The Infrastructure of a Global Field and Baby Step-Giant Step Algorithms

Dissertation

zur

Erlangung der naturwissenschaftlichen Doktorwürde
(Dr. sc. nat.)

vorgelegt der

Mathematisch-naturwissenschaftlichen Fakultät

der

Universität Zürich

von

Felix Wolfgang Fontein

aus

Deutschland

Promotionskomitee

Prof. Dr. Joachim Rosenthal (Vorsitz)
Prof. Dr. Markus Brodmann
Prof. Dr. Andrew Kresch
Prof. Dr. Andreas Stein (Oldenburg)

Zürich, 2009

Contents

0 Introduction **1**
- 0.1 Introduction . . . 4
- 0.2 Outline of the Thesis . . . 6
- 0.3 Results . . . 8

1 Background **11**
- 1.1 Preliminaries on Global Fields . . . 11
- 1.2 Notations . . . 13

2 Abstract Infrastructure **15**
- 2.1 One-Dimensional Infrastructure . . . 15
- 2.2 Obtaining Groups from Infrastructures . . . 18
- 2.3 Applications . . . 21
  - 2.3.1 Key Exchange . . . 21
  - 2.3.2 The Discrete Logarithm Problem for Infrastructures . 23
  - 2.3.3 Pohlig-Hellman . . . 23
  - 2.3.4 Baby Step-Giant Step Method . . . 24
- 2.4 Generalizing to Higher Dimensions . . . 25

3 Minima of Ideals in Global Fields **29**
- 3.1 Boxes . . . 29
- 3.2 Minima of Ideals . . . 32
- 3.3 The Neighbor Relation . . . 36
- 3.4 Connectivity of the Neighbor Graphs . . . 44
- 3.5 Baby Steps . . . 47
- 3.6 Representation by Ideals . . . 53

4 The Infrastructure of a Global Field **57**
- 4.1 Equivalence Classes of Reduced Ideals . . . 57
- 4.2 Infrastructure for Global Fields . . . 60

4.3 The Infrastructure and the Picard Group 64
4.4 Size of f-Representations 68
4.5 Discrete Infrastructures 73
4.6 Conclusion 74

5 Computation in the Function Field Case 77
5.1 The Algorithm of Heß 77
5.2 Computing the Infinite Primes 78
5.3 A Specialized Algorithm 79
5.4 Computing Giant Steps 80
5.5 Computing Baby Steps 83
5.6 Optimizations and Conclusion 88

6 Computations of Units 89
6.1 Computing Units in Global Fields 91
6.2 Algorithms for Function Fields 92
6.2.1 Voronoĭ's Algorithm 93
6.2.2 A Baby Step-Giant Step Algorithm for Function Fields 94
6.2.3 Lifting Units 95
6.2.4 Explicit Computations 99
6.3 Computing All Neighbors of a Minimum 105
6.3.1 Computations in the Function Field Case 109
6.4 Buchmann's Algorithms 112
6.4.1 The Generalized Lagrange Algorithm 112
6.4.2 The Baby Step Algorithm 114
6.4.3 The Baby Step-Giant Step Algorithm 118
6.5 A General Baby Step-Giant Step Algorithm 121
6.5.1 Computation of the Baby Stock 122
6.5.2 Computation of Giant Steps 125
6.5.3 The Baby Step-Giant Step Algorithm 127
6.6 Conclusion 132

Bibliography 135

List of Figures 144

Index 146

Abstract

In Computational Number Theory, one is interested in the computation of invariants. One such invariant is the regulator of a number field or a global function field. The regulator can be obtained from the unit lattice, whose structure corresponds to the structure of the so called infrastructure.

In this thesis, we generalize the infrastructure to the n-dimensional case; so far, the infrastructure was mainly investigated in the one-dimensional case. For that purpose, we generalize f-representations and use them to obtain a reduction map. Furthermore, we relate the infrastructure to the (Arakelov) divisor class group and describe the divisor class group using f-representations. This allows both to do explicit arithmetic in the divisor class group and to compute giant steps in the infrastructure. This extends work particularly by J. Buchmann and R. Schoof in the number field case and S. Paulus and H.-G. Rück in the function field case.

We also discuss an implementation of computation of boxes in the function field case, and explain how it can be used to compute giant steps and baby steps.

Moreover, we describe existing algorithms for computation of the unit lattice and, hence, the regulator. We present two approaches for the function field case, one using algorithms designed for operating on finite abelian groups in the case that one infinite place has degree one, and one using a lifting strategy for reducing to the case of at least one infinite place of degree one. Finally, we extend J. Buchmann's baby step-giant step algorithm for number fields to the global field case and combine it with an optimization by D. Terr for the classic baby step-giant step algorithm.

Acknowledgements

I would like to thank all persons without whom this thesis would not have been written.

First, I would like to thank my advisor, Joachim Rosenthal, for his constant support and encouragement. Then, I would like to thank Michael J. Jacobson and Hugh C. Williams for introducing me to the subject of infrastructures, and Andreas Stein for organizing the summer school on which this happened. Moreover, I would like to thank Andreas Stein for several discussions which inspired me a lot, and for inviting me to Oldenburg. I would also like to thank Renate Scheidler, Mark Bauer, Adrian Tang, Eric Landquist and others for discussions on certain aspects of computation of fundamental units. Finally, I would like to thank Johannes A. Buchmann for pointing me to his habilitation thesis.

I am obliged to Martin A. Michels for proof-reading my thesis and for giving me helpful comments. In addition I would like to thank Andreas Stein and Joachim Rosenthal for their valuable comments.

I am indebted to the Institut für Mathematik at the Carl von Ossietzky Universität Oldenburg and the Mathematics and Statistics Department at the University of Calgary for their hospitality during my visits and, of course, to the Institut für Mathematik at the Universität Zürich for providing me with an inspiring work environment and the possibility to carry out all computations.

Last, but not least, I am deeply obliged to all my friends and to my family, who supported me all the time.

Chapter 0

Introduction

The studying of number fields has its roots in the early history of mathematics, when integral solutions to certain equations were sought. A famous such equation is Pell's equation, $x^2 - Dy^2 = 1$, where $D \in \mathbb{Z}$ is given and $x, y \in \mathbb{Z}$ are sought; the study of this equation goes back the Indian mathematician Brahmagupta, who developed a method to solve such equations in 628. Another famous example is the Fermat equation, $x^n + y^n = z^n$, where $n \in \mathbb{N}$, $n \geq 3$ is given and $x, y, z \in \mathbb{Z}$ with $xyz \neq 0$ are sought. The study of these equations eventually led to the study of algebraic number fields. In the case of Pell's equation, one obtains the solutions as certain units in the order $\mathbb{Z}[\sqrt{D}]$ of the quadratic number field $\mathbb{Q}(\sqrt{D})$, assuming that $|D| > 1$ is squarefree. In case $D > 0$, every such unit is (up to sign) a power of a fundamental unit of the ring of integers of $\mathbb{Q}(\sqrt{D})$. Hence one can ask how to compute these. J.-L. Lagrange showed that this can be done using continued fraction expansion.

Similar questions can be studied where solutions are sought in the domain of algebraic functions, i.e. functions ρ which satisfy $f(x, \rho) = 0$ for a non-trivial polynomial $f \in \mathbb{C}[X, Y]$. This led to the study of function fields, whose foundations were laid by R. Dedekind and H. Weber. Mathematicians such as K. Hensel, G. Landsberg, H. Hasse, F. K. Schmidt, A. Weil, M. Deuring, M. Eichler and C. Chevalley continued and generalized these ideas. Besides the algebraic approach, function fields can also be studied as the fields of rational functions of a planar curve. A third approach was taken by E. Artin, who began to study valuations. This ultimately led to a unified theory for function fields and number fields, which shows many similarities in particular between number fields and function fields with finite fields of constants; such fields are called global fields.

Besides the purely theoretic interest in such fields, they were also used in applications. A prominent use of function fields came up in 1975, when V. D. Goppa constructed error correcting codes from global function fields with many places of degree one [Gop88]. A second application besides Coding Theory is the area of Public Key Cryptography; in 1985, N. Koblitz and V. Miller independently proposed [Mil86, Kob87] the use of the group of rational points of an elliptic curve over a finite field instead of, for example, the multiplicative group of a finite field. This group corresponds to a subgroup of the divisor class group of a global elliptic function field. Later, N. Koblitz suggested that one could also use the Jacobian of hyperelliptic curves. More generally, one can use the group of points of any abelian variety, of which the Jacobian varieties of curves are a special case; the rational points of the Jacobian variety of a projective smooth curve correspond to the elements of the divisor class group of the curve's function field. The use of abelian varieties and the special case of Jacobian varieties was described, for example, by G. Frey in [Fre01] together with consequences of Galois theory, Weil descent and Tate duality to cryptographic use of such varieties. A general overview of the use of mathematical primitives in Public Key Cryptography can be found in [FL05]. Besides applications of function fields, there also have been proposals to use the ideal class group of number fields for Public Key Cryptography, mainly by J. Buchmann and H. C. Williams; see, for example, [BW88a] or the survey [Buc91].

A vast majority of these systems which employ global fields are based on the Discrete Logarithm Problem (DLP). The DLP is, given a cyclic group $G = \langle g \rangle$ and $h \in G$, to find an $n \in \mathbb{Z}$ with $g^n = h$; this problem is hoped to be hard enough to allow the use of such groups in DLP based Public Key Cryptography, for example for a Diffie-Hellman Key Exchange. Besides this security aspect, there is a much more fundamental aspect in using such groups, namely that one has to be able to efficiently compute in them. In the case of elliptic curves, one has explicit formulas for adding two points. In the case of hyperelliptic function fields, one has the algorithm of D. G. Cantor [Can87]. In the case of real imaginary number fields, one uses composition of binary quadratic forms which goes back to C. F. Gauß. For superelliptic function fields, a method by S. Galbraith, S. Paulus and N. Smart exists [GPS02] and, for arbitrary function fields, one has algorithms by F. Heß [Hes99, Hes02] or K. Khuri-Makdisi [KM04, KM07]. Besides arithmetic in the divisor class group, one also has the ideal class group of the ring of integral functions, or in the number field case, the ideal class group of the maximal order.

Another structure is the *infrastructure*. One way to interpret it is as a kind of dual structure to the ideal class group, as it describes the kernel of the projection from the divisor class group onto the ideal class group; it describes the obstacle one has if one wants to compute in the ideal class group. It also has an arithmetic structure. Usually, one of the ideal class group and the infrastructure is small or even trivial, while the other one is large. One aim of this thesis is to analyze and understand this infrastructure and describe its exact relation to the arithmetic in the divisor class group. In the case the infrastructure is one-dimensional and belongs to a number field, it has been investigated in detail since D. Shanks first mentioned the existence of a giant step in it [Sha72], which is similar to a group operation. Important contributions have been made by H. W. Lenstra [Len82], R. Schoof [Sch82], H. C. Williams [Wil85] and J. Buchmann and H. C. Williams [BW88b]. Moreover, the one-dimensional infrastructure was also applied in Public Key Cryptography, the first occurrence being a key exchange protocol by J. Buchmann, H. C. Williams and R. Scheidler [BW90, SBW94]. The infrastructure was also generalized to function fields, starting with A. Stein [Ste92, SZ91] who described the infrastructure of a real quadratic function field, and later by R. Scheidler and A. Stein who described it in certain cubic function fields [SS98, Sch01]. So far, the most general study of the infrastructure, at least in the number field case, was done by R. Schoof in [Sch08] using Arakelov divisors.

The infrastructure is also giving a connection to the beginning of this motivation, as it allows to compute the structure of the group of units of the maximal order respectively the ring of integral functions. The computation of the structure of the group of units is equivalent to the computation of the structure of the infrastructure, and D. Shanks' discovery of the giant step allowed him to present an algorithm for real quadratic number fields which was considerably faster than the existing ones. This has been generalized by J. Buchmann in his habilitation thesis [Buc87c] to all number fields. The second aim of this thesis is to generalize their work to the case of arbitrary global fields, resulting in a unified baby step-giant step algorithm for the global field case incorporating ideas by J. Buchmann and A. Schmidt in [BS05] and D. Terr in [Ter00].

We begin with a more technical introduction, starting with three questions mentioned here, namely computation in the divisor class group, in the ideal class group and computation of the unit group.

0.1 Introduction

An important topic in Computational Number Theory is the computation of invariants of a global field K. In particular, one is interested in the divisor class group $\mathrm{Pic}^0(K)$, the ring of integers $\mathcal{O}$ (resulting in the discriminant) and its unit group $\mathcal{O}^*$ or its free part $\mathcal{O}^*/k^*$ (resulting in the regulator), its ideal class group $\mathrm{Pic}(\mathcal{O})$ (resulting in the class number), and information about the infinite places (resulting in the signature).

Consider the following diagram with exact rows and columns:

$$\begin{array}{ccccccccc} & & & & & & 0 & & \\ & & & & & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{O}^*/k^* & \longrightarrow & \mathrm{Div}^0_\infty(K) & \longrightarrow & T & \longrightarrow & 0 \\ & & & & & & \downarrow & & \\ & & & & & & \mathrm{Pic}^0(K) & & \\ & & & & & & \downarrow & & \\ & & & & & & \mathrm{Pic}(\mathcal{O}) & & \end{array}$$

where T is the cokernel of the map $\mathcal{O}^* \to \mathrm{Div}^0_\infty(K)$. (All required notation can be found in Section 1.1.) From an algorithmic point of view, there are many interesting problems, three of these being:

(a) how to compute a $\mathbb{Z}$-basis of $\mathcal{O}^*/k^*$,

(b) how to do effective arithmetic in $\mathrm{Pic}^0(K)$ and in its subgroup T, and

(c) how to do effective arithmetic in $\mathrm{Pic}(\mathcal{O})$ or in the image of $\mathrm{Pic}^0(K)$ in $\mathrm{Pic}(\mathcal{O})$.

The first two problems are related in the sense that understanding $\mathcal{O}^*/k^*$ is basically equivalent to understanding the group T, as T is isomorphic to $\mathrm{Div}^0_\infty(K)/(\mathcal{O}^*/k^*)$. Hence, if one can compute the morphism $\mathrm{Div}^0_\infty(K) \to T \subseteq \mathrm{Pic}^0(K)$, one can use arithmetic in $T \subseteq \mathrm{Pic}^0(K)$ to obtain information on $\ker(\mathrm{Div}^0_\infty(K) \to T) \cong \mathcal{O}^*/k^*$, and vice versa.

The third problem is also related to the first two: to compute in $\mathrm{Pic}(\mathcal{O})$ (or in the image of the morphism $\mathrm{Pic}^0(K) \to \mathrm{Pic}(\mathcal{O})$), one could use the representation $\mathrm{Pic}(\mathcal{O}) \cong \mathrm{Pic}^0(K)/T$, i.e. the main problem is testing for equality or, equivalently, checking whether an element in $\mathrm{Pic}(\mathcal{O})$ is neutral.

This is equivalent to whether the representative in $\mathrm{Pic}^0(K)$ lies in the kernel T. To efficiently check whether it lies in T, one needs to understand and know the structure of T.

In this thesis, we consider the *infrastructure* of K which, as we will see, is closely related to the arithmetic in $\mathrm{Pic}^0(K)$ and T. Infrastructures of number fields and, later, of function fields have been studied for a long time. As many other subjects, the foundations for infrastructures were laid by C. F. Gauß. The infrastructure first appeared explicitly on the search for generalizing continued fraction expansion. In his thesis, G. Voronoĭ found a generalization of continued fraction expansion by minima of lattices and formulated an algorithm to find a system of fundamental units of a cubic number field; a description can be found in the book by B. N. Delone and D. K. Faddeev, [DF64]. Similar geometric interpretations of continued fraction expansion are due to F. Klein and H. Minkowski.

The structure formed by these lattice minima together with a neighbor relation—which, in the context of continued fraction expansion, corresponds to computing the next approximation—has been intensively studied, both abstractly (for example, G. Bergmann's *Theorie der Netze*, [Ber63]) and in the concrete cases of number fields, function fields or, unified, for fields with a product formula (for example by Y. Hellegouarch, D. L. McQuillan and R. Paysant-Le Roux, see [PLRMH85, HPLR85, HPLR87, HMPLR87]). This resulted in several algorithms for computing independent or even fundamental units in number fields, for example [AO82, Ber63, PZ77, PZ82, PWZ82, HPLR87, Ste77]. J. Buchmann started to generalize Voronoĭ's algorithm [Buc85a, Buc85b] and finally, in his habilitation thesis, gave a generalization of Lagrange's algorithm which computes fundamental units for arbitrary number fields in $\mathcal{O}(RD^{\varepsilon})$ binary operations ($\varepsilon > 0$ arbitrary, R the regulator and D the absolute value of the discriminant of the number field) [Buc87a, Buc87c]. Note that $R = \mathcal{O}(\sqrt{D})$.

In 1972, Daniel Shanks discovered that the principal infrastructure of a real quadratic number field can be equipped with another operation besides the *baby steps*, which he called *giant steps* [Sha72]. A baby step walks to a (uniquely determined) neighbor, while giant steps mimic the behavior of group multiplication in a cyclic group. Using them, he was able to compute the regulator and, therefore, a fundamental unit (or, more precisely, its absolute values) of a real quadratic number field in $\mathcal{O}(\sqrt{R})$ steps instead of the $\mathcal{O}(R)$ steps the classical algorithm by Lagrange needed. His method was analyzed and refined by H. Lenstra, R. Schoof, H. C. Williams in [Len82, Sch82, Wil85]. It was also extended to certain cubic number fields [WDS83] and, finally, by J. Buchmann and H. C. Williams, to all number fields of

unit rank one [BW88b].

D. Shank's method was also extended to function fields. First, in his diploma thesis, A. Stein considered the case of real quadratic global function fields [Ste92, SZ91]. This was later improved by A. Stein and H. C. Williams [SW98, SW99] and extended to certain cubic function fields of unit rank one by R. Scheidler and A. Stein [SS98, Sch01]. The relations between the infrastructure in real quadratic (hyper-)elliptic function fields and the divisor class group in their imaginary counterparts were investigated by A. Stein in [Ste97], and by S. Paulus and H.-G. Rück in [PR99].

So far, all efficient algorithms based on the infrastructure need a giant step operation. This opens the question whether a giant step can be defined and used efficiently in the general case. In the number field case, Buchmann showed in his habilitation thesis [Buc87c] that one has such a giant step, and that this giant step can be used to compute approximations of the absolute values of fundamental units in $\mathcal{O}(\sqrt{R}D^{\varepsilon})$ binary operations (again, $\varepsilon > 0$ arbitrary, R is the regulator and D is the absolute value of the discriminant of the number field). Unfortunately, this algorithm was never published except in the thesis.

Later, R. Schoof presented a modern treatment of the general number field case using Arakelov divisor theory [Sch08]. This is so far the most general treatment of infrastructure, and it includes a reduction strategy and defines a giant step, even though it does not describes a baby step-giant step algorithm like Buchmann's.

In this thesis, we have two main goals. The first main goal is to give an concise interpretation of the infrastructure in the general case, and to obtain giant steps that are controllable in some sense; we do this by generalizing f-representations, as described in [Fon08], which were introduced by D. Hühnlein and S. Paulus [HP01] and M. J. Jacobson, R. Scheidler and H. C. Williams [JSW01] in the case of one-dimensional infrastructures obtained from number fields. This also leads to a close relationship between the infrastructure and $\mathrm{Pic}^0(K)$. The second main goal is to generalize Shank's baby step-giant step algorithm and Buchmann's generalization for number fields to an algorithm which computes $\mathcal{O}^*$ for an arbitrary global field.

0.2 Outline of the Thesis

In this chapter, we give an introduction, an outline and an overview over the results of this thesis. In Chapter 1 we give a short introduction on global fields and introduce all necessary notations.

In Chapter 2, we first introduce one-dimensional infrastructures in an abstract setting in Section 2.1. Then, in Section 2.2, we show how to obtain (cyclic) groups from such infrastructures, and we give applications such as cryptographic key exchange, a baby step-giant step method, and a Pohlig-Hellman adaption in Section 2.3. Finally, in Section 2.4, we discuss how infrastructures can be generalized to higher dimensions, sketching some ideas which will be used later on.

Chapter 3 is devoted to the study of minima of ideals in global fields, which will give the infrastructure. The chapter starts with Section 3.1, which introduces some number geometric concepts. Then, in Section 3.2, we define minima, and in Section 3.3, we consider the neighbor relation. After that, we show that the neighbor graph is connected for type (a) and (b) minima in Section 3.4. In Section 3.5 we define baby steps in a very general manner, and in Section 3.6, we consider ideal representations, a concept of great importance in the context of efficient computation.

Then, in Chapter 4, we present an infrastructure for arbitrary global fields. In Section 4.1, we investigate an equivalence relation which will give us the finiteness of the underlying set X of the infrastructure. After that, in Section 4.2, we obtain the infrastructure by defining the distance map and the reduction map. Then, in Section 4.3, we see how the previously defined infrastructure is related to the Picard group of the global field, and how we can use the infrastructure to describe the Picard group. The size of these representations is discussed in Section 4.4, and the question of whether the infrastructures obtained this way are discrete is answered in Section 4.5. Finally, in Section 4.6, we present an important special case of the generalized infrastructure.

The computation in the function field case is the main topic of Chapter 5. There, we present the algorithm of F. Heß for Riemann-Roch space computations in Section 5.1 and discuss the computation of the prime ideals for the infinite places in Section 5.2. Then, we describe a specialized algorithm for computing k-bases of boxes in Section 5.3. After that, we describe the computation of giant steps (Section 5.4) and baby steps (Section 5.5) and, finally, present some possible optimizations in Section 5.6.

The second main part of the thesis, besides generalizing the infrastructure in Chapter 4, is the discussion of baby step-giant step algorithms in Chapter 6. We begin by discussing the problem of computing units in global fields in Section 6.1, relating it to the infrastructure. Then, we first restrict to the function field case and describe a group theoretic adaption of Voronoĭ's method (Section 6.2.1), a baby step-giant step method (Section 6.2.2), a lifting method (Section 6.2.3) and a concrete implementation (Section 6.2.4) in

Section 6.2.

In Section 6.3, we show how J. Buchmann solved the problem of computing all neighbors of a given minimum, and explicitly describe the function field case in Section 6.3.1. After that, we describe J. Buchmann's algorithms for number fields in Section 6.4, namely the Generalized Lagrange algorithm (Section 6.4.1), the baby step algorithm (Section 6.4.2) and the baby step-giant step algorithm (Section 6.4.3).

Finally, we describe a baby step-giant step algorithm in Section 6.5 which can be applied both to number and function fields, and analyze the theoretical running time; then, in Section 6.6, we discuss the practical running time and applications to principal ideal tests.

0.3 Results

The first main result is the generalization of the infrastructure to arbitrary global fields, and even certain function fields which are not global. The general idea is sketched in Section 2.4 and, then, turned into practice in Chapter 4. The first ingredient is prepared in Chapter 3, namely the set X. The main work, which is providing a reduction map, is done in Section 4.2 and is presented in Proposition 4.2.7 (Infrastructure, Part I); the key tool for this are f-representations, which consist of the equivalence class of a reduced ideal and local information about the infinite valuations which are minimal in a certain sense. The equivalence relation is required as soon as minima having the same infinite absolute values do differ by something else than a constant, which can be the case if $\deg \mathfrak{p} > 1$ for all infinite places $\mathfrak{p}$. We get a bijection

$$\mathrm{Rep}^f(\mathfrak{a}) \to \mathbb{G}^n/\Lambda \supseteq T,$$

where $\mathrm{Rep}^f(\mathfrak{a})$ is the set of f-representations with reduced ideals inside the ideal class of $\mathfrak{a}$, $\Lambda \subseteq \mathbb{G}^n$ is the unit lattice and $n+1$ is the number of infinite places. Note that our reduction generalizes the known arithmetic in imaginary hyperelliptic function fields, superelliptic function fields and other function fields with one infinite place.

Then, we generalize a result by S. Paulus and H.-G. Rück [PR99], namely we describe the arithmetic in the (Arakelov) divisor class group $\mathrm{Pic}^0(K)$ using the infrastructure; this is done in Proposition 4.3.2 (Infrastructure, Part II). The main problem is to seek a replacement for $\mathrm{Pic}^0(K)$ in the case of certain function fields; it turns out that a good replacement is $\mathrm{Pic}(K)/\langle[\mathfrak{p}_{n+1}]\rangle$ for an infinite place $\mathfrak{p}_{n+1}$. As in [PR99], we describe arithmetic in $\mathrm{Pic}^0(K)$ respectively $\mathrm{Pic}(K)/\langle[\mathfrak{p}_{n+1}]\rangle$ using our f-representations;

this is done in Proposition 4.3.4 (Infrastructure, Part III).

We also discuss the size of f-representations, namely in Proposition 4.4.1 we give upper bounds for the parameters, and in Proposition 4.4.5, we give explicit bounds on the size of a reduced ideal in terms of representation on a computer. In case of a function field K of genus g with $d = [K : k(x)]$, we obtain that reduced ideals of type (b) can be represented by at most $\mathcal{O}(d^2 g)$ constant field elements and $\mathcal{O}(d^2)$ integers which are of magnitude $\mathcal{O}(dg)$.

Similar to a result in [Fon08], we also answer the question of which infrastructures are discrete (Proposition 4.5.2) and what f-representations of the form $([\mathfrak{a}]_\sim, 0)$ with a reduced principal ideal $\mathfrak{a}$ have finite order (Proposition 4.5.3). Firstly, the infrastructure of a global field is discrete if, and only if, the field is a function field or has exactly one infinite place. Secondly, in the number field case, an f-representation $([\mathfrak{a}]_\sim, 0)$ has finite order in $\mathrm{Rep}^f(\mathcal{O})$ if, and only if, $\mathfrak{a} = \mathcal{O}$, i.e. if it is the neutral element.

Then, in Chapter 5, we derive a variation of the algorithm of F. Heß for Riemann-Roch space computations which computes a k-basis of a box in a function field; we then use that algorithm to describe the computation of baby steps and giant steps in function fields.

The second main result can be found in Chapter 6, where we generalize Buchmann's baby step-giant step algorithm to arbitrary global fields and combine it with Terr's modification of the classic baby step-giant step algorithm [Ter00]. Our algorithm is explained in Section 6.5. The correctness of our algorithm, Algorithm 6.5.5, is shown in Proposition 6.5.6, and the running time is estimated in Proposition 6.5.7: one needs essentially $\mathcal{O}(D^\varepsilon \sqrt{R})$ operations in the infrastructure in the number field case and $\mathcal{O}(\kappa^n \sqrt{R})$ operations in the infrastructure in the function field case, where $\kappa = \mathcal{O}(g)$. As in the function field case, $g = \mathcal{O}(\deg \Delta)$ with Δ being the discriminant of $\mathcal{O}$, the running time for both the number field and the function field case is essentially the same. Again, we give special optimizations in the function field case.

Chapter 6 also contains baby step-giant step algorithms specialized to the function field case (Section 6.2.2), together with an approach which uses constant field extensions to remove the restriction that one of the infinite places should have degree one (Section 6.2.3). We give results of an implementation of the algorithms in Section 6.2.2 in Section 6.2.4.

The description of the one-dimensional infrastructure together with the Pohlig-Hellman algorithm applied to this case was already published in [Fon08]. The general infrastructure approach as described in Chapter 4, together with the algorithms in Chapter 5 for reduction and giant steps and

the sketches of Voronoĭ's algorithm for groups (Section 6.2.1) and a baby step-giant step algorithm for function fields (Section 6.2.2) have been published as a preprint [Fon09]. The material in Section 6.2.3 on lifting units in constant field extensions is joint work with Mark Bauer, University of Calgary.

This thesis has been supported in part by the Swiss National Science Foundation under grant no. 107887, and also in part by the Forschungskredit of the Universität Zürich under grant no. 57104102.

Chapter 1

Background

In this chapter, we want to present some background on number fields and function fields, and clarify some notations.

1.1 Preliminaries on Global Fields

Information on number fields can be found in [Neu99], [Sch08] and [Art06], and information on function fields can be found in [Sti93], [Gol03], [Ros02] and [Deu73].

Let K be a function field with field of constants k, or let K be an algebraic number field. In the latter case, denote the roots of unity of K by k^* and set $k = k^* \cup \{0\}$.

If K is an algebraic function field, we assume that k is the exact field of constants of K. Let $x \in K$ be transcendental over k. (Note that we do not assume that $K/k(x)$ is separable.) Let $\mathcal{O}$ denote the integral closure of $k[x]$ in K and let S denote the set of places of K/k which do not correspond to prime ideals of $\mathcal{O}$, i.e. the places of K lying over the infinite place of $k(x)$. Note that for any non-empty finite choice of S, one can find such an x that S is the set of places lying over the infinite place of $k(x)$. In the number field case, let $\mathcal{O}$ denote the integral closure of $\mathbb{Z}$ in K and let S denote the set of all archimedean places of K. In both cases, we denote by $\mathcal{P}_K$ the set of all places of K.

Divisors, Ideals and Units. In the function field case, the group of divisors $\mathrm{Div}(K)$ is the free abelian group generated by $\mathcal{P}_K$. For a divisor $D = \sum_{\mathfrak{p}\in\mathcal{P}_K} n_{\mathfrak{p}}\mathfrak{p}$, the degree is defined as $\deg D := \sum_{\mathfrak{p}\in\mathcal{P}_K} n_{\mathfrak{p}} \deg \mathfrak{p}$. The divisors of degree zero form a subgroup of $\mathrm{Div}(K)$, denoted by $\mathrm{Div}^0(K)$. For an ele-

ment $f \in K^*$, the principal divisor of f is defined by $(f) := \sum_{\mathfrak{p} \in \mathcal{P}_K} \nu_{\mathfrak{p}}(f)\mathfrak{p} \in \mathrm{Div}^0(K)$; the set of all such divisors forms the group $\mathrm{Princ}(K)$, and the quotient $\mathrm{Pic}^0(K) := \mathrm{Div}^0(K)/\mathrm{Princ}(K)$ is called the (degree zero) divisor class group of K. Moreover, we have the quotient $\mathrm{Pic}(K) := \mathrm{Div}(K)/\mathrm{Princ}(K)$ together with the exact sequence

$$0 \longrightarrow \mathrm{Pic}^0(K) \longrightarrow \mathrm{Pic}(K) \xrightarrow{\deg} \mathbb{Z}.$$

Note that the sequence (after the last map is made surjective) splits, i.e. we have $\mathrm{Pic}(K) \cong \mathrm{Pic}^0(K) \times \mathbb{Z}$.

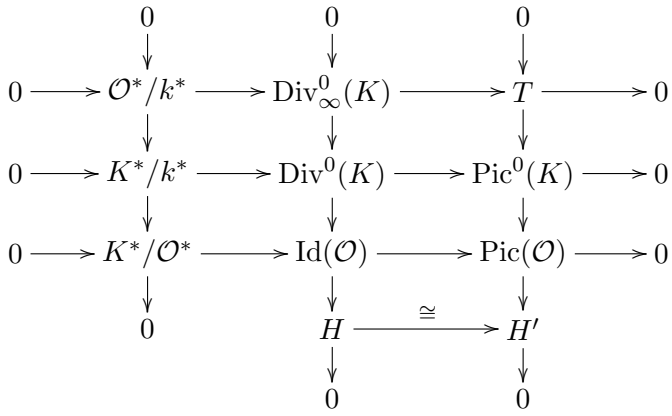
In the number field case, the group of divisors $\mathrm{Div}(K)$ is the direct product of the free abelian group generated by all places outside S, together with $\mathbb{R}^S$. For $\mathfrak{p} \in S$, let $\sigma : K \to \mathbb{C}$ be a corresponding embedding; define $\deg \mathfrak{p} := 1$ if $\sigma(K) \subseteq \mathbb{R}$ and $\deg \mathfrak{p} := 2$ otherwise. Define $\nu_{\mathfrak{p}}(f) := -\log|\sigma(f)|$. If $\mathfrak{p}$ is a finite place, define $\deg \mathfrak{p} := \log|\mathcal{O}_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}|$. The definition of the degree of a divisor and of a principal divisor is the same as in the function field case, as is the definition of $\mathrm{Pic}^0(K)$ and $\mathrm{Pic}(K)$, and we get $\mathrm{Pic}(K) \cong \mathrm{Pic}^0(K) \times \mathbb{R}$ in the same way as above.

If K is a global function field, fix $q = |k|$. For non-global function fields, let $q > 1$ be arbitrary. For number fields, let $q = e = \exp(1)$. Then, define $|f|_{\mathfrak{p}} := q^{-\nu_{\mathfrak{p}}(f)\deg \mathfrak{p}}$ for $f \in K^*$ and $|0|_{\mathfrak{p}} := 0$. The fact that principal divisors have degree zero translates to the product formula $\prod_{\mathfrak{p} \in \mathcal{P}_K} |f|_{\mathfrak{p}} = 1$ for $f \in K^*$.

In both cases, a finitely generated $\mathcal{O}$-submodule of K is called a fractional ideal. The set of non-zero fractional ideals $\mathrm{Id}(\mathcal{O})$ forms a free abelian group, with the set of non-zero prime ideals of $\mathcal{O}$ as a basis. These prime ideals correspond to the places of K outside S: if $\mathfrak{p}$ is such a place, let $\mathfrak{m}_{\mathfrak{p}}$ be its valuation ideal; then $\mathfrak{m}_{\mathfrak{p}} \cap \mathcal{O}$ is the corresponding prime ideal of $\mathcal{O}$. Moreover, we have a natural epimorphism $\mathrm{Div}(K) \to \mathrm{Id}(\mathcal{O})$ defined by $\sum n_{\mathfrak{p}}\mathfrak{p} \mapsto \prod_{\mathfrak{p} \notin S} (\mathfrak{m}_{\mathfrak{p}} \cap \mathcal{O})^{n_{\mathfrak{p}}}$. This epimorphism extends to a map $\mathrm{Pic}^0(K) \to \mathrm{Pic}(\mathcal{O})$, where $\mathrm{Pic}(\mathcal{O}) := \mathrm{Id}(\mathcal{O})/\mathrm{Princ}(\mathcal{O})$ is the ideal class group of $\mathcal{O}$, i.e. the quotient of $\mathrm{Id}(\mathcal{O})$ with the subgroup $\mathrm{Princ}(\mathcal{O})$ of non-zero principal fractional ideals, i.e. the ideals of the form $f\mathcal{O}$, $f \in K^*$.

Note that forming principal divisors or principal ideals out of elements of K^* give epimorphisms $K^* \to \mathrm{Princ}(K) \subseteq \mathrm{Div}^0(K)$ and $K^* \to \mathrm{Princ}(\mathcal{O}) \subseteq \mathrm{Id}(\mathcal{O})$. Finally, denote by $\mathrm{Div}^0_\infty(K)$ the set of divisors in $\mathrm{Div}^0(K)$ whose coefficients at places $\mathfrak{p} \notin S$ are zero. With these, we have the following

commuting diagram with exact rows and columns:



The object T is the kernel of $\mathrm{Pic}^0(K) \to \mathrm{Pic}(\mathcal{O})$.

If K is a number field, $\mathrm{Div}^0_\infty(K) \cong \mathbb{R}^{|S|-1}$, the image of $\mathcal{O}^*/k^*$ is a full lattice in $\mathbb{R}^{|S|-1}$ and, hence, T is an $(|S|-1)$-dimensional torus. Moreover, both $H = 0$ and $H' = 0$.

If K is a function field, $\mathrm{Div}^0_\infty(K) \cong \mathbb{Z}^{|S|-1}$. If k is finite, T is finite by Dirichlet's Unit Theorem. **During the whole thesis, we assume that T is finite**[1], i.e. that the image of $\mathcal{O}^*/k^*$ in $\mathbb{Z}^{|S|-1} \subseteq \mathbb{R}^{|S|-1}$ is a full lattice. We have that $H = 0 = H'$ if, and only if, $\gcd(\deg \mathfrak{p} \mid \mathfrak{p} \in S) = \gcd(\deg \mathfrak{p} \mid \mathfrak{p} \in \mathcal{P}_K)$, as the image of deg is $(\deg \mathfrak{p} \mid \mathfrak{p} \in \mathcal{P}_K)$; more precisely, $H \cong (\deg \mathfrak{p} \mid \mathfrak{p} \in \mathcal{P}_K)/(\deg \mathfrak{p} \mid \mathfrak{p} \in S)$.

Finally, let $\mathcal{O}^* = k^* \times \langle \varepsilon_1, \ldots, \varepsilon_n \rangle$ with $|S| = n+1$. If $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_{n+1}\}$, consider the matrix $A := (\nu_{\mathfrak{p}_i}(\varepsilon_j) \deg \mathfrak{p}_i)_{ij} \in \mathbb{R}^{n \times n}$; then $R := |\det A|$ is called the regulator of K [Ros02, p. 245, definition of the q-regulator].

1.2 Notations

We will use $A \subseteq B$ to denote that A is a subset of B or that A equals B, and $A \subsetneqq B$ if A is a subset of B but A does not equal B. We will use $|A|$ to denote the cardinality of a set A, and $A \setminus B$ to denote the difference set of two sets A and B. The natural numbers $\mathbb{N}$ include 0.

All rings in this thesis are commutative and have a unit, always denoted by 1. Subrings have the same 1, and ring morphisms preserve the 1. Ideals are denoted by old German letters $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{m}$, $\mathfrak{p}$, $\mathfrak{q}$, etc.

[1] The finiteness of T is mainly required for the set of reduced ideals inside an ideal class to be finite. Most of the general theory for computation in $\mathrm{Pic}^0(K)$ respectively $\mathrm{Pic}(K)/\langle[\mathfrak{p}]\rangle$ in this paper can be carried over to the case of infinite T without any change.

If R is a ring, M an R-module and $T \subseteq M$ a subset, then $\langle T \rangle_R$ or $\langle T \rangle$ denotes the sub-R-module of M generated by T. If $T = \{x_1, \ldots, x_n\}$ is finite, we often write $\langle x_1, \ldots, x_n \rangle_R$ instead of $\langle \{x_1, \ldots, x_n\} \rangle_R$.

The kernel of a morphism φ is denoted by $\ker \varphi$.

We will use $\bullet$ as a placeholder symbol; for example, $\sqrt{\bullet}$ will denote the square root map $x \mapsto \sqrt{x}$.

For real numbers $a, b \in \mathbb{R}$, we will use the notation $[a, b)$ for the half-open interval $\{r \in \mathbb{R} \mid a \leq r < b\}$.

Zero objects, like the zero ring, the zero ideal, the zero group, the zero module, etc., are denoted simply by 0.

If X is a set and $\sim$ an equivalence relation on X, we write $X/_\sim$ for the set of equivalence classes of $\sim$ and $[x]_\sim$ or $[x]$ for the equivalence class of $x \in X$ in $X/_\sim$.

We will use the symbol $\mathcal{O}(f)$ for a function $f : \mathbb{N}^k \to \mathbb{R}_{>0}$ for the class of functions which are bounded asymptotically by f, i.e. for the functions g such that there exists a constant $\lambda > 0$ with $\frac{g(n)}{f(n)} \leq \lambda$ for all $n \in \mathbb{N}^k$; for such a function g, we write $g = \mathcal{O}(f)$. Finally, for a second function $h : \mathbb{N}^k \to \mathbb{R}_{>0}$, if we write $g = \mathcal{O}(f^\varepsilon h)$, we mean that for every $\varepsilon > 0$, we have $g = \mathcal{O}(f^\varepsilon h)$; the $\mathcal{O}$-constant depends on ε. One use is to describe the running time of an algorithm by, for example, $\mathcal{O}(D^\varepsilon \sqrt{R})$; here, $(D, R) \in \mathbb{N}^2$ are the parameters of the functions $f : (D, R) \mapsto D$ and $h : (D, R) \mapsto \sqrt{R}$.

Chapter 2

Abstract Infrastructure

The classical infrastructure, as it was described by D. Shanks [Sha72] and H. W. Lenstra [Len82], is one-dimensional. In this chapter, we want to describe an abstract version of the (one-dimensional) infrastructure, which suffices to describe algorithms and applications such as key exchange in cryptography. Then, we want to discuss how the infrastructure can be generalized to higher dimensions.

2.1 One-Dimensional Infrastructure

The idea of the infrastructure with baby steps and giant steps goes back to D. Shanks [Sha72]; he considered the one-dimensional infrastructure of a real quadratic number field, for which he developed a baby step-giant step algorithm similar to the one he invented for the class groups of imaginary quadratic number fields in [Sha71].

We begin by sketching an abstract version of a one-dimensional infrastructure, similar to the one which can be found in [Fon08]. Our definition of a one-dimensional infrastructure and interpretation of baby steps and giant steps is based on H. W. Lenstra's interpretation of Shanks' infrastructure using a 'circle group' [Len82].

Roughly spoken, a one-dimensional infrastructure can be interpreted as a circle with a finite set of points on it.

Definition 2.1.1. *Let $R \in \mathbb{R}_{>0}$ be a positive real number. A* one-dimensional *(or* cyclic*)* infrastructure (X, d) *of* circumference R *is a non-empty finite set X with an injective map $d : X \to \mathbb{R}/R\mathbb{Z}$, called the* distance *function.*

In the case of Shanks, X is the set of reduced principal ideals $\frac{1}{\mu}\mathcal{O}$ of a real quadratic number field $K = \mathbb{Q}(\sqrt{D}) \subseteq \mathbb{R}$, $D > 1$ square-free, R the regulator of K and $d : X \to \mathbb{R}/R\mathbb{Z}$ defined by $\frac{1}{\mu}\mathcal{O} \mapsto -\log|\mu|$.

Definition 2.1.2. *We say that a one-dimensional infrastructure (X, d) of circumference R is* discrete *if $R \in \mathbb{Z}$ and $d(X) \subseteq \mathbb{Z}/R\mathbb{Z}$.*

One can interpret finite cyclic groups as discrete one-dimensional infrastructures as follows: Let $G = \langle g \rangle$ be a finite cyclic group of order m and $d : G \to \mathbb{Z}/m\mathbb{Z}$ be the *discrete logarithm* map[1] (to the base g), i.e. we have $g^{d(h)} = h$ for every $h \in \langle g \rangle$. By interpreting $\mathbb{Z}/m\mathbb{Z}$ as a subset of $\mathbb{R}/m\mathbb{Z}$, we get that (G, d) is a discrete one-dimensional infrastructure of circumference m.

An infrastructure has two operations, namely baby steps and giant steps. For their definition, we need the following notation:

Definition 2.1.3. *Let $R \in \mathbb{R}_{>0}$ and let $x, y \in \mathbb{R}/R\mathbb{Z}$. Write $x = \hat{x} + R\mathbb{Z}$ and $y = \hat{y} + R\mathbb{Z}$ with $\hat{x}, \hat{y} \in \mathbb{R}$ such that $\hat{x} \leq \hat{y} < \hat{x} + R$. Define*

$$[x, y] := \{t + R\mathbb{Z} \mid t \in \mathbb{R},\ \hat{x} \leq t \leq \hat{y}\}.$$

If one interprets $\mathbb{R}/R\mathbb{Z}$ as a circle with circumference R, and x and y as points on this circle, the set $[x, y]$ can be interpreted as the points on the circle which lie on the arc beginning at x and ending at y.

Now we can define baby steps and giant steps. We will exclude the case $|X| = 1$, as in this case the infrastructure is trivial and not of practical interest.

Proposition and Definition 2.1.4. *Let (X, d) be a one-dimensional infrastructure of circumference R. Assume that $|X| > 1$.*

(a) *Then there is a unique bijective fixed point free map* bs $: X \to X$ *such that for every $x \in X$, we have*

$$[d(x), d(\mathrm{bs}(x))] \cap d(X) = \{d(x), d(\mathrm{bs}(x))\}.$$

This map is called baby step *map.*

[1] The *discrete logarithm* of an element $h \in \langle g \rangle$ is sometimes, in particular in Elementary Number Theory, also called the *index* of h with respect to g.

(b) *Moreover, there is a unique map* $\mathrm{gs} : X \times X \to X$ *such that for every* $x, y \in X$*, we have*

$$[d(\mathrm{gs}(x,y)), d(x) + d(y)] \cap d(X) = \{d(\mathrm{gs}(x,y))\}.$$

This map is called giant step *map.*

Note that the description of giant steps here is slightly different than the one in [Fon08]; there, the giant step is defined by

$$[d(x) + d(y), d(\mathrm{gs}(x,y))] \cap d(X) = \{d(\mathrm{gs}(x,y))\},$$

i.e. the giant step of $x, y \in X$ is the element of X whose distance comes right next after $d(x) + d(y)$.

Proof. For $x \in X$, define $f := \inf\{e \in \mathbb{R} \mid e > 0,\ d(x) + e \in d(X)\}$; then $d(x) + f \in d(X)$ and $\mathrm{bs}(x) := d^{-1}(d(x) + f)$ satisfies the required properties.

For $x, y \in X$, define $f := \inf\{e \in \mathbb{R} \mid e \geq 0,\ d(x) + d(y) - e \in d(X)\}$; then $d(x) + d(y) - f \in d(X)$ and $\mathrm{gs}(x,y) := d^{-1}(d(x) + d(y) - f)$ satisfies the required properties. □

The baby step map assigns to every $x \in X$ the element of X which comes right after x, seen on the circle, in the sense that $f := d(\mathrm{bs}(x)) - d(x) > 0$ is the smallest positive number satisfying $d(x) + f \in d(X)$.

The giant step map assigns to $x, y \in X$ the element of X with largest distance not exceeding $d(x) + d(y)$: this means that $f := d(x) + d(y) - d(\mathrm{gs}(x,y)) \geq 0$ the smallest non-negative number satisfying $d(x) + d(y) - f \in d(X)$.

In the case $|X| = 1$, there is exactly one way to define functions $\mathrm{bs} : X \to X$ and $\mathrm{gs} : X \times X \to X$. Both maps satisfy the statements from the proposition except that bs is not fixed point free.

Also note that in Shanks' case, these functions can be computed efficiently by performing a certain amount of steps in the continued fraction expansion of μ respectively $\mu\mu'$ (which can be obtained form $\frac{1}{\mu}\mathcal{O}$), if $\mathrm{bs}(\frac{1}{\mu}\mathcal{O})$ respectively $\mathrm{gs}(\frac{1}{\mu}\mathcal{O}, \frac{1}{\mu'}\mathcal{O})$ is sought.

Example 2.1.5. Let $G = \langle g \rangle$ be a finite cyclic group of order n and let $d : G \to \mathbb{Z}/n\mathbb{Z}$ be the discrete logarithm map to the base g. Then, for the one-dimensional infrastructure (G, d), we have $\mathrm{bs}(h) = gh$ and $\mathrm{gs}(h, h') = hh'$ for all $h, h' \in G$. Applying d, this translates to $d(\mathrm{bs}(h)) = d(h) + 1$ and $d(\mathrm{gs}(h, h')) = d(h) + d(h')$. This shows that baby and giant steps in arbitrary infrastructures generalize the group operation of a finite cyclic group.

In the case of finite cyclic groups, both baby steps and giant steps are basically the same operation. In arbitrary infrastructures, this is not the case, as in general there is no element $x \in X$ with $\mathrm{gs}(x, y) = \mathrm{bs}(y)$ for all $y \in X$.

In general, one-dimensional infrastructures behave similar to cyclic finite groups, with the main difference being that the giant step operation is not necessarily associative, but "almost" associative in the sense that

$$d(\mathrm{gs}(x, y)) \approx d(x) + d(y).$$

Here, "$\approx$" for elements in $\mathbb{R}/R\mathbb{Z}$ means that both sides have representatives in $\mathbb{R}$ which are relatively close to each other.

Before ending this section, we want to describe how to obtain a one-dimensional infrastructure from certain global fields of unit rank one:

Example 2.1.6. Let K be a global field with $S = \{\mathfrak{p}_1, \mathfrak{p}_2\}$. Assume that $\deg \mathfrak{p}_i = 1$ for at least one i. We say that a principal $\mathcal{O}$-ideal $\mathfrak{a}$ is *reduced* if $1 \in \mathfrak{a}$ and, for every $f \in \mathfrak{a} \setminus \{0\}$, the inequalities $\nu_{\mathfrak{p}_i}(f) \geq 0$, $i = 1, 2$ imply $f \in k^*$ (see Definition 3.6.1). Denote the set of reduced principal $\mathcal{O}$-ideals by X (see Theorem 3.4.1).

Now $\mathcal{O}^* = k^* \times \langle \varepsilon \rangle$ for some $\varepsilon \in \mathcal{O}^*$; define $R := |\nu_{\mathfrak{p}_1}(\varepsilon)|$. Then, for a reduced principal ideal $\mathfrak{a} = (f)$, the expression $d(\mathfrak{a}) := \nu_{\mathfrak{p}_1}(f) + R\mathbb{Z} \in \mathbb{R}/R\mathbb{Z}$ is well-defined. This gives an injective map $d : X \to \mathbb{R}/R\mathbb{Z}$ (see Proposition 4.6.1).

Therefore, (X, d) is an infrastructure. Moreover, it is discrete if, and only if, K is a function field (see Proposition 4.5.2).

2.2 Obtaining Groups from One-Dimensional Infrastructures

Our aim is to embed a one-dimensional infrastructure into a one-dimensional torus and to describe arithmetic on the torus using the arithmetic of the infrastructure, i.e. by using giant and baby steps. For that, we pick up an idea by D. Hühnlein and S. Paulus and M. J. Jacobson, R. Scheidler and H. C. Williams, which was, for example, described in [HP01] and [JSW01].

Let (X, d) be a one-dimensional infrastructure of circumference R. The map

$$X \times \mathbb{R} \to \mathbb{R}/R\mathbb{Z}, \qquad (x, f) \mapsto d(x) + f$$

is clearly surjective, as X is non-empty. The idea of f-representations is to choose a subset of $X \times \mathbb{R}$ such that if we restrict the above map to this subject, we will obtain a bijection. One way to do this is the following:

Definition 2.2.1. *An* f-representation *is a pair* (x, f)*, where* $x \in X$ *and* $f \in [0, R)$ *such that* $[d(x), d(x) + f] \cap d(X) = \{d(x)\}$*. Denote the set of* f*-representations by* $\mathrm{Rep}^f(X, d)$*.*

If (X, d) *is discrete, define the subset*

$$\mathrm{Rep}^f_{\mathrm{discrete}}(X, d) := \{(x, d) \in \mathrm{Rep}^f(X, d) \mid d \in \mathbb{Z}\}.$$

Definition 2.2.2. *Define the* (absolute) distance *of a pair* $(x, f) \in X \times \mathbb{R}$ *by*

$$d(x, f) := d(x) + f \in \mathbb{R}/R\mathbb{Z}.$$

Then we have the following proposition:

Proposition 2.2.3. *The map*

$$d|_{\mathrm{Rep}^f(X,d)} : \mathrm{Rep}^f(X, d) \to \mathbb{R}/R\mathbb{Z}, \qquad (x, f) \mapsto d(x, f) = d(x) + f$$

gives a bijection between the set of f*-representations and* $\mathbb{R}/R\mathbb{Z}$*. If* (X, d) *is discrete, this restricts to a bijection*

$$d|_{\mathrm{Rep}^f_{\mathrm{discrete}}(X,d)} : \mathrm{Rep}^f_{\mathrm{discrete}}(X, d) \to \mathbb{Z}/R\mathbb{Z}.$$

□

Remark 2.2.4. If $(x, f) \in X \times \mathbb{R}$ is arbitrary, there exists a *unique* f-representation (x', f') such that $d(x, f) = d(x', f')$. More precisely, it is the pair (x', f') with $d(x, f) = d(x', f')$ such that $f' \geq 0$ is minimal.

If $|f|$ is small, (x', f') can be computed efficiently using baby steps by starting with (x, f) and minimizing f:

(1) While f is negative, replace (x, f) by $(\mathrm{bs}^{-1}(x), f + \Delta)$, where $\Delta := d(x) - d(\mathrm{bs}^{-1}(x)) \in [0, R)$.

(2) Compute $x'' := \mathrm{bs}(x)$ and $\Delta' := d(x'') - d(x) \in [0, R)$.

(3) If $\Delta' > f$, then (x, f) is an f-representation and we are done.

(4) Otherwise, replace (x, f) by $(x'', f - \Delta')$ and continue with step (2).

One quickly sees that all operations do not modify the distance $d(x, f)$. In case (X, d) is discrete, one needs at most $|f|$ (inverse) baby step computations.

Using this remark, we get the following proposition:

Proposition 2.2.5. *If (x, f) and (x', f') are f-representations, consider the tuple*

$$(\mathrm{gs}(x, x'), f + f' - (d(\mathrm{gs}(x, x')) - d(x) - d(x'))).$$

By the previous remark, it corresponds to a unique f-representation (x'', f''). If we define

$$(x, f) \circ (x', f') := (x'', f''),$$

we get that $(\mathrm{Rep}^f(X, d), \circ)$ is a group and

$$d|_{\mathrm{Rep}^f(X,d)} : (\mathrm{Rep}^f(X, d), \circ) \to (\mathbb{R}/R\mathbb{Z}, +)$$

is a group isomorphism. If (X, d) is discrete, we get that $(\mathrm{Rep}^f_{\mathrm{discrete}}(X, d), \circ)$ is a subgroup of $\mathrm{Rep}^f(X, d)$ and that

$$d|_{\mathrm{Rep}^f_{\mathrm{discrete}}(X,d)} : (\mathrm{Rep}^f_{\mathrm{discrete}}(X, d), \circ) \to (\mathbb{Z}/R\mathbb{Z}, +)$$

is a group isomorphism. The relationships between these structures are described in the following diagram:

$$\begin{array}{ccccc}
X \times \mathbb{R} & \supsetneq & \mathrm{Rep}^f(X, d) & \supsetneq & \mathrm{Rep}^f_{\mathrm{discrete}}(X, d) \\
\Big\downarrow{\scriptstyle d} & & \Big\downarrow{\scriptstyle \cong\, d|_{\mathrm{Rep}^f(X,d)}} & & \Big\downarrow{\scriptstyle \cong\, d|_{\mathrm{Rep}^f_{\mathrm{discrete}}(X,d)}} \\
\mathbb{R}/R\mathbb{Z} & = & \mathbb{R}/R\mathbb{Z} & \supsetneq & \mathbb{Z}/R\mathbb{Z}
\end{array}$$

□

Therefore, if we are able to effectively compute bs, bs^{-1} and gs and relative distances[2] for an infrastructure (X, d), we can efficiently compute in a group isomorphic to $\mathbb{R}/R\mathbb{Z}$ or $\mathbb{Z}/R\mathbb{Z}$, even if R is unknown and without the need to evaluate the function d for general elements of X. More precisely:

[2]The *relative distance* between x and its baby step $\mathrm{bs}(x)$ is the difference $d(\mathrm{bs}(x)) - d(x)$, and the *relative distance* between x, y and their giant step $\mathrm{gs}(x, y)$ is the difference $d(x) + d(y) - d(\mathrm{gs}(x, y))$. We interpret these relative distances as elements of $[0, R)$.

Corollary 2.2.6. *Let* (X, d) *be an infrastructure such that* bs, bs^{-1} *and* gs *are efficiently computable, together with the relative distances. Let*

$$d_{\min} := \min\{d(\mathrm{bs}(x)) - d(x) \mid x \in X\}$$
$$\textit{and} \qquad d_{\max} := \max\{d(\mathrm{bs}(x)) - d(x) \mid x \in X\}.$$

Then one group operation in $\mathrm{Rep}^f(X, d)$ *can be computed using one* gs *computation and at most* $\lceil \frac{3d_{\max}}{d_{\min}} \rceil$ *computations of* bs.

