Lattices over polynomial Rings and Applications to Function Fields

a Ph. D. dissertation to obtain the degree of
Doctor in Mathematics
presented by

Jens-Dietrich Bauch

Supervised by Professor Dr.

Enric Nart

Departament de Matemàtiques
Universitat Autònoma de Barcelona

UAB

May 2014

Memòria presentada per aspirar al grau de Doctor en Matemàtiques,

Jens-Dietrich Bauch
Aspirant

Certifico que la present memòria ha estat realitzada per Jens-Dietrich Bauch, sota la meva direcció.

Prof. Dr. Enric Nart
Director de tesi

Bellaterra, 14 de maig de 2014.

Abstract

This thesis deals with lattices over polynomial rings and its applications to algebraic function fields. In the first part, we consider the notion of lattices $(L, \| \ \|)$ over polynomial rings, where L is a finitely generated module over $k[t]$, the polynomial ring over the field k in the indeterminate t, and $\| \ \|$ is a real-valued length function on $L \otimes_{k[t]} k(t)$. A reduced basis of $(L, \| \ \|)$ is a basis of L whose vectors attain the successive minima of $(L, \| \ \|)$. We develop an algorithm which transforms any basis of L into a reduced basis of $(L, \| \ \|)$, for a given real-valued length function $\| \ \|$. Moreover, we generalize the Riemann-Roch theory for algebraic function fields to the context of lattices over $k[t]$. In the second part, we apply the previous results to algebraic function fields. For a divisor D of an algebraic function field F/k, we develop an algorithm for the computation of its Riemann-Roch space and the successive minima attached to the lattice $(I, \| \ \|_D)$, where I is a fractional ideal (obtained from the ideal representation of D) of the finite maximal order $\mathcal{O}_F$ of F and $\| \ \|_D$ is a certain length function on F. Let k_0 be the full constant field of F/k. Then, we can express the genus g of F in terms of $[k_0 : k]$ and the indices of certain orders of the finite and infinite maximal orders of F. If k is a finite field, the Montes algorithm computes the latter indices as a by-product. This leads us to a fast computation of the genus of global function fields. Our algorithm does not require the computation of any basis, neither of the finite nor the infinite maximal order. The concept of reduceness and the OM representations of prime ideals lead us in that context to a new method for the computation of $k[t]$-bases of fractional ideals of $\mathcal{O}_F$ and $k[t^{-1}]_{(t^{-1})}$-bases of fractional ideals of the infinite maximal order of F, respectively. In the last part, our algorithms are applied to a large number of relevant examples to illustrate its performance in comparison with the classical routines.

A María ....

Acknowledgements

This work would not have been possible without the support and advice of Enric Nart. His openness to all mathematical problems, and continual quest for correct formulation served as a model for my mathematical development.

Quiero agradecer a mi novia María por su apoyo y, sobre todo, por su paciencia y comprensión en los últimos años.

Ich möchte mich bei allen bedanken, die mir diese Arbeit ermöglicht haben: Ein ganz besonderer Dank geht an meine Eltern, die mir das Studium der Mathematik ermöglichten und mir auch während der Anfertigung der Doktorarbeit immerzu unterstützend und liebevoll zur Seite standen. Ganz besonderen Dank dafür, dass Sie immer das Beste für meine Geschwister und mich tun und alles Erdenkliche bereit sind, dafür zu geben.

Ganz großer Dank geht an meine Schwestern Kirstin und Kristina. Ihre Freundschaft bedeutet mir unbeschreiblich viel. Herzlichen Dank für jedwede Unterstützung und den großen Beistand, den sie jederzeit zu geben bereit sind.

Allen meinen lieben Freunden danke ich für die Ausdauer, Ruhe und Geduld, womit sie mir stets zur Seite standen und mich immer wieder aufgemuntert haben. Y, por último, muchas gracias a mis amigos de España.

Con el soporte económico del Programa FPU del Ministerio de Educación, del proyecto MTM2009-10359.

Contents

Introduction

This document is ostensibly concerned with lattices over polynomial rings and its applications to algebraic function fields.

An algebraic function field over an arbitrary field k is a finite algebraic extension over the rational function field $k(t)$ in the indeterminate t. The theory of algebraic function fields occurs in various branches of mathematics such as for instance algebraic geometry and number theory.

The theory of algebraic function fields was initially developed by Dedekind, Kronecker, and Weber in the 19^{th} century. Along the 20^{th} century, this approach was further developed by various mathematicians like Artin, Hasse, Schmidt and Weil. Nowadays it is a key ingredient in interdisciplinary fields like computer algebra, cryptography and coding theory.

In that context, the fast computation of basic objects in algebraic function fields (like the genus or the Riemann-Roch space of a divisor) by computer algebra systems like Magma, Sage, Singular, and Pari play a significant role.

In algebraic number fields, many computational issues are tackled by the theory of lattices over the integers. In the context of algebraic function fields this role is played by lattices over $k[t]$, the polynomial ring over k in the indeterminate t. In 1941 K. Mahler [21] laid the foundation for the theory of lattices over $k[t]$. In the second half of the 20^{th} century the concept of lattices over polynomial rings became an important tool for the basic arithmetic in function fields [30, 31] and the factorization of bivariate polynomials over finite fields [18].

In 1999 J. Montes [23] developed a new computational representation, the so-called OM representation, of prime ideals in Dedekind domains, which is heavily intertwined with the work of MacLane [20] and Okutsu [28]. This lead to a new computational approach to ideal theory in fields of fractions of Dedekind domains [9].

INTRODUCTION

By representing a function field by

$$F = k(t, \theta), \quad \text{with } f(t, \theta) = 0,$$

where $f(t, x) \in k[t, x]$ is monic an separable in x, the results of Montes, MacLane, and Okutsu become available for algebraic function fields. This allows a fundamental modification of the handling of algebraic function fields from an algorithmically perspective, which is in many cases superior to the classical and common methods [5, 6].

Along this memoir a Magma package has been developed, which provides the above mentioned OM representation of prime ideals in the context of algebraic function fields over finite fields and several subsequent algorithms. The reader may download the file from www.mat.uab.cat/∼bauch/resources/Dateien/GlobalFF.m.

The exposition is roughly divided into the theory of lattices over polynomial rings and its applications to algebraic function fields.

In the first chapter we introduce the theoretical and algorithmic background of algebraic function fields and present in that context the Montes algorithm and the OM representations of prime ideals as well as some of their applications.

The second chapter is the core of this thesis. We introduce the theory of real-valued lattices over polynomial rings and consider specific bases generating them; the so-called reduced bases. These bases play a fundamental role; for instance, the lengths of the vectors of a reduced basis $\mathcal{B}$ attain the successive minima of the lattice spanned by $\mathcal{B}$. Analogously to the theory of lattices over $\mathbb{Z}$, we define the determinant of a lattice and the orthogonal defect of a basis. This leads to a reduceness criterion for a set of vectors in a lattice and a reduction algorithm; that is, an algorithm, which transform any basis of a lattice into a reduced one. Afterwards we analyze the complexity of the reduction algorithm. We end the chapter by considering classes of lattices and the concept of weakly-reduceness (semi-reduceness), which allows us to accelerate the reduction algorithm.

In the third chapter we consider the Riemann-Roch theory on abstract lattices. We generalize to this abstract context the concept of a divisor and some other invariants

in algebraic function fields.

In the fourth chapter we apply the results of the previous chapters in the context of algebraic function fields. This leads to an algorithm for the computation of Riemann-Roch spaces. Moreover, the theory of lattices allows us to derive a formula for the genus g of a function fields, which afford a fast computation of g by the Montes algorithm.

Later, we present a method for the computation of the successive minima of a divisor which only applies techniques from linear algebra. Our algorithm does not require the computation of Puiseux series and can be applied for arbitrary function fields. We give a detailed complexity analysis of all the mentioned methods.

In the fifth chapter we generalize the concept of reduceness in the context of algebraic function fields. Using OM representations of prime ideals we deduce a new method for the computation of bases of fractional ideals in function fields. Moreover, the generalization of the ideas of Chapter 4 allows us to derive an algorithm for the computation of bases of certain holomorphic rings.

In the sixth chapter we present the practical performance of the presented routines for global function fields; that is, function fields over $\mathbb{F}_q$, the finite field with q elements. We show the running times of the mentioned algorithms by considering concrete function fields, which vary in g and q.

1. Fundamentals

1.1 Algebraic function fields

Let k be a field and denote by

$$A := k[t], \qquad K := k(t),$$

the polynomial ring and the rational function field in the indeterminate t over k, respectively. Let v_∞ be the discrete valuation on K defined by: For any rational function $x = a/b \in K$, where $a, b \in A$ are polynomials and $b \neq 0$,

$$v_\infty(x) = \begin{cases} \deg b - \deg a, & \text{if } x \neq 0, \\ \infty, & \text{if } x = 0. \end{cases}$$

Denote by $A_\infty := k[t^{-1}]_{(t^{-1})} \subset K$ the valuation ring of v_∞, and by $\mathfrak{m}_\infty$ its maximal ideal. By $U_\infty := \{a \in K \mid v_\infty(a) = 0\}$ we denote the group of units of A_∞. On K we may consider the *length function* determined by the degree; that is $|\ | := -v_\infty$. We call this length function the *degree function* on K, because $|h| = \deg h$, for $h \in A$.

Every monic and irreducible polynomial $p(t) \in A$ determines a discrete valuation $v_p : K \to \mathbb{Z} \cup \{\infty\}$ in the usual way, and induces a *place* $P_p := \{a \in K \mid v_p(a) > 0\}$ of the rational function field K/k, with residue class field $k_p := A/(p(t))$. We define the unique place at infinity of K by $P_\infty := \{a \in K \mid v_\infty(a) > 0\}$.

From now on F/k will denote an *algebraic function field* of one variable over the *constant field* k. That is, $F/k(t)$ is a separable extension of finite degree n, for $t \in F$ transcendental over k. We define *the full constant field* k_0 of F/k to be the algebraic closure of k in F.

A *place* of F/k is defined to be the maximal ideal of a valuation ring $\mathcal{O}$ of F/k. Denote by $\mathbb{P}_F$ the set of all places of F/k and let $\mathbb{P}_\infty(F) \subset \mathbb{P}_F$ be the set of all places over P_∞. We define $\mathbb{P}_0(F) := \mathbb{P}_F \setminus \mathbb{P}_\infty(F)$. Every place $P \in \mathbb{P}_F$ corresponds to a

surjective valuation $v_P : F \to \mathbb{Z} \cup \{\infty\}$, which vanishes on k. The valuation ring of P is $\mathcal{O}_P := \{z \in F \mid v_P(z) \geq 0\}$ and its *residue class field* is given by $F_P := \mathcal{O}_P/P$.

For a place P of F/k lying over P_p we write $P|P_p$ and denote its *ramification index* by $e(P/P_p)$. If $P \in \mathbb{P}_\infty(F)$ we write $P|P_\infty$ and $e(P/P_\infty)$, accordingly. The residue class field F_P of a place P is a finite extension of k_p and therefore a finite extension of k. The *degree* of P (over k) is defined to be the integer $\deg P := [F_P : k]$ and the *residual degree* of P over P_p is $\deg_{k_p} P := [F_P : k_p]$. For a place $P \in \mathbb{P}_\infty(F)$ the degree and the *residual degree* of $P|P_\infty$ coincide.

A *divisor* D of F/k is a formal (finite) $\mathbb{Z}$-linear combination of the places of F. The set of all divisors $\mathcal{D}_F$ of F/k is an abelian group which is called the *divisor group* of F/k. For a divisor $D = \sum_{P \in \mathbb{P}_F} a_P P$, we set $v_P(D) := a_P$ and define the *degree* of D (over k) by the integer

$$\deg D := \sum_{P \in \mathbb{P}_F} a_P \deg P.$$

The support of D is the set $\operatorname{supp}(D) := \{P \in \mathbb{P}_F \mid v_P(D) \neq 0\}$. A partial ordering on $\mathcal{D}_F$ is defined by: $D_1 \leq D_2$ if and only if $v_P(D_1) \leq v_P(D_2)$, for all $P \in \mathbb{P}_F$. We call $D \in \mathcal{D}_F$ effective if $D \geq 0$; that is, if all coefficients are nonnegative. Every $z \in F^*$ determines a *principal divisor* $(z) := \sum_{P \in \mathbb{P}_F} v_P(z)P$. Principal divisors have degree zero. Denote by

$$Z_z := \{P \in \mathbb{P}_F \mid v_P(z) > 0\}, \quad N_z := \{P \in \mathbb{P}_F \mid v_P(z) < 0\}$$

the sets of *zeros* and *poles* of z, respectively. These sets are finite and we call $(z)_0 := \sum_{P \in Z_z} v_P(z)P$ the *zero divisor* of z and $(z)_\infty := \sum_{P \in N_z} -v_P(z)P$ the *pole divisor* of z.

The *Riemann-Roch space* of a divisor D of F is the finite dimensional k-vector space

$$\mathcal{L}(D) := \{a \in F^* \mid (a) \geq -D\} \cup \{0\}.$$

Instead of $\dim_k \mathcal{L}(D)$, we write $\dim_k D$. Then, we may define the *genus* g of F as

$$g := \max\{\deg D - \dim_k D + 1 \mid D \in \mathcal{D}_F\}.$$

Let $\mathcal{O}_F := \operatorname{Cl}(A, F)$ and $\mathcal{O}_{F,\infty} := \operatorname{Cl}(A_\infty, F)$ be the integral closures of A and A_∞ in F, respectively. We may realize an algebraic function field F/k as the quotient field of the residue class ring $A[x]/(f(t,x))$, where

$$f(t,x) = x^n + a_1(t)x^{n-1} + \cdots + a_n(t) \in A[x]$$

is irreducible, monic and separable in x. A polynomial f satisfying these conditions is called a *defining polynomial* of F/k. Such a representation exists for every algebraic function field over a perfect constant field [33, p. 128]. We consider $\theta \in F$ with $f(t,\theta) = 0$, so that F can be expressed as $k(t,\theta)$. We call $A[\theta]$ the *finite equation order* of f, and we define

$$C_f := \max\{\lceil \deg a_i(t)/i \rceil \mid 1 \leq i \leq n\}, \quad f_\infty(t^{-1}, x) := t^{-nC_f} f(t, t^{C_f} x).$$

Then, f_∞ belongs to $k[t^{-1}, x] \subset A_\infty[x]$ and the quotient field of the residue class ring $A_\infty[x]/(f_\infty(t^{-1}, x))$ becomes a realization of the function field F/k. Clearly, $\theta_\infty := \theta/t^{C_f}$ is a root of f_∞. As θ_∞ is integral over A_∞, we may consider the *infinite equation order* $A_\infty[\theta_\infty]$.

