let $\epsilon = (\epsilon_1, \epsilon_2) \in A_1^{\times}$ and $B = ((\alpha_1, \alpha_2), (\beta_1, \beta_2))$ be an $\mathbb{R}$-basis of A_1. Note that $o(B) = sign(\alpha_2\beta_1 - \alpha_1\beta_2)$, $N(\epsilon) = (\epsilon_1\epsilon_2, \epsilon_1\epsilon_2)$ and $\epsilon B := ((\epsilon_1\alpha_1, \epsilon_2\alpha_2), (\epsilon_1\beta_1, \epsilon_2\beta_2))$.

Now, we have:

$$\begin{aligned} o(\epsilon B) &= sign(\epsilon_2\alpha_2\epsilon_1\beta_1 - \epsilon_1\alpha_1\epsilon_2\beta_2) \\ &= sign(\epsilon_1\epsilon_2(\alpha_2\beta_1 - \alpha_1\beta_2)) \\ &= sign(\epsilon_1\epsilon_2)sign(\alpha_2\beta_1 - \alpha_1\beta_2) \\ &= sign(N(\epsilon))o(B) \end{aligned}$$

□

Definition 3.3.7. Let $f(X, Y)$ be an integral binary quadratic form. The form f is called **irrational** if $f(X, Y) \neq 0$ for all $(X, Y) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$.

Example 3.3.5. The binary quadratic form $f(X, Y) = X^2 + Y^2$ is irrational, whereas the form $g(X, Y) = X^2 - Y^2$ is not as $g(1, 1) = 0$.

Remark 3.3.3. By Proposition 3.1.2, we have that an integral indefinite binary quadratic form f is irrational if and only if its discriminant Δ_f is not a perfect square.

Definition 3.3.8. Let L be a two-dimensional lattice in A_1. L is called **irrational** if L contains no zero divisors.

Definition 3.3.9. Let $B = (\alpha, \beta)$ be an $\mathbb{R}$-basis of A_1. B is called **irrational** if the corresponding lattice $L(B) := \mathbb{Z}\alpha + \mathbb{Z}\beta$ is irrational.

Definition 3.3.10. Let $\alpha = (\alpha_1, \alpha_2)$ be a point in A_1 such that $\alpha_1 \neq \alpha_2$. The point α is called **irrational** if the corresponding $\mathbb{R}$-basis $((1, 1), (\alpha_1, \alpha_2))$ is irrational.

Now we will classify irrational lattices, bases and points of A_1:

Proposition 3.3.6. *Let $\alpha = (\alpha_1, \alpha_2)$ be a point in A_1 such that $\alpha_1 \neq \alpha_2$. The point α is irrational if and only if α_1 and α_2 are irrational numbers.*

Proof. We will prove this by contraposition: Let $\alpha = (\alpha_1, \alpha_2)$ be a point in A_1 such that $\alpha_1 \neq \alpha_2$. Assume that α is not irrational. By definition, we then know that the basis $\{(1, 1), (\alpha_1, \alpha_2)\}$ is irrational, which implies that the lattice $\mathbb{Z}(1, 1) +$

$\mathbb{Z}(\alpha_1, \alpha_2)$ contains a zero-divisor, say $x(1,1) + y(\alpha_1, \alpha_2)$ where $x,\ y \in \mathbb{Z}$ and $y \neq 0$. By Proposition 3.3.2, we then know that exactly one coordinates of the point $x(1,1) + y(\alpha_1, \alpha_2)$ is zero so exactly one of the equalities $x + y\alpha_1 = 0$ or $x + y\alpha_2 = 0$ holds which implies that either α_1 or α_2 is a rational number. Conversely, assume that one of the coordinates of the point α is a rational number. Without loss of generality, say α_1 is rational. Then there exist $x \in \mathbb{Z}$, $y \in \mathbb{Z} \setminus \{0\}$ such that $\alpha_1 = \frac{x}{y}$. Clearly, the point $x(1,1) - y(\alpha_1, \alpha_2)$ is contained in the lattice $\mathbb{Z}(1,1) + \mathbb{Z}(\alpha_1, \alpha_2)$. Now, observe that the point

$$x(1,1) - y(\alpha_1, \alpha_2) = \left(x - y \cdot \frac{x}{y}, x - y\alpha_2\right) = (0, x - y\alpha_2)$$

is a zero-divisor by Proposition 3.3.2. Thus, α is not irrational. □

Proposition 3.3.7. *Let $B = (\alpha, \beta)$ be an $\mathbb{R}$-basis of A_1. The basis B is irrational if and only if α is a unit in A_1 and $\frac{\beta}{\alpha}$ is an irrational point.*

Proof. Let $B = (\alpha, \beta)$ be an irrational $\mathbb{R}$-basis of A_1. By definition, the lattice $\mathbb{Z}\alpha + \mathbb{Z}\beta$ contains no zero divisors. In particular, the non-zero element α is not a zero divisor of A_1 so it is a unit in A_1 by Corollary 3.3.3. Now observe that since α is a unit in A_1 and the lattice $\mathbb{Z}\alpha + \mathbb{Z}\beta$ is irrational by assumption, we have that the lattice $(\frac{1}{\alpha})(\mathbb{Z}\alpha + \mathbb{Z}\beta) = \mathbb{Z} + \frac{\beta}{\alpha}\mathbb{Z}$ contains no zero divisors. Thus the element $\frac{\beta}{\alpha}$ is an irrational point. Conversely, assume that the element α is a unit in A_1 and $\frac{\beta}{\alpha}$ is an irrational point. By definition we know that the corresponding basis $(1, \frac{\beta}{\alpha})$ is irrational which implies that the lattice $\mathbb{Z} + \mathbb{Z}(\frac{\beta}{\alpha})$ is irrational. Again, since α is a unit in A_1, we have that the lattice $\alpha(\mathbb{Z} + \mathbb{Z}(\frac{\beta}{\alpha})) = L(B)$ contains no zero divisors. Hence the basis B is irrational. □

Proposition 3.3.8. *Let L be a two dimensional lattice in A_1. Then the lattice L is irrational if and only if any two different points in L differ in both coordinates.*

Proof. Let L be a two dimensional lattice in A_1. To prove the necessary and sufficient conditions, let us apply contraposition: Suppose that the lattice L is not irrational. By definition, this implies that L contains a zero-divisor. Let us call that α. By Proposition 3.3.2, we know that either $\alpha = (0, a)$ or $\alpha = (a, 0)$ for some non-zero

real number a. Note also that since L is a lattice, it contains the point $(0,0)$ so either way we have two points in L, namely α and $(0,0)$, that differ in exactly one coordinate. Conversely, suppose that α_1 and α_2 are two different points in L that differ in exactly one coordinate. Without loss of generality, say $\alpha_1 = (a, a_1)$ and $\alpha_2 = (a, a_2)$ where a, a_1 and $a_2 \in \mathbb{R}$ with $a_1 \neq a_2$. Note that since L is a lattice, the point $\alpha_1 - \alpha_2 = (0, a_1 - a_2) \in L$ but by Proposition 3.3.2, we now know that the element $\alpha_1 - \alpha_2$ is a zero-divisor of A_1 which implies that the lattice L is not irrational. □

Definition 3.3.11. The **oriented norm form of an $\mathbb{R}$-basis** $B = (\alpha, \beta)$ of A_1 is the binary quadratic form defined as

$$f_B(X,Y) = o(B)(N(\alpha)X^2 + Tr(\alpha\sigma(\beta))XY + N(\beta)Y^2)$$

Definition 3.3.12. Let $\alpha = (\alpha_1, \alpha_2)$ be a point in A_1 such that $\alpha_1 \neq \alpha_2$.The **oriented norm form of the point** α is defined as $f_\alpha := f_{((1,1),(\alpha_1,\alpha_2))}$.

Remark 3.3.4. By Remark 3.3.2, we know that the two components of the norm and the trace of any element in A_1 are the same so by the coefficients $N(\alpha)$, $Tr(\alpha\sigma(\beta))$ and $N(\beta)$ in Definition 3.3.11, we mean their first components.

Example 3.3.6. Choose the $\mathbb{R}$-basis $B = ((1,1),(1,-1))$. The oriented norm form, $f_B(X,Y)$, of B is $X^2 - Y^2$. Indeed, by Example 3.3.4 we know that $o(B) = 1$ and

$$N((1,1)) = (1,1)\cdot(1,1) = (1,1)$$

$$Tr((1,1)(-1,1)) = Tr((-1,1)) = (-1,1) + (1,-1) = (0,0)$$

$$N((1,-1)) = (1,-1)\cdot(-1,1) = (-1,-1)$$

Similarly, the oriented norm form of the point $(1,-1) \in A_1$ is again the form $X^2 - Y^2$.

The following proposition naturally relates $\mathbb{R}$-bases of A_1 and the oriented norm forms:

Proposition 3.3.9. *([Buchmann and Vollmer, 2007], Proposition 4.3.6) If B is an $\mathbb{R}$-basis of A_1, then the form f_B is indefinite.*

Lemma 3.3.10. *Let ϵ be a unit in A_1, and B be any $\mathbb{R}$-basis of A_1. Then,*

$$f_{\epsilon B} = |N(\epsilon)| f_B$$

Proof. Let ϵ be a unit in A_1, and $B = (\alpha, \beta)$ be an $\mathbb{R}$-basis of A_1. Then $\epsilon B = (\epsilon\alpha, \epsilon\beta)$ and by definition, we have:

$$\begin{aligned}
f_{\epsilon B} &= o(\epsilon B)(N(\epsilon\alpha), Tr(\epsilon\alpha\sigma(\epsilon\beta)), N(\epsilon\beta)) \\
&= o(\epsilon B)(N(\epsilon)N(\alpha), Tr(\epsilon\alpha\sigma(\epsilon\beta)), N(\epsilon)N(\beta)) \text{ as norm is multiplicative} \\
&= o(\epsilon B)(N(\epsilon)N(\alpha), Tr(\epsilon\alpha\sigma(\epsilon)\sigma(\beta)), N(\epsilon)N(\beta)) \text{ as } \sigma \text{ is an automorphism} \\
&= o(\epsilon B)(N(\epsilon)N(\alpha), Tr(N(\epsilon)\alpha\sigma(\beta)), N(\epsilon)N(\beta)) \\
&= o(\epsilon B)(N(\epsilon)N(\alpha), N(\epsilon)Tr(\alpha\sigma(\beta)), N(\epsilon)N(\beta)) \\
&= sign(N(\epsilon))o(B)N(\epsilon)(N(\alpha), Tr(\alpha\sigma(\beta)), N(\beta)) \text{ by Lemma 3.3.5} \\
&= |N(\epsilon)|o(B)(N(\alpha), Tr(\alpha\sigma(\beta)), N(\beta)) \\
&= |N(\epsilon)| f_B
\end{aligned}$$

□

Definition 3.3.13. Let $\alpha = (\alpha_1, \alpha_2)$ and $\beta = (\beta_1, \beta_2)$ be two points in A_1.The **discriminant of the pair** (α, β) is the real number $(\alpha_2\beta_1 - \beta_2\alpha_1)^2$ and denoted by $\Delta(\alpha, \beta)$.

Definition 3.3.14. Let $\theta = (\theta_1, \theta_2)$ be a point in A_1. The **discriminant of** θ is defined as the discriminant of the pair $((1,1),(\theta_1,\theta_2))$ which will be denoted by $\Delta(\theta)$.

Example 3.3.7. Choose the pair $((1,1),(1,-1))$. Then its discriminant is

$$(1 \cdot 1 - (-1) \cdot 1)^2 = 2^2 = 4$$

Similarly, the discriminant of the point $(1,-1)$ is again 4.

Observation 3.3.2. Let $\theta = (\theta_1, \theta_2)$ be a point in A_1 such that $\theta_1 \neq \theta_2$. We claim that $\Delta(f_\theta) = \Delta(\theta)$. Indeed, set $B = ((1,1),(\theta_1,\theta_2))$ and observe that

$$f_\theta := f_B = o(B)(N(1,1), Tr((1,1)\sigma(\theta)), N(\theta))$$

By Example 3.3.6, we know that $N(1,1) = (1,1)$ and we have

$$Tr((1,1)\sigma(\theta)) = Tr(\sigma(\theta)) = Tr(\theta) = (\theta_1 + \theta_2, \theta_1 + \theta_2)$$

as the trace is fixed by the automorphism σ. We also see that $N(\theta) = (\theta_1\theta_2, \theta_1\theta_2)$. Combining, we have $f_\theta = o(B)(1, \theta_1 + \theta_2, \theta_1\theta_2)$ which implies that

$$\begin{aligned}
\Delta(f_\theta) &= (o(B)(\theta_1 + \theta_2))^2 - 4o(B)^2\theta_1\theta_2 \\
&= o(B)^2(\theta_1^2 + 2\theta_1\theta_2 + \theta_2^2 - 4\theta_1\theta_2) \\
&= \theta_1^2 - 2\theta_1\theta_2 + \theta_2^2 \\
&= (\theta_1 - \theta_2)^2 \\
&= \Delta(\theta)
\end{aligned}$$

Proposition 3.3.11. *Let $B = (\alpha, \beta)$ be an irrational $\mathbb{R}$-basis of A_1 and let $M \in \mathrm{GL}_2(\mathbb{Z})$. Then $f_{BM} = f_B M$.*

Proof. Let $B = (\alpha, \beta)$ be an irrational $\mathbb{R}$-basis of A_1 and $M \in \mathrm{GL}_2(\mathbb{Z})$. We know that

$$\begin{aligned}
f_B &= o(B)(N(\alpha), Tr(\alpha\sigma(\beta)), N(\beta)) \\
&= o(B)(\alpha\sigma(\alpha), \alpha\sigma(\beta) + \beta\sigma(\alpha), \beta\sigma(\beta))
\end{aligned}$$

We then have:

$$\begin{aligned}
M_{f_B} &= o(B) \begin{pmatrix} \alpha\sigma(\alpha) & \frac{\alpha\sigma(\beta)+\beta\sigma(\alpha)}{2} \\ \frac{\alpha\sigma(\beta)+\beta\sigma(\alpha)}{2} & \beta\sigma(\beta) \end{pmatrix} \\
&= \frac{o(B)}{2} \begin{pmatrix} \alpha & \sigma(\alpha) \\ \beta & \sigma(\beta) \end{pmatrix} \begin{pmatrix} \sigma(\alpha) & \sigma(\beta) \\ \alpha & \beta \end{pmatrix}
\end{aligned}$$

Since σ is a homomorphism of the commutative $\mathbb{R}$-algebra A_1, we have:

$$\begin{aligned}
M_{f_{BM}} &= \frac{o(BM)}{2} M^T \begin{pmatrix} \alpha & \sigma(\alpha) \\ \beta & \sigma(\beta) \end{pmatrix} \begin{pmatrix} \sigma(\alpha) & \sigma(\beta) \\ \alpha & \beta \end{pmatrix} M \\
&= \frac{sign(\det(M))o(B)}{2} M^T \begin{pmatrix} \alpha & \sigma(\alpha) \\ \beta & \sigma(\beta) \end{pmatrix} \begin{pmatrix} \sigma(\alpha) & \sigma(\beta) \\ \alpha & \beta \end{pmatrix} M \text{ by Observation 3.3.1} \\
&= (\det(M))M^T M_{f_B} M \text{ as } \det(M) \in \{\pm 1\} \\
&= M_{f_{BM}} \text{ by Observation 3.2.2}
\end{aligned}$$

Thus $f_{BM} = f_B M$. □

Our next aim is to associate a basis and an irrational point to a given irrational indefinite binary quadratic form.