Proof. Given $(x, f), (x', f') \in \mathrm{Rep}^f(X, f)$, one first computes (x'', f'') by $x'' := \mathrm{gs}(x, x')$ and $f'' := f + f' + (d(x) + d(x') - d(x''))$; then $d(x'', f'') = d(x, f) + d(x', f')$. As, by definition of the giant step function, $0 \leq d(x) + d(x') - d(x'') < d_{\max}$, we have $0 \leq f'' < 3d_{\max}$. When replacing (x'', f'') by $(\mathrm{bs}(x''), f'' - (d(\mathrm{bs}(x'')) - d(x'')))$, we have that f'' decreases at least by $d_{\min}$. Hence, we can do at most $\lceil \frac{3d_{\max}}{d_{\min}} \rceil$ baby steps before f'' gets negative. □

Remark 2.2.7. In case we want to compute in $\mathrm{Rep}^f(X, d)$ (which is, for example, necessary if (X, d) is not discrete), we need to work with (arbitrary) real numbers. As this is not possible on computers, one needs to approximate them using floating point numbers. More details on this can be found in [HP01] and [JSW01]; there, such representations are called CRIAD-representations respectively (f, p)-representations.

2.3 Applications

We present three applications of infrastructures in this section. Two of them have first been described without the interpretation of an one-dimensional infrastructure (X, d) as a subset sitting in a group, namely $\mathrm{Rep}^f(X, d)$ respectively $\mathrm{Rep}^f_{\mathrm{discrete}}(X, d)$. Including this interpretation makes it easier to understand how these applications work.

2.3.1 Key Exchange

In Cryptography, one often has the problem that two parties, call them Alice and Bob, want to exchange a *secret key*, i.e. some data which is only known to the two of them, over a *public channel*, i.e. some way where everyone can possibly be listening. W. Diffie and M. Hellman published a paper entitled *New Directions in Cryptography* in 1976, where they described a way to do such a key exchange. We first describe a more abstract version of their protocol.

First, Alice and Bob decide on a group G and an element $g \in G$; the order of g should be high. Then, Alice and Bob choose integers $a, b \in \mathbb{Z}$ such that a is only known to Alice and b is only known to Bob. Alice computes $g_{Alice} := g^a$ and sends it over the public channel to Bob, while Bob computes $g_{Bob} := g^b$ and sends it over the public channel to Alice. Then, both Alice and Bob can compute the secret key $g_{key} := g_{Alice}^b = g_{Bob}^a = g^{ab}$.

Any eavesdropper listening to their communication can deduce G, g, g_{Alice} and g_{Bob}, but has no other information on a and b than the relations $g^a = g_{Alice}$ and $g^b = g_{Bob}$.

One considers the following two problems:

(a) (*Diffie-Hellman Problem, DHP*) Given G, g, g_{Alice} and g_{Bob}, compute $g_{key} = g^{ab}$;

(b) (*Discrete Logarithm Problem, DLP*) Given G, g and g_{Alice}, compute any $a \in \mathbb{Z}$ such that $g^a = g_{Alice}$.

Obviously, if one can solve the DLP, one has a solution to the DHP by $g^{ab} = g_{Bob}^a$. Hence, the DLP is at least as hard as the DHP. In general, one seeks for groups in whose the DHP and the DLP is assumed to be hard. In a general cyclic group $G = \langle g \rangle$, the DLP is known to be hard by a result of V. Shoup [Sho97].

As the group G, one can also use the group of f-representations obtained from an infrastructure (X, d). The description of the protocol does not change for this new setting; only that instead of a group G with $g \in G$, one has to fix an infrastructure (X, d) together with an element $g \in \mathrm{Rep}^f(X, d)$ of small distance. We will discuss the discrete logarithm problem for infrastructures also in the next subsection.

In case one works with non-discrete infrastructures, one has to use floating point approximations to store f-representations. As it is unlikely that Alice and Bob will end up with the exact same f-representation due to rounding errors, it is a good idea to simply use the element of X from the resulting f-representations as a secret key. For the same reason, one might has to replace x by $\mathrm{bs}(x)$ or $\mathrm{bs}^{-1}(x)$ in case it turns out that one has the wrong key.

The implementation of such protocols is well-documented; a few of these can be found in [SBW94, JSW01, JSW06] using non-discrete infrastructures and [SSW96, JSS07] using discrete infrastructures.

2.3.2 The Discrete Logarithm Problem for Infrastructures

Let (X, d) be an infrastructure and $(x, f), (x', f') \in \mathrm{Rep}^f(X, d)$. Assume that $n(x, f) = (x', f')$ for some $n \in \mathbb{Z}$. Then, we have $nd(x) + nf = n(d(x) + f) = d(x') + f'$.

In case that $d(x) + f = 1$, we see that $d(x') + f' = n$. Thus, in this case, the distance of (x', f') is n. Hence, computing the distance of (x', f') is equivalent to computing n. Therefore, one can see the problem of computing distances of elements in infrastructures as a generalization of the Discrete Logarithm Problem in groups.

As every finite cyclic group can be interpreted as an infrastructure, by Shoup's result [Sho97], computation of distances can be a hard problem in at least certain instances of one-dimensional infrastructures. In certain infrastructures obtained from global fields, subexponential algorithms exist (see the end of Section 6.6).

In finite groups, for solving the Discrete Logarithm Problem one has three generic algorithms. First, one has the deterministic baby step-giant step method by D. Shanks, which we will discuss in Section 2.3.4, and one has the probabilistic Pollard ρ method by J. Pollard. Both can be used (the baby step-giant step method with a slight modification, see for example [Ter00, Tes01, ST05]) with no information on G except on how to compute with elements. The third method, the Pohlig-Hellman method [PH78], requires that the group order is known and that it has only relatively small prime factors. This method can also be applied to discrete infrastructures, as we will see in the next section.

2.3.3 Pohlig-Hellman

The Pohlig-Hellman method can be applied to discrete infrastructures; this was first noted by V. Müller, S. Vanstone and R. Zuccherato in 1998 for the special case of discrete infrastructures obtained from real quadratic function fields of characteristic 2 [MVZ98]. The general case of using Pohlig-Hellman for discrete infrastructures was described by the author in [Fon08].

As $\mathrm{Rep}^f_{\mathrm{discrete}}(X, d)$ is a finite cyclic group, the algorithm can be applied straightforward in case the order R of $\mathrm{Rep}^f_{\mathrm{discrete}}(X, d)$ is known and has only small prime factors. For that reason, we refrain from reviewing the algorithm in detail. The idea of the algorithm is based on two ideas:

(a) Using the Chinese Remainder Theorem, it suffices to investigate the discrete logarithm problem for one prime factor of R at the same time;

if p^e is the maximal power of p dividing R, one has to solve a DLP in a cyclic group of order p^e.

(b) Using the short exact sequence

$$0 \longrightarrow p^{e-1}\mathbb{Z}/p^e\mathbb{Z} \xrightarrow{\mathrm{id}} \mathbb{Z}/p^e\mathbb{Z} \xrightarrow{\cdot p} p\mathbb{Z}/p^e\mathbb{Z} \longrightarrow 0,$$

one reduces the DLP in $\mathbb{Z}/p^e\mathbb{Z}$ to a DLP in $p\mathbb{Z}/p^e\mathbb{Z} \cong \mathbb{Z}/p^{e-1}\mathbb{Z}$ and to one in $p^{e-1}\mathbb{Z}/p^e\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z}$. Applying this recursively to the DLP in $p\mathbb{Z}/p^e\mathbb{Z} \cong \mathbb{Z}/p^{e-1}\mathbb{Z}$, one reduces the DLP in $\mathbb{Z}/p^e\mathbb{Z}$ to e DLPs in $\mathbb{Z}/p\mathbb{Z}$.

We just want to note that up to now, the author is not aware that anyone was able to apply a variant of the Pohlig-Hellman method to non-discrete infrastructures. In particular, in the case of infrastructures (X, d) obtained from number fields, no elements $(x, 0) \in \mathrm{Rep}^f(X, d)$ of finite order exists except the neutral element (see Proposition 4.5.3); this makes it impossible to apply the Pohlig-Hellman method without severe modifications.

2.3.4 Baby Step-Giant Step Method

The baby step-giant step algorithm was invented by D. Shanks to compute orders of elements in class groups of imaginary fields. Later, he also used the algorithm for computing the circumference R of an one-dimensional infrastructure (X, d) obtained from real quadratic number fields [Sha72]. His description does not make use of an embedding of the infrastructure into a group like $\mathrm{Rep}^f(X, d)$.

The algorithm can be used for two purposes: a) computing R and b) computing $d(x)$ for some $x \in X$. For a), the idea is to first compute all $x \in X$ with $d(x) \in [0, A]$ together with their distance for some $A > 0$, which should be $\approx \sqrt{R}$; the set of these x is called the *baby stock*. Then use giant steps to compute a series $x_n := \mathrm{gs}(x_{n-1}, x_0)$ beginning with an element x_0 with $d(x_0) \approx A$, but $d(x_0) \leq A$, until x_n lies in the set of precomputed elements, i.e. $d(x_n)$ is known to be in $[0, A]$. Then one can add up the distances from the giant steps to obtain two different values for $d(x_n)$, which should differ by exactly R.

In case b), one starts with the element x_0 whose distance is sought, and computes $x_n := \mathrm{gs}(x_{n-1}, x')$ for some fixed x' with known $d(x') \approx A$, $d(x') \leq A$. If $d(x_n) \in [0, A]$ is known, one can use this relation to obtain $d(x_0)$.

Note that if the infrastructure is discrete, one could of course also use the group version of the algorithm and apply it to $\mathrm{Rep}^f_{\mathrm{discrete}}(X, d)$; the

disadvantage is that one stores in general more group elements than one would need, and one does too many baby steps which are not exactly needed.

The baby step-giant step method for infrastructures is, for example, described in [Len82, SZ91, SW99, Mau00]. A general overview of various optimizations of the baby step-giant step method for special cases can be found in [Tes01, ST05].

2.4 Generalizing to Higher Dimensions

We begin by reconsidering the one-dimensional case.

Remarks 2.4.1. Let (X, d) be a one-dimensional infrastructure of circumference R. The map

$$red : \mathbb{R}/R\mathbb{Z} \to X, \qquad v \mapsto \pi_1(d^{-1}(v)),$$

where $\pi_1 : X \times \mathbb{R} \to X$ denotes the projection onto the first component and where $d : \mathrm{Rep}^f(X, d) \to \mathbb{R}/R\mathbb{Z}$ is the bijection from Proposition 2.2.3, is somewhat arbitrary.

(a) If $red' : \mathbb{R}/R\mathbb{Z} \to X$ is any other map with $red'(d(x)) = x$ for every $x \in X$, one could define

$$\mathrm{Rep}^f{}_{red'}(X, d) := \{(x, f) \in X \times \mathbb{R}/R\mathbb{Z} \mid red'(d(x) + f) = x\}$$

to obtain a bijection

$$d_{red'} : \mathrm{Rep}^f{}_{red'}(X, d) \to \mathbb{R}/R\mathbb{Z}, \qquad (x, f) \mapsto d(x) + f$$

with $\pi_1 \circ (d_{red'})^{-1} = red'$. Note that the condition $red' \circ d = \mathrm{id}$ ensures that $(x, 0) \in \mathrm{Rep}^f{}_{red'}(X, d)$ for every $x \in X$.

(b) We want to note that our choice of red is not more natural than others. For example, other possible choices are to use f-representations with the largest non-positive f (instead with the smallest non-negative f) or with the smallest absolute value of f (with some adaptions in case $d(x) + f$ lies exactly between two elements of $d(X)$); the latter is for example used in [GHMM08].

(c) Note that one could define gs using the reduction map: for every $x, y \in X$, we have $\mathrm{gs}(x, y) = red(d(x) + d(y))$. In the same way, for any given reduction map $red' : \mathbb{R}/R\mathbb{Z} \to X$, we can define a giant step $\mathrm{gs}^{red'} : X \times X \to X$ by $(x, y) \mapsto red'(d(x) + d(y))$.

These considerations will be of importance when generalizing giant steps and f-representations.

To generalize a one-dimensional infrastructure to higher dimensions, one has to replace the circle $\mathbb{R}/R\mathbb{Z}$ with a higher dimensional analogon. The obvious choice is a torus $\mathbb{R}^n/\Lambda$, where $\Lambda \subseteq \mathbb{R}^n$ is a full lattice. A first definition of an n-dimensional infrastructure could read as follows:

Definition 2.4.2. *An* n-dimensional infrastructure *is a full lattice* $\Lambda \subseteq \mathbb{R}^n$ *together with a finite non-empty set* X *and an injective map* $d : X \to \mathbb{R}^n/\Lambda$.

We still have that the map

$$\Psi : X \times \mathbb{R}^n \to \mathbb{R}^n/\Lambda, \qquad (x, f) \mapsto d(x) + f$$

is surjective. Hence, as in the case $n = 1$, we are interested in reduction maps $red : \mathbb{R}^n/\Lambda \to X$ with $red \circ d = \mathrm{id}_X$. In that case, we can define

$$\mathrm{Rep}^f{}_{red}(X, d) := \{(x, f) \in X \times \mathbb{R}^n/\Lambda \mid red(d(x) + f) = x\}$$

and obtain a bijection

$$d_{red} : \mathrm{Rep}^f{}_{red}(X, d) \to \mathbb{R}^n/\Lambda, \qquad (x, f) \mapsto d(x) + f.$$

Again, using the reduction together with the natural group operation on $\mathbb{R}^n/\Lambda$, one could define a giant step:

$$\mathrm{gs}_{red} : X \times X \to X, \qquad (x, y) \mapsto red(d(x) + d(y)).$$

Generalizing baby steps is a different issue. On the one-dimensional torus $\mathbb{R}/R\mathbb{Z}$, there are basically two directions: positive and negative, i.e. clockwise or counter-clockwise if $\mathbb{R}/R\mathbb{Z}$ is considered as a circle. On the n-dimensional torus $\mathbb{R}^n/\Lambda \cong (\mathbb{R}/\mathbb{Z})^n$, there are infinitely many directions. Given a direction, one could define a baby step as "moving as long in the given direction until an element from X is near enough". This is rather inconcrete, and we will ignore this point during the rest of this thesis. Note that in the case of an n-dimensional infrastructure obtained from a function or number field, baby steps in certain directions (corresponding to elements of S) do exist and can be computed effectively. We will consider these in Section 3.5; also see [Buc85a] for a way to define them in number fields.

The main problem of n-dimensional infrastructures is finding a reduction map $red : \mathbb{R}^n/\Lambda \to X$. We have seen in Remark 2.4.1 that already in the one-dimensional case, there are several "obvious" reductions. In the n-dimensional case, there exist many more. For this reason, we give another definition of an n-dimensional infrastructure which respects this:

Definition 2.4.3. *An* n-dimensional infrastructure (X, d, red) *is a full lattice* $\Lambda \subseteq \mathbb{R}^n$ *together with a finite non-empty set* X*, an injective map* $d : X \to \mathbb{R}^n/\Lambda$ *and a map* $red : \mathbb{R}^n/\Lambda \to X$ *such that* $red \circ d = \mathrm{id}_X$.

Remark 2.4.4. Assume that $\Lambda \subseteq \mathbb{Z}^n$ is a full lattice, X a finite non-empty set and $d : X \to \mathbb{Z}^n/\Lambda$ injective. Moreover, assume that $red : \mathbb{Z}^n/\Lambda \to X$ satisfies $red \circ d = \mathrm{id}_X$. Then we can turn (X, d, red) into an infrastructure by considering Λ as a lattice in $\mathbb{R}^n$, using the embedding $\mathbb{Z}^n/\Lambda \subseteq \mathbb{R}^n/\Lambda$ and defining $\widehat{red} : \mathbb{R}^n/\Lambda \to X$ by $\widehat{red} := red \circ floor$, where

$$floor : \mathbb{R}^n/\Lambda \to \mathbb{Z}^n/\Lambda, \quad (x_1, \ldots, x_n) + \Lambda \mapsto (\lfloor x_1 \rfloor, \ldots, \lfloor x_n \rfloor) + \Lambda;$$

then $(X, d, \widehat{red})$ is an n-dimensional infrastructure in the above sense.

From now on, we will misuse the notation and simply say that (X, d, red) is an infrastructure even though we mean that $(X, d, \widehat{red})$ is one.

Note that we can interpret any finite abelian group as an infrastructure: assume that a finite abelian group G is generated by $g_1, \ldots, g_n$. Then define

$$\Lambda := \left\{ (\lambda_1, \ldots, \lambda_n) \in \mathbb{Z}^n \;\middle|\; \sum_{i=1}^{n} \lambda_i g_i = 0 \right\} \subseteq \mathbb{Z}^n;$$

this is a full lattice with $\mathbb{Z}^n/\Lambda \cong G$, with the isomorphism given by $\varphi : \mathbb{Z}^n/\Lambda \to G$, $(\lambda_1, \ldots, \lambda_n) + \Lambda \mapsto \sum_{i=1}^{n} \lambda_i g_i$. Define $X := G$, $d := \varphi^{-1}$ and $red := \varphi$; then (X, d, red) is an n-dimensional infrastructure.

Before we will concentrate on the case of an infrastructure obtained from a function or number field, we want to present a method for constructing reduction maps which is pretty much related to the method introduced for number and function fields in Chapter 4.

The aim is to generalize the f-representations defined in Section 2.2, i.e. for every $v \in \mathbb{R}^n/\Lambda$ we want to associate a unique $x \in X$ and $f \in \mathbb{R}^n_{\geq 0}$ with $d(x) + f = v$. In some sense, f should be minimal. One could take a total order $<$ on $\mathbb{R}^n_{\geq 0}$ which satisfies $0 < v$ for every $v \in \mathbb{R}^n_{\geq 0} \setminus \{0\}$ and which attains a minimum on every discrete subset of $\mathbb{R}^n_{\geq 0}$. For $v \in \mathbb{R}^n/\Lambda$, we consider the discrete set

$$A_v := \{f \in \mathbb{R}^n_{\geq 0} \mid \exists x \in X : d(x) + f = v\}.$$

By hypothesis, there exists a minimal element $f_{v,<}$ in A_v with respect to $<$, and we denote $d^{-1}(v - f_{v,<})$ by $red^<(v)$. Then $(X, d, red^<)$ is an n-dimensional infrastructure.

Remark 2.4.5. Another interpretation is to "unroll" the torus under the preimage map associated to the projection $\pi : \mathbb{R}^n \to \mathbb{R}^n/\Lambda$:

We define $\hat{X} := \pi^{-1}(d(X))$ and pick one preimage $\hat{v} \in \mathbb{R}^n$ of v, i.e. $\pi(\hat{v}) = v$. Then we consider the set

$$\hat{A}_v := \{\hat{x} \in \hat{X} \mid \hat{x} \leq \hat{v}\},$$

where $\leq$ on $\mathbb{R}^n$ denotes the component-wise partial order induced by the standard order on $\mathbb{R}$. Then the map

$$\hat{A}_v \to A_v, \qquad \hat{x} \mapsto \hat{v} - \hat{x}$$

gives a bijection and $<$ on A_v induces an order $\hat{<}$ on $\hat{A}_v$.

One way to obtain such orders $<$ on $\mathbb{R}^n_{\geq 0}$ is to use some kind of degree balanced lexicographic order. For that, define a degree map $deg : \mathbb{R}^n_{\geq 0} \to \mathbb{R}_{\geq 0}$ with $deg(0) = 0$, for example by choosing positive real numbers $\lambda_1, \ldots, \lambda_n \in \mathbb{R}_{>0}$ and setting

$$deg(v) := \sum_{i=1}^{n} \lambda_i v_i \quad \text{for } v = (v_1, \ldots, v_n) \in \mathbb{R}^n_{\geq 0}.$$

Then one can define $<_{deg}$ by defining

$$v <_{deg} w :\Longleftrightarrow \begin{cases} deg(v) < deg(w) \text{ or} \\ deg(v) = deg(w) \text{ and } v <_{\ell ex} w, \end{cases}$$

where

$$v <_{\ell ex} w :\Longleftrightarrow \exists i \in \{1, \ldots, n\} : v_1 = w_1 \wedge \cdots \wedge v_{i-1} = w_{i-1} \wedge v_i < w_i$$

is the usual lexicographic order on $\mathbb{R}^n$.

If one requires that for every $\delta > 0$, the set $\{x \in \mathbb{R}^n \mid deg(x) \leq \delta\}$ is compact (which is satisfied by defining deg as above), then $<_{deg}$ satisfies the requirement that $0 <_{deg} v$ for every $v \in \mathbb{R}^n \setminus \{0\}$ and that $<_{deg}$ attains a minimum on every discrete subset of $\mathbb{R}^n_{\geq 0}$, i.e. $<_{deg}$ gives a reduction map $red_{<_{deg}}$.

Finally, note that the degree map we will implicitly use later is similar to the one defined above, i.e. we will have numbers $\lambda_1, \ldots, \lambda_n \in \mathbb{N}$ and bounds $c, C \in \mathbb{R}$ such that

$$c \leq \deg(v) - \sum_{i=1}^{n} \lambda_i v_i \leq C$$

for all $v = (v_1, \ldots, v_n) \in \mathbb{R}^n_{\geq 0}$. Moreover, note that our degree map will depend on x.

Chapter 3

Minima of Ideals in Global Fields

The aim of this chapter is to investigate the set of minima of an ideal. Later on, this will lead us to the infrastructure of a global field. The study of the set of minima with the neighbor relation poses several interesting questions on its own, and will be of importance for Buchmann's algorithms (see Sections 6.3 and 6.4). Finally, the structure of the minima allows to define baby steps, which is an operation which has apparently no good generalization to higher dimensional infrastructures.

3.1 Boxes

The definition of minima and reduced ideals is rather geometric, in the sense of the Geometry of Numbers introduced by H. Minkowski [Min68] in the number field case and K. Mahler [Mah41] in the function field case. We begin by describing certain parallelepipeds intersected with lattices, for which we will use the term *boxes*.

Let $\mathfrak{a} \in \mathrm{Id}(\mathcal{O})$ and $t_\mathfrak{p} \in \mathbb{R}$ for $\mathfrak{p} \in S$. Consider

$$\begin{aligned} B(\mathfrak{a}, (t_\mathfrak{p})_{\mathfrak{p}\in S}) &:= \{f \in \mathfrak{a} \mid \forall \mathfrak{p} \in S : |f|_\mathfrak{p} \leq q^{t_\mathfrak{p} \deg \mathfrak{p}}\} \\ &= \{f \in \mathfrak{a} \mid \forall \mathfrak{p} \in S : \nu_\mathfrak{p}(f) \geq -t_\mathfrak{p}\}; \end{aligned}$$

if K is a number field, this is a finite set, and if K is a function field, this is a finite dimensional vector space over the field of constants k.

Define $\mathrm{div}(\mathfrak{a}) := -\sum_{\mathfrak{p}\notin S} n_\mathfrak{p}\mathfrak{p}$, where $\mathfrak{a} = \prod_{\mathfrak{p}\notin S}(\mathfrak{m}_\mathfrak{p} \cap \mathcal{O})^{n_\mathfrak{p}}$ is the prime

ideal decomposition of $\mathfrak{a}$. Then we have

$$B(\mathfrak{a}, (t_\mathfrak{p})_{\mathfrak{p}\in S}) = \left\{ f \in K^* \;\middle|\; (f) \geq -\operatorname{div}(\mathfrak{a}) - \sum_{\mathfrak{p}\in S} t_\mathfrak{p}\mathfrak{p} \right\} \cup \{0\}$$
$$= L\left(\operatorname{div}(\mathfrak{a}) + \sum_{\mathfrak{p}\in S} t_\mathfrak{p}\mathfrak{p} \right),$$

if we allow real coefficients for divisors in the case of function fields; here, $L(D)$ denotes the Riemann-Roch space for the divisor D.

In the case of function fields, define $t'_\mathfrak{p} := \lfloor t_\mathfrak{p} \rfloor$. Then

$$B(\mathfrak{a}, (t_\mathfrak{p})_{\mathfrak{p}\in S}) = B(\mathfrak{a}, (t'_\mathfrak{p})_{\mathfrak{p}\in S}) = L(D')$$

for $D' = \operatorname{div}(\mathfrak{a}) + \sum_{\mathfrak{p}\in S} t'_\mathfrak{p}\mathfrak{p}$. If κ is a canonical divisor of K and g the genus of K, the *Theorem of Riemann-Roch* [Sti93, p. 28, Theorem I.5.15] says

$$\dim_k L(D'') - \dim_k L(\kappa - D'') = 1 - g + \deg D''$$

for any divisor $D'' \in \operatorname{Div}(K)$. This, together with some more ingredients, gives the following result:

Proposition 3.1.1. *Let K be a function field of genus g and let $D \in \operatorname{Div}(K)$.*

(a) *[Sti93, p. 17, Lemma I.4.7 (b)] if $\deg D < 0$, then $\dim_k L(D) = 0$;*

(b) *if $\deg D = 0$,*

$$L(D) = \begin{cases} kf^{-1} & \text{if } D = (f) \in \operatorname{Princ}(K), \\ \{0\} & \text{otherwise;} \end{cases}$$

(c) *(*Riemann's Inequality*, [Sti93, p. 21, Theorem I.4.17]) we have*

$$\dim_k L(D) \geq \deg D + 1 - g,$$

with equality if $\deg D > 2g - 2$;

(d) *[Sti93, p. 17, Lemma I.4.8] if $D \leq D'$ for $D' \in \operatorname{Div}(K)$, i.e. if $\nu_\mathfrak{p}(D) \leq \nu_\mathfrak{p}(D')$ for all $\mathfrak{p} \in \mathcal{P}_K$, then $L(D) \subseteq L(D')$ and $0 \leq \dim_k L(D') - \dim_k L(D) \leq \deg D' - \deg D$.*

The analogon to Riemann's Inequality in the number field case is Minkowski's Lattice Point Theorem [Neu99, p. 32, Theorem 5.3]. Both say that if the box $B(\mathfrak{a}, (t_\mathfrak{p})_{\mathfrak{p}\in S})$ or, more precisely, the quantity $\sum_{\mathfrak{p}\in S} t_\mathfrak{p} \deg \mathfrak{p}$, is "large enough", it contains at least one non-trivial point.

For convenience, we make the following definitions:

Definition 3.1.2. *Let* $\mu_1, \ldots, \mu_t \in K^*$.

(a) *Define*

$$B(\mathfrak{a}, \mu_1, \ldots, \mu_t) := \Big\{ f \in \mathfrak{a} \;\Big|\; |f|_\mathfrak{p} \leq \max_{i=1,\ldots,t} |\mu_i|_\mathfrak{p} \text{ for all } \mathfrak{p} \in S \Big\}.$$

(b) *Define*

$$\mathring{B}(\mathfrak{a}, \mu_1, \ldots, \mu_t) := \Big\{ f \in \mathfrak{a} \;\Big|\; |f|_\mathfrak{p} < \max_{i=1,\ldots,t} |\mu_i|_\mathfrak{p} \text{ for all } \mathfrak{p} \in S \Big\}.$$

(c) *Define*

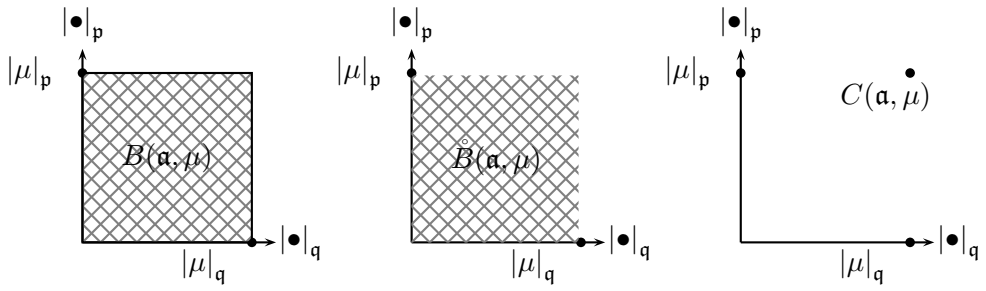
$$C(\mathfrak{a}, \mu_1, \ldots, \mu_t) := \Big\{ f \in \mathfrak{a} \;\Big|\; |f|_\mathfrak{p} = \max_{i=1,\ldots,t} |\mu_i|_\mathfrak{p} \text{ for all } \mathfrak{p} \in S \Big\}.$$

Note that $B(\mathfrak{a}, \mu_1, \ldots, \mu_t) = B(\mathfrak{a}, (t_\mathfrak{p})_{\mathfrak{p}\in S})$ with $t_\mathfrak{p} = -\min_{i=1,\ldots,t} \nu_\mathfrak{p}(\mu_i)$, $\mathfrak{p} \in S$.

These sets can best be interpreted geometrically. Consider the *absolute space* $A_K := \mathbb{R}^S_{\geq 0}$ and the absolute map

$$a_K : K \to A_K, \qquad f \mapsto (|f|_\mathfrak{p})_{\mathfrak{p}\in S}.$$

Denote the $\mathfrak{p}$-axis by $x_\mathfrak{p}$. Then $B(\mathfrak{a}, \mu)$ is the set of all elements in $\mathfrak{a}$ whose images under a_K lie in the volume bounded by $x_\mathfrak{p} \leq |\mu|_\mathfrak{p}$. Moreover, $\mathring{B}(\mathfrak{a}, \mu)$ is the set of all elements in $\mathfrak{a}$ whose images under a_K lie in the volume bounded by $x_\mathfrak{p} < |\mu|_\mathfrak{p}$. Finally, $C(\mathfrak{a}, \mu)$ is the set of all elements in $\mathfrak{a}$ whose images under a_K lie exactly on the corner of the volume bounded by $x_\mathfrak{p} \leq |\mu_\mathfrak{p}|$ that lie on no axis:



Because of these pictures, the terms B for *box*, $\mathring{B}$ for *open box* and C for *corner* where chosen. These sets will be extensively needed in the next sections, to describe different types of minima.

3.2 Minima of Ideals

In this section, we want to define different kinds of minima and investigate their structure. Most of these results and definitions can be found, for example, in [PLRMH85, HPLR85, HPLR87, HMPLR87].

Fix an ideal $\mathfrak{a} \in \mathrm{Id}(\mathcal{O})$. We begin by defining three kinds of minima. A priori, it is not clear that they exist.

Definition 3.2.1. *Let $\mu \in \mathfrak{a} \setminus \{0\}$.*

(a) *We say that μ is a* minimum of type (a) *of $\mathfrak{a}$ if every $f \in \mathfrak{a} \setminus \{0\}$ with $|f|_\mathfrak{p} \leq |\mu|_\mathfrak{p}$ for all $\mathfrak{p} \in S$ satisfies $|f|_\mathfrak{p} = |\mu|_\mathfrak{p}$ for some $\mathfrak{p} \in S$, i.e. that*

$$\mathring{B}(\mathfrak{a}, \mu) = \{0\}.$$

(b) *We say that μ is a* minimum of type (b) *of $\mathfrak{a}$ if every $f \in \mathfrak{a} \setminus \{0\}$ with $|f|_\mathfrak{p} \leq |\mu|_\mathfrak{p}$ for all $\mathfrak{p} \in S$ satisfies $|f|_\mathfrak{p} = |\mu|_\mathfrak{p}$ for all $\mathfrak{p} \in S$, i.e. that*

$$B(\mathfrak{a}, \mu) = C(\mathfrak{a}, \mu) \cup \{0\}.$$

(c) *We say that μ is a* minimum of type (c) *of $\mathfrak{a}$ if every $f \in \mathfrak{a} \setminus \{0\}$ with $|f|_\mathfrak{p} \leq |\mu|_\mathfrak{p}$ for all $\mathfrak{p} \in S$ satisfies $\frac{\mu}{f} \in k^*$, i.e. that*

$$B(\mathfrak{a}, \mu) = k^* \mu \cup \{0\}.$$

In [HMPLR87, HPLR85] these definitions are made for $\mathfrak{a} = \mathcal{O}$. There, the name *comma* is used for a minimum of type (c), *extremal point* (*point extrémal*) for a minimum of type (b) and *edge* (*arête*) for a minimum of type (a).

Clearly, every minimum of type (c) is also of type (b), and every minimum of type (b) is also of type (a). Minima of type (a) will not be of interest in the next chapter, but will appear again in Section 6.3.

One motivation of looking at minima is the fact that every unit is a minimum of $\mathcal{O}$:

Example 3.2.2. If $\mathfrak{a} = \mathcal{O}$, then every unit $u \in \mathcal{O}^*$ is a minimum of type (a), (b) and (c). (See also [HMPLR87, p. 17, Proposition 2].) This follows from the Product Formula.

Therefore, as finding units is hard in general, but finding minima is easier, the general idea is to search for minima and find the units among them.

Remarks 3.2.3.

(a) Note that if $f \in K^*$ and $g \in k^*$, then $|fg|_{\mathfrak{p}} = |f|_{\mathfrak{p}}$ for every $\mathfrak{p} \in \mathcal{P}_K$. Hence, if f is contained in B, $\mathring{B}$ or C, then so is gf.

(b) In the case of function fields, an element $\mu \in \mathfrak{a} \setminus \{0\}$ is a minimum of type (c) if, and only if, $\dim_k B(\mathfrak{a}, \mu) = 1$:

As we always have $\mu \in B(\mathfrak{a}, \mu)$, we also have $(k^* \cup \{0\})\mu = k\mu \subseteq B(\mathfrak{a}, \mu)$, whence $\dim_k B(\mathfrak{a}, \mu) \geq 1$. Now $\dim_k B(\mathfrak{a}, \mu) = 1$ if, and only if, no other element of $\mathfrak{a}$ except the ones in $k^*\mu \cup \{0\}$ lies inside $B(\mathfrak{a}, \mu)$.

We denote by $\mathcal{A}(\mathfrak{a})$ the set of minima of type (a) of $\mathfrak{a}$, by $\mathcal{E}(\mathfrak{a})$ the set of minima of type (b) of $\mathfrak{a}$, and by $\mathcal{C}(\mathfrak{a})$ the set of minima of type (c) of $\mathfrak{a}$. In any case, we have

$$\mathcal{C}(\mathfrak{a}) \subseteq \mathcal{E}(\mathfrak{a}) \subseteq \mathcal{A}(\mathfrak{a}).$$

At the moment, these are sets without any structure. We will later add a relation to them, turning them into undirected graphs.

Remark 3.2.4. In the case of number fields, one has that minima of type (a) are already minima of type (b), i.e. $\mathcal{A}(\mathfrak{a}) = \mathcal{E}(\mathfrak{a})$, as is shown in [HMPLR87, p. 18, Remarque 1 after Proposition 5] and [AO82, p. 285, (8)]. The argument shows that we always have

$$B(\mathfrak{a}, \mu) = \mathring{B}(\mathfrak{a}, \mu) \cup C(\mathfrak{a}, \mu)$$

in the number field case.

In the case of function fields, this is not true in general, as the example on page 19 in [HMPLR87] shows.

The following proposition sums up several important properties:

Proposition 3.2.5.

(a) *[HMPLR87, p. 18, Proposition 5] If any of the places in S has degree one, $\mathcal{E}(\mathfrak{a}) = \mathcal{C}(\mathfrak{a})$.*

(b) *[HMPLR87, p. 17, Proposition 3] The unit group $\mathcal{O}^*$ acts on $\mathcal{C}(\mathfrak{a})$, $\mathcal{E}(\mathfrak{a})$ and $\mathcal{A}(\mathfrak{a})$ by multiplication.*

(c) *More generally, if $f \in K^*$ and $\mu \in \mathcal{C}(\mathfrak{a})$ (or $\mathcal{E}(\mathfrak{a})$ or $\mathcal{A}(\mathfrak{a})$), then $f\mu \in \mathcal{C}(f\mathfrak{a})$ (or $\mathcal{E}(f\mathfrak{a})$ or $\mathcal{A}(f\mathfrak{a})$).*

(d) *If $\mathfrak{a} = (f)$ for some $f \in K^*$, then $f \in \mathcal{C}(\mathfrak{a})$.*

Proof.

(a) If K is a number field, having an infinite place of degree one means that there exists a real embedding. But then, if $|f|_{\mathfrak{p}} = |g|_{\mathfrak{p}}$ for $\mathfrak{p} \in S$ corresponding to a real embedding, we get $f = \pm g$, i.e. $f = ug$ with $u \in k^*$.

If K is a function field, $\mathfrak{p} \in S$ has degree one and $\mu \in \mathcal{E}(\mathfrak{a})$, then $L(\operatorname{div}(\mathfrak{a}) - \sum_{\mathfrak{q} \in S} \nu_{\mathfrak{q}}(\mu)\mathfrak{q}) = B(\mathfrak{a}, \mu) = C(\mathfrak{a}, \mu) \cup \{0\}$, whence $L(\operatorname{div}(\mathfrak{a}) - \sum_{\mathfrak{q} \in S} \nu_{\mathfrak{q}}(\mu)\mathfrak{q} - \mathfrak{p}) = \{0\}$. But, by Corollary 3.1.1 (d), the dimensions of the two Riemann-Roch spaces differ at most by $\deg \mathfrak{p} = 1$, whence the dimension of $B(\mathfrak{a}, \mu)$ must have been 1, which, by Remark 3.2.3 (b), means $\mu \in \mathcal{C}(\mathfrak{a})$.

(b) Follows from (c), as $u\mathfrak{a} = \mathfrak{a}$ for all $u \in \mathcal{O}^*$.

(c) As the $\nu_{\mathfrak{p}}$'s are group morphisms,

$$f \cdot B(\mathfrak{a}, \mu) = B(f\mathfrak{a}, f\mu), \qquad f \cdot \mathring{B}(\mathfrak{a}, \mu) = \mathring{B}(f\mathfrak{a}, f\mu)$$
$$\text{and} \qquad f \cdot C(\mathfrak{a}, \mu) = C(f\mathfrak{a}, f\mu).$$

(d) Note that $(f) = f\mathcal{O}$, whence the proof of (d) follows from (c) with Example 3.2.2. □

Denote by $[\mathcal{A}(\mathfrak{a}) : \mathcal{O}^*]$, $[\mathcal{E}(\mathfrak{a}) : \mathcal{O}^*]$ and $[\mathcal{C}(\mathfrak{a}) : \mathcal{O}^*]$ the number of orbits (possibly infinite) of the elements in $\mathcal{A}(\mathfrak{a})$, $\mathcal{E}(\mathfrak{a})$ and $\mathcal{C}(\mathfrak{a})$, respectively, under the action of $\mathcal{O}^*$. We then have the following finiteness result:

Theorem 3.2.6. *If $|k^*| < \infty$, then $[\mathcal{A}(\mathfrak{a}) : \mathcal{O}^*]$ and $[\mathcal{E}(\mathfrak{a}) : \mathcal{O}^*]$ are finite. In any case, $[\mathcal{C}(\mathfrak{a}) : \mathcal{O}^*]$ is finite.*

In the case $\mathfrak{a} = \mathcal{O}$, this was shown in [HMPLR87, p. 20, Théorème 4 and its Corollaire].

Proof. The requirement $|k^*| < \infty$ ensures that K is a global field. In global fields, the number of conjugacy classes of elements in $\mathfrak{a}$ of bounded norm are finite.

Now the condition $\mathring{B}(\mathfrak{a}, \mu) = \{0\}$ is satisfied if $-\sum_{\mathfrak{p} \in S} \nu_{\mathfrak{p}}(\mu) \deg \mathfrak{p}$ can be bounded in terms of $\mathfrak{a}$ (for function fields, using Riemann's Inequality, Proposition 3.1.1 (c), and for number fields, using Minkowski's Lattice Point Theorem). In the case of number fields, $e^{-\sum_{\mathfrak{p} \in S} \nu_{\mathfrak{p}}(\mu) \deg \mathfrak{p}}$ equals the absolute value of the norm of μ, whence the number of different norms of elements in $\mathcal{A}(\mathfrak{a})$ is finite in this case.

In the case of function fields, note that $-\sum_{\mathfrak{p} \in S} \nu_{\mathfrak{p}}(\mu) \deg \mathfrak{p}$ equals the degree of the norm of μ. Now, as the field of constants is finite, there are only finitely many polynomials in $k[x]$ of bounded degree, whence the number of different norms of elements in $\mathcal{A}(\mathfrak{a})$ is also finite in this case.

As $\mathcal{C}(\mathfrak{a}) \subseteq \mathcal{E}(\mathfrak{a}) \subseteq \mathcal{A}(\mathfrak{a})$, the finiteness of $[\mathcal{A}(\mathfrak{a}) : \mathcal{O}^*]$ implies the finiteness of $[\mathcal{E}(\mathfrak{a}) : \mathcal{O}^*]$ and $[\mathcal{C}(\mathfrak{a}) : \mathcal{O}^*]$.

Now we drop the assumption that K is global, and assume that K is any function field and let $S' = S \setminus \{\mathfrak{q}\}$ for some $\mathfrak{q} \in S$. Consider the map $\varphi : K^* \to \mathbb{Z}^{S'}$, $\mu \mapsto (\nu_{\mathfrak{p}}(\mu))_{\mathfrak{p} \in S'}$. Note that $\Lambda := \varphi(\mathcal{O}^*)$ is a full lattice in $\mathbb{Z}^{S'}$ by our general assumption in Section 1.1, whence $\mathbb{Z}^{S'}/\Lambda$ is finite. Now, for $\mu, \mu' \in \mathcal{C}(\mathfrak{a})$, assume that $\varphi(\mu) + \Lambda = \varphi(\mu') + \Lambda$; this is equivalent to $\varphi(\mu') = \varphi(\varepsilon\mu)$ for some $\varepsilon \in \mathcal{O}^*$, i.e. $\varphi(\mu'\mu^{-1}\varepsilon^{-1}) = 0$. If $\nu_{\mathfrak{q}}(\mu'\mu^{-1}\varepsilon^{-1}) \leq 0$, we get $\mu\varepsilon \in B(\mathfrak{a}, \mu') = \mu' k$, i.e. $\mu'\mu^{-1}\varepsilon^{-1} \in k^*$. Conversely, if $\nu_{\mathfrak{q}}(\mu'\mu^{-1}\varepsilon^{-1}) \geq 0$, we get $\mu'\varepsilon^{-1} \in B(\mathfrak{a}, \mu) = \mu k$, i.e. $\mu'\mu^{-1}\varepsilon^{-1} \in k^*$. In both cases, we get that μ and μ' are conjugated under $\mathcal{O}^*$. This means that $\overline{\varphi} : \mathcal{C}(\mathfrak{a})/\mathcal{O}^* \to \mathbb{Z}^{S'}/\Lambda$ is injective and that $|\mathcal{C}(\mathfrak{a})/\mathcal{O}^*| = [\mathcal{C}(\mathfrak{a}) : \mathcal{O}^*] < \infty$. □

Finally, we close this section by showing that minima of type (a) and (b) always exist.

Lemma 3.2.7. *Let $\mu \in \mathfrak{a} \setminus \{0\}$. Then there exists a $\mu' \in \mathcal{E}(\mathfrak{a}) \cap B(\mathfrak{a}, \mu)$.*

Proof. If K is a number field, there are finitely many elements in $X := B(\mathfrak{a}, \mu) \setminus \{0\}$. To see the claim, set $X_0 := X$. If $X_0 \subsetneqq \mathcal{E}(\mathfrak{a})$, there exists an $x_0 \in X_0 \setminus \mathcal{E}(\mathfrak{a})$, i.e. $B(\mathfrak{a}, x_0) \setminus C(\mathfrak{a}, x_0) \neq \{0\}$. Select $x_0' \in B(\mathfrak{a}, x_0) \setminus (C(\mathfrak{a}, x_0) \cup \{0\})$, and define $X_1 := B(\mathfrak{a}, x_0') \setminus \{0\}$. Clearly $X_1 \subsetneqq X_0$. Continuing inductively, we reach a point when we must have that $X_i \subseteq \mathcal{E}(\mathfrak{a})$, as all X_j's are finite and non-empty.

If K is a function field, we proceed slightly different. Choose $\mu_0 \in B(\mathfrak{a}, \mu) \setminus \{0\}$. If $\mu_0 \notin \mathcal{E}(\mathfrak{a})$, there must exist an element $\mu_1 \in B(\mathfrak{a}, \mu) \setminus (C(\mathfrak{a}, \mu) \cup \{0\})$. As $|\mu_1|_\mathfrak{p} < |\mu_0|_\mathfrak{p}$ for some $\mathfrak{p} \in S$ and $|\mu_1|_\mathfrak{q} \leq |\mu_0|_\mathfrak{q}$ for all $\mathfrak{q} \in S$, the dimension of $B(\mathfrak{a}, \mu_1)$ must be less than the dimension of $B(\mathfrak{a}, \mu_0)$ by Corollary 3.1.1 (d), as $B(\mathfrak{a}, \mu) = L(\operatorname{div}(\mathfrak{a}) - \sum_{\mathfrak{q} \in S} \nu_\mathfrak{q}(\mu)\mathfrak{q})$. Therefore, if we continue inductively, some μ_i must be in $\mathcal{E}(\mathfrak{a})$. □

Corollary 3.2.8. *We have $\mathcal{A}(\mathfrak{a}) \neq \emptyset$ and $\mathcal{E}(\mathfrak{a}) \neq \emptyset$.*

Proof. As $\mathfrak{a} \neq 0$, there exists a $\mu \in \mathfrak{a} \setminus \{0\}$. By Lemma 3.2.7, an $\mu' \in B(\mathfrak{a}, \mu) \cap \mathcal{E}(\mathfrak{a})$ exists, whence $\mathcal{E}(\mathfrak{a}) \neq \emptyset$. As $\mathcal{E}(\mathfrak{a}) \subseteq \mathcal{A}(\mathfrak{a})$, the claim follows. □

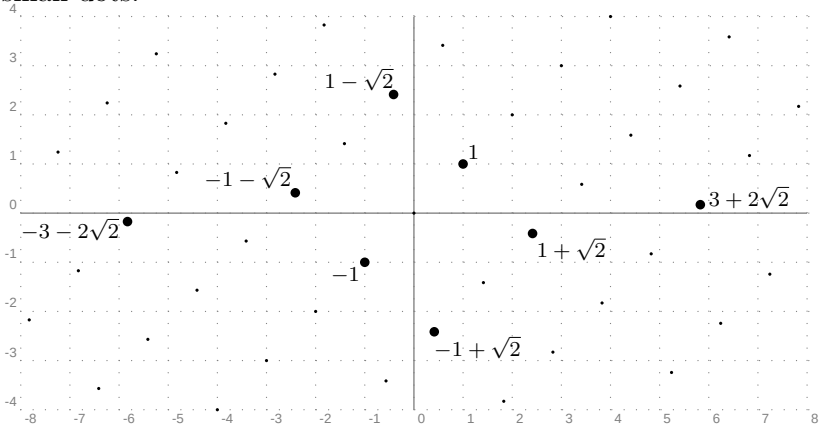
3.3 The Neighbor Relation

In this section, we want to define the neighbor relation on $\mathcal{C}(\mathfrak{a})$, $\mathcal{E}(\mathfrak{a})$ and $\mathcal{A}(\mathfrak{a})$. We will discuss the existence of neighbors and show the connection to compute non-trivial units of $\mathcal{O}$. Finally we will present a theorem which, in the function field case, gives more concrete information on neighbors than just their existence; this is important for computational reasons.

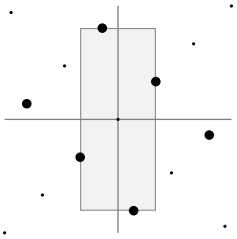
Definition 3.3.1. *If $\mu, \mu' \in \mathcal{A}(\mathfrak{a})$ (or $\mathcal{E}(\mathfrak{a})$ or $\mathcal{C}(\mathfrak{a})$), we say that μ and μ' are* neighbors *of type (a) (or type (b) or type (c)) if $\mathring{B}(\mathfrak{a}, \mu, \mu') = 0$.*

Example 3.3.2. Consider $K = \mathbb{Q}(\sqrt{2})$ and $\mathfrak{a} = \mathcal{O} = \mathbb{Z}[\sqrt{2}]$. By Proposition 3.2.5 (a) and Remark 3.2.4, we have $\mathcal{A}(\mathfrak{a}) = \mathcal{E}(\mathfrak{a}) = \mathcal{C}(\mathfrak{a})$.

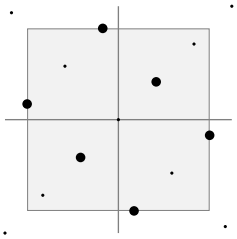
The following picture depicts the image of $\mathfrak{a}$ under the Minkowski embedding of K into $\mathbb{R}^2$ by $M : K \to \mathbb{R}^2$, $f \mapsto (\sigma_1(f), \sigma_2(f))$, where $\sigma_1, \sigma_2 : K \to \mathbb{R}$ are the two distinct embeddings of K into $\mathbb{R}$. The minima are drawn with big dots and are labeled, the elements of $\mathfrak{a}$ which are no minima are drawn with small dots:



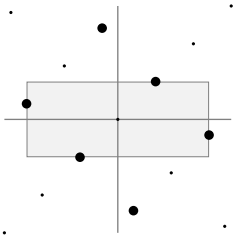
Then we have:



1 and $1-\sqrt{2}$ are neighbors;



$1-\sqrt{2}$ and $1+\sqrt{2}$ are *not* neighbors;



1 and $1+\sqrt{2}$ are neighbors.

Remark 3.3.3.

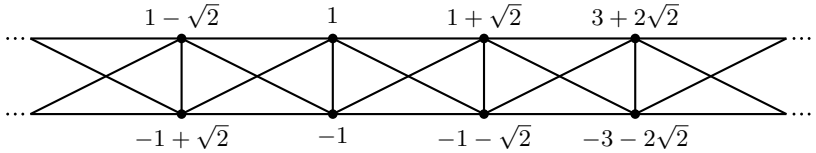
(a) Note that the neighbor relation is symmetric and reflexive.

(b) If $\mu, \mu' \in \mathcal{A}(\mathfrak{a})$ and $f \in K^*$, then μ, μ' are neighbors if, and only if, $f\mu, f\mu' \in \mathcal{A}(f\mathfrak{a})$ are neighbors.

Proof. The statement (a) is clear. Statement (b) follows directly from the fact that $f \cdot \mathring{B}(\mathfrak{a}, \mu, \mu') = \mathring{B}(f\mathfrak{a}, f\mu, f\mu')$. □

Hence, the neighbor relation on $\mathcal{A}(\mathfrak{a})$ (or $\mathcal{E}(\mathfrak{a})$ or $\mathcal{C}(\mathfrak{a})$) is compatible with the action of $\mathcal{O}^*$. We denote by $\mathscr{A}(\mathfrak{a})$, $\mathscr{E}(\mathfrak{a})$ and $\mathscr{C}(\mathfrak{a})$ the graphs of the neighbor relation, i.e. the graphs whose vertices are the elements of $\mathcal{A}(\mathfrak{a})$, $\mathcal{E}(\mathfrak{a})$ and $\mathcal{C}(\mathfrak{a})$, respectively, and there are edges between two elements μ, μ' if, and only if, they are neighbors.

Example 3.3.4. For $K = \mathbb{Q}(\sqrt{2})$ and $\mathfrak{a} = \mathcal{O} = \mathbb{Z}[\sqrt{2}]$, the graph $\mathscr{A}(\mathfrak{a}) = \mathscr{E}(\mathfrak{a}) = \mathscr{C}(\mathfrak{a})$ looks as follows:



Note that the loops at every vertex were omitted.

Define the *quotient graphs* $\overline{\mathscr{A}}(\mathfrak{a})$, $\overline{\mathscr{E}}(\mathfrak{a})$ and $\overline{\mathscr{C}}(\mathfrak{a})$ of $\mathscr{A}(\mathfrak{a})$, $\mathscr{E}(\mathfrak{a})$ and $\mathscr{C}(\mathfrak{a})$, respectively, under the action of $\mathcal{O}^*$ as in [HPLR87, p. 292, Section 2], i.e. let the vertices be the orbits under the action of $\mathcal{O}^*$ and put edges between two orbits F, G if, and only if, there exists elements $\mu \in F$, $\mu' \in G$ such that μ, μ' are neighbors.

Example 3.3.5. For $K = \mathbb{Q}(\sqrt{2})$ and $\mathfrak{a} = \mathcal{O} = \mathbb{Z}[\sqrt{2}]$, one quickly checks that $\mathcal{O}^*$ equals the set of minima, whence each of the quotient graphs $\overline{\mathscr{A}}(\mathfrak{a})$, $\overline{\mathscr{E}}(\mathfrak{a})$ and $\overline{\mathscr{C}}(\mathfrak{a})$ consists of exactly one vertex.

We want to state an important result which allows to describe the neighbor structure for type (a) and type (b) minima without knowing $\mathfrak{a}$, but only the set $\mathcal{A}(\mathfrak{a})$ respectively $\mathcal{E}(\mathfrak{a})$:

Lemma 3.3.6.

(a) *Let $\mu, \mu' \in \mathcal{A}(\mathfrak{a})$ be two type (a) minima. Then μ and μ' are neighbors if, and only if,*
$$\mathring{B}(\mathfrak{a}, \mu, \mu') \cap \mathcal{A}(\mathfrak{a}) = \emptyset.$$

(b) *Let $\mu, \mu' \in \mathcal{E}(\mathfrak{a})$ be two type (b) minima. Then μ and μ' are neighbors if, and only if,*
$$\mathring{B}(\mathfrak{a}, \mu, \mu') \cap \mathcal{E}(\mathfrak{a}) = \emptyset.$$

Proof. Let $\mu, \mu' \in \mathcal{A}(\mathfrak{a}) \supseteq \mathcal{E}(\mathfrak{a})$. If μ and μ' are not neighbors, i.e. if $\mathring{B}(\mathfrak{a}, \mu, \mu') \neq \{0\}$, there exists a $\mu'' \in \mathring{B}(\mathfrak{a}, \mu, \mu') \setminus \{0\}$. By Lemma 3.2.7, there exists an $\mu''' \in B(\mathfrak{a}, \mu'') \cap \mathcal{E}(\mathfrak{a})$, whence $\mu'' \in \mathring{B}(\mathfrak{a}, \mu, \mu') \cap \mathcal{E}(\mathfrak{a}) \subseteq \mathring{B}(\mathfrak{a}, \mu, \mu') \cap \mathcal{A}(\mathfrak{a})$, so these sets are not empty. □

Before studying the existence of neighbors, note that in the case $|S| = 1$, the neighbor relation is not interesting:

Proposition 3.3.7. *Assume that $S = \{\mathfrak{p}\}$. Then there are two cases:*

(i) *We have $\mathcal{C}(\mathfrak{a}) = \mathcal{E}(\mathfrak{a}) = \mathcal{A}(\mathfrak{a}) = k^*\mu$ for some $\mu \in \mathfrak{a}$;*

(ii) *We have $\mathcal{C}(\mathfrak{a}) = \emptyset$ and $\mathcal{E}(\mathfrak{a}) = \mathcal{A}(\mathfrak{a})$, and both have strictly more than $|k^*|$ elements (in the case that k^* is finite) and all elements have the same valuation $\nu_\mathfrak{p}(\bullet)$.*

Proof. As $\nu_\mathfrak{p}(f) \leq -\frac{\deg \operatorname{div}(\mathfrak{a})}{\deg \mathfrak{p}}$ for every $f \in \mathfrak{a}$, $f \neq 0$, we have that $m := \max\{\nu_\mathfrak{p}(f) \mid f \in \mathfrak{a}, f \neq 0\}$ exists. Choose any $\mu \in \mathfrak{a} \setminus \{0\}$ with $\nu_\mathfrak{p}(\mu) = m$. We first claim that
$$\mathcal{A}(\mathfrak{a}) = \mathcal{E}(\mathfrak{a}) = \{f \in \mathfrak{a} \setminus \{0\} \mid \nu_\mathfrak{p}(f) = m\}.$$
For that, if $f \in \mathcal{A}(\mathfrak{a})$ with $\nu_\mathfrak{p}(f) < m$, then $\mu \in \mathring{B}(\mathfrak{a}, f)$, a contradiction. Hence, $\nu_\mathfrak{p}(f) = m$. Conversely, if $\nu_\mathfrak{p}(f) = m$, then $\mathring{B}(\mathfrak{a}, f) = \{h \in \mathfrak{a} \mid$

$\nu_{\mathfrak{p}}(h) > m\} = \{0\}$. As $|S| = 1$, we have $\mathring{B}(\mathfrak{a}, f) \cup C(\mathfrak{a}, f) = B(\mathfrak{a}, f)$, whence $f \in \mathcal{E}(\mathfrak{a})$.