Any element $a \in F$ yields a K-linear map $\mu_a : F \to F$, defined by $\mu_a(z) := a \cdot z$. We define the *norm* and the *trace* with respect to the extension F/K by

$$N_{F/K}(a) := \det \mu_a, \quad \mathrm{Tr}_{F/K}(a) := \mathrm{Trace}(\mu_a),$$

respectively.

1.2 Ideals in function fields

The rings $\mathcal{O}_F$ and $\mathcal{O}_{F,\infty}$ are Dedekind domains. Hence, any nonzero fractional ideal of $\mathcal{O}_F$ or $\mathcal{O}_{F,\infty}$ has an unique decomposition into a product of nonzero prime ideals.

Any nonzero prime ideal in A is principal and generated by a monic irreducible polynomial $p(t) \in A$. Then, $p(t)\mathcal{O}_F = \prod_{\mathfrak{p}|p} \mathfrak{p}^{e(\mathfrak{p}/p)}$, for some nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}_F$. If $\mathfrak{p}|p$, we say that $\mathfrak{p}$ lies over $p(t)$. Then, we call $e(\mathfrak{p}/p)$ the *ramification index* of $\mathfrak{p}$ over $p(t)$, and we define the *residual degree* of $\mathfrak{p}$ over $p(t)$ by $f(\mathfrak{p}/p) := [\mathcal{O}_F/\mathfrak{p} : A/(p(t))]$.

The only prime ideal in A_∞ is $\mathfrak{m}_\infty$, which is generated by t^{-1}. It holds $t^{-1}\mathcal{O}_{F,\infty} = \prod_{\mathfrak{p}|\mathfrak{m}_\infty} \mathfrak{p}^{e(\mathfrak{p}/\mathfrak{m}_\infty)}$, for some nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}_{F,\infty}$. Again, we say that those $\mathfrak{p}$ lie over $\mathfrak{m}_\infty$, we define the ramification index of $\mathfrak{p}$ by $e(\mathfrak{p}/\mathfrak{m}_\infty)$, and the residual degree by $f(\mathfrak{p}/\mathfrak{m}_\infty) := [\mathcal{O}_{F,\infty}/\mathfrak{p} : A_\infty/\mathfrak{m}_\infty]$.

Any nonzero prime ideal $\mathfrak{p}$ of F, that is a nonzero prime ideal of $\mathcal{O}_F$ or $\mathcal{O}_{F,\infty}$, determines a discrete valuation $v_\mathfrak{p}$ on F, which vanishes on k. Therefore, the prime ideal $\mathfrak{p}$ corresponds uniquely to place of F. Every place of F is attached in this way to a prime ideal of F.

1.2.1 Indices of free modules

Let V be a K-vector space of dimension n. If $\mathcal{B} = (b_1, \dots, b_n)$ is a basis of V we denote by $c_{\mathcal{B}}$ the K-isomorphism

$$c_{\mathcal{B}} : V \to K^n,$$

mapping $x \in V$ to its coordinate vector with respect to the basis $\mathcal{B}$.

Definition 1.2.1. *Let $\mathcal{B} = (b_1, \dots, b_n)$ and $\mathcal{B}' = (b'_1, \dots, b'_n)$ be two bases of V. The* transition matrix *from $\mathcal{B}$ to $\mathcal{B}'$ is defined to be the unique matrix $T = T(\mathcal{B} \to \mathcal{B}') \in \mathrm{GL}_n(K)$ such that*

$$T(b'_1 \dots b'_n)^{\mathrm{tr}} = (b_1 \dots b_n)^{\mathrm{tr}}.$$

Thus, if $(a_1, \dots, a_n)$ are the coordinates of a vector u in V with respect to the basis $\mathcal{B}$, then $(a_1 \dots a_n)T$ is the coordinate vector of u with respect to the basis $\mathcal{B}'$.

For arbitrary bases $\mathcal{B}, \mathcal{B}', \mathcal{B}''$ of V we have

$$T(\mathcal{B} \to \mathcal{B}'') = T(\mathcal{B} \to \mathcal{B}')T(\mathcal{B}' \to \mathcal{B}'').$$

We may identify an $m \times n$ matrix with a K-linear map via the K-isomorphism

$$K^{m \times n} \to L(K^m, K^n), \quad M \mapsto [(a_1, \dots, a_m) \mapsto (a_1, \dots, a_m)M].$$

In this way, if $T = T(\mathcal{B} \to \mathcal{B}')$, the following diagram commutes:

$$\begin{array}{ccc} E & \xrightarrow{c_{\mathcal{B}}} & K^n \\ & \searrow^{c_{\mathcal{B}'}} & \downarrow T \\ & & K^n \end{array}$$

For $R \in \{A, A_\infty\}$, a basis of a free R-module M of finite rank can be considered as a basis of the finite dimensional K-vector space $M \otimes_R K$. Hence, for two R-modules of rank n with bases $\mathcal{B}$ and $\mathcal{B}'$ we can define a transition matrix from $\mathcal{B}$ to $\mathcal{B}'$, analogously.

Since R is a principal ideal domain, the set of fractional ideals of R is the set of all R-modules $I = hR$, for some $h \in K$. By $h_1R \cdot h_2R := (h_1h_2)R$, for $h_1, h_2 \in K$, the set I_R of nonzero fractional ideals becomes an abelian group, the *ideal group* of R, where R is the identity element.

Definition 1.2.2 (Index)**.** *Let M and M' be two free R-modules of rank n. The* index *$[M : M'] \in I_R$ is defined to be the nonzero fractional ideal generated by the determinant of the transition matrix from a basis of M' to a basis of M.*

If we change the R-bases of M and M', we change the determinant of the transition matrix by a factor in R^*, the unit group of R. Hence, the index $[M : M']$ is independent of the choice of the bases of M and M' and in particular well-defined.

For any monic and irreducible polynomial $p(t)$ in A, we can extend its induced valuation v_p to I_A by $v_p(hA) := v_p(h)$. Analogously, we set $v_\infty(hR) := v_\infty(h)$ in order to extend the valuation v_∞ to I_R. In particular, the degree function $|\ |$ can be defined for fractional ideals of R, as $|\ | = -v_\infty$.

We summarize some of the basic properties of the index of free modules of finite rank over principal ideal domains. Details can be found in [17, 32].

Lemma 1.2.3. *Let L, M, and N be free R-modules of rank n.*

1. $[L : N] = [L : M][M : N]$.
2. $[M : N] = [N : M]^{-1}$.
3. $[aM : aN] = [M : N]$, *for all* $a \in K^*$.
4. *If $N \subset M$, then $[M : N] = h_1 \cdots h_n R$, for certain $h_1, \ldots, h_n \in R$ such that*

$$M/N \cong R/h_1R \times \cdots \times R/h_nR, \qquad h_1 | \cdots | h_n.$$

   In particular, $[M : N]M \subseteq N$.

5. *If $N \subset M$, then $M = N$ if and only if $[M : N] = R$.*

Definition 1.2.4. *A matrix $M = (m_{i,j}) \in A^{n\times n} \cap \mathrm{GL}_n(K)$ is in (row-)* Hermite normal form *over A (HNF) if*

1. *M is a lower triangular matrix.*
2. *The diagonal entries are monic.*
3. *For all $1 \leq i < j \leq n$, $m_{j,i}$ belongs to a fixed subset of representatives of $A/m_{i,i}A$.*

Note that the third condition is equivalent to $m_{j,i} = 0$ or $0 \leq |m_{j,i}| < |m_{i,i}|$, for $1 \leq i < j \leq n$.

Definition 1.2.5. *A matrix $M = (m_{i,j}) \in A_\infty^{n\times n} \cap \mathrm{GL}_n(K)$ is in (row-)* Hermite normal form *over A_∞ (HNF) if*

1. *M is a lower triangular matrix.*

2. *The diagonal entries are t^{-1}-powers.*

3. *For all $1 \leq i < j \leq n$, $m_{j,i}$ belongs to a fixed subset of representatives of $A_\infty / m_{i,i} A_\infty$.*

Note that the third condition is equivalent to $m_{i,j} = 0$ or $0 \leq v_\infty(m_{j,i}) < v_\infty(m_{i,i})$, for $1 \leq i < j \leq n$. Moreover, the fixed subset of representatives can be chosen to lie in $k[t^{-1}]$. In that case M belongs to $k[t^{-1}]^{n \times n}$.

Any matrix $M \in R^{n \times n} \cap \mathrm{GL}_n(K)$ can be transformed into a unique matrix in HNF by elementary row operations in R. Details can be found in [29].

1.2.2 Bases of fractional ideals

Since F/k is a separable extension of degree n, any fractional ideal of $\mathcal{O}_F$ is a free A-module of rank n and any fractional ideal of $\mathcal{O}_{F,\infty}$ is a free A_∞-module of rank n [32]. Hence, the index is well-defined for fractional ideals. We consider again $R \in \{A, A_\infty\}$ and define

$$\mathcal{O}_R := \begin{cases} \mathcal{O}_F, & \text{if } R = A \\ \mathcal{O}_{F,\infty}, & \text{if } R = A_\infty. \end{cases}$$

We summarize some well-known properties of the index of fractional ideals of Dedekind domains. Details can be found in [17, 32].

Lemma 1.2.6. *For fractional ideals I, I' of $\mathcal{O}_R$, it holds:*

1. $[\mathcal{O}_R : I] = N_{F/K}(I)$.

2. $[\mathcal{O}_R : I^{-1}] = [\mathcal{O}_R : I]^{-1} = [I : \mathcal{O}_R]$.

3. $[\mathcal{O}_R : II'] = [\mathcal{O}_R : I][\mathcal{O}_R : I']$.

A basis $\mathcal{B}$ of a fractional ideal I of $\mathcal{O}_F$ is defined to be an A-basis of I. Analogously, we define a basis $\mathcal{B}'$ of an fractional ideal I_∞ of $\mathcal{O}_{F,\infty}$ to be an A_∞-basis of I_∞. By θ_R we denote θ if $R = A$, and θ_∞, for $R = A_\infty$. We define $\mathcal{B}_{\theta_R}$ to be the family $(1, \theta_R, \ldots, \theta_R^{n-1})$. Clearly, $\mathcal{B}_{\theta_R}$ is a basis of $R[\theta_R]$.

In this subsection we consider canonical bases of fractional ideals in function fields. These canonical bases consist of elements having "small" size, which is comfortable from the computational point of view. Moreover, we can determine concrete bounds for the entries of the transition matrix from such a canonical basis to $\mathcal{B}_{\theta_R}$. These bounds will play an important role in further complexity analyses in Chapter 4.

Let $I = \prod_{\mathfrak{p}\in \mathrm{Max}(\mathcal{O}_R)} \mathfrak{p}^{a_\mathfrak{p}}$, with $a_\mathfrak{p} \in \mathbb{Z}$ and almost all of them equal zero, be a nonzero fractional ideal of $\mathcal{O}_R$. We define

$$I^* := \prod_{\mathfrak{p}\in \mathrm{Max}(\mathcal{O}_R)} \mathfrak{p}^{-|a_\mathfrak{p}|}. \tag{1.1}$$

Clearly, I^* is again a fractional ideal of $\mathcal{O}_R$.

Definition 1.2.7. *The* height *of the fractional ideal I of $\mathcal{O}_F$ or I_∞ of $\mathcal{O}_{F,\infty}$ is defined to be the integer*

$$h(I) := |[I^* : A[\theta]]| \quad or \quad h(I_\infty) := -|[I_\infty^* : A_\infty[\theta_\infty]]|.$$

Additionally, we define the absolute height *of I or I_∞ by*

$$H(I) := |[I^* : \mathcal{O}_F]| + |\operatorname{disc} f| \quad or \quad H(I_\infty) := -|[I_\infty^* : \mathcal{O}_{F,\infty}]| - |\operatorname{disc} f_\infty|.$$

Lemma 1.2.8. *Let I and I_∞ be as in the last definition. Then, it holds*

1. $h(I),\ h(I_\infty),\ H(I),\ H(I_\infty) \geq 0$,
2. $h(I) \leq |[I^* : \mathcal{O}_F]| + \frac{1}{2}|\operatorname{disc} f| \leq H(I)$,
3. $h(I_\infty) \leq -|[I_\infty^* : \mathcal{O}_{F,\infty}]| - \frac{1}{2}|\operatorname{disc} f_\infty| \leq H(I_\infty)$.

Proof. Since the exponents in the decomposition of I^* and I_∞^* are nonpositive integers, we have $A[\theta] \subseteq \mathcal{O}_F \subseteq I^*$ and $A_\infty[\theta_\infty] \subseteq \mathcal{O}_{F,\infty} \subseteq I_\infty^*$. Then, by the properties of the index of modules we deduce $[I^* : A[\theta]] = rA$ with $r \in A$ and $[I_\infty^* : A_\infty[\theta_\infty]] = r'A_\infty$ with $r' \in A_\infty$; hence, $h(I) = |r| \geq 0$ and $h(I_\infty) = -|r'| \geq 0$. Since $|\operatorname{disc} f|,\ -|\operatorname{disc} f_\infty| \geq 0$, we deduce $H(I),\ H(I_\infty) \geq 0$.