Definition 3.3.15. Let $f = (a, b, c)$ be an irrational indefinite binary quadratic form with discriminant Δ. The basis $((a, a), (\frac{b+\sqrt{\Delta}}{2}, \frac{b-\sqrt{\Delta}}{2}))$ is called the **basis associated to the form** f and will be denoted by $B(f)$.

Example 3.3.8. Consider the indefinite binary quadratic form $f = (1, 1, -1)$ with discriminant $\Delta = 5$. Then the basis $B(f) = ((1, 1), (\frac{1+\sqrt{5}}{2}, \frac{b-\sqrt{5}}{2}))$ is the basis associated to the form $(1, 1, -1)$.

Definition 3.3.16. Let $f = (a, b, c)$ be an irrational indefinite binary quadratic form with discriminant Δ. The point $(\frac{b+\sqrt{\Delta}}{2a}, \frac{b-\sqrt{\Delta}}{2a})$ in A_1 is called the **irrational point associated to the form** f and will be denoted by $\theta(f)$.

Remark 3.3.5. We remark that the definition of the irrational point associated to an irrational indefinite binary quadratic form $f = (a, b, c)$ is well-defined. The fact that the form f is irrational guarantees that $a \neq 0$.

Example 3.3.9. Consider again the form $f = (1, 1, -1)$. The irrational point associated to f is the point $\theta(f) = (\frac{1+\sqrt{5}}{2}, \frac{b-\sqrt{5}}{2})$.

We now introduce some facts that relates the oriented norm forms, irrational points and bases.

Proposition 3.3.12. *Let $B = (\alpha, \beta)$ be an irrational basis of A_1, $\theta = (\theta_1, \theta_2)$ with $\theta_1 \neq \theta_2$ be an irrational point of A_1 and $f = (a, b, c)$ be an indefinite irrational binary quadratic form. We have:*

1. $\theta(f_\theta) = \theta$
2. $\theta(f_B) = \frac{\beta}{\alpha}$
3. $f_{\theta(f)} = \frac{1}{|a|} f$

4. $f_{B(f)} = |a|f$

Proof. Let $B = (\alpha, \beta)$ be an irrational basis of A_1, $\theta = (\theta_1, \theta_2)$ with $\theta_1 \neq \theta_2$ be an irrational point of A_1 and $f = (a, b, c)$ be an indefinite irrational binary quadratic form of discriminant Δ.

1. Observation 3.3.2 implies that $f_\theta = o(B)(1, \theta_1 + \theta_2, \theta_1\theta_2)$ and $\Delta(f_\theta) = \Delta(\theta)$ where $B = ((1,1),(\theta_1,\theta_2))$. We then have:

$$\begin{aligned}
\theta(f_\theta) &= \left(\frac{o(B)(\theta_1+\theta_2)+\sqrt{\Delta(f_\theta)}}{2o(B)}, \frac{o(B)(\theta_1+\theta_2)-\sqrt{\Delta(f_\theta)}}{2o(B)}\right) \\
&= \left(\frac{o(B)(\theta_1+\theta_2)+\sqrt{\Delta(\theta)}}{2o(B)}, \frac{o(B)(\theta_1+\theta_2)-\sqrt{\Delta(\theta)}}{2o(B)}\right) \\
&= \left(\frac{o(B)(\theta_1+\theta_2)+o(B)(\theta_1-\theta_2)}{2o(B)}, \frac{o(B)(\theta_1+\theta_2)-o(B)(\theta_1-\theta_2)}{2o(B)}\right) \\
&= \left(\frac{\theta_1+\theta_2+\theta_1-\theta_2}{2}, \frac{\theta_1+\theta_2-\theta_1+\theta_2}{2}\right) \\
&= (\theta_1, \theta_2) \\
&= \theta
\end{aligned}$$

2. First note that since B is an irrational basis of A_1 we know that α is a unit of A_1 by Proposition 3.3.7. We have:

$$\begin{aligned}
\theta(f_B) &= \theta(f_{\alpha(1,\frac{\beta}{\alpha})}) \text{ where } 1 := (1,1) \\
&= \theta(|N(\alpha)|f_{\frac{\beta}{\alpha}}) \text{ by Lemma 3.3.10} \\
&= \frac{\beta}{\alpha} \text{ by Proposition 3.3.12-1}
\end{aligned}$$

3. Recall $\theta(f) = \left(\frac{b+\sqrt{\Delta}}{2a}, \frac{b-\sqrt{\Delta}}{2a}\right)$ and observe that

$$o(\theta(f)) = sign\Big(\frac{b+\sqrt{\Delta}}{2a} - \frac{b-\sqrt{\Delta}}{2a}\Big) = sign\Big(\frac{\sqrt{\Delta}}{2a}\Big) = sign(a)$$

as $\Delta > 0$. We also have

$$Tr(\theta(f)) = \Big(\frac{b+\sqrt{\Delta}}{2a} + \frac{b-\sqrt{\Delta}}{2a}, \frac{b+\sqrt{\Delta}}{2a} + \frac{b-\sqrt{\Delta}}{2a}\Big) = \Big(\frac{b}{a}, \frac{b}{a}\Big)$$

and

$$N(\theta(f)) = \Big(\frac{b^2-\Delta}{4a^2}, \frac{b^2-\Delta}{4a^2}\Big) = \Big(\frac{c}{a}, \frac{c}{a}\Big)$$

Now, we have:

$$\begin{aligned} f_{\theta(f)} &= sign(a)\Big(1, \frac{b}{a}, \frac{c}{a}\Big) \\ &= \frac{sign(a)}{a}(a,b,c) \\ &= \frac{1}{|a|}f \end{aligned}$$

4. Recall that $B(f) = ((a,a), (\frac{b+\sqrt{\Delta}}{2}, \frac{b\sqrt{\Delta}}{2}))$. We have:

$$\begin{aligned} f_{B(f)} &= f_{a((1,1),\theta(f))} \\ &= a^2 f_{\theta(f)} \\ &= \frac{a^2}{|a|}f \text{ by Proposition 3.3.12-3} \\ &= |a|f \end{aligned}$$

□

3.4 Reduction of indefinite binary quadratic forms

In order to understand the automorphism group of an indefinite binary quadratic form, we need to study on an algorithm which is about the "reduction" of an indefinite form. From now on, we assume that $f = (a,b,c)$ is an indefinite binary quadratic form of discriminant $\Delta_f = \Delta$.

Definition 3.4.1. The indefinite binary quadratic form f is called **reduced** if it satisfies the following inequality:

$$|\sqrt{\Delta} - 2|a|| < b < \sqrt{\Delta}$$

Example 3.4.1. Consider the form $f = (1,3,-1)$. Then f is indefinite. Indeed, $\Delta_f = 3^2 - 4\times 1\times(-1) = 13 > 0$. f is also reduced as $|\sqrt{13}-2| < 3 < \sqrt{13}$. On the other hand, the indefinite form $f = (1,0,-5)$ is not reduced as $b = 0$ is not positive.

For an indefinite binary quadratic form $f = (a, b, c)$, we set the matrix

$$U(f) := \begin{pmatrix} 0 & -1 \\ 1 & s(f) \end{pmatrix}$$

where the integer $s(f)$ is defined as $\begin{cases} sign(c) \left\lfloor \frac{b}{2|c|} \right\rfloor, & \text{if } |c| \geq \sqrt{\Delta} \\ sign(c) \left\lfloor \frac{b+\sqrt{\Delta}}{2|c|} \right\rfloor, & \text{otherwise} \end{cases}$

Then put $\rho(f) := (c, -b + 2s(f)c, cs(f)^2 - bs(f) + a)$ and check whether the resulting form is reduced or not. If not, then apply the same algorithm to the resulting form. Observe that in terms of the group action, the binary quadratic form $\rho(f)$ is obtained by $\rho(f) = fU(f)$, applying the matrix $U(f)$ to the form f. Observe also that the entries of the matrix $U(f)$ are integers and its determinant is 1. Therefore $U(f) \in \mathrm{SL}_2(\mathbb{Z})$ and the forms f and $\rho(f)$ are properly equivalent.

The algorithm introduced earlier is called the **Reduction Algorithm** and Gauss showed that this algorithm terminates which means that if the Reduction Algorithm is applied repeatedly to any indefinite integral binary quadratic form, one eventually obtains a reduced form.

Example 3.4.2. By Example 3.4.1, we know that the form $f = (1, 0, -5)$ is not reduced. Let us apply the Reduction Algorithm on f. We have $\Delta = 20$ and $|c| = 5 > \sqrt{20}$ so $s(f) = -\lfloor \frac{0}{10} \rfloor = 0$ and $\rho(f) = (-5, 0, 1)$. Observe that $\rho(f)$ is not reduced as $b = 0$. Therefore we again apply the Reduction Algorithm. As $|c| = 1 < \sqrt{20}$, we have $s(\rho(f)) = |\frac{\sqrt{20}+0}{2}| = 2$. Therefore,

$$\rho^2(f) = \rho(\rho(f)) = (1, 2 \cdot 2 \cdot 1, 1 \cdot 2^2 - 5) = (1, 4, -1)$$

Observe that $(1, 4, -1)$ is a reduced form. Indeed,

$$|\sqrt{\Delta} - 2|a|| = |\sqrt{20} - 2| < 4 < \sqrt{20}$$

and the Reduction Algorithm terminates for the form f.

Now, we would like to give a useful equivalent condition on indefinite forms to show their reducedness. This is the reason why we introduced following theorem:

Theorem 3.4.1. *If an indefinite binary quadratic form $f = (a, b, c)$ of discriminant Δ is reduced, then $|a| + |c| < \sqrt{\Delta}$ and the coefficients a and c have opposite sign.*

Proof. Let $f = (a, b, c)$ be a reduced indefinite binary quadratic form of discriminant Δ. Since f is indefinite, we know that $\Delta > 0$ and since f is reduced, the following inequality holds by definition:

$$|\sqrt{\Delta} - 2|a|| < b < \sqrt{\Delta}$$

From the discriminant of f, we obtain $4ac = b^2 - \Delta$. As f is reduced, $0 < b < \sqrt{\Delta}$ which shows that $b^2 - \Delta = 4ac < 0$. Therefore, a and c have opposite signs. Now, for the inequality $|a| + |c| < \sqrt{\Delta}$, let us keep in mind that $|2|a| - \sqrt{\Delta}| < b$ and observe:

$$\begin{aligned} 4|a|(|a| + |c| - \sqrt{\Delta}) &= 4a^2 - 4|a|\sqrt{\Delta} + 4|a||c| && (3.1)\\ &= 4a^2 - 4|a|\sqrt{\Delta} + \Delta - b^2 && (3.2)\\ &= (2|a| - \sqrt{\Delta})^2 - b^2 < 0 && (3.3) \end{aligned}$$

Hence, we have $|a| + |c| - \sqrt{\Delta} < 0$, which is the same as the inequality

$$|a| + |c| < \sqrt{\Delta}.$$

□

Corollary 3.4.2. *The number of reduced indefinite integral binary quadratic forms of a fixed discriminant is finite.*

Proof. Fix a positive discriminant Δ which is not a square. Given any reduced indefinite integral binary quadratic form $f = (a, b, c)$ of discriminant Δ, we now know that $|a| + |c| < \sqrt{\Delta}$ and $0 < b < \sqrt{\Delta}$. This shows that there are only finitely many possibilities for the coefficients a, b and c. Hence the number of reduced indefinite integral binary quadratic forms of discriminant Δ is finite. □

Proposition 3.4.3. *The indefinite binary quadratic form $f = (a, b, c)$ is reduced if and only if $|\theta_1(f)| > 1$, $|\theta_2(f)| < 1$ and the signs of $\theta_1(f)$ and $\theta_2(f)$ are opposite.*

Proof. First, assume that the indefinite binary quadratic form $f = (a, b, c)$ is reduced. By definition, we know that the coefficients a, b and c satisfy the following inequality:

$$|\sqrt{\Delta} - 2|a|| < b < \sqrt{\Delta}$$

From the latter, we derive:

$$0 < b < \sqrt{\Delta} \text{ and } -b < \sqrt{\Delta} - 2|a| < b$$

Recall that $|\theta_1(f)| = \left|\frac{b+\sqrt{\Delta}}{2a}\right| = \frac{b+\sqrt{\Delta}}{2|a|}$. We know that $2|a| > b + \sqrt{\Delta}$, which implies $|\theta_1(f)| > 1$. Similarly, $|\theta_2(f)| = \left|\frac{b-\sqrt{\Delta}}{2a}\right| = \frac{\sqrt{\Delta}-b}{2|a|}$. Since $\sqrt{\Delta} - 2|a| < b$, we have that $|\theta_2(f)| < 1$. In order to prove that the signs of $\theta_1(f)$ and $\theta_2(f)$ are opposite, it suffices to show that $\theta_1(f)\theta_2(f) = \frac{c}{a} < 0$. Since the form f is reduced, by Theorem 3.4.1 we know that a and c have opposite sign. Thus $\theta_1(f)\theta_2(f) < 0$. Conversely, let $f = (a, b, c)$ be an indefinite binary quadratic form such that $|\theta_1(f)| > 1$, $|\theta_2(f)| < 1$ and the signs of $\theta_1(f)$ and $\theta_2(f)$ are opposite. We show that f is reduced. By assumption, $\theta_1(f)\theta_2(f) = \frac{c}{a} < 0$ so the a and c have opposite sign, which implies that we can describe the discriminant Δ of f of the form $b^2 + 4|a||c|$. This shows that $b^2 < \Delta$ and hence $|b| < \sqrt{\Delta}$. We now know that $|\theta_1(f)| = \frac{b+\sqrt{\Delta}}{2|a|} > 1$ and $|\theta_2(f)| = \frac{\sqrt{\Delta}-b}{2|a|} < 1$. Thus $|\sqrt{\Delta} - 2|a|| < b$. Combining, we observe that the coefficients a, b and c satisfy $|\sqrt{\Delta}-2|a|| < b < \sqrt{\Delta}$. Thus, the form f is reduced. □

Corollary 3.4.4. *If the form (a, b, c) is reduced, then so is the form (c, b, a).*

Proof. Let (a, b, c) be a reduced form. We compute

$$\theta_1(c, b, a) = \frac{b + \sqrt{\Delta}}{2c} = \frac{b^2 - \Delta}{2c(b - \sqrt{\Delta})} = \frac{2a}{b - \sqrt{\Delta}} = \frac{1}{\theta_2(a, b, c)}$$

$$\theta_2(c, b, a) = \frac{b - \sqrt{\Delta}}{2c} = \frac{b^2 - \Delta}{2c(b + \sqrt{\Delta})} = \frac{2a}{b + \sqrt{\Delta}} = \frac{1}{\theta_1(a, b, c)}$$

By Proposition 3.4.3, we know that $|\theta_1(a, b, c)| > 1$, $|\theta_2(a, b, c)| < 1$ and $\theta_1(a, b, c)\theta_2(a, b, c) < 0$ as (a, b, c) is reduced by assumption. Again by Proposition 3.4.3, we deduce that the form (c, b, a) is reduced. □

Observation 3.4.1. Let $f = (a, b, c)$ be an irrational indefinite integral binary quadratic form of discriminant Δ. If f is reduced, then $|s(f)| \geq 1$. If f is reduced

then by definition we know that $b < \sqrt{\Delta}$. By Theorem 3.4.1 we know also that $|c| < \sqrt{\Delta}$ which implies that $|s(f)| = |\lfloor \frac{b+\sqrt{\Delta}}{2|c|} \rfloor|$. Now,

$$|s(f)| = \left|\left\lfloor \frac{b+\sqrt{\Delta}}{2|c|} \right\rfloor\right| \geq \left|\left\lfloor \frac{b+\sqrt{\Delta}}{2\sqrt{\Delta}} \right\rfloor\right| \geq \left|\left\lfloor \frac{\sqrt{\Delta}+\sqrt{\Delta}}{2\sqrt{\Delta}} \right\rfloor\right| = 1$$

We will prove that the Reduction Algorithm terminates. We now introduce the so-called normal forms and relate them with reduced forms to this end.