Note that $B(\mathfrak{a}, \mu) = \mathcal{E}(\mathfrak{a}) \cup \{0\}$. Hence, if $\mathcal{E}(\mathfrak{a}) = k^*\mu$, then $B(\mathfrak{a}, \mu) = k^*\mu \cup \{0\}$, whence $\mathcal{E}(\mathfrak{a}) = \mathcal{C}(\mathfrak{a})$. Otherwise, there exists an $f \in \mathcal{E}(\mathfrak{a}) \setminus k^*\mu$, whence $|\mathcal{E}(\mathfrak{a})| > |k^*|$ if k^* is finite, and we get that $\mathcal{C}(\mathfrak{a})$ must be empty. □

From now on, we will concentrate on the case $|S| > 1$. Using Minkowski's Lemma or Riemann's Inequality, one gets the following result on the existence of neighbors:

Proposition 3.3.8. *Assume that $|S| > 1$ and let $\mathfrak{p} \in S$.*

(i) *Let $\mu \in \mathcal{A}(\mathfrak{a})$ be a type (a) minimum and $\mathfrak{p} \in S$. Then there exists a type (a) minimum $\mu' \in \mathcal{A}(\mathfrak{a})$ with $|\mu'|_{\mathfrak{p}} > |\mu|_{\mathfrak{p}}$ and $|\mu'|_{\mathfrak{q}} < |\mu|_{\mathfrak{q}}$ for all $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$.*

(ii) *Let $\mu \in \mathcal{E}(\mathfrak{a})$ be a type (b) minimum and $\mathfrak{p} \in S$. Then there exists a type (b) minimum $\mu' \in \mathcal{E}(\mathfrak{a})$ which is a neighbor of μ with $|\mu'|_{\mathfrak{p}} > |\mu|_{\mathfrak{p}}$ and $|\mu'|_{\mathfrak{q}} < |\mu|_{\mathfrak{q}}$ for all $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$.*

Unfortunately, we do not have a similar result for type (c) minima. Except in the case that $\deg \mathfrak{q} = 1$ for some $\mathfrak{q} \in S$; then, by Proposition 3.2.5 (a), $\mathcal{C}(\mathfrak{a}) = \mathcal{E}(\mathfrak{a})$.

Also, note that in (i), it might be that no neighbor μ' with the required properties exist.

Proof.

(i) Let $t_{\mathfrak{q}} = -\nu_{\mathfrak{q}}(\mu)$, $\mathfrak{q} \in S$. Then $\mathring{B}(\mathfrak{a}, \mu) = \mathring{B}(\mathfrak{a}, (t_{\mathfrak{q}})_{\mathfrak{q} \in S})$. As μ is a minimum, $\mathring{B}(\mathfrak{a}, \mu) = \{0\}$. By increasing $t_{\mathfrak{p}}$, the size of the box $\mathring{B}(\mathfrak{a}, (t_{\mathfrak{q}})_{\mathfrak{q} \in S})$ increases.

In the case of function fields, by Riemann's Inequality (Corollary 3.1.1 (c)), we get that $\mathring{B}(\mathfrak{a}, (\hat{t}_{\mathfrak{q}})_{\mathfrak{q} \in S}) \neq \{0\}$ with $\hat{t}_{\mathfrak{q}} = t_{\mathfrak{q}}$ for $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$ if $\hat{t}_{\mathfrak{p}}$ is large enough. As $\hat{t}_{\mathfrak{p}}$ is integer valued here, there exists a smallest one such that this is the case. Set $t_{\mathfrak{p}} := \hat{t}_{\mathfrak{p}} - 1$.

Similarly, in the case of number fields, the volume of the parallelepiped $\{(x_{\mathfrak{q}})_{\mathfrak{q} \in S} \in \mathbb{R}^S \mid |x_{\mathfrak{q}}| < q^{\hat{t}_{\mathfrak{q}} \deg \mathfrak{q}} \text{ for } \mathfrak{q} \in S\}$ with $\hat{t}_{\mathfrak{q}} = t_{\mathfrak{q}}$ for $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$ is increasing if $\hat{t}_{\mathfrak{p}}$ is increasing, whence eventually, a non-zero element of the lattice $\mathfrak{a}$ will be contained in it. The infimum $t_{\mathfrak{p}}$ of all such $\hat{t}_{\mathfrak{p}}$ such that $\mathring{B}(\mathfrak{a}, (\hat{t}_{\mathfrak{q}})_{\mathfrak{q} \in S}) \neq \{0\}$ exists and, as the lattice is discrete,

the elements inside these sets which have minimal $|\bullet|_\mathfrak{p}$ satisfy $|\bullet|_\mathfrak{p} = q^{t_\mathfrak{p} \deg \mathfrak{p}}$.

In any case, all elements $f \in \mathring{B}(\mathfrak{a}, (t_\mathfrak{q})_{\mathfrak{q}\in S}) \setminus \{0\}$ with minimal $|f|_\mathfrak{p}$ will satisfy $|f|_\mathfrak{p} = q^{t_\mathfrak{p} \cdot \deg \mathfrak{p}} > |\mu|_\mathfrak{p}$ and $|f|_\mathfrak{q} < |\mu|_\mathfrak{q}$ for all $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$. In particular, all these elements will be in $\mathcal{A}(\mathfrak{a})$ and all are neighbors to μ.

(ii) We proceed similarly as in (i). The main difference is that not necessarily every element in $\mathring{B}(\mathfrak{a}, (\hat{t}_\mathfrak{q})_{\mathfrak{q}\in S}) \setminus \{0\}$ with minimal $|\bullet|_\mathfrak{p}$ and with large enough $\hat{t}_\mathfrak{p}$ (as in (i)) is a type (b) minimum. However, we can pick a type (b) minimum out of the set of these elements by Lemma 3.2.7. □

Before refining this result, we want to give a first result on units which directly leads to an algorithm for finding non-trivial units:

Proposition 3.3.9. *[HMPLR87, p. 22, Théorème 5]*

(a) *If $[\mathcal{E}(\mathfrak{a}) : \mathcal{O}^*] < \infty$ and $|S| > 1$, there exists a family of units $\varepsilon_\mathfrak{p} \in \mathcal{O}^*$, $\mathfrak{p} \in S$, such that $|\varepsilon_\mathfrak{p}|_\mathfrak{p} > 1$ and $|\varepsilon_\mathfrak{p}|_\mathfrak{q} < 1$ for all $\mathfrak{p}, \mathfrak{q} \in S$, $\mathfrak{p} \neq \mathfrak{q}$.*

(b) *If $(\varepsilon_\mathfrak{p})_{\mathfrak{p}\in S}$ is a indexed family of units as in (a), then any proper subfamily is free, i.e. if $N \subsetneqq \{\varepsilon_\mathfrak{p} \mid \mathfrak{p} \in S\}$, then $\langle N \rangle$ is a free abelian group of rank $|N|$.*

Note that for global fields, the hypothesis $[\mathcal{E}(\mathfrak{a}) : \mathcal{O}^*] < \infty$ of part (a) is satisfied by Theorem 3.2.6.

Proof.

(a) Take x_0 as an arbitrary minimum in $\mathcal{E}(\mathfrak{a})$.

Fix $\mathfrak{p} \in S$ and take as x_{n+1} one arbitrary neighbor of x_n in $\mathcal{E}(\mathfrak{a})$ with $|x_{n+1}|_\mathfrak{p} > |x_n|_\mathfrak{p}$ and $|x_{n+1}|_\mathfrak{q} < |x_n|_\mathfrak{q}$, $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$, which exists due to Proposition 3.3.8 (b).

As $[\mathcal{E}(\mathfrak{a}) : \mathcal{O}^*] < \infty$, there will exist two indices $0 \leq i < j$ such that $\varepsilon_\mathfrak{p} := \frac{x_i}{x_j} \in \mathcal{O}^*$ and, by construction, we have $\nu_\mathfrak{p}(\varepsilon_\mathfrak{p}) = \nu_\mathfrak{p}(x_j) - \nu_\mathfrak{p}(x_i) < 0$ and $\nu_\mathfrak{q}(\varepsilon_\mathfrak{p}) = \nu_\mathfrak{q}(x_j) - \nu_\mathfrak{q}(x_i) > 0$ for all $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$.

(b) It suffices to show this for $|N| = |S| - 1$, say $N = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ with $n = |S| - 1$. Consider the matrix $A := (a_{ij})_{ij} \in \mathbb{R}^{n\times n}$ with $a_{ij} = \nu_{\mathfrak{p}_j}(\varepsilon_{\mathfrak{p}_i})$. Then we have $a_{ii} < 0$ and $a_{ij} > 0$ for $i \neq j$, and we know $\sum_{\substack{j=1 \\ j\neq i}}^{n} a_{ij} < -a_{ii}$, $1 \leq i \leq k$. By a standard result, $\det A \neq 0$, which

implies that the rows are linearly independent. As the row-space of A is the image of $\langle \varepsilon_{\mathfrak{p}_1}, \dots, \varepsilon_{\mathfrak{p}_n} \rangle$ under the homomorphism $\mathcal{O}^* \to \mathbb{R}^n$, $\varepsilon \mapsto (\nu_{\mathfrak{p}_1}(\varepsilon), \dots, \nu_{\mathfrak{p}_n}(\varepsilon))$, this implies the claim. □

Remark 3.3.10. Using the proof of part (a) of this theorem, one can easily construct an algorithm to find a subgroup of $\mathcal{O}^*$ of finite index, if a type (b) minimum μ is given:

for every $\mathfrak{p} \in S$, construct a chain of minima starting at μ in direction $\mathfrak{p}$ (in the sense of Proposition 3.3.8 (a)). For every new element in the chain, check whether the quotient of any previous element in the chain by the new element is a unit. If it is, we have found $\varepsilon_{\mathfrak{p}}$ as desired; otherwise, continue.

In the case of type (b) minima, we get a more sophisticated result than Proposition 3.3.8. We first give the result for function fields:

Theorem 3.3.11. *Let K be a function field and assume that $|S| > 1$. Let $\mu \in \mathcal{E}(\mathfrak{a})$ be a type (b) minimum and $\mathfrak{p} \in S$. Then there exists a type (b) minimum $\mu' \in \mathcal{E}(\mathfrak{a})$ with $|\mu'|_{\mathfrak{p}} > |\mu|_{\mathfrak{p}}$ and $|\mu'|_{\mathfrak{q}} < |\mu|_{\mathfrak{q}}$ for all $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$, which satisfies the following properties:*

(i) *We have that μ and μ' are neighbors.*

(ii) *We have*

$$\nu_{\mathfrak{p}}(\mu) - \nu_{\mathfrak{p}}(\mu') \leq \left\lceil \frac{g + \sum\limits_{\mathfrak{q} \in S \setminus \{\mathfrak{p}\}} \deg \mathfrak{q}}{\deg \mathfrak{p}} \right\rceil, \qquad (*)$$

where g is the genus of the function field.

If $\mathfrak{a}$ is not generated by μ (for example, because $\mathfrak{a}$ is not principal) and if $\deg \mathfrak{p}$ divides $g + \sum\limits_{\mathfrak{q} \in S \setminus \{\mathfrak{p}\}} \deg \mathfrak{q}$, we have a strict inequality.

(iii) *If $\deg \mathfrak{p} = 1$, μ' is a type (c) minimum and it is uniquely (up to constants) determined by the conditions $\mu' \in \mathcal{C}(\mathfrak{a})$, $|\mu'|_{\mathfrak{q}} < |\mu|_{\mathfrak{q}}$ for all $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$ and that $|\mu'|_{\mathfrak{p}}$ is minimal.*

Proof. We have already shown the existence of μ in the proof of Proposition 3.3.8 (b). We will repeat the step of increasing the box in more detail, which allows us to obtain the results.

Let $t_{\mathfrak{q}} := -\nu_{\mathfrak{q}}(\mu)$, $\mathfrak{q} \in S$. We have

$$0 \neq \mu \in B(\mathfrak{a}, \mu) = L\Big(\operatorname{div}(\mathfrak{a}) + \sum_{\mathfrak{q} \in S} t_{\mathfrak{q}} \mathfrak{q}\Big)$$

and, hence, by Corollary 3.1.1 (a), $\deg\left(\operatorname{div}(\mathfrak{a}) + \sum_{\mathfrak{q}\in S} t_{\mathfrak{q}}\mathfrak{q}\right) \geq 0$.

Set $D := \operatorname{div}(\mathfrak{a}) + \sum_{\mathfrak{q}\in S\setminus\{\mathfrak{p}\}}(t_{\mathfrak{q}}-1)\mathfrak{q} + t_{\mathfrak{p}}\mathfrak{p}$. Then $\deg D \geq -\sum_{\mathfrak{q}\in S\setminus\{\mathfrak{p}\}} \deg \mathfrak{q}$ and $L(D) = \{0\}$ as f is a type (b) minimum. Hence, if one considers the ascending sequence

$$L(D) \subseteq L(D+\mathfrak{p}) \subseteq \cdots \subseteq L(D+\ell\mathfrak{p}), \quad \ell \in \mathbb{N},$$

by Riemann's Inequality (Corollary 3.1.1 (b)), we must have $L(D+m\mathfrak{p}) = \{0\}$ and $L(D+(m+1)\mathfrak{p}) \neq \{0\}$ for some m as the degree of the divisor $D+m\mathfrak{p}$ increases with m. Now, as in the proof of Proposition 3.3.8 (b), we can choose a type (b) minimum μ' from $L(D+(m+1)\mathfrak{p})$ as required which, by construction, is a type (b) neighbor of μ.

(a) By Riemann's Inequality, we have $L(D+(m'+1)\mathfrak{p}) \neq \{0\}$ guaranteed if

$$\deg(D+(m'+1)\mathfrak{p}) + 1 - g > 0.$$

Now

$$\begin{aligned} &\deg(D+(m'+1)\mathfrak{p}) + 1 - g \\ =\ &\deg D + (m'+1)\deg\mathfrak{p} + 1 - g \\ \geq\ &-\sum_{\mathfrak{q}\in S\setminus\{\mathfrak{p}\}} \deg\mathfrak{q} + (m'+1)\deg\mathfrak{p} + 1 - g. \end{aligned} \tag{$**$}$$

Now, the last term is ≥ 1 if, and only if,

$$m' \geq \frac{g + \sum_{\mathfrak{q}\in S\setminus\{\mathfrak{p}\}} \deg\mathfrak{q}}{\deg\mathfrak{p}} - 1. \tag{$***$}$$

The smallest such integer m' is given by

$$\left\lceil \frac{g + \sum_{\mathfrak{q}\in S\setminus\{\mathfrak{p}\}} \deg\mathfrak{q}}{\deg\mathfrak{p}} \right\rceil - 1$$

and, hence, as $\nu_i(\mu) - \nu_i(\mu') = m+1$, the inequality from (i) follows.

(b) We have $\deg(\operatorname{div}(\mathfrak{a}) + \sum_{\mathfrak{q}\in S} t_{\mathfrak{q}}\mathfrak{q}) = 0$ if, and only if, $\operatorname{div}(\mathfrak{a}) + \sum_{\mathfrak{q}\in S} t_{\mathfrak{q}}\mathfrak{q} \in \operatorname{Princ}(K)$, by Corollary 3.1.1 (b). If this is the case, $\operatorname{div}(\mathfrak{a}) + \sum_{\mathfrak{q}\in S} t_{\mathfrak{q}}\mathfrak{q} = (f^{-1})$ for some $f \in K^*$. Then $\mathfrak{a} = (f)$ and $\nu_{\mathfrak{q}}(f) = \nu_{\mathfrak{q}}(\mu) = -t_{\mathfrak{q}}$ for all $\mathfrak{q} \in S$. As $f \in \mathcal{C}(\mathfrak{a})$, $\frac{\mu}{f} \in k^*$. Therefore, if $\deg(\operatorname{div}(\mathfrak{a}) + \sum_{\mathfrak{q}\in S} t_{\mathfrak{q}}\mathfrak{q}) = 0$, we have $\mathfrak{a} = (\mu)$.

Next, assume that $\deg\mathfrak{p}$ divides $g + \sum_{\mathfrak{q}\in S\setminus\{\mathfrak{p}\}} \deg\mathfrak{q}$. If $\mathfrak{a} \neq (\mu)$, we have $\deg(\operatorname{div}(\mathfrak{a}) + \sum_{\mathfrak{q}\in S} t_{\mathfrak{q}}\mathfrak{q}) > 0$, whence we have a strict inequality in $(**)$ and, thus, in $(***)$. This completes the proof of (i).

(c) If $\deg \mathfrak{p} = 1$, by Corollary 3.1.1 (d), the dimension of $L(D + \ell\mathfrak{p})$ can increase by at most by one if ℓ increases by one. Hence, we must have $\dim L(D + (m+1)\mathfrak{p}) = 1$. This implies that it contains a unique (up to constants) type (c) minimum. □

For number fields, one has the following result:

Proposition 3.3.12. *[Buc87a, p. 11, Proposition 2.4] Let K be a number field and $\mu, \mu' \in \mathcal{E}(\mathfrak{a})$ two elements which are neighbors. Then, for every $\mathfrak{p} \in S$,*

$$|\mu'|_{\mathfrak{p}} \in \left[\frac{N(\mathfrak{a})}{C_{\mathfrak{a}}^{|S|-1}} |\mu|_{\mathfrak{p}} \left(\prod_{\mathfrak{q} \in S} |\mu|_{\mathfrak{q}} \right)^{|S|-2}, \frac{C_{\mathfrak{a}}}{\prod_{\mathfrak{q} \in S \setminus \{\mathfrak{p}\}} |\mu|_{\mathfrak{q}}} \right].$$

Here, $N(\mathfrak{a})$ denotes the norm of $\mathfrak{a}$, and $C_{\mathfrak{a}} = \left(\frac{2}{\pi}\right)^t N(\mathfrak{a})\sqrt{D}$, where $t = |\{\mathfrak{q} \in S \mid \deg \mathfrak{q} = 2\}|$ is the number of pairwise conjugated complex embeddings of K into $\mathbb{C}$ and D is the discriminant of $\mathcal{O}$. □

One might wonder whether and, if, in which sense, the neighbors of a minimum are unique. If $|S| = 2$, the answer is positive for the case of type (b) minima:

Proposition 3.3.13. *Let $|S| = 2$ and $\mathfrak{p} \in S$, and write $S = \{\mathfrak{p}, \mathfrak{q}\}$. Let $\mu \in \mathcal{E}(\mathfrak{a})$ be any type (b) minimum. Then, by Proposition 3.3.8 (b), there exists a type (b) minimum μ' with $|\mu'|_{\mathfrak{p}} > |\mu|_{\mathfrak{p}}$ and $|\mu'|_{\mathfrak{q}} < |\mu|_{\mathfrak{q}}$, which is a neighbor of μ.*

Then μ' is unique (up to same absolute values $|\bullet|_{\mathfrak{p}}$, $\mathfrak{p} \in S$) and can be characterized as follows:

(1) *We have that μ' is characterized by the conditions that $\mu' \in \mathcal{E}(\mathfrak{a})$ is a neighbor of μ and that $|\mu'|_{\mathfrak{p}} > |\mu|_{\mathfrak{p}}$.*

(2) *We have that μ' is characterized by the conditions that $\mu' \in \mathcal{E}(\mathfrak{a})$ has minimal $|\mu'|_{\mathfrak{p}}$ such that $|\mu'|_{\mathfrak{p}} > |\mu|_{\mathfrak{p}}$.*

Proof. Let $\mu'' \in \mathfrak{a}$ be any type (b) neighbor of μ with $|\mu''|_{\mathfrak{p}} > |\mu|_{\mathfrak{p}}$. We have to show that $|\mu''|_{\mathfrak{r}} = |\mu'|_{\mathfrak{r}}$ for all $\mathfrak{r} \in S$.

If $|\mu''|_{\mathfrak{q}} \geq |\mu|_{\mathfrak{q}}$, we would have $\mu \in B(\mathfrak{a}, \mu'') \setminus C(\mathfrak{a}, \mu'')$, a contradiction. Hence, we must have $|\mu''|_{\mathfrak{q}} < |\mu|_{\mathfrak{q}}$. If $|\mu''|_{\mathfrak{p}} < |\mu'|_{\mathfrak{p}}$, we would have $\mu'' \in \mathring{B}(\mathfrak{a}, \mu, \mu')$, a contradiction; hence, $|\mu''|_{\mathfrak{p}} \geq |\mu'|_{\mathfrak{p}}$. With the same argument, with μ' and μ'' reversed, we get $|\mu''|_{\mathfrak{p}} = |\mu'|_{\mathfrak{p}}$.

Hence, we know $|\mu'|_\mathfrak{p} = |\mu''|_\mathfrak{p}$ and $|\mu'|_\mathfrak{q}, |\mu''|_\mathfrak{q} < |\mu|_\mathfrak{q}$. If $|\mu'|_\mathfrak{q} < |\mu''|_\mathfrak{q}$, we would have $\mu' \in B(\mathfrak{a}, \mu'') \setminus C(\mathfrak{a}, \mu'')$, a contradiction. The same argument, with μ' and μ'' reversed, shows that $|\mu'|_\mathfrak{q} = |\mu''|_\mathfrak{q}$.

Hence, μ' is unique up to absolute values. The above discussion also shows characterization (1), and we are left to show characterization (2).

For characterization (2), let μ'' be any type (b) minimum of $\mathfrak{a}$ with $|\mu''|_\mathfrak{p} > |\mu|_\mathfrak{p}$ such that $|\mu''|_\mathfrak{p}$ is minimal under this condition. Therefore, $|\mu''|_\mathfrak{p} \leq |\mu'|_\mathfrak{p}$. If $|\mu''|_\mathfrak{p} = |\mu'|_\mathfrak{p}$, then we must have that $|\mu''|_\mathfrak{q} = |\mu'|_\mathfrak{q}$ as otherwise one of μ', μ'' is contained in $B(\mathfrak{a}, \bullet) \setminus C(\mathfrak{a}, \bullet)$ of the other, violating that they are type (b) minima.

Hence, assume that $|\mu|_\mathfrak{p} < |\mu''|_\mathfrak{p} < |\mu'|_\mathfrak{p}$. We must have $|\mu''|_\mathfrak{q} \geq |\mu|_\mathfrak{q}$ as otherwise $\mu'' \in \mathring{B}(\mathfrak{a}, \mu, \mu')$, contradicting that μ and μ' are neighbors. But in that case, $\mu \in B(\mathfrak{a}, \mu'') \setminus C(\mathfrak{a}, \mu'')$, contradicting that μ'' is a type (b) minimum of $\mathfrak{a}$. Therefore, this case cannot happen. This shows characterization (2). □

In the case $|S| > 2$, the neighbors in each direction are usually *not* unique (up to absolute values).

3.4 Connectivity of the Neighbor Graphs

In this section, we want to investigate whether the graphs $\mathcal{A}(\mathfrak{a})$, $\mathcal{C}(\mathfrak{a})$, $\mathcal{E}(\mathfrak{a})$ and their quotient graphs are connected. The connectedness is of importance for example for Buchmann's Generalized Lagrange Algorithm for computation of units (see Section 6.4.1). Moreover, we have seen in Example 3.2.2 that every unit $u \in \mathcal{O}^*$ is a type (c) minimum of $\mathcal{O}$ and, hence, also a type (b) minimum. Therefore, starting with $\mu = 1$, we can reach *every* unit of $\mathcal{O}$—in particular, a set of fundamental units—with a finite amount of "going to a neighbor" operations. This will be used in Sections 6.3 and 6.5.1.

According to [HPLR87, p. 294, Théorème 2], the quotient graphs of $\mathcal{A}(\mathfrak{a})$, $\mathcal{C}(\mathfrak{a})$ and $\mathcal{E}(\mathfrak{a})$ are connected; this is stated as Lagrange's Theorem in their paper:

Theorem 3.4.1. *[HPLR87, p. 294, Théorème 2] If K is a global field and $\mathfrak{a}$ is principal, the graphs $\overline{\mathscr{A}}(\mathfrak{a})$, $\overline{\mathscr{E}}(\mathfrak{a})$ and $\overline{\mathscr{C}}(\mathfrak{a})$ are finite and connected.*

In [HPLR87], a proof has been omitted for the statement that the graphs are connected. First, note that it suffices to show that $\mathscr{A}(\mathfrak{a})$, $\mathscr{E}(\mathfrak{a})$ and $\mathscr{C}(\mathfrak{a})$ are connected, as $\overline{\mathscr{A}}(\mathfrak{a})$, $\overline{\mathscr{E}}(\mathfrak{a})$ and $\overline{\mathscr{C}}(\mathfrak{a})$ are quotient graphs of those. For

$\mathscr{A}(\mathfrak{a})$ and $\mathscr{E}(\mathfrak{a})$ we will prove connectedness in this section; the result will be stated in Corollary 3.4.5.

We begin with some auxiliary results. The first result was shown by J. Buchmann in [Buc87a], where he proved the following:

Proposition 3.4.2. *[Buc87a, p. 12, Theorem 2.10] Let K be a number field and let μ, μ' be two minima of type (a) and $\mathfrak{p} \in S$ with $|\mu|_\mathfrak{p} \geq |\mu'|_\mathfrak{p}$ and $|\mu|_\mathfrak{q} \leq |\mu'|_\mathfrak{q}$ for every $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$. Then there exists a sequence of type (a) minima $\mu = \mu_0, \mu_1, \ldots, \mu_n = \mu'$ such that μ_{i-1} is a neighbor of μ_i for $i = 1, \ldots, n$.* □

From this we obtain:

Corollary 3.4.3. *If K is a number field, both the graphs $\mathscr{A}(\mathfrak{a})$ and $\mathscr{E}(\mathfrak{a})$ are connected.*

Proof. First, note that by Remark 3.2.4, we have $\mathscr{A}(\mathfrak{a}) = \mathscr{E}(\mathfrak{a})$, whence we can restrict to show this for $\mathscr{A}(\mathfrak{a})$. Let $\mu, \mu' \in \mathcal{A}(\mathfrak{a})$. If $|\mu|_\mathfrak{p} = |\mu'|_\mathfrak{p}$ for all $\mathfrak{p} \in S$, we have that μ and μ' are neighbors. Otherwise, there exists an $\mathfrak{p} \in S$ with $|\mu|_\mathfrak{p} \neq |\mu'|_\mathfrak{p}$. Without loss of generality, assume that $|\mu|_\mathfrak{p} < |\mu'|_\mathfrak{p}$.

Now, by Proposition 3.3.9 (a), there exists an $\varepsilon \in \mathcal{O}^*$ with $|\varepsilon|_\mathfrak{p} > 1$ and $|\varepsilon|_\mathfrak{q} < 1$, $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$. Hence, $\mu_n := \varepsilon^n \mu' \in \mathcal{A}(\mathfrak{a})$ satisfies $|\mu_n|_\mathfrak{p} = |\mu'|_\mathfrak{p} \cdot |\varepsilon|_\mathfrak{p}^n \to \infty$ for $n \to \infty$, and $|\mu_n|_\mathfrak{q} = |\mu'|_\mathfrak{q} \cdot |\varepsilon|_\mathfrak{q}^n \to 0$ for $n \to \infty$, $\mathfrak{q} \neq \mathfrak{p}$. Choose $n \in \mathbb{N}$ such that $|\mu_n|_\mathfrak{q} < |\mu|_\mathfrak{q}$ for all $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$.

Then, by applying Proposition 3.4.2 both to μ and μ_n and to μ' and μ_n, we get the required chain. □

Our next step is to prove an analogue of Buchmann's Proposition 3.4.2 for function fields, which gives the connectedness result:

Proposition 3.4.4. *Let K be a function field and let μ, μ' be two minima of type (a). Then there exists a sequence of type (a) minima $\mu = \mu_0, \mu_1, \ldots, \mu_n = \mu'$ such that μ_{i-1} is a neighbor of μ_i for $i = 1, \ldots, n$.*

One can choose all μ_i, $i = 1, \ldots, n-1$, to be minima of type (b), and that $|\mu_i|_\mathfrak{q} \leq \max\{|\mu|_\mathfrak{q}, |\mu'|_\mathfrak{q}\}$ for every i.

In particular, $\mathcal{A}(\mathfrak{a})$ and $\mathcal{E}(\mathfrak{a})$ are connected.

Proof. By Lemma 3.2.7, we can replace μ (respectively μ') by a neighbor which is a type (b) minima. (It is easy to see that the minimum whose existence is shown in that lemma is a neighbor of μ respectively μ'.)

We proceed by induction on

$$b(\mu,\mu') := \sum_{\mathfrak{p}\in S} \max\{-\nu_\mathfrak{p}(\mu), -\nu_\mathfrak{p}(\mu')\} \deg \mathfrak{p} \in \mathbb{Z},$$

where μ' is fixed. As $\mathfrak{a} = \{f \in K \mid (f)_{finite} \geq \operatorname{div}(\mathfrak{a})\}$, we have

$$\sum_{\mathfrak{p}\in S} -\nu_\mathfrak{p}(f) \deg \mathfrak{p} = -\deg(f) + \deg(f)_{finite} = \deg(f)_{finite} \geq \deg \operatorname{div}(\mathfrak{a})$$

for every $f \in \mathfrak{a} \setminus \{0\}$; therefore, as μ' is fixed, $b(\mu,\mu')$ can be bounded from below in terms of $\deg \operatorname{div}(\mathfrak{a})$ and $\nu_\mathfrak{q}(\mu')$, $\mathfrak{q} \in S$.

Hence, assume that the claim is true for all $\mu'' \in \mathcal{E}(\mathfrak{a})$ (replacing μ) with $b(\mu'',\mu') < b(\mu,\mu')$. If $\nu_\mathfrak{p}(\mu) \geq \nu_\mathfrak{p}(\mu')$ for all $\mathfrak{p} \in S$ or $\nu_\mathfrak{p}(\mu) \leq \nu_\mathfrak{p}(\mu')$ for all $\mathfrak{p} \in S$, we have $\nu_\mathfrak{p}(\mu) = \nu_\mathfrak{p}(\mu')$ for all $\mathfrak{p} \in S$ and we have that μ and μ' are neighbors.

If μ and μ' are not neighbors, we have that $A := \{\mathfrak{q} \in S \mid -\nu_\mathfrak{q}(\mu) > -\nu_\mathfrak{q}(\mu')\}$ is a proper, non-empty subset of S, and, with $\overline{A} := S \setminus A$,

$$\mathring{B}(\mathfrak{a},\mu,\mu') = \left\{ f \in \mathfrak{a} \,\middle|\, \begin{matrix} \forall \mathfrak{q} \in A : -\nu_\mathfrak{q}(f) \leq -\nu_\mathfrak{q}(\mu) - 1 \\ \forall \mathfrak{q} \in \overline{A} : -\nu_\mathfrak{q}(f) \leq -\nu_\mathfrak{q}(\mu') - 1 \end{matrix} \right\} \neq \{0\}.$$

Moreover, we have

$$T(t_\mathfrak{q}, \mathfrak{q} \in \overline{A}) := \left\{ f \in \mathfrak{a} \,\middle|\, \begin{matrix} \forall \mathfrak{q} \in A : -\nu_\mathfrak{q}(f) \leq -\nu_\mathfrak{q}(\mu) - 1 \\ \forall \mathfrak{q} \in \overline{A} : -\nu_\mathfrak{q}(f) \leq t_\mathfrak{q} \end{matrix} \right\} = \{0\},$$

where $t_\mathfrak{q} := -\nu_\mathfrak{q}(\mu) \leq -\nu_\mathfrak{q}(\mu')$ for all $\mathfrak{q} \in \overline{A}$.

Choose $s_\mathfrak{q}, \mathfrak{q} \in \overline{A}$ with $t_\mathfrak{q} \leq s_\mathfrak{q} \leq -\nu_\mathfrak{q}(\mu')$, $\mathfrak{q} \in \overline{A}$ such that $T(s_\mathfrak{q}, \mathfrak{q} \in \overline{A}) \neq \{0\}$, where the $s_\mathfrak{q}$ are chosen to be minimal under this condition, i.e. if one of the $s_\mathfrak{q}$'s is decreased by one, the set would be $\{0\}$. Pick $\mu'' \in T(s_\mathfrak{q}, \mathfrak{q} \in \overline{A}) \setminus \{0\}$; then, $\mu'' \in \mathcal{E}(\mathfrak{a})$ and μ'' and μ are neighbors. Now, $b(\mu'',\mu') < b(\mu,\mu')$, whence by induction hypothesis, there exists a chain of type (b) minima between μ' and μ''. Therefore, we can conclude. □

With the preceeding discussion, we have shown several cases of Theorem 3.4.1:

Corollary 3.4.5 (Lagrange, Part I). *Let $\mathfrak{a} \in \operatorname{Id}(\mathcal{O})$. Then $\mathscr{E}(\mathfrak{a})$ and $\mathscr{A}(\mathfrak{a})$ are connected. Moreover, if S contains a place of degree one, $\mathscr{C}(\mathfrak{a}) = \mathscr{E}(\mathfrak{a})$ by Proposition 3.2.5 (i) and, hence, $\mathscr{C}(\mathfrak{a})$ is connected as well. In particular, in this case, Theorem 3.4.1 is true.* □

In fact, this is slightly more general, as we did not assumed that K is a global field. Unfortunately, a proof for the connectedness of $\mathscr{C}(\mathfrak{a})$ in general is still missing.

3.5 Baby Steps

In this section, we want to analyze baby steps. These can be seen as a (more or less) natural generalization of the baby steps in the case of one-dimensional infrastructures. We want to do this as general as possible; later, in particular in the section on computation of baby steps in function fields (Section 5.5), we will specialize to more concrete choices.

Let $\mathfrak{a} \in \mathrm{Id}(\mathcal{O})$ and assume that $|S| > 1$. We want to **restrict to type (b) minima** in this section, as they turn out to be the right choice to use them for infrastructures. We have seen in Proposition 3.3.8 (b) that, given a minimum $\mu \in \mathcal{E}(\mathfrak{a})$ and $\mathfrak{p} \in S$, we can find a neighbor in $\mathfrak{p}$-direction, i.e. we can find a minimum $\mu' \in \mathcal{E}(\mathfrak{a})$ which is a neighbor of μ such that $|\mu|_\mathfrak{p} < |\mu'|_\mathfrak{p}$ and $|\mu|_\mathfrak{q} < |\mu'|_\mathfrak{q}$ for all $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$. Moreover, we obtained bounds for the absolute values in Theorem 3.3.11 for function fields respectively Proposition 3.3.12 for number fields.

We want to formalize this notion, to obtain an operation on $\mathcal{E}(\mathfrak{a})$ which, given $\mu \in \mathcal{E}(\mathfrak{a})$ and $\mathfrak{p} \in S$, "goes" to a neighbor of μ in direction $\mathfrak{p}$. As we will see, in case $\deg \mathfrak{p} = 1$, we easily get a unique such element if one parameter is chosen in the right way, but in the general case, we need an order on $\mathcal{E}(\mathfrak{a})$, or more precisely, one for each $\mathfrak{p} \in S$.

Definition 3.5.1. *Let $\leq$ be a total preorder*[1] *on $\mathfrak{a} \setminus \{0\}$ and $\mathfrak{p} \in S$. We say that $\leq$ is an* $\mathfrak{p}$-order *on $\mathfrak{a}$ if it satisfies the following:*

(i) *for $\mu, \mu' \in \mathfrak{a} \setminus \{0\}$ with $|\mu|_\mathfrak{p} < |\mu'|_\mathfrak{p}$, we have $\mu \leq \mu'$;*

(ii) *if $\mu, \mu' \in \mathfrak{a} \setminus \{0\}$, then $\mu \leq \mu'$ and $\mu' \leq \mu$ if, and only if, $|\mu|_\mathfrak{q} = |\mu'|_\mathfrak{q}$ for every $\mathfrak{q} \in S$; and*

(iii) *if μ is a minimal element with respect to $\leq$ in $B(\mathfrak{a}, (t_\mathfrak{q})_{\mathfrak{q}\in S}) \setminus \{0\}$ for some $t_\mathfrak{q} \in \mathbb{R}$, $\mathfrak{q} \in S$, then $\mu \in \mathcal{E}(\mathfrak{a})$.*

Definition 3.5.2. *Let $\mathfrak{p} \in S$. A* universal $\mathfrak{p}$-order *is a relation $\leq$ on K^* which, for every $\mathfrak{a} \in \mathrm{Id}(\mathcal{O})$, restricts to a $\mathfrak{p}$-order on $\mathfrak{a}$.*

The most important example, which we will actually use in several occasions, is the lexicographic order:

[1] A relation $\leq$ on a set S is called a *total preorder* if, for every $x, y, z \in S$, we have: (i) $x \leq x$, (ii) $x \leq y$ or $y \leq x$, (iii) $x \leq y$ and $y \leq z$ implies $x \leq z$.

Example 3.5.3. Let $\mathfrak{p} \in S$ and write $S = \{\mathfrak{p}, \mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$ where $|S| = n+1$. For $\mu, \mu' \in K^*$, define

$$\mu \leq \mu' :\Longleftrightarrow (|\mu|_{\mathfrak{p}}, |\mu|_{\mathfrak{q}_1}, \ldots, |\mu|_{\mathfrak{q}_n}) \leq_{\ell ex} (|\mu'|_{\mathfrak{p}}, |\mu'|_{\mathfrak{q}_1}, \ldots, |\mu'|_{\mathfrak{q}_n}),$$

where $\leq_{\ell ex}$ is the lexicographic order on $\mathbb{R}^{n+1}$, i.e. we have

$$\begin{aligned}(x_1, \ldots, x_{n+1}) \leq_{\ell ex} (y_1, \ldots, y_{n+1}) :\Longleftrightarrow (x_1, \ldots, x_{n+1}) = (y_1, \ldots, y_{n+1}) \\ \vee \exists i : (x_i < y_i \wedge \forall j < i : x_j = y_j).\end{aligned}$$

Then $\leq$ is a universal $\mathfrak{p}$-order, as for every $\mathfrak{a} \in \mathrm{Id}(\mathcal{O})$, $\leq|_{\mathfrak{a}\setminus\{0\}}$ is a $\mathfrak{p}$-order on $\mathfrak{a}$.

Next, we want to introduce baby step shapes, which control the area from which the baby step should be chosen. In the one-dimensional case, i.e. if $|S| = 2$, there is only one choice, but for $|S| > 2$ there are different ones.

Definition 3.5.4. *Let $X \subseteq \mathbb{R}^n_{\geq 0}$.*

(a) *We say that X is* symmetric *if, for every permutation σ of $\{1, \ldots, n\}$, the map*

$$\hat{\sigma} : \mathbb{R}^n_{\geq 0} \to \mathbb{R}^n_{\geq 0}, \qquad (x_1, \ldots, x_n) \mapsto (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

satisfies $\hat{\sigma}(X) = X$.

(b) *We say that X is* rectangular *if, for every $x = (x_1, \ldots, x_n) \in X$, the rectangle set*

$$\{(y_1, \ldots, y_n) \in \mathbb{R}^n_{\geq 0} \mid \forall i : y_i \leq x_i\}$$

lies inside X.

(c) *We say that X is a* baby step shape *if X is symmetric, rectangular, and we have*

$$[0,1)^n \subseteq X \subsetneqq [0,1]^n.$$

Remark 3.5.5. If $n = 1$, the only baby step shape is $[0, 1)$.

As we want to work with type (b) minima, and these are usually just unique up to absolute values, we define an equivalence relation which identifies minima if their absolute values coincide. Let $\sim$ be the relation on K defined by

$$\mu \sim \mu' :\Longleftrightarrow \forall \mathfrak{q} \in S : |\mu|_{\mathfrak{q}} = \left|\mu'\right|_{\mathfrak{q}}.$$

Remarks 3.5.6.

(a) Assume that $\deg \mathfrak{q} = 1$ for some $\mathfrak{q} \in S$. Then $\mu \sim \mu'$ for $\mu, \mu' \in \mathcal{E}(\mathfrak{a})$ if, and only if, $\frac{\mu}{\mu'} \in k^*$.

(b) If $\leq$ is a $\mathfrak{p}$-order on $\mathfrak{a}$, then $\leq$ induces a total order on $(\mathfrak{a} \setminus \{0\})/_\sim$.

Now we are able to define baby steps. Note that the well-definedness is shown in the proposition following the definition.

Definition 3.5.7. *Let $X \subsetneqq [0,1]^n$ be a baby step shape, and let $\mathfrak{p} \in S$. Let $\leq$ be an $\mathfrak{p}$-order on $\mathfrak{a}$, and write $S = \{\mathfrak{p}, \mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$ with $|S| = n+1$.*

For $\mu \in \mathcal{E}(\mathfrak{a})$, consider

$$X^{\mu,\mathfrak{p}} := \left\{ f \in \mathfrak{a} \setminus \{0\} \;\middle|\; \left(\left|\frac{f}{\mu}\right|_{\mathfrak{q}_1}, \ldots, \left|\frac{f}{\mu}\right|_{\mathfrak{q}_n} \right) \in X,\ \left|\frac{f}{\mu}\right|_{\mathfrak{p}} > 1 \right\}.$$

Define the baby step in $\mathfrak{p}$-direction *with* shape X *and* order $\leq$, *denoted by* $\mathrm{bs}_{\mathfrak{p}}^{X,\leq}(\mu) := \mathrm{bs}_{\mathfrak{p}}^{X,\leq}(\mu, \mathfrak{a})$, *as the set of smallest elements in $X^{\mu,\mathfrak{p}}$ with respect to $\leq$.*

Proposition 3.5.8. *We have that $\mathrm{bs}_{\mathfrak{p}}^{X,\leq}$ defines a function $\mathcal{E}(\mathfrak{a})/_\sim \to \mathcal{E}(\mathfrak{a})/_\sim$ such that for every $\mu \in \mathcal{E}(\mathfrak{a})$, we have that μ is a neighbor of every element in $\mathrm{bs}_{\mathfrak{p}}^{X,\leq}(\mu)$.*

Proof. Clearly, all choices of elements only depend on their absolute values $|\bullet|_{\mathfrak{q}}$, $\mathfrak{q} \in S$, whence it makes sense to work modulo $\sim$.

Note that $X_{\mathfrak{p}}^{\mu,\leq}$ is non-empty by Minkowski's Lattice Point Theorem or Riemann's Inequality; consider $X = [0,1)^n$; then

$$\{0\} \cup X^{\mu,\mathfrak{p}} = \bigcup_{n \in \mathbb{N}} \mathring{B}(\mathfrak{a}, (-\nu_{\mathfrak{q}}(\mu))_{\mathfrak{q} \in S} + n e_{\mathfrak{p}}),$$

where $e_{\mathfrak{p}} \in \mathbb{Z}^S$ is the vector with a 1 at the $\mathfrak{p}$-component and 0's elsewhere and $T(\mu) = (t_{\mathfrak{q}})_{\mathfrak{q} \in S}$ with $t_{\mathfrak{q}} = -\nu_{\mathfrak{q}}(\mu)$, $\mathfrak{q} \in S$.

Then, as either $\mathfrak{a}$ is an euclidean lattice (number field case) or as $\nu_{\mathfrak{p}}$ is discrete (function field case), elements in $X_{\mathfrak{p}}^{\mu,\mathfrak{p}}$ with minimal $|\bullet|_{\mathfrak{p}}$ exist. Modulo $\sim$, these are finitely many, whence a minimum exists. Let μ' be a minimal element of $X^{\mu,\mathfrak{p}}$.

We have to show $\mu' \in \mathcal{E}(\mathfrak{a})$ and that μ and μ' are neighbors. The first fact follows as $B(\mathfrak{a}, \mu') \subseteq X^{\mu,\mathfrak{p}} \cup \{0\}$, whence μ' is a minimal element of $B(\mathfrak{a}, \mu')$ with respect to $\leq$. As $\leq$ is a $\mathfrak{p}$-order, this implies that $\mu' \in \mathcal{E}(\mathfrak{a})$. The second fact follows from the construction of $\mathrm{bs}_{\mathfrak{p}}^{X,\leq}$, as $|\mu|_{\mathfrak{p}}$ is minimal and $[0,1)^n \subseteq X$, whence $\mathring{B}(\mathfrak{a}, \mu, \mu') = \{0\}$. □

As already mentioned, in certain cases, the baby step does not depend on the order $\leq$:

Proposition 3.5.9. *Assume that* $\deg \mathfrak{p} = 1$. *If K is a number field, or if K is a function field and $X = [0,1)^n$, then* $\mathrm{bs}_{\mathfrak{p}}^{X,\leq}$ *is independent of the order* $\leq$.

Remark 3.5.10. In the case of $n = 1$, i.e. $|S| = 2$, the only baby step shape is $[0,1) = [0,1] \setminus \{1\}$ (see Remark 3.5.5). Hence, if we in addition have $\deg \mathfrak{p} = 1$, $\mathrm{bs}_{\mathfrak{p}}^{X,\leq}$ does not depend on $\leq$.

Actually, this has already been shown in Proposition 3.3.13 *without* the requirement $\deg \mathfrak{p} = 1$; there, we even saw that $|S| = 2$ already ensures that $\mathrm{bs}_{\mathfrak{p}}^{X,\leq}$ does not depends on X and $\leq$ without any requirement on $\deg \mathfrak{p}$.

Proof of Proposition 3.5.9. If K is a number field, then $|x|_{\mathfrak{p}} = |y|_{\mathfrak{p}}$ implies $x = \pm y$. This implies that there exists only one $\mathfrak{p}$-order, namely the one defined by

$$x \leq y :\Longleftrightarrow |x|_{\mathfrak{p}} \leq |y|_{\mathfrak{p}}.$$

If K is a function field and $X = [0,1)^n$, then, with $t_{\mathfrak{q}} := -\nu_{\mathfrak{q}}(\mu) - 1$ for $\mathfrak{q} \in S$, we have $X_{\mathfrak{p}}^{\mu,\leq} = \bigcup_{n\in\mathbb{N}} L(\mathrm{div}(\mathfrak{a}) + \sum_{\mathfrak{q}\in S} t_{\mathfrak{q}}\mathfrak{q} + n\mathfrak{p})$. Now $\dim L(\mathrm{div}(\mathfrak{a}) + \sum_{\mathfrak{q}\in S} t_{\mathfrak{q}}\mathfrak{q} + n\mathfrak{p})$ increases by at most $\deg \mathfrak{p} = 1$ if n increases by one, whence there exists a minimal n with $\dim L(\mathrm{div}(\mathfrak{a}) + \sum_{\mathfrak{q}\in S} t_{\mathfrak{q}}\mathfrak{q} + n\mathfrak{p}) = 1$. But in this space, every non-zero element has the same absolute values $|\bullet|_{\mathfrak{q}}$, $\mathfrak{q} \in S$, whence every element is a minimum in $X_{\mathfrak{p}}^{\mu,\leq}$ with respect to any $\mathfrak{p}$-order $\leq$. □

Remark 3.5.11. In the function field case, this is not in general if $X \neq [0,1)^n$: consider $K = \mathbb{F}_7(x,y)$ with $y^3 = (x^4+x^3+x^2+4)x^2$. This is a purely cubic field of genus 3, with three infinite places $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ of degree one:

$$\mathfrak{m}_{\mathfrak{p}_1} = (\tfrac{1}{x}, \tfrac{y}{x^2} + 3), \quad \mathfrak{m}_{\mathfrak{p}_2} = (\tfrac{1}{x}, \tfrac{y}{x^2} + 5) \quad \text{and} \quad \mathfrak{m}_{\mathfrak{p}_3} = (\tfrac{1}{x}, \tfrac{y}{x^2} + 6).$$

Consider $\mathfrak{a} = \mathcal{O}$ and $\mu = 1$. Then $L(n\mathfrak{p}_3) = \mathbb{F}_7 \cdot 1$ for $n = 0,1,2,3$ and $L(4\mathfrak{p}_3) = \mathbb{F}_7 \cdot 1 + \mathbb{F}_7 \cdot f$ with $f = \frac{x+5}{x}y^2 + (x^2+3x+5)y + (x^4+x^2+2x) \in \mathcal{O}$. Moreover,

$$\nu_{\mathfrak{p}_1}(f) = 0, \quad \nu_{\mathfrak{p}_2}(f) = 1 \quad \text{and} \quad \nu_{\mathfrak{p}_3}(f) = -4$$

and

$$\nu_{\mathfrak{p}_1}(f+3) = 1, \quad \nu_{\mathfrak{p}_2}(f+3) = 0 \quad \text{and} \quad \nu_{\mathfrak{p}_3}(f+3) = -4,$$

which shows that $\mathrm{bs}_{\mathfrak{p}_3}^{X,\leq}(\mu)$ with $X = [0,1]^2 \setminus \{(1,1)\}$ depends on $\leq$.

In the literature, usually the shape $X = [0,1]^n \setminus \{(1,\dots,1)\}$ is taken [Buc85a, LSY03]. An alternative is $X' = [0,1)^n$. Even though the alternative X' leads to more unique (in some sense) baby steps in the function field case by Proposition 3.5.9, it has the disadvantage that the distances are larger, we we will see in Theorem 3.5.18.

For the following, in particular for the next section, we need that baby steps behave well with scaling, i.e. with multiplication by non-zero elements. For that, we need that the order behaves well with scaling, too.

Definition 3.5.12. *Let $\leq$ be a relation on K^*. We say that $\leq$ is* scale-invariant *if, for every $f, g, h \in K^*$, we have $f \leq g$ if, and only if, $hf \leq hg$.*

Remark 3.5.13. The lexicographic order in Example 3.5.3 is scale-invariant.

Lemma 3.5.14. *Let $X \subsetneq [0,1]^n$ be a baby step shape, and let $\mathfrak{p} \in S$. Let $\leq$ be a scale-invariant universal $\mathfrak{p}$-order on K^*. If $\mu \in \mathcal{E}(\mathfrak{a})$ and $h \in K^*$, then*

$$h \operatorname{bs}_{\mathfrak{p}}^{X,\leq}(\mu, \mathfrak{a}) = \operatorname{bs}_{\mathfrak{p}}^{X,\leq}(h\mu, h\mathfrak{a}).$$

Proof. First, we have $X_{h\mathfrak{a}}^{h\mu,\mathfrak{p}} = hX_{\mathfrak{a}}^{\mu,\mathfrak{p}}$. Then, $hf \leq hg$ if, and only if, $f \leq g$ for all $f, g \in \mathfrak{a}$ as $\leq$ is scale-invariant. These two facts combined give the result. □

We want to investigate another equivalence relation which extends $\sim$. It is related to the concept of *ideal representations* which will be introduced in Section 3.6: the ideal representation of a minimum $\mu \in \mathcal{E}(\mathfrak{a})$ is $\frac{1}{\mu}\mathfrak{a}$. Note that two minima μ, μ' of $\mathfrak{a}$ have the same ideal representation if, and only if, $\frac{\mu}{\mu'} \in \mathcal{O}^*$.

Remark 3.5.15. Recall that for two minima $f, g \in \mathcal{E}(\mathfrak{a})$, we wrote $f \sim g$ if, and only if, $|f|_{\mathfrak{p}} = |g|_{\mathfrak{p}}$ for every $\mathfrak{p} \in S$. Opposed to this, the ideal representation of f and g is the same if, and only if, $\frac{f}{g} \in \mathcal{O}^*$. Now, $f \sim g$ and $\frac{f}{g} \in \mathcal{O}^*$ coincide if, and only if, $\frac{f}{g} \in k^*$, i.e. f and g are equal up to constants.

Note that if $f \sim g$ and $\varepsilon \in \mathcal{O}^*$, then $\varepsilon f \sim \varepsilon g$. Hence, it makes sense to consider the relation $\sim_{\mathcal{O}^*}$ defined by

$$f \sim_{\mathcal{O}^*} g :\Longleftrightarrow \exists \varepsilon \in \mathcal{O}^* : f \sim \varepsilon g,$$

which can be seen as a combination of $\sim$ and equivalence modulo $\mathcal{O}^*$. Again, $\sim_{\mathcal{O}^*}$ is an equivalence relation. Consider the map

$$\Phi : K^* \to \mathbb{R}^S, \qquad f \mapsto (\nu_{\mathfrak{p}}(f))_{\mathfrak{p} \in S}.$$

Then $\Phi(\mathcal{O}^*)$ is a subgroup of $\mathbb{R}^S$ (in fact, it is a $(|S|-1)$-dimensional lattice in $\mathbb{R}^S$), and we have

$$f \sim_{\mathcal{O}^*} g \iff \Phi(f) - \Phi(g) \in \Phi(\mathcal{O}^*).$$

(Also compare Lemma 4.1.1.) Note that this relation will be considered again in the next section and in Section 4.1.

Now, we can state some corollaries of Lemma 3.5.14:

Corollary 3.5.16. *Let $X \subsetneqq [0,1]^n$ be a baby step shape, and let $\mathfrak{p} \in S$. Let $\leq$ be a scale-invariant universal $\mathfrak{p}$-order on K. Then, the baby step function $\mathrm{bs}_{\mathfrak{p}}^{X,\leq}(\bullet, \mathfrak{a})$ on $\mathcal{E}(\mathfrak{a})$ induces a function on $\mathcal{E}(\mathfrak{a})/_{\sim_{\mathcal{O}^*}}$.* □

Corollary 3.5.17. *If $\deg \mathfrak{q} = 1$ for some $\mathfrak{q} \in S$, then $f \sim_{\mathcal{O}^*} g$ for $f, g \in \mathcal{E}(\mathfrak{a})$ if, and only if, $\frac{f}{g} \in \mathcal{O}^*$.*

Therefore, if $X \subsetneqq [0,1]^n$ is a baby step shape and $\mathfrak{p} \in S$, and if $\leq$ is a scale-invariant universal $\mathfrak{p}$-order on K, then the baby step function $\mathrm{bs}_{\mathfrak{p}}^{X,\leq}(\bullet, \mathfrak{a})$ induces a function on $\mathcal{E}(\mathfrak{a})/\mathcal{O}^*$.

Proof. If $\deg \mathfrak{q} = 1$ for some $\mathfrak{q} \in S$, then, by Proposition 3.2.5 (a), $f, g \in \mathcal{C}(\mathfrak{a})$. In that case, $f \sim g$ implies $f \in B(\mathfrak{a}, g)$, whence $\frac{f}{g} \in k^* \subseteq \mathcal{O}^*$. This shows the first part of the claim. The second follows from the first together with Corollary 3.5.16 □

Finally, we want to give estimates on the distances obtained from baby steps in the function field case. It can be seen as an extension of Theorem 3.3.11; there, we essentially showed the existence of baby steps with the baby step shape $[0,1)^n$.

Theorem 3.5.18. *Let $X \subsetneqq [0,1]^n$ be a baby step shape, and let $\mathfrak{p} \in S$. Let $\leq$ be a $\mathfrak{p}$-order on $\mathfrak{a}$, $\mu \in \mathcal{E}(\mathfrak{a})$ and $\mu' \in \mathrm{bs}_{\mathfrak{p}}^{X,\leq}(\mu)$.*

(a) *If $X' \subsetneqq [0,1]^n$ is another baby step shape with $X \subseteq X'$, and if $\mu'' \in \mathrm{bs}_{\mathfrak{p}}^{X',\leq}(\mu)$, then $|\mu''|_{\mathfrak{p}} \leq |\mu'|_{\mathfrak{p}}$.*

(b) *Assume that K is a function field of genus g. Then, we have*

$$0 < \nu_{\mathfrak{p}}(\mu) - \nu_{\mathfrak{p}}(\mu') \leq \left\lceil \frac{g + \sum\limits_{\mathfrak{q} \in S \setminus \{\mathfrak{p}\}} \deg \mathfrak{q}}{\deg \mathfrak{p}} \right\rceil.$$

If $\mathfrak{a}$ is not generated by μ and if $\deg \mathfrak{p}$ divides $g + \sum\limits_{\mathfrak{q} \in S \setminus \{\mathfrak{p}\}} \deg \mathfrak{q}$, we have a strict inequality.