For the second statement we use the transitivity of the index

$$[I^* : A[\theta]] = [I^* : \mathcal{O}_F][\mathcal{O}_F : A[\theta]].$$

Denote by $\mathcal{B} = (b_0, \ldots, b_{n-1})$ a basis of $\mathcal{O}_F$ and let $\mathcal{B}_\theta := (1, \theta, \ldots, \theta^{n-1})$. By [29] it holds

$$\operatorname{disc} f = \det(\mathrm{Tr}_{F/K}(\theta^{i+j}))_{0\leq i,j<n} = (\det T(\mathcal{B}_\theta \to \mathcal{B}))^2 \cdot \det(\mathrm{Tr}_{F/K}(b_i b_j))_{0\leq i,j<n}.$$

Then, $(\det T(\mathcal{B}_\theta \to \mathcal{B}))^2$ divides $\operatorname{disc} f$ and therefore $(\operatorname{disc} f)A \subset (\det T(\mathcal{B}_\theta \to \mathcal{B}))^2 A = [\mathcal{O}_F : A[\theta]]^2$. Hence, $|(\operatorname{disc} f)A| = |\operatorname{disc} f| \geq 2|[\mathcal{O}_F : A[\theta]]|$, and in particular $|[I^* : A[\theta]]| = |[I^* : \mathcal{O}_F][\mathcal{O}_F : A[\theta]]| \leq |[I^* : \mathcal{O}_F]| + \frac{1}{2}|\operatorname{disc} f| \leq H(I)$. Item *3* can be shown analogously. □

Definition 1.2.9. *Let $\mathcal{B}$ be a basis of a fractional ideal I of $\mathcal{O}_R$ and T the transition matrix from $\mathcal{B}$ to $\mathcal{B}_{\theta_R}$. We call $\mathcal{B}$ an* Hermite basis *of I, if hT is in HNF, for any $h \in R \setminus R^*$ such that $hT \in R^{n\times n}$.*

Let M be in $R^{n\times n} \cap \mathrm{GL}_n(K)$. The HNF of the matrix PM coincides with the HNF of M, for any $P \in \mathrm{GL}_n(R)$.

Lemma 1.2.10. *Every ideal I of $\mathcal{O}_R$ admits a unique Hermite basis.*

Let $\mathcal{B}$ be an Hermite basis of I and $T = T(\mathcal{B} \to \mathcal{B}_{\theta_R})$. The diagonal entries $d_1, \ldots, d_n \in K$ of T are canonical invariants of the fractional ideal I, which only depend on f, the defining polynomial of F/k. In particular, $[R[\theta_R] : I] = (d_1 \cdots d_n)R$.

From the fact that I is an ideal we deduce $d_n | \cdots | d_1$; that is, $d_i/d_{i+1} \in R$ for all i. We call these elements the *elementary divisors* of I. If I is contained in $R[\theta_R]$, by Lemma 1.2.3 we obtain $d_1, \ldots, d_n \in R$ and

$$R[\theta_R]/I \cong R/d_1R \times \cdots \times R/d_nR.$$

For any subset $S \subset R$, we call an element $h \in S \setminus \{0\}$ minimal if $\deg h$ or $v_\infty(h)$ is minimal among all other elements in S, for $R = A$ or $R = A_\infty$, respectively.

Lemma 1.2.11. *Let $\mathcal{B}$ be an Hermite basis of a fractional ideal I of $\mathcal{O}_R$ and $(t_{i,j}) = T(\mathcal{B} \to \mathcal{B}_{\theta_R})$. For $g \in R$ minimal such that $gT \in R^{n\times n}$ it holds,*

$$|gt_{i,j}| \le H(I) \quad \text{or} \quad v_\infty(gt_{i,j}) \le H(I)$$

according to $R = A$ or $R = A_\infty$.

In order to proof this statement we will use the following lemma.

Lemma 1.2.12. *For $I = \prod_{\mathfrak{p}\in \mathrm{Max}(\mathcal{O}_R)} \mathfrak{p}^{a_\mathfrak{p}}$, we write $I = I_1 \cdot I_2$, where $I_1 := \prod_{a_\mathfrak{p}<0} \mathfrak{p}^{a_\mathfrak{p}}$ and $I_2 := \prod_{a_\mathfrak{p}>0} \mathfrak{p}^{a_\mathfrak{p}}$. Then,*

$$h(I_1) + h(I_2) \le H(I).$$

Proof. Let $R = A$, the case $R = A_\infty$ can be treated analogously. Clearly, $I^* = I_1^* \cdot I_2^*$ by definition. Then, Lemma 1.2.6 shows that

$$[I^* : \mathcal{O}_F][\mathcal{O}_F : A[\theta]]^2 = [I_1^* : A[\theta]][I_2^* : A[\theta]].$$

According to the proof of Lemma 1.2.8 we have $|[\mathcal{O}_F : A[\theta]]| \le \frac{1}{2}|\operatorname{disc} f|$; hence, $h(I_1) + h(I_2) = |[I^* : \mathcal{O}_F]| + 2|[\mathcal{O}_F : A[\theta]]| \le H(I)$. □

Proof of Lemma 1.2.11. We consider the case $R = A$. The case $R = A_\infty$ can be treated analogously. Let $I = I_1 \cdot I_2$ with I_1, I_2 defined as in Lemma 1.2.12.

As $[I_1 : A[\theta]] = rA$ with $r \in A$, we deduce $|g| \leq |r| = |[I_1 : A[\theta]]| = h(I_1)$, by the minimality of $|g|$.

Since $\mathcal{B}$ is an Hermite basis of I, the matrix $T := T(\mathcal{B} \to \mathcal{B}_{\theta_R})$ is triangular and the entries of the j-th column satisfy $|t_{i,j}| \leq |t_{j,j}|$, for $j \leq i \leq n$. We consider the matrix $T^{-1} = T(\mathcal{B}_{\theta_R} \to \mathcal{B})$ which has the diagonal entries $t_{j,j}^{-1}$ for $1 \leq j \leq n$. Let $g' \in A \setminus \{0\}$ be of minimal degree such that $g'A[\theta] \subset I$ (or equivalently $g'T^{-1} \in A^{n\times n}$). Then, $|g't_{j,j}^{-1}| \geq 0$ and equivalently $|g'| \geq |t_{j,j}|$.

Since $[\mathcal{O}_F : I_2] = r'A$ with $r' \in A$, we obtain $|g'| \leq |r'| = |[\mathcal{O}_F : I_2]|$ by the minimality of $|g'|$. Now, $[\mathcal{O}_F : I_2] = [\mathcal{O}_F : (I_2^*)^{-1}] = [I_2^* : \mathcal{O}_F]$, so that $|g'| \leq |[I_2^* : \mathcal{O}_F]| \leq h(I_2)$.

Finally, we deduce $|gt_{i,j}| \leq h(I_1) + h(I_2) \leq H(I)$, by Lemma 1.2.12. □

Corollary 1.2.13. *Let $\mathcal{B}$ be an Hermite basis of a fractional ideal I of $\mathcal{O}_R$. Suppose that $T = T(\mathcal{B} \to \mathcal{B}_{\theta_R}) = (f_{i,j}/h_{i,j})$ with coprime polynomials $f_{i,j}, h_{i,j} \in A$, and let $g \in A \setminus \{0\}$ be of minimal degree such that $gT \in A^{n\times n}$. For $1 \leq i, j \leq n$, we have*

$$|g| + \max\{|f_{i,j}|, |h_{i,j}|\} \leq 2H(I).$$

Proof. For $R = A$ the statement is a direct consequence of Lemma 1.2.11.

Let $R = A_\infty$. We consider the elementary divisors $d_1, \ldots, d_n$ of I, which satisfy $d_i = t^{\alpha_i}$ with $\alpha_i \in \mathbb{Z}$ and $\alpha_1 \leq \cdots \leq \alpha_n$, since $d_i/d_{i+1} \in A_\infty$ for all i. We fix $g' = t^{-\beta}$, where $\beta := \max\{\alpha_n, 0\}$. Then, $g' \in A_\infty$ is minimal with $g'T \in A_\infty^{n\times n}$. Lemma 1.2.11 shows that $v_\infty(g't_{i,j}) \leq H(I)$, where $(t_{i,j}) = T$. Since $g'T$ is in HNF, the diagonal entries are t^{-1}-powers, and in particular $v_\infty(g't_{i,i}) = \deg_{t^{-1}}(g't_{i,i})$ holds. Hence, the entries in $g'T$ satisfy $\deg_{t^{-1}}(g't_{i,j}) \leq H(I)$ by the definition of the HNF in that context. For any $h \in k[t^{-1}]$ of t^{-1}-degree equal m we can write $h = t^m h/t^m$ with $t^m h \in A$ and $|t^m h| \leq m$. Thus, any entry of $g'T$ can be written as $f_{i,j}/t^{m_{i,j}}$ with $f_{i,j} \in A$, $|f_{i,j}| \leq H(I)$, and $0 \leq m_{i,j} \leq H(I)$. Clearly, there exists $m \in \mathbb{Z}$, with $m \leq H(I)$, such that $t^m f_{i,j}/t^{m_{i,j}} \in A$, for all $1 \leq i, j \leq n$. We set $g := t^m$ and $h_{i,j} := t^{m_{i,j}}$ and obtain $|g| + \max\{|f_{i,j}|, |h_{i,j}|\} \leq 2H(I)$, for $1 \leq i, j \leq n$. □

1.2.3 Ideal representation of divisors

Let F/k be a function field. The places $Q \in \mathbb{P}_0$ and $P \in \mathbb{P}_\infty$ are in 1:1 correspondence with prime ideals $\mathfrak{q}$ of $\mathcal{O}_F$ and $\mathfrak{p}$ of $\mathcal{O}_{F,\infty}$, respectively. If Q lies over P_p, then $\mathfrak{q}$ lies over

$p(t)$ and it holds

$$e(Q/P_p) = e(\mathfrak{q}/p), \quad \deg Q = [k_p : k] \cdot f(\mathfrak{q}/p), \quad v_Q = v_{\mathfrak{q}}.$$

For the places P at infinity of F we analogously deduce:

$$e(P/P_\infty) = e(\mathfrak{p}/\mathfrak{m}_\infty), \quad \deg P = f(\mathfrak{p}/\mathfrak{m}_\infty), \quad v_P = v_{\mathfrak{p}}.$$

This identification leads to an ideal theoretical representation of a divisor D of F/k. For

$$D = \sum_{Q \in \mathbb{P}_0(F)} a_Q \cdot Q + \sum_{P \in \mathbb{P}_\infty(F)} b_P \cdot P$$

with $\alpha_Q, \beta_P \in \mathbb{Z}$, we consider the pair (I, I_∞), where $I := \prod_{Q \in \mathbb{P}_0} \mathfrak{q}^{-a_Q}$ and $I_\infty := \prod_{P \in \mathbb{P}_\infty} \mathfrak{p}^{-b_P}$ are fractional ideals of $\mathcal{O}_F$ and $\mathcal{O}_{F,\infty}$, respectively. We call (I, I_∞) the *ideal representation* of the divisor D.

1.3 Algorithms and complexity

For all considered algorithms we assume that the field k is computable; that is, the zero and one in k are available and basic operations as $+, -, \cdot, /$, and the comparison of equality of two elements in k can be performed. We can extend this operations to the ring $k[t]$ and the rational function field $k(t)$; hence, $k[t]$ and $k(t)$ become computable. In any runtime analysis we count the number of operations in k.

In the complexity estimations we use the big O notation: Let $g, h : \mathbb{R}^{>0} \to \mathbb{R}$ two functions. We write $g = O(h)$, if there exist constants $c, x_0 \in \mathbb{R}$, such that $|g(x)| \leq ch(x)$ for all $x \geq x_0$.

1.4 Montes algorithm in function fields

Let F/k be a function field with defining polynomial $f \in k[t, x]$ and let $p(t)$ be a monic and irreducible polynomial in A. Denote by $K_p := k_p((p(t)))$ the completion of K at the place P_p, where $k_p = A/(p(t))$. The valuation v_p extends in an obvious way to K_p. Denote by $\hat{A}_p := k_p[[p(t)]]$ the valuation ring of v_p and by $\hat{\mathfrak{m}}_p = p(t)\hat{A}_p$ its maximal ideal.

Moreover, let $K_\infty := k((t^{-1}))$ be the completion of K at the place P_∞. The valuation can be extended to K_∞ analogously. By $\hat{A}_\infty \subset K_\infty$ and $\hat{\mathfrak{m}}_\infty$ we denote the valuation ring of v_∞ and its maximal ideal.

By the classical theorem of Hensel [15] the prime ideals of $\mathcal{O}_F$ lying over $p(t)$ are in one-to-one correspondence with the monic irreducible factors of f in $\hat{A}_p[x]$. The same yields for prime ideals of $\mathcal{O}_{F,\infty}$ and monic irreducible factors of f_∞ in $\hat{A}_\infty[x]$.

The aim of the section is to describe the Montes algorithm, which determines for the input of f and $p(t)$ a parametrization of the irreducible factors of f in $\hat{A}_p[x]$. Denote by $\mathfrak{p}$ a prime ideal of $\mathcal{O}_F$ lying over $p(t)$ and denote by $f_\mathfrak{p} \in \hat{A}_p[x]$ the corresponding irreducible factor of f. Then, the Montes algorithm produces a list of data, a so-called *type*,

$$\mathbf{t} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_{r+1}, \lambda_{r+1}, \psi_{r+1})),$$

which is a representation of the irreducible factor $f_\mathfrak{p}$ and therefore a representation the prime ideal $\mathfrak{p}$. We call this representation an OM-representation of $\mathfrak{p}$ (cf. Definition 1.4.3).

The Montes algorithm can be seen as a factorization algorithm, which detects the factorization of $f \in \hat{A}_p[x]$, but never computes it. To this purpose, a kind of Hensel's lemma of higher order is applied [8, Theorem 3.7]. At any level $i \geq 1$, besides the fundamental data $\phi_i \in A[x]$, $\lambda_i \in \mathbb{Q}_{>0}$, $\psi_i \in \mathbb{F}_i[y]$, where $\mathbb{F}_i$ is a finite extension of k_p, the type supports:

- $N_i : \hat{A}_p[x] \to 2^{\mathbb{R}^2}$ a **Newton polygon operator**,
- $R_i : \hat{A}_p[x] \to \mathbb{F}_i[y]$ a **residual polynomial operator**,
- $v_{i-1} : K_p(x) \to \mathbb{Z} \cup \{\infty\}$ a **discrete valuation**.

Below we give an overview of the Montes algorithm, the OM-representation of prime ideals, and certain applications, which will be useful for further considerations. The results are mainly extracted from [8] and [9]. A comprehensive explanation of the Montes algorithm can be found in [7].