Definition 3.4.2. Let $f = (a, b, c)$ be an integral indefinite binary quadratic form of discriminant Δ. We say that f is a **normal** form if:

$$\begin{cases} -|a| < b \leq |a| & \text{if } |a| \geq \sqrt{\Delta} \\ \sqrt{\Delta} - 2|a| < b < \sqrt{\Delta} & \text{if } |a| < \sqrt{\Delta} \end{cases}$$

Observation 3.4.2. If $f = (a, b, c)$ is an indefinite reduced form, then f is normal. Indeed, if $f = (a, b, c)$ is reduced then $|a| < \sqrt{\Delta}$ by Theorem 3.4.1 and we know that

$$|\sqrt{\Delta} - 2|a|| < b < \sqrt{\Delta}$$

which implies that $\sqrt{\Delta} - 2|a| < b < \sqrt{\Delta}$.

Below we will transform a given indefinite binary quadratic form $f = (a, b, c)$ into a normal form.

Set $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and define the following infinite subgroup of $\mathrm{SL}_2(\mathbb{Z})$

$$\Gamma := \langle T \rangle = \left\{ T^m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \ : \ m \in \mathbb{Z} \right\}$$

We also set $s := \begin{cases} sign(a)\left\lfloor \frac{|a|-b}{2|a|} \right\rfloor, & \text{if } |a| \geq \sqrt{\Delta} \\ sign(a)\left\lfloor \frac{\sqrt{\Delta}-b}{2|a|} \right\rfloor, & \text{if } |a| < \sqrt{\Delta} \end{cases}$ and claim that the form

$$\begin{aligned} fT^s &= (f(1,0), 2as + b, f(s,1)) \\ &= (a, b + 2as, as^2 + bs + c) \end{aligned}$$

is normal. If $|a| \geq \sqrt{\Delta}$, then $s = sign(a)\left\lfloor \frac{|a|-b}{2|a|} \right\rfloor$ and we need to show that

$$-|a| < b + 2as \leq |a|$$

Note that

$$\begin{aligned} b + 2as &= b + 2asign(a) \left\lfloor \frac{|a| - b}{2|a|} \right\rfloor \\ &= b + 2|a| \left\lfloor \frac{|a| - b}{2|a|} \right\rfloor \end{aligned}$$

As $0 \leq \frac{|a|-b}{2|a|} - \left\lfloor \frac{|a|-b}{2|a|} \right\rfloor < 1$, we have

$$0 \leq |a| - b - 2|a| \left\lfloor \frac{|a| - b}{2|a|} \right\rfloor < 2|a|$$

which implies that

$$-|a| \leq -\left(b + 2|a| \left\lfloor \frac{|a| - b}{2|a|} \right\rfloor \right) < |a|$$

Therefore, $-|a| < b + 2as \leq |a|$. If $|a| < \sqrt{\Delta}$, then $s = sign(a)\left\lfloor \frac{\sqrt{\Delta}-b}{2|a|} \right\rfloor$ and we show that

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

Note that $b + 2as = b + 2|a|\left\lfloor \frac{\sqrt{\Delta}-b}{2|a|} \right\rfloor$ and $0 \leq \frac{\sqrt{\Delta}-b}{2|a|} - \left\lfloor \frac{\sqrt{\Delta}-b}{2|a|} \right\rfloor < 1$ Therefore we have

$$0 \leq \sqrt{\Delta} - b - 2|a| \left\lfloor \frac{\sqrt{\Delta} - b}{2|a|} \right\rfloor < 2|a|$$

which implies that

$$-\sqrt{\Delta} \leq -\left(b + 2|a| \left\lfloor \frac{\sqrt{\Delta} - b}{2|a|} \right\rfloor \right) < 2|a| - \sqrt{\Delta}$$

Since $|a| < \sqrt{\Delta}$, we are done.

Definition 3.4.3. The form fT^s is called the **normalization of** f. Replacing a form f by its normalization is called **normalizing** f.

Remark 3.4.1. Applying the reduction operator ρ to an indefinite form $f = (a, b, c)$ is the same as normalizing the form $(c, -b, a)$. Therefore $\rho(f)$ is a normal form for any indefinite binary quadratic form f.

Lemma 3.4.5. *Let $f = (a, b, c)$ be a normal form such that $|a| \leq \frac{\sqrt{\Delta}}{2}$. Then f is reduced.*

Proof. Let $f = (a, b, c)$ be a normal form of discriminant Δ such that $|a| \leq \frac{\sqrt{\Delta}}{2}$. Since $|a| \leq \frac{\sqrt{\Delta}}{2} < \sqrt{\Delta}$, we have $\sqrt{\Delta} - 2|a| < b < \sqrt{\Delta}$. We also have $2|a| \leq \sqrt{\Delta}$ which implies that $\sqrt{\Delta} - 2|a| \geq 0$. Therefore,

$$\sqrt{\Delta} - 2|a| = |\sqrt{\Delta} - 2|a|| < b < \sqrt{\Delta}$$

and f is reduced. □

Lemma 3.4.6. *Let $f = (a, b, c)$ be a normal form of discriminant Δ such that $|a| < \sqrt{\Delta}$. Then $\rho(f)$ is reduced.*

Proof. Let $f = (a, b, c)$ be a normal form of discriminant Δ such that $|a| < \sqrt{\Delta}$. We will show that

$$\rho(f) = (c, -b + 2sc, cs^2 - bs + a)$$

is reduced where $s = s(f)$. If $|c| \leq \frac{\sqrt{\Delta}}{2}$, then $\rho(f)$ is reduced by Lemma 3.4.5. Note that since f is normal and $|a| < \sqrt{\Delta}$, we have:

$$-\sqrt{\Delta} < \sqrt{\Delta} - 2|a| < b < \sqrt{\Delta}$$

It follows then that $0 < \sqrt{\Delta} - b < 2|a|$, $0 < b + \sqrt{\Delta}$ and $|b| < \sqrt{\Delta}$. If $|c| > \frac{\sqrt{\Delta}}{2}$, then we have

$$\frac{b + \sqrt{\Delta}}{2|c|} = \frac{2|a|}{\sqrt{\Delta} - b} > 1$$

which implies that $b + \sqrt{\Delta} > 2|c|$. We also have

$$-b + 2|c| > -\sqrt{\Delta} + 2|c| = |\sqrt{\Delta} - 2|c||$$

Combining we get

$$|\sqrt{\Delta} - 2|c|| < -b + 2|c| < \sqrt{\Delta}$$

and $s = sign(c)$. Hence

$$\rho(f) = (c, -b + 2sc, cs^2 - bs + a) = (c, -b + 2|c|, a - sign(c)b + c)$$

is reduced. □

Proposition 3.4.7. *If the form f is reduced, then so is $\rho(f)$.*

Proof. Let $f = (a, b, c)$ be a reduced form. Then we know that f is normal and by Theorem 3.4.1 we know that $|a| < \sqrt{\Delta}$. Thus $\rho(f)$ is reduced by Lemma 3.4.6. □

Lemma 3.4.8. *Let $f = (a, b, c)$ be an indefinite normal binary quadratic form of discriminant Δ with $|a| \geq \sqrt{\Delta}$. Then $|c| \leq \frac{|a|}{4}$.*

Proof. Let $f = (a, b, c)$ be an indefinite normal binary quadratic form of discriminant Δ with $|a| \geq \sqrt{\Delta}$. Then $a^2 \geq \Delta$ and since f is normal we know that $-|a| < b \leq |a|$. This shows that $b^2 \leq a^2$. Write $\Delta = b^2 - 4|a||c|$ and observe that

$$|c| = \frac{\Delta - b^2}{4|a|} \leq \frac{a^2}{4|a|} = \frac{|a|}{4}$$

and we are done. □

Theorem 3.4.9. *The Reduction Algorithm eventually terminates.*

Proof. We know that in order to reduce a given indefinite form (a, b, c) of discriminant Δ, we normalize the form $f = (c, -b, a)$ in each reduction step. Say the resulting normal form is $f' = (a', b', c')$. If $a \geq \sqrt{\Delta}$, then by Lemma 3.4.8, we have $a' = c \leq \frac{a}{4}$ which implies that after at most $\frac{1}{2}\log_2(\frac{a}{\sqrt{\Delta}}) + 1$ iterations, the algorithm ends up with a normal form (A, B, C) such that $A < \sqrt{\Delta}$. Therefore, at most one more step one gets a reduced form as it is guaranteed by Lemma 3.4.6 that $\rho(A, B, C)$ is a reduced form. □

Corollary 3.4.10. *If f is an indefinite binary quadratic form, then the proper equivalence class of f contains a reduced form.*

Proof. This follows from Theorem 3.4.9, $\rho(f) = fU(f)$ and $U(f) \in \mathrm{SL}_2(\mathbb{Z})$ for any indefinite form f. □

By Proposition 3.4.7, we know that $\rho(f)$ is a reduced form if f is a reduced form. Moreover, we discussed that the forms f and $\rho(f)$ are properly equivalent. Below we will show that the reduction operator actually permutes the set of all reduced forms that are properly equivalent to a given indefinite form f.

Theorem 3.4.11. *Let $\mathfrak{F}^+(g)$ denote the set of all reduced forms that are properly equivalent to the irrational indefinite integral binary quadratic form g. Then the map*

$$\begin{aligned} \mathcal{P} : \mathfrak{F}^+(g) &\to \mathfrak{F}^+(g) \\ f &\mapsto \rho(f) \end{aligned}$$

is a bijection.

Proof. Let g be an irrational indefinite binary quadratic form. We first prove that $\mathcal{P}$ is surjective. Given a reduced form $f = (a, b, c) \in \mathfrak{F}^+(g)$, we claim that its inverse image under the map $\mathcal{P}$ is:

$$\mathcal{P}^{-1} =: \rho^{-1}(f) = (at^2 - bt + c, -b + 2at, a)$$

where $t = sign(a)\lfloor \frac{b+\sqrt{\Delta}}{2|a|} \rfloor$. Observe that $\rho^{-1}(f) = f \begin{pmatrix} t & 1 \\ -1 & 0 \end{pmatrix}$. Indeed, set the matrix $V(f) := \begin{pmatrix} t & 1 \\ -1 & 0 \end{pmatrix}$ and

$$\begin{aligned} fV &= (f(t, -1), 2(1at + c(-1)0) + b(0t - 1), f(-1, 0)) \\ &= (at^2 - bt + c, -b + 2at, a) \\ &= \rho^{-1}(f) \end{aligned}$$

Clearly, $V \in \mathrm{SL}_2(\mathbb{Z})$, which shows that the forms f and $\rho^{-1}(f)$ are properly equivalent. We still need to show that $\mathcal{P}(\rho^{-1}(f)) = \rho(\rho^{-1}(f)) = f$ and the form $\rho^{-1}(f)$ is reduced. We show that $\rho^{-1}(f)$ is reduced: Since f is reduced, we know that $|a| < \sqrt{\Delta}$ by Theorem 3.4.1 and the form (c, b, a) is reduced by Corollary 3.4.4. Then $\rho(c, b, a) = (a, -b + 2at, at^2 - bt + c)$ is reduced by Proposition 3.4.7. By Corollary 3.4.4, we have that $\rho^{-1}(f) = (at^2 - bt + c, -b + 2at, a)$ is reduced. Now, let us show that $rho(\rho^{-1}(f)) = f$. In terms of the matrices it is equivalent to show that $(fV(f))U(\rho^{-1}(f)) = f$ but by the group action we know that

$$(fV(f))U(\rho^{-1}(f)) = f(V(f)U(\rho^{-1}(f)))$$

so it suffices to verify that $V(f)U(\rho^{-1}(f)) = I_2$. We have:

$$V(f)U(f) = \begin{pmatrix} t & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & s(\rho^{-1}(f)) \end{pmatrix} = \begin{pmatrix} 1 & -t + s(f) \\ 0 & 1 \end{pmatrix}$$

We show that $t = s(\rho^{-1}(f))$. We have that $s(\rho^{-1}(f)) = sign(a)\lfloor \frac{-b+2at+\sqrt{\Delta}}{2|a|} \rfloor$ as $|a| < \sqrt{\Delta}$. Then it suffices to show that $\lfloor \frac{b+\sqrt{\Delta}}{2|a|} \rfloor = \lfloor \frac{-b+2at+\sqrt{\Delta}}{2|a|} \rfloor$. We have:

$$\begin{aligned} \left\lfloor \frac{-b+2at+\sqrt{\Delta}}{2|a|} \right\rfloor &= \left\lfloor \frac{-b+2asign(a)\lfloor \frac{b+\sqrt{\Delta}}{2|a|} \rfloor + \sqrt{\Delta}}{2|a|} \right\rfloor \\ &= \left\lfloor \frac{-b+2|a|\lfloor \frac{b+\sqrt{\Delta}}{2|a|} \rfloor + \sqrt{\Delta}}{2|a|} \right\rfloor \\ &= \left\lfloor \left\lfloor \frac{b+\sqrt{\Delta}}{2|a|} \right\rfloor + \frac{-b+\sqrt{\Delta}}{2|a|} \right\rfloor \end{aligned}$$

Now observe that $0 < \frac{-b+\sqrt{\Delta}}{2|a|} < 1$. Indeed, since f is reduced we know that $0 < b < \sqrt{\Delta}$ and $|a| < \sqrt{\Delta}$. We have:

$$0 < \frac{-b+\sqrt{\Delta}}{2|a|} < \frac{\sqrt{\Delta}}{2|a|} < \frac{\sqrt{\Delta}}{2\sqrt{\Delta}} < \frac{1}{2} < 1$$

Therefore, $\left\lfloor \frac{-b+2at+\sqrt{\Delta}}{2|a|} \right\rfloor = \left\lfloor \frac{b+\sqrt{\Delta}}{2|a|} \right\rfloor$ and $t = s(\rho^{-1}(f))$. This proves surjectivity. Now we show that $\mathcal{P}$ is injective. Let $f = (a, b, c)$, $f' = (a', b', c') \in \mathfrak{F}^+(g)$ such that $\rho(f) = \rho(f')$. We prove that $f = f'$. By assumption, we know that:

$$(c, -b + 2sc, cs^2 - bs + a) = (c', -b' + 2s'c', c'(s')^2 - b's' + a')$$

where $s = s(f)$ and $s' = s(f')$. We immediately see that $c = c'$. Combined with the coefficients of the term XY in both forms, the latter implies that $b \equiv b' \pmod{2|c|}$. Now since f and f' are reduced, we know that $\rho(f)$ and $\rho(f')$ are reduced by Proposition 3.4.7. We then have $b = b'$. Since $\Delta_f = \Delta_{f'}$ we deduce that $a = a'$. Hence $f = f'$ and $\mathcal{P}$ is a bijection. □

3.4.1 Minimal points and bases

The aim of this subsection is to introduce necessary geometric tools and prove that the reduction operator is a transitive permutation.

Definition 3.4.4. Let L be a two-dimensional irrational lattice in A_1 and $\mu = (\mu_1, \mu_2)$ be a nonzero point in L. The point μ is called a **minimal point of** L if there is no nonzero point $\theta = (\theta_1, \theta_2)$ in L which satisfy the inequalities $|\theta_1| < |\mu_1|$ and $|\theta_2| < |\mu_2|$.