(c) *Assume that K is a function field of genus g and that $X = [0,1]^n \setminus \{(1,\dots,1)\}$. Then,*

$$0 < \nu_{\mathfrak{p}}(\mu) - \nu_{\mathfrak{p}}(\mu') \leq \left\lceil \frac{g + \min\limits_{\mathfrak{q} \in S \setminus \{\mathfrak{p}\}} \deg \mathfrak{q}}{\deg \mathfrak{p}} \right\rceil .$$

If $\mathfrak{a}$ is not generated by μ and if $\deg \mathfrak{p}$ divides $g + \min\limits_{\mathfrak{q} \in S \setminus \{\mathfrak{p}\}} \deg \mathfrak{q}$, we have a strict inequality.

Proof.

(a) Clearly, $X_{\mathfrak{a}}^{\mu,\mathfrak{p}} \subseteq (X')_{\mathfrak{a}}^{\mu,\mathfrak{p}}$, which gives the claim together with the fact that $\leq$ is a $\mathfrak{p}$-order.

(b) For $X = [0,1)^n$, this is Theorem 3.3.11 (a). For other baby step shapes X', this follows with $X = [0,1)^n$ and (a).

(c) This can be proved analogous to Theorem 3.3.11 (a), as one can fill $X_{\mathfrak{a}}^{\mu,\mathfrak{p}}$ with $|S| - 1$ chains of ascending Riemann-Roch spaces, one for every $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$, where we start with divisors whose degree differs from the one for μ by $\deg \mathfrak{q}$. □

3.6 Representation by Ideals

In this section, we want to investigate the representation of minima by ideals. This will be essential in the later chapters, as it allows a compact representation of minima and leads to an efficient arithmetic in $\mathrm{Pic}^0(K)$. We will describe an equivalence relation on the set of type (b) reduced ideals which will be used all over the next chapter, and show that baby steps behave well in this setting.

We begin with the notion of a reduced ideal:

Definition 3.6.1. *Let $\mathfrak{a} \in \mathrm{Id}(\mathcal{O})$.*

(a) *We say that $\mathfrak{a}$ is* reduced of type (a) *if $1 \in \mathcal{A}(\mathfrak{a})$.*

(b) *We say that $\mathfrak{a}$ is* reduced of type (b) *if $1 \in \mathcal{E}(\mathfrak{a})$.*

(c) *We say that $\mathfrak{a}$ is* reduced of type (c) *if $1 \in \mathcal{C}(\mathfrak{a})$.*

Denote the set of reduced ideals of type (a), (b) and (c) by $\mathrm{Red}^{(a)}(K)$, $\mathrm{Red}^{(b)}(K)$ and $\mathrm{Red}^{(c)}(K)$, respectively. For a fixed ideal $\mathfrak{b} \in \mathrm{Id}(\mathcal{O})$, define

$$\begin{aligned} \mathrm{Red}^{(a)}(\mathfrak{b}) &:= \{\mathfrak{a} \in \mathrm{Red}^{(a)}(K) \mid \exists f \in K^* : f\mathfrak{a} = \mathfrak{b}\}, \\ \mathrm{Red}^{(b)}(\mathfrak{b}) &:= \{\mathfrak{a} \in \mathrm{Red}^{(b)}(K) \mid \exists f \in K^* : f\mathfrak{a} = \mathfrak{b}\} \\ \text{and} \qquad \mathrm{Red}^{(c)}(\mathfrak{b}) &:= \{\mathfrak{a} \in \mathrm{Red}^{(c)}(K) \mid \exists f \in K^* : f\mathfrak{a} = \mathfrak{b}\}. \end{aligned}$$

The rationale behind this representation is explained by the following proposition:

Proposition 3.6.2. *Let* $\mathfrak{a} \in \mathrm{Id}(\mathcal{O})$.

(a) *The map*
$$\mathcal{A}(\mathfrak{a})/\mathcal{O}^* \to \mathrm{Red}^{(a)}(\mathfrak{a}), \qquad \mu \mapsto \tfrac{1}{\mu}\mathfrak{a}$$
gives a bijection from $\mathcal{A}(\mathfrak{a})/\mathcal{O}^*$ *onto the set of type (a) reduced ideals equivalent to* $\mathfrak{a}$.

(b) *The map*
$$\mathcal{E}(\mathfrak{a})/\mathcal{O}^* \to \mathrm{Red}^{(b)}(\mathfrak{a}), \qquad \mu \mapsto \tfrac{1}{\mu}\mathfrak{a}$$
gives a bijection from $\mathcal{E}(\mathfrak{a})/\mathcal{O}^*$ *onto the set of type (b) reduced ideals equivalent to* $\mathfrak{a}$.

(c) *The map*
$$\mathcal{C}(\mathfrak{a})/\mathcal{O}^* \to \mathrm{Red}^{(c)}(\mathfrak{a}), \qquad \mu \mapsto \tfrac{1}{\mu}\mathfrak{a}$$
gives a bijection from $\mathcal{C}(\mathfrak{a})/\mathcal{O}^*$ *onto the set of type (c) reduced ideals equivalent to* $\mathfrak{a}$.

Here, two ideals $\mathfrak{a}$ *and* $\mathfrak{a}'$ *are equivalent if* $\mathfrak{a}\,\mathrm{PId}(\mathcal{O}) = \mathfrak{a}'\,\mathrm{PId}(\mathcal{O})$, *i.e. if there exists some* $f \in K^*$ *such that* $\mathfrak{a} = f\mathfrak{a}'$.

Proof. This follows from Proposition 3.2.5 (c), as $1 = \frac{\mu}{\mu} \in \frac{1}{\mu}\mathfrak{a}$. □

Definition 3.6.3. *We call* $\frac{1}{f}\mathfrak{a}$ *the* ideal representation *of a minimum* f *of* $\mathfrak{a}$.

Recall the equivalence relation $\sim_{\mathcal{O}^*}$. We want to investigate how this relation behaves on the ideal representations of two type (b) minima.

Lemma 3.6.4. *Let* $\mathfrak{a} \in \mathrm{Id}(\mathcal{O})$ *and* $\mu, \mu' \in \mathcal{E}(\mathfrak{a})$. *Then* $\mu \sim_{\mathcal{O}^*} \mu'$ *if, and only if,* $\frac{1}{\mu}\mathfrak{a} = \lambda\frac{1}{\mu'}\mathfrak{a}$ *for some* $\lambda \in K^*$ *with* $\nu_{\mathfrak{p}}(\lambda) = 0$ *for all* $\mathfrak{p} \in S$.

If $\mu \in \mathcal{C}(\mathfrak{a})$ *or* $\mu' \in \mathcal{C}(\mathfrak{a})$, *it necessarily follows that* $\lambda \in k^*$.

Proof. Note that $\frac{1}{\mu}\mathfrak{a} = \frac{1}{\mu'}\mathfrak{a}$ if, and only if, there exists a unit $\varepsilon \in \mathcal{O}^*$ such that $\mu = \varepsilon\mu'$.

Hence, if $\mu \sim_{\mathcal{O}^*} \mu'$, with $\varepsilon \in \mathcal{O}^*$ such that $\nu_{\mathfrak{p}}(\mu'\mu^{-1}\varepsilon) = 0$ for all $\mathfrak{p} \in S$, define $\lambda := \mu'\mu^{-1}\varepsilon$. Then $\lambda\frac{1}{\mu'}\mathfrak{a} = \frac{\mu'}{\mu}\varepsilon\frac{1}{\mu'}\mathfrak{a} = \frac{1}{\mu}\mathfrak{a}$.

Conversely, assume that $\frac{1}{\mu}\mathfrak{a} = \lambda\frac{1}{\mu'}\mathfrak{a}$ for some $\lambda \in K^*$ such that $\nu_{\mathfrak{p}}(\lambda) = 0$ for all $\mathfrak{p} \in S$. Then there exists an $\varepsilon \in \mathcal{O}^*$ with $\mu = \varepsilon\frac{\mu'}{\lambda}$, i.e. $\mu(\mu')^{-1}\varepsilon^{-1} = \lambda^{-1}$. But this means $\mu' \sim_{\mathcal{O}^*} \mu$, and as $\sim_{\mathcal{O}^*}$ is symmetric, $\mu \sim_{\mathcal{O}^*} \mu'$.

Finally, if $\mu \in \mathcal{C}(\mathfrak{a})$, from $\lambda\mu = \varepsilon\mu' \in \mathcal{E}(\mathfrak{a})$, we get $\lambda\mu \in \mathfrak{a}$. As $\nu_{\mathfrak{p}}(\lambda) = 0$ for all $\mathfrak{p} \in S$, we have $\lambda\mu \in B(\mathfrak{a}, \mu) = k^*\mu \cup \{0\}$, whence we must have $\lambda \in k^*$. If $\mu' \in \mathcal{C}(\mathfrak{a})$, one uses the same argument to show that $\lambda^{-1} \in k^*$. □

Next, we want to define the notion of two ideals being equivalent. Note that the usual definition (as in Proposition 3.6.2) is different, as it means that the two ideals lie in the same ideal class. For our purposes, we want to identify ideals who satisfy the condition from the lemma:

Definition 3.6.5. *Two reduced ideals $\mathfrak{b}, \mathfrak{b}'$ of type (b) are said to be* equivalent*, written as $\mathfrak{b} \sim \mathfrak{b}'$, if $\mathfrak{b} = \lambda\mathfrak{b}'$ for some $\lambda \in K^*$ with $\nu_{\mathfrak{p}}(\lambda) = 0$ for all $\mathfrak{p} \in S$.*

Then $\mu \sim_{\mathcal{O}^*} \mu'$ for $\mu, \mu' \in \mathcal{E}(\mathfrak{a})$ if, and only if, $\frac{1}{\mu}\mathfrak{a} \sim \frac{1}{\mu'}\mathfrak{a}$. This allows us to carry over baby steps to ideal representations. We begin with the following result:

Proposition 3.6.6. *Let $X \subsetneqq [0,1]^n$ be a baby step shape, and let $\mathfrak{p} \in S$. Let $\leq$ be a scale-invariant universal $\mathfrak{p}$-order on K. Let $f \in \mathcal{E}(\mathfrak{a})$. Then*

$$\tfrac{1}{\mu}\,\mathrm{bs}_{\mathfrak{p}}^{X,\leq}(\mu, \mathfrak{a}) = \mathrm{bs}_{\mathfrak{p}}^{X,\leq}(1, \tfrac{1}{\mu}\mathfrak{a}).$$

In particular, if $\mu' \in \mathrm{bs}_{\mathfrak{p}}^{X,\leq}(\mu, \mathfrak{a})$, then $\frac{\mu'}{\mu} \in \mathrm{bs}_{\mathfrak{p}}^{X,\leq}(1, \frac{1}{\mu}\mathfrak{a})$ and

$$\frac{1}{\mu'}\mathfrak{a} = \frac{1}{\frac{\mu'}{\mu}} \cdot \tfrac{1}{\mu}\mathfrak{a},$$

i.e. it is possible to compute the ideal representation of some[2] element in $\mathrm{bs}_{\mathfrak{p}}^{X,\leq}(f, \mathfrak{a})$ from the ideal representation of f.

Proof. This is an immediate consequence of Lemma 3.5.14. □

[2]Recall that $\mathrm{bs}_{\mathfrak{p}}^{X,\leq}(f, \mathfrak{a})$ is defined up to the equivalence relation $\sim$, i.e. the result is only unique up to absolute values $|\bullet|_{\mathfrak{q}}$, $\mathfrak{q} \in S$.

Using our new equivalence relation from Definition 3.6.5, we get:

Corollary 3.6.7. *Let $X \subsetneqq [0,1]^n$ be a baby step shape, and let $\mathfrak{p} \in S$. Let $\leq$ be a scale-invariant universal $\mathfrak{p}$-order on K. Then $\mathrm{bs}_{\mathfrak{p}}^{X,\leq}$ induces a function*

$$\mathrm{Red}^{(b)}(\mathfrak{a})/_{\sim} \to \mathrm{Red}^{(b)}(\mathfrak{a})/_{\sim}, \qquad [\mathfrak{b}]_{\sim} \mapsto \left[\tfrac{1}{\mu}\mathfrak{b}\right]_{\sim},$$

where $\mu \in \mathrm{bs}_{\mathfrak{p}}^{X,\leq}(1,\mathfrak{b})$ is arbitrary. We denote this function by $\mathrm{bs}_{\mathfrak{p}}^{X,\leq}$. □

Chapter 4

The Infrastructure of a Global Field

In this chapter, we want to describe how an infrastructure can be constructed for a global field of arbitrary unit rank. We begin by investigating the equivalence relation $\sim$ on reduced ideals introduced in Section 3.6. The set of reduced ideals of type (b) inside one ideal class modulo this equivalence relation will turn out to be the finite set X for our infrastructure. Then we will describe the distance map and introduce f-representations, to obtain a reduction map which gives the infrastructure. After that, we will relate the infrastructure to the Picard group of K and show a generalization of a result by S. Paulus and H.-G. Rück [PR99] and another result by R. Schoof [Sch08]. After that, we analyze the size of f-representations. Then we investigate whether the obtained infrastructures are discrete, and study the question of which elements in the principal ideal infrastructure of a number field have finite order. Finally, we give some conclusions.

We fix the following notation. Let $S' \subseteq S$ be a subset with $|S'| = |S| - 1$, and write $S' = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ and $S = S' \cup \{\mathfrak{p}_{n+1}\}$ with $|S| = n+1$. Let $\mathbb{G} = \mathbb{Z}$ if K is a function field and $\mathbb{G} = \mathbb{R}$ if K is a number field. Let $\Psi : K^* \to \mathbb{R}^{S'}$ be the map defined by

$$f \mapsto (-\nu_{\mathfrak{p}}(f))_{\mathfrak{p} \in S'}.$$

Then $\Lambda := \Psi(\mathcal{O}^*)$ is a full lattice in $\mathbb{R}^{S'}$,

4.1 Equivalence Classes of Reduced Ideals

Recall the equivalence relation $\sim_{\mathcal{O}^*}$ on $\mathcal{E}(\mathfrak{a})$: we have $\mu \sim_{\mathcal{O}^*} \mu'$ if, and only if, there exists a unit $\varepsilon \in \mathcal{O}^*$ such that $\nu_{\mathfrak{p}}(\mu' \mu^{-1} \varepsilon) = 0$ for all $\mathfrak{p} \in S$.

We begin by showing how the relation $\sim_{\mathcal{O}^*}$ naturally appears as the kernel of a map from $\mathcal{E}(\mathfrak{a})$ to an n-dimensional torus.

Lemma 4.1.1. *For $\mathfrak{a} \in \mathrm{Id}(\mathcal{O})$, we get the map*

$$\psi : \mathcal{E}(\mathfrak{a}) \to \mathbb{R}^{S'}/\Lambda, \qquad \mu \mapsto \Psi(\mu) + \Lambda.$$

Then $\psi(\mu) = \psi(\mu')$ for $\mu, \mu' \in \mathcal{E}(\mathfrak{a})$ if, and only if, $\mu \sim_{\mathcal{O}^*} \mu'$.

In particular, if one of μ and μ' lies in $\mathcal{C}(\mathfrak{a})$, we have $\psi(\mu) = \psi(\mu')$ if, and only if, $\mu\mathcal{O}^* = \mu'\mathcal{O}^*$ or, equivalently, $\frac{1}{\mu}\mathfrak{a} = \frac{1}{\mu'}\mathfrak{a}$.

Proof. If $\mu \sim_{\mathcal{O}^*} \mu'$, we have $\nu_{\mathfrak{p}}(\mu'\mu^{-1}\varepsilon) = 0$ for some $\varepsilon \in \mathcal{O}^*$ and all $\mathfrak{p} \in S$; but then, $\Psi(\mu) = \Psi(\mu') + \Psi(\varepsilon)$, whence $\psi(\mu) = \psi(\mu')$.

We have $\psi(\mu) = \psi(\mu')$ if, and only if, $\Psi(\mu) = \Psi(\mu') + \Psi(\varepsilon)$ for some $\varepsilon \in \mathcal{O}^*$. But this is equivalent to $\Psi(\mu^{-1}\mu'\varepsilon) = 0$, i.e. $\nu_{\mathfrak{p}}(\mu^{-1}\mu'\varepsilon) = 0$ for every $\mathfrak{p} \in S'$. If we can show $\nu_{\mathfrak{p}_{n+1}}(\mu^{-1}\mu'\varepsilon) = 0$, we get $\mu \sim_{\mathcal{O}^*} \mu'$. First, without loss of generality, we replace μ' by $\mu'\varepsilon$, i.e. we assume that $\varepsilon = 1$, i.e. that $\Psi(\mu) = \Psi(\mu')$.

Assume that $\nu_{\mathfrak{p}_{n+1}}(\mu) \leq \nu_{\mathfrak{p}_{n+1}}(\mu')$; otherwise, interchange μ and μ'. Then $|\mu|_{\mathfrak{p}_{n+1}} \geq |\mu'|_{\mathfrak{p}_{n+1}}$, whence $\mu' \in B(\mathfrak{a}, \nu) = C(\mathfrak{a}, \mu) \cup \{0\}$, i.e. we must have $|\mu|_{\mathfrak{p}} = |\mu'|_{\mathfrak{p}}$ for all $\mathfrak{p} \in S$, i.e. we have $\mu \sim_{\mathcal{O}^*} \mu'$.

The last statement follows from Lemma 3.6.4. □

Finally, we want to give an explicit criterion on how to decide whether $\mu \sim_{\mathcal{O}^*} \mu'$ which is based on the ideal representations of μ and μ':

Proposition 4.1.2. *Let $\mathfrak{b} \in \mathrm{Id}(\mathcal{O})$ and $\mu, \mu' \in \mathcal{E}(\mathfrak{b})$. Then the following conditions are equivalent:*

(i) *we have $\mu \sim_{\mathcal{O}^*} \mu'$;*

(ii) *for $\mathfrak{a} = \frac{1}{\mu}\mathfrak{b}$ and $\mathfrak{a}' = \frac{1}{\mu'}\mathfrak{b}$, we have $\mathfrak{a} \sim \mathfrak{a}'$;*

(iii) *for $\mathfrak{a} = \frac{1}{\mu}\mathfrak{b}$ and $\mathfrak{a}' = \frac{1}{\mu'}\mathfrak{b}$ we have that*

  (a) *$L(\mathrm{div}(\mathfrak{a}(\mathfrak{a}')^{-1})) = k^*h \cup \{0\}$ for some $h \in K^*$; and*
  (b) *$h\mathcal{O} = \mathfrak{a}(\mathfrak{a}')^{-1}$;*

(iv) *for $\mathfrak{a} = \frac{1}{\mu}\mathfrak{b}$ and $\mathfrak{a}' = \frac{1}{\mu'}\mathfrak{b}$ we have that*

  (a) *$L(\mathrm{div}(\mathfrak{a}(\mathfrak{a}')^{-1})) \neq \{0\}$; and*
  (b) *$\deg \mathrm{div}(\mathfrak{a}) = \deg \mathrm{div}(\mathfrak{a}')$;*

(v) *for* $\mathfrak{a} = \frac{1}{\mu}\mathfrak{b}$ *and* $\mathfrak{a}' = \frac{1}{\mu'}\mathfrak{b}$ *we have that* $\mathfrak{a}(\mathfrak{a}')^{-1} = h\mathcal{O}$ *for some* $h \in K^*$ *with* $|h|_{\mathfrak{p}} = 1$ *for every* $\mathfrak{p} \in S$.

Proof. First, by Lemma 3.6.4, (i) and (ii) are equivalent.

Assume (i), i.e. that there exists an $\varepsilon \in \mathcal{O}^*$ such that $\nu_{\mathfrak{p}}(\mu'\mu^{-1}\varepsilon) = 1$ for every $\mathfrak{p} \in S$. Then $\mathfrak{a}(\mathfrak{a}')^{-1} = \frac{\varepsilon\mu'}{\mu}\mathcal{O} = \frac{\mu'}{\mu}\mathcal{O}$. Now $\left|\varepsilon\mu'\mu^{-1}\right|_{\mathfrak{p}} = 1$ for every $\mathfrak{p} \in S$, whence $\frac{\varepsilon\mu'}{\mu} \in L(\operatorname{div}(\mathfrak{a}(\mathfrak{a}')^{-1}))$. Moreover, as $\mathcal{C}(\mathfrak{a}(\mathfrak{a}')^{-1}) = \mathcal{C}(\frac{\mu'}{\mu}\mathcal{O}) = \frac{\varepsilon\mu'}{\mu}\mathcal{C}(\mathcal{O})$, we have $L(\operatorname{div}(\mathfrak{a}(\mathfrak{a}')^{-1})) = k^*\frac{\varepsilon\mu'}{\mu} \cup \{0\}$ as $1 \in \mathcal{C}(\mathcal{O})$. This gives (iii).

Now assume (iii), i.e. $\mathfrak{a}(\mathfrak{a}')^{-1} = h\mathcal{O}$ and $L(\operatorname{div}(\mathfrak{a}(\mathfrak{a}')^{-1})) = k^*h \cup \{0\}$. The latter implies $|h|_{\mathfrak{p}} \leq 1$ for every $\mathfrak{p} \in S$. Now we have $h = \varepsilon\frac{\mu'}{\mu}$ for some $\varepsilon \in \mathcal{O}^*$; hence, we have $|\varepsilon\mu'|_{\mathfrak{p}} \leq |\mu|_{\mathfrak{p}}$ for every $\mathfrak{p} \in S$. As $\mu \in \mathcal{E}(\mathfrak{a})$ and $\varepsilon\mu' \in \mathfrak{a}$, we get $|\varepsilon\mu'|_{\mathfrak{p}} = |\mu|_{\mathfrak{p}}$ for all $\mathfrak{p} \in S$, i.e. $|h|_{\mathfrak{p}} = 1$ for every $\mathfrak{p} \in S$. This gives (v) and also (iv), as this implies that $\operatorname{div}(\mathfrak{a}) - \operatorname{div}(\mathfrak{a}') = \operatorname{div}(\mathfrak{a}(\mathfrak{a}')^{-1}) = (h^{-1})$ is principal and, thus, of degree zero.

Next, assume (iv). By hypothesis we have $\deg \operatorname{div}(\mathfrak{a}(\mathfrak{a}')^{-1}) = 0$, whence $L(\operatorname{div}(\mathfrak{a}(\mathfrak{a}')^{-1})) \neq \{0\}$ implies that $\operatorname{div}(\mathfrak{a}(\mathfrak{a}')^{-1})$ is principal. Hence, there exists some $h \in K^*$ with $\operatorname{div}(\mathfrak{a}(\mathfrak{a}')^{-1}) = (h^{-1})$. This gives $|h|_{\mathfrak{p}} = 1$ for every $\mathfrak{p} \in S$ and $\mathfrak{a}(\mathfrak{a}')^{-1} = h\mathcal{O}$, i.e. we have (v).

Now (v) clearly implies (ii), as $\mathfrak{a}(\mathfrak{a}')^{-1} = h\mathcal{O}$ is equivalent to $\mathfrak{a} = h\mathfrak{a}'$. □

We quickly get the following corollary:

Corollary 4.1.3. *Let* $\mathfrak{a}, \mathfrak{a}' \in \operatorname{Red}^{(b)}(K)$. *Then the following are equivalent:*

(i) *we have* $\mathfrak{a} \sim \mathfrak{a}'$;

(ii) *we have that*

  (a) $L(\operatorname{div}(\mathfrak{a}(\mathfrak{a}')^{-1})) = k^*h \cup \{0\}$ *for some* $h \in K^*$; *and*
  (b) $h\mathcal{O} = \mathfrak{a}(\mathfrak{a}')^{-1}$;

(iii) *we have that*

  (a) $L(\operatorname{div}(\mathfrak{a}(\mathfrak{a}')^{-1})) \neq \{0\}$; *and*
  (b) $\deg \operatorname{div}(\mathfrak{a}) = \deg \operatorname{div}(\mathfrak{a}')$;

(iv) *we have that* $\mathfrak{a}(\mathfrak{a}')^{-1} = h\mathcal{O}$ *for some* $h \in K^*$ *with* $|h|_{\mathfrak{p}} = 1$ *for every* $\mathfrak{p} \in S$.

Proof. Note that if $\mathfrak{a}$ and $\mathfrak{a}'$ are not in the same ideal class, conditions (i) to (iv) are all not satisfied. If $\mathfrak{a}$ and $\mathfrak{a}'$ are in the same ideal class, the equivalence of conditions (i) to (iv) follows from the previous proposition. □

4.2 Infrastructure for Global Fields

Recall the map

$$\Psi : K^* \to \mathbb{R}^{S'}, \qquad f \mapsto (-\nu_{\mathfrak{p}}(f))_{\mathfrak{p}\in S'}$$

defined at the beginning of this chapter; then we have that $\Lambda = \Psi(\mathcal{O}^*)$ is a full lattice in $\mathbb{R}^{S'}$. Fix an ideal $\mathfrak{a} \in \mathrm{Id}(\mathcal{O})$.

Lemma 4.2.1. *We have that* $\mathrm{Red}^{(b)}(\mathfrak{a})/_\sim$ *is finite and that the map*

$$d^{\mathfrak{a}} : \mathrm{Red}^{(b)}(\mathfrak{a})/_\sim \to \mathbb{R}^{S'}/\Lambda, \qquad [\tfrac{1}{\mu}\mathfrak{a}]_\sim \mapsto \Psi(\mu) + \Lambda$$

is injective.

Proof. The injectivity of this map is Lemma 4.1.1. If K is a number field, $\mathrm{Red}^{(b)}(\mathfrak{a})$ has the same number of elements as $\mathcal{E}(\mathfrak{a})/\mathcal{O}^*$ by Proposition 3.6.2 (b), and $[\mathcal{E}(\mathfrak{a}) : \mathcal{O}^*]$ is finite by Theorem 3.2.6.

If K is a function field, we have that the image of Ψ lies in $\mathbb{Z}^{S'}$. Hence, $\Lambda \subseteq \mathbb{Z}^{S'}$ and we see that the image of $d^{\mathfrak{a}}$ actually lies in the finite group $\mathbb{Z}^{S'}/\Lambda$. Therefore, as $d^{\mathfrak{a}}$ is injective, $\mathrm{Red}^{(b)}(\mathfrak{a})/_\sim$ must be finite. □

Therefore, defining $X := \mathrm{Red}^{(b)}(\mathfrak{a})/_\sim$ and $d := d^{\mathfrak{a}}$ almost gives an n-dimensional infrastructure (X, d); what is missing is a reduction map

$$\mathbb{R}^n/\Lambda \to X.$$

Recall that $\mathbb{G}$ denotes $\mathbb{R}$ if K is a number field and $\mathbb{Z}$ if a K is a function field. In the following, we will use $\mathbb{G}^n/\Lambda$ instead of $\mathbb{R}^n/\Lambda$ to avoid the handling of real numbers in the function field case, which simply have to be truncated. As explained in Remark 2.4.4, it suffices to find a reduction map $\mathbb{Z}^n/\Lambda \to X$ in the function field case.

For obtaining a reduction map, we start by introducing f-representations.

We define an order $<$ on K^* by

$$f < g :\Longleftrightarrow \begin{cases} (-\nu_{\mathfrak{p}_{n+1}}(f), -\nu_{\mathfrak{p}_1}(f), \ldots, -\nu_{\mathfrak{p}_n}(f)) \\ <_{\ell ex} (-\nu_{\mathfrak{p}_{n+1}}(f), -\nu_{\mathfrak{p}_1}(f), \ldots, -\nu_{\mathfrak{p}_n}(f)), \end{cases}$$

where $<_{\ell ex}$ is the usual lexicographic order defined on $\mathbb{R}^{n+1}$. This choice is rather random, but has the following, important property:

Remark 4.2.2. If μ is a smallest element in $B(\mathfrak{a}, (t_1, \ldots, t_n, t_{n+1})) \setminus \{0\}$ with respect to $<$, then μ is a minimum of type (b) of $\mathfrak{a}$.

Note that $<$ is the universal $\mathfrak{p}_{n+1}$-order defined in Example 3.5.3.

Definition 4.2.3. *A tuple* $([\mathfrak{b}]_\sim, (t_i)_{i=1,\dots,n}) \in \mathrm{Red}^{(b)}(\mathfrak{a})/_\sim \times \mathbb{G}^n$ *is called an* f-representation (of type (b)) *if* 1 *is a smallest element with respect to* $<$ *in* $B(\mathfrak{b}, (t_1, \dots, t_n, 0)) \setminus \{0\}$. *Denote the set of all these* f*-representations by* $\mathrm{Rep}^f(\mathfrak{a})$.

Remarks 4.2.4.

(a) Note that the condition on $B(\mathfrak{b}, (t_1, \dots, t_n, 0)) \setminus \{0\}$ does not depends on the representative $\mathfrak{b}$ of $[\mathfrak{b}]_\sim$, as every two representatives differ by a factor $h \in K^*$ with $|h|_\mathfrak{p} = 1$ for every $\mathfrak{p} \in S$. This implies that an element with a specific set of infinite valuations exists in $\mathfrak{b}$ if, and only if, such an element exists in a different representative $\mathfrak{b}'$.

(b) If $\deg \mathfrak{p}_{n+1} = 1$, then $([\mathfrak{b}_\sim], (t_i)_i)$ is an f-representation if, and only if,

$$B(\mathfrak{b}, (t_1, \dots, t_n, 0)) = k^* \cup \{0\}.$$

(c) Let $\mathfrak{b}$ be an arbitrary ideal and $(t_1, \dots, t_n) \in \mathbb{G}^n$, and assume that 1 is a smallest element with respect to $<$ in $B(\mathfrak{b}, (t_1, \dots, t_n, 0)) \setminus \{0\}$. The condition $1 \in B(\mathfrak{b}, (t_1, \dots, t_n, 0))$ implies $t_1 \geq 0$, $\dots$, $t_n \geq 0$, and that it is a smallest element implies $1 \in \mathcal{E}(\mathfrak{b})$ by Remark 4.2.2, i.e. that $\mathfrak{b}$ is reduced of type (b).

(d) If $\mathfrak{a} \in \mathrm{Red}^{(b)}(\mathfrak{a})$, then $(\mathfrak{a}, (0)_i) \in \mathrm{Rep}^f(\mathfrak{a})$.

Before we start investigating the infrastructure, we need two auxiliary lemmas on f-representations. The first one will give the injectivity of certain maps.

Lemma 4.2.5 (Uniqueness). *Let* $([\mathfrak{b}]_\sim, (t_i)_i) \in \mathrm{Rep}^f(\mathfrak{a})$ *and* $f \in K^*$ *such that*

$$([\tfrac{1}{f}\mathfrak{b}]_\sim, (t_i + \nu_{\mathfrak{p}_i}(f))_i) \in \mathrm{Rep}^f(\mathfrak{a}).$$

Then $|f|_\mathfrak{p} = 1$ *for every* $\mathfrak{p} \in S$, *i.e.* $([\mathfrak{b}]_\sim, (t_i)_i) = ([\tfrac{1}{f}\mathfrak{b}]_\sim, (t_i + \nu_{\mathfrak{p}_i}(f))_i)$.

Proof. If $\frac{1}{f}\mathfrak{b}$ is reduced of type (b), we have $1 \in \frac{1}{f}\mathfrak{b}$, i.e. $f \in \mathfrak{b}$. As $1 \in B(\frac{1}{f}\mathfrak{b}, (t_1 + \nu_{\mathfrak{p}_1}(f), \dots, t_n + \nu_{\mathfrak{p}_n}(f), 0))$, we have $t_i + \nu_{\mathfrak{p}_i}(f) \geq 0$, i.e. $\nu_{\mathfrak{p}_i}(f) \geq -t_i$. Hence, $f \in B(\mathfrak{b}, (t_1, \dots, t_n, -\nu_{\mathfrak{p}_{n+1}}(f)))$.

Now, that 1 is a smallest element in $B(\mathfrak{b}, (t_1, \ldots, t_n, 0)) \setminus \{0\}$ with respect to $<$ means it is also a smallest element in

$$B(\mathfrak{b}, (t_1, \ldots, t_n, \max\{0, -\nu_{\mathfrak{p}_{n+1}}(f)\})),$$

whence $1 \leq f$. This means $0 \leq -\nu_{\mathfrak{p}_{n+1}}(f)$, i.e.

$$1 \in B(\mathfrak{b}, (t_1, \ldots, t_n, -\nu_{\mathfrak{p}_{n+1}}(f))).$$

But then, $\frac{1}{f}$ is a smallest element with respect to $<$ in

$$\begin{aligned} &\tfrac{1}{f} B(\mathfrak{b}, (t_1, \ldots, t_n, -\nu_{\mathfrak{p}_{n+1}}(f))) \setminus \{0\} \\ &= B\big(\tfrac{1}{f}\mathfrak{b}, (t_1 + \nu_{\mathfrak{p}_1}(f), \ldots, t_n + \nu_{\mathfrak{p}_n}(f), 0)\big) \setminus \{0\}, \end{aligned}$$

but so is 1, whence $|f|_{\mathfrak{p}} = |1|_{\mathfrak{p}} = 1$ for every $\mathfrak{p} \in S$. □

The second lemma is a "reduction lemma", which we will need at several places, mainly for showing surjectivity of certain maps. In the case of imaginary (hyper-)elliptic function fields, this is exactly the usual reduction, as it is in the case of superelliptic curves [GPS02]. F. Heß used the same reduction, along an arbitrary, but fixed rational place, to describe general arithmetic in global function fields having a rational place [Hes02].

Lemma 4.2.6 (Reduction). *Let $\mathfrak{b} \in \mathfrak{a}\,\mathrm{PId}(\mathcal{O})$ and $(t_i)_i \in \mathbb{G}^n$. Then there exists a minimal $\ell \in \mathbb{G}$ with $B(\mathfrak{b}, (t_1, \ldots, t_n, \ell)) \neq \{0\}$ and an element μ minimal with respect to $<$ in $B(\mathfrak{b}, (t_1, \ldots, t_n, \ell)) \setminus \{0\}$. Moreover, $\nu_{\mathfrak{p}}(\mu) = -\ell$ and we have*

$$([\tfrac{1}{\mu}\mathfrak{b}]_{\sim}, (t_1 + \nu_{\mathfrak{p}_1}(\mu), \ldots, t_n + \nu_{\mathfrak{p}_n}(\mu))) \in \mathrm{Rep}^f(\mathfrak{a}).$$

Finally, this f-representation does not depends on the choice of μ.

Proof. First, by Riemann's Inequality or Minkowski's Lattice Point Theorem, $B_\ell := B(\mathfrak{b}, (t_1, \ldots, t_n, \ell)) \neq \{0\}$ for large enough ℓ. If K is a number field, B_ℓ is a finite set, whence the existence of ℓ is clear. If K is a function field, $B_\ell = L(D_\ell)$ for some divisor D_ℓ whose degree decreases with ℓ (see Section 3.1); hence, $B_\ell = \{0\}$ for $\ell \ll 0$. Therefore, there exists a minimal $\ell \in \mathbb{Z}$ with $B_\ell \neq \{0\}$.

Clearly, μ exists: in the number field case, B_ℓ is a finite set, and in the function field case, $\dim B_\ell \leq \deg \mathfrak{p}_{n+1}$ and the elements in B_ℓ have only finitely many different infinite valuations.

Finally,

$$\begin{aligned} &B(\tfrac{1}{\mu}\mathfrak{b}, (t_1 + \nu_{\mathfrak{p}_1}(\mu), \ldots, t_n + \nu_{\mathfrak{p}_n}(\mu), 0)) \\ = &\tfrac{1}{\mu} B(\mathfrak{b}, (t_1, \ldots, t_n, -\nu_{\mathfrak{p}_{n+1}}(\mu))) = \tfrac{1}{\mu} B_\ell, \end{aligned}$$

which shows that $1 = \frac{\mu}{\mu}$ is minimal with respect to $<$ in $\frac{1}{\mu}B_\ell$, i.e. that $([\frac{1}{\mu}\mathfrak{b}]_\sim, (t_1 + \nu_{\mathfrak{p}_1}(\mu), \ldots, t_n + \nu_{\mathfrak{p}_n}(\mu))) \in \mathrm{Rep}^f(\mathfrak{a})$. The uniqueness follows from Lemma 4.2.5. □

We begin with investigating the classical infrastructure located inside one ideal class.

The following proposition shows that in the case of the infrastructure inside one ideal class, one gets a bijection between $\mathrm{Rep}^f(\mathfrak{b})$ and $\mathbb{G}^n/\Lambda$, as in Proposition 2.2.3:

Proposition 4.2.7 (Infrastructure, Part I). *We have that*

$$d^{\mathfrak{a}} : \mathrm{Rep}^f(\mathfrak{a}) \to \mathbb{G}^n/\Lambda, \qquad ([\tfrac{1}{\mu}\mathfrak{a}]_\sim, (t_i)_i) \mapsto \Psi(\mu) + (t_i)_i + \Lambda$$

is a bijection.

Note that T from the diagram in Section 1.1 injects naturally into $\mathbb{G}^n/\Lambda$; in the function field case, its image is the subgroup

$$\left\{ (t_1, \ldots, t_n) + \Lambda \;\middle|\; \deg \mathfrak{p}_{n+1} \text{ divides } \sum_{i=1}^{n} t_i \deg \mathfrak{p}_i \right\},$$

while in the number field case, the image is the whole of $\mathbb{G}^n/\Lambda$.

Proof. Surjectivity follows directly from Lemma 4.2.6, as

$$d^{\mathfrak{b}}([\tfrac{1}{\mu}\mathfrak{a}]_\sim, (t_i + \nu_{\mathfrak{p}_i}(\mu))_i) = (t_i)_i + \Lambda.$$

For injectivity, let $([\mathfrak{b}]_\sim, (t_i)_i), ([\mathfrak{b}']_\sim, (s_i)_i) \in \mathrm{Rep}^f(\mathfrak{a})$ with

$$d^{\mathfrak{b}}([\mathfrak{b}]_\sim, (t_i)_i) = d^{\mathfrak{b}}([\mathfrak{b}']_\sim, (s_i)_i).$$

Write $\mathfrak{b} = \frac{1}{\mu}\mathfrak{a}$ and $\mathfrak{b}' = \frac{1}{\mu'}\mathfrak{a}$; then

$$\Psi(\mu) - \Psi(\mu') + (t_i)_i - (s_i)_i \in \Lambda.$$

Hence, there exists a unit $\varepsilon \in \mathcal{O}^*$ with $\Psi(\varepsilon) = \Psi(\frac{\mu}{\mu'}) + (t_i - s_i)_i$. Define $f := \frac{\mu'}{\mu}\varepsilon$; then, $\Psi(f) = -\Psi(\frac{\mu}{\mu'}) + \Psi(\varepsilon) = (t_i - s_i)_i$ and, hence,

$$([\tfrac{1}{f}\mathfrak{b}]_\sim, (t_i)_i - \Psi(f)) = ([\tfrac{\mu}{\mu'}\varepsilon^{-1} \cdot \tfrac{1}{\mu}\mathfrak{a}]_\sim, (t_i)_i + (s_i - t_i)_i) = ([\mathfrak{b}']_\sim, (s_i)_i).$$

Hence, by Lemma 4.2.5, $|f|_\mathfrak{p} = 1$ for every $\mathfrak{p} \in S$, which implies that $[\mathfrak{b}]_\sim = [\frac{1}{f}\mathfrak{b}]_\sim = [\mathfrak{b}']_\sim$ and $\Psi(f) = 0$, i.e. $t_i = s_i$. □

In particular, we get a reduction map

$$red^\mathfrak{a} : \mathbb{G}^n/\Lambda \to \mathrm{Red}^{(b)}(\mathfrak{a})/_\sim, \qquad v \mapsto \pi_1((d^\mathfrak{a})^{-1}(v)),$$

where $\pi_1 : \mathrm{Rep}^f(\mathfrak{a}) \to \mathrm{Red}^{(b)}(\mathfrak{a})/_\sim$ is the projection on the first component.

Therefore, we turned $(X, d^\mathfrak{a})$ into an n-dimensional infrastructure $(X, d^\mathfrak{a}, red^\mathfrak{a})$. In the case $\mathfrak{a} = \mathcal{O}$, we can describe how to compute giant steps; this will be done at the end of the next section.

4.3 The Infrastructure and the Picard Group

Assume for a moment that K is a number field or that $\gcd(\deg \mathfrak{p} \mid \mathfrak{p} \in S) = \gcd(\deg \mathfrak{p} \mid \mathfrak{p} \in \mathcal{P}_K)$. Consider the short exact sequence

$$0 \longrightarrow T \longrightarrow \mathrm{Pic}^0(K) \longrightarrow \mathrm{Pic}(\mathcal{O}) \longrightarrow 0.$$

This shows that $\mathrm{Pic}^0(K)$ is covered by $|\mathrm{Pic}(\mathcal{O})|$ copies of T. As T can be embedded into $\mathbb{G}^n/\Lambda$, which can be covered by all reduced ideals of type (b) inside one (fixed) ideal class in $\mathrm{Pic}(\mathcal{O})$ together with some information for the places at infinity, one can ask whether one could cover the whole of $\mathrm{Pic}^0(K)$ with f-representations. In the case of real hyperelliptic function fields, this has been done by S. Paulus and H.-G. Rück in [PR99]; considering the whole of $\mathrm{Pic}^0(K)$ (or, more precisely, a cover of $\mathrm{Pic}^0(K)$) has also been done by R. Schoof in the case of number fields [Sch08].

Moreover, we want to use all of $\mathbb{G}^n/\Lambda$ and not simply the (possibly proper) subset which corresponds to T, and we do not want the restriction $\gcd(\deg \mathfrak{p} \mid \mathfrak{p} \in S) = \gcd(\deg \mathfrak{p} \mid \mathfrak{p} \in \mathcal{P}_K)$. Note that T corresponds to a proper subset of $\mathbb{G}^n/\Lambda$ if, and only if, K is a function field and $\deg \mathfrak{p}_{n+1} > \gcd(\deg \mathfrak{p} \mid \mathfrak{p} \in S)$. In case K is a function field and $\deg \mathfrak{p}_{n+1} > \gcd(\deg \mathfrak{p} \mid \mathfrak{p} \in \mathcal{P}_K)$, it turns out that we must enlarge $\mathrm{Pic}^0(K)$.

Note that we have an exact sequence

$$0 \longrightarrow \mathrm{Pic}^0(K) \longrightarrow \mathrm{Pic}(K) \longrightarrow \mathbb{G} \longrightarrow 0,$$

where the map $\mathrm{Pic}(K) \to \mathbb{G}$ is given by deg if K is a number field and $\frac{1}{d}\deg$ with $d = \gcd(\deg \mathfrak{p} \mid \mathfrak{p} \in \mathcal{P}_K)$ if K is a function field.

Definition 4.3.1. *Define* $\mathrm{Rep}^f(K) := \bigcup_{\mathfrak{a} \in \mathrm{Id}(\mathcal{O})} \mathrm{Rep}^f(\mathfrak{a})$.

Proposition 4.3.2 (Infrastructure, Part II).

(a) *If K is a number field, the map*

$$\begin{aligned} \Phi : \mathrm{Rep}^f(K) &\to \mathrm{Pic}^0(K) \\ ([\mathfrak{a}]_\sim, (t_i)_i) &\mapsto \left[\mathrm{div}(\mathfrak{a}) + \sum_{i=1}^n t_i \mathfrak{p}_i - \frac{\deg \mathrm{div}(\mathfrak{a}) + \sum_{i=1}^n t_i \deg \mathfrak{p}_i}{\deg \mathfrak{p}_{n+1}} \mathfrak{p}_{n+1}\right] \end{aligned}$$

is a bijection.

(b) *If K is a function field, the map*

$$\begin{aligned} \Phi : \mathrm{Rep}^f(K) &\to \mathrm{Pic}(K)/\langle [\mathfrak{p}_{n+1}] \rangle, \\ ([\mathfrak{a}]_\sim, (t_i)_i) &\mapsto \left[\mathrm{div}(\mathfrak{a}) + \sum_{i=1}^n t_i \mathfrak{p}_i\right] \end{aligned}$$

is a bijection. Moreover, $\Phi^{-1}(\mathrm{Pic}^0(K))$ is given by

$$\left\{ ([\mathfrak{a}]_\sim, (t_i)_i) \in \mathrm{Rep}^f(K) \;\middle|\; \deg \mathfrak{p}_{n+1} \text{ divides } \deg \mathrm{div}(\mathfrak{a}) + \sum_{i=1}^n t_i \deg \mathfrak{p}_i \right\}.$$

In particular, if $\deg \mathfrak{p}_{n+1} = \gcd(\deg \mathfrak{p} \mid \mathfrak{p} \in \mathcal{P}_K)$, we have that Φ is a bijection $\mathrm{Rep}^f(K) \to \mathrm{Pic}^0(K)$.

Remark 4.3.3. In the function field case, the sequence

$$0 \longrightarrow T \longrightarrow \mathrm{Pic}^0(K) \longrightarrow \mathrm{Pic}(\mathcal{O}) \longrightarrow 0$$

is in general not right-exact. The proposition shows that if one replaces $\mathrm{Pic}^0(K)$ by $\mathrm{Pic}(K)/\langle [\mathfrak{p}_{n+1}] \rangle$ and T by $\mathbb{G}^n/\Lambda$, one obtains a short exact sequence

$$0 \longrightarrow \mathbb{G}^n/\Lambda \longrightarrow \mathrm{Pic}(K)/\langle [\mathfrak{p}_{n+1}] \rangle \longrightarrow \mathrm{Pic}(\mathcal{O}) \longrightarrow 0$$

which can be interpreted as the "right" generalization to make the map to $\mathrm{Pic}(\mathcal{O})$ surjective.

Proof of Proposition 4.3.2. By ignoring the valuations at $\mathfrak{p}_{n+1}$, we can consider both cases at the same time. One quickly sees that Φ is well-defined.

To see that Φ is surjective, let $[D]$ be a divisor class in $\mathrm{Pic}^0(K)$ respectively $\mathrm{Pic}(K)/\langle[\mathfrak{p}_{n+1}]\rangle$. Then there exists an $\mathfrak{a} \in \mathrm{Id}(\mathcal{O})$ and $t_1, \ldots, t_n, \ell \in \mathbb{G}$ with $D = \mathrm{div}(\mathfrak{a}) + \sum_{i=1}^n t_i\mathfrak{p}_i + \ell\mathfrak{p}_{n+1}$. By Lemma 4.2.6, there exists an element $\mu \in \mathfrak{a}$ with $([\frac{1}{\mu}\mathfrak{a}]_\sim, (s_i)_i) \in \mathrm{Rep}^f(K)$ for $s_i := t_i + \nu_{\mathfrak{p}_i}(\mu)$. Now, ignoring $\mathfrak{p}_{n+1}$,

$$\Phi([\tfrac{1}{\mu}\mathfrak{a}]_\sim, (s_i)_i) = \left[\mathrm{div}(\mathfrak{a}) + \sum_{i=1}^n t_i\mathfrak{p}_i + (\mu)_{finite} + \sum_{i=1}^n \nu_{\mathfrak{p}_i}(\mu)\mathfrak{p}_i\right],$$

and

$$(\mu)_{finite} + \sum_{i=1}^n \nu_{\mathfrak{p}_i}(\mu)\mathfrak{p}_i = (\mu) - \nu_{\mathfrak{p}_{n+1}}(\mu)\mathfrak{p}_{n+1}.$$

This shows that $\Phi([\frac{1}{\mu}\mathfrak{a}]_\sim, (s_i)_i) = [D]$.

For injectivity, let $([\mathfrak{a}]_\sim, (t_i)_i), ([\mathfrak{a}']_\sim, (s_i)_i) \in \mathrm{Rep}^f(K)$ with

$$\Phi([\mathfrak{a}]_\sim, (t_i)_i) = \Phi([\mathfrak{a}']_\sim, (s_i)_i),$$

i.e. $\mathrm{div}(\mathfrak{a}) + \sum_{i=1}^n t_i\mathfrak{p}_i = \mathrm{div}(\mathfrak{a}') + \sum_{i=1}^n s_i\mathfrak{p}_i + (f) + \ell\mathfrak{p}_{n+1}$ for some $f \in K^*$ and $\ell \in \mathbb{G}$. Now

$$\mathrm{div}(\mathfrak{a}') + \sum_{i=1}^n s_i\mathfrak{p}_i + (f) = \mathrm{div}(\tfrac{1}{f}\mathfrak{a}') + \sum_{i=1}^n (s_i + \nu_{\mathfrak{p}_i}(f))\mathfrak{p}_i + \nu_{\mathfrak{p}_{n+1}}(f)\mathfrak{p}_{n+1},$$

whence this means that $\mathfrak{a} = \frac{1}{f}\mathfrak{a}'$ and $t_i = s_i + \nu_{\mathfrak{p}_i}(f)$, $1 \le i \le n$. Therefore, by Lemma 4.2.5, $|f|_\mathfrak{p} = 1$ for every $\mathfrak{p} \in S$, which implies that $[\mathfrak{a}]_\sim = [\frac{1}{f}\mathfrak{a}']_\sim = [\mathfrak{a}']_\sim$ and $t_i = s_i$, $1 \le i \le n$.

Finally, let K be a function field and denote the set in part (b) of the claim by X; we have to show $\Phi^{-1}(\mathrm{Pic}^0(K)) = X$. This follows from the fact that $\deg : \mathrm{Pic}(K) \to \mathbb{Z}$ induces a map

$$d : \mathrm{Pic}(K)/\langle[\mathfrak{p}_{n+1}]\rangle \to \mathbb{Z}/(\deg \mathfrak{p}_{n+1})\mathbb{Z},$$

and we see that $d(\Phi([\mathfrak{a}]_\sim, (t_i)_i)) = \deg \mathrm{div}(\mathfrak{a}) + \sum_{i=1}^n t_i \deg \mathfrak{p}_i + (\deg \mathfrak{p}_{n+1})\mathbb{Z}$. As $\ker d = \mathrm{Pic}^0(K)$, we see that $\Phi([\mathfrak{a}]_\sim, (t_i)_i) \in \mathrm{Pic}^0(K)$ if, and only if, $\deg \mathrm{div}(\mathfrak{a}) + \sum_{i=1}^n t_i \deg \mathfrak{p}_i \in (\deg \mathfrak{p}_{n+1})\mathbb{Z}$. □

Finally, as Paulus and Rück did in the real hyperelliptic function field case, we can describe the operations induced by the ones in $\mathrm{Pic}^0(K)$ respectively $\mathrm{Pic}(K)/\langle[\mathfrak{p}_{n+1}]\rangle$ on $\mathrm{Rep}^f(K)$:

Proposition 4.3.4 (Infrastructure, Part III). *Let* $([\mathfrak{a}]_\sim, (t_i)_i), ([\mathfrak{a}']_\sim, (s_i)_i) \in \mathrm{Rep}^f(K)$. *Let* Φ *be a bijection from the previous proposition.*

(a) *Consider* $B_\ell := B(\mathfrak{a}\mathfrak{a}', (t_1 + s_1, \ldots, t_n + s_n, \ell)) \setminus \{0\}$, $\ell \in \mathbb{G}$. *Then there exists a minimal* $\ell \in \mathbb{G}$ *with* $B_\ell \neq \emptyset$. *If* $f \in B_\ell$ *is minimal with respect to* $<$ *for the minimal* ℓ *with* $B_\ell \neq \emptyset$, *define* $\mathfrak{a}'' := \frac{1}{f}\mathfrak{a}\mathfrak{a}'$ *and* $u_i := t_i + s_i + \nu_{\mathfrak{p}_i}(f)$. *Then* $([\mathfrak{a}'']_\sim, (u_i)_i) \in \mathrm{Rep}^f(K)$ *and*

$$\Phi([\mathfrak{a}'']_\sim, (u_i)_i) = \Phi([\mathfrak{a}]_\sim, (t_i)_i) + \Phi([\mathfrak{a}']_\sim, (s_i)_i).$$

(b) *Consider* $B_\ell := B(\mathfrak{a}^{-1}, (-t_1, \ldots, -t_n, \ell)) \setminus \{0\}$, $\ell \in \mathbb{G}$. *Then there exists a minimal* $\ell \in \mathbb{G}$ *with* $B_\ell \neq \emptyset$. *If* $f \in B_\ell$ *is minimal with respect to* $<$ *for the minimal* ℓ *with* $B_\ell \neq \emptyset$, *define* $\mathfrak{a}''' := \frac{1}{f}\mathfrak{a}^{-1}$ *and* $v_i := -t_i + \nu_{\mathfrak{p}_i}(f)$. *Then* $([\mathfrak{a}''']_\sim, (v_i)_i) \in \mathrm{Rep}^f(K)$ *and*

$$\Phi([\mathfrak{a}''']_\sim, (v_i)_i) = -\Phi([\mathfrak{a}]_\sim, (t_i)_i).$$

Proof. The existence of ℓ and μ and that

$$([\mathfrak{a}'']_\sim, (u_i)_i), ([\mathfrak{a}''']_\sim, (v_i)_i) \in \mathrm{Rep}^f(K)$$

follows from Lemma 4.2.6. The equalities under Φ follow from the definition of Φ and the arithmetic in $\mathrm{Pic}^0(K)$ respectively $\mathrm{Pic}(K)/\langle[\mathfrak{p}_{n+1}]\rangle$. □

One main consequence of this is that we get an effectively computable giant step operation for the principal ideal infrastructure $(\mathrm{Red}^{(b)}(\mathcal{O})/_\sim, d^{\mathcal{O}}, red^{\mathcal{O}})$, as $\mathbb{G}^n/\Lambda \cong \mathrm{Rep}^f(\mathcal{O})$ is a subgroup of $\mathrm{Pic}^0(K)$ in the number field case respectively $\mathrm{Pic}(K)/\langle[\mathfrak{p}_{n+1}]\rangle$ in the function field case.

We want to note that basically, this arithmetic in $\mathrm{Pic}^0(K)$—at least in the function field case where $\deg \mathfrak{p}_{n+1} = 1$—has already been described by F. Heß [Hes02], without any reference to the infrastructure: if, in his case, the divisor A equals a place of degree one in S, the ideal corresponding to the finite part of an A-reduced divisor is a type (c) reduced ideal $\mathfrak{a}$ in our sense, and the ideal corresponding to the infinite part encodes exactly the t_i's of an f-representation $([\mathfrak{a}]_\sim, (t_i)_i)$ in our sense.

The advantage of our approach over the one by F. Heß is that we do not need to store and multiply an ideal in $\mathcal{O}_\infty = \bigcap_{\mathfrak{p}\in S} \mathcal{O}_\mathfrak{p}$ which is rather slow, but use the fact that $\mathcal{O}_\infty$ is a principal ideal domain and that we know generators of the prime ideals to replace the ideal by its prime ideal power representation and to find an explicit representation when needed. Hence, in case one of the places in S has degree one and small generators of the

prime ideals at infinity are known, we expect our method to be slightly faster than the method of F. Heß, which is, for example, implemented in MAGMA [BCP97] and KANT[1]. However, it seems that the most expensive part in the method of F. Heß is the actual call to the lattice reduction algorithm (as described, for example, in [Pau98]) and not ideal arithmetic, whence this speed-up is probably only minimal or even negligible. An explicit way to compute using this possible speed-up is explained in Chapter 5.

A third approach would be to store a generator of the principal ideal of $\mathcal{O}_\infty$ instead of the ideal or the prime ideal exponents; in that case, there is no need to evaluate valuations when reducing, because the valuations itself are not needed. The main disadvantage of this approach is that there is no unique way to represent this element and, even worse, there is no way to bound its coefficients as it can be multiplied by any element of

$$\{f \in K^* \mid \nu_\mathfrak{p}(f) = 0 \text{ for all } \mathfrak{p} \in S\}$$

without changing the represented element of $\mathrm{Pic}^0(K)$. Hence, this approach appears not to be of any interest in practice.