1.4.1 Types

Denote $v_p : K_p \to \mathbb{Q}$ the canonical $p(t)$-adic valuation on the Laurent series ring K_p. We extend v_p to a discrete valuation v_0 on $K_p(x)$, determined by

$$v_0 : K_p[x] \to \mathbb{Z} \cup \{\infty\}, \quad v_0(c_0 + \cdots + c_r x^r) := \min\{v_p(c_i) \mid 0 \le j \le r\}. \tag{1.2}$$

Types of order zero

We denote by $\mathbb{F}_0 := k_p = A/(p(t))$ and define the 0-th residual polynomial operator

$$R_0 : \hat{A}_p[x] \to \mathbb{F}_0[y], \quad g(x) \mapsto \overline{g(y)/p^{v_0(g)}},$$

where $\bar{\ } : \hat{A}_p[y] \to \mathbb{F}_0[y]$ is the natural reduction map. A *type of order zero*,

$$\mathbf{t} = (\psi_0),$$

is determined by $\psi_0(y) \in \mathbb{F}_0[y]$, a monic irreducible polynomial. A *representative* of $\mathbf{t}$ is any monic polynomial $\phi_1(x) \in A[x]$ such that $R_0(\phi) = \psi_0$.

We consider the defining polynomial f of the function field F/k. From a factorization of $R_0(f)(y) = \psi_{1,0}^{n_1} \cdots \psi_{\kappa,0}^{n_\kappa}$ into the product of irreducible monic polynomials $\psi_{i,0}(y) \in \mathbb{F}_0[y]$ we deduce types of order zero. Each irreducible factor $\psi_{i,0}(y)$ singles out one type of order zero. For convenience, we consider one fixed factor, denote it by ψ_0, and consider a representative $\phi_1 \in A[x]$. Let $m_1 := \deg \phi_1$.

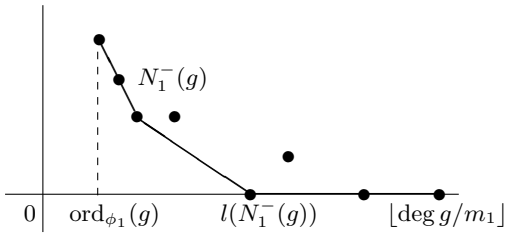
Types of order one:

Newton polygon operator. The Newton polygon of a polynomial $g(x) \in K_p[x]$ is determined by the pair (v_0, ϕ_1). If $\sum_{s\ge 0} a_s(x)\phi_1(x)^s$ is the ϕ_1-adic development of $g(x)$, then

$$N_1(g) := N_{v_0,\phi_1}(g) \tag{1.3}$$

is defined to be the lower convex hull of the set of points of the plane with coordinates $(s, v_0(a_s(x)\phi_1(x)^s))$. However, we only consider the principal part of this polygon, $N_1^-(g) = N_{v_0,\phi_1}^-(g)$, formed by the sides of negative slopes of $N_1(g)$. The length $l(N_1^-(g))$ of the polygon $N_1^-(g)$ is, by definition, the abscissa of its right end point. The typical shape of $N_1^-(g)$ for a monic polynomial g is as shown below.

Figure 1.1: Newton polygon of g.



Residual polynomial operator. We fix $\mathbb{F}_1 := \mathbb{F}_0(y)/(\psi_0(y))$ and we set z_0 to be the class of y in $\mathbb{F}_1$, so that $\mathbb{F}_1 = \mathbb{F}_0[z_0]$. The polygon $N := N_1^-(g)$ has a residual coefficient c_s at each integer abscissa, $\mathrm{ord}_{\phi_1} g \leq s \leq l(N)$, defined as follows:

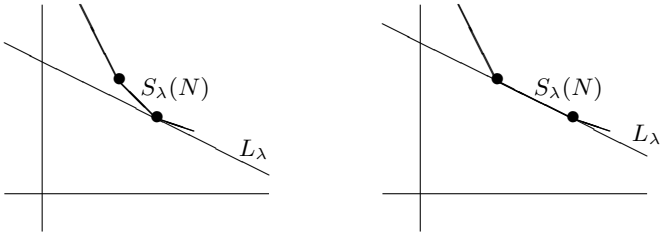
$$c_s := \begin{cases} 0, & \text{if } (s, v_0(a_s)) \text{ lies above } N, \\ R_0(a_s)(z_0) \in \mathbb{F}_1, & \text{if } (s, v_0(a_s)) \text{ lies on } N. \end{cases}$$

Denote by $\mathrm{Slopes}(N)$ the set of slopes of N. Given any $\lambda \in \mathbb{Q}_{>0}$, we define:

$$S_\lambda(N) := \{(x,y) \in N \mid y + \lambda x \text{ is minimal}\} = \begin{cases} \text{a vertex}, & \text{if } -\lambda \notin \mathrm{Slopes}(N), \\ \text{a side}, & \text{if } -\lambda \in \mathrm{Slopes}(N). \end{cases}$$

The following picture illustrates both possibilities. In this picture L_λ is the line of slope $-\lambda$ having first contact with N from below.

Figure 1.2: λ-component of a polygon.



In any case, $S_\lambda(N)$ is a segment of $\mathbb{R}^2$ with end points having integer coordinates. Any such segment has a degree. If $\lambda = h/e$ with h, e positive coprime integers, the degree of $S_\lambda(N)$ is defined as:

$$d := d(S_\lambda(N)) := l(S_\lambda(N))/e,$$

where $l(S_\lambda(N))$ is the length of the projection of $S_\lambda(N)$ to the horizontal axis. Note that S_λ splits into d minimal subsegments, whose end points have integer coordinates. Denote s_0 and s_1 the abscissas of the endpoints of S_λ. Then, the abscissas of the points on S_λ with integer coordinates are given by $s_0, s_0+e, \dots, s_1 = s_0+de$. We define the residual polynomial of first order of $f(x)$, with respect to v_0, ϕ_1, λ, as:

$$R_{v_0,\phi_1,\lambda}(g)(y) := c_{s_0} + c_{s_0+e}y + \cdots + c_{s_1}y^d \in \mathbb{F}_1[y].$$

Note that $c_{s_0}c_{s_1} \neq 0$; thus, the degree of $R_{v_0,\phi_1,\lambda}(g)$ is always equal to d. Let h_1, e_1 be coprime positive integers and consider the positive rational number $\lambda_1 = h_1/e_1$. Let $\psi_1(y) \in \mathbb{F}_1[y]$ be a monic irreducible polynomial $\psi_1(y) \neq y$. Then,

$$\mathbf{t} = (\psi_0; (\phi_1, \lambda_1, \psi_1)),$$

is called a *type of order one*. Such a type supports a *residual polynomial operator* of the first order $R_1 := R_{v_0,\phi_1,\lambda_1}$. Given any such type, one can compute a *representative* of $\mathbf{t}$; that is, any monic polynomial $\phi_2(x) \in A[x]$ of degree $e_1 \deg\psi_1 \deg\phi_1$, satisfying $R_1(\phi_2)(y) = \psi_1(y)$. This polynomial is necessarily irreducible in $\hat{A}_p[x]$.

Discrete valuation. The triple (v_0, ϕ_1, λ_1) also determines a discrete valuation on $K_p(x)$ as follows: For $g \in K_p[x]$ nonzero, we consider the intersection point $(0, H)$ of the vertical axis with the line of slope $-\lambda_1$ containing $S_{\lambda_1}(N_1^-(g))$. Then, we set $v_1(g(x)) := e_1H$.

Types of order r:

Now we may start over again with the pair (v_1, ϕ_2) and repeat all constructions in order two. The iteration of this procedure leads to the concept of a *type of order r*.

A type of order $r \geq 1$ is a chain:

$$\mathbf{t} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \dots; (\phi_r, \lambda_r, \psi_r)),$$

where $\phi_1(x), \dots, \phi_r(x) \in A[x]$ are monic and irreducible in $\hat{A}_p[x]$, $\lambda_1, \dots, \lambda_r \in \mathbb{Q}_{>0}$, and $\psi_0(y) \in \mathbb{F}_0[y], \dots, \psi_r(y) \in \mathbb{F}_r[y]$ are monic irreducible polynomials over certain fields $\mathbb{F}_0 \subset \cdots \subset \mathbb{F}_r$ that satisfy the following recursive properties:

1. $R_0(\phi_1)(y) = \psi_0(y)$. We define $\mathbb{F}_1 := \mathbb{F}_0(y)/(\psi_0(y))$.

2. For all $1 \leq i < r$,

- $\deg \phi_i | \deg \phi_{i+1}$,
- $N_i(\phi_{i+1}) := N_{v_{i-1},\phi_i}(\phi_{i+1})$ is one-sided of slope $-\lambda_i$, and
- $R_i(\phi_{i+1})(y) := R_{v_{i-1},\phi_i,\lambda_i}(\phi_{i+1})(y) = \psi_i(y)$.

We define $\mathbb{F}_{i+1} := \mathbb{F}_i[y]/(\psi_i(y))$.

3. $\psi_r(y) \neq y$. We define $\mathbb{F}_{r+1} := \mathbb{F}_r[y]/(\psi_r(y))$.

Thus, a type of order r is an object structured in r levels. In the computational representation of a type, several invariants are stored at each level, $1 \leq i \leq r$. The most important ones are:

$\phi_i(x)$,	monic polynomial in $A[x]$, irreducible in $\hat{A}_p[x]$,
m_i,	$\deg \phi_i(x)$,
$V_i := v_{i-1}(\phi_i)$,	nonnegative integer,
$\lambda_i = h_i/e_i$,	h_i, e_i positive coprime integers
$\psi_i(y)$,	monic irreducible polynomial in $\mathbb{F}_i[y]$,
f_i,	$\deg \psi_i(y)$,
z_i,	the class of y in $\mathbb{F}_{i+1}$, so that $\psi_i(z_i) = 0$ and $\mathbb{F}_{i+1} = \mathbb{F}_i[z_i]$.

Take $f_0 := \deg \psi_0$. Note that

$$m_i = (f_0 f_1 \cdots f_{i-1})(e_1 \cdots e_{i-1}) = e_{i-1} f_{i-1} m_{i-1}, \quad \dim_{\mathbb{F}_0} \mathbb{F}_{i+1} = f_0 f_1 \cdots f_i. \tag{1.4}$$

The discrete valuations $v_0, \ldots, v_r$ on the field $K_p(x)$ are essential invariants of the type.

Definition 1.4.1. *Let $g(x) \in \hat{A}_p[x]$ be a monic polynomial, and $\mathbf{t}$ a type of order $r \geq 1$.*

1. *We say that* $\mathbf{t}$ divides $g(x)$, *if $\psi_r(y)$ divides $R_r(g)(y)$ in $\mathbb{F}_r[y]$. We denote* $\mathrm{ord}_{\mathbf{t}}(g) := \mathrm{ord}_{\psi_r}(R_r(g))$

2. *We say that* $\mathbf{t}$ *is* g-complete *if* $\mathrm{ord}_{\psi_r}(R_r(g)) = 1$. *In this case,* $\mathbf{t}$ *singles out a monic irreducible factor $g_{\mathbf{t}}(y) \in \hat{A}_p[x]$ of $g(x)$, uniquely determined by the property $R_r(g_{\mathbf{t}}(x))(y) = \psi_r(y)$. If $K_{\mathbf{t}}$ is the extension field of K_p determined by $g_{\mathbf{t}}(x)$, then*

$$e(K_{\mathbf{t}}/K_p) = e_1 \cdots e_r, \quad f(K_{\mathbf{t}}/K_p) = f_0 f_1 \cdots f_r.$$

3. *A* representative *of* $\mathbf{t}$ *is a monic polynomial $\phi_{r+1}(x) \in A[x]$, of degree $m_{r+1} = e_r f_r m_r$ such that $R_r(\phi_{r+1})(y) = \psi_r(y)$. This polynomial is necessarily irreducible in $\hat{A}_p[x]$. By definition of a type, each ϕ_{i+1} is a representative of the truncated type of order i*

$$\mathrm{Trunc}_i(\mathbf{t}) := (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_i, \lambda_i, \psi_i)).$$

4. *We say that* $\mathbf{t}$ *is optimal if* $m_1 < \cdots < m_r$*, or equivalently, if* $e_i f_i > 2$*, for all* $1 \leq i < r$*.*

A type $\mathbf{t}$ *of order* 0 *is by definition optimal.*

Lemma 1.4.2. *With the above notation,* $\mathrm{ord}_{\mathbf{t}}(g) = l(N_{r+1}^{-}(g))$*.*

1.4.2 The Montes algorithm

At the input of $f(x)$ and $p(t)$, the Montes algorithm computes a family $\mathbf{t}_1, \ldots, \mathbf{t}_\kappa$ of f-complete and optimal types in one-to-one correspondence with the irreducible factors of $f_{\mathbf{t}_1}, \ldots, f_{\mathbf{t}_\kappa}$ of f in $\hat{A}_p[x]$. This one-to-one correspondence is determined by

1. For all $1 \leq i \leq \kappa$, the type $\mathbf{t}_i$ is $f_{\mathbf{t}_i}$-complete.
2. For all $j \neq i$, the type $\mathbf{t}_j$ does not divide $f_{\mathbf{t}_i}$.

The algorithm starts by computing the order zero types determined by the irreducible factors of $f(x)$ modulo $p(t)$, and then processes to enlarge them in a convenient way until the whole list of f-complete optimal types is obtained. Let us briefly explain how that enlargement is realized along the Montes algorithm. Suppose a type of order $i-1$ dividing $f(x)$ is considered,

$$\mathbf{t} := (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_{i-1}, \lambda_{i-1}, \psi_{i-1})).$$

A representative $\phi_i(x)$ is constructed. The type $\mathbf{t}$ branches in principle into as many types as pairs $(\lambda, \psi(y))$, where $-\lambda$ runs on the slopes of $N_i^{-}(f)$ and $\psi(y)$ runs on the different monic irreducible factors of $R_{v_{i-1},\phi_i,\lambda}(f)(y) \in \mathbb{F}_i[y]$.

Every output $\mathbf{t}$ of the Montes algorithm is a type of order $r+1$, where r is called the *Okutsu depth* of the corresponding irreducible factor $f_{\mathbf{t}}(x)$. The sequence $[\phi_1, \ldots, \phi_r]$ is an *Okutsu frame* of $f_{\mathbf{t}}(x)$. Details can be found in [11].