Definition 3.4.5. Let L be a two-dimensional irrational lattice in A_1 and $B = ((\alpha_1, \alpha_2), (\beta_1, \beta_2)$ be a basis of L. The basis B is called a **minimal basis of** L if $|\alpha_1| < |\beta_1|$, $|\alpha_2| > |\beta_2|$ and if there is no point (θ_1, θ_2) in L which is nonzero and satisfies $|\theta_1| < |\beta_1|$ and $|\theta_2| < |\alpha_2|$.

Observation 3.4.3. If $B = ((\alpha_1, \alpha_2), (\beta_1, \beta_2))$ is a minimal basis of the two dimensional irrational lattice L, then the point (α_1, α_2) is a minimal point of L. Indeed, say there exists a point $\theta = (\theta_1, \theta_2) \in L$ with $|\theta_1| < |\alpha_1|$ and $|\theta_2| < |\alpha_2|$. We need to show that $\theta_1 = \theta_2 = 0$. Since B is a minimal basis of L, we know that $|\alpha_1| < |\beta_1|$ so we have $|\theta_1| < |\beta_1|$ and $|\theta_2| < |\alpha_2|$ which implies that $\theta_1 = \theta_2 = 0$ again by the minimality of the basis B.

Lemma 3.4.12. *Let ϵ be a unit of A_1, $(\alpha, \beta) \in A_1^2$, and L be a two-dimensional irrational lattice in A_1. Then (α, β) is a minimal basis of L if and only if $(\epsilon\alpha, \epsilon\beta)$ is a minimal basis of ϵL.*

Proof. Let $\epsilon = (\epsilon_1, \epsilon_2)$ be a unit of A_1, $B = (\alpha, \beta) = ((\alpha_1, \alpha_2), (\beta_1, \beta_2)) \in A_1^2$, and L be a two-dimensional irrational lattice in A_1. First, note that since ϵ is a unit of A_1 we clearly have that B is an $\mathbb{R}$-basis of L if and only if ϵB is an $\mathbb{R}$-basis of ϵL. Assume that B is a minimal basis of L and there exists a point $\theta = (\theta_1, \theta_2) \in \epsilon L$ such that $|\theta_1| < |\epsilon_1\beta_1|$ and $|\theta_2| < |\epsilon_2\alpha_2|$. We need to show that $\theta_1 = \theta_2 = 0$. Note that $\epsilon_1 \neq 0$ and $\epsilon_2 \neq 0$ as $\epsilon \in A_1^{\times}$. Observe that $|\alpha_1| < |\beta_1|$ if and only if $|\epsilon_1\alpha_1| < |\epsilon_1\beta_1|$ and $|\alpha_2| > |\beta_2|$ if and only if $|\epsilon_2\alpha_2| > |\epsilon_2\beta_2|$. Now, We have $|\frac{\theta_1}{\epsilon_1}| < |\beta_1|$ and $|\frac{\theta_2}{\epsilon_2}| < |\alpha_2|$. Note that $(\frac{\theta_1}{\epsilon_1}, \frac{\theta_2}{\epsilon_2}) \in L$ and since B is minimal we have that $\frac{\theta_1}{\epsilon_1} = \frac{\theta_2}{\epsilon_2} = 0$, which implies that $\theta_1 = \theta_2 = 0$. Thus $(\epsilon\alpha, \epsilon\beta)$ is a minimal basis of ϵL. Conversely, assume that $(\epsilon\alpha, \epsilon\beta)$ is a minimal basis of ϵL and there exists a point $\theta = (\theta_1, \theta_2) \in L$ such that $|\theta_1| < |\beta_1|$ and $|\theta_2| < |\alpha_2|$. We need to show that $\theta_1 = \theta_2 = 0$. We know that $|\epsilon_1\theta_1| < |\epsilon_1\beta_1|$ and $|\epsilon_2\theta_2| < |\epsilon_2\alpha_2|$. Again by the minimality of $(\epsilon\alpha, \epsilon\beta)$, we have $\epsilon_1\theta_1 = \epsilon_2\theta_2 = 0$. Thus $\theta_1 = \theta_2 = 0$ and B is a minimal basis of L.

□

Theorem 3.4.13. *Let $f = (a, b, c)$ be an integral indefinite binary quadratic form with discriminant Δ and let $L = \frac{1}{a}L(f) = \mathbb{Z}(1, 1) + \mathbb{Z}(\frac{b+\sqrt{\Delta}}{2a}, \frac{b-\sqrt{\Delta}}{2a})$. Then f is a reduced form if and only if the pair $((1, 1), \theta(f))$ is a minimal basis of L.*

Proof. Let $f = (a, b, c)$ be an integral indefinite binary quadratic form with discriminant Δ and let $L = \mathbb{Z}(1, 1) + \mathbb{Z}(\frac{b+\sqrt{\Delta}}{2a}, \frac{b-\sqrt{\Delta}}{2a})$. Set $\theta_1 := \frac{b+\sqrt{\Delta}}{2a}$ and $\theta_2 := \frac{b-\sqrt{\Delta}}{2a}$ and suppose that f is reduced. By Proposition 3.4.3 we know that $|\theta_1| > 1$, $|\theta_2| < 1$ and $\theta_1\theta_2 < 0$. Let $(x + y\theta_1, x + y\theta_2) \in L$ such that $|x + y\theta_1| < |\theta_1|$ and $|x + y\theta_2| < 1$. In order to show that $((1, 1), \theta(f))$ is a minimal basis of L, it suffices to prove that $x = y = 0$. Note that x, $y \in \mathbb{Z}$. Now, if $y = 0$, then by the second inequality we have that $x = 0$ since x is an integer. If $y \neq 0$, then the first inequality implies that $x \neq 0$ and x and $y\theta_1$ have opposite sign. Since $\theta_1\theta_2 < 0$, we deduce that x and $y\theta_2$ have the same sign which contradicts the second inequality. Conversely, suppose that $((1, 1), \theta(f))$ is a minimal basis of L. By definition, we know that $|\theta_1| > 1$ and $|\theta_2| < 1$. By Proposition 3.4.3, if we show that $\theta_1\theta_2 < 0$, then we may deduce that the form f is reduced. Say $\theta_1\theta_2 > 0$. Here we remark that $\theta_1\theta_2 \neq 0$ since the discriminant Δ is not a perfect square which implies that $c \neq 0$. Note that by construction the point $(1 - sign(\theta_1)\theta_1, 1 - sign(\theta_1)\theta_2) \in L$ and $(1, 1)$ is a minimal point of L. Since $\theta_1\theta_2 > 0$, we have $|1 - sign(\theta_1)\theta_1| < |\theta_1|$ and $|1 - sign(\theta_1)\theta_2| < 1$ which is a contradiction with the minimality of the point $(1, 1)$. □

Corollary 3.4.14. *Let L be a two-dimensional irrational lattice in A_1 and $B = (\alpha, \beta)$ be a basis of L. Then f_B is a reduced form if and only if B is a minimal basis of L.*

Proof. Let L be a two-dimensional irrational lattice in A_1 and $B = (\alpha, \beta)$ be a basis of L. By Proposition 3.3.12-2, we know that $\theta(f_B) = \frac{\beta}{\alpha}$. Since L is irrational, we know that α is a unit of A_1 by Proposition 3.3.7. So by Lemma 3.4.12 we know that B is a minimal basis of L if and only if $(1, \frac{\beta}{\alpha})$ is a minimal basis of $L(\theta(f_B))$. By Theorem 3.4.13, we have that f_B is a reduced form if and only if B is a minimal basis of L. □

Now let $f = (a, b, c)$ be a primitive indefinite integral binary quadratic form with discriminant Δ. Suppose that the form f is reduced and also that $a > 0$. Let L denote the lattice

$$\frac{1}{a}L(f) = \mathbb{Z}(1,1) + \mathbb{Z}\left(\frac{b+\sqrt{\Delta}}{2a}, \frac{b-\sqrt{\Delta}}{2a}\right) \tag{3.4}$$

The aim of the following construction is to determine all reduced forms that are properly equivalent to the form f.

For any integer i, we set $f_i = \rho^i(f)$ so that $f_0 = f$. We also set

$$B_0 := \frac{1}{a}B(f_0) = \left((1,1), \left(\frac{b+\sqrt{\Delta}}{2a}, \frac{b-\sqrt{\Delta}}{2a}\right)\right).$$

Observe that $B_0 = ((1,1), (\theta(f)))$ so by Proposition 3.3.12-3, we have $f_{B_0} = \frac{1}{a}f$. Observe also that B_0 is positively oriented as a basis of L because

$$o(B_0) = sign\left(\frac{b+\sqrt{\Delta}}{2a} - \frac{b-\sqrt{\Delta}}{2a}\right) = sign\left(\frac{\sqrt{\Delta}}{a}\right) > 0$$

For $i \geq 0$, we define $B_{i+1} = B_i U(f_i)$ and for $i < 0$, we set $B_{i-1} = B_i V(f_i)$. Since the matrices $U(f_i) \in \mathrm{GL}_2(\mathbb{Z})$ and $V(f_i) \in \mathrm{GL}_2(\mathbb{Z})$ for all integer i by Observation 3.3.1 we see that B_i is a positively oriented basis of L for all $i \in \mathbb{Z}$. By construction, we also have $f_{i+1} = f_i U(f_i)$ and $f_{i-1} = f_i V(f_i)$ for all $i \in \mathbb{Z}$. By Proposition 3.3.12, we have $f_{B_i} = \frac{1}{a}f_i$ for all $i \in \mathbb{Z}$. Notice that for any integer i, the form f_i is reduced as f is reduced. Hence by Corollary 3.4.14 we deduce that B_i is a minimal basis of L for all $i \in \mathbb{Z}$. For $i \in \mathbb{Z}$, write $B_i = (\mu_i, \mu_{i+1})$ and by Proposition 3.3.12-2 observe that $\theta(f_i) = \frac{\mu_{i+1}}{\mu_i}$. Since $\mu_i \in A_1$, we write $\mu_i = (\mu_{i,1}, \mu_{i,2})$ for $i \in \mathbb{Z}$.

Proposition 3.4.15. *For any integer i, the inequalities $|\mu_{i+1,1}| > |\mu_{i,1}|$ and $|\mu_{i+2,1}| > 2|\mu_{i,1}|$ hold.*

Proof. Let $i \in \mathbb{Z}$. Since B_i is a minimal basis of the lattice L, we know by definition that that $|\mu_{i,1}| < |\mu_{i+1,1}|$ which is the same as the first inequality. In order to prove the second one, we define:

$$\alpha_1 := sign(\mu_{i+2,1})\mu_{i+2,1} - sign(\mu_{i,1})\mu_{i,1}$$

$$\alpha_2 := sign(\mu_{i+2,1})\mu_{i+2,2} - sign(\mu_{i,1})\mu_{i,2}$$

$$\alpha := (\alpha_1, \alpha_2)$$

and assume not and say $|\mu_{i+2,1}| \leq 2|\mu_{i,1}|$. Then

$$|\mu_{i,1}| < |\mu_{i+1,1}| < |\mu_{i+2,1}| \leq 2|\mu_{i,1}|$$

which implies that

$$|\alpha_1| = ||\mu_{i+2,1}| - |\mu_{i,1}|| \leq |\mu_{i,1}|$$

By Proposition 3.4.3 we have that $\frac{N(\mu_{i+1})}{N(\mu_i)} < 0$ as f_i is a reduced form which shows that $sign(N(\mu_i)) = sign(N(\mu_{i+2}))$ which implies that the real numbers $sign(\mu_{i+2,1})\mu_{i+2,2}$ and $sign(\mu_{i,1})\mu_{i,1}$ have the same sign. By the minimality of the bases B_i and B_{i+1} we have $|\mu_{i+2,2}| < |\mu_{i,2}|$. Combining we get

$$|\alpha_2| = |sign(\mu_{i+2,1})\mu_{i+2,2} - sign(\mu_{i,1})\mu_{i,2}| < |\mu_{i,2}|$$

Since B_i is a minimal basis of L, we know that μ_i is a minimal point of L and clearly α is a non-zero point in L. Combining with the inequalities $|\alpha_1| \leq |\mu_{i,1}|$ and $|\alpha_2| < |\mu_{i,2}|$ we derive a contradiction. □

Remark 3.4.2. We remark that by Proposition 3.4.15, we conclude $\lim_{i\to+\infty}|\mu_{i,1}| = \infty$ and $\lim_{i\to-\infty}|\mu_{i,1}| = 0$.

Theorem 3.4.16. *The set of all minimal points of L is*

$$MP(L) := \{\pm\mu_i : i \in \mathbb{Z}\}$$

and the set of all positively oriented minimal bases of L is

$$MB(L) := \{\pm B_i : i \in \mathbb{Z}\}$$

Proof. Let L be as in (3.4). Let us begin with the discussion of the minimal points of L: Let $\alpha = (\alpha_1, \alpha_2)$ be a minimal point of L. We will show that $\alpha \in MP(L)$. By Remark 3.4.2 we know that there exists an integer i such that $|\mu_{i,1}| \leq |\alpha_1| < |\mu_{i+1,1}|$. It suffices to show that either $\alpha = \mu_i$ or $\alpha = -\mu_i$. Assume not and say $\alpha \neq \pm\mu_i$. Then we have $|\mu_{i,1}| < |\alpha_1| < |\mu_{i+1,1}|$. We know that $B_i = (\mu_i, \mu_{i+1})$ is a minimal basis of L so by definition we have that $|\mu_{i,2}| < |\alpha_2|$. The inequalities $|\mu_{i,1}| < |\alpha_1|$ and $|\mu_{i,2}| < |\alpha_2|$ contradicts the minimality of the point α. Note that μ_i is a minimal point of L for all $i \in \mathbb{Z}$ as B_i is a minimal basis of L for all $i \in \mathbb{Z}$. Now, about

the discussion on positively oriented minimal bases of L, we already know that for all $i \in \mathbb{Z}$, B_i is a minimal basis of the lattice L with positive orientation. It follows that $-B_i$ is a minimal basis of L with positive orientation for all $i \in \mathbb{Z}$. Conversely, let $B = (\alpha, \beta) = ((\alpha_1, \alpha_2), (\beta_1, \beta_2))$ be a positively oriented minimal basis of L. We will show that $B \in MB(L)$. Since B is a minimal basis of L, we know that α is a minimal point of L so by the first part of this theorem we know that there exists an integer i and $j \in \{\pm 1\}$ such that $\alpha = j\mu_i$. We will show that $jB_i = B$. Observe that both jB_i and B are positively oriented minimal bases of L with a common element α which implies that it suffices to show that $\beta = j\mu_{i+1}$. Assume not and say $\beta \neq j\mu_{i+1}$. Since B is a minimal basis of L by definition we know that $|\beta_2| < |\alpha_2| = |\mu_{i,2}|$. Now if $|\beta_1| < |\mu_{i+1,1}|$ then we have a contradiction with the fact that B_i is a minimal basis of L. Similarly if $|\beta_1| > |\mu_{i+1,1}|$ then we have contradiction with the minimality of the basis B so by Proposition 3.3.8 we have that $\beta = \pm\mu_{i+1}$. Thus $B = jB_i$. □

Corollary 3.4.17. *Let f be an integral indefinite reduced form. Then the set of all reduced forms that are properly equivalent to f is $\{\rho^i(f) : i \in \mathbb{Z}\}$.*

Proof. Let f be a integral indefinite reduced form and let g be a reduced indefinite binary quadratic form that is properly equivalent to f. Then we know that there exists a matrix $U \in \mathrm{SL}_2(\mathbb{Z})$ such that $g = fU$. We have:

$$\begin{aligned} g &= fU \\ &= af_{B_0}U \text{ by Proposition 3.3.12} \\ &= af_C \text{ by Proposition 3.3.11} \end{aligned}$$

Since g is a reduced form, by Corollary 3.4.14 we have that C is a minimal basis of L. It follows from the Theorem 3.4.16 that there exists an integer i such that $B_i = C$. Hence

$$g = af_{B_i} = f_i := \rho^i(f)$$

□

3.5 The automorphism group of indefinite forms

3.5.1 Cycles of forms

Given any indefinite integral binary quadratic form $f = (a, b, c)$, we set the following operator:

$$\tau(f) := f \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = (-a, b, -c)$$

Observe that the τ operator commutes with the reduction operator ρ and τ^2 is the identity operator. Indeed,

$$\tau\rho(f) = \rho\tau(f) = (-c, -b + 2s(f)c, -(cs(f)^2 - bs(f) + a))$$

and

$$\tau^2((a, b, c)) = \tau(\tau(a, b, c)) = \tau((-a, b, -c)) = (a, b, c)$$

for any binary quadratic form (a, b, c). Notice also that the forms f and $\tau(f)$ are equivalent they are not necessarily properly equivalent. To see this, take $f = (-1, 1, 1)$ and compute $\tau(f) = f$. We also have that $f \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = (-1, 1, 1)$. In this case f and $\tau(f)$ are properly equivalent as $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

Definition 3.5.1. Let f be an primitive integral indefinite binary quadratic form.