4.4 Size of f-Representations

In this section, we want to estimate certain properties of f-representations. We begin with the following proposition:

Proposition 4.4.1. *Let* $([\mathfrak{a}]_\sim, (f_i)_i) \in \mathrm{Rep}^f(K)$. *Then* $\mathrm{div}(\mathfrak{a}) \geq 0$ *and* $f_i \geq 0$ *for* $1 \leq i \leq n$. *If* K *is a function field of genus* g, *we have*

$$0 \leq \deg \mathrm{div}(\mathfrak{a}) + \sum_{i=1}^{n} f_i \deg \mathfrak{p}_i \leq g + (\deg \mathfrak{p}_{n+1} - 1).$$

If K *is a number field with the discriminant of* $\mathcal{O}$ *being* Δ *and* K *having* r *real embeddings and* $2s$ *complex embeddings, then*

$$0 \leq \deg \mathrm{div}(\mathfrak{a}) + \sum_{i=1}^{n} f_i \deg \mathfrak{p}_i \leq s \log \tfrac{2}{\pi} + \tfrac{1}{2} \log |\Delta|.$$

Note that in [Neu99, p. 214, Definition 3.5], the genus of the number field K is defined as

$$g = \log \frac{|k^*| \sqrt{|\Delta|}}{2^r (2\pi)^s} = (s \log \tfrac{2}{\pi} + \tfrac{1}{2} \log |\Delta|) + (\log |k^*| - [K : \mathbb{Q}] \log 2),$$

[1] See `http://www.math.tu-berlin.de/~kant/kash.html`.

where K has r embeddings into $\mathbb{R}$ and $2s$ embeddings into $\mathbb{C}$ and $\Delta \in \mathbb{Z}$ is the discriminant of $\mathcal{O}$. In the function field case, we can also consider the discriminant $\Delta \in k[x]$ of $\mathcal{O}$. In that case, we have (see [Ros02, p. 85, Proposition 7.9 (ii)] and [Sti93, p. 89, Theorem III.5.1 and p. 88, Theorem III.4.12])

$$\begin{aligned} g &= \tfrac{1}{2}\deg\Delta + 1 - \tfrac{1}{2}[K : k(x)] + \tfrac{1}{2}\sum_{\mathfrak{p}\in S}\deg\mathfrak{p} \\ &= \tfrac{1}{2}\deg\Delta + 1 - \tfrac{1}{2}\sum_{\mathfrak{p}\in S}(e_{\mathfrak{p}} - 1)\deg\mathfrak{p}, \end{aligned}$$

where $e_{\mathfrak{p}}$ is the ramification index of $\mathfrak{p}$ over the infinite place of $k(x)$. Note that $\log_q|\Delta| = \deg\Delta$; hence, both bounds are very similar in nature.

Proof of Proposition 4.4.1. Let $D = \operatorname{div}(\mathfrak{a}) + \sum_{i=1}^{n} f_i\mathfrak{p}_i$. Then

$$L(D) = B(\mathfrak{a}, (f_1, \ldots, f_n, 0)) \supseteq k$$

and

$$L(D - \varepsilon\mathfrak{p}_{n+1}) = B(\mathfrak{a}, (f_1, \ldots, f_n, -\varepsilon)) = \{0\}$$

for $\varepsilon \in \mathbb{G}$, $\varepsilon > 0$. The inclusion shows $D \geq 0$ as $1 \in k$, whence $\operatorname{div}(\mathfrak{a}) \geq 0$ and $f_i \geq 0$, $1 \leq i \leq n$.

If K is a function field of genus g, by Riemann's Inequality,

$$\begin{aligned} 0 = \dim L(D - \mathfrak{p}_{n+1}) &\geq 1 - g + \deg(D - \mathfrak{p}_{n+1}) \\ &= 1 - g + \deg\operatorname{div}(\mathfrak{a}) + \sum_{i=1}^{n} f_i\deg\mathfrak{p}_i - \deg\mathfrak{p}_{n+1}, \end{aligned}$$

whence $\deg\operatorname{div}(\mathfrak{a}) + \sum_{i=1}^{n} f_i\deg\mathfrak{p}_i \leq g - 1 + \deg\mathfrak{p}_{n+1}$.

If K is a number field with signature (r, s) and Δ is the discriminant of $\mathcal{O}$, we would have that $B(\mathfrak{a}, (f_1, \ldots, f_n, -\varepsilon)) \neq \{0\}$ for $\varepsilon > 0$ if

$$e^{-\varepsilon\deg\mathfrak{p}_{n+1}}\prod_{i=1}^{n} e^{f_i\deg\mathfrak{p}_i} > \left(\tfrac{2}{\pi}\right)^s\sqrt{|\Delta|}N(\mathfrak{a})$$

by Minkowski's Lattice Point Theorem [Neu99, p. 32, Theorem 5.3]. Hence, we must have

$$e^{\sum_{i=1}^{n} f_i\deg\mathfrak{p}_i - \varepsilon\deg\mathfrak{p}_{n+1}} \leq \left(\tfrac{2}{\pi}\right)^s\sqrt{|\Delta|}e^{-\deg\operatorname{div}(\mathfrak{a})}.$$

Therefore,

$$\deg \operatorname{div}(\mathfrak{a}) + \sum_{i=1}^{n} f_i \deg \mathfrak{p}_i \leq \varepsilon \deg \mathfrak{p}_{n+1} + s \log \tfrac{2}{\pi} + \tfrac{1}{2} \log |\Delta|$$

for all $\varepsilon > 0$, whence $\deg \operatorname{div}(\mathfrak{a}) + \sum_{i=1}^{n} f_i \deg \mathfrak{p}_i \leq s \log \frac{2}{\pi} + \frac{1}{2} \log |\Delta|$. □

In the function field case, this allows us to give bounds on the set of reduced ideals with respect to the regulator

$$R = |T| \cdot \frac{\prod_{\mathfrak{p} \in S} \deg \mathfrak{p}}{\gcd(\deg \mathfrak{p} \mid \mathfrak{p} \in S)} = |\mathbb{Z}^n / \Lambda| \cdot \prod_{i=1}^{n} \deg \mathfrak{p}_i,$$

similarly to the results in [Sch08, Section 7] and [Buc87b] for the number field case.

Corollary 4.4.2. *Let K be a function field of genus g. Then*

$$\begin{aligned} &\frac{R}{\prod_{\mathfrak{p} \in S} \deg \mathfrak{p}} \cdot \frac{(|S|-1)!}{(g + \deg \mathfrak{p}_{n+1} + |S| - 2)^{|S|-1}} \\ &\leq \frac{R}{\binom{g+\deg \mathfrak{p}_{n+1}+|S|-2}{g+\deg \mathfrak{p}_{n+1}-1} \prod_{\mathfrak{p} \in S} \deg \mathfrak{p}} \leq |\operatorname{Red}(\mathfrak{a})/\!\sim| \leq \frac{R}{\prod_{\mathfrak{p} \in S} \deg \mathfrak{p}}. \end{aligned}$$

Moreover, if k is a finite field of q elements, then

$$\begin{aligned} &\frac{(\sqrt{q}-1)^{2g} \cdot (|S|-1)!}{(g + \deg \mathfrak{p}_{n+1} + |S| - 2)^{|S|-1}} \\ &\leq \frac{(\sqrt{q}-1)^{2g}}{\binom{g+\deg \mathfrak{p}_{n+1}+|S|-2}{g+\deg \mathfrak{p}_{n+1}-1}} \leq \frac{|\operatorname{Red}(K)/\!\sim|}{\deg \mathfrak{p}_{n+1}} \leq (\sqrt{q}+1)^{2g}. \end{aligned}$$

Proof. Elementary combinatorics shows that the set

$$\left\{ (x_1, \ldots, x_n) \in \mathbb{N}^n \;\middle|\; \sum_{i=1}^{n} x_i \leq g + \deg \mathfrak{p}_{n+1} - 1 \right\}$$

has $\sum_{i=0}^{g+\deg \mathfrak{p}_{n+1}-1} \binom{n+i-1}{i} = \binom{n+g+\deg \mathfrak{p}_{n+1}-1}{g+\deg \mathfrak{p}_{n+1}-1}$ elements. Hence, every equivalence class of reduced ideals appears in at least one and at most

$$\binom{g + \deg \mathfrak{p}_{n+1} + |S| - 2}{g + \deg \mathfrak{p}_{n+1} - 1}$$

f-representations. The first claim follows with Proposition 4.2.7 and the facts that $|\mathbb{Z}^n/\Lambda| \cdot \prod_{i=1}^n \deg \mathfrak{p}_i = R$ and that

$$\binom{g + \deg \mathfrak{p}_{n+1} + |S| - 2}{g + \deg \mathfrak{p}_{n+1} - 1} \leq \frac{(g + \deg \mathfrak{p}_{n+1} + |S| - 2)^{|S|-1}}{(|S|-1)!},$$

whence

$$\frac{1}{\binom{g+\deg \mathfrak{p}_{n+1}+|S|-2}{g}} \geq \frac{(|S|-1)!}{(g + \deg \mathfrak{p}_{n+1} + |S| - 2)^{|S|-1}}.$$

For the second claim, one gets a bijection $\mathrm{Rep}^f(K) \cong \mathrm{Pic}(K)/\langle [\mathfrak{p}_{n+1}] \rangle$ by Proposition 4.3.2. Now $\gcd(\deg \mathfrak{p} \mid \mathfrak{p} \in \mathcal{P}_K) = 1$ by [Sti93, p. 164, Corollary V.1.11] as k is finite, whence $|\mathrm{Pic}(K)/\langle [\mathfrak{p}_{n+1}] \rangle| = \left|\mathrm{Pic}^0(K)\right| \cdot \deg \mathfrak{p}_{n+1}$. Finally, by the Hasse-Weil bounds [Lor96, p. 287, Corollary 6.3 and Remark 6.4], $(\sqrt{q}-1)^{2g} \leq \left|\mathrm{Pic}^0(K)\right| \leq (\sqrt{q}+1)^{2g}$. □

Next, we want to estimate the parameters for reduction in the function field case. In particular, this shows that one needs to do at most $\left\lceil \frac{g}{\deg \mathfrak{p}_{n+1}} \right\rceil + 1$ Riemann-Roch space computations to compute a reduction.

Lemma 4.4.3. *Let K be a function field of genus g and let $\mathfrak{a} \in \mathrm{Id}(\mathcal{O})$ and $f_1, \ldots, f_n \in \mathbb{Z}$. For $\ell \in \mathbb{Z}$, define $B_\ell := B(\mathfrak{a}, (f_1, \ldots, f_n, \ell))$. If ℓ is minimal with $B_\ell \neq \{0\}$, then*

$$\left\lceil -\frac{\deg \mathrm{div}(\mathfrak{a}) + \sum_{i=1}^n f_i \deg \mathfrak{p}_i}{\deg \mathfrak{p}_{n+1}} \right\rceil \leq \ell \leq \left\lceil \frac{g - \deg \mathrm{div}(\mathfrak{a}) - \sum_{i=1}^n f_i \deg \mathfrak{p}_i}{\deg \mathfrak{p}_{n+1}} \right\rceil.$$

If $\mathfrak{a}$ is not principal and $\deg \mathfrak{p}_{n+1}$ divides $\deg \mathrm{div}(\mathfrak{a}) + \sum_{i=1}^n f_i \deg \mathfrak{p}_i$, the first "$\leq$" can be replaced by "$<$".

Proof. We have $B_\ell = L(D_\ell)$ with $D_\ell = \mathrm{div}(\mathfrak{a}) + \sum_{i=1}^n f_i \mathfrak{p}_i + \ell \mathfrak{p}_{n+1}$. Now $B_\ell = \{0\}$ for $\deg D_\ell < 0$, i.e. for $\ell < \frac{-\deg \mathrm{div}(\mathfrak{a}) - \sum_{i=1}^n f_i \deg \mathfrak{p}_i}{\deg \mathfrak{p}_{n+1}}$. Hence, if ℓ is minimal with $B_\ell \neq \{0\}$, we must have $\frac{-\deg \mathrm{div}(\mathfrak{a}) - \sum_{i=1}^n f_i \deg \mathfrak{p}_i}{\deg \mathfrak{p}_{n+1}} \leq \ell$. If $\mathfrak{a}$ is not principal, D_ℓ can never be principal, whence $B_\ell = \{0\}$ for $\deg D_\ell = 0$; this gives "$<$" instead of "$\leq$".

Finally, by Riemann's Inequality, $\dim B_\ell \geq 1 - g + \deg D_\ell$, whence $B_\ell \neq \{0\}$ for $1 - g + \deg D_\ell \geq 1$, i.e. for $\ell \geq \frac{g - \deg \mathrm{div}(\mathfrak{a}) - \sum_{i=1}^n f_i \deg \mathfrak{p}_i}{\deg \mathfrak{p}_{n+1}}$. □

If K is a number field, let $R = \mathbb{Z}$ and $Q = \mathbb{Q}$. If K is a function field, let $R = k[x]$ and $Q = k(x)$. Let $d := [K : Q]$.

Assume that we are given a R-basis $v_1, \ldots, v_d$ of $\mathcal{O}$, and we assume that $v_1 = 1$. Then, a non-zero fractional ideal $\mathfrak{a}$ can be written as

$$\mathfrak{a} = \frac{1}{d(\mathfrak{a})} \sum_{i=1}^{d} \left(\sum_{j=1}^{d} a_{ij} v_j \right) R$$

with $d(\mathfrak{a}) \in R$, monic[2] and of minimal degree respectively minimal absolute value, and $A = (a_{ij})_{ij} \in R^{d \times d}$ in *Hermite normal form*, i.e. $a_{ij} = 0$ for $j > i$, a_{ii} being monic, and $0 \leq a_{ij} < a_{ii}$ respectively $\deg a_{ij} < \deg a_{ii}$ for $j < i$. Note that this representation is unique and only depends on the basis $v_1, \ldots, v_n$ of $\mathcal{O}$.

Our aim is to estimate the size of such a representation of a reduced ideal. In the case of number fields, this has been done in [Thi95, p. 316, Corollary 3.7]. There, it is shown that one can represent a reduced ideal in a number field of discriminant Δ with at most

$$(d^2 + 1) \log_2 \sqrt{|\Delta|}$$

bits (note that $d \leq 8 \cdot \frac{1}{2} \log_2 |\Delta|$). In the number field case, $\frac{1}{2} \log |\Delta| = g - s \log \frac{2}{\pi} - \log |k^*| + d \log 2$, whence the bound on the size of a reduced ideal can be expressed as

$$(d^2 + 1)(g + (d \log 2 - s \log \tfrac{2}{\pi} - \log |k^*|)).$$

This is similar to the bound which we will obtain in Corollary 4.4.5.

We need the following standard result:

Lemma 4.4.4. *We have* $-\deg \operatorname{div}(\mathfrak{a}) = -d \deg d(\mathfrak{a}) + \sum_{i=1}^{d} \deg a_{ii}$. *Moreover,* $\mathfrak{a} \cap k(x) = \frac{a_{11}}{d(\mathfrak{a})} k[x]$. *In particular, if* $\mathfrak{a}$ *is reduced,* $a_{11} = d(\mathfrak{a})$. □

Using this, we obtain a similar result for function fields:

Corollary 4.4.5. *Let K be a function field. Reduced ideals of type (b) can be represented by at most* $(d-1)d(g + \deg \mathfrak{p}_{n+1} - 1)$ *elements of k and* $\frac{d(d+1)}{2}$ *integers in* $\{0, 1, \ldots, (d-1)(g + \deg \mathfrak{p}_{n+1} - 1)\}$.

Proof. By Proposition 4.4.1, we know $0 \leq \deg \operatorname{div}(\mathfrak{a}) \leq g + \deg \mathfrak{p}_{n+1} - 1$ and $\operatorname{div}(\mathfrak{a}) \geq 0$. Because of the latter,

$$\nu_p(d(\mathfrak{a})) = \left\lceil \max_{\substack{\mathfrak{q} \in \mathcal{P}_K \\ \mathfrak{q} | p}} -\frac{\nu_{\mathfrak{q}}(\mathfrak{a})}{e_{\mathfrak{q}}} \right\rceil$$

[2] We say an element $z \in \mathbb{Z}$ is *monic* if $z > 0$.

for all finite places p of $k(x)$ and, thus, $\deg d(\mathfrak{a}) \leq \deg \operatorname{div}(\mathfrak{a})$.

Now $\sum_{i=1}^{d} \deg a_{ii} = d \deg d(\mathfrak{a}) - \deg \operatorname{div}(\mathfrak{a})$ implies

$$\sum_{i=1}^{d} \deg a_{ii} \leq (d-1) \deg \operatorname{div}(\mathfrak{a}) \leq (d-1)(g + \deg \mathfrak{p}_{n+1} - 1).$$

As the a_{ii}'s are monic, it suffices to store $\deg a_{ii}$ field elements for every diagonal element. Moreover, as $\deg a_{ij} < \deg a_{ii}$, the number of field elements required to represent the matrix A is bounded by $\sum_{i=1}^{d} i \deg a_{ii}$. This sum is maximal under the condition $\sum_{i=1}^{d} \deg a_{ii} \leq (d-1)(g + \deg \mathfrak{p}_{n+1} - 1)$ if $\deg a_{dd} = (d-1)(g + \deg \mathfrak{p}_{n+1} - 1)$ and $\deg a_{ii} = 0$ for $i < d$, which gives the claim. □

4.5 Discrete Infrastructures

As in the one-dimensional case, one can make the following definition:

Definition 4.5.1. *An infrastructure (X, d, red) with $d : X \to \mathbb{R}^n/\Lambda$ is said to be* discrete *if $\Lambda \subseteq \mathbb{Z}^n$ and $d(X) \subseteq \mathbb{Z}^n/\Lambda$.*

Clearly, as the valuations of function fields are always integer-valued, infrastructures obtained from function fields are always discrete.

Proposition 4.5.2. *Let (X, d, red) be an infrastructure obtained from a global field, as described in Section 4.2. Then (X, d, red) is discrete if, and only if, one of the two conditions holds:*

(a) *K is a function field;*

(b) *K is a number field and $|S| = 1$.*

If (X, d, red) is not discrete, it is far from being discrete, i.e. even if one scales Λ, d and red with an algebraic constant $\lambda \neq 0$, it will never become discrete.

Proof. If K is a function field, this is clear. If $|S| = 1$, then $n = 0$, whence clearly the infrastructure is discrete. Therefore, assume that K is a number field and that $|S| > 1$.

Let ε be any non-trivial unit of $\mathcal{O}$, i.e. let $\varepsilon \in \mathcal{O}^* \setminus k^*$. If $\mathfrak{p} \in S$ and $\sigma : K \to \mathbb{C}$ is an embedding corresponding to $\mathfrak{p}$, we have that $|\sigma(\varepsilon)|$ is algebraic over $\mathbb{Q}$. Therefore, $\log |\sigma(\varepsilon)| = \nu_{\mathfrak{p}}(\varepsilon)$ is either transcendental or 0

by Lindemann's Theorem; in particular, every element of Λ is either 0 or has at least one transcendental component.

Hence, if $\lambda \neq 0$ is any algebraic element in $\mathbb{R}$, $\lambda\Lambda \not\subseteq \mathbb{Z}^n$. □

In [Fon08, p. 303, Proposition 4], the author showed that for one-dimensional infrastructures obtained from number fields, the f-representations of the form $(\mathfrak{a}, 0)$ in the principal ideal infrastructure never have finite order in $\mathrm{Rep}^f(\mathcal{O})$.

Proposition 4.5.3. *Let K be a number field and let $\mathfrak{a} \in \mathrm{Red}^{(b)}(\mathcal{O})$. Then $([\mathfrak{a}]_\sim, (0, \ldots, 0)) \in \mathrm{Rep}^f(\mathcal{O})$ has finite order if, and only if, $\mathfrak{a} = \mathcal{O}$.*

Proof. Clearly, $([\mathcal{O}]_\sim, (0, \ldots, 0))$ has finite order in $\mathrm{Rep}^f(\mathcal{O})$, as it is the neutral element.

Now assume that $\mathfrak{a} = \frac{1}{\mu}\mathcal{O}$ with $\mu \in \mathcal{E}(\mathcal{O})$ and that $([\mathfrak{a}]_\sim, (0, \ldots, 0))$ has finite order. This means that there exists an $n \in \mathbb{N}$ such that there exists an $\varepsilon \in \mathcal{O}^*$ with $n\nu_\mathfrak{p}(\mu) = \nu_\mathfrak{p}(\varepsilon)$ for every $\mathfrak{p} \in S'$, i.e. $\left|\mu^n\varepsilon^{-1}\right|_\mathfrak{p} = 1$. By [AO82, p. 285, (8)], we must have $\left|\mu^n\varepsilon^{-1}\right|_{\mathfrak{p}_{n+1}} = 1$ as well. Now, clearly, $\mu^n\varepsilon^{-1} \in \mathcal{O}$, whence $\mu^n\varepsilon^{-1} \in B(\mathcal{O}, 1) = k^* \cup \{0\}$. But this means that $\varepsilon' := \mu^n \in \mathcal{O}^*$ and $\nu_\mathfrak{q}(\mu) = \frac{1}{n}\nu_\mathfrak{q}(\varepsilon') = 0$ for all $\mathfrak{q} \in \mathcal{P}_K \setminus S$, i.e. that $\mu \in \mathcal{O}^*$. But then, $\mathfrak{a} = \frac{1}{\mu}\mathcal{O} = \mathcal{O}$. □

First note that the crucial ingredient which is not available for function fields is [AO82, p. 285, (8)], which says that if $|f|_\mathfrak{p} \leq |g|_\mathfrak{p}$ for all $\mathfrak{p} \in S$, then either $|f|_\mathfrak{p} < |g|_\mathfrak{p}$ for all $\mathfrak{p} \in S$ or $|f|_\mathfrak{p} = |g|_\mathfrak{p}$ for all $\mathfrak{p} \in S$.

Finally, note that this shows that as soon as $X \neq \{[\mathcal{O}]_\sim\}$, $(X, d^\mathcal{O}, red^\mathcal{O})$ can never be discrete in the number field case, even if we multiply by a transcendental scaling factor, as in a discrete infrastructure, every element must have a finite order (which divides the order of $\mathbb{Z}^n/\Lambda$, by Lagrange's Theorem).

4.6 Conclusion

An important consequence from Corollary 4.3.4 is that computing inverses in infrastructures obtained from global fields is as hard as inversion of ideals and reduction. If one wants efficient arithmetic for the infrastructure, reduction has to be reasonably fast. Ideal inversion, on the other hand, is not fast, but also not that slow, as there exist polynomial-time algorithms for computing inverses of ideals.

Finally, we want to present the most important special case of the theory developed in this chapter, namely the case of the infrastructure if $\deg \mathfrak{p}_{n+1} = 1$. In that case, we have several simplifications:

Corollary 4.6.1 (Infrastructure, Degree One Case). *Assume that* $\deg \mathfrak{p}_{n+1} = 1$. *In that case,* $[\mathfrak{a}]_\sim = [\mathfrak{a}']_\sim$ *for* $\mathfrak{a}, \mathfrak{a}' \in \mathrm{Red}^{(b)}(K)$ *if, and only if,* $\mathfrak{a} = \mathfrak{a}'$.

(a) *From Proposition 4.3.2, we obtain a bijection* $\Phi : \mathrm{Rep}^f(K) \to \mathrm{Pic}^0(K)$ *and can compute the group law in* $\mathrm{Pic}^0(K)$ *for elements in* $\mathrm{Rep}^f(K)$ *using the algorithms in Proposition 4.3.4.*

(b) *If* $\mathfrak{b} \in \mathrm{Id}(\mathcal{O})$ *is fixed, we get a bijection*

$$\begin{aligned} d :\ & \mathrm{Rep}^f(\mathfrak{b}) \to T \cong \mathbb{G}^n/\Lambda, \\ & ([\tfrac{1}{\mu}\mathfrak{b}]_\sim, (f_i)_i) \mapsto (-\nu_{\mathfrak{p}_i}(\mu) + f_i)_{i=1,\dots,n} + \Lambda. \end{aligned}$$

In case $\mathfrak{b} = \mathcal{O}$, *the group law in* $\mathbb{G}^n/\Lambda$ *can be computed for elements in* $\mathrm{Rep}^f(\mathfrak{b})$ *using the algorithms in Proposition 4.3.4; in particular, this gives a giant step*

$$\begin{aligned} \mathrm{gs} :\ & \mathrm{Red}^{(b)}(\mathcal{O}) \times \mathrm{Red}^{(b)}(\mathcal{O}) \to \mathrm{Red}^{(b)}(\mathcal{O}), \\ & (\mathfrak{a}, \mathfrak{a}') \mapsto \pi_1(\Phi^{-1}(\Phi(\mathfrak{a}, (0)_i) + \Phi(\mathfrak{a}', (0)_i))), \end{aligned}$$

where $\pi_1 : \mathrm{Rep}^f(K) \to \mathrm{Red}^{(b)}(K)$ *is defined by* $([\mathfrak{a}]_\sim, (f_i)_i) \mapsto \mathfrak{a}$ *and where* Φ *is as in (a).*

Note that our giant step function is similar to the one described by Schoof in [Sch08, p. 29, Algorithm 10.4], in the sense that the distance between the result of our algorithm and the algorithm by Schoof is small.

Chapter 5

Computation in the Function Field Case

In this chapter, we will describe the algorithm of F. Heß for computing Riemann-Roch spaces in function fields and derive a specialized algorithm for computing a k-basis of $B(\mathfrak{a}, (t_\mathfrak{p})_{\mathfrak{p}\in S})$. Then, we give algorithms for computing giant steps and baby steps. Finally, we will consider some optimizations.

Throughout this chapter, let $d = [K : k(x)]$.

5.1 The Algorithm of Heß

Denote by $\mathrm{Div}_{fin}(K)$ the set of divisors $D \in \mathrm{Div}(K)$ with $\nu_\mathfrak{p}(D) = 0$ for all $\mathfrak{p} \in S$. Then we have an isomorphism

$$\mathrm{Div}_{fin}(K) \times \mathrm{Div}_\infty(K) \to \mathrm{Div}(K), \qquad (D_f, D_\infty) \mapsto D_f + D_\infty.$$

Let $D_f = \sum_{\mathfrak{p}\notin S} n_\mathfrak{p}\mathfrak{p} \in \mathrm{Div}_{fin}(K)$ and $D_\infty = \sum_{\mathfrak{p}\in S} n_\mathfrak{p}\mathfrak{p} \in \mathrm{Div}_\infty(K)$. Define $\mathrm{ideal}(D_f) := \prod_{\mathfrak{p}\notin S}(\mathfrak{m}_\mathfrak{p} \cap \mathcal{O})^{-n_\mathfrak{p}}$; then $\mathrm{div}(\mathrm{ideal}(D_f)) = D_f$.

Let $\mathfrak{o}_\infty$ be the valuation ring of the infinite place of $k(x)$, and $\mathcal{O}_\infty$ the integral closure of $\mathfrak{o}_\infty$ in K. Then $\mathcal{O}_\infty$ is a principal ideal domain by [Sti93, p. 71, Proposition III.2.10], whose non-zero prime ideals are exactly $\mathfrak{m}_\mathfrak{p} \cap \mathcal{O}_\infty$, $\mathfrak{p} \in S$. Define $\mathrm{ideal}(D_\infty) := \prod_{\mathfrak{p}\in S}(\mathfrak{m}_\mathfrak{p} \cap \mathcal{O}_\infty)^{-n_\mathfrak{p}}$.

Then, we have

$$L(D_f + D_\infty) = \mathrm{ideal}(D_f) \cap \mathrm{ideal}(D_\infty).$$

F. Heß [Hes99, Hes02] exploits this for computing a k-basis of $L(D_f + D_\infty)$, by using a $k[x]$-basis of $\mathrm{ideal}(D_f)$ and an $\mathfrak{o}_\infty$-basis of $\mathrm{ideal}(D_\infty)$. Let

$v_1, \ldots, v_d$ be a $k[x]$-basis of ideal(D_f) and $w_1, \ldots, w_d$ be an $\mathfrak{o}_\infty$-basis of ideal(D_∞). Both of them are $k(x)$-bases of K, whence there exists an invertible matrix $M \in k(x)^{d\times d}$ such that $(w_1, \ldots, w_d)M = (v_1, \ldots, v_d)$. Using the reduction algorithm of S. Paulus [Pau98] applied to the columns of M, one obtains a unimodular matrix $T_2 \in k[x]^{d\times d}$ (i.e. $\det T_2 \in k^*$). Let $-d_i$ be the degree[1] of the i-th column of MT_2 and define $\hat{v}_i$ as the i-th column of $(v_1, \ldots, v_d)T_2$; then

$$\text{ideal}(D_f) \cap \text{ideal}(D_\infty) = \left\langle v_i x^j \mid 0 \le j \le d_i,\ 1 \le i \le d \right\rangle_k,$$

where the $(v_i x^j)_{i,j}$ are a k-basis of this k-vector space; i.e.

$$\dim_k(\text{ideal}(D_f) \cap \text{ideal}(D_\infty)) = \sum_{i=1}^{d} \max\{0, d_i + 1\}.$$

Note that for our use, we want to compute $L(D)$ for $D = \text{div}(\mathfrak{a}) + \sum_{\mathfrak{p}\in S} t_\mathfrak{p}\mathfrak{p}$, where $\mathfrak{a} \in \text{Id}(\mathcal{O})$ is given together with integers $t_\mathfrak{p} \in \mathbb{Z}$, $\mathfrak{p} \in S$. Assuming that $\mathfrak{a}$ is given in form of a $k[x]$-basis, we have to find an $\mathfrak{o}_\infty$-basis of ideal$(\sum_{\mathfrak{p}\in S} t_\mathfrak{p}\mathfrak{p}) = \prod_{\mathfrak{p}\in S}(\mathfrak{m}_\mathfrak{p} \cap \mathcal{O}_\infty)^{-t_\mathfrak{p}}$.

5.2 Computing the Infinite Primes

We know that $\mathcal{O}_\infty$ is a principal ideal domain; hence, if $h_\mathfrak{p}$ is a generator of the principal $\mathcal{O}_\infty$-ideal $\mathfrak{m}_\mathfrak{p} \cap \mathcal{O}_\infty$, $\mathfrak{p} \in S$, we get that $\prod_{\mathfrak{p}\in S} h_\mathfrak{p}^{-t_\mathfrak{p}} \hat{w}_i$, $i = 1, \ldots, d$ is an $\mathfrak{o}_\infty$-basis of ideal$(\sum_{\mathfrak{p}\in S} t_\mathfrak{p}\mathfrak{p})$, if $\hat{w}_1, \ldots, \hat{w}_d$ is an $\mathfrak{o}_\infty$-basis of $\mathcal{O}_\infty$.

Hence, we need elements $h_\mathfrak{p} \in \mathcal{O}_\infty$ with $\nu_\mathfrak{p}(h_\mathfrak{p}) = 1$ and $\nu_\mathfrak{q}(h_\mathfrak{p}) = 0$ for $\mathfrak{q} \ne \mathfrak{p}$, $\mathfrak{p}, \mathfrak{q} \in S$. To compute such elements, assume that $K/k(x)$ is separable and that $\mathcal{O}_\infty = \mathfrak{o}_\infty[\rho]$ for some $\rho \in \mathcal{O}_\infty$, i.e. that $1, \rho, \rho^2, \ldots, \rho^{d-1}$ is an $\mathfrak{o}_\infty$-basis for $\mathcal{O}_\infty$. Let $f \in \mathfrak{o}_\infty[t]$ be the minimal polynomial of ρ over $k(x)$ and consider the projection $\pi : \mathfrak{o}_\infty \to \mathfrak{o}_\infty/\mathfrak{m}_\infty \cong k$. Compute the factorization $\pi(f) = \prod_{i=1}^{k} g_i^{e_i}$ with pairwise distinct monic irreducible polynomials $g_i \in k[t]$ and $e_i \in \mathbb{N}_{>0}$.

Then, by Kummer's Theorem [Sti93, p. 76, Theorem III.3.7], the infinite places S of K correspond to the g_i, where $\mathfrak{p} \in S$ is the unique common zero of $\frac{1}{x}$ and $g_i(\rho)$. Moreover, if $\mathfrak{p}$ corresponds to g_i, we have $\deg g_i = \deg \mathfrak{p}$ is the degree of $\mathfrak{p}$, $e_i = e_\mathfrak{p}$ is the ramification index of $\mathfrak{p}$ and $\mathfrak{m}_\mathfrak{p} \cap \mathcal{O}_\infty = \frac{1}{t}\mathcal{O}_\infty + f_i\mathcal{O}_\infty$. In particular, if we set $f_i := g_i(\rho)$, we have $\nu_\mathfrak{p}(f_i) > 0$ and $\nu_\mathfrak{q}(f_i) = 0$ for $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$. In case $e_i > 1$, we have $\nu_\mathfrak{p}(f_i) = 1$. If $e_i = 1$,

[1] The degree of a vector $v = (v_1, \ldots, v_n) \in k(x)^n$ is defined as $\deg v = \max_{i=1,\ldots,n} \deg v_i$.

i.e. $\mathfrak{p}$ is unramified, it could be that $\nu_{\mathfrak{p}}(f_i) > 1$; in that case, replace f_i by $f_i + \frac{1}{x}$; then $\nu_{\mathfrak{p}}(f_i) = 1$ and $\nu_{\mathfrak{q}}(f_i) = 0$ for $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$.

To test whether $\nu_{\mathfrak{p}}(f_i) > 1$, one checks whether $f_i \in (\mathfrak{m}_{\mathfrak{p}} \cap \mathcal{O}_\infty)^2 = f_i^2\mathcal{O}_\infty + \frac{1}{x^2}\mathcal{O}_\infty + \frac{f_i}{x}\mathcal{O}_\infty$ by computing a $\mathfrak{o}_\infty$-basis of the ideal and writing f_i in terms of this basis, and by checking whether the coefficients lie in $\mathfrak{o}_\infty$. Alternatively, one could check whether $\frac{1}{x}$ lies in the principal $\mathcal{O}_\infty$-ideal generated by f_i; this is the case if, and only if, $\nu_{\mathfrak{p}}(f_i) \leq e_i = 1$.

5.3 A Specialized Algorithm

In this section, we want to present an algorithm which is specialized on computing a k-basis of $B(\mathfrak{a}, (t_{\mathfrak{p}})_{\mathfrak{p}\in S}) = L(D)$ for $D = \operatorname{div}(\mathfrak{a}) + \sum_{\mathfrak{p}\in S} t_{\mathfrak{p}}\mathfrak{p}$. Let $\mathfrak{b} := \prod_{\mathfrak{p}\in S}(\mathfrak{m}_{\mathfrak{p}} \cap \mathcal{O}_\infty)^{-t_{\mathfrak{p}}} = \operatorname{ideal}(\sum_{\mathfrak{p}\in S} t_{\mathfrak{p}}\mathfrak{p})$; then $L(D) = \mathfrak{a} \cap \mathfrak{b}$. We assume that we want to compute $B(\mathfrak{a}, (t_{\mathfrak{p}})_{\mathfrak{p}\in S})$ for many different choices of $\mathfrak{a}$ and $(t_{\mathfrak{p}})_{\mathfrak{p}\in S}$ in a fixed function field.

Let $\hat{v}_1, \ldots, \hat{v}_d$ be a $k[x]$-basis of $\mathcal{O}$ and let $\hat{w}_1, \ldots, \hat{w}_d$ be an $\mathfrak{o}_\infty$-basis of $\mathcal{O}_\infty$. Assume that $\mathfrak{a}$ is given in the form $\mathfrak{a} = \sum_{i=1}^{d} v_i k[x]$, where

$$(v_1, \ldots, v_n) = (\hat{v}_1, \ldots, \hat{v}_n)T_{\mathfrak{a}}$$

with $T_{\mathfrak{a}} \in k(x)^{n\times n}$. Let $M \in k(x)^{d\times d}$ with $(\hat{v}_1, \ldots, \hat{v}_n) = (\hat{w}_1, \ldots, \hat{w}_n)M$. Then

$$(v_1, \ldots, v_n) = (\hat{v}_1, \ldots, \hat{v}_n)T_{\mathfrak{a}} = (\hat{w}_1, \ldots, \hat{w}_n)MT_{\mathfrak{a}}.$$

Let $M_{\mathfrak{p}} \in k(x)^{d\times d}$ be a matrix with $(h_{\mathfrak{p}}\hat{w}_1, \ldots, h_{\mathfrak{p}}\hat{w}_d)M_{\mathfrak{p}} = (\hat{w}_1, \ldots, \hat{w}_d)$, where $h_{\mathfrak{p}}$ was defined in the previous section. Then

$$(w_1, \ldots, w_d) := (\hat{w}_1, \ldots, \hat{w}_d)T_{\mathfrak{b}}^{-1}$$

is the $\mathfrak{o}_\infty$-basis of $\mathfrak{b}$ described in the previous section with $T_{\mathfrak{b}} := \prod_{\mathfrak{p}\in S} M_{\mathfrak{p}}^{-t_{\mathfrak{p}}}$. Hence, we have

$$(w_1, \ldots, w_d)T_{\mathfrak{b}}MT_{\mathfrak{a}} = (\hat{w}_1, \ldots, \hat{w}_d)MT_{\mathfrak{a}} = (v_1, \ldots, v_d).$$

Clearly, the $M_{\mathfrak{p}}$ and $M_{\mathfrak{p}}^{-1}$, $\mathfrak{p} \in S$ can be precomputed, whence computation of $T_{\mathfrak{b}}MT_{\mathfrak{a}}$ amounts in (at most) $\sum_{\mathfrak{p}\in S} |t_{\mathfrak{b}}| + 1$ matrix multiplications. Moreover, if the product $T_{\mathfrak{b}}MT_{\mathfrak{a}}$ has been computed for a choice $(t_{\mathfrak{p}})_{\mathfrak{p}\in S}$ and if one $t_{\mathfrak{p}}$ is increased by one, it suffices to multiply the product by the corresponding $M_{\mathfrak{p}}$ from the left to obtain the product for the new choice $(\hat{t}_{\mathfrak{p}})_{\mathfrak{p}\in S}$.

Now, to compute $\mathfrak{a} \cap \mathfrak{b}$ in case we are given $T := T_{\mathfrak{b}}MT_{\mathfrak{a}}$ with

$$(w_1, \ldots, w_d)T = (v_1, \ldots, v_d),$$

the reduction algorithm described in [Pau98], which is essentially Lenstra's adaption of LLL to the rational function field case, gives two matrices $T_1 \in Gl_d(\mathfrak{o}_\infty)$ and $T_2 \in Gl_d(k[x])$ and integers $\lambda_1, \ldots, \lambda_d \in \mathbb{Z}$ with

$$T_1 T T_2 = \begin{pmatrix} x^{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & x^{\lambda_d} \end{pmatrix}.$$

Hence, if $(\tilde{w}_1, \ldots, \tilde{w}_d) = (w_1, \ldots, w_d)T_1^{-1}$ and $(\tilde{v}_1, \ldots, \tilde{v}_d) = (v_1, \ldots, v_d)T_2 = (\hat{v}_1, \ldots, \hat{v}_d)T_{\mathfrak{a}}T_2$, then $\tilde{w}_i x^{\lambda_i} = \tilde{v}_i$. In particular, the elements of $\mathfrak{a}$ are exactly the ones of the form $f = \sum_{i=1}^d r_i \tilde{v}_i$ with $r_i \in k[x]$, and we have

$$\begin{aligned} f \in \mathfrak{b} &\iff \sum_{i=1}^d r_i x^{\lambda_i} \tilde{w}_i \in \mathfrak{b} \iff \forall i : x^{\lambda_i} r_i \in \mathfrak{o}_\infty \\ &\iff \forall i : \lambda_i + \deg r_i \leq 0 \iff \deg r_i \leq -\lambda_i. \end{aligned}$$

Hence, a k-basis of $\mathfrak{a} \cap \mathfrak{b}$ is given by

$$\{\tilde{v}_i x^j \mid 0 \leq j \leq -\lambda_i,\ 1 \leq i \leq d\}$$

and $\dim_k(\mathfrak{a} \cap \mathfrak{b}) = \sum_{i=1}^d \max\{0, -\lambda_i + 1\}$. Note that the reduction algorithm as given in [Pau98] computes T_2 and not T_1, and the λ_i's can be extracted as the maximum degree appearing in the i-th column of TT_2. Hence, this suffices to compute the dimension and, if necessary, a basis of $\mathfrak{a} \cap \mathfrak{b}$.

According to [Pau98, pp. 5f], the running time of the reduction algorithm to compute TT_2 from T is $\mathcal{O}(d^4(\max_{i,j} \deg t_{ij})^2)$ operations in k, where $T = (t_{ij})_{ij}$ is assumed to be integral. This running time is given without computation of T_2; to do that, one needs to perform an elementary matrix operation every time the inner loop is executed, and according to [Pau98, p. 6], the number of iteration is $\mathcal{O}(d^2 \max_{i,j} \deg t_{ij})$; every operation takes d operations in k, whence the costs for creating T_2 are negligible in comparison to the costs for computing TT_2 and, hence, the λ_i's.

5.4 Computing Giant Steps

Assume that we are given two f-representations

$$([\mathfrak{a}]_\sim, (t_1, \ldots, t_n)), ([\mathfrak{a}']_\sim, (s_1, \ldots, s_n)) \in \mathrm{Rep}^f(K),$$

and we want to compute their sum. If $t_i = s_i = 0$ for all i, this corresponds to the computation of giant steps together with relative distances in $\mathrm{Red}^{(b)}(\mathcal{O})/_\sim$.

By Proposition 4.3.4, we have to compute $B_\ell := B(\mathfrak{a}\mathfrak{a}', (t_1+s_1, \ldots, t_n+s_n, \ell)) \setminus \{0\}$ for various $\ell \in \mathbb{Z}$ to find the smallest such that $B_\ell \neq \emptyset$. For that, one computes ℓ minimal such that

$$\deg(\mathrm{div}(\mathfrak{a})) + \deg(\mathrm{div}(\mathfrak{a}')) + \sum_{i=1}^{n}(t_i + s_i)\deg \mathfrak{p}_i + \ell \deg \mathfrak{p}_{n+1} \geq 0,$$

and increases ℓ until the dimension gets positive.

As soon as it is positive, one chooses an element of $B(\mathfrak{a}\mathfrak{a}', (t_1+s_1, \ldots, t_n+s_n, \ell))$ which is smallest with respect to $\leq$ as μ and computes $\mathfrak{a}'' := \frac{1}{\mu}\mathfrak{a}\mathfrak{a}'$ and $u_i := t_i + s_i + \nu_{\mathfrak{p}_i}(\mu)$, to obtain $([\mathfrak{a}'']_\sim, (u_1, \ldots, u_n))$ as the sum of $([\mathfrak{a}]_\sim, (t_1, \ldots, t_n))$ and $([\mathfrak{a}']_\sim, (s_1, \ldots, s_n))$.

Assuming that $\deg \mathfrak{p}_{n+1} = 1$ and that we can efficiently evaluate valuations $\nu_{\mathfrak{p}_i}(\bullet)$, $i = 1, \ldots, n$, we can use the following, special algorithm:

Algorithm 5.4.1: Giant Step Computation, Special Version.

Input: f-representations $([\mathfrak{a}]_\sim, (t_1, \ldots, t_n)), ([\mathfrak{a}']_\sim, (s_1, \ldots, s_n))$.

Output: f-representation $([\frac{1}{\mu}\mathfrak{a}\mathfrak{a}']_\sim, (t_i + s_i + \nu_{\mathfrak{p}_i}(\mu))_i)$ together with $(\nu_{\mathfrak{p}_i}(\mu))_{i=1,\ldots,n+1}$.

(1) Compute $\mathfrak{a}'' := \mathfrak{a}\mathfrak{a}'$.

(2) Let
$$\ell := -\deg(\mathrm{div}(\mathfrak{a}'')) - \sum_{i=1}^{n}(t_i + s_i)\deg \mathfrak{p}_i.$$

(3) Compute a basis B of $B(\mathfrak{a}'', (t_1 + s_1, \ldots, t_n + s_n, \ell))$.

(4) If $|B| = 1$, continue with Step (7).

(5) Otherwise, set $\ell := \ell + 1$.

(6) Continue with Step (3).

(7) Let μ be the unique element in B and compute $\frac{1}{\mu}\mathfrak{a}''$.

(8) Compute $u_i := \nu_{\mathfrak{p}_i}(\mu)$, $i = 1, \ldots, n$.

(9) Return $([\frac{1}{\mu}\mathfrak{a}'']_\sim, (s_i + t_i + u_i)_i)$ and $(u_1, \ldots, u_n, -\ell)$.

If $\deg \mathfrak{p}_{n+1} > 1$, or if valuations cannot be evaluated efficiently, one can proceed as follows:

Algorithm 5.4.2: Giant Step Computation, General Version.

Input: f-representations $([\mathfrak{a}]_\sim, (t_1, \ldots, t_n)), ([\mathfrak{a}']_\sim, (s_1, \ldots, s_n))$.

Output: f-representation $([\frac{1}{\mu}\mathfrak{a}\mathfrak{a}']_\sim, (t_i + s_i + \nu_{\mathfrak{p}_i}(\mu))_i)$ together with $(\nu_{\mathfrak{p}_i}(\mu))_{i=1,\ldots,n+1}$.

(1) Compute $\mathfrak{a}'' := \mathfrak{a}\mathfrak{a}'$.

(2) Let

$$\ell := \left\lceil -\frac{1}{\deg \mathfrak{p}_{n+1}} \left(\deg(\operatorname{div}(\mathfrak{a}'')) + \sum_{i=1}^{n} (t_i + s_i) \deg \mathfrak{p}_i \right) \right\rceil.$$

(3) Compute a basis B of $B(\mathfrak{a}'', (t_1 + s_1, \ldots, t_n + s_n, \ell))$.

(4) If $|B| \geq 1$, continue with Step (7).

(5) Otherwise, set $\ell := \ell + 1$.

(6) Continue with Step (3).

(7) Set $u_i := 0$ for $i = 1, \ldots, n$.

(8) For $i = 1, \ldots, n$, do the following:

  (i) Set $u_i := u_i + 1$.

  (ii) Compute a basis B of $B(\mathfrak{a}'', (t_1 + s_1 - u_1, \ldots, t_n + s_n - u_n, \ell))$.

  (iii) If $|B| > 0$, continue with Step (8 i).

  (iv) Set $u_i := u_i - 1$.

(9) Compute a basis B of $B(\mathfrak{a}'', (t_1 + s_1 - u_1, \ldots, t_n + s_n - u_n, \ell))$.

(10) Let μ be an arbitrary element of B and compute $\frac{1}{\mu}\mathfrak{a}''$.

(11) Return $([\frac{1}{\mu}\mathfrak{a}'']_\sim, (u_i)_i)$ and $(u_1 - t_1 - s_1, \ldots, u_n - t_n - s_n, -\ell)$.

Proposition 5.4.3. *The two algorithms terminate and return a valid result.*

Proof. If ℓ is one less than the one defined in Step (2), then $\deg(\operatorname{div}(\mathfrak{a}'') + \sum_{i=1}^{n}(t_i + s_i)\mathfrak{p}_i + \ell\mathfrak{p}_{n+1}) < 0$, whence $B(\mathfrak{a}'', (t_1 + s_1, \ldots, t_n + s_n, \ell)) = \{0\}$.

If ℓ is increased by one, the dimension of $B(\mathfrak{a}'', (t_1 + s_1, \ldots, t_n + s_n, \ell))$

increases at most by $\deg \mathfrak{p}_{n+1}$. By Riemann's Inequality, it will increase eventually, whence we will reach Step (7).

In the first algorithm, we have $|B| = 1$ in that case as $\deg \mathfrak{p}_{n+1} = 1$, whence μ can be chosen as the unique element in B.

In the second algorithm, it can be that $|B| > 1$, i.e. we do not know whether we can chose any element of B as μ. Moreover, we need to compute the valuations of μ in some way. For that, as $\leq$ is the lexicographic order, we chose $u_i \geq 0$ maximal, beginning with $i = 1$, such that $B(\mathfrak{a}'', (t_1 + s_1 - u_1, \ldots, t_n + s_n - u_n, \ell)) \neq \{0\}$. This is achieved with the loop in Step (8). Then, we know that all elements in $B(\mathfrak{a}'', (t_1 + s_1 - u_1, \ldots, t_n + s_n - u_n, \ell))$ have the same infinite valuations $\nu_{\mathfrak{p}_i}(\bullet) = -t_i - s_i + u_i$, $i = 1, \ldots, n$ and $\nu_{\mathfrak{p}_{n+1}}(\bullet) = -\ell$. □

5.5 Computing Baby Steps

Assume that we are given a type (b) reduced ideal $\mathfrak{b} = \frac{1}{\mu}\mathfrak{a}$ in the ideal class of $\mathfrak{a} \in \mathrm{Id}(\mathcal{O})$, i.e. we have $\mu \in \mathcal{E}(\mathfrak{a})$. Let $\mathfrak{p} \in S$, let X be a baby step shape and let $\leq$ be a scale-invariant universal $\mathfrak{p}$-order on K. Our aim is to compute an ideal representation of an element in $\mathrm{bs}_{\mathfrak{p}}^{X,\leq}(\mu, \mathfrak{a})$, i.e. we want to compute $\frac{1}{\mu'}\mathfrak{b}$ for some $\mu' \in \mathrm{bs}_{\mathfrak{p}}^{X,\leq}(1, \mathfrak{b})$ (see Corollary 3.6.6).

Note that as soon one place $\mathfrak{q} \in S$ with $\deg \mathfrak{q} = 1$ exist, the elements in $\mathrm{bs}_{\mathfrak{p}}^{X,\leq}(1, \mathfrak{b})$ differ only by constants (by Corollary 3.6.7).

In the following, we restrict to the cases $X = X_1 := [0, 1)^n$ and $X = X_2 := [0, 1]^n \setminus \{(1, \ldots, 1)\}$. We consider both the cases $\deg \mathfrak{p} = 1$ and $\deg \mathfrak{p} > 1$, and restrict to certain orders $\leq$ in some of these cases.

Baby Steps for $X = X_1$. We begin with the case $X = X_1$ and $\deg \mathfrak{p} = 1$. In that case, the baby step in $\mathfrak{p}$-direction does not depends on $\leq$:

Algorithm 5.5.1: Baby Step Computation for $X = [0,1)^n$, Special Version.

Input: reduced ideal $\mathfrak{b}$, $\mathfrak{p} \in S$.

Output: $\mu \in \mathrm{bs}_{\mathfrak{p}}^{[0,1)^n,\leq}(1, \mathfrak{b})$.

(1) Let $t_{\mathfrak{q}} := -1$ for all $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$.

(2) Let
$$t_{\mathfrak{p}} := \max\left\{ \sum_{\mathfrak{q} \in S \setminus \{\mathfrak{p}\}} \deg \mathfrak{q} - \deg \operatorname{div}(\mathfrak{b}), 1 \right\}.$$

(3) Compute a basis B of $B(\mathfrak{b}, (t_{\mathfrak{q}})_{\mathfrak{q}})$.

(4) If $|B| = 1$, return the only element of B.

(5) Otherwise, set $t_{\mathfrak{p}} := t_{\mathfrak{p}} + 1$.

(6) Continue with Step (3).

Lemma 5.5.2. *This algorithm terminates and returns a valid result.*

Proof. If $t_{\mathfrak{p}}$ is by one less than in Step (2), $B(\mathfrak{b}, (t_{\mathfrak{q}})_{\mathfrak{q}})$ contains only 0 as either (if 1 is the maximum) $1 \in \mathcal{E}(\mathfrak{b})$ or as (if 1 is not the maximum) the degree of the divisor $\operatorname{div}(\mathfrak{b}) + \sum_{\mathfrak{q} \in S} t_{\mathfrak{q}} \mathfrak{q}$ is strictly negative.

Now, if $t_{\mathfrak{p}}$ is increased by one, the degree of the divisor increases by $\deg \mathfrak{p} = 1$, whence the dimension of $B(\mathfrak{b}, (t_{\mathfrak{q}})_{\mathfrak{q}})$ can increase at most by one. By Riemann's Inequality, it will eventually increase. For that reason, $|B|$ will start with 0 or 1 and increase at most by 1 in every step, i.e. at one point it will equal 1. In that case, the only element in B will be (up to constants) the only element in $X^{1,\leq}$ of minimal absolute value $|\bullet|_{\mathfrak{p}}$, whence it is an element of $\mathrm{bs}_{\mathfrak{p}}^{X,\leq}(1, \mathfrak{b})$. □

Now assume that $\deg \mathfrak{p} > 1$. In that case, we need to know how "$\leq$" looks like, as the dimension of $B(\mathfrak{b}, (t_{\mathfrak{q}})_{\mathfrak{q}})$ may increase by up to $\deg \mathfrak{p} > 1$ if $t_{\mathfrak{p}}$ is increased by 1. We assume that $\leq$ is a lexicographic order as in Example 3.5.3. For that, write $S \setminus \{\mathfrak{p}\} = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$, and define

$$\mu \leq \mu' :\Longleftrightarrow (|\mu|_{\mathfrak{p}}, |\mu|_{\mathfrak{q}_1}, \ldots, |\mu|_{\mathfrak{q}_n}) \leq_{\ell ex} (|\mu'|_{\mathfrak{p}}, |\mu'|_{\mathfrak{q}_1}, \ldots, |\mu'|_{\mathfrak{q}_n}).$$

Algorithm 5.5.3: Baby Step Computation for $X = [0,1)^n$, General Version.

Input: reduced ideal $\mathfrak{b}$, $\mathfrak{p} \in S$ and the order $\leq$ as defined above.

Output: $\mu \in \mathrm{bs}_{\mathfrak{p}}^{[0,1)^n,\leq}(1,\mathfrak{b})$ together with $(\nu_{\mathfrak{q}}(\mu))_{\mathfrak{q}\in S}$.

(1) Let $t_{\mathfrak{q}} := -1$ for all $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$.

(2) Let

$$t_{\mathfrak{p}} := \max\left\{ \left\lceil \frac{1}{\deg \mathfrak{p}} \Big(\sum_{\mathfrak{q}\in S\setminus\{\mathfrak{p}\}} \deg \mathfrak{q} - \deg \mathrm{div}(\mathfrak{b}) \Big) \right\rceil, 1 \right\}.$$

(3) Compute a basis B of $B(\mathfrak{b}, (t_{\mathfrak{q}})_{\mathfrak{q}})$.

(4) If $|B| \geq 1$, continue with Step (7).

(5) Otherwise, set $t_{\mathfrak{p}} := t_{\mathfrak{p}} + 1$.

(6) Continue with Step (3).

(7) For $i = 1, \ldots, n$, do the following:

  (i) Set $t_{\mathfrak{q}_i} := t_{\mathfrak{q}_i} - 1$.

  (ii) Compute a basis B of $B(\mathfrak{b}, (t_{\mathfrak{q}})_{\mathfrak{q}})$.

  (iii) If $|B| > 0$, continue with Step (7 i).

  (iv) Set $t_{\mathfrak{q}_i} := t_{\mathfrak{q}_i} + 1$.

(8) Compute a basis B of $B(\mathfrak{b}, (t_{\mathfrak{q}})_{\mathfrak{q}})$.

(9) Return an arbitrary element of B together with $(-t_{\mathfrak{q}})_{\mathfrak{q}\in S}$.

Lemma 5.5.4. *This algorithm terminates and returns a valid result.*

Proof. If $t_{\mathfrak{p}}$ is by one less than in Step (2), $B(\mathfrak{b}, (t_{\mathfrak{q}})_{\mathfrak{q}})$ contains only 0 as either (if 1 is the maximum) $1 \in \mathcal{E}(\mathfrak{b})$ or as (if 1 is not the maximum) the degree of the divisor $\mathrm{div}(\mathfrak{b}) + \sum_{\mathfrak{q}\in S} t_{\mathfrak{q}}\mathfrak{q}$ is strictly negative.