The invariants v_i, h_i, e_i, f_i at each level $0 \leq i \leq r$ are canonical (depend only on $f(x)$). The $(r+1)$-level $\mathbf{t}$ carries only the invariants:

$$\phi_{r+1}, m_{r+1}, V_{r+1}, \lambda_{r+1} = -h_{r+1}, e_{r+1} = 1, \psi_{r+1}, f_{r+1} = 1.$$

If $\mathfrak{p}$ is the prime ideal corresponding to $\mathbf{t}$, we denote

$$f_{\mathfrak{p}}(x) := f_{\mathbf{t}}(x) \in \hat{A}_p[x], \quad \phi_{\mathfrak{p}}(x) := \phi_{r+1}(x) \in A[x], \quad \mathbb{F}_{\mathfrak{p}} := \mathbb{F}_{r+1},$$
$$\psi_{\mathfrak{p}}(y) := \psi_{r+1}(y) \in \mathbb{F}_{\mathfrak{p}}[y], \quad n_{\mathfrak{p}} := m_{r+1} = \deg f_{\mathfrak{p}} = \deg \phi_{\mathfrak{p}},$$
$$\mathbf{t}_{\mathfrak{p}} := \mathbf{t} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_r, \lambda_r, \psi_r); (\phi_{\mathfrak{p}}, \lambda_{r+1}, \psi_{\mathfrak{p}})).$$

The polynomial $\phi_{\mathfrak{p}}$ is an *Okutsu approximation* to $f_{\mathfrak{p}}$. It is a sufficiently good approximation for many purposes.

Definition 1.4.3. *We say that* $\mathbf{t}_{\mathfrak{p}}$ *an OM* representation *of* $\mathfrak{p}$.

Remark 1.4.4. *In order to deal with the prime ideals of* $\mathcal{O}_{F,\infty}$*, the infinite maximal order, we can apply the Montes algorithm to the defining polynomial* $f_\infty(t^{-1},x) \in k[t^{-1},x]$ *and the irreducible polynomial* $t^{-1} \in k[t^{-1}]$*. Then, the OM representation of* $\mathfrak{p}$ *in* $\mathcal{O}_{F,\infty}$ *is given by a certain type with* ϕ*-polynomials* $\phi_1,\dots,\phi_r,\phi_{\mathfrak{p}} \in k[t^{-1},x]$.

Example 1.4.5. Let $\mathbb{F} = \{0,1,2\}$ be the field with three elements. We consider the function field $F/\mathbb{F}$ with defining polynomial $f(t,x) = x^4 + t^3x^3 + (2t^8 + t^6 + 2t)x^2 + 2x + t^{12} \in \mathbb{F}[t,x]$ and the irreducible polynomial $p(t) = t \in \mathbb{F}[t]$. Let us determine the f-complete and optimal types which correspond to the prime ideals of $\mathcal{O}_F$ lying over $p(t)$. We set $\mathbb{F}_0 := \mathbb{F}$ and obtain

$$R_0(f)(y) = y^4 + 2y = (y+2)^3 y \in \mathbb{F}_0[y].$$

The two irreducible factors $\psi_0(y) := y + 2$ and $\psi_0'(y) := y$ of $R_0(f)(y)$ determine two types $\mathbf{t}$ and $\mathbf{t}'$ of order 0, respectively.

Since $\operatorname{ord}_{\psi_0'}(R_0(f)(y)) = 1$, the type $\mathbf{t}' = (\psi_0')$ is already f-complete and optimal. A representative of $\mathbf{t}'$ is given by $\phi_1'(x) = x \in \mathbb{F}[t,x]$ and we have detected the first prime ideal $\mathfrak{p}'$ lying over $p(t)$, given by its OM representation

$$\mathbf{t}_{\mathfrak{p}'} = (y;(x,12,y+2)), \quad \phi_{\mathfrak{p}'}(x) = x.$$

The data of the last level are determined by the computation of $N_1^-(f)$, one-sided of slope -12, and $R_1(f)(y) = 2y + 1$. The Okutsu depth of $f_{\mathfrak{p}'}$ is zero and we have $e(\mathfrak{p}'/p) = f(\mathfrak{p}'/p) = 1$.

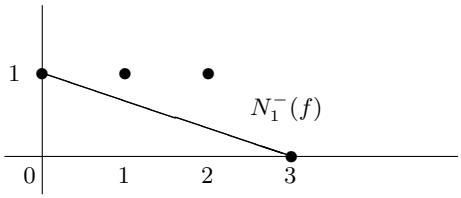
Clearly, $\phi_1(x) = x + 2$ is a representative of $\mathbf{t}$. As $\mathbf{t}$ is not f-complete, we have to enlarge the type. By Lemma 1.4.2, the Newton polygon $N_1^-(f) = N_{v_0,\phi_i}^-(f)$ has length equal to $\operatorname{ord}_{\mathbf{t}}(f) = 3$. Hence, in order to compute this polygon, we need only to consider the first four coefficients of the ϕ_1-development $f = \sum_{s\geq 0} a_s\phi_1^s$:

$$\begin{aligned} a_0 &= t^{12} + 2t^8 + t^6 + t^3 + 2t, \quad a_1 = t^8 + 2t^6 + t, \\ a_2 &= 2t^8 + t^6 + 2t, \quad a_3 = t^3 + 1. \end{aligned}$$

The Newton polygon $N_1^-(f)$ is shown in Figure 1.3.

Since $N_1^-(f)$ is just a side of slope $-\lambda := -1/3$, it holds $S_\lambda(N_1^-(f)) = N_1^-(f)$. Hence, we deduce $R_1(f)(y) = R_{v_0,\phi_1,\lambda}(f)(y) = R_0(a_0)(z_0) + R_0(a_3)(z_0)y = 2 + y \in \mathbb{F}_1[y]$,

Figure 1.3: Newton polygon of $N_1^-(f)$.



where $\mathbb{F}_1 = \mathbb{F}_0[y]/(\psi_0) = \mathbb{F}_0$. We set $\lambda_1 := 1/3,\ \psi_1(y) := y+2$, and enlarge the type $\mathbf{t}$ to a type of order 1,

$$\mathbf{t} = (\psi_0; (\phi_1, \lambda_1, \psi_1)).$$

Clearly, $\mathbf{t}$ is f-complete and optimal. Thus we have detected the second prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$ over $p(t)$. An easy computation shows that $\phi_2(x) := x^3+2t+2$ is a representative of $\mathbf{t}$. The OM representation of $\mathfrak{p}$ is given by

$$\mathbf{t}_\mathfrak{p} = (y+2; (x+2, 1/3, y+2); (x^3+2t+2, 1, y+1)),$$

because $N_2^-(f) := N_{v_1,\phi_2}^-$ is one-sided of slope -1 and $R_2(f) = y+1$. The Okutsu depth of $f_\mathfrak{p}$ is one and we get $e(\mathfrak{p}/p) = 3,\ f(\mathfrak{p}/p) = 1$. Also, we have the following approximate factorization of f in $\hat{A}_p[x]$:

$$f \approx x \cdot (x^3 + 2t + 2).$$

1.4.3 Secondary invariants and applications

Let $p(t) \in A$ be an irreducible polynomial and $\mathfrak{p}$ a prime ideal of $\mathcal{O}_F$ lying over $p(t)$ corresponding to a f-complete type $\mathbf{t}_\mathfrak{p}$ of order $r+1$. By item *2* of Definition 1.4.1 we know that

$$e(\mathfrak{p}/p) = e_1 \cdots e_r, \quad f(\mathfrak{p}/p) = f_0 f_1 \cdots f_r.$$

We consider all prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ of $\mathcal{O}_F$ lying over $p(t)$ and their corresponding f-complete types $\mathbf{t}_1, \ldots, \mathbf{t}_s$. We denote by $f_{\mathfrak{p}_i} \in \hat{A}_p[x]$ the irreducible factor of f corresponding to $\mathbf{t}_i$, for $1 \le i \le s$.

The *index* $\mathrm{ind}(f_{\mathfrak{p}_i})$ is defined to be the length as an $\hat{A}_p$-module of $\mathcal{O}_{\mathfrak{p}_i}/\hat{A}_p[\theta_{\mathfrak{p}_i}]$, where $\mathcal{O}_{\mathfrak{p}_i}$ is the integral closure of $\hat{A}_p$ in $K_p(\theta_{\mathfrak{p}_i})$. The number $\mathrm{ind}(f_{\mathfrak{p}_i})$ may be expressed by a closed formula in terms of the data attached to $\mathbf{t}_i$:

$$\mathrm{ind}(f_{\mathfrak{p}_i}) = n_{\mathfrak{p}_i}\Big(e(\mathfrak{p}_i/p)^{-1} - 1 + \sum_{j=1}^{r}\Big(\frac{n_{\mathfrak{p}_i}}{m_j} - 1\Big)\frac{h_j}{e_1 \cdots e_j}\Big),$$

where e_j, f_j are the invariants of the type $\mathbf{t}_i$ and r is the Okutsu depth of $f_{\mathfrak{p}_i}$. Then, the valuation of the index $[\mathcal{O}_F : A[\theta]]$ at $p(t)$ may be computed as

$$v_p([\mathcal{O}_F : A[\theta]]) = \sum_{j=1}^{s} \operatorname{ind}(f_{\mathfrak{p}_j}) + \sum_{0 \le i < j \le s} v_p(\operatorname{Res}(f_{\mathfrak{p}_i}, f_{\mathfrak{p}_j})). \tag{1.5}$$

Details can be found in [13].

For $1 \le i, j \le s$ with $i \ne j$, we define the *index of coincidence* between the types $\mathbf{t}_i$ and $\mathbf{t}_j$ as

$$i(\mathbf{t}_i, \mathbf{t}_j) = \begin{cases} 0, & \text{if } \psi_{0,i} \ne \psi_{0,j} \\ \min\{l \in \mathbb{Z}_{>0} \mid (\phi_{l,i}, \lambda_{l,i}, \psi_{l,i}) \ne (\phi_{l,j}, \lambda_{l,j}, \psi_{l,j})\}, & \text{if } \psi_{0,i} = \psi_{0,j}. \end{cases}$$

Lemma 1.4.6. *Let $1 \le i, j \le s$ with $i \ne j$ and let $l = i(\mathbf{t}_i, \mathbf{t}_j)$ be their index of coincidence. Then,*

$$v_p(\operatorname{Res}(f_{\mathfrak{p}_i}, f_{\mathfrak{p}_j})) = \frac{n_{\mathfrak{p}_i} n_{\mathfrak{p}_j} \left(V_l + \min\left\{ \lambda_{\mathfrak{p}_i}^{\mathfrak{p}_j}, \lambda_{\mathfrak{p}_j}^{\mathfrak{p}_i} \right\} \right)}{e_1 \cdots e_{l-1} m_l},$$

where $\lambda_{\mathfrak{p}_i}^{\mathfrak{p}_j}, \lambda_{\mathfrak{p}_j}^{\mathfrak{p}_i} \in \mathbb{Q}$ are the hidden slopes *of the pair $(\mathbf{t}_i, \mathbf{t}_j)$, defined in [9].*

The hidden slopes are computed along the Montes algorithm; hence, according to the last lemma and (1.5) the integer $v_p([\mathcal{O}_F : A[\theta]])$ is computed by the Montes algorithm as a by-product.

If we consider f_∞ instead of f and and all f_∞-complete types $\mathbf{t}_1, \ldots, \mathbf{t}_s$, which correspond to all prime ideals of $\mathcal{O}_{F,\infty}$, we analogously obtain a concrete formula for $v_\infty([\mathcal{O}_{F,\infty} : A_\infty[\theta_\infty]])$.

Summarizing, the Montes algorithm computes the important invariants as the ramification index, the residual degree, and the "local indices" as a by-product.

Algorithm 1: Montes algorithm

Input: A defining polynomial f (resp. f_∞) of a function field F/k and a monic irreducible polynomial $p(t)$ in A (resp. t^{-1}).

Output: A family $\mathbf{t}_1, \ldots, \mathbf{t}_s$ of f-complete (resp. f_∞-complete) and optimal types, parameterizing the monic irreducible factors $f_{\mathfrak{p}_1}(x), \ldots, f_{\mathfrak{p}_s}(x)$ of f in $\hat{A}_p[x]$ (resp. of f_∞ in $\hat{A}_\infty[x]$).

1.4.4 Okutsu approximations

Denote $\mathfrak{p}$ a prime ideal of $\mathcal{O}_F$ over $p(t)$ (resp. of $\mathcal{O}_{F,\infty}$ over t^{-1}) and let

$$\mathbf{t}_\mathfrak{p} = (\psi_0; (\phi_1, \lambda_1, \psi_1); \ldots; (\phi_r, \lambda_r, \psi_r); (\phi_\mathfrak{p}, \lambda_{r+1}, \psi_\mathfrak{p}))$$

be an OM representation of $\mathfrak{p}$. The polynomial $\phi_\mathfrak{p}(x)$ is an *Okutsu approximation* to the $p(t)$-adic irreducible factor $f_\mathfrak{p}(x) := f_{\mathbf{t}_\mathfrak{p}}(x)$ [11, Sect. 4.1]. The value $\lambda_{r+1} = h_{r+1}$ is not a canonical invariant of $f_\mathfrak{p}$. It mesures how close is $\phi_\mathfrak{p}$ to $f_\mathfrak{p}$; we have $\phi_\mathfrak{p} = f_\mathfrak{p}$ if and only if $h_{r+1} = \infty$.

Later we will describe algorithms involving prime ideals (cf. Algorithm 8), which require the computation of an Okutsu approximation $\phi_\mathfrak{p}$ with sufficiently large value $\lambda_{r+1} = h_{r+1}$. This can be achieved by applying the *single-factor lifting* algorithm of [12], which improves the Okutsu approximation to $f_\mathfrak{p}$ with quadratic convergence; that is, doubling the value of h_{r+1} at each iteration. By [9, p. 744] it holds

$$v_\mathfrak{p}(\phi_\mathfrak{p}(\theta)) = V_{r+1} + \lambda_{r+1},$$

where $V_{r+1} = e_r f_r (e_r V_r + h_r)$ (cf. [1, p. 141]) is an invariant of the type $\mathbf{t}_\mathfrak{p}$. By [9, Proposition 4.7] the value $v_\mathfrak{q}(\phi_\mathfrak{p}(\theta))$ is given by a closed formula in terms of the data attached to the types $\mathbf{t}_\mathfrak{p}$, $\mathbf{t}_\mathfrak{q}$, for any prime ideal $\mathfrak{q}$ of $\mathcal{O}_F$ lying over $p(t)$ (resp. of $\mathcal{O}_{F,\infty}$ over $\mathfrak{m}_\infty$) different from $\mathfrak{p}$. Hence, the single-factor lifting algorithm can produce an element $\phi_\mathfrak{p}(\theta)$ in F with arbitrary large valuation at $\mathfrak{p}$ and constant value $v_\mathfrak{q}(\phi_\mathfrak{p}(\theta))$, for $\mathfrak{q}|p$ (resp. $\mathfrak{q}|\mathfrak{m}_\infty$) with $\mathfrak{q} \neq \mathfrak{p}$.