- The **proper cycle of** f is the sequence $(\rho^i(g))_{i\in\mathbb{Z}}$ where g is a reduced form with $g = fU$ for some matrix $U \in \mathrm{SL}_2(\mathbb{Z})$.

- The **cycle of** f is the sequence $((\tau\rho)^i(g))_{i\in\mathbb{Z}}$ where $g = (A, B, C)$ is a reduced form with A being positive such that $g = fU$ for some matrix $U \in \mathrm{GL}_2(\mathbb{Z})$.

Remark 3.5.1. Given any primitive integral indefinite binary quadratic form f, its cycle is an invariant of its equivalence class.

By Corollary 3.4.2, we know that there are finitely many reduced forms in the cycle and the proper cycle of f, so we will denote them by their period $(f_0, f_1, \ldots, f_{l-1})$ where f_0 is an arbitrary reduced form that is in the cycle of f.

Example 3.5.1. Let us find the cycle and the proper cycle of the form $f = (1, 3, -1)$ which is already reduced by Example 3.4.1. Note that $s(f) = -\left\lfloor \frac{3+\sqrt{13}}{2} \right\rfloor = -3$ as $|c| = 1 < \sqrt{13}$. Then

$$(\tau\rho)(f) = (1, -3 + 2(-3)(-1), -((-1)(-3)^2 - 3(-3) + 1)) = (1, 3, -1) = f$$

Therefore $l = 1$ and (f) is the cycle of f. For the proper cycle of f, we compute:

$$\rho(f) = (-1, -3 + 2(-3)(-1), (-1)(-3)^2 - 3(-3) + 1) = (-1, 3, 1)$$

and $s(\rho(f)) = \left\lfloor \frac{3+\sqrt{13}}{2} \right\rfloor = 3$. Then,

$$\rho^2(f) = \rho(\rho(f)) = (1, -3 + 2 \cdot 3 \cdot 1, 1 \cdot 3^2 - 3 \cdot 3 - 1) = (1, 3, -1) = f$$

Therefore, $((1, 3, -1), (-1, 3, 1))$ is the proper cyle of f.

Proposition 3.5.1. *If f is a primitive integral indefinite binary quadratic form, then the cycle of f contains all reduced forms (A, B, C) with $A > 0$ that are equivalent to f.*

Proof. Let $f = (a, b, c)$ be a primitive integral indefinite binary quadratic form. The equivalence class of the form f contains a reduced form (x, y, z) with positive x. Indeed, by the Reduction Algorithm the equivalence class of f contains a reduced form, say (a', b', c'). If a' is positive, we are done. If not, then by Theorem 3.4.1 we know that c' is positive and by Corollary 3.4.4 the form (c', b', a') is reduced so without loss of generality, we may assume that $a > 0$. By the definition of the cycle of f, any reduced form (A, B, C) with $A > 0$ which is equivalent to f is in the cycle of f. Conversely, if (A, B, C) is a reduced form in the equivalence class of f with $A > 0$, then either the form (A, B, C) or the form $\tau(A, B, C) = (-A, B, -C)$ is properly equivalent to f. Indeed, $(A, B, C) = fU$ for some matrix $U \in \mathrm{GL}_2(\mathbb{Z})$. If $U \in \mathrm{SL}_2(\mathbb{Z})$, we have that the form (A, B, C) is properly equivalent to f. Otherwise, $\det(U) = -1$ and

$$\tau(A, B, C) = (A, B, C)\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = (fU)\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = f\left(U\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right)$$

Clearly, the matrix $U\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$ is in $\mathrm{SL}_2(\mathbb{Z})$ which implies that $(-A, B, -C)$ is properly equivalent to f. If (A, B, C) is in the proper cycle of f, by Proposition 3.5.2, $(A, B, C) = \rho^i(f)$ for some $i \in \mathbb{Z}$. Moreover, we observe that i is even as both the coefficients A and a are positive and the sign of the coefficient of X^2 of the form $\rho^j(f)$ is determined by $(-1)^j$. We know that τ^2 is identity and the operators τ and ρ commute. This implies that $(A, B, C) = (\tau\rho)^i(f)$. Thus the form (A, B, C) is in the cycle of f. If $(-A, B, -C)$ belongs to the proper cycle of f, then

$$(-A, B, -C) = \tau(A, B, C) = \rho^i(f)$$

for some odd integer i as $-A < 0$. Hence

$$(A, B, C) = \tau(\rho^i(f)) = (\tau\rho^i)(f) = (\tau\rho)^i(f)$$

because i is odd which implies that (A, B, C) is in the cycle of f. □

Proposition 3.5.2. *If f is a primitive integral indefinite binary quadratic form, then the proper cycle of f consists of all reduced forms which are properly equivalent to f.*

Proof. This proposition directly follows from Corollary 3.4.17. □

Now, we will introduce an algorithm that computes the cycle of a given indefinite integral binary quadratic form $f = (a, b, c)$ with $a > 0$ of discriminant Δ:
Set $f_0 = (a_0, b_0, c_0) = f$ and $s_i := |s(f_i)| = \left\lfloor \frac{b_i + \lfloor\sqrt{\Delta}\rfloor}{2|c_i|} \right\rfloor$ We then have:

$$\begin{aligned} f_{i+1} &= (|c_i|, -b_i + 2s_i|c_i|, -(a_i + b_i s_i + c_i s_i^2)) \\ &:= (a_{i+1}, b_{i+1}, c_{i+1}) \\ &= f_i \begin{pmatrix}0 & 1\\ 1 & s_i\end{pmatrix} \end{aligned}$$

In order to find matrices $T_i := \begin{pmatrix}p_i & p_{i+1}\\ q_i & q_{i+1}\end{pmatrix}$ that satisfies $f_i = fT_i$, we set $T_0 = I_2$ and recursively get $p_{i+2} = s_i p_{i+1} + p_i$ and $q_{i+2} = s_i q_{i+1} + q_i$ for $i \in \mathbb{Z}_{\geq 0}$. In fact, we

have

$$T_i = \prod_{j=0}^{i-1} \begin{pmatrix} 0 & 1 \\ 1 & s_j \end{pmatrix} \text{ for } i \in \mathbb{Z}_{\geq 0}. \tag{3.5}$$

Observation 3.5.1. ([Buchmann and Vollmer, 2007], Lemma 6.10.8)

- For $i \in \mathbb{Z}_{\geq 3}$, we have $p_{i+1} > p_i > 0$ and $p_{i+2} \geq 2p_i$.
- For $i \in \mathbb{Z}_{\geq 2}$, we have $q_{i+1} > q_i > 0$ and $q_{i+2} \geq 2q_i$.

3.5.2 Aut(f)

The aim of the following discussion is to determine the automorphism group of a given irrational integral indefinite binary quadratic form. Let $f = (a, b, c)$ be an irrational integral indefinite binary quadratic form, $U \in \mathrm{GL}_2(\mathbb{Z})$ such that the form $f_0 := fU$ is reduced. Say $f_0 = (A, B, C)$ and suppose that $A > 0$. Note that the existence of such a form f_0 in the equivalence class of f follows from Corollary 3.4.10 and Proposition 3.5.1. Denote the cycle of f by $(f_0, f_1, \ldots, f_{l-1})$ which is of length $l \in \mathbb{Z}$. Let T_l be the matrix as in (3.5). By construction, we know that $f_0 = f_0 T_l$ which implies that T_l is an automorphism of f_0. Since $f_0 := fU$, we have that $fU = fUT_l$ so $f = fUT_lU^{-1}$. Therefore we see that the matrix UT_lU^{-1} is an automorphism of the form f. From now on, we set $T := UT_lU^{-1}$ and relate T with $Aut(f)$.

Lemma 3.5.3. *The cyclic group $\langle T \rangle = \{T^i : i \in \mathbb{Z}\}$ is of infinite order.*

Proof. It suffices to show that the matrices T^i and T^j are distinct for any $i, j \in \mathbb{Z}_{\geq 0}$ with $i \neq j$. By fact (3.5), we know that $T_l = \prod_{i=0}^{l-1} \begin{pmatrix} 0 & 1 \\ 1 & s_i \end{pmatrix}$ and by Observation 3.5.1 we have that the entries of T are positive except for the one which is in the $(1,1)$-position. Observe also that for any integer i, we have $T^i = UT_l^iU^{-1}$. Combining, we see that the entry that is in the $(2,2)$-position in the matrix T^i is strictly increasing. Therefore the matrices T^i are pairwise distinct for $i \in \mathbb{Z}_{\geq 0}$ which implies that $\langle T \rangle$ is an infinite group. □

Theorem 3.5.4. *The automorhism group of f, $Aut(f)$, is given by*

$$\langle -1 \rangle \times \langle T \rangle = \{\pm T^i : i \in \mathbb{Z}\}$$

Proof. By construction, we have $\langle -1 \rangle \times \langle T \rangle \subset Aut(f)$. Conversely, let us consider first the case where $U = I_2$ which implies that $f_0 = f$ and $T_l = T$. Recall the construction that is just before the Proposition 3.4.15: For any $i \in \mathbb{Z}$, we have $f_{B_i} = \frac{1}{a} f_i$ where B_i denotes the minimal basis of L as in (3.4). Let $V \in Aut(f)$. We have:

$$\begin{aligned} f_{B_0 V} &= f_{B_0} V \text{ by Proposition 3.3.11} \\ &= \frac{1}{a} f_0 V \\ &= \frac{1}{a} f_0 \text{ as } V \in Aut(f) \\ &= \frac{1}{a} f \text{ as } f_0 = f \end{aligned}$$

Observe that the form $f_{B_0 V}$ is reduced as f is reduced so by Corollary 3.4.14 we know that $B_0 V$ is a minimal basis of L. By Theorem 3.4.16 there exists an integer i such that $B_0 V \in \{\pm B_i\}$. But by construction we know that $B_i = B_0 T_i$ hence $V \in \{\pm T_i\}$. Again by construction we know that $f_i = f T_i = fV = f$, we deduce that $i \equiv 0 \pmod{l}$ as l is the length of the cycle of f therefore minimal. Combining, we get $V \in \{\pm T_l^j\}$ for some $j \in \mathbb{Z}$. Thus, $V \in \langle -1 \rangle \times \langle T \rangle$. Now, for the general case observe first that for $V \in \mathrm{GL}_2(\mathbb{Z})$, we have:

$$\begin{aligned} V \in Aut(f) &\iff fV = f \\ &\iff fVU = fU \\ &\iff fUU^{-1}VU = fU \\ &\iff f_0 U^{-1} V U = f_0 \\ &\iff U^{-1} V U \in Aut(f_0) \end{aligned}$$

which implies that $U^{-1}VU \in \{\pm T_l^i : i \in \mathbb{Z}\}$ but this holds if and only if $V \in \{\pm T^i : i \in \mathbb{Z}\}$. □

Definition 3.5.2. The matrix T is called the **fundamental automorphism of** f.

Example 3.5.2. Let us determine the fundamental automorphism of the form $f = (1, 3, -1)$. By Example 3.5.1, we know that $U = I_2$ and $T_l = \begin{pmatrix} 0 & 1 \\ 1 & 3 \end{pmatrix}$. Therefore $T = I_2 \begin{pmatrix} 0 & 1 \\ 1 & 3 \end{pmatrix} I_2 = T_l$ is the fundamental automorphism of f and

$$Aut(f) = \left\{ \pm \begin{pmatrix} 0 & 1 \\ 1 & 3 \end{pmatrix}^i : i \in \mathbb{Z} \right\}$$

Below we state a theorem which is not used in the rest of our work but still worth mentioning because it beautifully relates $Aut(f)$, $Aut^+(f)$ and the cycle of f:

Theorem 3.5.5. *([Buchmann and Vollmer, 2007], Theorem 6.12.4) Let T be the fundamental automorphism of f. If the length l of the cycle of f is odd, then $Aut(f) = \langle -1 \rangle \times \langle T^2 \rangle$ and if l is even, then $Aut^+(f) = Aut(f)$.*

Chapter 4

REAL QUADRATIC NUMBER FIELDS

In this chapter we will concentrate on real quadratic number fields. First, we fix a real quadratic number field K and to each element of $\mathrm{Cl}^+(K)$, we attach a primitive integral indefinite binary quadratic form and show that this correspondence is one to one. We then express each element of $\widetilde{\mathrm{Pic}^0(K)}$ in the language of binary quadratic forms.

4.1 Forms and fractional ideals

Let us start with some important yet basic facts on real quadratic fields: It is known that any real quadratic number field is of the form

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$$

where d is a square-free positive integer. For such a number field, its ring of integers is :

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

and its discriminant is :

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

Notice that any real quadratic field can be expressed as $\mathbb{Q}(\sqrt{\Delta_K})$. Those $\Delta \in \mathbb{R}_{>0}$ which are the discriminants of a quadratic number field are called fundamental discriminants. Throughout this chapter, we fix a real quadratic field $K = \mathbb{Q}(\sqrt{\Delta_K})$. Let σ_1 denote the identity embedding of K and σ_2 denote the embedding of K that

sends each element of K to its Galois conjugate. Namely, for $a + b\sqrt{\Delta_K} \in K$:

$$\sigma_1(a + b\sqrt{\Delta_K}) = a + b\sqrt{\Delta_K}$$
$$\sigma_2(a + b\sqrt{\Delta_K}) = a - b\sqrt{\Delta_K}$$

Set $\bar{\alpha} := \sigma_2(\alpha)$ for $\alpha \in K$. Let $I \in Id(K)$. Then I has a basis of the form $\{\alpha_1, \alpha_2\}$ as a $\mathbb{Z}$-module. We have:

$$\det\left(\begin{pmatrix} \alpha_1 & \alpha_2 \\ \bar{\alpha_1} & \bar{\alpha_2} \end{pmatrix}\right)^2 = \Delta_K \cdot N(I)^2 \tag{4.1}$$

so that

$$\det\begin{pmatrix} \alpha_1 & \alpha_2 \\ \bar{\alpha_1} & \bar{\alpha_2} \end{pmatrix} = \pm\sqrt{\Delta_K} \cdot N(I)$$

This motivates the following definition:

Definition 4.1.1. Let $I = \langle \alpha_1, \alpha_2 \rangle \in Id(K)$. The $\mathbb{Z}$-basis $\{\alpha_1, \alpha_2\}$ of the fractional ideal I is called **normalized** if

$$\det\begin{pmatrix} \alpha_1 & \alpha_2 \\ \bar{\alpha_1} & \bar{\alpha_2} \end{pmatrix} = \sqrt{\Delta_K} \cdot N(I) \tag{4.2}$$

Remark 4.1.1. Given any $I = \langle \alpha_1, \alpha_2 \rangle \in Id(K)$, exactly one of the $\mathbb{Z}$-bases $\{\alpha_1, \alpha_2\}$, $\{\alpha_2, \alpha_1\}$ is normalized.