Now, if $t_{\mathfrak{p}}$ is increased by one, the degree of the divisor increases by $\deg \mathfrak{p} > 1$. By Riemann's Inequality, it will eventually increase. For that reason, in Step (7) $t_{\mathfrak{p}}$ will be minimal such that $B(\mathfrak{b}, (t_{\mathfrak{q}})_{\mathfrak{q}}) \neq \{0\}$. By our choice of $\leq$, the loop in Step (7) will choose $t_{\mathfrak{q}_1}, \ldots, t_{\mathfrak{q}_n}$ minimal such that $B(\mathfrak{a}, (t_{\mathfrak{q}})_{\mathfrak{q}}) \neq \{0\}$; the order in which the $t_{\mathfrak{q}}$, $\mathfrak{q} \in S$ are minimized ensures that all minimal elements with respect to $\leq$ are still inside. After Step (7), all elements in $B(\mathfrak{a}, (t_{\mathfrak{q}})_{\mathfrak{q}}) \setminus \{0\}$ will have the same absolute values $|\bullet|_{\mathfrak{q}}$, $\mathfrak{q} \in S$,

whence they will all be equivalent under $\leq$. Hence, any non-zero element, such as a basis element, gives a valid result, and its valuation at $\mathfrak{q} \in S$ is given by $-t_{\mathfrak{q}}$. □

Baby Steps for $X = X_2$. We continue with the case $X = X_2 = [0,1]^n \setminus \{(1,\dots,1)\}$. Here, we always assume that $\leq$ is a lexicographic order as in Example 3.5.3. For that, write $S \setminus \{\mathfrak{p}\} = \{\mathfrak{q}_1, \dots, \mathfrak{q}_n\}$ and, as above, define

$$\mu \leq \mu' :\Longleftrightarrow (|\mu|_{\mathfrak{p}}, |\mu|_{\mathfrak{q}_1}, \dots, |\mu|_{\mathfrak{q}_n}) \leq_{\ell ex} (|\mu'|_{\mathfrak{p}}, |\mu'|_{\mathfrak{q}_1}, \dots, |\mu'|_{\mathfrak{q}_n}).$$

First, assume that $\deg \mathfrak{p} = 1$ and that $\deg \mathfrak{p}' = 1$ for another $\mathfrak{p}' \in S \setminus \{\mathfrak{p}\}$.

Algorithm 5.5.5: Baby Step Computation for $X = [0,1]^n \setminus \{(1,\dots,1)\}$, Special Version.

Input: reduced ideal $\mathfrak{b}$, $\mathfrak{p} \in S$ and the order $\leq$ as defined above.

Output: $\mu \in \mathrm{bs}_{\mathfrak{p}}^{[0,1]^n \setminus \{(1,\dots,1)\},\leq}(1, \mathfrak{b})$.

(1) Let $t_{\mathfrak{q}} := 0$ for all $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$, and $t_{\mathfrak{p}} := 1$.

(2) Compute a basis B of $B(\mathfrak{b}, (t_{\mathfrak{q}})_{\mathfrak{q}})$.

(3) If $|B| = 2$, continue with Step (6).

(4) Otherwise, set $t_{\mathfrak{p}} := t_{\mathfrak{p}} + 1$.

(5) Continue with Step (2).

(6) For $i = 1, \dots, n$, do the following:

  (i) Set $t_{\mathfrak{q}_i} := -1$.

  (ii) Compute a basis B of $B(\mathfrak{b}, (t_{\mathfrak{q}})_{\mathfrak{q}})$.

  (iii) If $|B| = 1$, return the element in B.

  (iv) Set $t_{\mathfrak{q}_i} := 0$.

Lemma 5.5.6. *This algorithm terminates and returns a valid result.*

Proof. For $(t_{\mathfrak{q}})_{\mathfrak{q}} = (0)_{\mathfrak{q}}$, we have $\dim_k B(\mathfrak{a}, (t_{\mathfrak{q}})_{\mathfrak{q}}) = 1$. Now, if $t_{\mathfrak{p}}$ is increased by one, the degree of the divisor increases by $\deg \mathfrak{p} = 1$, whence the dimension of $B(\mathfrak{b}, (t_{\mathfrak{q}})_{\mathfrak{q}})$ can increase at most by one. By Riemann's Inequality, it will eventually increase. For that reason, at one point it will equal 2.

In that case, there must be an element $f \in B(\mathfrak{b}, (t_{\mathfrak{q}})_{\mathfrak{q}})$ with $0 < |f|_{\mathfrak{p}'} < 1$, as when $t_{\mathfrak{p}'}$ is decreased by one, $\dim B(\mathfrak{b}, (t_{\mathfrak{q}})_{\mathfrak{q}})$ can decrease by most at one (it has to decrease exactly by one, since 1 is not an element anymore).

Now, for $\mu \in \mathrm{bs}_{\mathfrak{p}}^{X,\leq}(1,\mathfrak{b})$, there exists an i such that $-\nu_{\mathfrak{q}_i}(\mu) < 0$ (namely, for $\mathfrak{q}_i = \mathfrak{p}'$, as $\deg \mathfrak{p}' = 1$). Hence, if we choose the minimal i such that, for $t_{\mathfrak{q}_i} = -1$, $\dim_k B(\mathfrak{b}, (t_{\mathfrak{q}})_{\mathfrak{q}}) = 1$, we have that $\mathrm{bs}_{\mathfrak{p}}^{X,\leq}(1,\mathfrak{b}) = B(\mathfrak{b}, (t_{\mathfrak{q}})_{\mathfrak{q}}) \setminus \{0\}$. □

We are left with the case that $\deg \mathfrak{p} > 1$, or that $\deg \mathfrak{q} > 1$ for all $\mathfrak{q} \neq \mathfrak{p}$. In these cases, one proceeds as follows:

Algorithm 5.5.7: Baby Step Computation for $X = [0,1]^n \setminus \{(1,\ldots,1)\}$, General Version.

Input: reduced ideal $\mathfrak{b}$, $\mathfrak{p} \in S$ and the order $\leq$ as defined above.

Output: $\mu \in \mathrm{bs}_{\mathfrak{p}}^{[0,1]^n \setminus \{(1,\ldots,1)\},\leq}(1,\mathfrak{b})$ together with $(\nu_{\mathfrak{q}}(\mu))_{\mathfrak{q}\in S}$.

(1) Let $t_{\mathfrak{q}}^{(i)} := 0$ for all $\mathfrak{q} \in S \setminus \{\mathfrak{p}, \mathfrak{q}_i\}$ and $t_{\mathfrak{q}_i}^{(i)} := -1$, $1 \leq i \leq n$.

(2) Let

$$t_{\mathfrak{p}}^{(i)} := \max\left\{ \left\lceil \frac{1}{\deg \mathfrak{p}} \left(\sum_{\mathfrak{q}\in S\setminus\{\mathfrak{p},\mathfrak{q}_i\}} \deg \mathfrak{q} - \deg \mathrm{div}(\mathfrak{b}) \right) \right\rceil, 1 \right\}$$

for $i = 1, \ldots, n$.

(3) For $i = 1, \ldots, n$, do the following:

(i) Compute a basis B of $B(\mathfrak{b}, (t_{\mathfrak{q}}^{(i)})_{\mathfrak{q}})$.

(ii) If $|B| > 0$, continue with Step (6).

(4) Set $t_{\mathfrak{p}}^{(i)} := t_{\mathfrak{p}}^{(i)} + 1$ for $i = 1, \ldots, n$.

(5) Continue with Step (3).

(6) For $j = 1, \ldots, n$, do the following:

(i) Set $t_{\mathfrak{q}_j}^{(i)} := t_{\mathfrak{q}_j}^{(i)} - 1$.

(ii) Compute a basis B of $B(\mathfrak{b}, (t_{\mathfrak{q}}^{(i)})_{\mathfrak{q}})$.

(iii) If $|B| > 0$, continue with Step (6 i).

(iv) Set $t_{\mathfrak{q}_j}^{(i)} := t_{\mathfrak{q}_j}^{(i)} + 1$.

(7) Compute a basis B of $B(\mathfrak{b}, (t_{\mathfrak{q}}^{(i)})_{\mathfrak{q}})$.

(8) Return an arbitrary element of B together with $(-t_{\mathfrak{q}}^{(i)})_{\mathfrak{q}\in S}$.

Lemma 5.5.8. *This algorithm terminates and returns a valid result.*

Proof. This follows from the same arguments as the ones in the proofs of the Lemmas 5.5.4 and 5.5.6. □

5.6 Optimizations and Conclusion

Note that in all these algorithms in the last two sections, the tuples $(t_i)_i$ and ℓ for $B(\mathfrak{a}, (t_1, \ldots, t_n, \ell))$ range over a relatively small set, as the t_i's and ℓ can be bounded by Proposition 4.4.1 linearly in g and the $\frac{1}{\deg \mathfrak{p}}$'s, $\mathfrak{p} \in S$. Hence, one can precompute all the matrices $T_{\mathfrak{b}}M$ mentioned above to reduce the Riemann-Roch space computation to compute one $d \times d$-matrix multiplication with entries in $k(x)$, where $d = [K : k(x)]$, and one application of Paulus' algorithm to the resulting matrix. In this case, the precomputation requires storage of $\mathcal{O}(d^2 g^{|S|})$ elements of $k(x)$; hence, it only makes sense if all of d, $|S|$ and g are small.

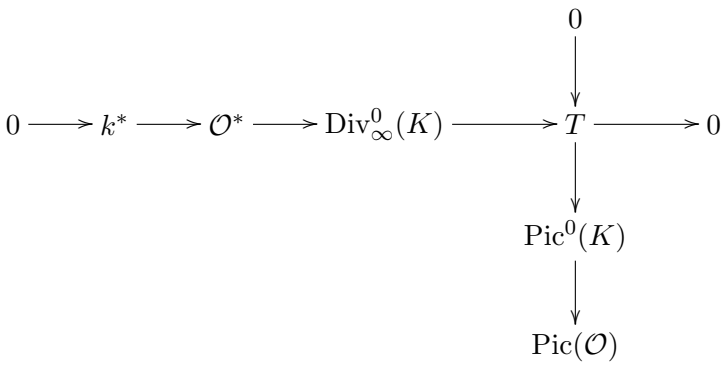
The main disadvantage of working with matrices instead of ideals of $\mathcal{O}_\infty$ is that the entries can get large, in particular if the t_i and ℓ get large. If one works with ideals of $\mathcal{O}_\infty$ by storing them by $\mathfrak{o}_\infty$-bases in Hermite Normal Form, the entries are bounded by the norm of the ideal.

It appears that our approach is best suited for function fields where small and simple generators of the ideals $\mathfrak{m}_\mathfrak{p} \cap \mathcal{O}_\infty$, $\mathfrak{p} \in S$ are known.

Chapter 6

Computations of Units and Baby Step-Giant Step Algorithms

In Computational Number Theory, one is interested in computing invariants of global fields; for example, one is interested in the structure of the (divisor) class group or in the regulator. Both these invariants are related by the following diagram with exact rows and columns:



Note that the regulator measures the 'size' of T.

Moreover, we will see in Section 6.1 that computation of the unit group amounts to the same as computation of the structure of the kernel T of the homomorphism $\mathrm{Pic}^0(K) \to \mathrm{Pic}(\mathcal{O})$. This essentially follows from the fact that the image of $\mathcal{O}^*$ in $\mathrm{Div}^0_\infty(K)$ equals $\mathrm{Princ}(K) \cap \mathrm{Div}^0_\infty(K)$, and that $T \cong \mathrm{Div}^0_\infty(K)/(\mathrm{Princ}(K) \cap \mathrm{Div}^0_\infty(K))$.

The first algorithm to compute the structure of T—in the special case $|S| = 2$—goes back to Lagrange: in the case of real quadratic number fields (i.e. $[K : \mathbb{Q}] = 2$ and $|S| = 2$), he used a sequence of baby steps to find two minima which are conjugated under $\mathcal{O}^*$. For $[K : \mathbb{Q}] = 3$, one has $|S| \in \{2, 3\}$; for $|S| = 2$ one can proceed essentially in the same way, but for $|S| = 3$ one needs a new idea. In his doctoral thesis, G. Voronoĭ presented an algorithm for this case. We will describe the basic idea behind this algorithm in Section 6.2.1. Note that the running times of these algorithms are $\mathcal{O}(D^\varepsilon R)$, where $D = |\Delta|$ is the absolute value of the discriminant Δ of K and R is the regulator of K.

The first improvement to this running time was made by D. Shanks, who applied his baby step-giant step algorithm to the computation of units in real quadratic number fields; the running time of his algorithm is $\mathcal{O}(D^\varepsilon \sqrt{R})$. J. Buchmann later generalized Voronoĭ's method to the general case of number fields with $|S| = 3$ [Buc85a, Buc85b]. As Voronoĭ's algorithm does not generalize to $|S| > 3$, Buchmann generalized Lagrange's method to the case of general number fields [Buc87a]; the running time is $\mathcal{O}(D^\varepsilon R)$. Finally, in his habilitation thesis, Buchmann managed to generalize the baby step-giant step method to arbitrary number fields [Buc87c], with the running time $\mathcal{O}(D^\varepsilon \sqrt{R})$.

In this chapter, we want to sketch these algorithms and present a baby step-giant step algorithm specialized to the case of function fields (see Section 6.2.2). Moreover, we will present a 'lifting' algorithm which is special to the case of function fields in Section 6.2.3. Then we will generalize Buchmann's algorithm to the unified case of global fields; we will present an algorithm which adapts an idea described by D. Terr [Ter00] in Section 6.5. Finally, we will discuss the practical aspects of the algorithms in Section 6.6, together with the possibility to use them for principal ideal tests.

We fix the same notation as in Chapter 4. Let $S' \subseteq S$ be a subset with $|S'| = |S| - 1$, and write $S' = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ and $S = S' \cup \{\mathfrak{p}_{n+1}\}$ with $|S| = n + 1$. Let $\mathbb{G} = \mathbb{Z}$ if K is a function field and $\mathbb{G} = \mathbb{R}$ if K is a number field.

Let $\Psi : K^* \to \mathbb{G}^{S'}$ be the map defined by

$$f \mapsto (-\nu_\mathfrak{p}(f))_{\mathfrak{p} \in S'}.$$

Then $\Lambda := \Psi(\mathcal{O}^*)$ is a full lattice in $\mathbb{G}^{S'}$, and for $\mathfrak{a} \in \mathrm{Id}(\mathcal{O})$, we get the map

$$\psi : \mathcal{E}(\mathfrak{a}) \to \mathbb{G}^{S'}/\Lambda, \qquad \mu \mapsto \Psi(\mu) + \Lambda.$$

Note that $R = \det \Lambda \cdot \prod_{i=1}^{n} \deg \mathfrak{p}_i$, whence $\det \Lambda = \mathcal{O}(R)$.

6.1 Computing Units in Global Fields

We have the exact sequence

$$0 \longrightarrow k^* \longrightarrow \mathcal{O}^* \xrightarrow{\Psi|_{\mathcal{O}^*}} \mathbb{G}^{S'} \longrightarrow \mathbb{G}^{S'}/\Lambda \longrightarrow 0,$$

and we have that $\mathbb{G}^{S'}/\Lambda \cong \mathrm{Rep}^f(\mathcal{O})$. Moreover, by Dirichlet's Unit Theorem, we know that $k^* \to \mathcal{O}^*$ splits, i.e. we have $\mathcal{O}^* = k^* \oplus \langle \varepsilon_1, \dots, \varepsilon_n \rangle$ for a set of units $\varepsilon_1, \dots, \varepsilon_n \in \mathcal{O}^*$. The set of all such generators $(\varepsilon_1, \dots, \varepsilon_n)$ corresponds (up to constants in k^*) to the set of all $\mathbb{Z}$-bases of the lattice $\Lambda \subseteq \mathbb{G}^{S'}$. Such a set of units $(\varepsilon_1, \dots, \varepsilon_n)$ is called a set of *fundamental units* of $\mathcal{O}$.

Therefore, computing a set of fundamental units corresponds to computing a $\mathbb{Z}$-basis of Λ. Moreover, as units are type (c) minima of $\mathcal{O}$, being able to compute $B(\mathcal{O}, (t_\mathfrak{p})_\mathfrak{p})$ allows to compute a set of fundamental units from a $\mathbb{Z}$-basis of Λ:

Lemma 6.1.1. *Assume that $(t_1, \dots, t_n) \in \Lambda$. Then*

$$B := B\left(\mathcal{O}, \left(t_1, \dots, t_n, -\frac{1}{\deg \mathfrak{p}_{n+1}} \sum_{i=1}^{n} t_i \deg \mathfrak{p}_i\right)\right) \setminus \{0\}$$

is exactly the set of all $\varepsilon \in \mathcal{O}^*$ with $\Psi(\varepsilon) = (t_1, \dots, t_n)$.

In particular, if K is a function field $(t_1, \dots, t_n)$ can never lie in Λ if $\deg \mathfrak{p}_{n+1}$ does not divide $\sum_{i=1}^{n} t_i \deg \mathfrak{p}_i$.

Proof. If $\varepsilon \in \mathcal{O}^*$ satisfies $\Psi(\varepsilon) = (t_1, \dots, t_n)$, we must have

$$\nu_{\mathfrak{p}_{n+1}}(\varepsilon) \deg \mathfrak{p}_{n+1} = -\sum_{i=1}^{n} \nu_{\mathfrak{p}_i}(\varepsilon) \deg \mathfrak{p}_i = \sum_{i=1}^{n} t_i \deg \mathfrak{p}_i.$$

Therefore, all such ε lie in B.

Conversely, if $\varepsilon \in \mathcal{O} \setminus \{0\}$ satisfies $\nu_{\mathfrak{p}_i}(\varepsilon) \geq -t_i$ for $i = 1, \dots, n$ and $\nu_{\mathfrak{p}_{n+1}}(\varepsilon) \geq \frac{1}{\deg \mathfrak{p}_{n+1}} \sum_{i=1}^{n} t_i \deg \mathfrak{p}_i$, then $\sum_{i=1}^{n+1} \nu_{\mathfrak{p}_i}(\varepsilon) \deg \mathfrak{p}_i \geq 0$. As we have $\sum_{\mathfrak{p} \notin S} \nu_\mathfrak{p}(\varepsilon) \deg \mathfrak{p} \geq 0$ (because $\varepsilon \in \mathcal{O}$) and $\sum_{\mathfrak{p} \in \mathcal{P}_K} \nu_\mathfrak{p}(\varepsilon) \deg \mathfrak{p} = 0$ (by the Product Formula), we must have that $\nu_\mathfrak{p}(\varepsilon) = 0$ for all $\mathfrak{p} \notin S$, i.e. we have $\varepsilon \in \mathcal{O}^*$.

The last statement follows from the fact that if the division condition would be false, $\nu_{\mathfrak{p}_{n+1}}(\varepsilon)$ would not be an integer, which cannot happen in the function field case. □

Therefore, computing a set of fundamental units is equivalent to computing a lattice basis of Λ. Note that with 'equivalent', we do not mean that changing from one representation to another can be computed efficiently; this is by no means the case, as only writing down a set of fundamental units has running time $\mathcal{O}(R)$ (where R is the regulator of $\mathcal{O}$), while writing down (an approximation of) a lattice basis of Λ can be done much faster.

For that reason, we will mainly be interested in computing a lattice basis of Λ, as this can be done in time faster than $\mathcal{O}(R)$.

We know that $\mathbb{G}^n$ is generated (as a $\mathbb{G}$-module) by the unit vectors $e_1, \ldots, e_n$, where e_i is the element of $\mathbb{G}^n$ whose i-th coordinate is 1 and whose other coordinates are 0. One can interpret relations of these elements in $\mathbb{G}^n/\Lambda$ as exactly the elements of Λ: using the tempting, but incorrect (in case $\mathbb{G} = \mathbb{R}$) notation of $\lambda(v + \Lambda)$ for $(\lambda v) + \Lambda$ for $\lambda \in \mathbb{G}$, $v \in \mathbb{G}^n$, we have for $\lambda_1, \ldots, \lambda_n \in \mathbb{G}$

$$\sum_{i=1}^{n} \lambda_i (e_i + \Lambda) = 0 \text{ in } \mathbb{G}^n/\Lambda \iff (\lambda_1, \ldots, \lambda_n) \in \Lambda.$$

Therefore, one way to compute elements of Λ is to compute relations of $e_1 + \Lambda, \ldots, e_n + \Lambda$ in $\mathbb{G}^n/\Lambda$. This also motivates that we call Λ the *relation lattice* of the elements $e_1 + \Lambda, \ldots, e_n + \Lambda$.

Now, $\mathbb{G}^n/\Lambda \cong \mathrm{Rep}^f(\mathcal{O})$, and we can compute the image of elements $(t_1, \ldots, t_n) \in \mathbb{G}^n$ in $\mathrm{Rep}^f(\mathcal{O})$ by reducing $([\mathcal{O}]_\sim, (t_1, \ldots, t_n))$ to an f-representation. This is what will be exploited in the next sections.

6.2 Algorithms for Function Fields

In the function field case, $\mathrm{Rep}^f(\mathcal{O}) \cong \mathbb{G}^n/\Lambda$ is a finite abelian group, and we know a set of generators. Hence, we can apply any algorithm for computing the structure of such a finite abelian group, as it will return a basis of the relation lattice of these generators, which is exactly Λ.

Note that baby steps in the infrastructure can be interpreted as adding generators to elements. Using this interpretation, we sketch how Voronoĭ's method can be understood and applied in the case of function fields in Section 6.2.1. Then, we will apply an algorithm by J. Buchmann and A. Schmidt to obtain a baby step-giant step algorithm in Section 6.2.2. After that, we will exploit the fact that for function fields, one can do constant field extensions, to ease computation of units in certain cases (Section 6.2.3). Finally, in Section 6.2.4, we will give implementation results.

6.2.1 Voronoĭ's Algorithm

In Lagrange's method, one does baby steps in one direction until one obtains two minima which are conjugated under $\mathcal{O}^*$. In the original setting, i.e. $|S| = 2$, the obtained sequence of minima modulo $\mathcal{O}^*$ will be purely periodic.

If one does the same in a general global field, by Theorem 3.2.6 we obtain that the sequence is periodic, but the preperiod may be non-trivial. Nonetheless, one obtains a non-trivial unit this way. Voronoĭ (and, in a more general setting, Buchmann [Buc85a, Buc85b] and Y. Lee, R. Scheidler and C. Yarrish [LSY03]) showed how one can obtain a second non-trivial unit such that both units together with the constants generate the unit group in case $|S| = 3$.

We will begin by describing the algorithms in the context of finite abelian groups. As finite abelian groups can be interpreted as infrastructures (see Section 2.4), we can apply Lagrange's and Voronoĭ's algorithm to such groups. Only baby steps are used in these algorithms, and we use the fact that at least in the one-dimensional case, baby steps correspond to multiplication by a generator of the group.

Given a finite abelian group G with one generator g, one computes the structure of G by computing the order of g; one way to do this is computing $g, 2g, 3g, \ldots, ng$ until $ng = 0$: then $G \cong \mathbb{Z}/n\mathbb{Z}$ and the isomorphism is given by $\mathbb{Z}/n\mathbb{Z} \to G$, $z + n\mathbb{Z} \mapsto zg$. This corresponds to Lagrange's algorithm. Using the same analogy, Voronoĭ's algorithm works as follows:

Remark 6.2.1 (Voronoĭ's Algorithm). Let G be a finite abelian group with two generators a_1, a_2.

(1) Compute $a_1, 2a_1, 3a_1, \ldots, n_1a_1$ until $n_1a_1 = 0$.

(2) Compute $a_2, 2a_2, 3a_2, \ldots$ until $n_2a_2 \in \langle a_1 \rangle$, by comparing every n_2a_2 with every element ta_1, $0 \leq t < n_1$.

If $n_2a_2 = ta_1$, then $|G| = n_1n_2$. Moreover, if G is given as $G = \mathbb{Z}^2/\Lambda$ and $a_i = e_i + \Lambda$, then $(n_1, 0), (-t, n_2)$ is a basis of Λ.

The general technique behind this can be described as follows: if G is generated by $g_1, \ldots, g_n$, compute iteratively, $1 \leq i \leq n$, the order a_{ii} of g_i in $G/\langle g_1, \ldots, g_{i-1} \rangle$ and compute a representation $-a_{ii}g_i = a_{i1}g_1 + \cdots + a_{i,i-1}g_{i-1}$. With $a_{ij} = 0$ for $j > i$, the matrix $(a_{ij})_{1 \leq i,j \leq n}$ generates the relation lattice of $g_1, \ldots, g_n$.

In the function field case, one can apply this directly to the infrastructure obtained from such a field, to obtain algorithms for computing the unit

group. Unfortunately, these algorithms are both slow and use a large amount of memory. If $|G| = \langle g_1, \ldots, g_n \rangle$, then one needs to store $|\langle g_1, \ldots, g_{n-1} \rangle| = \mathcal{O}(|G|)$ group elements and needs to compute

$$|\langle g_1, \ldots, g_{n-1} \rangle| + |G/\langle g_1, \ldots, g_{n-1} \rangle| = \mathcal{O}(|G|)$$

group operations. Note that the running time is minimal if

$$|G/\langle g_1, \ldots, g_{n-1} \rangle| \approx |\langle g_1, \ldots, g_{n-1} \rangle| \approx \sqrt{|G|}.$$

6.2.2 A Baby Step-Giant Step Algorithm for Function Fields

We have seen that computing units of a function fields amounts to compute the structure of the finite abelian group $G = \mathrm{Rep}^f(\mathcal{O}) \cong \mathbb{G}^n/\Lambda$. Two modern algorithms for achieving this goal are the following:

(1) the algorithm by J. Buchmann and A. Schmidt [BS05], which can be seen as a direct generalization of Shanks' baby step-giant step algorithm;

(2) the algorithm by E. Teske [Tes98], which uses a variant of the Pollard ρ algorithm.

If the order $|\mathbb{G}^n/\Lambda|$ or a multiple is known and happens to only have moderately large prime factors, one can also use another algorithm by E. Teske [Tes99], which is a variation of the Pohlig-Hellman method.

Note that all of these algorithms do not require to compute inverses (with the exception that the Buchmann-Schmidt algorithm requires the inverses of the generators, which can be as easy computed as the generators itself). Hence, there is no need for ideal inversion.

Also note that these algorithms rely (more or less) heavily on comparisons of elements in the infrastructure. If $\deg \mathfrak{p} > 1$ for all $\mathfrak{p} \in S$, the relation $\sim$ on reduced ideals can be non-trivial, whence one has to use something as the conditions from Proposition 4.1.2 to do a comparison; unfortunately, this is slow. For an idea how to circumvent this, see Section 6.2.3.

For the rest of this section, we want to sketch how the Buchmann-Schmidt algorithm works. Recall that the aim is to compute the order a_{ii} of g_i in $G/\langle g_1, \ldots, g_{i-1} \rangle$ for $i = 1, \ldots, n$. Buchmann's and Schmidt's algorithm uses a variation of Shanks' baby step-giant step algorithm, as described in [Ter00], to compute orders, and combines it with a baby step-giant step technique for checking if an element lies in $\langle g_1, \ldots, g_{i-1} \rangle$.

The running time of this algorithm is $\mathcal{O}(n\sqrt{|G|})$ group operations, and one needs to store $\mathcal{O}(\sqrt{|G|})$ group elements. Hence, in our case, as $|\mathbb{G}^n/\Lambda| =$

$\mathcal{O}(R)$, we have that the algorithm requires $\mathcal{O}(\sqrt{R})$ operations in the infrastructure (note that we incorporate $|S|-1 \leq [K : k(x)]$ into the $\mathcal{O}$-constant).

Therefore, if one applies Buchmann's and Schmidt's algorithm to infrastructures obtained from global function fields with $\deg \mathfrak{p} = 1$ for some $\mathfrak{p} \in S$, one can see this as a direct generalization of Shanks' baby step-giant step method for the case of unit rank one.

Note that we will use a very similar strategy for our algorithm in Section 6.5.

6.2.3 Lifting Units

This subsection is joint work with Mark Bauer (University of Calgary).

In the case $\deg \mathfrak{p} > 1$ for all $\mathfrak{p} \in S$, one could proceed as follows. First, one does a constant field extension, i.e. one chooses a finite field extension k'/k and considers $K' = k'K$. If k'/k is chosen such that at least one of the infinite primes splits such that one of the resulting primes has degree one, one can use the techniques we described to compute the units of K'. Then, one can try to use them to compute the units of K.

Assume that k'/k is Galois. We then know that K'/K is a Galois extension with $[K' : K] = [k' : k]$, and k' is the full field of constants of K'. Denote the set of all places of K' by $\mathcal{P}_{K'}$. Let S' be the set of places of K' which lie over places in S. Note that S' is *not* $S \setminus \{\mathfrak{p}_{n+1}\}$ as in the rest of this chapter.

Assume that $\{f_1, \ldots, f_n\}$ is a $k(x)$-basis of K; in that case, it is also a $k'(x)$-basis of K'. If $\sigma \in \mathrm{Gal}(k'/k)$, then σ induces an automorphism $\sigma^* \in \mathrm{Gal}(K'/K)$ by

$$\sum_{i=1}^{n} \frac{\lambda_i}{\mu_i} f_i \mapsto \sum_{i=1}^{n} \frac{\sigma^*(\lambda_i)}{\sigma^*(\mu_i)} f_i,$$

where $\lambda_i, \mu_i \in k'[x]$ and $\sigma^*(\sum_{i=0}^{\ell} a_i x^i) = \sum_{i=0}^{\ell} \sigma(a_i) x^i$ for $a_i \in k'$. More precisely, the map

$$\mathrm{Gal}(k'/k) \to \mathrm{Gal}(K'/K), \qquad \sigma \mapsto \sigma^*$$

is a group isomorphism.

Lemma 6.2.2. *Let*

$$\Phi : (K')^* \to \mathbb{Z}^{\mathcal{P}_{K'}}, \qquad f \mapsto (\nu_{\mathfrak{p}}(f))_{\mathfrak{p} \in \mathcal{P}_{K'}}$$

and let $\mathrm{Gal}(K'/K)$ *act on* $\mathbb{Z}^{\mathcal{P}_{K'}}$ *by*

$$\sigma \mapsto \begin{cases} \mathbb{Z}^{\mathcal{P}_{K'}} \to \mathbb{Z}^{\mathcal{P}_{K'}}, \\ (z_{\mathfrak{p}})_{\mathfrak{p}\in\mathcal{P}_{K'}} \mapsto (z_{\sigma^{-1}(\mathfrak{p})})_{\mathfrak{p}\in\mathcal{P}_{K'}} \end{cases}$$

Then Φ *is a morphism of* $\mathrm{Gal}(K'/K)$*-modules.*

Proof. This follows from the fact that $\nu_{\mathfrak{p}} : K^* \to \mathbb{Z}$ is a group homomorphism and that $\nu_{\sigma^{-1}(\mathfrak{p})}(f) = \nu_{\mathfrak{p}}(\sigma(f))$ for all $f \in K^*$ and $\sigma \in \mathrm{Gal}(K'/K)$. □

Proposition 6.2.3. *Assume that the Galois extension* k'/k *is cyclic. Let* $U \subseteq (K')^*$ *be a subset which is closed under multiplication by elements of* $(k')^*$*. Then*

$$\Phi(U^{\mathrm{Gal}(K'/K)}) = \Phi(U)^{\mathrm{Gal}(K'/K)},$$

where we write

$$V^{\mathrm{Gal}(K'/K)} := \{v \in V \mid \sigma(v) = v \text{ for all } \sigma \in \mathrm{Gal}(K'/K)\}$$

for any subset V *of a* $\mathrm{Gal}(K'/K)$*-module.*

Proof. Clearly, by the lemma, $\Phi(U^{\mathrm{Gal}(K'/K)}) \subseteq \Phi(U)^{\mathrm{Gal}(K'/K)}$. Let $u \in U$ be any element with $\Phi(u) \in \Phi(U)^{\mathrm{Gal}(K'/K)}$, i.e. $\Phi(\sigma(u)) = \Phi(u)$ for a generator σ of $\mathrm{Gal}(K'/K)$. This means $\Phi(\frac{\sigma(u)}{u}) = 0$, whence we have $\frac{\sigma(u)}{u} \in (k')^*$. By Hilbert's Theorem 90, $\frac{\sigma(u)}{u} = \frac{\sigma(v)}{v}$ for some $v \in (k')^*$, whence $\frac{\sigma(uv^{-1})}{uv^{-1}} = 1$. That means that $uv^{-1} \in (K')^{\mathrm{Gal}(K'/K)} = K$, and as U is closed under multiplication by elements of $(k')^*$, we have $uv^{-1} \in U$. Hence, $\Phi(u) = \Phi(uv^{-1}) \in \Phi(U^{\mathrm{Gal}(K'/K)})$. □

This abstract result gives a way to solve our original problem on units:

Corollary 6.2.4. *Assume that* $\mathrm{Gal}(k'/k) = \langle\sigma\rangle$*. Consider*

$$\Psi' : (K')^* \to \mathbb{Z}^{S'}, \qquad f \mapsto (\nu_{\mathfrak{p}}(f))_{\mathfrak{p}\in S'}.$$

Let the group of S'*-units of* K' *be decomposed as* $(\mathcal{O}')^* = (k')^* \times \langle u'_1, \ldots, u'_n\rangle$*. Let* $\mathfrak{p}_1, \ldots, \mathfrak{p}_{|S|}$ *be representatives of the orbits of* S' *under* $\mathrm{Gal}(K'/K)$ *and define* $v_i := (x_{\mathfrak{p}})_{\mathfrak{p}\in S'}$ *with* $x_{\mathfrak{p}} = 1$ *if* $\mathrm{Gal}(K'/K)\mathfrak{p} = \mathrm{Gal}(K'/K)\mathfrak{p}_i$ *and* $x_{\mathfrak{p}} = 0$ *otherwise,* $1 \le i \le |S|$*.*

Then $v_1, \ldots, v_{|S|}$ *is a basis of the lattice*

$$\{(x_{\mathfrak{p}})_{\mathfrak{p}\in S'} \in \mathbb{Z}^{S'} \mid x_{\sigma^*(\mathfrak{p})} = x_{\mathfrak{p}} \text{ for every } \mathfrak{p} \in S'\}.$$

If $\tilde{u}_1, \dots, \tilde{u}_\ell$ is a basis of the lattice $\langle \Psi'(u'_1), \dots, \Psi'(u'_n)\rangle \cap \langle v_1, \dots, v_{|S|}\rangle$, then

$$\Psi'(\mathcal{O}^*) = \langle \tilde{u}_1, \dots, \tilde{u}_\ell \rangle.$$

In particular, if $u_1, \dots, u_\ell \in \mathcal{O}^*$ with $\Psi'(u_i) = \tilde{u}_i$, $1 \le i \le \ell$, then $\mathcal{O}^* = k^* \times \langle u_1, \dots, u_\ell \rangle$.

Note that instead of to the whole group of $(\mathcal{O}')^*$, one could also apply this to any subgroup $U \subseteq (\mathcal{O}')^*$ with $k^* \subseteq U$.

Proof. Set $L := \{(x_\mathfrak{p})_{\mathfrak{p}\in S'} \in \mathbb{Z}^{S'} \mid x_{\sigma^*(\mathfrak{p})} = x_\mathfrak{p} \text{ for every } \mathfrak{p} \in S'\}$. Clearly, $(x_\mathfrak{p})_\mathfrak{p} \in L$ if, and only if, $x_\mathfrak{p} = x_\mathfrak{q}$ for all $\mathfrak{p}, \mathfrak{q} \in S'$ with $\mathrm{Gal}(K'/K)\mathfrak{p} = \mathrm{Gal}(K'/K)\mathfrak{q}$. Hence, $(x_\mathfrak{p})_\mathfrak{p} = \sum_{i=1}^{|S|} x_{\mathfrak{p}_i} v_i$. This shows that $v_1, \dots, v_{|S|}$ is a basis of L.

Next, $\mathcal{O}^* = (\mathcal{O}')^* \cap K = ((\mathcal{O}')^*)^{\mathrm{Gal}(K'/K)}$ and $(\mathcal{O}')^*$ is closed under multiplication by elements of $(k')^*$. Moreover, all elements $u \in (\mathcal{O}')^*$ satisfy $\nu_\mathfrak{p}(u) = 0$ for all $\mathfrak{p} \notin S'$. Therefore, by the proposition,

$$\Psi'(\mathcal{O}^*) = \Psi'(((\mathcal{O}')^*)^{\mathrm{Gal}(K'/K)}) = \Psi'((\mathcal{O}')^*)^{\mathrm{Gal}(K'/K)} = \Phi((\mathcal{O}')^*) \cap L$$

as $L = (\mathbb{Z}^{S'})^{\mathrm{Gal}(K'/K)}$. Finally, $\mathcal{O}^*$ is fully determined by $\Psi'(\mathcal{O}^*)$ up to elements in k^*. □

Therefore, to determine a set of fundamental units for $\mathcal{O}^*$, we have to find a basis of the intersection of $\Psi'(\mathcal{O}^*) = \langle \Psi'(u'_1), \dots, \Psi'(u'_n)\rangle$ and $L = \langle v_1, \dots, v_{|S|}\rangle$. Set $\tilde{u}'_i := \Psi'(u'_i)$, $1 \le i \le n$.

Computing intersections of $\mathbb{Z}$-lattices $\langle \tilde{u}'_1, \dots, \tilde{u}'_n\rangle$ and $\langle v_1, \dots, v_{|S|}\rangle$ is equivalent to computing all solutions $(\lambda_1, \dots, \lambda_n, \mu_1, \dots, \mu_{|S|}) \in \mathbb{Z}^{n+|S|}$ of the system of linear equations $\sum_{i=1}^n \lambda_i \tilde{u}'_i + \sum_{j=1}^{|S|} \mu_j v_j = 0$:

if $w_1, \dots, w_t \in \mathbb{Z}^{n+|S|}$ is a basis for the set of solutions, then $\pi_1 : \mathbb{Z}^{n+|S|} \to \mathbb{Z}^{|S'|}$, $(x_i)_i \mapsto \sum_{i=1}^n x_i \tilde{u}'_i$ and $\pi_2 : \mathbb{Z}^{n+|S|} \to \mathbb{Z}^{|S'|}$, $(x_i)_i \mapsto -\sum_{j=1}^{|S|} x_{n+j} v_j$ satisfy $\pi_1(w_i) = \pi_2(w_i)$, $1 \le i \le t$ and that $\pi_1(w_1), \dots, \pi_1(w_t)$ generate $\langle \tilde{u}'_1, \dots, \tilde{u}'_n\rangle \cap \langle v_1, \dots, v_{|S|}\rangle$.

Hence, using two Hermite Normal Form computations (one for computing the set of all solutions and one for turning the generating set into a basis), one can compute a basis of $\langle \tilde{u}'_1, \dots, \tilde{u}'_n\rangle \cap \langle v_1, \dots, v_{|S|}\rangle$.

Note that we are only interested in the absolute values of the units, as the units itself will be too large. Hence, there is no need to compute valuations or find elements with specified valuations, except for finding out the action of $\mathrm{Gal}(K'/K)$ on S'.

Splitting of the Infinite Places and the Action of $\mathrm{Gal}(K'/K)$**.** We want to investigate on how to compute S' and the action of $\mathrm{Gal}(K'/K)$ on S'. This contains and extends the discussion in Section 5.2.

Let $\mathfrak{o}_\infty$ denote the valuation ring of the infinite place of $k(x)$, i.e. $\mathfrak{o}_\infty = \{f \in k(x) \mid \deg f \leq 0\}$. Then its maximal ideal is $\mathfrak{p}_\infty = \{f \in k(x) \mid \deg f < 0\}$. Let $\mathcal{O}_\infty$ be the integral closure of $\mathfrak{o}_\infty$ in K and $\mathcal{O}'_\infty$ be the integral closure of $\mathfrak{o}_\infty$ in K', which equals $k'\mathcal{O}_\infty$.

Then, by [Sti93, p. 71, Proposition III.2.10], $\mathcal{O}_\infty$ is a principal ideal domain, and its non-zero prime ideal correspond to the places in S. By the same argument, $\mathcal{O}'_\infty$ is a principal ideal domain whose non-zero prime ideals correspond to the places in S'. Assume that $\mathcal{O}_\infty = \mathfrak{o}_\infty[\rho]$ for some $\rho \in K^*$ and let $f \in \mathfrak{o}_\infty[t]$ be the minimal polynomial of ρ over $k(x)$.

Consider the projection $\pi : \mathfrak{o}_\infty \to \mathfrak{o}_\infty/\mathfrak{m}_\infty = k$ and compute the factorization of $\pi(f)$; for example, $\pi(f) = \prod_{i=1}^{\ell} g_i^{e_i} \in k[t]$ with pairwise distinct monic prime polynomials $g_i \in k[t]$ and $e_i \in \mathbb{N}$. By Kummer's Theorem [Sti93, p. 76, Theorem III.3.7], the places in S correspond to the g_i: if $\mathfrak{m}_\mathfrak{p}$ is the valuation ideal of the place $\mathfrak{p}$, then $\mathfrak{m}_\mathfrak{p} \cap \mathcal{O}_\infty = \frac{1}{x}\mathcal{O}_\infty + g_i(\rho)\mathcal{O}_\infty$, $\deg \mathfrak{p} = \deg g_i$ and e_i is the ramification index of $\mathfrak{p}$ over $\mathfrak{m}_\infty$. Define $f_i := g_i(\rho)$.

If $e_i > 1$, then $\nu_\mathfrak{p}(f_i) = 1$ and $\nu_\mathfrak{q}(f_i) = 0$ for $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$. If $e_i = 1$, either f_i satisfies this, or $f_i + \frac{1}{x}$ does; in the latter case, replace f_i by $f_i + \frac{1}{x}$, i.e. we have $\nu_\mathfrak{p}(f_i) = 1$ and $\nu_\mathfrak{q}(f_i) = 0$ for $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$. The case $\nu_\mathfrak{p}(g_i(\rho)) = 1$ can be detected by checking whether $\frac{1}{x}$ lies in the $\mathcal{O}'_\infty$-ideal generated by $g_i(\rho)$; it lies in there if, and only if, $\nu_\mathfrak{p}(g_i(\rho)) \leq e_i = 1$.

Let $\mathfrak{o}'_\infty = \{f \in k'(x) \mid \deg f \leq 0\}$ and $\mathfrak{m}'_\infty = \{f \in k'(x) \mid \deg f < 0\}$, and $\pi' : \mathfrak{o}'_\infty \to \mathfrak{o}'_\infty/\mathfrak{m}'_\infty = k'$. One has $\mathcal{O}'_\infty = \mathfrak{o}'_\infty[\rho]$. Similarly, one can consider $\pi'(f) \in k'[t]$. As $\pi'(f) = \pi(f) = \prod_{i=1}^{\ell} g_i^{e_i}$ and as k'/k is Galois we get $g_i = h_{i1} \cdots h_{in_i}$ for some distinct irreducible polynomials $h_{ij} \in k'[t]$, i.e. the prime factorization of $\pi'(f)$ is $\prod_{i=1}^{\ell} \prod_{j=1}^{n_i} h_{ij}^{f_i}$. Again, the places in S' correspond to the h_{ij}, with $\deg \mathfrak{p} = \deg h_{ij}$, and the place of K' corresponding to h_{ij} lies over the place of K corresponding to g_i. Using the same method as above, one can find generators f_{ij} of the prime ideals of $\mathcal{O}'_\infty$ corresponding to the h_{ij}.

Let $\sigma \in \mathrm{Gal}(k'/k)$. Then one can determine the behavior of σ^* on S' as follows: first, the orbit of a place $\mathfrak{p}$ corresponding to h_{ij} is the set of places corresponding to $h_{i1}, \ldots, h_{in_i}$. Second, $(\sigma^*)^{-1}(\mathfrak{p})$ can be found by computing $\sigma^*(h_{ij})$ and checking whether $\sigma^*(h_{ij}) \in h_{ij'}\mathcal{O}'_\infty = h_{ij'}\mathfrak{o}'_\infty[\rho]$, $1 \leq j' \leq n_i$. This can be done by computing a $\mathfrak{o}'_\infty$-basis of $h_{ij'}\mathfrak{o}'_\infty[\rho]$ and writing $\sigma^*(h_{ij})$ in terms of this basis (treated as a $k'(x)$-basis); if the coefficients lie in $\mathfrak{o}'_\infty$,

then $\sigma^*(h_{ij}) \in h_{ij'}\mathfrak{o}'_\infty[\rho]$. Alternatively, one can compute $\frac{\sigma^*(h_{ij})}{h_{ij'}}$ (or $\frac{h_{ij'}}{\sigma^*(h_{ij})}$) and test if it lies in $\mathfrak{o}'_\infty[\rho]$.

6.2.4 Explicit Computations

We implemented our algorithm for computing in $\mathrm{Pic}^0(K)$ using the infrastructure for a function field K with at least one infinite place of degree one in MAGMA [BCP97] and in C++. The C++ implementation relies on MAGMA to compute the infinite places, integral bases of the maximal orders and multiplication tables.

The C++ implementation also shows that the integral bases, their multiplication tables, the degrees of the infinite places and generators of their prime ideals suffice to do computations in the infrastructure.

We did several experiments using the C++ version and will present the running times in this section. For the experiments, we used three cubic and two quartic equations over various prime fields $\mathbb{F}_p$, where $p \leq 100$ or $p \leq 200$, such that the exact constant field is $\mathbb{F}_p$ and all infinite places have degree one.

The fields are as follows:

(1) The first cubic field is defined by the equation $y^3 = x^3 + x^2 + x + 1$ and is of genus 1 (with

$$p \in \{7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, \\ 103, 109, 127, 139, 151, 157, 163, 181, 193, 199\});$$

the regulator is rather small (the largest value is 217 for $p = 199$).

(2) The second cubic field is defined by the equation $y^3 = x^6+x^3+x^2+x+1$ and is of genus 4 (with

$$p \in \{7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97\});$$

the regulator is of medium size, i.e. begins in the range of $4.8 \cdot 10^3$ for $p = 7$ and ends in the range of $7.7 \cdot 10^7$ for $p = 97$.

(3) The third cubic field is defined by the equation $y^3 = x^9 + x^5 + x^3 + x^2 + x + 1$ and is of genus 7 (with

$$p \in \{7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97\});$$

its regulator is large, i.e. begins in the range of $1.6 \cdot 10^6$ for $p = 7$ and ends in the range of $2.6 \cdot 10^{12}$ for $p = 97$.

(4) The first quartic field is defined by the equation $y^4 = x^4 + x^3 + x + 1$ and is of genus 1 (with

$$p \in \{5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, \\ 101, 109, 113, 137, 149, 157, 173, 181, 193, 197\});$$

the regulator is again rather small, i.e. never exceeds 200 for all $p \leq 200$.

(5) The second quartic field is defined by the equation $y^4 = x^4 + x + 1$ and is of genus 3 (with

$$p \in \{5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, \\ 101, 109, 113, 137, 149, 157, 173, 181, 193, 197\});$$

the regulator is of medium size, i.e. begins with 549 for $p = 5$ and attains a maximum in the range of $6.8 \cdot 10^6$ for $p = 181$.

In Figure 6.1 (see page 101), the relative running times for MAGMA and our implementations are presented. Relative means that we divided the effective running times by the expected theoretic running times and plotted the quotient. For MAGMA, we plotted

$$\frac{t}{\exp(\sqrt{2 \cdot (2g \log p) \cdot \log(2g \log p)})},$$

where t is the running time, g the genus and p the size of the prime field (this is in fact the expected theoretic running time for computing the structure of the divisor class group, which is done by MAGMA before computing the unit group; see [Hes99]). For applying the Buchmann-Schmidt algorithm [BS05], which we call *BSGS*, and for applying Teske's algorithm [Tes98], which we call *Pollard* ρ, we plotted $\frac{t}{\sqrt{R}}$, where t is the running time and R the regulator. Finally, for the group theoretic version of Voronoĭ's algorithm (as described in Section 6.2.1), denoted by *Voronoĭ* in the graphs, we plotted $\frac{t}{R}$, where t is the running time and R the regulator. For the probabilistic algorithms (MAGMA and Pollard ρ), we did at least five runs and took the arithmetic median; an interval in which the running times for all runs lie is also plotted.

The absolute running times (in seconds) together with the exact regulators can be found in the tables in Figures 6.2, 6.3, 6.4, 6.5 and 6.6 (see pages 102–104). The results show that for the Buchmann-Schmidt algorithm (*BSGS*) and Teske's algorithm (*Pollard* ρ), the running time behaves (up to some small changes) as expected.

The same is more or less true for Voronoĭ's algorithm; there are some exceptions, most notably for the second cubic field for $p = 7$ and $p = 13$. It turns out that one has two extreme cases here: for $p = 7$, the order of the second generator in the residue group is 1, while for $p = 13$, the order of the second generator in the residue group is 152. Hence, for $p = 7$, one has to do $R = 4881$ group operations, while for $p = 13$, one has to do $\frac{R}{152} + 152 = 608$ group operations. In particular, the quotient $\frac{\text{group operations}}{R}$ for $p = 7$ is 1, while the quotient for $p = 13$ is $\approx 8.8 \cdot 10^{-3}$.

Please note that we did not applied Voronoĭ's algorithm for fields with $R \geq 10^7$. Also note that the C++ implementation is not exactly optimized and in a very general form. Finally, note that the overall running time for all runs, including the MAGMA computations, was 889 CPU days; the computations were done on a Sun Fire 6800 machine with 900 and 1050 MHz UltraSPARC III CPUs and enough main memory to store all required data without swapping.

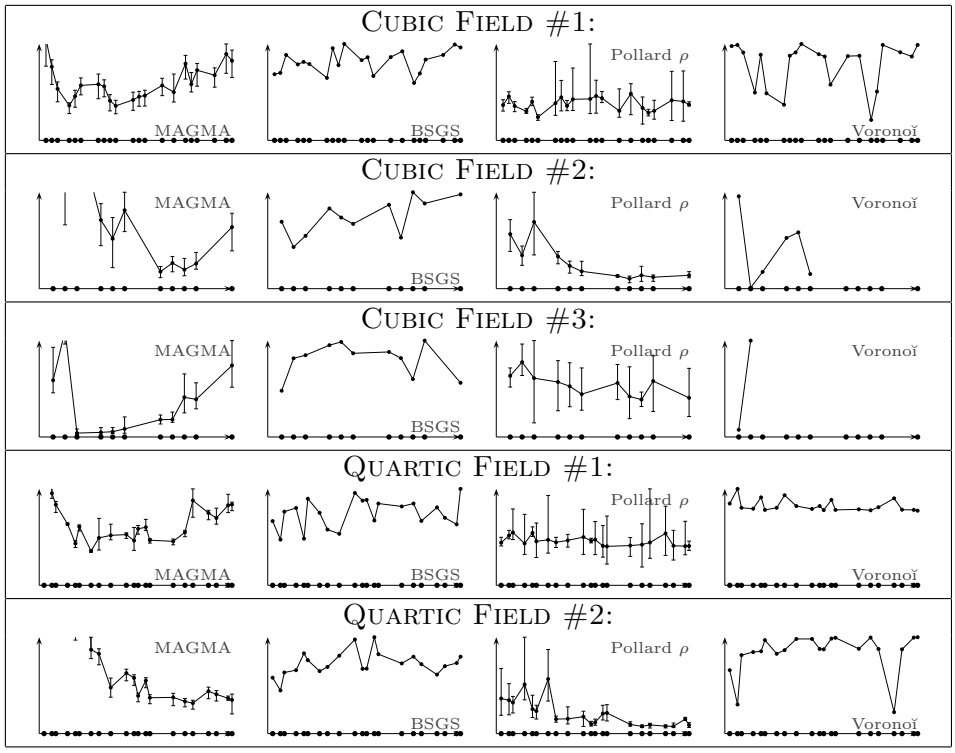


Figure 6.1: Relative running times of the various algorithms for different global function fields.

p	MAGMA	BSGS	Pollard ρ	Voronoĭ	R
7	0.49 s	0.16 s	1.64 s	0.11 s	13
13	0.83 s	0.12 s	1.50 s	0.06 s	7
19	0.93 s	0.25 s	1.93 s	0.15 s	19
31	1.12 s	0.27 s	1.99 s	0.12 s	28
37	1.74 s	0.19 s	1.80 s	0.10 s	13
43	2.55 s	0.37 s	2.16 s	0.22 s	52
61	3.79 s	0.21 s	2.40 s	0.08 s	25
67	4.02 s	0.55 s	4.94 s	0.60 s	79
73	3.23 s	0.22 s	1.94 s	0.15 s	19
79	3.06 s	0.53 s	4.33 s	0.58 s	67
97	4.42 s	0.30 s	2.97 s	0.24 s	31
103	5.06 s	0.55 s	5.63 s	0.73 s	97
109	5.48 s	0.15 s	1.89 s	0.06 s	12
127	7.85 s	0.34 s	2.31 s	0.28 s	37
139	7.52 s	0.69 s	6.94 s	1.01 s	133
151	12.98 s	0.51 s	5.54 s	0.32 s	175
157	9.87 s	0.18 s	1.42 s	0.07 s	16
163	12.78 s	0.73 s	5.12 s	1.55 s	181
181	13.13 s	0.47 s	4.23 s	0.53 s	67
193	18.48 s	0.55 s	4.29 s	0.55 s	73
199	17.54 s	0.92 s	6.79 s	1.86 s	217

Figure 6.2: Absolute running times and regulators for Cubic Field #1.

p	MAGMA	BSGS	Pollard ρ	Voronoĭ	R
7	2.6 s	27.0 s	126.6 s	200.9 s	4 881
13	4.5 s	63.2 s	290.9 s	27.1 s	69 312
19	19.7 s	17.4 s	126.7 s	24.4 s	3 276
31	30.6 s	235.4 s	545.7 s	5864.2 s	259 428
37	34.7 s	306.4 s	565.6 s	14059.1 s	559 588
43	79.2 s	683.0 s	1053.6 s	21849.6 s	3 346 357
61	40.0 s	2194.2 s	1911.8 s	—	20 631 747
67	75.2 s	1402.6 s	1564.0 s	—	22 671 433
73	68.2 s	3369.6 s	2688.8 s	—	36 795 697
79	107.8 s	1842.9 s	1431.7 s	—	14 112 084
97	423.3 s	4776.9 s	3893.8 s	—	77 237 641

Figure 6.3: Absolute running times and regulators for Cubic Field #2.

p	MAGMA	BSGS	Pollard ρ	Voronoĭ	R
7	10.2 s	1477.1 s	2227.8 s	21818.4 s	1 633 392
13	263.2 s	4339.5 s	4717.0 s	870578.8 s	4 876 327
19	42.0 s	54904.5 s	45075.9 s	—	723 127 183
31	297.4 s	414424.4 s	283480.3 s	—	32 682 723 157
37	633.5 s	443362.8 s	270150.6 s	—	34 979 256 673
43	1615.0 s	1020965.8 s	596191.2 s	—	238 666 301 611
61	11144.3 s	2184373.3 s	1583595.0 s	—	1 057 595 131 051
67	15255.5 s	1420462.6 s	834426.8 s	—	520 474 243 332
73	45766.3 s	3241791.7 s	2392991.9 s	—	5 044 078 887 939
79	55785.2 s	3628127.1 s	2410106.1 s	—	2 274 806 801 467
97	203321.1 s	2192901.1 s	1810233.7 s	—	2 634 205 238 352

Figure 6.4: Absolute running times and regulators for Cubic Field #3.

p	MAGMA	BSGS	Pollard ρ	Voronoĭ	R
5	1.08 s	0.48 s	6.94 s	0.19 s	8
13	1.38 s	0.27 s	6.39 s	0.14 s	5
17	1.69 s	0.87 s	13.56 s	0.45 s	20
29	2.42 s	1.29 s	15.23 s	0.89 s	40
37	2.18 s	0.37 s	9.04 s	0.23 s	9
41	3.43 s	1.65 s	18.22 s	1.14 s	52
53	2.65 s	1.21 s	16.55 s	0.90 s	40
61	4.26 s	0.53 s	8.91 s	0.34 s	13
73	5.40 s	0.43 s	8.16 s	0.23 s	10
89	6.72 s	2.44 s	27.72 s	2.22 s	100
97	6.48 s	1.00 s	11.44 s	0.46 s	20
101	8.51 s	2.30 s	26.82 s	2.27 s	104
109	9.45 s	0.92 s	12.17 s	0.72 s	29
113	7.61 s	2.16 s	22.37 s	2.19 s	100
137	8.96 s	2.24 s	24.56 s	2.56 s	116
149	11.74 s	2.52 s	27.33 s	2.96 s	136
157	19.74 s	1.14 s	16.53 s	1.02 s	45
173	18.49 s	1.30 s	18.88 s	1.01 s	40
181	17.97 s	1.14 s	14.54 s	0.90 s	41
193	22.73 s	0.82 s	11.46 s	0.57 s	26
197	23.37 s	3.60 s	31.95 s	4.34 s	200

Figure 6.5: Absolute running times and regulators for Quartic Field #1.

p	MAGMA	BSGS	Pollard ρ	Voronoĭ	R
5	1.0 s	11.9 s	120.6 s	24.7 s	549
13	1.7 s	18.3 s	227.2 s	44.5 s	2 160
17	10.2 s	38.5 s	315.5 s	268.7 s	4 825
29	46.6 s	38.3 s	478.7 s	255.1 s	4 411
37	2.5 s	123.2 s	609.4 s	1672.0 s	28 600
41	15.7 s	151.0 s	750.0 s	3403.7 s	51 264
53	4.1 s	14.9 s	211.1 s	39.4 s	696
61	5.2 s	349.4 s	1226.3 s	19678.3 s	332 077
73	4.3 s	218.0 s	669.6 s	6375.3 s	94 955
89	8.4 s	431.4 s	1254.9 s	17103.2 s	254 400
97	9.1 s	674.5 s	1622.8 s	78833.6 s	1 311 115
101	6.7 s	618.6 s	1717.9 s	65657.7 s	1 097 496
109	10.8 s	263.3 s	882.3 s	6098.8 s	90 480
113	7.8 s	232.8 s	979.9 s	7075.2 s	103 952
137	11.3 s	960.4 s	2034.6 s	136721.8 s	2 273 520
149	11.8 s	1283.7 s	1956.8 s	230774.7 s	3 384 511
157	12.3 s	1229.6 s	2493.1 s	228308.8 s	3 804 216
173	20.4 s	883.4 s	1798.6 s	41335.9 s	2 723 200
181	20.5 s	1592.7 s	2805.5 s	404710.2 s	6 765 847
193	20.8 s	448.8 s	1483.0 s	33448.4 s	491 045
197	20.6 s	920.3 s	1628.4 s	118620.5 s	1 734 000

Figure 6.6: Absolute running times and regulators for Quartic Field #2.