Algorithm 2: Single-factor lifting

Input: An OM representation $\mathbf{t}_\mathfrak{p}$ of a prime ideal $\mathfrak{p}$, with an Okutsu approximation $\phi_\mathfrak{p}$ and $h \in \mathbb{Z}$.

Output: An Okutsu approximation $\phi'_\mathfrak{p}$ with $v_\mathfrak{p}(\phi'_p(\theta)) \geq V_{r+1} + h$.

1.4.5 Divisor polynomials

The notion of *divisor polynomials* is due to Okutsu [28]. These polynomials will play a fundamental role in Chapter 5 in the context of the computation of bases of fractional ideals in function fields. The results are extracted from [11]. A comprehensive explanation and proofs can be found there.

For any prime ideal $\mathfrak{p}$ of F lying over $p(t)$ (resp. $\mathfrak{m}_\infty$), we consider the data

$$\mathbf{t}_\mathfrak{p},\ f_\mathfrak{p}(x),\ \phi_\mathfrak{p}.$$

Additionally, we choose a root $\theta_\mathfrak{p}$ in $\overline{K}_p$ (resp. $\overline{K}_\infty$) and consider the local field $\hat{F}_\mathfrak{p} := K_p(\theta_\mathfrak{p})$ (resp. $\hat{F}_\mathfrak{p} := K_\infty(\theta_\mathfrak{p})$). In particular, $\hat{F}_\mathfrak{p}$ is an extension of K_p (resp. K_∞) of degree $n_\mathfrak{p} = \deg f_\mathfrak{p}$. As before, we denote by v_p the discrete valuation on K induced by the monic and irreducible polynomial $p(t)$ and denote by $\hat{v}$ its canonical extension to an algebraic closure of K_p. The same applies to v_∞ and K_∞. Consider the topological embedding $\iota_\mathfrak{p} : F \hookrightarrow \hat{F}_\mathfrak{p}$, determined by $\theta \mapsto \theta_\mathfrak{p}$ (resp. $\theta_\infty \mapsto \theta_\mathfrak{p}$). Let v_0 be defined as in (1.2) and let $v_p = v_\infty$ if we consider $\hat{A}_\infty$.

Proposition 1.4.7. *For any integer $0 \leq m < n_\mathfrak{p}$, there exist a monic polynomial $g_m(x) \in \hat{A}_p[x]$ (resp. $\hat{A}_\infty[x]$) of degree m such that*

$$\hat{v}(g_m(\theta_\mathfrak{p})) \geq \hat{v}(g(\theta_\mathfrak{p})) - v_0(g(x)),$$

for all polynomials $g(x) \in \hat{A}_p[x]$ (resp. $\hat{A}_\infty[x]$) having degree m.

Note that the valuation condition from the last proposition do not depend on the choice of the root θ_p of $f_\mathfrak{p}$.

Definition 1.4.8. *We call $g_m(x)$ a* divisor polynomial *of degree m of $f_\mathfrak{p}$.*

Lemma 1.4.9. *Let $0 \leq i < j < n_\mathfrak{p}$ and $g_i(x), g_j(x)$ two divisor polynomials of $f_\mathfrak{p}$. Then,*

$$\hat{v}(g_j(\theta_\mathfrak{p})) \geq \hat{v}(g_i(\theta_\mathfrak{p})).$$

Proof. Since $x^{j-i}g_i(x) \in \hat{A}_p[x]$ is monic and has degree equal j, the last proposition shows that

$$\hat{v}(g_j(\theta_\mathfrak{p})) \geq \hat{v}(\theta_\mathfrak{p}^{j-i}g_i(\theta_\mathfrak{p})) \geq \hat{v}(g_i(\theta_\mathfrak{p})).$$

□

Let $\mathbf{t}_\mathfrak{p}$ be an OM representation of the prime ideal $\mathfrak{p}$ lying over $p(t)$, with ϕ-polynomials $\phi_1, \ldots, \phi_r$. We fix $\phi_0 := x$. Recall that $m_i = \deg \phi_i$, for $0 \leq i \leq r$.

Theorem 1.4.10. *For $0 < m < n_\mathfrak{p}$, we write uniquely*

$$m = \sum_{i=0}^{r} c_i m_i, \quad 0 \leq c_i < \frac{m_{i+1}}{m_i}.$$

Then, $g_m(x) := \prod_{i=0}^{r} \phi_i(x)^{c_i}$ is a divisor polynomial of degree m of $f_\mathfrak{p}$.

Definition 1.4.11. *For a prime ideal* $\mathfrak{p}$ *of* F *we define*

$$\mathcal{B}_{\mathfrak{p}} := \{1, g_1(x), \ldots, g_{n_{\mathfrak{p}}-1}(x)\}.$$

Note that, for a prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$, the set $\mathcal{B}_{\mathfrak{p}}$ is a subset of $A[x]$. For a prime ideal $\mathfrak{p}$ of $\mathcal{O}_{F,\infty}$, it holds $\mathcal{B}_{\mathfrak{p}} \subset A_\infty[x]$.

The set of all $g_m(\theta_{\mathfrak{p}})/p(t)^{\lfloor \hat{v}(g_m(\theta_{\mathfrak{p}}))\rfloor}$, for $0 \leq m < n_{\mathfrak{p}}$, is an $\hat{A}_p$-basis of the integral closure of $\hat{A}_p$ in the finite extension $K_p(\theta_p)$. This basis is called the *Okutsu basis* of $\mathfrak{p}$. Analogously, the set of all $g_m(\theta_{\mathfrak{p}})/t^{-\lfloor \hat{v}(g_m(\theta_{\mathfrak{p}}))\rfloor}$, $0 \leq m < n_{\mathfrak{p}}$, is an A_∞-basis of the integral closure of K_∞ in the finite extension $K_\infty(\theta_p)$.

2. Lattices over polynomial rings

The theory of lattices over the integers is an important tool in algebraic number theory. The notion of lattices over $\mathbb{Z}$ has an analogous concept, lattices over polynomial rings. The role of $\mathbb{Z}$ is played by $k[t]$, the polynomial ring in an indeterminate t over k. For this ground ring, the theory of lattices becomes simpler. For instance, the problem of finding a shortest vector in a lattice can be solved in polynomial time; whereas this particular problem shall be deemed to be difficult in a lattice over $\mathbb{Z}$. The theory of lattices over $k[t]$ is in substance due to Mahler [21]. In the end of the the 20^{th} century lattices over polynomial rings (or Puiseux series rings) were applied in order to factorize multivariate polynomials [18] and to compute Riemann-Roch spaces in algebraic function fields over $\mathbb{C}$ [30] or over $\mathbb{F}_q$ [31]. In that context it is necessary to determine a reduced basis (cf. Section 2.2) of a lattice. This led to several reduction algorithms [18, 24, 30, 31, 35]; that is, algorithms, which transform any basis of a lattice into a reduced one. While these methods cover particular cases we present a reduction algorithm, which determines a reduced basis in a general setting (cf. Section 2.7).

2.1 Lattices and normed spaces

Although for many applications it is sufficient to deal only with lattices over the polynomial ring $A = k[t]$, we consider a more general situation.

Let $K_\infty := k((t^{-1}))$ be the completion of K at the place P_∞. The valuation v_∞ extends in an obvious way to K_∞, and it determines a degree function on K_∞ as in Chapter 1: $|\ | := -v_\infty$. Let $\hat{A}_\infty \subset K_\infty$ be the valuation ring of v_∞, and $\hat{\mathfrak{m}}_\infty$ its maximal ideal.

Consider a principal ideal domain R with field of fractions $K_R \subset K_\infty$. Typical instances for R will be $R = A,\ A_\infty$, or $\hat{A}_\infty$.

Definition 2.1.1. *Let X be a finitely generated R-module. A* norm*, or* length function *on X is a mapping*

$$\| \| \colon X \longrightarrow \{-\infty\} \cup \mathbb{R}$$

satisfying the following conditions:

1. $\|x+y\| \leq \max\{\|x\|, \|y\|\}$*, for all* $x, y \in X$*,*
2. $\|ax\| = |a| + \|x\|$*, for all* $a \in R$*,* $x \in X$*,*
3. $\|x\| = -\infty$ *if and only if* $x = 0$*.*

Clearly, the degree function itself $| \, | : R \to \{-\infty\} \cup \mathbb{R}$ is a norm on R.

Remark 2.1.2. *Let $e > 1$ be a real number. By using $e^{|\ |}$ instead of $|\ |$, and $e^{\|\ \|}$ instead of $\|\ \|$, we would get the usual properties of a norm: $\|0\| = 0$, $\|ax\| = |a|\|x\|$. However, we prefer to use additive length functions because then $|a| \in \mathbb{Z}$ is the ordinary degree of a, for any $a \in K_\infty$. Another psychologically disturbing consequence of our choice is the fact that a lattice may have negative volume (cf. Section 2.5).*

Lemma 2.1.3. *Let X be a finitely generated R-module and $\| \| \colon X \longrightarrow \{-\infty\} \cup \mathbb{R}$ a norm on X, then for any $x_1, x_2 \in X$ with $\|x_1\| \neq \|x_2\|$ holds*

$$\|x_1 + x_2\| = \max\{\|x_1\|, \|x_2\|\}.$$

Proof. Since $\|x_1\| \neq \|x_2\|$, we can assume $\|x_1\| > \|x_2\|$. Suppose that $\|x_1 + x_2\| < \max\{\|x_1\|, \|x_2\|\} = \|x_1\|$. We obtain $\|x_1\| = \|(x_1+x_2)-x_2\| \leq \max\{\|x_1+x_2\|, \|x_2\|\} < \|x_1\|$, a contradiction. □

Definition 2.1.4. *Let X be a finitely generated R-module. For $r \in \mathbb{R}$ we define*

$$X_{\leq r} := \{x \in X \mid \|x\| \leq r\}, \qquad X_{<r} := \{x \in X \mid \|x\| < r\}.$$

Definition 2.1.5. *A* lattice *over R is a pair $(L, \| \|)$, where L is a finitely generated R-module, and $\| \|$ is a norm on L such that*

$$\dim_k L_{\leq r} < \infty, \qquad \text{for all } r \in \mathbb{R}.$$

For simplicity, we write L instead of $(L, \| \|)$.

Definition 2.1.6. *A* normed space over K_R *is a pair $(E, \| \|)$, where E is a finite dimensional K_R-vector space equipped with a norm $\| \|$ such that $(L, \| \|)$ is a lattice for all finitely generated R-submodules $L \subset E$ of full rank.*

Lemma 2.1.7. *Let E be a finite dimensional K_R-vector space equipped with a norm $\| \ \|$ admitting a lattice $(L, \| \ \|)$ with $L \subset E$ a full rank submodule. Then, $(E, \| \ \|)$ is a normed space.*

Proof. Let $L' \subset E$ be a finitely generated R-submodule of full rank. Since there exists an $a \in K_R \setminus \{0\}$ with $aL' \subset L$ and $(L, \| \ \|)$ is a lattice, we obtain

$$\dim_k L'_{\leq r} = \dim_k (aL')_{\leq r} < \infty, \quad \text{for all } r \in \mathbb{R}.$$

□

Clearly, if $(L, \| \ \|)$ is a lattice, then $L \otimes_R K_R$ is a normed space, with the norm function obtained by extending $\| \ \|$ in an obvious way. The second property in Definition 2.1.1 of a norm shows that L has no R-torsion, so that L is a free R-module and it is embedded into the normed space $L \otimes_R K_R$. Conversely, if $(E, \| \ \|)$ is a normed space, then any R-submodule of full rank is a lattice with the norm function obtained by restricting $\| \ \|$ to L.

As in Definition 2.1.1, many concepts can be introduced both for lattices and normed spaces. By the above considerations it is easy to deduce one from each other. In the sequel we give several definitions for lattices over A and we leave to the reader the formulation of similar concepts for more general lattices or normed spaces.

Definition 2.1.8. *A* lattice homomorphism *between two lattices, $(L, \| \ \|)$ and $(L', \| \ \|')$, is an A-linear map, $\varphi \colon L \longrightarrow L'$ such that $\|\varphi(x)\|' = \|x\|$, for all $x \in L$.*

A length-preserving A-module isomorphism is called an isometry *between $(L, \| \ \|)$ and $(L', \| \ \|')$.*

A morphism between two normed spaces $(E, \| \ \|)$ and $(E', \| \ \|')$ is a K-linear map $\varphi : E \to E'$ such that $\|\varphi(x)\|' = \|x\|$, for all $x \in E$.

A length-preserving K-isomorphism is called an *isometry* between $(E, \| \ \|)$ and $(E', \| \ \|')$.

Definition 2.1.9. *The* orthogonal sum *of two lattices $(L, \| \ \|)$, $(L', \| \ \|')$ is defined as:*

$$L \perp L' := (L \oplus L', \| \ \|), \quad \|(x, x')\| := \max\{\|x\|, \|x'\|'\},$$

for all $x \in L$, $x' \in L'$. Instead of $\perp_{i=1}^{n} L$ we write for simplicity L^n.

Definition 2.1.10. *Given a lattice $\mathcal{L} = (L, \| \ \|)$ and a real number r, we define the* twisted lattice $\mathcal{L}(r)$ *to be the pair $(L, \| \ \|')$, where $\|x\|' := \|x\| + r$, for all $x \in L$.*

We define in a completely analogous way the twisted normed space $\mathcal{E}(r)$ *of a given normed space $\mathcal{E} = (E, \| \ \|)$.*

Example 2.1.11. The lattice $\mathcal{O}$ is by definition the pair $(A, |\ |)$, where $|\ |$ is the ordinary degree function. Analogously, we define the normed space $\mathcal{K} = (K, |\ |)$.