Definition 4.1.2. Let $I = \langle \alpha_1, \alpha_2 \rangle \in Id(K)$ with normalized basis $\{\alpha_1, \alpha_2\}$. The binary quadratic form

$$P_{\{\alpha_1,\alpha_2\}}(X, Y) := \frac{N_{K/\mathbb{Q}}(\alpha_1 X + \alpha_2 Y)}{N(I)}$$

is called the **form associated to** I.

Observation 4.1.1. We have:

$$\begin{aligned} N_{K/\mathbb{Q}}(\alpha_1 X + \alpha_2 Y) :&= (\alpha_1 X + \alpha_2 Y)(\bar{\alpha_1} X + \bar{\alpha_2} Y) \\ &= \alpha_1\bar{\alpha_1} X^2 + (\alpha_1\bar{\alpha_2} + \bar{\alpha_1}\alpha_2) XY + \alpha_2\bar{\alpha_2} Y^2 \end{aligned}$$

Therefore, $P_{\{\alpha_1,\alpha_2\}} = \left(\frac{\alpha_1\bar{\alpha_1}}{N(I)}, \frac{\alpha_1\bar{\alpha_2}+\bar{\alpha_1}\alpha_2}{N(I)}, \frac{\alpha_2\bar{\alpha_2}}{N(I)}\right) = \left(\frac{N_{K/\mathbb{Q}}(\alpha_1)}{N(I)}, \frac{Tr_{K/\mathbb{Q}}(\alpha_1\bar{\alpha_2})}{N(I)}, \frac{N_{K/\mathbb{Q}}(\alpha_2)}{N(I)}\right)$.

Proposition 4.1.1. *If $I = \langle \alpha_1, \alpha_2 \rangle \in Id(K)$ with normalized basis $\{\alpha_1, \alpha_2\}$, then $P_{\{\alpha_1,\alpha_2\}}(X, Y)$ is a primitive integral indefinite binary quadratic form of discriminant Δ_K.*

Proof. Let $I = \langle \alpha_1, \alpha_2 \rangle \in Id(K)$ with normalized basis $\{\alpha_1, \alpha_2\}$. Since I is a fractional ideal, we know that there exists a non-zero integer α such that $\alpha I \subset \mathbb{Z}_K$, which shows that without loss of generality we may assume that I is an integral ideal of K so that α_1 and α_2 are algebraic integers. We first show that the form associated to I is integral: For any integers X and Y, we have $b := \alpha_1 X + \alpha_2 Y \in I$ which implies that $I \big| (b)$ as ideals. Therefore, $N(I) \big| N((b)) = N_{K/\mathbb{Q}}(b)$ in $\mathbb{Z}$. Set $P := P_{\{\alpha_1,\alpha_2\}}$ and observe that $P(1,0) = \frac{N_{K/\mathbb{Q}}(\alpha_1)}{N(I)}$, $P(0,1) = \frac{N_{K/\mathbb{Q}}(\alpha_2)}{N(I)}$ and $P(1,1) = \frac{N_{K/\mathbb{Q}}(\alpha_1)}{N(I)} + \frac{Tr_{K/\mathbb{Q}}(\alpha_1\bar{\alpha_2})}{N(I)} + \frac{N_{K/\mathbb{Q}}(\alpha_2)}{N(I)}$ are all integers which implies that P is an integral form by Observation 4.1.1. Let us compute the discriminant of P:

$$\begin{aligned}
\Delta_P &= \frac{1}{N(I)^2}\left(\alpha_1\bar{\alpha_2} + \bar{\alpha_1}\alpha_2\right)^2 - \frac{4}{N(I)^2}\alpha_1\bar{\alpha_1}\alpha_2\bar{\alpha_2} \\
&= \frac{1}{N(I)^2}\left[\left(\alpha_1\bar{\alpha}_2 + \bar{\alpha}_1\alpha_2\right)^2 - 4\left(\alpha_1\bar{\alpha}_1\alpha_2\bar{\alpha}_2\right)\right] \\
&= \frac{1}{N(I)^2}\left[\alpha_1^2\bar{\alpha_2}^2 + 2\alpha_1\bar{\alpha}_2\bar{\alpha}_1\alpha_2 + \bar{\alpha_1}^2\alpha_2^2 - 4\alpha_1\bar{\alpha}_1\alpha_2\bar{\alpha}_2\right] \\
&= \frac{1}{N(I)^2}\left[\alpha_1\bar{\alpha_2} - \bar{\alpha}_1\alpha_2\right]^2 \\
&= \frac{1}{N(I)^2}\cdot N(I)^2 \cdot \Delta_K \text{ by (4.1)} \\
&= \Delta_K
\end{aligned}$$

We now show that P is a primitive form: Set $a := \frac{N_{K/\mathbb{Q}}(\alpha_1)}{N(I)}$, $b := \frac{Tr_{K/\mathbb{Q}}(\alpha_1\bar{\alpha_2})}{N(I)}$ and $c := \frac{N_{K/\mathbb{Q}}(\alpha_2)}{N(I)}$. Assume not and say there exists a prime number p such that $p|a$, $p|b$ and $p|c$. Then $p^2 \big| \Delta_P = \Delta_K$. If $d \equiv 1 \pmod 4$ we have a contradiction as d is square-free. If $d \equiv 2, 3 \pmod 4$, then $p^2 \big| 4$ which happens if and only if $p = 2$. We

then have:

$$\begin{aligned} d &= \frac{1}{4}D_K \\ &= \frac{1}{4}(b^2 - 4ac) \\ &= \left(\frac{b}{2}\right)^2 - 4\frac{a}{2}\frac{c}{2} \\ &\equiv \left(\frac{b}{2}\right)^2 \pmod 4 \\ &\equiv 0, 1 \pmod 4 \end{aligned}$$

which again leads to a contradiction. □

Lemma 4.1.2. *Let I be a fractional ideal of K. Any two normalized bases of I give rise to properly equivalent forms associated to I.*

Proof. Let $I \in Id(K)$ and let $\alpha = \{\alpha_1, \alpha_2\}$, $\beta = \{\beta_1, \beta_2\}$ be two normalized bases of I. We know that there exists a matrix $U \in \mathrm{GL}_2(\mathbb{Z})$, which is in fact the change of basis matrix, such that $\beta = U\alpha$. Since α and β are both normalized, they both satisfy the Equation (4.2) which implies that $U \in \mathrm{SL}_2(\mathbb{Z})$. Observe that

$$\beta_1 X + \beta_2 Y = \begin{pmatrix} \beta_1 & \beta_2 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} = U \begin{pmatrix} \alpha_1 & \alpha_2 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} = U\left(\alpha_1 X + \alpha_2 Y\right)$$

Therefore, $N_{K/\mathbb{Q}}(\beta_1 X + \beta_2 Y) = N_{K/\mathbb{Q}}(U\left(\alpha_1 X + \alpha_2 Y\right))$ which implies that

$$P_{\{\beta_1,\beta_2\}} = P_{\{\alpha_1,\alpha_2\}} U.$$

□

Lemma 4.1.3. *Let I_1, $I_2 \in Id(K)$ with normalized bases $\{\alpha_1, \alpha_2\}$, $\{\beta_1, \beta_2\}$, respectively. Suppose that I_1 and I_2 are in the same narrow ideal class. Then the forms associated to I_1 and I_2 are properly equivalent.*

Proof. Let I_1, $I_2 \in Id(K)$ be two fractional ideals that are in the same narrow ideal class with normalized bases $\{\alpha_1, \alpha_2\}$, $\{\beta_1, \beta_2\}$, respectively. We then know that there exists a totally positive element $\gamma \in K^\times$ such that $I_2 = (\gamma)I_1$. Clearly, the

set $\{\gamma\alpha_1, \gamma\alpha_2\}$ is another $\mathbb{Z}$-basis of the fractional ideal I_2. Moreover, this basis is normalized as:

$$\det \begin{pmatrix} \gamma\alpha_1 & \gamma\alpha_2 \\ \bar{\gamma}\bar{\alpha_1} & \bar{\gamma}\bar{\alpha_2} \end{pmatrix} = N_{K/\mathbb{Q}}(\gamma) \det \begin{pmatrix} \alpha_1 & \alpha_2 \\ \bar{\alpha_1} & \bar{\alpha_2} \end{pmatrix} > 0$$

by the total positivity of the element γ. We also have:

$$\begin{aligned} P_{\{\gamma\alpha_1,\gamma\alpha_2\}} &= \frac{N_{K/\mathbb{Q}}(\gamma\alpha_1 X + \gamma\alpha_2 Y)}{N((\gamma)I_1)} \\ &= \frac{N_{K/\mathbb{Q}}(\gamma(\alpha_1 X + \alpha_2 Y))}{N((\gamma)I_1)} \\ &= \frac{N_{K/\mathbb{Q}}(\gamma)N_{K/\mathbb{Q}}(\alpha_1 X + \alpha_2 Y)}{N_{K/\mathbb{Q}}(\gamma)N(I_1)} \text{ as } N_{K/\mathbb{Q}} \text{ is multiplicative and } (\gamma) \text{ is principal.} \\ &= \frac{N_{K/\mathbb{Q}}(\alpha_1 X + \alpha_2 Y)}{N(I_1)} \\ &= P_{\{\alpha_1,\alpha_2\}} \end{aligned}$$

Now, the result follows from Lemma 4.1.2. □

Theorem 4.1.4. *The map*

$$\begin{aligned} \mathscr{C} : \mathrm{Cl}^+(K) &\to \mathscr{F}(\Delta_K)/\mathrm{SL}_2(\mathbb{Z}) \\ [\langle\alpha_1, \alpha_2\rangle] &\mapsto \left[P_{\{\alpha_1,\alpha_2\}}\right] \end{aligned}$$

is a well-defined bijection, where $\mathscr{F}(\Delta_K)$ is set of primitive integral indefinite binary quadratic forms of discriminant Δ_K and the set $\{\alpha_1, \alpha_2\}$ is a normalized basis of the fractional ideal $\langle\alpha_1, \alpha_2\rangle$.

Proof. The fact that the map $\mathscr{C}$ is well-defined follows from Lemma 4.1.3. We show that $\mathscr{C}$ is surjective: Let $f = (a, b, c) \in \mathscr{F}(\Delta_K)$. Then, $I = \langle a, \frac{b-\sqrt{\Delta_K}}{2}\rangle \in Id(K)$. Set $\gamma := \sqrt{\Delta_K}$ if $a < 0$ and take $\gamma := 1$ if $a > 0$. Observe that $\gamma I = \langle \gamma a, \gamma\frac{b-\sqrt{\Delta_K}}{2}\rangle \in Id(K)$. We compute the ideal norm of γI:

$$\begin{aligned} N(\gamma I) &= |N_{K/\mathbb{Q}}(\gamma)|N(I) \\ &= |N_{K/\mathbb{Q}}(\gamma)|)\left|\frac{1}{\sqrt{\Delta_K}} \det \begin{pmatrix} a & \frac{b-\sqrt{\Delta_K}}{2} \\ a & \frac{b+\sqrt{\Delta_K}}{2} \end{pmatrix}\right| \\ &= |aN_{K/\mathbb{Q}}(\gamma)| \end{aligned}$$

so the $\mathbb{Z}$-basis of γI is always normalized. We also compute:

$$\begin{aligned} N_{K/\mathbb{Q}}\left(\gamma a X + \gamma\frac{b-\sqrt{\Delta_K}}{2}Y\right) &= N_{K/\mathbb{Q}}(\gamma)N_{K/\mathbb{Q}}\left(aX + \frac{bY}{2} - \frac{\sqrt{\Delta_K}Y}{2}\right) \\ &= N_{K/\mathbb{Q}}(\gamma)\left[\left(aX+\frac{bY}{2}\right)^2 - \frac{\Delta_K}{4}Y^2\right] \\ &= N_{K/\mathbb{Q}}(\gamma)\left(a^2X^2 + \frac{2aXbY}{2} + \frac{b^2Y^2}{4} - \frac{\Delta_K Y^2}{4}\right) \\ &= N_{K/\mathbb{Q}}(\gamma)\left(a^2X^2 + abXY + \frac{Y^2\left(b^2-b^2+4ac\right)}{4}\right) \\ &= N_{K/\mathbb{Q}}(\gamma)\left(a^2X^2 + abXY + acY^2\right) \end{aligned}$$

We claim that $\mathscr{C}([\gamma I]) = P_{\{\gamma a, \gamma\frac{b-\sqrt{\Delta_K}}{2}\}} = f$. Indeed,

$$\begin{aligned} P_{\{\gamma a,\gamma\frac{b-\sqrt{\Delta_K}}{2}\}}(X,Y) &= \frac{N_{K/\mathbb{Q}}\left(\gamma a X + \gamma\frac{b-\sqrt{\Delta_K}}{2}Y\right)}{N(\gamma I)} \\ &= \frac{N_{K/\mathbb{Q}}(\gamma)\left(a^2X^2+abXY+acY^2\right)}{|aN_{K/\mathbb{Q}}(\gamma)|} \\ &= f(X,Y) \end{aligned}$$

We now show that $\mathscr{C}$ is injective: Let $I_1,\ I_2 \in Id(K)$ with normalized bases $\alpha = \{\alpha_1,\alpha_2\}$, $\beta = \{\beta_1,\beta_2\}$, respectively. Assume that $P_{\{\beta_1,\beta_2\}} = P_{\{\alpha_1,\alpha_2\}}U$ for some $U \in \mathrm{SL}_2(\mathbb{Z})$. If we replace the $\mathbb{Z}$-basis β of I_2 by βU then we deduce that the forms associated to I_1 and I_2 are the same so we may assume that $P_{\{\beta_1,\beta_2\}} = P_{\{\alpha_1,\alpha_2\}}$. We need to find a totally positive element $\gamma \in K^\times$ such that $I_1 = (\gamma)I_2$. Consider the roots of the polynomial:

$$P_{\{\alpha_1,\alpha_2\}}(1,Y) = \frac{1}{N(I_1)}(\alpha_1\bar{\alpha_1} + (\alpha_1\bar{\alpha_2} + \bar{\alpha_1}\alpha_2)Y + \alpha_2\bar{\alpha_2})$$

which are $-\frac{\alpha_1}{\alpha_2}$ and $-\frac{\bar{\alpha_1}}{\bar{\alpha_2}}$. Similarly, the roots of the polynomial $P_{\{\beta_1,\beta_2\}}(1,Y)$ are $-\frac{\beta_1}{\beta 2}$ and $-\frac{\bar{\beta_1}}{\bar{\beta_2}}$. Since these two polynomials are the same, either $\frac{\alpha_1}{\alpha_2} = \frac{\beta_1}{\beta 2}$ or $\frac{\alpha_1}{\alpha_2} = \frac{\bar{\beta_1}}{\bar{\beta_2}}$. First, assume that $\frac{\alpha_1}{\alpha_2} = \frac{\bar{\beta_1}}{\bar{\beta_2}}$. Set $\lambda := \frac{\alpha_2}{\bar{\beta_2}} = \frac{\bar{\beta_1}}{\bar{\alpha_1}}$. Then $\alpha_1 = \lambda\bar{\beta_1}$ and $\alpha_2 = \lambda\bar{\beta_2}$. We have:

$$\det\begin{pmatrix}\alpha_1 & \alpha_2\\ \bar{\alpha_1} & \bar{\alpha_2}\end{pmatrix} = \det\begin{pmatrix}\lambda\bar{\beta_1} & \lambda\bar{\beta_2}\\ \bar{\lambda}\beta_1 & \bar{\lambda}\beta_2\end{pmatrix} = -N_{K/\mathbb{Q}}(\lambda)\det\begin{pmatrix}\beta_1 & \beta_2\\ \bar{\beta_1} & \bar{\beta_2}\end{pmatrix}$$