6.3 Computing All Neighbors of a Minimum

In the two algorithms by J. Buchmann, which we will present in the next section, one needs to enumerate all minima in a certain area or to enumerate all neighbors of already found minima until a complete set of non-conjugated minima is found. To find all minima in a certain area, one cannot proceed to try to find them all by doing baby steps, as it is possible to 'miss' minima when doing this as soon as $|S| > 2$. One way to solve this problem is to simply compute all neighbors of a minimum, and then to do the same for all of these recursively.

Clearly, one can use bounds on the absolute values of the neighbors and compute all elements in the ideal which lie in these bounds; then, one can pick all neighbors out of these. Unfortunately, this is far from efficient, as the number of elements in that area grows exponential in $[K : \mathbb{Q}]$.

A different approach is taken by Buchmann in [Buc87a] and [Buc87c]. He uses so called *minimal sets* to walk between all neighbors of a given minimum.

Let $\mathfrak{a} \in \mathrm{Id}(\mathcal{O})$. We begin with a few auxiliary definitions:

Definition 6.3.1. *Let $M \subseteq \mathfrak{a}$ be finite and non-empty. For $\mathfrak{p} \in S$ define*

$$\begin{aligned} \nu_{\mathfrak{p}}(M) &:= \min\{\nu_{\mathfrak{p}}(f) \mid f \in M\}, \\ |M|_{\mathfrak{p}} &:= \max\{|f|_{\mathfrak{p}} \mid f \in M\} = q^{-\nu_{\mathfrak{p}}(M)\deg \mathfrak{p}} \\ \textit{and} \qquad M(\mathfrak{p}) &:= \{f \in M \mid |f|_{\mathfrak{p}} = |M|_{\mathfrak{p}} \wedge \forall \mathfrak{q} \in S \setminus \{\mathfrak{p}\} : |f|_{\mathfrak{q}} < |M|_{\mathfrak{q}}\} \\ &= M \cap \mathring{B}(\mathfrak{a}, (-\nu_{\mathfrak{q}}(M) + \delta_{\mathfrak{p},\mathfrak{q}})_{\mathfrak{q}\in S}) \end{aligned}$$

where $\delta_{\mathfrak{p},\mathfrak{q}} = 1$ if $\mathfrak{p} = \mathfrak{q}$ and $\delta_{\mathfrak{p},\mathfrak{q}} = 0$ otherwise.

Using this, we can define:

Definition 6.3.2. *A finite non-empty subset $M \subseteq \mathfrak{a} \setminus \{0\}$ is called* minimal *if*

$$S = B(\mathfrak{a}, (-\nu_{\mathfrak{q}}(M))_{\mathfrak{q}\in S}) \setminus \{0\}$$

and

$$\mathring{B}(\mathfrak{a}, (-\nu_{\mathfrak{q}}(M))_{\mathfrak{q}\in S}) = \{0\}.$$

Remarks 6.3.3.

(a) We have that $M \subseteq \mathfrak{a}$ is a minimal set if, and only if, there exist elements $\mu_1, \ldots, \mu_t \in M$, $t \geq 1$, such that $M = B(\mathfrak{a}, \mu_1, \ldots, \mu_t) \setminus \{0\}$ and $\mathring{B}(\mathfrak{a}, \mu_1, \ldots, \mu_t) = \{0\}$.

(b) If $M \subseteq \mathfrak{a}$ is a minimal set, $M \subseteq \mathcal{A}(\mathfrak{a})$. Moreover, by Lemma 3.2.7, $M \cap \mathcal{E}(\mathfrak{a}) \neq \emptyset$. Moreover, every two elements in M are neighbors.

Proposition and Definition 6.3.4. *Let $M \subseteq \mathfrak{a}$ be a minimal set and $\mathfrak{p} \in S$. Then there exists a unique minimal set $M' \subseteq \mathfrak{a}$ such that $|M|_{\mathfrak{q}} = |M'|_{\mathfrak{q}}$ for all $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$ and $M'(\mathfrak{p}) \neq \emptyset$. This minimal set is called the* $\mathfrak{p}$-expansion *of M and denoted by $e_{\mathfrak{p}}(M)$.*

Proof. For $\varepsilon \in \mathbb{G}$, $\varepsilon \geq 0$ consider the set $B_\varepsilon := \mathring{B}(\mathfrak{a}, (-\nu_{\mathfrak{q}}(M) + \varepsilon\delta_{\mathfrak{p},\mathfrak{q}})_{\mathfrak{q}\in S}) \setminus \{0\}$, where $\delta_{\mathfrak{p},\mathfrak{p}} = 1$ and $\delta_{\mathfrak{p},\mathfrak{q}} = 0$ for $\mathfrak{p} \neq \mathfrak{q}$. There exists some $\varepsilon > 0$ such that $B_\varepsilon \neq \emptyset$. Let ℓ be the infimum over all such ε if K is a number field or let ℓ be one less than the smallest of such ε if K is a function field. Then $M' := B(\mathfrak{a}, (-\nu_{\mathfrak{q}}(M) + \ell\delta_{\mathfrak{p},\mathfrak{q}})_{\mathfrak{q}\in S}) \setminus \{0\}$ satisfies the requirements. □

Proposition and Definition 6.3.5. *Let $M \subseteq \mathfrak{a}$ be a minimal set and $\mathfrak{p} \in S$. Define $c_{\mathfrak{p}}(M) := \{f \in M \mid |f|_{\mathfrak{p}} < |M|_{\mathfrak{p}}\}$. Then either $c_{\mathfrak{p}}(M) = \emptyset$, or $c_{\mathfrak{p}}(M)$ is a minimal set. In the latter case, $c_{\mathfrak{p}}(M)$ is called the* $\mathfrak{p}$-compression *of M.* □

Note that these two operations are not exactly inverse to each other, but can be inverted using a finite number of each of them. For expansions, this can be done as follows:

Lemma 6.3.6. *Let $M \subseteq \mathfrak{a}$ be a minimal set and $\mathfrak{p} \in S$. There exists an $\ell \in \mathbb{N}$ such that for $M' := e_{\mathfrak{p}}(M)$, we have $M = c_{\mathfrak{p}}^{(\ell)}(M')$.*

Here, for $\ell \in \mathbb{N}$, we write $c_{\mathfrak{p}}^{(\ell)}(M)$ for the ℓ-fold $\mathfrak{p}$-compression of M, i.e. $c_{\mathfrak{p}}^{(\ell)}(M) = c_{\mathfrak{p}}(c_{\mathfrak{p}}(\cdots c_{\mathfrak{p}}(M)\cdots))$, where $c_{\mathfrak{p}}^{(0)}(M) = M$.

Proof. This follows from the definition of $e_{\mathfrak{p}}(M)$ and $c_{\mathfrak{p}}(M)$ and the fact that the number of infinite valuations attained by elements of $e_{\mathfrak{p}}(M)$ is finite. □

Compressions can also be inverted by a sequence of compressions and expansions, but not as easily as in the case of expansions, as there might exist a $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$ with $|c_{\mathfrak{p}}(M)|_{\mathfrak{q}} < |M|_{\mathfrak{q}}$ for a minimal set M with $c_{\mathfrak{p}}(M) \neq \emptyset$. The fact that compressions can be inverted follows from following, more general result, which can be seen as a more effective version of Corollary 3.4.3:

Proposition 6.3.7. *[Buc87a, p. 13, Proposition 3.2] Let M and M' be two minimal sets. Then there exists a sequence of minimal sets*

$$M = M_1, M_2, \ldots, M_{\ell-1}, M_\ell = M'$$

such that M_{i+1} is either a compression or an expansion of M_i, $1 \leq i < \ell$.

Moreover, if $\mu \in M \cap M'$, one can assume that $\mu \in M_i$ for all i.

We follow Buchmann's proof, which is based on ideas Bergmann used in [Ber63]. We begin with a definition, which will allow to describe the minimal sets in a geometric way:

Definition 6.3.8. *For $t_\mathfrak{q} \in \mathbb{R}$, $\mathfrak{q} \in S$ define*

$$N((t_\mathfrak{q})_{\mathfrak{q}\in S}) := \{x \in \mathbb{R}^S \mid |x_\mathfrak{q}| \leq q^{t_\mathfrak{q} \deg \mathfrak{q}} \text{ for all } \mathfrak{q} \in S\}.$$

For a minimal set M, define

$$\begin{aligned} N(M) &:= N((-\nu_\mathfrak{q}(M))_{\mathfrak{q}\in S}) \\ &= \{x \in \mathbb{R}^S \mid |x_\mathfrak{q}| \leq |M|_\mathfrak{q} \text{ for all } \mathfrak{q} \in S\}. \end{aligned}$$

We begin with a finiteness lemma:

Lemma 6.3.9. *[Buc87a, p. 13, Lemma 3.4] For any choice $t_\mathfrak{q} \in \mathbb{R}$, $\mathfrak{q} \in S$, the set of minimal sets M satisfying*

$$N((t_\mathfrak{q})_{\mathfrak{q}\in S}) \subseteq N(M)$$

is finite.

Proof. Using Minkowski's Lattice Point Theorem or Riemann's Inequality, one obtains a bound B for $|M|_\mathfrak{q}$ for every $\mathfrak{q} \in S$. As the number of valuations $\nu_\mathfrak{q}$ attained on $\mathfrak{a}$ with $|\bullet|_\mathfrak{q} \leq B$ for every $\mathfrak{q} \in S$ is finite, we get that the number of minimal sets is finite, too. □

Now we have the following lemma, which will be essential for the proof of Proposition 6.3.7:

Lemma 6.3.10. *[Buc87a, p. 14, Lemma 3.5] Let M and M' be two minimal sets with $M' \not\subseteq M$. Then there exists a sequence of minimal sets $M = M_1, M_2, \ldots, M_{\ell-1}, M_\ell$ such that M_{i+1} is either a compression or an expansion of M_i, $1 \leq i < \ell$, and that $N(M) \cap N(M') \subsetneqq N(M_\ell) \cap N(M')$.*

Moreover, if $\mu \in M \cap M'$, one can assume that $\mu \in M_i$ for all i.

Proof. Let $\mathfrak{p} \in S$ such that $|M|_\mathfrak{p} < |M'|_\mathfrak{p}$; such a $\mathfrak{p}$ exists as otherwise $M' \subseteq M$. If $M(\mathfrak{p}) = \emptyset$, set $M_1 = M$ and $M_2 = e_\mathfrak{p}(M)$; then $M_1 \subsetneqq M_2$ and $N(M) \cap N(M') \subsetneqq N(M_2) \cap N(M')$.

Otherwise, assume that $M(\mathfrak{p}) \neq \emptyset$. Let $\mu' \in M(\mathfrak{p})$; there exists a $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$ with $|M'|_\mathfrak{q} \leq |\mu'|_\mathfrak{q} < |M|_\mathfrak{q}$ as M' is a minimal set. Set $M_1 := M$.

We want to set $M_2 := c_{\mathfrak{q}}(M_1)$ and $M_3 := c_{\mathfrak{q}}(M_2)$ etc., until $|M_i|_{\mathfrak{q}} = |\mu'|_{\mathfrak{q}}$. The problem is that it might happen that $N(M_i) \cap N(M')$ might get smaller if some of the elements in M_{i-1} with $|\bullet|_{\mathfrak{q}} = |M_{i-1}|_{\mathfrak{q}}$ were the only ones with $|\bullet|_{\mathfrak{q}'} = |M_{i-1}|_{\mathfrak{q}'}$ for another $\mathfrak{q}' \in S$. In that case, one has to do a $\mathfrak{q}'$-expansion (and maybe some more $\mathfrak{q}''$-expansions in other directions $\mathfrak{q}''$ with the same problems as the $\mathfrak{q}'$-direction) before doing the $\mathfrak{q}$-compression.

Eventually, we will have $|M_i|_{\mathfrak{q}} = |\mu'|_{\mathfrak{q}}$; then $\mu' \notin M_i(\mathfrak{p})$, while $|M_i|_{\mathfrak{p}} = |M|_{\mathfrak{p}}$. Moreover, by construction, we have $N(M) \cap N(M') = N(M_j) \cap N(M')$ for $1 \leq j \leq i$.

Now, we can continue with another element of $M_i(\mathfrak{p})$ in the same manner until we obtain $M_m(\mathfrak{p}) = \emptyset$ with $N(M) \cap N(M') = N(M_j) \cap N(M')$ and $|M_j|_{\mathfrak{p}} = |M|_{\mathfrak{p}}$ for all $1 \leq j \leq m$, i.e. we can set $\ell := m + 1$ and $M_\ell := e_{\mathfrak{p}}(M_\ell)$. □

Proof of Proposition 6.3.7. If $M' \subseteq M$, it suffices to apply a certain amount of compressions to M to find the M_i.

If $M' \not\subseteq M$, we can replace M by M'' via a sequence of compressions and expansions such that $T(M) \cap T(M') \subsetneqq T(M'') \cap T(M')$ (this is Lemma 6.3.10). As the set of minimal sets containing $T(M) \cap T(M')$ is finite by Lemma 6.3.9, by repeating this process we eventually come to the point that we cannot enlarge $T(M'') \cap T(M')$ by applying compressions and expansions to M'' anymore, i.e. we must have that $T(M'') \cap T(M')$ is maximal – which, by Lemma 6.3.10, is only possible if it is equal to $T(M')$, i.e. if $M' \subseteq M''$. But then, by the first case, we can apply a finite amount of compressions to obtain M' from M''. □

Next, we have the following result:

Proposition 6.3.11. *[Buc87c, p. 56, Satz 12.3] Every neighbor of $\mu \in \mathcal{A}(\mathfrak{a})$ belongs to some minimal subset of $\mathfrak{a}$ which contains μ.*

Proof. If $\mu' \in \mathcal{A}(\mathfrak{a})$ is a neighbor of μ, clearly

$$M := B(\mathfrak{a}, \mu, \mu') \setminus \{0\}$$

is a minimal subset of $\mathfrak{a}$. □

So far, the minimal sets did not give anything new. What makes them so interesting is the following result, which allows to compute all minimal sets which contain a given minimum μ and, hence, by the previous proposition, all neighbors of that minimum:

Proposition 6.3.12. *[Buc87c, pp. 56f] The following algorithm computes all neighbors of $\mu \in \mathcal{A}(\mathfrak{a})$:*

Algorithm 6.3.13: Computes all neighbors of μ in $\mathcal{A}(\mathfrak{a})$.

Input: minimum $\mu \in \mathcal{A}(\mathfrak{a})$

Output: set N of all neighbors of μ in $\mathfrak{a}$.

(1) Set $\ell := 1$, $p := 1$, $N := \emptyset$ and $S_1 := B(\mathfrak{a}, \mu) \setminus \{0\}$;

(2) while $\ell \leq p$, repeat the following steps:

  (i) for $\mathfrak{p} \in S$ do

    (a) compute $S' := e_{\mathfrak{p}}(S_\ell)$;

    (b) if $S' \neq S_j$ for $1 \leq j \leq p$, do $p := p + 1$, $S_p := S'$ and $N := N \cup S'$;

    (c) if $|S_\ell|_{\mathfrak{p}} > |\mu|_{\mathfrak{p}}$, do

      - compute $S' := c_{\mathfrak{p}}(S_\ell)$;
      - if $S' \neq S_j$ for $1 \leq j \leq p$, do $p := p + 1$ and $S_p := S'$;

  (ii) set $\ell := \ell + 1$.

If K is a number field, the number of iterations is $\mathcal{O}(D^\varepsilon)$.

Proof. First, note that by Remark 6.3.3 (a), every element of a minimal set containing μ is a neighbor of μ. Moreover, by Proposition 6.3.11, every neighbor of μ appears as an element in a minimal set which also contains μ. Finally, by Proposition 6.3.7, one can walk between any two minimal sets containing μ by a finite sequence of compressions and expansions, each intermediate minimal set also containing μ. Therefore, the algorithm computes all neighbors of μ. For the statement on the number of iterations, see [Buc87c, p. 57, Satz 12.6]. □

Note that while this algorithm is effective, it is rather slow in practice, according to Buchmann [Buc87c, p. 47].

6.3.1 Computations in the Function Field Case

The computation of compressions and expansions in the number field case is explained in [Buc87c, pp. 60–62, Kapitel 14]. In the function field case, this can be done using Riemann-Roch space computations. Computing an expansion is relatively easy:

Algorithm 6.3.14: Computing the $\mathfrak{p}$-Expansion of a Minimal Set.

Input: minimal set S specified by $t_\mathfrak{q} = -\nu_\mathfrak{q}(S)$, $\mathfrak{q} \in S$

Output: minimal set $e_\mathfrak{p}(S)$ specified by $t'_\mathfrak{q} = -\nu_\mathfrak{q}(e_\mathfrak{p}(S))$, $\mathfrak{q} \in S$.

(1) Set $t_\mathfrak{q} := t_\mathfrak{q} - 1$ for all $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$.

(2) Compute a basis B of $B(\mathfrak{a}, (t_\mathfrak{q})_{\mathfrak{q}\in S})$.

(3) If $|B| > 0$, continue with Step (6).

(4) Set $t_\mathfrak{p} := t_\mathfrak{p} + 1$.

(5) Continue with Step (2).

(6) Set $t'_\mathfrak{q} := t_\mathfrak{q} + 1$ for all $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$ and $t'_\mathfrak{p} := t_\mathfrak{p}$.

(7) Return $(t'_\mathfrak{q})_{\mathfrak{q}\in S}$.

Computing a compression can be done in two ways. First, if one is able to evaluate $\nu_\mathfrak{p}$, one can proceed as follows:

Algorithm 6.3.15: Computing the $\mathfrak{p}$-Compression of a Minimal Set, Variant 1.

Input: minimal set S specified by $t_\mathfrak{q} = -\nu_\mathfrak{q}(S)$, $\mathfrak{q} \in S$

Output: minimal set $c_\mathfrak{p}(S)$ specified by $t'_\mathfrak{q} = -\nu_\mathfrak{q}(c_\mathfrak{p}(S))$, $\mathfrak{q} \in S$, or $\emptyset$.

(1) Set $t_\mathfrak{p} := t_\mathfrak{p} - 1$.

(2) Compute a basis B of $B(\mathfrak{a}, (t_\mathfrak{q})_{\mathfrak{q}\in S})$.

(3) If $B = \emptyset$, return $\emptyset$.

(4) Compute $t'_\mathfrak{q} := \max\{-\nu_\mathfrak{q}(b) \mid b \in B\}$ for all $\mathfrak{q} \in S$.

(5) Return $(t'_\mathfrak{q})_{\mathfrak{q}\in S}$.

Note that $\max\{-\nu_\mathfrak{p}(b) \mid b \in B\} = \max\{-\nu_\mathfrak{p}(f) \mid f \in \langle B\rangle_k\}$. Finally, if evaluating valuations is inefficient, one has to use additional Riemann-Roch space computations to find $t'_\mathfrak{p}$:

Algorithm 6.3.16: Computing the $\mathfrak{p}$-Compression of a Minimal Set, Variant 2.

Input: minimal set S specified by $t_\mathfrak{q} = -\nu_\mathfrak{q}(S)$, $\mathfrak{q} \in S$

Output: minimal set $c_\mathfrak{p}(S)$ specified by $t'_\mathfrak{q} = -\nu_\mathfrak{q}(c_\mathfrak{p}(S))$, $\mathfrak{q} \in S$, or $\emptyset$.

(1) Compute a basis B of $B(\mathfrak{a}, (t_\mathfrak{q})_{\mathfrak{q}\in S})$.

(2) Set $t_\mathfrak{p} := t_\mathfrak{p} - 1$.

(3) Compute a basis B' of $B(\mathfrak{a}, (t_\mathfrak{q})_{\mathfrak{q}\in S})$.

(4) If $B' = \emptyset$, return $\emptyset$.

(5) If $|B'| < |B|$, continue with Step (9).

(6) Set $t_\mathfrak{p} := t_\mathfrak{p} - 1$.

(7) Compute a basis B' of $B(\mathfrak{a}, (t_\mathfrak{q})_{\mathfrak{q}\in S})$.

(8) Continue with Step (5).

(9) For $\mathfrak{q} \in S$ do:

  (i) Set $t_\mathfrak{q} := t_\mathfrak{q} - 1$.

  (ii) Compute a basis B'' of $B(\mathfrak{a}, (t_\mathfrak{q})_{\mathfrak{q}\in S})$.

  (iii) If $|B''| = |B'|$, continue with Step (9 i).

  (iv) Set $t_\mathfrak{q} := t_\mathfrak{q} + 1$.

(10) Return $(t_\mathfrak{q})_{\mathfrak{q}\in S}$.

The problem of computing $M \cap \mathcal{E}(\mathfrak{a})$ for a minimal set M in the function field case remains. First, we have $\mathcal{E}(\mathfrak{a}) \subsetneqq \mathcal{A}(\mathfrak{a})$ in general. Moreover, the Riemann-Roch space computation gives a k-basis of M, which does not necessarily contains any type (b) minimum or, even if it does, may not contain all of them.

For that, it suffices to note that given a minimal set M, for any $\mu \in M \cap \mathcal{E}(\mathfrak{a})$ there exists a series of compressions which reduces M to a minimal set M' with $\mu \in M'$ such that $|M'|_\mathfrak{q} = |\mu|_\mathfrak{q}$ for all $\mathfrak{q} \in S$.

Hence, if one extends the algorithm in Proposition 6.3.12 to compute compressions regardless of the condition "$|S_k|_\mathfrak{p} > |\mu|_\mathfrak{p}$" (without computing expansions for the ones which are too small), one will eventually obtain also all minimal subsets which contain only type (b) neighbors of μ: as soon as we have a minimal set M' such that all $\mathfrak{q}$-compressions $c_\mathfrak{q}(M')$, $\mathfrak{q} \in S$ are empty, we have that $M' = B(\mathfrak{a}, \mu') \setminus \{0\}$ for some neighbor $\mu' \in \mathcal{E}(\mathfrak{a})$ of μ.

6.4 Buchmann's Algorithms

In the number field case, $\mathbb{G}^n/\Lambda$ is not a finite abelian group. Therefore, one cannot simply apply algorithms for computing the structure of such groups in order to obtain a basis of Λ.

Nonetheless, J. Buchmann presented algorithms for computing units in arbitrary number fields in a paper [Buc87a] and his habilitation thesis [Buc87c]. The algorithm in the paper is of complexity $\mathcal{O}(D^\varepsilon R)$ binary operations, D being the absolute value of the discriminant of the number field and R the regulator, while he presents a generalization of the baby step-giant step algorithm in the thesis which is of complexity $\mathcal{O}(D^\varepsilon\sqrt{R})$. Moreover, he presents another baby step algorithm in the thesis, which has the same asymptotic complexity as the algorithm in the paper.

We want to sketch these three algorithms in this section.

Note that one of the main problems in the number field case is that one has to approximate all valuations, as these are either 0 or transcendental. We will ignore this issue throughout this section and concentrate on the algorithms themselves.

Moreover, note that we use $-\nu_\mathfrak{p}(\bullet)$ for infinite primes, while Buchmann uses $\log|\bullet|_\mathfrak{p} = -\nu_\mathfrak{p}(\bullet)\cdot\deg\mathfrak{p}$.

6.4.1 The Generalized Lagrange Algorithm

In the case $|S| = 2$, Lagrange's algorithm works by starting with a minimum and computing baby steps in one direction, until it finds a minimum which is conjugated to the first one. As baby step chains in the case $|S| = 2$ are purely periodic, this is equivalent to finding a complete set of pairwise non-conjugated minima. This is exactly what Buchmann's generalization is doing in the arbitrary number field case.

One difference to the one-dimensional case is that one cannot use baby steps, as baby steps might miss certain minima, i.e. there is no way to reach certain minima by baby steps. Still, by Corollary 3.4.3 respectively Proposition 3.4.4, one can reach every minimum by going to neighbors. Hence, using the methods presented in Section 6.3, we can reach every minimum.

Fix $\mathfrak{a} \in \mathrm{Id}(\mathcal{O})$.

Definition 6.4.1.

(a) *Let C be a non-empty set of type (b) minima of $\mathfrak{a}$ such that no two elements of C are associated and that given an element μ of C and a*

neighbor $\mu' \in \mathcal{E}(\mathfrak{a})$ of μ, we have that μ' is associated to one element in C. Then C is called a cycle *of minima of $\mathfrak{a}$.*

(b) *Let C be a cycle of minima of $\mathfrak{a}$. Define the set of* boundary units *of C as*

$$U(C) := \left\{ \varepsilon \in \mathcal{O}^* \;\middle|\; \exists \mu, \mu' \in C, \mu'' \in \mathcal{E}(\mathfrak{a}) : \mu' \; N \; \mu'' \wedge \varepsilon = \frac{\mu}{\mu''} \right\}.$$

Here, $\mu' \; N \; \mu''$ means that μ' and μ'' are neighbors.

Using the methods from Section 6.3, we can compute a cycle of minima of $\mathfrak{a}$ given one minimum to start with. To test minima μ, μ' for being conjugated, one can use their ideal representations: we have that μ and μ' are conjugated under $\mathcal{O}^*$ if, and only if, $\frac{1}{\mu}\mathfrak{a} = \frac{1}{\mu'}\mathfrak{a}$. The main result on cycles is:

Proposition 6.4.2. *[Buc87a, p. 14, Theorem 4.2] Assume that K is a global field. The sets C and $U(C)$ are finite, every minimum of $\mathfrak{a}$ is associated to exactly one minimum in C, and we have $\mathcal{O}^* = \langle U(M) \rangle$.*

Proof. The finiteness of C follows from Theorem 3.2.6. As every minimum can only have a finite number of neighbors (see [Buc87a, p. 4, Corollary 2.5]; in the function field case, this follows from the fact that the distance to a neighbor is bounded and that all valuations are integers), we have that $U(C)$ is finite, too.

Let μ be a minimum of $\mathfrak{a}$ and let μ' be any element of C. By Corollary 3.4.3 or Proposition 3.4.4, there exists a sequence of minima

$$\mu' = \mu_1, \mu_2, \ldots, \mu_{\ell-1}, \mu_\ell = \mu$$

such that μ_i is a neighbor of μ_{i+1}, $1 \leq i < \ell$. Now $\mu_1 \in C$ by assumption, and if μ_i is associated to a minimum $\mu_i' \in C$, then μ_{i+1} will be associated to a minimum $\mu_{i+1}' \in C$ as C is a cycle. Hence, by induction, μ will be associated to an element of C.

It is left to show that $\mathcal{O}^*$ is generated by $U(C)$. Let $\varepsilon \in \mathcal{O}^*$ be arbitrary and choose any $\mu \in C$. Then, by Corollary 3.4.3 or Proposition 3.4.4, there exists a sequence of minima $\mu = \mu_1, \mu_2, \ldots, \mu_{\ell-1}, \mu_\ell = \varepsilon\mu$ such that μ_i is a neighbor of μ_{i+1}, $1 \leq i < \ell$. Define $\varepsilon_1 := 1$, and inductively define ε_i as follows: by assumption, μ_{i-1} is associated to an element of C, say, by a unit ε_{i-1}', i.e. $\varepsilon_{i-1}'\mu_{i-1} \in C$. Now $\varepsilon_{i-1}'\mu_i$ is a neighbor of $\varepsilon_{i-1}'\mu_{i-1}$, whence $\varepsilon_{i-1}'\mu_i$ is associated to an element $\mu_i' \in C$ by a boundary unit $\varepsilon_i \in U(C)$,

i.e. $\varepsilon_i = \frac{\mu'_i}{\varepsilon'_{i-1}\mu_i}$. Finally, choose $\varepsilon'_\ell \in \mathcal{O}^*$ such that $\varepsilon'_\ell \mu_\ell \in C$, i.e. $(\varepsilon'_\ell)^{-1} = \varepsilon$. Note that we have $\varepsilon_i \varepsilon'_{i-1}\mu_i = \mu'_i = \varepsilon'_i \mu_i$, $1 < i \leq \ell$.

We claim that $\prod_{i=1}^{t} \varepsilon_i = \varepsilon'_t$ for $t = 1, \ldots, \ell$. Clearly, $\prod_{i=1}^{1} \varepsilon_i = \varepsilon_1 = 1 = \varepsilon'_1$ as $1 \cdot \mu_1 = \mu \in C$. Assume that $\prod_{i=1}^{t} \varepsilon_i = \varepsilon'_t$ for $t < \ell$; then, by induction,

$$\prod_{i=1}^{t+1} \varepsilon_i = \varepsilon'_t \varepsilon_{t+1} = \varepsilon'_t \frac{\mu'_{t+1}}{\varepsilon'_t \mu_{t+1}} = \frac{\mu'_{t+1}}{\mu_{t+1}} = \frac{\varepsilon'_{t+1}\mu_{t+1}}{\mu_{t+1}} = \varepsilon'_{t+1}.$$

Hence, $\varepsilon = (\varepsilon'_\ell)^{-1} = \prod_{i=1}^{\ell} \varepsilon_i^{-1} \in \langle U(C) \rangle$. □

As $|C| = \mathcal{O}(R)$ and as $|U(C)| = \mathcal{O}(R)$, where the $\mathcal{O}$-constants only depend on the field degree, we obtain an algorithm which computes a generating set for $\mathcal{O}^*$ in $\mathcal{O}(R)$ steps in the infrastructure. Buchmann showed that in the number field case, one step can be done with $\mathcal{O}(D^\varepsilon)$ binary operations. Therefore, he obtained:

Theorem 6.4.3. *[Buc87a, pp. 18f] Let K be a number field of discriminant $\pm D$, $D > 0$ and with regulator R. The algorithm computes a basis of $\Psi(\mathcal{O}^*)$ in $\mathcal{O}(D^\varepsilon R)$ binary operations.* □

6.4.2 The Baby Step Algorithm

In his habilitation thesis, Buchmann presented another generalization of Lagrange's method. This one, called the baby step algorithm, uses a more structured enumeration of the minima of $\mathcal{O}$. For itself, this is maybe not of too much interest, but the ideas and results from this section will be used both for Buchmann's and our baby step-giant step algorithm; therefore, we will describe them in detail.

The idea is similar to the idea in Section 6.2, i.e. one iteratively seeks for lattice elements $b_1, \ldots, b_n \in \Lambda$ such that $\langle b_1, \ldots, b_n \rangle = \Lambda$. Assume that $b_1, \ldots, b_{k-1}$ have already been found, for $k \in \{1, \ldots, n\}$. Let $V = \langle b_1, \ldots, b_{k-1} \rangle_{\mathbb{R}}$ and $\hat{V} = V^\perp$ the orthogonal complement of V in $\mathbb{R}^n$.

Pick suitable elements $e_k, \ldots, e_n$ such that $(b_1, \ldots, b_{k-1}, e_k, \ldots, e_n)$ is a basis of $\mathbb{R}^n$. Then, apply the Gram-Schmidt decomposition to the basis $(b_1, \ldots, b_{k-1}, e_k, \ldots, e_n)$ to obtain a orthonormal basis $b_1^*, \ldots, b_n^*$ of $\mathbb{R}^n$; then $b_i^* = \frac{\hat{b}_i}{\|\hat{b}_i\|}$ if we have $b_i = \hat{b}_i + \sum_{j=1}^{i-1} \mu_{i,j} \hat{b}_j$, $1 \leq i < k$ with $\mu_{i,j} = \frac{\langle b_i, \hat{b}_j \rangle}{\langle \hat{b}_j, \hat{b}_j \rangle}$, $1 \leq j < i < k$.

Denote by $\hat{\pi} : \mathbb{R}^n \to \hat{V}$ the orthogonal projection onto $\hat{V}$ and define $\hat{\Lambda} := \hat{\pi}(\Lambda)$. Then $\hat{\Lambda}$ is a full lattice in $\hat{V}$, and $\dim \hat{V} = n - k + 1$. For a

vector $v \in \mathbb{R}^n$, define $\hat{v} := \hat{\pi}(v)$. Write $v = \sum_{i=1}^{n} \lambda_i b_i^*$, i.e. $\hat{v} = \sum_{i=k}^{n} \lambda_i b_i^*$; then we define $|\hat{v}| := \max_{i=k,\dots,n} |\lambda_i|$ and call this the *height* of v.

Buchmann's algorithm tries to find a non-trivial element of $\hat{\Lambda}$ of 'small enough' height; then, the following result states that we can use such an element as b_k:

Proposition 6.4.4. *[Buc87c, p. 17, Satz 5.1] Let $b_k \in \Lambda$ be such that $|\hat{v}| > \frac{1}{2}|\hat{b_k}|$ for every $\hat{v} \in \hat{\Lambda}$, $\hat{v} \neq 0$. Then there exist elements $b_{k+1}, \dots, b_n \in \Lambda$ with $\Lambda = \langle b_1, \dots, b_n \rangle$.*

Proof. Assume that $b_1, \dots, b_k$ cannot be extended to a basis of Λ. By the Elementary Divisor Theorem, there exists a basis $b_1', \dots, b_n'$ of Λ and positive integers $d_1, \dots, d_k$ such that $d_1 b_1', \dots, d_k b_k'$ is a basis of $\langle b_1, \dots, b_k \rangle$. That $b_1, \dots, b_k$ cannot be completed to a basis of Λ means that $\Lambda / \langle b_1, \dots, b_k \rangle$ has non-trivial torsion, whence we must have $d_i > 1$ for some $i \in \{1, \dots, k\}$. In particular, we can write $b_i' = \sum_{j=1}^{k} a_j b_j$ with $a_j \in \mathbb{Q}$ and not all $a_j \in \mathbb{Z}$. Then $b^* := b_i' - \sum_{j=1}^{k} \mathrm{Round}(a_j) b_j = \sum_{j=1}^{k} \hat{a}_j b_j$ satisfies $|\hat{a}_j| \leq \frac{1}{2}$, and at least one $\hat{a}_j$ must be non-zero (here, $\mathrm{Round}(x) \in \mathbb{Z}$ satisfies $|\mathrm{Round}(x) - x| \leq \frac{1}{2}$ for all $x \in \mathbb{R}$).

Now, if $\hat{a}_k = 0$, we see that $b_i' \in \langle b_1, \dots, b_{k-1} \rangle_{\mathbb{Q}} \setminus \langle b_1, \dots, b_{k-1} \rangle_{\mathbb{Z}}$, whence already $b_1, \dots, b_{k-1}$ cannot be extended to a basis of Λ, a contradiction. Hence, $\hat{a}_k \neq 0$, whence $|\hat{b^*}| = |\hat{a}_k| \cdot \|b_k\| \leq \frac{1}{2}\|b_k\|$. □

Hence, it suffices to check all elements of small height. The following result shows that it suffices to check a certain region:

Proposition 6.4.5. *[Buc87c, p. 17, Satz 5.2] Let $v \in \Lambda$. Then there exists a $w \in \Lambda$ such that $\hat{v} = \hat{w}$ and*

$$w = \hat{w} + \sum_{j=1}^{k-1} \lambda_j \hat{b}_j$$

with $|\lambda_j| \leq \frac{1}{2}$ for $1 \leq j < k$.

Proof. We have $\lambda_j = \frac{\langle v, \hat{b}_j \rangle}{\langle \hat{b}_j, \hat{b}_j \rangle}$. As $\langle b_j, \hat{b}_j \rangle = \langle \hat{b}_j, \hat{b}_j \rangle$ for all j, we can obtain $|\lambda_{k-1}| \leq \frac{1}{2}$ by adding an element of $\mathbb{Z} b_{k-1}$ to v; note that this does not changes $\hat{v}$. Then, by adding an element of $\mathbb{Z} b_{k-2}$ to v, we can change λ_{k-2} without changing λ_{k-1}. Continuing iteratively until adding something in $\mathbb{Z} b_1$, we can reach $|\lambda_j| \leq \frac{1}{2}$ for $j = k-1, k-2, \dots, 2, 1$. □

Hence, it suffices to search the space

$$P_\infty = \left\{ \sum_{j=1}^{k-1} \lambda_j \hat{b}_j + \sum_{j=k}^{r} \lambda_j b_j^* \;\middle|\; \begin{array}{l} \lambda_j \in \mathbb{R} \text{ for all } j, \\ |\lambda_j| \leq \frac{1}{2} \text{ for } 1 \leq j < k \end{array} \right\} :$$

Corollary 6.4.6. *[Buc87c, p. 18, Korollar 5.1] Let $b_k \in P_\infty \cap \Lambda$ be a vector such that $\frac{1}{2}|\hat{b_k}| < |\hat{v}|$ for every $v \in P_\infty \cap \Lambda$, $|\hat{v}| \neq 0$. Then $b_1, \ldots, b_k$ can be extended to a basis of Λ.* □

Now, Buchmann's idea is to use a baby step (or baby step-giant step, for the algorithm in Section 6.4.3) strategy to search $P_\infty \cap \Lambda$ for vectors with small enough non-zero height.

For a choice $\delta_1, \ldots, \delta_n > 0$ define $b'_j := \delta_j b_j^*$, $1 \leq j \leq n$ and

$$P' := \left\{ \sum_{j=1}^{n} \lambda_j b'_j \;\middle|\; |\lambda_j| \in [-\tfrac{1}{2}, \tfrac{1}{2}] \right\}.$$

Moreover, for $z = (z_1, \ldots, z_n) \in \mathbb{Z}^n$, define

$$m'(z) := \sum_{j=1}^{n} z_j b'_j$$

and

$$P'(z) := m'(z) + P', \qquad \big|m'(z)\big| := \max_{j=k,\ldots,n} |z_j|.$$

Then $|m'(z)|$ is said to be the height of $P'(z)$ and of z.

Lemma 6.4.7. *Let $N_1, \ldots, N_{k-1} \in \mathbb{N}$. Define*

$$\delta_j = \frac{\|\hat{b}_j\|}{2N_j + 1}$$

for $1 \leq j < k$, and let $\delta_k, \ldots, \delta_n > 0$. Then

$$P_\infty = \bigcup_{\substack{z=(z_1,\ldots,z_n)\in\mathbb{Z}^n \\ |z_j| \leq N_j,\ 1 \leq j < k}} P'(z).$$

Note that in the actual algorithm, we might have to chose $\delta_j > \frac{\|\hat{b}_j\|}{2N_j+1}$ if $\|\hat{b}_j\|$ is too short, to be able to guarantee the existence of minima in $P'(z)$; then, we will actually search an area slightly larger than P_∞.

Proof of Lemma 6.4.7. If $z = (z_1, \ldots, z_n) \in \mathbb{Z}^n$ with $|z_j| \leq N_j$ for $1 \leq j < k$ and if $v = \sum_{j=1}^n \lambda_j b'_j \in P'$, then $m'(z) + v = \sum_{j=1}^n (\lambda_j + z_j)\delta_j b_j^*$. Now $|(\lambda_j + z_j)\delta_j| \leq (\frac{1}{2} + N_j)\frac{\|\hat{b}_j\|}{2N_j+1} = \frac{1}{2}\|\hat{b}_j\|$, whence $m'(z) + v \in P_\infty$.

Conversely, if $v = \sum_{j=1}^n \lambda_j b'_j \in P_\infty$, we have $|\lambda_j|\delta_j \leq \frac{1}{2}\|\hat{b}_j\|$ for $1 \leq j < k$, i.e. $|\lambda_j| \leq N_k + \frac{1}{2}$. Hence, we can write $\lambda_j = z_j + \lambda'_j$ with $|\lambda'_j| \leq \frac{1}{2}$ and $z_j \in \{-N_j, \ldots, N_j\}$, $1 \leq j < k$. For $j = k, \ldots, n$, we can also write $\lambda_j = z_j + \lambda'_j$ with $|\lambda'_j| \leq \frac{1}{2}$ and $z_j \in \mathbb{Z}$. Then, $v = m'(z) + v'$ with $z = (z_1, \ldots, z_n)$ and $v' = \sum_{j=1}^n \lambda'_j b'_j \in P'$. □

We will see how to enumerate all minima inside $P'(z)$ and, using that, the union

$$P_\infty = \bigcup_{\substack{z=(z_1,\ldots,z_n)\in\mathbb{Z}^n \\ |z_j|\leq N_j,\ 1\leq j<k}} P'(z)$$

with ascending height of $P'(z)$, in Section 6.5.1.

Using this, Buchmann designed the following algorithm [Buc87c, p. 33, Algorithmus 8.1]:

Algorithm 6.4.8: Buchmann's Baby Step Algorithm for Computing a Basis of $\Lambda = \Psi(\mathcal{O}^*)$.

Input: a reduced ideal $\mathfrak{a}$ of the number field K.

Output: a basis $b_1, \ldots, b_n$ of Λ.

(1) Set $k := 0$, $\kappa := \frac{1}{2}\log D + s\log\frac{2}{\pi}$. Moreover, set $\delta_j := \sqrt{n}\kappa$ for $j = 1, \ldots, n$.

(2) Set $k := k + 1$; if $k > n$, we are done.

(3) If $k > 1$, set $N_{k-1} := \max\left\{0, \left\lfloor \frac{1}{2\sqrt{n}\kappa}\|\hat{b}_{k-1}\| - \frac{1}{2} \right\rfloor\right\}$ and

$$\delta_{k-1} := \begin{cases} \frac{\|\hat{b}_{k-1}\|}{2N_{k-1}+1} & \text{if } \|\hat{b}_{k-1}\| \geq \sqrt{n}\kappa \\ \sqrt{n}\kappa & \text{otherwise.} \end{cases}$$

(4) Compute a orthonormal basis $b_k^*, \ldots, b_n^*$ of the orthogonal complement of $V = \langle b_1, \ldots, b_{k-1}\rangle$.

(5) Compute b_k as follows:

  (a) Set $N := -1$.

  (b) Set $N := N + 1$.

(c) For every $z = (z_1, \ldots, z_n) \in \mathbb{Z}^n$ with $|z_j| \leq N_j$ for $j \in \{1, \ldots, k-1\}$ and with $\max_{k \leq j \leq n} |z_j| = N$ compute the representations $\frac{1}{\mu}\mathfrak{a}$ together with $\Psi(\mu)$ for all $\mu \in \mathcal{E}(\mathfrak{a})$ with $\Psi(\mu) \in P'(z)$, until $\frac{1}{\mu}\mathfrak{a} = \mathfrak{a}$ for a non-trivial μ.

(d) If $\frac{1}{\mu}\mathfrak{a} = \mathfrak{a}$ for a μ with non-zero height:

(i) if z has height > 1, while nothing was found for smaller heights, choose $b_1 = \Psi(\mu)$ and go to Step (6);

(ii) otherwise, find all other μ with $\frac{1}{\mu}\mathfrak{a} = \mathfrak{a}$ where $\Psi(\mu) \in P'(z')$ with the height of z' being equal to the height of z and with the height of $\Psi(\mu)$ being non-zero;

(iii) of the ones found, choose $\Psi(\mu)$ whose height is minimal as b_1, and go to Step (6).

(e) Go to Step (5 b).

(6) Compute b_k^* such that $b_1^*, \ldots, b_k^*$ is an orthonormal basis of $\langle b_1, \ldots, b_k \rangle$, and go to Step (2).

Theorem 6.4.9. *[Buc87c, p. 10, Satz 3.1] Let K be a number field of discriminant $\pm D$, $D > 0$ and with regulator R. The algorithm computes a basis of $\Psi(\mathcal{O}^*)$ in $\mathcal{O}(D^{\varepsilon}R)$ binary operations.* □

6.4.3 The Baby Step-Giant Step Algorithm

The most important algorithm in Buchmann's habilitation thesis is his baby step-giant step algorithm, which can compute a set of absolute values of fundamental units in $\mathcal{O}(D^{\varepsilon}\sqrt{R})$ binary operations. Unfortunately, the algorithm has never been published except in the thesis. We will sketch the algorithm in this section using the notations from the previous section.

Define $M_j := \left\lfloor \sqrt{\|\hat{b}_j\|} \right\rfloor$ and $\Delta_j := \frac{\|\hat{b}_j\|}{2M_j+1}$ for $1 \leq j < k$. Further, define

$$\tilde{b}_j := \Delta_j b_j^*$$

and

$$\tilde{P} := \left\{ \sum_{j=1}^{n} \lambda_j \tilde{b}_j \;\middle|\; |\lambda_j| \leq \tfrac{1}{2} \text{ for } 1 \leq j \leq n \right\}.$$

For $z = (z_1, \ldots, z_n) \in \mathbb{Z}^n$, define

$$\tilde{m}(z) := \sum_{j=1}^{n} z_j \tilde{b}_j \qquad \text{and} \qquad \tilde{P}(z) := \tilde{Z} + \tilde{m}(z).$$

Assume that we can find, for every $z \in \mathbb{Z}^n$, a minimum $\mu(z) \in \mathcal{E}(\mathfrak{a})$ with $\Psi(\mu(z)) \in \tilde{m}(z) + P'$; the proof of Proposition 6.5.1 will show that such a minimum exists. (The computation of $\mu(z)$ will be described at the end of this section.) Then, we have the following result:

Proposition 6.4.10. *[Buc87c, p. 37, Satz 9.1] Let $z \in \mathbb{Z}^n$. If $\Psi(\varepsilon) \in \tilde{P}(z) \cap \Lambda$ for $\varepsilon \in \mathcal{O}^*$, then $\Psi(\mu(z)\varepsilon^{-1}) \in \tilde{P} + P'$.*

Proof. We have $\Psi(\varepsilon^{-1}) \in -\tilde{P}(z)$, whence

$$\Psi(\mu(z)\varepsilon^{-1}) \in (\tilde{m}(z) + P') - (\tilde{P} + \tilde{m}(z)) = P' + \tilde{P}.$$

□

Hence, we can check whether $\tilde{P}(z) \cap \Lambda \neq \emptyset$ by comparing the reduced ideal $\frac{1}{\mu(z)}\mathfrak{a}$ with the reduced ideals $\frac{1}{\mu}\mathfrak{a}$ for all $\mu \in \mathcal{E}(\mathfrak{a})$ with $\Psi(\mu) \in P' + \tilde{P}$. Using this, Buchmann designed the following algorithm [Buc87c, p. 38, Algorithmus 8.1]:

Algorithm 6.4.11: Buchmann's Baby Step-Giant Step Algorithm for Computing a Basis of $\Lambda = \Psi(\mathcal{O}^*)$.

Input: the ring of integers $\mathcal{O}$ of the number field K.

Output: a basis $b_1, \ldots, b_n$ of Λ.

(1) Set $k := 0$, $\kappa := \frac{1}{2}\log D + s\log\frac{2}{\pi}$. Moreover, set $\delta_j := \sqrt{n}\kappa$ for $j = 1, \ldots, n$.

(2) Set $k := k + 1$; if $k > n$, we are done.

(3) If $k > 1$, set $M_{k-1} := \left\lceil \sqrt{\|\hat{b}_{k-1}\|} \right\rceil$, $\Delta_{k-1} := \frac{1}{2M_{k-1}+1}\|\hat{b}_{k-1}\|$.

(4) Compute a orthonormal basis $b_k^*, \ldots, b_n^*$ of the orthogonal complement of $V = \langle b_1, \ldots, b_{k-1}\rangle$.

(5) Compute b_k as follows:

  (a) Set $\ell := 1$ and $\Delta_0 := \lceil\delta\rceil$, where $\delta := \sqrt{n}\kappa$.

  (b) Define $\Delta := 2^\ell\delta$ and set $\Delta_j := \Delta$ for $j = k, \ldots, n$.

  (c) Compute the *baby stock*: use the baby step algorithm from Section 6.4.2 to compute the representations $\frac{1}{\mu}\mathcal{O}$ together with $\Psi(\mu)$ for all $\mu \in \mathcal{E}(\mathcal{O})$ with $\Psi(\mu) \in P' + \tilde{P}$.

  (d) If $k = 1$ and $\frac{1}{\mu}\mathcal{O} = \mathcal{O}$ for some μ with non-zero height, proceed as follows:

(i) if the non-trivial element was found in $P'(z)$ with the height of z being > 1, while nothing was found for smaller heights, choose that element as b_1 and go to Step (6);

(ii) otherwise, find all elements with non-zero height of Λ in all $P'(z')$ with the height of z' being equal to the height of z;

(iii) of the ones found, choose one whose height is minimal as b_1, and go to Step (6).

(e) Do the giant steps:

(i) Set $N := -1$.

(ii) Set $N := N + 1$. If $N > \Delta$, set $\ell := \ell + 1$ and go to Step (5 b).

(iii) For every $z = (z_1, \ldots, z_n) \in \mathbb{Z}^n$ with $|z_j| \leq M_j$ for $j \in \{1, \ldots, k-1\}$ and with $\max_{k \leq j \leq n} |z_j| = N$ compute $\frac{1}{\mu(z)}\mathcal{O}$ and $\Psi(\mu(z))$:

- if $\frac{1}{\mu(z)}\mathcal{O} \neq \frac{1}{\mu}\mathcal{O}$ for all $\frac{1}{\mu}\mathcal{O}$ computed in Step (5 c), go to Step (5 e ii);
- if $\frac{1}{\mu(z)}\mathcal{O} = \frac{1}{\mu}\mathcal{O}$ and if $N > 1$, let $b_k := \Psi(\mu(z)) - \Psi(\mu)$;
- if $N = 1$ and $\frac{1}{\mu(z)}\mathcal{O} = \frac{1}{\mu}\mathcal{O}$ appears, find all such μ and choose $b_k := \Psi(\mu(z)) - \Psi(\mu)$ with minimal positive height $|\hat{b}_k|$.

(6) Compute b_k^* such that $b_1^*, \ldots, b_k^*$ is an orthonormal basis of $\langle b_1, \ldots, b_k \rangle$, and go to Step (2).

Theorem 6.4.12. *[Buc87c, p. 10, Satz 3.3] Let K be a number field of discriminant $\pm D$, $D > 0$ and with regulator R. The algorithm computes a basis of $\Psi(\mathcal{O}^*)$ in $\mathcal{O}(D^{\varepsilon}\sqrt{R})$ binary operations.* □

Before ending, we want to describe how to compute the giant steps.

Computation of Giant Steps. Let $\mathfrak{a} = \mathcal{O}$. Assume that we have already computed all minima $\mu \in \mathcal{E}(\mathfrak{a})$ with $\Psi(\mu) \in P'(z)$ for several z with small height, in the sense that we know $\frac{1}{\mu}\mathcal{O}$ and $\Psi(\mu)$ for every such minimum. Then, given a $z' = (z'_1, \ldots, z'_n) \in \mathbb{Z}^n$, we can use these minima to find $\mu(z') \in \tilde{m}(z') + P'$ as follows:

(1) Choose representations $(\mathfrak{b}_{\pm j}, v_{\pm j}) = (\frac{1}{\mu_{\pm j}}\mathcal{O}, \Psi(\mu_{\pm j}))$ with $v_{\pm j} \in \pm\tilde{b}_j + P'$ for $j \in \{1, \ldots, n\}$.

(2) Reduce the tuples $([\mathfrak{b}_{\pm j}]_\sim, \pm\tilde{b}_j - v_{\pm j})$ to f-representations $G_{\pm j}$.

(3) In $\mathrm{Rep}^f(K)$, compute $([\mathfrak{b}]_\sim, (t_1, \ldots, t_n)) = \sum_{j=1}^n |z'_j| G_{\pm j}$ with the appropriate sign for $G_{\pm j}$.

(4) Reduce $([\mathfrak{b}]_\sim, (t_1 + \frac{1}{2}\kappa, \ldots, t_n + \frac{1}{2}\kappa))$ and choose the resulting reduced ideal for $\mu(z')$.

By Proposition 6.5.1, such representations $(\mathfrak{b}_{\pm j}, v_{\pm j})$ exists. If a large enough baby stock has been computed, they can be found among these.

Obviously, one can proceed without using f-representations: simply multiply the corresponding ideals, add the relative distances, and try to do baby steps to minimize the relative distances.

6.5 A General Baby Step-Giant Step Algorithm for Global Fields

In this section, we want to describe a general baby step-giant step algorithm for *all* global fields. We will use the same techniques used by Buchmann in the number field case, together with a variation of Terr's modification of the baby step-giant step technique for computing orders [Ter00], to obtain an algorithm which computes a basis of $\Lambda = \Psi(\mathcal{O}^*)$ in $\mathcal{O}(\sqrt{R})$ infrastructure operations. The idea to apply Terr's modification is taken from Buchmann's and Schmidt's algorithm for computing the structure of a finite abelian group [BS05], which we used in Section 6.2.2. The same idea has been applied to Shanks algorithm for real quadratic number fields in [BV06].

Assume that $b_1, \ldots, b_{k-1}$ have already been computed and are elements of Λ which can be continued to a basis of Λ. The aim is to compute b_k such that $b_1, \ldots, b_{k-1}, b_k$ can be continued to a basis of Λ. We compute an orthonormal basis $b_1^*, \ldots, b_{k-1}^*$ of $V = \langle b_1, \ldots, b_{k-1}\rangle$ and an orthonormal basis $b_k^*, \ldots, b_n^*$ of the orthogonal complement of V.