Example 2.1.12. Let F/k be an algebraic function field and denote $\mathbb{P}_\infty(F)$ the set of places over P_∞ of F. Then,

$$\| \ \| := \min_{P \in \mathbb{P}_\infty(F)} \left\{ \frac{-v_P(\ )}{e(P/P_\infty)} \right\}$$

is a norm on F and $(F, \| \ \|)$ becomes a normed space over K (cf. Theorem 4.0.1).

Example 2.1.13. Let F/K be as in Example 2.1.12, and for each place P of F above P_∞ let $\hat{F}_P$ be the completion of F at P. The function $\| \ \|_P := -v_P(\ )/e(P/P_\infty)$ is a norm on the finite dimensional K_∞-vector space $\hat{F}_P$. By fixing embeddings $F \hookrightarrow \hat{F}_P$, we get a canonical embedding

$$F \hookrightarrow \perp_{P|P_\infty} \hat{F}_P, \quad x \mapsto (x, \ldots, x).$$

The induced structure of a normed space over K that F inherits from this embedding, coincides with that described in Example 2.1.12.

Lemma 2.1.14. *Let $(E, \| \ \|)$ be a normed space over K with $\dim_K E = n$ and $L \subset E$ an A-lattice. For $1 \leq i \leq n$, consider*

$$\mathcal{R}_i := \{\max\{\|x_1\|, \ldots, \|x_i\|\} \mid x_1, \ldots, x_i \in L \text{ are } A\text{-linearly independent } \}.$$

Then, $r_i := \inf(\mathcal{R}_i)$ exists and is attained by some vector in L.

Proof. Suppose $\lambda_1 > \lambda_2 > \ldots$ is a strictly decreasing sequence in $\mathcal{R}_i$. Then, we obtain a chain of k-vector spaces

$$L_{\leq \lambda_1} \supsetneq L_{\leq \lambda_2} \supsetneq \ldots.$$

This is a contradiction to the fact that L is a lattice. □

Definition 2.1.15 (Successive minima)**.** *Let $(L, \| \ \|)$ be a lattice of rank n. The* successive minima *of L are the real numbers $r_1 \leq \cdots \leq r_n$ defined as in Lemma 2.1.14. For each $1 \leq i \leq n$, the number r_i is minimal among all real numbers $r \in \mathbb{R}$ for which there exist A-linearly independent vectors $x_1, \ldots, x_i \in L_{\leq r}$.*

2.2 Reduced bases

We fix throughout this section a normed space $(E, \| \ \|)$ over K of dimension n. By a basis of E we mean a K-basis. By a basis of a lattice $L \subset E$ we mean an A-basis. Any basis of L is in particular a basis of E. Conversely, any basis $\mathcal{B}$ of E, is a basis of the lattice $L := \left\langle \mathcal{B} \right\rangle_A$, the A-submodule generated by $\mathcal{B}$.

Definition 2.2.1. *Let $\mathcal{B} = \{b_1, \ldots, b_m\}$ be a subset of E. We say that $\mathcal{B}$ is* reduced *if any of the following two equivalent conditions are satisfied:*

1. $\|a_1 b_1 + \cdots + a_m b_m\| = \max\limits_{1 \leq i \leq m} \{\|a_i b_i\|\}$, *for all* $a_1, \ldots, a_m \in K$.
2. $\|a_1 b_1 + \cdots + a_m b_m\| = \max\limits_{1 \leq i \leq m} \{\|a_i b_i\|\}$, *for all* $a_1, \ldots, a_m \in A$.

The following observations are an immediate consequence of the definition of reduceness.

Lemma 2.2.2.

1. *A reduced family is K-linearly independent.*
2. *Let $\mathcal{B} = \{b_1, \ldots, b_m\} \subset E$ be a reduced set. Then, for any $a_1, \ldots, a_m \in K^*$, the set $\{a_1 b_1, \ldots, a_m b_m\}$ is reduced.*

Definition 2.2.3. *A reduced basis of E is a reduced family of n vectors $\mathcal{B} = (b_1, \ldots, b_n)$.*

For a basis $\mathcal{B} = (b_1, \ldots, b_n) \in E^n$, denote by $c_{\mathcal{B}} : E \to K^n$ the K-isomorphism mapping $x \in E$ to its coordinates in K^n with respect to the basis $\mathcal{B}$.

Lemma 2.2.4. *Let $\mathcal{B} = (b_1, \ldots, b_n) \in E^n$ be a basis of E with the vectors ordered by increasing length:*

$$r_1 := \|b_1\| \leq \cdots \leq r_n := \|b_n\|.$$

Then, the following conditions are equivalent:

1. *$\mathcal{B}$ is a reduced basis of E.*
2. *$c_{\mathcal{B}} : E \to \mathcal{K}(r_1) \perp \cdots \perp \mathcal{K}(r_n)$ is an isometry.*
3. *The lattice $L := \left\langle \mathcal{B} \right\rangle_A$ is isometric to $\mathcal{O}(r_1) \perp \cdots \perp \mathcal{O}(r_n)$.*

Proof. The fact that $c_{\mathcal{B}}$ is an isometry is a reformulation of condition *1* of Definition 2.2.1. Analogously, the fact that the A-isomorphism

$$L \to A^n, \qquad \sum_{i=1}^{n} a_i b_i \mapsto (a_1, \ldots, a_n)$$

is an isometry between L and $\mathcal{O}(r_1) \perp \cdots \perp \mathcal{O}(r_n)$ is a reformulation of condition *2* of Definition 2.2.1 □

Proposition 2.2.5. *Let $\mathcal{B} = (b_1, \ldots, b_n) \in E^n$ be a reduced basis of E with*

$$r_1 := \|b_1\| \leq \cdots \leq r_n := \|b_n\|.$$

Let $L = \left\langle \mathcal{B} \right\rangle_A$ be the lattice generated by $\mathcal{B}$. Then,

1. *The set $\|E\| := \{\|x\| \mid x \in E\}$ of all lengths of vectors in E is the discrete subset:*

$$(\|E\| \setminus \{-\infty\})/\mathbb{Z} = (r_1 + \mathbb{Z}) \cup \cdots \cup (r_n + \mathbb{Z}) \subset \mathbb{R}/\mathbb{Z}.$$

2. *$r_1 \leq \cdots \leq r_n$ are the successive minima of L.*

3. *For any $r \in \mathbb{R}$, the following family is a k-basis of $L_{\leq r}$:*

$$\{b_i t^{j_i} \mid 1 \leq i \leq n, \quad 0 \leq j_i \leq \lfloor r - r_i \rfloor\}.$$

   In particular, take $r_0 := -\infty$, $r_{n+1} := \infty$ and let $0 \leq \kappa \leq n$ be the index for which $r_\kappa \leq r < r_{\kappa+1}$. Then,

$$\dim_k L_{\leq r} = \sum_{i=1}^{\kappa} (\lfloor r - r_i \rfloor + 1).$$

Proof. The length of any nonzero vector $x = \sum_{i=1}^{n} a_i b_i \in E$ is of the form

$$\|x\| = \max_{1 \leq i \leq n} \{\|a_i b_i\|\} = |a_j| + \|b_j\| = |a_j| + r_j \in r_j + \mathbb{Z}.$$

This proves the first item.

For any $1 \leq j \leq n$, the vectors $x = \sum_{i=1}^{n} a_i b_i \in L$ satisfying

$$\|b_j\| > \|x\| = \max_{1 \leq i \leq n} \{\|a_i b_i\|\}$$

lie necessarily in the submodule $\left\langle b_1, \ldots, b_{j-1} \right\rangle_A$. Hence, for any A-linearly independent family $x_1, \ldots, x_j \in L$, we know that

$$\max\{\|x_1\|, \ldots, \|x_j\|\} \geq \|b_j\|,$$

because the elements $x_1, \ldots, x_j$ cannot all lie in the submodule $\langle b_1, \ldots, b_{j-1} \rangle_A$, which has rank $j-1$. This proves the second item.

For the last statement, the element $x = \sum_{i=1}^{n} a_i b_i$ belongs to $L_{\leq r}$ if and only if

$$\|x\| = \max_{1 \leq i \leq n} \{\|a_i b_i\|\} \leq r.$$

This is equivalent to $a_{\kappa+1} = \cdots = a_n = 0$ and

$$|a_i| \leq r - r_i, \qquad 1 \leq i \leq \kappa.$$

The subset of all polynomials $a \in A$ satisfying $|a| \leq r - r_i$ is a k-vector subspace with basis $1, t, \ldots, t^{\lfloor r - r_i \rfloor}$. This ends the proof of the last item. □

The following observation is a direct consequence of item *1* of Proposition 2.2.5.

Lemma 2.2.6. *For any real numbers $r < s$, the set $\|E\| \cap [r, s]$ is finite.*

The most relevant property of a reduced basis is that the lengths of the vectors attain the successive minima of the lattice generated by the basis. Actually, this property characterizes reduceness as shown by Theorem 2.2.8 below. This fact guarantees the existence of reduced bases in any normed space.

Lemma 2.2.7. *Let $(L, \| \ \|)$ be a lattice and $r_1 \leq \cdots \leq r_n$ its successive minima. Choose $b_1 \ldots, b_m \in L$ such that $\|b_1\| = r_1, \ldots, \|b_m\| = r_m$. Then, $\{b_1, \ldots, b_m\}$ is reduced.*

Proof. We apply induction on m. Clearly, for $m = 1$ the statement is true.

Assume the statement holds for $m-1$. We take $a_1, \ldots, a_m \in A$ and set $u := a_1 b_1 + \cdots + a_{m-1} b_{m-1}$. We have to show that

$$\|u + a_m b_m\| = \max\{\|u\|, \|a_m b_m\|\},$$

since by induction hypothesis it holds $\|u\| = \max_{1 \leq i < m}\{\|a_i b_i\|\}$. For $\|u\| \neq \|a_m b_m\|$ the statement yields by Lemma 2.1.3.

Suppose $\|u\| = \|a_m b_m\| = |a_m| + r_m$ and $\|u + a_m b_m\| < \max\{\|u\|, \|a_m b_m\|\} = \|u\|$. In particular, we have $a_m \neq 0$. We write $a_m := \lambda_m t^{\alpha_m} + a'_m$, where $\lambda_m \in k^*$ and $|a'_m| < |a_m| =: \alpha_m$. We fix $I := \{1 \leq j < m \mid \|a_i b_i\| = \|u\|\}$. For $j \in I$ we write $a_i := \lambda_i t^{\alpha_i} + a'_i$, where $\lambda_i \in k^*$ and $|a'_i| < |a_i| =: \alpha_i$. Then,

$$u + a_m b_m = \sum_{i \in I} \lambda_i t^{\alpha_i} b_i + \lambda_m t^{\alpha_m} b_m + u',$$

where u' collects all summands with strictly lower norm than $\|u\|$. We set $u_0 := \sum_{i\in I} \lambda_i t^{\alpha_i} b_i$. Since $\|u + a_m b_m\| < \|u\|$, we obtain

$$\|u_0 + \lambda_m t^{\alpha_m} b_m\| < \|u\| = |a_i| + r_i = \alpha_i + r_i, \ \forall i \in I \cup \{m\}. \tag{2.1}$$

Since $r_i \leq r_m$, we have $\alpha_m \leq \alpha_i$ for $i \in I$. By (2.1) we deduce $b := t^{-\alpha_m} u_0 + \lambda_m b_m \in L$ with $\|b\| = -\alpha_m + \|u_0 + \lambda_m t^{\alpha_m} b_m\| < r_m$. Since $b_1, \dots b_{m-1}, b$ are linearly independent in L, we have a contradiction to the minimality of r_m. □

Theorem 2.2.8. *Let $L \subset E$ be a lattice and $r_1 \leq \cdots \leq r_n$ its successive minima. Let $\mathcal{B} = (b_1, \dots, b_n)$ be a family of elements in L such that $\|b_i\| = r_i$, for all $1 \leq i \leq n$. Then, $\mathcal{B}$ is a reduced basis of L.*

Proof. From Lemmas 2.2.2 and 2.2.7 we know that $\mathcal{B}$ is reduced and a linearly independent family. Thus, we only have to show that $\mathcal{B}$ generates L.

Assume there exists an element $b \in L$ with $b \notin \left\langle \mathcal{B} \right\rangle_A$. Since $\mathcal{B}$ is a K-basis of E, we obtain $b = \sum_{i=1}^{n} \lambda_i b_i$ with at least one $\lambda_i \in K \setminus A$. We set $I := \{1 \leq i \leq n \mid \lambda_i \notin A\}$ and consider

$$\sum_{i\in I} \lambda_i b_i = b - \sum_{i\in\{1,\dots,n\}\setminus I} \lambda_i b_i \in L. \tag{2.2}$$

As the set $\mathcal{B}$ is reduced, it holds

$$\Big\| \sum_{i\in I} \lambda_i b_i \Big\| = \max_{i\in I}\{\|\lambda_i b_i\|\} = \|\lambda_j b_j\|,$$

for some $j \in I$. If $|\lambda_j| \geq 0$ we can write $\lambda_j = a + \lambda_j'$ with $a \in A$ and $\lambda_j' \in \mathfrak{m}_\infty$ and subtract ab_j in (2.2) from both sides. Therefore, we can assume that $|\lambda_j| < 0$ and get $\|\sum_{i\in I} \lambda_i b_i\| < \|b_j\| = r_j$. By setting $b_j' := \sum_{i\in I} \lambda_i b_i$, we obtain the set $\{b_1, \dots, b_{j-1}, b_j', b_{j+1}, \dots, b_n\}$ of A-linearly independent elements in L. This is in contradiction with the minimality of $\|b_j\| = r_j$. □

Normed spaces always admit reduced bases, and this is a crucial property, which follows immediately from the last theorem.

Corollary 2.2.9. *Every lattice admits a reduced basis.*

2.3 Reduceness criteria

In this section we define a reduction map, which leads us to a practical criterion to check wether a basis in a normed space $(E, \| \ \|)$ is reduced or not. For any $r \in \mathbb{R}$ the subspaces

$$E_{\leq r} = \{x \in E \mid \|x\| \leq r\} \supset E_{<r} = \{x \in E \mid \|x\| < r\}$$

are A_∞-submodules of E such that $\mathfrak{m}_\infty E_{\leq r} \subset E_{<r}$. Their quotient,

$$V_r := E_{\leq r}/E_{<r}$$

is a k-vector space, and it admits a kind of *reduction map*:

$$\mathrm{red}_r \colon E_{\leq r} \longrightarrow V_r, \quad x \mapsto x + E_{<r}.$$

Clearly, V_r is nonzero if and only if $r \in \|E\|$.