Since both bases are normalized, we have $N_{K/\mathbb{Q}}(\lambda) < 0$. On the other hand, $P_{\{\beta_1,\beta_2\}} = P_{\{\alpha_1,\alpha_2\}}$ implies $N_{K/\mathbb{Q}}(\lambda) > 0$ which shows that this case cannot arise. Now, we know that $\frac{\alpha_1}{\alpha_2} = \frac{\beta_1}{\beta_2}$. We have: $\alpha_1 = \beta_1\frac{\alpha_2}{\beta_2}$ and $\alpha_2 = \beta_2\frac{\alpha_1}{\beta_1}$. Set $\Gamma := \frac{\alpha_2}{\beta_2} = \frac{\alpha_1}{\beta_1}$. Again, since both bases are normalized, we have:

$$\sqrt{\Delta_K}N(I_1) = \det\begin{pmatrix}\alpha_1 & \alpha_2\\ \bar{\alpha_1} & \bar{\alpha_2}\end{pmatrix} = N_{K/\mathbb{Q}}(\Gamma)\det\begin{pmatrix}\beta_1 & \beta_2\\ \bar{\beta_1} & \bar{\beta_2}\end{pmatrix} = N_{K/\mathbb{Q}}(\Gamma)\sqrt{\Delta_K}N(I_2)$$

Therefore, $N_{K/\mathbb{Q}}(\Gamma) > 0$. Define

$$\gamma := \begin{cases}\Gamma & \text{if } \Gamma > 0\\ -\Gamma & \text{if } \Gamma < 0\end{cases}$$

Clearly, γ is a totally positive element of $K^\times$ and $I_1 = (\gamma)I_2$. □

4.2 Forms and $\widetilde{\mathrm{Div}^0(K)}$

In this section, we combine the theory of indefinite binary quadratic forms and oriented Arakelov class groups. We first explain a way of representing each element of $\mathscr{F}(\Delta_K)$ as an element of $\widetilde{\mathrm{Div}^0(K)}$. Notice first that by Corollary 2.2.2, we know that $K_{\mathbb{R}}^\times \cong \mathbb{R}^\times \times \mathbb{R}^\times$. To this end, given any $f = (a,b,c) \in \mathscr{F}(\Delta_K)$, we define $I_f := \langle 1, \frac{b-\sqrt{\Delta_K}}{2a}\rangle \in Id(K)$ and $\infty_f := \left(\frac{b-\sqrt{\Delta_K}}{2\sqrt{|c|}}, \frac{b+\sqrt{\Delta_K}}{2\sqrt{|c|}}\right) \in K_{\mathbb{R}}^\times$. By Equation (4.1), we have that $N(I_f) = \frac{1}{|a|}$. We claim that $(I_f, \infty_f) \in \widetilde{\mathrm{Div}^0(K)}$. We need to check that it is of degree 0. It suffices to show that $N(I_f)\mathcal{N}(|\infty_f|) = 1$. We have:

$$\begin{aligned}N(I_f)\mathcal{N}(|\infty_f|) &= \frac{1}{|a|}\frac{|b-\sqrt{\Delta_K}|}{2\sqrt{|c|}}\frac{|b+\sqrt{\Delta_K}|}{2\sqrt{|c|}}\\ &= \frac{1}{|a|}\frac{4|a||c|}{4|c|} \text{ as } \Delta_K = \Delta_f = b^2-4ac\\ &= 1\end{aligned}$$

Hence, we showed that the map:

$$\begin{aligned}&\mathbf{D} : \mathscr{F}(\Delta_K) \to \widetilde{\mathrm{Div}^0(K)}\\ &f = (a,b,c) \mapsto \left(\left\langle 1, \frac{b-\sqrt{\Delta_K}}{2a}\right\rangle, \left(\frac{b-\sqrt{\Delta_K}}{2\sqrt{|c|}}, \frac{b+\sqrt{\Delta_K}}{2\sqrt{|c|}}\right)\right)\end{aligned}$$

is well-defined.

By Proposition 2.4.2, we know that $\widetilde{\mathrm{Div}^0(K)} \cong (K^{\times}_{\mathbb{R},+})^0 \otimes (Id(K) \times \{\pm 1\}^2)$. We decompose (I_f, ∞_f) in $(K^{\times}_{\mathbb{R},+})^0 \otimes (Id(K) \times \{\pm 1\}^2)$ as follows: By Observation 2.4.2 we know that from the element (I_f, ∞_f), we derive

$$\left(\left(\frac{|b-\sqrt{\Delta_K}|}{2\sqrt{|c|}} \cdot \sqrt{\frac{1}{|a|}}, \frac{|b+\sqrt{\Delta_K}|}{2\sqrt{|c|}} \cdot \sqrt{\frac{1}{|a|}}\right), (I_f, sign(\infty_f))\right) = \left(\left(\frac{|b-\sqrt{\Delta_K}|}{2\sqrt{|ac|}}, \frac{|b+\sqrt{\Delta_K}|}{2\sqrt{|ac|}}\right), (I_f, sign(\infty_f))\right)$$

As K is a real quadratic field, we have

$$(K^{\times}_{\mathbb{R},+})^0 = \{(x_1, x_2) \in \mathbb{R}_{>0} \times \mathbb{R}_{>0} : x_1 x_2 = 1\}$$

In addition $\frac{|b-\sqrt{\Delta_K}|}{2\sqrt{|ac|}} \cdot \frac{|b+\sqrt{\Delta_K}|}{2\sqrt{|ac|}} = 1$. We conclude that the element $\left(\frac{|b-\sqrt{\Delta_K}|}{2\sqrt{|ac|}}, \frac{|b+\sqrt{\Delta_K}|}{2\sqrt{|ac|}}\right)$ is an element of $(K^{\times}_{\mathbb{R},+})^0$.

Let us discuss the two fundamental properties of the map $\mathbf{D}$:

- $\mathbf{D}$ is not injective: Let $f = (a, b, c)$, $g = (d, e, f) \in \mathscr{F}(\Delta_K)$ such that $\mathbf{D}(f) = \mathbf{D}(g)$. Then,

$$\left(\left\langle 1, \frac{b-\sqrt{\Delta_K}}{2a}\right\rangle, \left(\frac{b-\sqrt{\Delta_K}}{2\sqrt{|c|}}, \frac{b+\sqrt{\Delta_K}}{2\sqrt{|c|}}\right)\right) = \left(\left\langle 1, \frac{e-\sqrt{\Delta_K}}{2d}\right\rangle, \left(\frac{e-\sqrt{\Delta_K}}{2\sqrt{|f|}}, \frac{e+\sqrt{\Delta_K}}{2\sqrt{|f|}}\right)\right)$$

  which implies that $I_f = I_g$ and $\infty_f = \infty_g$. Since $\infty_f = \infty_g$, we have that $\frac{b-\sqrt{\Delta_K}}{2\sqrt{|c|}} = \frac{e-\sqrt{\Delta_K}}{2\sqrt{|f|}}$ and $\frac{b+\sqrt{\Delta_K}}{2\sqrt{|c|}} = \frac{e+\sqrt{\Delta_K}}{2\sqrt{|f|}}$ so that

$$e\sqrt{|c|} - \sqrt{|c|}\sqrt{\Delta_K} = b\sqrt{|f|} - \sqrt{|f|}\sqrt{\Delta_K} \tag{4.3}$$

$$e\sqrt{|c|} + \sqrt{|c|}\sqrt{\Delta_K} = b\sqrt{|f|} + \sqrt{|f|}\sqrt{\Delta_K} \tag{4.4}$$

  We then get $e\sqrt{|c|} = b\sqrt{|f|}$. By substituting into the Equation (4.3), we obtain that $\sqrt{|c|} = \sqrt{|f|}$, which implies that $e = b$. We also have $c = \pm f$. If $c = -f$, we have:

$$\Delta_K = b^2 - 4ac = b^2 - 4df$$

  so $ac = df$. It follows that $d = -a$. In this case

$$f = (a, b, c) \neq (-a, b, -c) = g.$$

  Therefore, $\mathbf{D}$ is not injective.

- **D** is not surjective: Consider the element $(\mathbb{Z}_K, (1,1)) \in \widetilde{\mathrm{Div}^0(K)}$ and say there exists an element $f = (a,b,c) \in \mathscr{F}(\Delta_K)$ such that $\mathbf{D}(f) = (\mathbb{Z}_K, (1,1))$. We then have

$$\left(\left\langle 1, \frac{b-\sqrt{\Delta_K}}{2a}\right\rangle, \left(\frac{b-\sqrt{\Delta_K}}{2\sqrt{|c|}}, \frac{b+\sqrt{\Delta_K}}{2\sqrt{|c|}}\right)\right) = (\mathbb{Z}_K, (1,1))$$

  which implies that $\frac{b-\sqrt{\Delta_K}}{2\sqrt{|c|}} = \frac{b+\sqrt{\Delta_K}}{2\sqrt{|c|}}$. Therefore, $b-\sqrt{\Delta_K} = b+\sqrt{\Delta_K}$ so that $-1 = 1$ which is a contradiction. Hence, **D** is not surjective.

Given any $f = (a,b,c) \in \mathscr{F}(\Delta_K)$, we set $\alpha_f = \left(\frac{|b-\sqrt{\Delta_K}|}{2\sqrt{|ac|}}, \frac{|b+\sqrt{\Delta_K}|}{2\sqrt{|ac|}}\right)$ and consider the matrix $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $g := fS = (c, -b, a)$. Then $I_g = \langle 1, \frac{b-\sqrt{\Delta_K}}{2c}\rangle$ and $\infty_g = \left(\frac{b-\sqrt{\Delta_K}}{2\sqrt{|a|}}, \frac{b+\sqrt{\Delta_K}}{2\sqrt{|a|}}\right)$. The image of the form g under the map **D** splits in $(K^\times_{\mathbb{R},+})^0 \otimes (Id(K) \times \{\pm 1\}^2)$ as

$$\left(\left(\frac{|b+\sqrt{\Delta_K}|}{2\sqrt{|ac|}}, \frac{|b-\sqrt{\Delta_K}|}{2\sqrt{|ac|}}\right), (I_g, sign(\infty_g))\right).$$

Now, consider $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and the form $h := fT = (a, b+2a, a+b+c)$. In $(K^\times_{\mathbb{R},+})^0 \otimes (Id(K) \times \{\pm 1\}^2)$, the image of h under **D** looks like

$$\left(\left(\frac{|b+2a-\sqrt{\Delta_K}|}{2\sqrt{|a^2+ab+ac|}}, \frac{|b+2a+\sqrt{\Delta_K}|}{2\sqrt{|a^2+ab+ac|}}\right), (I_h, sign(\infty_h))\right)$$

where $I_h = \langle 1, \frac{b+2a-\sqrt{\Delta_K}}{2a}\rangle$ and $\infty_g = \left(\frac{b+2a-\sqrt{\Delta_K}}{2\sqrt{|a|}}, \frac{b+2a+\sqrt{\Delta_K}}{2\sqrt{|a|}}\right)$. We define $\alpha_g := \left(\frac{|b+\sqrt{\Delta_K}|}{2\sqrt{|ac|}}, \frac{|b-\sqrt{\Delta_K}|}{2\sqrt{|ac|}}\right)$ and $\alpha_h := \left(\frac{|b+2a-\sqrt{\Delta_K}|}{2\sqrt{|a^2+ab+ac|}}, \frac{|b+2a+\sqrt{\Delta_K}|}{2\sqrt{|a^2+ab+ac|}}\right)$.

4.3 Topological structure of $(K^\times_{\mathbb{R},+})^0$

In this section, we first identify the multiplicative group $(K^\times_{\mathbb{R},+})^0$ with hyperplane $x + y = 0 \subseteq \mathbb{R}^2$, which can be seen as a 1-dimensional $\mathbb{R}$-vector space. This will allow us to define a norm on $(K^\times_{\mathbb{R},+})^0$. By the induced metric, we will be able to measure the distance between elements of $\widetilde{\mathrm{Div}^0(K)}$.

Consider the map

$$\begin{aligned} \mathbf{Log} : (K_{\mathbb{R},+}^{\times})^0 &\to \mathbb{R}^2 \\ (\alpha_1, \alpha_2) &\mapsto (\log(\alpha_1), \log(\alpha_2)) \end{aligned}$$

which is well-defined as $\alpha_1,\ \alpha_2 > 0$. We claim that $(K_{\mathbb{R},+}^{\times})^0$ maps bijectively onto $x + y = 0$ in $\mathbb{R}^2$ via **Log** map. The image of $(K_{\mathbb{R},+}^{\times})^0$ under **Log** is indeed the hyperplane $x + y = 0$ as $\alpha_1\alpha_2 = 1$ so $\log(\alpha_1) = -\log(\alpha_2)$ for all $(\alpha_1, \alpha_2) \in (K_{\mathbb{R},+}^{\times})^0$. Note that **Log** is injective as the log map is injective hence **Log** is a bijection onto its image. We may now identify the set $(K_{\mathbb{R},+}^{\times})^0$ with $x + y = 0$. Given any $\alpha = (\alpha_1, \alpha_2) \in (K_{\mathbb{R},+}^{\times})^0$, we define

$$\|\alpha\| := \sqrt{\log(\alpha_1)^2 + \log(\alpha_2)^2}$$

which turns out to be a norm on $(K_{\mathbb{R},+}^{\times})^0$. Indeed,

- Let $\alpha = (\alpha_1, \alpha_2) \in (K_{\mathbb{R},+}^{\times})^0$ such that $\|\alpha\| = \sqrt{\log(\alpha_1)^2 + \log(\alpha_2)^2} = 0$. Then $\log(\alpha_1) = \log(\alpha_2) = 0$ and $\alpha_1 = \alpha_2 = 1$.

- Let $\lambda \in \mathbb{R}$, $\alpha = (\alpha_1, \alpha_2) \in (K_{\mathbb{R},+}^{\times})^0$. We have:

$$\begin{aligned} \|\lambda\alpha\| &= \sqrt{(\lambda \log(\alpha_1))^2 + (\lambda \log(\alpha_2))^2} \\ &= \sqrt{\lambda^2(\log(\alpha_1)^2 + \log(\alpha_2)^2)} \\ &= |\lambda|\sqrt{\log(\alpha_1)^2 + \log(\alpha_2)^2} \\ &= |\lambda| \cdot \|\alpha\| \end{aligned}$$

- Let $\alpha = (\alpha_1, \alpha_2),\ \beta = (\beta_1, \beta_2) \in (K_{\mathbb{R},+}^{\times})^0$. We need to show that

$$\|\alpha + \beta\| \leq \|\alpha\| + \|\beta\|$$

  which is the same as showing $\|\alpha + \beta\|^2 \leq (\|\alpha\| + \|\beta\|)^2$ since both sides of the

inequality are non-negative. We have:

$$\begin{aligned}
\|\alpha+\beta\|^2 &= (\log(\alpha_1)+\log(\beta_1))^2 + (\log(\alpha_2)+\log(\beta_2))^2 \\
&= \log(\alpha_1)^2 + \log(\alpha_2)^2 + \log(\beta_1)^2 + \log(\beta_2)^2 + 2(\log(\alpha_1)\log(\beta_1) + \log(\alpha_2)\log(\beta_2)) \\
&= \|\alpha\|^2 + \|\beta\|^2 + 2(\log(\alpha_1)\log(\beta_1) + \log(\alpha_2)\log(\beta_2)) \\
&\leq \|\alpha\|^2 + \|\beta\|^2 + 2\sqrt{\log(\alpha_1)^2 + \log(\alpha_2)^2} \cdot \sqrt{\log(\beta_1)^2 + \log(\beta_2)^2} \\
&= \|\alpha\|^2 + 2\|\alpha\| \cdot \|\beta\| + \|\beta\|^2 \\
&= (\|\alpha\| + \|\beta\|)^2
\end{aligned}$$

where the above inequality step follows from Cauchy-Schwarz Inequality.