If K is a function field of genus g, let

$$\kappa := g + \deg \mathfrak{p}_{n+1} - 1.$$

If K is a number field with $2s$ complex embeddings and discriminant $\pm D$, $D > 0$, let

$$\kappa := \tfrac{1}{2}\log D + s \log \tfrac{2}{\pi}.$$

Choose $\delta_j := \sqrt{n}\kappa$ for $1 \leq j \leq n$. In Section 6.4.2, we defined $b'_j := \delta_j b^*_j$ and $P' := \{\sum_{j=1}^n \lambda_j b'_j \mid |\lambda_j| \leq \frac{1}{2}\}$, and for $z = (z_1, \ldots, z_n) \in \mathbb{Z}^n$ we defined $m'(z) := \sum_{j=1}^n x_j b'_j$ and $P'(z) := P' + m'(z)$.

The idea is to use a classic baby step-giant step approach for the directions $b^*_1, \ldots, b^*_{k-1}$, while using an approach similar to Terr's for the directions $b^*_k, \ldots, b^*_n$.

Define $N_j := \left\lceil \frac{\|\hat{b}_j\|}{2\delta_j} \right\rceil$ for $1 \leq j < k$; then

$$P_\infty \subseteq \bigcup_{\substack{z=(z_1,\ldots,z_n)\in\mathbb{Z}^n \\ |z_j|\leq N_j \text{ for } j<k}} P'(z).$$

The baby stock computed in iteration N will contain the minima in

$$\bigcup_{\substack{z=(z_1,\ldots,z_n)\in\mathbb{Z}^n \\ |z_j|\leq \frac{1}{2}\lceil\sqrt{N_j}\rceil+1 \text{ for } j<k \\ |z_j|\leq N+1 \text{ for } j\geq k}} P'(z),$$

while the giant step minima will lie in $P'(z)$ with $z_j = n_j\lceil\sqrt{N_j}\rceil$ for $n_j = -\lceil\sqrt{N_j}\rceil, \ldots, \lceil\sqrt{N_j}\rceil$ if $j = 1, \ldots, k-1$ and $z_j = -N^2 + 2n_jN$ for $n_j = 0, \ldots, N$ if $j = k, \ldots, n$, and with $\max_{k\leq j\leq n} |z_j| = N^2$.

We begin with describing how to compute the baby stock. For that, we proceed similarly as Buchmann in [Buc87c]. Then, in Section 6.5.2 we will see how to compute the giant steps. Finally, in Section 6.5.3, we will describe our baby step-giant step algorithm and prove that the algorithm requires $\mathcal{O}(\sqrt{R})$ operations in the infrastructure.

6.5.1 Computation of the Baby Stock

In this section, we want to show how to compute all elements in $\Psi(\mathcal{E}(\mathfrak{a})) \cap P'(z)$. This allows us to compute the baby stock, which is the union of these sets for $z \in \mathbb{Z}^n$ with bounded components.

Recall that we defined $b'_j = \delta_j b^*_j$ for a choice of $\delta_j > 0$. Moreover, we defined $m'(z_1, \ldots, z_n) = \sum_{j=1}^n z_j b'_j$, $P' = \{\sum_{j=1}^n \lambda_j b'_j \mid |\lambda_j| \leq \frac{1}{2}\}$ and $P'(z) := m'(z) + P'$ for $z \in \mathbb{Z}^n$.

We begin with showing that $\Psi(\mathcal{E}(\mathfrak{a})) \cap P'(z)$ is non-empty for every $z \in \mathbb{Z}^n$ if the δ_j are chosen in the right way.

Proposition 6.5.1. *Choose $\delta_j > 0$, $1 \leq j \leq n$ such that $\delta_j \geq \sqrt{n}\kappa$. Then, $\Psi(\mathcal{E}(\mathfrak{a})) \cap P'(z) \neq \emptyset$.*

Proof. Write $m'(z) = (v_1, \ldots, v_n)$ and consider the tuple

$$([\mathfrak{a}]_\sim, (v_1 + \tfrac{1}{2}\kappa, \ldots, v_n + \tfrac{1}{2}\kappa));$$

using Lemma 4.2.6, we get a minimum $\mu \in \mathcal{E}(\mathfrak{a})$ such that $([\frac{1}{\mu}\mathfrak{a}]_\sim, (v_1 + \frac{1}{2}\kappa + \nu_{\mathfrak{p}_1}(\mu), \ldots, v_n + \frac{1}{2}\kappa + \nu_{\mathfrak{p}_n}(\mu))) \in \mathrm{Rep}^f(K)$. But then, by Proposition 4.4.1, we have

$$0 \leq \sum_{i=1}^{n} (v_i + \tfrac{1}{2}\kappa + \nu_{\mathfrak{p}_i}(\mu)) \deg \mathfrak{p}_i \leq \kappa$$

and $v_i + \frac{1}{2}\kappa + \nu_{\mathfrak{p}_i}(\mu) \geq 0$ for every i. Hence, $0 \leq v_i + \frac{1}{2}\kappa + \nu_{\mathfrak{p}_i}(\mu) \leq \kappa$, i.e. we have $|v_i - (-\nu_{\mathfrak{p}_i}(\mu))| \leq \frac{1}{2}\kappa$. But then, $\|m'(z) - \Psi(\mu)\| \leq \sqrt{n}\frac{1}{2}\kappa$.

Hence, it suffices to show that $X := \{x \in \mathbb{R}^n \mid \|x\| \leq \sqrt{n}\frac{1}{2}\kappa\} \subseteq P'$. For that, let $x \in X$ and write $x = \sum_{j=1}^{n} \lambda_j b'_j$. As the $b'_j = \delta_j b_j^*$ are orthogonal, we get $x_j = \frac{\langle x, b_j^* \rangle}{\delta_j}$, i.e. $|x_j| \leq \frac{1}{\delta_j}\|x\| \cdot \|b_j^*\| = \frac{\|x\|}{\delta_j} \leq \frac{\sqrt{n}\frac{1}{2}\kappa}{\delta_j}$ by Cauchy-Schwarz. Now, by the choice of the δ_j, this is $\leq \frac{1}{2}$, whence $x \in P'$. □

Next, we want to show that one can find a chain of neighbors between two minima whose absolute values are bounded.

Proposition 6.5.2. *[Buc87c, p. 48, Satz 10.6] Let $\mu, \mu' \in \mathcal{E}(\mathfrak{a})$. Then there exists a sequence $\mu = \mu_1, \mu_2, \ldots, \mu_{t-1}, \mu_t = \mu'$ such that μ_i is a neighbor of μ_{i+1}, $1 \leq i < t$, and that $|\mu_i|_\mathfrak{p} \leq \max\{|\mu|_\mathfrak{p}, |\mu'|_\mathfrak{p}\}$ for every $\mathfrak{p} \in S$ and $i \in \{1, \ldots, t\}$.*

Proof. In the function field case, this follows from Proposition 3.4.4. In the number field case, the same strategy as in the proof of Proposition 3.4.4 can be used; the induction argument has to be replaced by the fact that the set of minima in $B(\mathfrak{a}, \mu, \mu')$ is finite and, hence, the set of values $b(\mu'', \mu')$ can attain is finite. As $b(\mu'', \mu')$ will decrease in every step, eventually the constructed sequence will reach μ'. □

Finally, we want to show that we can find all minima in $\Psi(\mathcal{E}(\mathfrak{a})) \cap P'(z)$ in a bounded area. Note that if we fix a minimum $\mu' \in \mathcal{E}(\mathfrak{a})$, then we have the bijection $\mathcal{E}(\frac{1}{\mu'}\mathfrak{a}) \to \mathcal{E}(\mathfrak{a})$, $\mu \mapsto \mu\mu'$.

Proposition 6.5.3. *[Buc87c, p. 46, Satz 10.3] Fix $\mu' \in \mathcal{E}(\mathfrak{a})$ such that $\Psi(\mu') \in P'(z')$. Define*

$$B_{\mathfrak{p}_i} = q^{\sum_{j=1}^{n} (|b'_{ji}| + (z_j - z'_j) b'_{ji}) \deg \mathfrak{p}_i}$$

for $i = 1, \dots, n$ *and*

$$B_{\mathfrak{p}_{n+1}} = \frac{|N(\frac{1}{\mu'}\mathfrak{a})|q^{\kappa}}{q^{\sum_{i=1}^{n}\sum_{j=1}^{n}(-|b'_{ji}|+(z_j-z'_j)b'_{ji})\deg \mathfrak{p}_i}} = q^{-\deg \operatorname{div}(\frac{1}{\mu'}\mathfrak{a})+\kappa-\sum_{i=1}^{n}\sum_{j=1}^{n}(-|b'_{ji}|+(z_j-z'_j)b'_{ji})\deg \mathfrak{p}_i}.$$

If $\mu \in \mathcal{E}(\frac{1}{\mu'}\mathfrak{a})$ *satisfies* $\Psi(\mu\mu') \in P'(z)$*, then* $|\mu|_{\mathfrak{p}} \leq B_{\mathfrak{p}}$ *for* $\mathfrak{p} \in S$*.*

Proof. Write $\Psi(\mu') = \sum_{j=1}^{n}(z'_j+\zeta_j)b'_j$ with $|\zeta_j| \leq \frac{1}{2}$ and $\Psi(\mu\mu') = \sum_{j=1}^{n}(z_j+\xi_j)b'_j$ with $|\xi_j| \leq \frac{1}{2}$. Then,

$$\Psi(\mu) = \sum_{j=1}^{n}((z_j - z'_j) + (\xi_j - \zeta_j))b'_j.$$

Now

$$-\nu_{\mathfrak{p}_i}(\mu) = \sum_{j=1}^{n}((z_j - z'_j) + (\xi_j - \zeta_j))b'_{ji},$$

if $b'_j = (b'_{j1}, \dots, b'_{jn})$. Therefore,

$$\sum_{j=1}^{n}(-|b'_{ji}| + (z_j - z'_j)b'_{ji}) \leq -\nu_{\mathfrak{p}_i}(\mu) \leq \sum_{j=1}^{n}(|b'_{ji}| + (z_j - z'_j)b'_{ji}).$$

This shows $|\mu|_{\mathfrak{p}_i} \leq B_{\mathfrak{p}_i}$ for $i = 1, \dots, n$.

Finally, we know $\prod_{i=1}^{n+1}|\mu|_{\mathfrak{p}_i} = |N(\mu)| \leq |N(\frac{1}{\mu'}\mathfrak{a})|q^{\kappa}$, whence

$$|\mu|_{\mathfrak{p}_{n+1}} \leq \frac{|N(\frac{1}{\mu'}\mathfrak{a})|q^{\kappa}}{\prod_{i=1}^{n}|\mu|_{\mathfrak{p}_i}} \leq \frac{|N(\frac{1}{\mu'}\mathfrak{a})|q^{\kappa}}{\prod_{i=1}^{n}q^{\sum_{j=1}^{n}(-|b'_{ji}|+(z_j-z'_j)b'_{ji})\deg \mathfrak{p}_i}} = B_{\mathfrak{p}_{n+1}}.$$

□

Then we can enumerate all minima $\mu \in \mathcal{E}(\frac{1}{\mu'}\mathfrak{a})$ with $\Psi(\mu\mu') \in P'(z)$ as follows: first, find one such minimum μ. Then, using the algorithm presented in Section 6.3, compute all neighbors μ'' of μ and store the ones which satisfy $|\mu''|_{\mathfrak{p}} \leq B_{\mathfrak{p}}$, $\mathfrak{p} \in S$, with $B_{\mathfrak{p}}$ defined as in Proposition 6.5.3. Continue with these, until all minima satisfying this are found. Then, find among these the ones with $\Psi(\bullet) \in P'(z)$.

Beginning with $z = 0$ and $\mu = 1$ if $\mathfrak{a}$ is reduced, this allows us to compute $P'(z)$; and, given $P'(z)$ for some z, we can compute $P'(z \pm e_i)$ if e_i is a vector with zeros in every component but one 1 in the i-th component: take a minimum of $P'(z)$ which is at the border to $P'(z \pm e_i)$ and compute its neighbors, until one finds one which lies in $P'(z \pm e_i)$. Using that one, one can compute all elements in $P'(z \pm e_i)$.

Function Field Optimizations. Note that in the function field case, $\Psi(\mathcal{E}(\mathfrak{a}))$ in general lies rather dense in $\mathbb{Z}^n$; hence, an alternative strategy is to enumerate all $t \in \mathbb{Z}^n$ with $t \in P'(z)$ and to check for every such t if a minimum $\mu \in \mathcal{E}(\mathfrak{a})$ exists with $\Psi(\mu) = t$. For that, one can proceed as follows.

Choose an f-representation $([\frac{1}{\mu'}\mathfrak{a}]_\sim, (t_1, \ldots, t_n))$ with

$$\Psi(\mu') + (t_1, \ldots, t_n) \in P'(z) \cap \mathbb{Z}^n$$

such that the $|t_i|$ are small. Then, reduce this f-representation to, say, $([\frac{1}{\mu\mu'}\mathfrak{a}]_\sim, (\tilde{t}_1, \ldots, \tilde{t}_n))$ with $\tilde{t}_i = t_i + \nu_{\mathfrak{p}_i}(\mu)$; if $\tilde{t}_i = 0$ for all i, then $\mu\mu' \in \mathcal{E}(\mathfrak{a})$ and $\Psi(\mu\mu') = \Psi(\mu') + (t_1, \ldots, t_n) \in P'(z) \cap \Psi(\mathcal{E}(\mathfrak{a}))$; otherwise, there exists no minimum $\mu'' \in \mathcal{E}(\mathfrak{a})$ with $\Psi(\mu'') = \Psi(\mu') + (t_1, \ldots, t_n)$. In the second case, the information obtained gives information on $\Psi(\mathcal{E}(\mathfrak{a}))$, too: one knows that $\Psi(\mu\mu') = \Psi(\mu') + (t_1, \ldots, t_n) - (\tilde{t}_1, \ldots, \tilde{t}_n) \in \Psi(\mathcal{E}(\mathfrak{a}))$ and that $\Psi(\mathcal{E}(\mathfrak{a})) \cap \{(t_i - s_i)_i \in \mathbb{Z}^n \mid 0 \leq s_i \leq \tilde{t}_i\} = \{\Psi(\mu'\mu)\}$; the latter statement follows from a small fact on f-representations:

Remark 6.5.4. Let $([\mathfrak{b}]_\sim, (t_1, \ldots, t_n)) \in \mathrm{Rep}^f(K)$ and let $s = (s_1, \ldots, s_n) \in \mathbb{G}^n$ such that $0 \leq s_i \leq t_i$ for all i. Then $([\mathfrak{b}]_\sim, (s_1, \ldots, s_n)) \in \mathrm{Rep}^f(K)$, as $1 \in B(\mathfrak{b}, (s_1, \ldots, s_n, 0)) \subseteq B(\mathfrak{b}, (t_1, \ldots, t_n, 0))$.

Hence, one could proceed by allocating an array which stores, for each possible $t \in \mathbb{Z}^n$ with $t \in P'(z)$, whether $t \in \Psi(\mathcal{E}(\mathfrak{a}))$, $t \notin \Psi(\mathcal{E}(\mathfrak{a})$ or whether this has not been yet tested. Then, starting from one point, one iterates over the entries which have not been yet tested and which are near to positively tested elements (i.e. near to elements of $\Psi(\mathcal{E}(\mathfrak{a}))$) and tests them.

6.5.2 Computation of Giant Steps

Given $z \in \mathbb{Z}^n$, we want to compute $\frac{1}{\mu}\mathcal{O}$ and $\Psi(\mu)$ for a $\mu \in \mathcal{E}(\mathcal{O})$ with $\Psi(\mu) \in P'(z)$. Using the arguments in the proof of Proposition 6.5.1, it suffices to reduce the tuple $([\mathcal{O}]_\sim, v) \in \mathrm{Red}(K)/_\sim \times \mathbb{G}^n$ with $v = m'(z) + (\frac{1}{2}\kappa, \ldots, \frac{1}{2}\kappa)$.

For that, we find f-representations $G_{\pm j} = ([\frac{1}{\mu_{\pm j}}\mathcal{O}]_\sim, v_{\pm j})$ with $\Psi(\mu_{\pm j}) + v_{\pm j} = \pm b'_j$. Moreover, find an f-representation $G' = ([\frac{1}{\mu'}\mathcal{O}]_\sim, v')$ with $\Psi(\mu') + v' = (\frac{1}{2}\kappa, \ldots, \frac{1}{2}\kappa)$. These can be found by taking tuples $([\frac{1}{\mu}\mathcal{O}]_\sim, v)$ where $\Psi(\mu)$ is 'near' to the sought $\Psi(\mu_{\pm j})$ respectively $\Psi(\mu')$; such μ can be found while computing the baby stock. Then, one reduces these tuples to obtain f-representations.

Now that we have the f-representations $G_{\pm j}$ and G', we can compute $G = \sum_{j=1}^{n} |z_j| R_{\pm j} + G'$, where the appropriate signs are taken. For this, we can use a standard double-and-add method, or also a ternary expansion of the coefficients as we have f-representations for $R_{\pm j}$ and $-R_{\pm j} = R_{\mp j}$.

Then, if $G = ([\frac{1}{\mu}\mathcal{O}]_\sim, v)$, we have that $\Psi(\mu) + v = m'(z) + (\frac{1}{2}\kappa, \ldots, \frac{1}{2}\kappa)$, whence we can take $\frac{1}{\mu}\mathcal{O}$ as the sought reduced ideal, and we know that $\Psi(\mu) = m'(z) + (\frac{1}{2}\kappa, \ldots, \frac{1}{2}\kappa) - v \in m'(z) + P' = P'(z)$.

Note that in general, we do not want to compute a giant step for an arbitrary $z \in \mathbb{Z}^n$, but we already computed giant steps to similar points. Hence, one can reduce the amount of infrastructure operations dramatically.

6.5.3 The Baby Step-Giant Step Algorithm

We are ready to present our algorithm:

Algorithm 6.5.5: Baby Step-Giant Step Algorithm for Computing a Basis of $\Lambda = \Psi(\mathcal{O}^*)$.

Input: the ring of integers $\mathcal{O}$ of the global field K.

Output: a basis $b_1, \ldots, b_n$ of Λ.

(1) Set $k := 0$ and $\kappa := \frac{1}{2}\log D + s\log\frac{2}{\pi}$ if K is a number field with $2s$ complex embeddings or $\kappa := g + \deg \mathfrak{p}_{n+1} - 1$ if K is a function field of genus g.

(2) Set $\delta_j := \sqrt{n}\kappa$ for all j.

(3) Set $k := k + 1$; if $k > n$, we are done.

(4) If $k > 1$, set $N_{k-1} := \left\lceil \frac{\|\hat{b}_{k-1}\|}{2\delta_{k-1}} \right\rceil$.

(5) Compute a orthonormal basis $b_k^*, \ldots, b_n^*$ of the orthogonal complement of $V = \langle b_1, \ldots, b_{k-1}\rangle_{\mathbb{R}}$.

(6) Compute b_k as follows:

  (a) Set $N := 1$.

  (b) Compute the *baby stock*: use the baby step algorithm from Section 6.5.1 to compute the representations $\frac{1}{\mu}\mathcal{O}$ together with $\Psi(\mu)$ for all $\mu \in \mathcal{E}(\mathcal{O})$ with $\Psi(\mu) \in P'(z)$ with $z = (z_1, \ldots, z_n) \in \mathbb{Z}^n$ with $|z_j| \leq \frac{1}{2}\lceil\sqrt{N_j}\rceil + 1$ for $1 \leq j < k$ and $|z_j| \leq N + 1$ for $j = k, \ldots, n$.

  (c) If $k = 1$ and $\frac{1}{\mu}\mathcal{O} = \mathcal{O}$ for some μ with non-zero height, proceed as follows:

    (i) if the non-trivial element was found in $P'(z)$ with the height of z being > 1, while nothing was found for smaller heights, choose that element as b_1 and go to Step (7);

    (ii) otherwise, find all elements with non-zero height of Λ in all $P'(z')$ with the height of z' being equal to the height of z;

    (iii) of the ones found, choose one whose height is minimal as b_1, and go to Step (7).

  (d) Do the *giant steps*:

(i) For $z' = (n_1\lceil\sqrt{N_1}\rceil, \ldots, n_{k-1}\lceil\sqrt{N_{k-1}}\rceil, -N^2+2n_kN, \ldots, -N^2+2n_nN) \in \mathbb{Z}^n$ with $(n_1, \ldots, n_n) \in \mathbb{Z}^n$, $|n_j| \leq \lceil\sqrt{N_j}\rceil$ for $1 \leq j < k$ and $0 \leq n_j \leq N$ for $j = k, \ldots, n$ and with $\{n_k, \ldots, n_n\} \cap \{0, N\} \neq \emptyset$, compute the giant step $\frac{1}{\mu'}\mathcal{O}$ and $\Psi(\mu')$ with $\Psi(\mu') \in P'(z')$:

- if $\frac{1}{\mu'}\mathcal{O} = \frac{1}{\mu}\mathcal{O}$ and if $N > 3$, let $b_k := \Psi(\mu') - \Psi(\mu)$ and go to Step (7);
- if $N \in \{2, 3\}$ and $\frac{1}{\mu'}\mathcal{O} = \frac{1}{\mu}\mathcal{O}$ appears, find all such μ' and choose $b_k := \Psi(\mu') - \Psi(\mu)$ with minimal non-zero height $|\hat{b}_k|$ and go to Step (7); if no b_k exists with non-zero height, continue with Step (6 e);
- if $N = 1$ and $\frac{1}{\mu'}\mathcal{O} = \frac{1}{\mu}\mathcal{O}$ appears, find all such μ for $N = 1$ and $N = 2$ and choose $b_k := \Psi(\mu') - \Psi(\mu)$ with minimal non-zero height $|\hat{b}_k|$ and go to Step (7); if no b_k exists with non-zero height, continue with Step (6 e).

(e) Set $N := N + 1$ and go to Step (6 b).

(7) Compute b_k^* such that $b_1^*, \ldots, b_k^*$ is an orthonormal basis of $\langle b_1, \ldots, b_k\rangle_{\mathbb{R}}$, compute $\hat{b}_k$ and go to Step (3).

Note that for each iteration of Step (6 b), one only needs to compute the $P'(z)$ whose height is exactly N.

Proposition 6.5.6. *The algorithm is correct. Moreover, in Step (7), we have* $N = \mathcal{O}\Big(\frac{1}{\delta_k}\sqrt{|\hat{b}_k|}\Big)$.

Proof. First, we show that the algorithm computed a valid b_k if it jumps to Step (7).

- First, assume that the algorithm jumps to Step (7) from Step (6 c i). Then the height of each minimum in $P'(z)$ with height N is between $(N - \frac{1}{2})\delta_j$ and $(N + \frac{1}{2})\delta_j$; hence, as $N \geq 2$, we have $\frac{1}{2}(N + \frac{1}{2})\delta_j < (N - \frac{1}{2})\delta_j$, whence by Corollary 6.4.6 the choice of b_k is valid.
- Next, assume that the algorithm jumps to Step (7) from Step (6 c iii). In that case, by the way b_k was chosen and by Corollary 6.4.6, the choice of b_k is valid.

- Finally, assume that the algorithm jumps to Step (7) from Step (6 d i).

  If $N > 3$, we have $\frac{1}{2}(N^2+N+1) < N^2-N-1$, whence the minimum height a vector b_k can have is greater than half of the maximum height. Hence, any b_k in this set with positive height will satisfy the requirements of Corollary 6.4.6.

  Now assume that $N \leq 3$. If $N \in \{2,3\}$, we have $(N+1)^2-(N+1)-1 > \frac{1}{2}(N^2+N+1)$, whence it cannot happen that for $N+1$ we obtain a $b_k \in \Lambda$ which has height $\leq$ of half of a height of a $b_k \in \Lambda$ obtained for N. Hence, for $N \in \{2,3\}$, it suffices to compute all b_k for the current N to be sure that the requirements of Corollary 6.4.6 hold.

  Finally, if $N = 1$, it can happen that for $N = 2$, we obtain a b_k whose height is $\leq$ half the height of a b_k obtained for $N = 1$. But as in this case, we also checked all b_k for $N = 2$, so we can rule out this case.

Hence, if the algorithm terminates, it returns a valid result. Next, we show that it will terminate.

Let $b_k \in \Lambda$ with $|\hat{b}_k| > 0$. Choose $N \in \mathbb{N}$ minimal such that $\delta_k(N^2+N) \geq |\hat{b}_k|$. Write $b_k = \sum_{j=1}^{n} \lambda_j b'_j$. By Proposition 6.4.5, we can assume $|\lambda_j| \leq \frac{1}{2\delta_j}\|\hat{b}_j\| \leq N_j$, $1 \leq j < k$. By assumption, we have $|\lambda_j| \leq N^2+N$ for $k \leq j \leq n$ and there exists an $i \in \{k,\ldots,n\}$ with $|\lambda_i| > (N-1)^2+(N-1) = N^2-N$.

For $j \in \{1,\ldots,k-1\}$, write $\lambda_j = n_j\lceil\sqrt{N_j}\rfloor + r_j$ with $n_j \in \{-\lceil\sqrt{N_j}\rfloor, \ldots, \lceil\sqrt{N_j}\rfloor\}$ and $r_j \in \mathbb{R}$ with $|r_j| \leq \frac{1}{2}\lceil\sqrt{N_j}\rfloor$. Write $r_j = z_j + \tilde{r}_j$ with $z_j \in \mathbb{Z}$ and $|\tilde{r}_j| \leq \frac{1}{2}$ such that $|z_j| \leq \frac{1}{2}\lceil\sqrt{N_j}\rfloor$.

For $j \in \{k,\ldots,n\}$, write $\lambda_j = -N^2+2n_jN+z_j+\lambda'_j$ with $n_j \in \{0,\ldots,N\}$, $z_j \in \{-N,\ldots,N\}$ and $|\lambda'_j| \leq \frac{1}{2}$, where $-N \leq z_j+\lambda'_j \leq N$. Note that for $j = i$, we have $n_j \in \{0,N\}$, as otherwise $|\lambda_j| \leq N^2-2N+N = N^2-N$, a contradiction.

Then $|n_j| \leq \lceil\sqrt{N_j}\rfloor$ and $|z_j| \leq \frac{1}{2}\lceil\sqrt{N_j}\rfloor$ for $1 \leq j < k$, and $0 \leq n_j \leq N$ and $|z_j| \leq N$ for $k \leq j \leq n$. Now there exists a $\mu' \in \mathcal{E}(\mathfrak{a})$ with $\Psi(\mu') \in P'(z')$, where $z' = (n_1\lceil\sqrt{N_1}\rfloor, \ldots, n_{k-1}\lceil\sqrt{N_{k-1}}\rfloor, -N^2+2n_kN, \ldots, -N^2+2n_nN)$, and the height of $P'(z')$ is N^2. If $\Psi(\varepsilon) = b_k$ for $\varepsilon \in \mathcal{O}^*$, then $\mu'\varepsilon^{-1} \in \mathcal{E}(\mathfrak{a})$. We want to show that $\Psi(\mu'\varepsilon^{-1}) \in P'(z)$ for $z = (-z_1,\ldots,-z_n)$.

We have $\Psi(\mu'\varepsilon^{-1}) = \Psi(\mu') - b_k \in P'(z') - b_k$. Now $m'(z') - b_k$ can be

rewritten as

$$\begin{aligned}
&= \sum_{j=1}^{k-1} \left[n_j \left\lceil \sqrt{N_j} \right\rceil - \left(n_j \left\lceil \sqrt{N_j} \right\rceil + r_j \right) \right] b'_j \\
&+ \sum_{j=k}^{n} \left[(-N^2 + 2n_j N) - \left(-N^2 + 2n_j N + z_j + \lambda'_j \right) \right] b'_j \\
&= m'(z) - \sum_{j=1}^{k-1} \tilde{r}_j b'_j - \sum_{j=k}^{n} \lambda'_j b'_j.
\end{aligned}$$

Hence,

$$\Psi(\mu' \varepsilon^{-1}) \in P'(z) - \sum_{j=1}^{k-1} \tilde{r}_j b'_j - \sum_{j=k}^{n} \lambda'_j b'_j \subseteq P'(z) + P'.$$

Therefore, if we modify z in each component by at most one, we can obtain $\Psi(\mu' \varepsilon^{-1}) \in P'(z)$. □

Proposition 6.5.7. *The algorithm needs $\mathcal{O}(D^{\varepsilon}\sqrt{R})$ computations in the infrastructure in the number field case and $\mathcal{O}(\kappa^n \sqrt{R})$ computations in the infrastructure in the function field case, where the $\mathcal{O}$-constant only depends on the degree of K over $\mathbb{Q}$ respectively $k(x)$.*

We denote by $\lambda_j(\Lambda)$ the j-th successive minimum of Λ with respect to the Euclidean norm on $\mathbb{R}^n$. Note that $\lambda_1(\Lambda) \leq \cdots \leq \lambda_n(\Lambda)$.

Proof. By [Buc87c, p. 22, Satz 5.5], we have $\|b_k\|^2 < n \cdot (k+3) \cdot \lambda_k(\Lambda)^2$. Note that $|\hat{b}_k| \leq \|b_k\|$, whence

$$N = \mathcal{O}\left(\sqrt{|\hat{b}_k|} \right) = \mathcal{O}(\sqrt[4]{n \cdot (k+3)} \cdot \sqrt{\lambda_k(\Lambda)}) = \mathcal{O}(\sqrt{\lambda_k(\Lambda)}).$$

Moreover, $\frac{1}{\delta_j} = \mathcal{O}(1)$ and $\|\hat{b}_j\| \leq \|b_j\| = \mathcal{O}(\lambda_j(\Lambda))$.

To compute the baby stock for N, we have to enumerate at most

$$\begin{aligned}
&(2N+3)^{n-k+1} \cdot \prod_{j=1}^{k-1} \left(\left\lceil \sqrt{\tfrac{\|\hat{b}_j\|}{2\delta_j}} \right\rceil + 5 \right) \\
&= \mathcal{O}\left(\lambda_k(\Lambda)^{\frac{n-k+1}{2}} \prod_{j=1}^{k-1} \sqrt{\|b_j\|} \right) \\
&= \mathcal{O}\left(\prod_{j=k}^{n} \sqrt{\lambda_j(\Lambda)} \cdot \prod_{j=1}^{k-1} \sqrt{\lambda_j(\Lambda)} \right)
\end{aligned}$$

parallelepipeds; by Minkowski [Buc87c, p. 9, Satz 2.1], this amount is

$$\mathcal{O}\Big(\sqrt{\gamma_n^{n/2}\det\Lambda}\Big),$$

where γ_n is the n-th Hermite constant. As $\det\Lambda\cdot\prod_{i=1}^{n}\deg\mathfrak{p}_i = R$, we get that the number of parallelepipeds is $\mathcal{O}(\sqrt{R})$.

In the number field case, by [Buc87c, p. 45, Korollar 10.1], the number of minima in $P'(z)$ is $\mathcal{O}(D^{\varepsilon})$. Hence, together with Proposition 6.3.12, we see that we need $\mathcal{O}(D^{\varepsilon})$ computations in the infrastructure to enumerate $P'(z)$.

In the function field case, the maximal number of minima in $P'(z)$ is bounded by $\mathcal{O}(\kappa^n)$, and they can be enumerated using the discussed strategy in this many operations.

The number of giant step minima which have to be computed is bounded by

$$\sum_{\hat{N}=1}^{N}[(\hat{N}+1)^{n-k+1}-(\hat{N}-1)^{n-k+1}]\cdot\prod_{j=1}^{k-1}\left(2\left\lceil\sqrt{N_j}\right\rceil+1\right)$$

if $N>1$. As before,

$$\prod_{j=1}^{k-1}\left(2\left\lceil\sqrt{N_j}\right\rceil+1\right)=\mathcal{O}\left(\prod_{j=1}^{k-1}\sqrt{\lambda_j(\Lambda)}\right).$$

Now $(\hat{N}+1)^{n-k+1}-(\hat{N}-1)^{n-k+1}=\mathcal{O}(\hat{N}^{n-k})=\mathcal{O}(N^{n-k})$, whence

$$\begin{aligned}&\sum_{\hat{N}=1}^{N}[(\hat{N}+1)^{n-k+1}-(\hat{N}-1)^{n-k+1}]=\mathcal{O}(N^{n-k+1})\\ &=\mathcal{O}\Big(\sqrt{\lambda_k(\Lambda)}^{n-k+1}\Big)=\mathcal{O}\left(\prod_{j=k}^{n}\sqrt{\lambda_j(\Lambda)}\right).\end{aligned}$$

Therefore, as above, we get $\mathcal{O}(\sqrt{R})$ giant step computations. □

Note that our algorithm would also work for arbitrary n-dimensional infrastructures as defined in Section 2.4, as long as we can guarantee an analogue to Proposition 6.5.1 and if we are able to efficiently compute all minima inside $P'(z)$.

6.6 Conclusion

According to J. Buchmann, the main bottleneck of the baby step-giant step algorithm is the computation of the baby stock. This boils down to computation of all neighbors of a given minimum, as described in Section 6.3, as one cannot use baby steps as defined in Section 3.5 to reach every minimum. Buchmann writes,

> *"In der Tat scheint die Suche nach den zulässigen Minima in $\mathcal{B}$ das Hauptproblem unseres Verfahrens zu sein. Wir können zwar einen $\mathcal{O}(\mathcal{D}^{\varepsilon})$-Algorithmus zur Lösung des Problems angeben, dieser ist aber in der Praxis noch ziemlich zeitraubend."*[1]
>
> [Buc87c, p. 47]

In the function field case, one has the advantage that $\Psi(\mathcal{E}(\mathfrak{a})) \subseteq \mathbb{Z}^n$, and that one can efficiently test using f-representations whether for a given $t \in \mathbb{Z}^n$, there exists a minimum $\mu \in \mathcal{E}(\mathfrak{a})$ with $\Psi(\mu) = t$ (see the end of Section 6.5.1). By Proposition 4.4.1, we see that if the number of reduced principal ideals $\mathfrak{a}$ with $\operatorname{div}(\mathfrak{a}) = g + (\deg \mathfrak{p}_{n+1} - 1)$ is large, then basically every $t \in \mathbb{Z}^n$ appears as $\Psi(\mu) = t$. If $\mathfrak{a} = (\frac{1}{\mu})$ for some $\mu \in \mathcal{E}(\mathcal{O})$, then $\deg \operatorname{div}(\mathfrak{a}) = \deg N_{K/k(x)}(\mu)$. In the case $\deg \mathfrak{p}_{n+1} = 1$, if one assumes that $N_{K/k(x)}(\mu) \in k[t]$ is a random polynomial of degree $\leq g$, the probability that the degree equals g is $\frac{(q-1)q^g}{q^{g+1}-1} = 1 - \frac{1}{q} + \mathcal{O}(q^{-g-1})$ if $q = |k|$. In some experiments with some of the function fields used in Section 6.2.4, it seems to be that the empirical probability for a reduced ideal having maximal degree equals the predicted one up to an error term of $\mathcal{O}(q^{-g/2})$, which implies that a vast majority of the reduced ideals have degree $g + \deg \mathfrak{p}_{n+1} - 1$ in these cases. Hence, the strategy described at the end of Section 6.5.1 seems to be pretty efficient under this assumption. Moreover, note that one can use a similar strategy to speed up the baby stock computations in the Buchmann-Schmidt algorithm applied to the infrastructure of a function field (see Section 6.2.2).

As mentioned in the introduction, understanding the principal ideal infrastructure $\operatorname{Rep}^f(\mathcal{O}) \cong \mathbb{G}^n/\Lambda$, i.e. knowing a basis for Λ, allows to do comparisons in $\operatorname{Pic}(\mathcal{O})$. If we want to know whether $\mathfrak{a}$ and $\mathfrak{b}$ lie in the same ideal class, i.e. if there exists an $f \in K^*$ such that $\mathfrak{a} = f\mathfrak{b}$, it suffices to test

[1] Translation: *"Indeed, the search for the admissible minima in $\mathcal{B}$ seems to be the main problem of our method. We are able to give an $\mathcal{O}(D^{\varepsilon})$-algorithm to solve this problem, but in practice, it is very time-consuming"*

whether $\mathfrak{a}\mathfrak{b}^{-1}$ is a principal ideal $f\mathcal{O}$, $f \in K^*$. To test for that, find a minimum $\mu \in \mathcal{E}(\mathfrak{a}\mathfrak{b}^{-1})$ and compute $\mathfrak{c} := \frac{1}{\mu}\mathfrak{a}\mathfrak{b}^{-1}$; then $\mathfrak{c} \in \mathrm{Red}^{(b)}(K)$. Hence, $\mathfrak{a}\,\mathrm{PId}(\mathcal{O}) = \mathfrak{b}\,\mathrm{PId}(\mathcal{O})$ is equivalent to $\mathfrak{c} \in \mathrm{Red}^{(b)}(\mathcal{O})$.

Now, if we know a basis $b_1, \ldots, b_n$ of Λ, we can use the baby step-giant step strategy as described in Algorithms 6.4.11 and 6.5.5 to compare $\mathfrak{c}$ to all reduced ideals in $\mathrm{Red}^{(b)}(\mathcal{O})$ in $\mathcal{O}(\sqrt{R})$ steps. In the number field case, Buchmann showed in [Buc87c, p. 10, Satz 3.4] that, assuming that the representation of $\mathfrak{a}\mathfrak{b}^{-1}$ requires B bits, the number of bit operations required to test whether $\mathfrak{a}\mathfrak{b}^{-1}$ is principal is $\mathcal{O}(D^{\varepsilon}(\sqrt{R} + B))$.

Finally, we want to note that there exist subexponential algorithms which solve some of these problems. The first algorithm is the one by Buchmann [Buc90] which computes the structure of the class group $\mathrm{Pic}(\mathcal{O})$ of a number field K together with the regulator. Unfortunately, this algorithm does not compute a basis of Λ but just its determinant, which equals the regulator up to a scaling factor. An extension of this algorithm is explained in terms of the Arakelov divisor class group in [Sch08]; that version also allows the computation of a basis of Λ.

In the function field case, there also exist subexponential algorithms for computing a basis of Λ. In his doctoral thesis [Hes99], F. Heß presented a subexponential algorithm for computing the structure of the divisor class group of a function field K with at least one place of degree one. Assuming that the structure is computed, one can use the algorithm to write elements of $\mathrm{Pic}^0(K)$ in terms of a basis. Hence, if one considers the residue classes of $\frac{\deg \mathfrak{p}_i}{\gcd(\deg \mathfrak{p}_i, \deg \mathfrak{p}_{n+1})}\mathfrak{p}_{n+1} - \frac{\deg \mathfrak{p}_{n+1}}{\gcd(\deg \mathfrak{p}_i, \deg \mathfrak{p}_{n+1})}\mathfrak{p}_i$, $1 \leq i \leq n$ in $\mathrm{Pic}^0(K)$ and computes a representation in terms of a basis of $\mathrm{Pic}^0(K)$, one can determine the relation lattice and, hence, Λ. This is, for example, sketched in [Hes99, p. 90, Section 6.3] and [Hes], and is implemented in MAGMA. Note that the expected running time is $\mathcal{O}(\exp(\sqrt{2 \cdot (2g \log p) \cdot \log(2g \log p)}))$ for $g \to \infty$; if g is fixed and small, say $g \in \{1, 2, 3\}$, the running time becomes exponential, whence baby step-giant step algorithms are competitive in such cases.

Bibliography

[AO82] H. Appelgate and H. Onishi. Periodic expansion of modules and its relation to units. *J. Number Theory*, 15(3):283–294, 1982.

[Art06] E. Artin. *Algebraic numbers and algebraic functions*. AMS Chelsea Publishing, Providence, RI, 2006. Reprint of the 1967 original.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3–4):235–265, 1997. Computational algebra and number theory (London, 1993).

[Ber63] G. Bergmann. Theorie der Netze. *Mathematische Annalen*, 149:361–418, 1963.

[BS05] J. A. Buchmann and A. Schmidt. Computing the structure of a finite abelian group. *Math. Comp.*, 74(252):2017–2026 (electronic), 2005.

[Buc85a] J. A. Buchmann. A generalization of Voronoĭ's unit algorithm. I. *J. Number Theory*, 20(2):177–191, 1985.

[Buc85b] J. A. Buchmann. A generalization of Voronoĭ's unit algorithm. II. *J. Number Theory*, 20(2):192–209, 1985.

[Buc87a] J. A. Buchmann. On the computation of units and class numbers by a generalization of Lagrange's algorithm. *J. Number Theory*, 26(1):8–30, 1987.

[Buc87b] J. A. Buchmann. On the period length of the generalized Lagrange algorithm. *J. Number Theory*, 26(1):31–37, 1987.

[Buc87c] J. A. Buchmann. Zur Komplexität der Berechnung von Einheiten und Klassenzahl algebraischer Zahlkörper. Habilitationsschrift, October 1987.

[Buc90] J. A. Buchmann. A subexponential algorithm for the determination of class groups and regulators of algebraic number fields. In C. Goldstein, editor, *Séminaire de Théorie des Nombres, Paris 1988–1989*, volume 91 of *Progr. Math.*, pages 27–41, Boston, MA, 1990. Birkhäuser Boston.

[Buc91] J. A. Buchmann. Number theoretic algorithms and cryptology. In *FCT '91: Proceedings of the 8th International Symposium on Fundamentals of Computation Theory*, pages 16–21, London, UK, 1991. Springer-Verlag.

[BV06] Johannes Buchmann and Ulrich Vollmer. A Terr algorithm for computations in the infrastructure of real-quadratic number fields. *J. Théor. Nombres Bordeaux*, 18(3):559–572, 2006.

[BW88a] J. A. Buchmann and H. C. Williams. A key-exchange system based on imaginary quadratic fields. *J. Cryptology*, 1(2):107–118, 1988.

[BW88b] J. A. Buchmann and H. C. Williams. On the infrastructure of the principal ideal class of an algebraic number field of unit rank one. *Math. Comp.*, 50(182):569–579, 1988.

[BW90] J. A. Buchmann and H. C. Williams. A key exchange system based on real quadratic fields (extended abstract). In *Advances in cryptology—CRYPTO '89 (Santa Barbara, CA, 1989)*, volume 435 of *Lecture Notes in Comput. Sci.*, pages 335–343. Springer, New York, 1990.

[Can87] D. G. Cantor. Computing in the Jacobian of a hyperelliptic curve. *Math. Comp.*, 48(177):95–101, 1987.

[Deu73] M. Deuring. *Lectures on the theory of algebraic functions of one variable*. Springer-Verlag, Berlin, 1973. Lecture Notes in Mathematics, Vol. 314.

[DF64] B. N. Delone and D. K. Faddeev. *The theory of irrationalities of the third degree*. Translations of Mathematical Monographs, Vol. 10. American Mathematical Society, Providence, R.I., 1964.

[FL05] G. Frey and T. Lange. Mathematical background of public key cryptography. In *Arithmetic, geometry and coding theory (AGCT 2003)*, volume 11 of *Sémin. Congr.*, pages 41–73. Soc. Math. France, Paris, 2005.

[Fon08] F. Fontein. Groups from cyclic infrastructures and Pohlig-Hellman in certain infrastructures. *Adv. Math. Commun.*, 2(3):293–307, August 2008.

[Fon09] F. Fontein. The infrastructure of a global field of arbitrary unit rank, 2009. In preparation; preprint available at `http://arxiv.org/abs/0809.1685`.

[Fre01] G. Frey. Applications of arithmetical geometry to cryptographic constructions. In *Finite fields and applications (Augsburg, 1999)*, pages 128–161. Springer, Berlin, 2001.

[GHMM08] S. D. Galbraith, M. Harrison, and D. J. Mireles Morales. Efficient hyperelliptic arithmetic using balanced representation for divisors. In A. J. van der Poorten and A. Stein, editors, *Algorithmic Number Theory, 8th International Symposium, ANTS-VIII, Banff, Canada, May 17-22, 2008*, volume 5011 of *Lecture Notes in Computer Science*, pages 342–356, Berlin, 2008. Springer.

[Gol03] D. M. Goldschmidt. *Algebraic functions and projective curves*, volume 215 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2003.

[Gop88] V. D. Goppa. *Geometry and codes*, volume 24 of *Mathematics and its Applications (Soviet Series)*. Kluwer Academic Publishers Group, Dordrecht, 1988. Translated from the Russian by N. G. Shartse.

[GPS02] S. D. Galbraith, S. M. Paulus, and N. P. Smart. Arithmetic on superelliptic curves. *Math. Comp.*, 71(237):393–405 (electronic), 2002.

[Hes] F. Hess. Computing relations in divisor class groups of algebraic curves over finite fields. Submitted to J. Symbolic Comp.; available at `http://www.math.tu-berlin.de/~hess/`.

[Hes99] F. Hess. *Zur Divisorklassengruppenberechnung in globalen Funktionenkörpern.* Ph.D. thesis, Technische Universität Berlin, 1999.

[Hes02] F. Hess. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symbolic Comput.*, 33(4):425–445, 2002.

[HMPLR87] Y. Hellegouarch, D. L. McQuillan, and R. Paysant-Le Roux. Unités de certains sous-anneaux des corps de fonctions algébriques. *Acta Arith.*, 48(1):9–47, 1987.

[HP01] D. Hühnlein and S. M. Paulus. On the implementation of cryptosystems based on real quadratic number fields (extended abstract). In *Selected areas in cryptography (Waterloo, ON, 2000)*, volume 2012 of *Lecture Notes in Comput. Sci.*, pages 288–302. Springer, Berlin, 2001.

[HPLR85] Y. Hellegouarch and R. Paysant-Le Roux. Commas, points extrémaux et arêtes des corps possédant une formule du produit. *C. R. Math. Rep. Acad. Sci. Canada*, 7(5):291–296, 1985.

[HPLR87] Y. Hellegouarch and R. Paysant-Le Roux. Invariants arithmétiques des corps possédant une formule du produit; applications. *Astérisque*, (147-148):291–300, 345, 1987. Journées arithmétiques de Besançon (Besançon, 1985).

[JSS07] M. J. Jacobson, Jr., R. Scheidler, and A. Stein. Cryptographic protocols on real hyperelliptic curves. *Adv. Math. Commun.*, 1(2):197–221, 2007.

[JSW01] M. J. Jacobson, Jr., R. Scheidler, and H. C. Williams. The efficiency and security of a real quadratic field based key exchange protocol. In *Public-key cryptography and computational number theory (Warsaw, 2000)*, pages 89–112. de Gruyter, Berlin, 2001.

[JSW06] M. J. Jacobson, Jr., R. Scheidler, and H. C. Williams. An improved real-quadratic-field-based key exchange procedure. *Journal of Cryptology*, 19(2):211–239, 2006.

[KM04] K. Khuri-Makdisi. Linear algebra algorithms for divisors on an algebraic curve. *Math. Comp.*, 73(245):333–357 (electronic), 2004.

[KM07] K. Khuri-Makdisi. Asymptotically fast group operations on Jacobians of general curves. *Math. Comp.*, 76(260):2213–2239 (electronic), 2007.

[Kob87] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177):203–209, 1987.

[Len82] H. W. Lenstra. On the computation of regulators and class numbers of quadratic fields. In J. V. Armitage, editor, *Journées Arithmétiques 1980 (Exeter, 13th–19th April 1980)*, number 56 in London Mathematical Society Lecture Notes, pages 123–150, Cambridge, 1982. Cambridge University Press.

[Lor96] D. Lorenzini. *An invitation to arithmetic geometry*, volume 9 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1996.

[LSY03] Y. Lee, R. Scheidler, and C. Yarrish. Computation of the fundamental units and the regulator of a cyclic cubic function field. *Experiment. Math.*, 12(2):211–225, 2003.

[Mah41] K. Mahler. An analogue to Minkowski's geometry of numbers in a field of series. *Ann. of Math. (2)*, 42:488–522, 1941.

[Mau00] M. Maurer. *Regulator approximation and fundamental unit computation for real-quadratic orders*. Ph.D. thesis, Technische Universität Darmstadt, 2000.

[Mil86] V. S. Miller. Use of elliptic curves in cryptography. In *Advances in cryptology—CRYPTO '85 (Santa Barbara, Calif., 1985)*, volume 218 of *Lecture Notes in Comput. Sci.*, pages 417–426. Springer, Berlin, 1986.

[Min68] H. Minkowski. *Geometrie der Zahlen*. Bibliotheca Mathematica Teubneriana, Band 40. Johnson Reprint Corp., New York, 1968.

[MVZ98] V. Müller, S. Vanstone, and R. Zuccherato. Discrete logarithm based cryptosystems in quadratic function fields of characteristic 2. *Des. Codes Cryptogr.*, 14(2):159–178, 1998.

[Neu99] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag,

Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Pau98] S. M. Paulus. Lattice basis reduction in function fields. In *Algorithmic number theory (Portland, OR, 1998)*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 567–575, Berlin, 1998. Springer.

[PH78] S. C. Pohlig and M. E. Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. *IEEE Trans. Information Theory*, IT-24(1):106–110, 1978.

[PLRMH85] R. Paysant-Le Roux, D. L. McQuillan, and Y. Hellegouarch. Unités de certains sous-anneaux de corps de fonctions algébriques. *C. R. Math. Rep. Acad. Sci. Canada*, 7(1):91–96, 1985.

[PR99] S. M. Paulus and H.-G. Rück. Real and imaginary quadratic representations of hyperelliptic function fields. *Math. Comp.*, 68(227):1233–1241, 1999.

[PWZ82] M. Pohst, P. Weiler, and H. Zassenhaus. On effective computation of fundamental units. II. *Math. Comp.*, 38(157):293–329, 1982.

[PZ77] M. Pohst and H. Zassenhaus. An effective number geometric method of computing the fundamental units of an algebraic number field. *Math. Comp.*, 31(139):754–770, 1977.

[PZ82] M. Pohst and H. Zassenhaus. On effective computation of fundamental units. I. *Math. Comp.*, 38(157):275–291, 1982.

[Ros02] M. Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[SBW94] R. Scheidler, J. A. Buchmann, and H. C. Williams. A key-exchange protocol using real quadratic fields. *J. Cryptology*, 7(3):171–199, 1994.

[Sch82] R. J. Schoof. Quadratic fields and factorization. In *Computational methods in number theory, Part II*, volume 155 of *Math. Centre Tracts*, pages 235–286. Math. Centrum, Amsterdam, 1982.

[Sch01] R. Scheidler. Ideal arithmetic and infrastructure in purely cubic function fields. *J. Théor. Nombres Bordeaux*, 13(2):609–631, 2001.

[Sch08] R. J. Schoof. *Computing Arakelov class groups*, volume 44 of *MSRI Publications*, pages 447–495. Cambridge University Press, Cambridge, 2008.

[Sha71] D. Shanks. Class number, a theory of factorization, and genera. In D. J. Lewis, editor, *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*, pages 415–440, Providence, R.I., 1971. Amer. Math. Soc.

[Sha72] D. Shanks. The infrastructure of a real quadratic field and its applications. In *Proceedings of the Number Theory Conference (Univ. Colorado, Boulder, Colo., 1972)*, pages 217–224, Boulder, Colo., 1972. Univ. Colorado.

[Sho97] V. Shoup. Lower bounds for discrete logarithms and related problems. In W. Fumy, editor, *Advances in cryptology—EUROCRYPT '97 (Konstanz)*, volume 1233 of *Lecture Notes in Comput. Sci.*, pages 256–266, Berlin, 1997. Springer.

[SS98] R. Scheidler and A. Stein. Unit computation in purely cubic function fields of unit rank 1. In *Algorithmic number theory (Portland, OR, 1998)*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 592–606, Berlin, 1998. Springer.

[SSW96] R. Scheidler, A. Stein, and H. C. Williams. Key-exchange in real quadratic congruence function fields. *Des. Codes Cryptogr.*, 7(1-2):153–174, 1996. Special issue dedicated to Gustavus J. Simmons.

[ST05] A. Stein and E. Teske. Optimized baby step–giant step methods. *J. Ramanujan Math. Soc.*, 20(1):27–58, 2005.

[Ste77] R. Steiner. On the units in algebraic number fields. In *Proceedings of the Sixth Manitoba Conference on Numerical Mathematics (Univ. Manitoba, Winnipeg, Man., 1976)*, Congress. Numer., XVIII, pages 413–435, Winnipeg, Man., 1977. Utilitas Math.

[Ste92] A. Stein. Baby step-giant step-Verfahren in reellquadratischen Kongruenzfunktionenkörpern mit Charakteristik ungleich 2. Diplomarbeit, Universität des Saarlandes, Saarbrücken, 1992.

[Ste97] A. Stein. Equivalences between elliptic curves and real quadratic congruence function fields. *J. Théor. Nombres Bordeaux*, 9(1):75–95, 1997.

[Sti93] H. Stichtenoth. *Algebraic function fields and codes*. Universitext. Springer-Verlag, Berlin, 1993.

[SW98] A. Stein and H. C. Williams. An improved method of computing the regulator of a real quadratic function field. In *Algorithmic number theory (Portland, OR, 1998)*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 607–620. Springer, Berlin, 1998.

[SW99] A. Stein and H. C. Williams. Some methods for evaluating the regulator of a real quadratic function field. *Experiment. Math.*, 8(2):119–133, 1999.

[SZ91] A. Stein and H. G. Zimmer. An algorithm for determining the regulator and the fundamental unit of hyperelliptic congruence function field. In *Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation, ISSAC '91, Bonn, Germany, July 15-17, 1991*, pages 183–184. Association for Computing Machinery, 1991.

[Ter00] D. C. Terr. A modification of Shanks' baby-step giant-step algorithm. *Math. Comp.*, 69(230):767–773, 2000.

[Tes98] E. Teske. A space efficient algorithm for group structure computation. *Math. Comp.*, 67(224):1637–1663, 1998.

[Tes99] E. Teske. The Pohlig-Hellman method generalized for group structure computation. *J. Symbolic Comput.*, 27(6):521–534, 1999.

[Tes01] E. Teske. Square-root algorithms for the discrete logarithm problem (a survey). In *Public-key cryptography and computational number theory (Warsaw, 2000)*, pages 283–301. de Gruyter, Berlin, 2001.

[Thi95] C. Thiel. Short proofs using compact representations of algebraic integers. *J. Complexity*, 11(3):310–329, 1995.

[WDS83] H. C. Williams, G. W. Dueck, and B. K. Schmid. A rapid method of evaluating the regulator and class number of a pure cubic field. *Math. Comp.*, 41(163):235–286, 1983.

[Wil85] H. C. Williams. Continued fractions and number-theoretic computations. *Rocky Mountain J. Math.*, 15(2):621–655, 1985. Number theory (Winnipeg, Man., 1983).

List of Figures

6.1 Relative running times of the various algorithms for different global function fields. 101
6.2 Absolute running times and regulators for Cubic Field #1. . 102
6.3 Absolute running times and regulators for Cubic Field #2. . 102
6.4 Absolute running times and regulators for Cubic Field #3. . 103
6.5 Absolute running times and regulators for Quartic Field #1. 103
6.6 Absolute running times and regulators for Quartic Field #2. 104

Index

absolute distance, 19
absolute space, 31

baby step, 16, 49
    computation, 83
baby step shape, 48
baby step-giant step method, 24, 89, 94, 118, 121, 127
baby stock, 24, 119, 122
boundary units, 113
box, 32
Buchmann's baby step method, 114

comma, 32
compression, 106
cycle of minima, 113

Diffie-Hellman Problem, 22
discrete logarithm, 16
Discrete Logarithm Problem, 22
distance, 15, 19
DLP, *see* Discrete Logarithm Problem

edge, 32
equivalent ideals, 55
expansion, 106
extremal point, 32

f-representation, 19, 61
fundamental units, 91

Generalized Lagrange algorithm, 112
giant step, 17
    computation, 80

ideal representation, 51, 54
infrastructure
    cyclic, 15
    discrete, 16, 73
    n-dimensional, 26, 27
    of a global field, 64
    one-dimensional, 15

key exchange, 21

minimal set, 105
minimum, 32

neighbor, 36

$\mathfrak{p}$-order, 47
    universal, 47
Pohlig-Hellman method, 23

rectangular set, 48
reduced ideal, 53
reduction, 62
relative distance, 20
Riemann's Inequality, 30
Riemann-Roch, 30

scale invariant preorder, 51
symmetric set, 48

Voronoĭ's algorithm, 93