From the norm $\|\cdot\|$, we induce the following metric on $(K^{\times}_{\mathbb{R},+})^0$:

$$d(\alpha,\beta) := \left[\big(\log(\alpha_1) - \log(\beta_1)\big)^2 + \big(\log(\alpha_2) - \log(\beta_2)\big)^2\right]^{\frac{1}{2}}$$

for $\alpha = (\alpha_1, \alpha_2),\ \beta = (\beta_1, \beta_2) \in (K^{\times}_{\mathbb{R},+})^0$.

Example 4.3.1. Let us find the distance between the images of forms f, fS under the map D and those of f, fT. First, we compute the distance between the images of f and fS, which is given by $d(\alpha_f, \alpha_g)$. We have:

$$\begin{aligned}
d(\alpha_f,\alpha_g) &= \left[\left(\log\left(\frac{|b-\sqrt{\Delta_K}|}{2\sqrt{|ac|}}\right) - \log\left(\frac{|b+\sqrt{\Delta_K}|}{2\sqrt{|ac|}}\right)\right)^2 + \left(\log\left(\frac{|b+\sqrt{\Delta_K}|}{2\sqrt{|ac|}}\right) - \log\left(\frac{|b-\sqrt{\Delta_K}|}{2\sqrt{|ac|}}\right)\right)^2\right]^{\frac{1}{2}} \\
&= \sqrt{2}\left|\log\left(\frac{|b-\sqrt{\Delta_K}|}{2\sqrt{|ac|}}\right) - \log\left(\frac{|b+\sqrt{\Delta_K}|}{2\sqrt{|ac|}}\right)\right| \\
&= \sqrt{2}\left|\log\left(\frac{|b-\sqrt{\Delta}|}{|b+\sqrt{\Delta}|}\right)\right|
\end{aligned}$$

We now compute $d(\alpha_f, \alpha_h)$:

$$\begin{aligned}
d(\alpha_f,\alpha_h) &= \left[\left(\log\left(\frac{|b-\sqrt{\Delta_K}|}{2\sqrt{|ac|}}\right) - \log\left(\frac{|b+2a-\sqrt{\Delta_K}|}{2\sqrt{|a^2+ab+ac|}}\right)\right)^2 + \left(\log\left(\frac{|b+\sqrt{\Delta_K}|}{2\sqrt{|ac|}}\right) - \log\left(\frac{|b+2a+\sqrt{\Delta_K}|}{2\sqrt{|a^2+ab+ac|}}\right)\right)^2\right]^{\frac{1}{2}} \\
&= \left[\left(\log\left(\frac{|b-\sqrt{\Delta_K}|}{|b+2a-\sqrt{\Delta_K}|}\right) + \log\left(\frac{\sqrt{|a+b+c|}}{\sqrt{|c|}}\right)\right)^2 + \left(\log\left(\frac{|b+\sqrt{\Delta_K}|}{|b+2a+\sqrt{\Delta_K}|}\right) + \log\left(\frac{\sqrt{|a+b+c|}}{\sqrt{|c|}}\right)\right)^2\right]^{\frac{1}{2}}
\end{aligned}$$

Since $\left|\frac{b-\sqrt{\Delta_K}}{b+2a-\sqrt{\Delta_K}}\right| = \left|\frac{b+2c-\sqrt{\Delta_K}}{2(a+b+c)}\right|$ and $\left|\frac{b+\sqrt{\Delta_K}}{b+2a+\sqrt{\Delta_K}}\right| = \left|\frac{b+2c+\sqrt{\Delta_K}}{2(a+b+c)}\right|$, we have:

$$d(\alpha_f,\alpha_h) = \left[\log\left(\frac{1}{2}\cdot\frac{|b+2c-\sqrt{\Delta_K}|}{\sqrt{|c(a+b+c)|}}\right)^2 + \log\left(\frac{1}{2}\cdot\frac{|b+2c+\sqrt{\Delta_K}|}{\sqrt{|c(a+b+c)|}}\right)^2\right]^{\frac{1}{2}}$$

The norm $\|\cdot\|$ also induces a norm on $(K^{\times}_{\mathbb{R},+})^0/\mathbb{Z}^{\times}_{K,+}$ by:

$$\|\alpha\cdot\mathbb{Z}^{\times}_{K,+}\|^2_{\widetilde{\mathrm{Pic}^0}} := \min_{\epsilon\in\mathbb{Z}^{\times}_{K,+}}\{\|(\epsilon\alpha_1,\bar{\epsilon}\alpha_2)\|^2\}$$

for $\alpha=(\alpha_1,\alpha_2)\in(K^{\times}_{\mathbb{R},+})^0$.

The above norms, induce a distance on oriented Arakelov divisors:

Definition 4.3.1. Let $D=(\alpha,(I,(a_1,a_2)))$, $D'=(\beta,(J,(b_1,b_2)))$ be two arbitrary oriented Arakelov divisors such that the fractional ideals I and J belong to the same narrow ideal class of K. Then distance between D and D' is defined as $d(\alpha,\beta)$. Whenever I and J represent different ideal classes in $\mathrm{Cl}^+(K)$ the distance $d(D,D')$ is not defined (or defined to be ∞).

The above metric induces a metric on the Picard group as well :

Definition 4.3.2. Given any oriented Arakelov divisor of the form $D=(\mathbb{Z}_K,\alpha)$ where $\alpha\in(K^{\times}_{\mathbb{R},+})^0$, we set $\|D\|_{\widetilde{\mathrm{Pic}^0}} := \|\alpha\cdot\mathbb{Z}^{\times}_{K,+}\|_{\widetilde{\mathrm{Pic}^0}}$.

The norm defined in Definition 4.3.2 gives rise to a distance on $\widetilde{\mathrm{Pic}^0(K)}$: By Theorem 2.4.7, we know that the sequence

$$1\longrightarrow(K^{\times}_{\mathbb{R},+})^0/\mathbb{Z}^{\times}_{K,+}\longrightarrow\widetilde{\mathrm{Pic}^0(K)}\longrightarrow\mathrm{Cl}^+(K)\longrightarrow 1$$

is exact which implies that the class of any oriented divisors $D-D'$ in $\widetilde{\mathrm{Pic}^0(K)}$ whose fractional ideals are in the same narrow ideal class can be represented by the divisor $(\mathbb{Z}_K,\alpha)$ for some unique $\alpha\in(K^{\times}_{\mathbb{R},+})^0$. The function

$$d_{\widetilde{\mathrm{Pic}^0}}(D,D') := \|\alpha\cdot\mathbb{Z}^{\times}_{K,+}\|_{\widetilde{\mathrm{Pic}^0}}$$

defines a distance on $\widetilde{\mathrm{Pic}^0(K)}$.

Observation 4.3.1. Let $D=(I,u)\in\widetilde{\mathrm{Div}^0(K)}$ and let $f=(a,b,c)\in\mathscr{F}(\Delta_K)$. Set $u:=(u_1,u_2)\in\mathbb{R}^{\times}\times\mathbb{R}^{\times}$. By Observation 2.4.2 we know that

$$\big((|u_1|\sqrt{N(I)},|u_2|\sqrt{N(I)}),(I,sign(u))\big)\in(K^{\times}_{\mathbb{R},+})^0\otimes(Id(K)\times\{\pm1\}^2).$$

Then, the element

$$D - \mathbf{D}(f) = \left(\left(|u_1|\sqrt{N(I)}\frac{|b+\sqrt{\Delta_K}|}{2\sqrt{|ac|}}, |u_2|\sqrt{N(I)}\frac{|b-\sqrt{\Delta_K}|}{2\sqrt{|ac|}} \right), (I \cdot I_f^{-1}, sign(u \cdot \infty_f^{-1})) \right)$$

is in $(K_{\mathbb{R},+}^{\times})^0 \otimes (Id(K) \times \{\pm 1\}^2)$ as $\left(\frac{|b-\sqrt{\Delta_K}|}{2\sqrt{|ac|}}\right)^{-1} = \frac{|b+\sqrt{\Delta_K}|}{2\sqrt{|ac|}}$ in $(K_{\mathbb{R},+}^{\times})^0$.

Theorem 4.3.1. *The class of the image* $\boldsymbol{D}(\mathscr{F}(\Delta_K))$ *is dense in* $(\widetilde{\mathrm{Pic}^0(K)}, d_{\widetilde{\mathrm{Pic}^0}})$.

Proof. We need to show that given any $D = (I, (u_1, u_2)) \in \widetilde{\mathrm{Div}^0(K)}$ and given any $\varepsilon > 0$, there exists a binary quadratic form $f = (a, b, c) \in \mathscr{F}(\Delta_K)$ with the fractional ideals I and I_f are in the same narrow ideal class such that

$$d_{\widetilde{\mathrm{Pic}^0}}(D, \mathbf{D}(f)) = \left[\min_{\zeta \in \mathbb{Z}_{K,+}^{\times}} \left\{ \log\left(|u_1|\sqrt{N(I)}\frac{|b+\sqrt{\Delta_K}|}{2\sqrt{|ac|}}\zeta \right)^2 + \log\left(|u_2|\sqrt{N(I)}\frac{|b-\sqrt{\Delta_K}|}{2\sqrt{|ac|}}\bar{\zeta} \right)^2 \right\} \right]^{\frac{1}{2}} < \varepsilon$$

Let $D = (I, (u_1, u_2)) \in \widetilde{\mathrm{Div}^0(K)}$. Then $N(I)|u_1||u_2| = 1$. Choose $\varepsilon > 0$ sufficiently small so that the contributions of $\log(\zeta)$ and $\log(\bar{\zeta})$ are negligible for $\zeta \in \mathbb{Z}_{K,+}^{\times}$. Note that $|u_2|\sqrt{N(I)} = (|u_1|\sqrt{N(I)})^{-1}$ and $\left(\frac{|b-\sqrt{\Delta_K}|}{2\sqrt{|ac|}}\right)^{-1} = \frac{|b+\sqrt{\Delta_K}|}{2\sqrt{|ac|}}$. Then,

$$\log\left(|u_2|\sqrt{N(I)}\frac{|b-\sqrt{\Delta_K}|}{2\sqrt{|ac|}} \right) = -\log\left(|u_1|\sqrt{N(I)}\frac{|b+\sqrt{\Delta_K}|}{2\sqrt{|ac|}} \right)$$

which implies that

$$\log\left(|u_1|\sqrt{N(I)}\frac{|b+\sqrt{\Delta_K}|}{2\sqrt{|ac|}} \right)^2 + \log\left(|u_2|\sqrt{N(I)}\frac{|b-\sqrt{\Delta_K}|}{2\sqrt{|ac|}} \right)^2 = 2\log\left(|u_1|\sqrt{N(I)}\frac{|b+\sqrt{\Delta_K}|}{2\sqrt{|ac|}} \right)^2$$

It is enough to find a binary quadratic form $f \in \mathscr{F}(\Delta_K)$ so that the fractional ideals I and I_f are in the same narrow ideal class with the property that

$$|u_1|\sqrt{N(I)}\frac{|b+\sqrt{\Delta_K}|}{2\sqrt{|ac|}} \xrightarrow[a\to\infty]{} 1$$

For this, choose $f = (a, b, c)$ so that $|u_1|\sqrt{N(I)}|b + \sqrt{\Delta_K}| > 1$. It is not so hard to see that such a b exists. Indeed starting from any $f = (a, b, c)$; one can find $f_+ = (a_+, b_+, c_+)$ which is equivalent to f and $a_+, b_+, c_+ \in \mathbb{Z}_{>0}$. By acting on f_+ with powers of element T one secures the mentioned inequality. Now, as was observed in Example 4.3.1 the rate of growth of the denominator is faster than that of the nominator in the above equation. This guarantees the existence of such a form. Therefore, $d_{\widetilde{\mathrm{Pic}^0}}(D, \mathbf{D}(f)) < \varepsilon$ as required, and hence image is dense. □

BIBLIOGRAPHY

[Baeza, 2009] Baeza, R. (2009). *Quadratic Forms–Algebra, Arithmetic, and Geometry: Algebra, Arithmetic, and Geometry*, volume 493. American Mathematical Soc.

[Buchmann and Vollmer, 2007] Buchmann, J. and Vollmer, U. (2007). Binary quadratic forms. Springer.

[Buell, 1989] Buell, D. A. (1989). *Binary quadratic forms: classical theory and modern computations*. Springer Science & Business Media.

[Charlton,] Charlton, S. Quadratic forms and quadratic number fields. `http://guests.mpim-bonn.mpg.de/spc/teaching/primes_17/handout2_quadratic_field.pdf`.

[Cohen, 2013] Cohen, H. (2013). *A course in computational algebraic number theory*, volume 138. Springer Science & Business Media.

[Conrad,] Conrad, K. Ideal factorization. `https://kconrad.math.uconn.edu/blurbs/gradnumthy/idealfactor.pdf`.

[Conrad, 2014] Conrad, K. (2014). Factoring in quadratic fields. *preprint, https://kconrad.math.uconn.edu/blurbs/gradnumthy/quadraticgrad.pdf (accessed 4 October 2017)*, 143.

[Gauss, 1801] Gauss, C. F. (1801). Disquisitiones arithmeticae, trans. arthur a. clarke.

[Goldstein et al., 2007] Goldstein, C., Schappacher, N., and Schwermer, J. (2007). *The shaping of arithmetic after CF Gauss's Disquisitiones Arithmeticae*. Springer Science & Business Media.

[Hecke et al., 1981] Hecke, E., Goldman, J. R., and Kotzen, R. (1981). *Lectures on the theory of algebraic numbers*, volume 77. Springer.

[Jarvis, 2014] Jarvis, F. (2014). *Algebraic number theory*. Springer.

[Lamé, 1847] Lamé, G. (1847). Démonstration générale du théorème de fermat sur l'impossibilité, en nombres entiers, de l'équation $x^n + y^n = z^n$. *C. R. Acad. Sci., Paris*, 1(6):310–315.

[Lenstra, 1982] Lenstra, Jr., H. W. (1982). 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.

[Lorenzini, 1996] Lorenzini, D. (1996). *An invitation to arithmetic geometry*, volume 9. American Mathematical Soc.

[Milne, 2008] Milne, J. S. (2008). *Algebraic number theory*. JS Milne.

[Neukirch, 2013] Neukirch, J. (2013). *Algebraic number theory*, volume 322. Springer Science & Business Media.

[Schoof,] Schoof, R. Arakelov class groups. lecture notes, by j. voight.

[Schoof, 2008] Schoof, R. (2008). Computing Arakelov class groups. In *Algorithmic number theory. Lattices, number fields, curves and cryptography*, pages 447–495. Cambridge: Cambridge University Press.