Definition 2.3.1. *For any $\mathcal{B} \subset E$ and $\rho \in \mathbb{R}/\mathbb{Z}$, we denote*

$$\mathcal{B}_\rho := \{b \in \mathcal{B} \mid \|b\| + \mathbb{Z} = \rho\}.$$

Clearly, if $\mathcal{B}$ does not contain the zero vector, then $\mathcal{B}$ admits a partition:

$$\mathcal{B} = \bigcup_{\rho \in \mathbb{R}/\mathbb{Z}} \mathcal{B}_\rho.$$

By item *1* of Proposition 2.2.5, only a finite number of subsets $\mathcal{B}_\rho$ are nonempty.

Lemma 2.3.2. *Let $\mathcal{B} = (b_1, \ldots, b_n)$ be a basis of E, and let $\mathcal{B} = \bigcup_{\rho \in \mathbb{R}/\mathbb{Z}} \mathcal{B}_\rho$ be the partition determined by classifying all vectors in $\mathcal{B}$ according to its length modulo $\mathbb{Z}$. Then, $\mathcal{B}$ is reduced if and only if all subsets $\mathcal{B}_\rho$ are reduced.*

Proof. Any subset of a reduced family is reduced. Thus, we need only to show that $\mathcal{B}$ is reduced if all $\mathcal{B}_\rho$ are reduced.

Let $I := \{\rho \in \mathbb{R}/\mathbb{Z} \mid \mathcal{B}_\rho \neq \emptyset\}$. We have $E = \bigoplus_{\rho \in I} E_\rho$, where E_ρ is the subspace of E generated by $\mathcal{B}_\rho$. Take $a_1, \ldots, a_n \in K$ and let $x = \sum_{i=1}^n a_i b_i$. This element splits as $x = \sum_{\rho \in I} x_\rho$, where $x_\rho = \sum_{b_i \in \mathcal{B}_\rho} a_i b_i$. Since all values $\|x_\rho\|$ are different (because $\|a_i b_i\| \equiv \|b_i\| \bmod \mathbb{Z}$), we have $\|x\| = \max_{\rho \in I}\{\|x_\rho\|\}$. On the other hand, since all $\mathcal{B}_\rho$ are reduced, we have $\|x_\rho\| = \max_{b_i \in \mathcal{B}_\rho}\{\|a_i b_i\|\}$. Thus, $\mathcal{B}$ is reduced. □

The next result is inspired by a criterion of W.M. Schmidt [30, 31], which was developed in the context of Puiseux expansions of functions in function fields.

Theorem 2.3.3. *Let $\mathcal{B}$ be a basis of E, $I := \{\|b\| + \mathbb{Z} \mid b \in \mathcal{B}\} \subset \mathbb{R}/\mathbb{Z}$, and let $\mathcal{B} = \bigcup_{\rho \in I} \mathcal{B}_\rho$ be the partition determined by classifying all vectors in $\mathcal{B}$ according to its length modulo $\mathbb{Z}$. For each $\rho \in I$ choose a real number $r \in \rho$, and write*

$$\|b\| = r - m_b, \quad m_b \in \mathbb{Z}, \quad \textit{for all } b \in \mathcal{B}_\rho.$$

Then, $\mathcal{B}$ is reduced if and only if the elements $\{\mathrm{red}_r(t^{m_b} b) \mid b \in \mathcal{B}_\rho\} \subset V_r$ are k-linearly independent for all $\rho \in I$.

Proof. By Lemma 2.3.2 we can assume that all elements in $\mathcal{B}$ have the same length modulo $\mathbb{Z}$. Thus, $I = \{\rho\}$ contains a single element and $\|t^{m_b} b\| = r$ for all $b \in \mathcal{B}$.

By Lemma 2.2.2, $\mathcal{B}$ is reduced if and only if $\{t^{m_b} b \mid b \in \mathcal{B}\}$ is reduced. Thus, we may assume that $m_b = 0$ for all $b \in \mathcal{B}$; or equivalently, $\|b\| = r$ for all $b \in \mathcal{B}$.

Suppose $\mathcal{B}$ is reduced. Let $(\epsilon_b)_{b \in \mathcal{B}}$ be a family of elements in k, not all of them equal to zero. By reduceness,

$$\left\| \sum\nolimits_{b \in \mathcal{B}} \epsilon_b b \right\| = \max\nolimits_{b \in \mathcal{B}} \{\|\epsilon_b b\|\} = r. \tag{2.3}$$

Hence, the family $\{\mathrm{red}_r(b) \mid b \in \mathcal{B}\} \subset V_r$ is k-linearly independent.

Conversely, suppose that this family is k-linearly independent. Then, (2.3) holds for any family $(\epsilon_b)_{b \in \mathcal{B}}$ of elements in k, not all of them equal to zero. Now, let $(a_b)_{b \in \mathcal{B}}$ be a family of elements in K, not all of them equal to zero. Let $m = \max_{b \in \mathcal{B}} \{|a_b|\}$, and $\mathcal{C} = \{b \in \mathcal{B} \mid |a_b| = m\}$. Clearly, $\max_{b \in \mathcal{B}} \{\|a_b b\|\} = m + r$, and we want to show that $\| \sum_{b \in \mathcal{B}} a_b b\| = m + r$. Since $\| \sum_{b \notin \mathcal{C}} a_b b\| < m + r$, it is sufficient to check that $\| \sum_{b \in \mathcal{C}} a_b b\| = m + r$. For all $b \in \mathcal{C}$, if we write $a_b = \epsilon_b t^m + a'_b$, with $|a'_b| < m$, we have again $\| \sum_{b \in \mathcal{C}} a'_b b\| < m + r$, so that we need only to show that $\| \sum_{b \in \mathcal{C}} \epsilon_b t^m b\| = m + r$, which is true by (2.3). Thus, $\mathcal{B}$ is reduced. □

Corollary 2.3.4. *Let $\mathcal{B}$ be a reduced basis of E, and $r \in \|E\|$. Consider the subset $\mathcal{C} := \{b \in \mathcal{B} \mid \|b\| \equiv r \bmod \mathbb{Z}\}$, and write*

$$\|b\| = r - m_b, \quad m_b \in \mathbb{Z}, \quad \textit{for all } b \in \mathcal{C}.$$

Then, $(\mathrm{red}_r(t^{m_b} b) \mid b \in \mathcal{C})$ is a k-basis of V_r. In particular, it holds $\dim_k V_r = \#\mathcal{C}$.

Proof. By the previous theorem, this family is k-linearly independent. Let us show that it generates V_r as well. Suppose $x \in E$ has $\|x\| = r$, and write it as $x = \sum_{b \in \mathcal{B}} a_b b$, for some $a_b \in K$. By reduceness,

$$r = \|x\| = \max_{b \in \mathcal{B}} \{\|a_b b\|\} = \max_{b \in \mathcal{C}} \{\|a_b b\|\} = r + \max_{b \in \mathcal{C}} \{|a_b t^{-m_b}|\}.$$

Hence, $|a_b| \leq m_b$ for all $b \in \mathcal{C}$ and $\mathcal{C}' := \{b \in \mathcal{C} \mid |a_b| = m_b\} \neq \emptyset$. For every $b \in \mathcal{C}$ we write $a_b = \epsilon_b t^{m_b} + a'_b$, with $\epsilon_b \in k^*$ and $|a'_b| < m_b$. Arguing as we did at the end of the proof of Theorem 2.3.3, we see that $x \in \sum_{b \in \mathcal{C}'} \epsilon_b t^{m_b} b + E_{<r}$. □

Notation 2.3.5. *Let L be a lattice of rank n, and $r_1 \leq \cdots \leq r_n$ its successive minima. We denote by*

$$\mathrm{sm}(L) = (r_1, \ldots, r_n), \quad \overline{\mathrm{sm}}(L) = \{r_1 + \mathbb{Z}, \ldots, r_n + \mathbb{Z}\},$$

the vector of successive minima of L and the multiset formed by their classes in $\mathbb{R}/\mathbb{Z}$.

Lemma 2.3.6. *Let E be a normed space. All lattices $L \subset E$ have the same multiset $\overline{\mathrm{sm}}(L)$. We denote by $\mathrm{sm}(E)$ this common multiset.*

Proof. Let L be a lattice in $(E, \| \ \|)$. By Corollary 2.2.9 there exists a reduced basis $\mathcal{B} = (b_1, \ldots, b_n)$ of L. By Proposition 2.2.5, the underlying set of $\overline{\mathrm{sm}}(L)$ coincides with the image of the set $\|E\| \setminus \{-\infty\}$ under the mapping $\mathbb{R} \to \mathbb{R}/\mathbb{Z}$. Finally, for each $\rho = r_i + \mathbb{Z}$ with $r_i \in \mathbb{R}$, the multiplicity of ρ as an element of the multiset $\overline{\mathrm{sm}}(L)$ is the cardinality of the set $\mathcal{B}_\rho$ from Definition 2.3.1. By Corollary 2.3.4 this multiplicity is $\#\mathcal{B}_\rho = \dim_k V_r$, for any $r \in \rho$. Thus, the set $\overline{\mathrm{sm}}(L)$ depends only on E and not on L. □

Corollary 2.3.7.

Two lattices L, L' are isometric if and only if $\mathrm{sm}(L) = \mathrm{sm}(L')$.

Two normed spaces E, E' are isometric if and only if $\mathrm{sm}(E) = \mathrm{sm}(E')$.

Proof. By the existence of reduced bases, Lemma 2.2.4 and Proposition 2.2.5, the two statements are equivalent to:

$$\mathcal{O}(r) \cong \mathcal{O}(r') \Longleftrightarrow r = r'$$
$$\mathcal{K}(r) \cong \mathcal{K}(r') \Longleftrightarrow r + \mathbb{Z} = r' + \mathbb{Z},$$

respectively, for any given real numbers $r, r' \in \mathbb{R}$. These equivalences are an immediate consequence of $\mathrm{Aut}_A(A) = k^*$ and $\mathrm{Aut}_K(K) = K^*$, respectively. □

2.4 Orthonormal bases and isometry group

Definition 2.4.1. *Let E be a normed space and $\mathcal{B} = (b_1, \ldots, b_n)$ a reduced basis of E. We say that $\mathcal{B}$ is* orthonormal *if $-1 < \|b_1\| \leq \cdots \leq \|b_n\| \leq 0$.*

Clearly, two orthonormal bases of the same normed space E have the same multiset of lengths of their vectors.

The aim of this section is to describe maps between normed spaces. In particular, we want to derive properties of the transition matrices between orthonormal bases.

Definition 2.4.2. *The set of all isometries* $(E, \| \ \|) \to (E, \| \ \|)$ *is denoted by* $\mathrm{Aut}(E, \| \ \|)$.

This set has a natural group structure. We call it the *isometry group* on the normed space $(E, \| \ \|)$.

Lemma 2.4.3. *Every morphism of normed spaces is injective and maps a reduced set to a reduced one.*

Proof. Let $(E, \| \ \|)$ and $(E', \| \ \|')$ be normed spaces and $\{b_1, \ldots, b_m\}$ be a reduced set in E. We consider a morphism φ from $(E, \| \ \|)$ to $(E', \| \ \|')$. Since φ preserves the length of the vectors, necessarily $\mathrm{Ker}(\varphi) = \{0\}$ and φ is injective. For any $\lambda_1, \ldots, \lambda_m \in K$ it holds

$$\Big\| \sum_{i=1}^{m} \lambda_i \varphi(b_i) \Big\|' = \Big\| \sum_{i=1}^{m} \lambda_i b_i \Big\| = \max_{1 \le i \le m} \{\|\lambda_i b_i\|\} = \max_{1 \le i \le m} \{\|\lambda_i \varphi(b_i)\|'\},$$

so that the set $\varphi(\mathcal{B})$ is reduced. □

Lemma 2.4.4. *Let* $(E, \| \ \|)$ *and* $(E', \| \ \|')$ *be normed spaces with* $\mathrm{sm}(E) = \mathrm{sm}(E')$ *and* $\varphi : E \to E'$ *be a* K*-linear map. Then, the following statements are equivalent:*

1. *The map* φ *is an isometry.*
2. *The map* φ *sends orthonormal bases of* E *to orthonormal bases of* E'*.*
3. *The map* φ *sends a fixed orthonormal basis of* E *to an orthonormal basis of* E'*.*

Proof. The first statement implies the second one by Lemma 2.4.3, and the second one implies trivially the third one.

We show that the third statement implies the first one. Since φ maps an orthonormal basis $\mathcal{B} = (b_1, \ldots, b_n)$ of E to an orthonormal basis $\varphi(\mathcal{B})$ of E', the K-linear map φ is an isomorphism. As $\mathrm{sm}(E) = \mathrm{sm}(E')$, the two sequences of lengths

$$-1 < \|b_1\| \le \cdots \le \|b_n\| \le 0, \quad -1 < \|\varphi(b_1)\|' \le \cdots \le \|\varphi(b_n)\|' \le 0$$

coincide. Therefore, for any $x \in E$ with $x = \sum_{i=1}^{n} \lambda_i b_i$, we have

$$\|x\| = \max_{1 \le i \le n} \{\|\lambda_i b_i\|\} = \max_{1 \le i \le n} \{\|\lambda_i \varphi(b_i)\|'\} = \Big\| \sum_{i=1}^{n} \lambda_i \varphi(b_i) \Big\|' = \|\varphi(x)\|'.$$

□

Definition 2.4.5. *Let $m = m_1 + \cdots + m_\kappa$ be a partition of a positive integer m into a sum of positive integers. Let T be an $m \times m$ matrix with entries in A_∞. The partition of m determines a decomposition of T into blocks:*

$$T = (T_{ij}), \quad T_{ij} \in A_\infty^{m_i \times m_j},\ 1 \leq i, j \leq \kappa.$$

The orthonormal group $O(m_1, \ldots, m_\kappa, A_\infty)$ *is the set of all $T \in A_\infty^{m \times m}$, which satisfy the following two conditions:*

1. $T_{ii} \in \mathrm{GL}_{m_i}(A_\infty)$, *for all* $1 \leq i \leq \kappa$.
2. $T_{ij} \in \mathfrak{m}_\infty^{m_i \times m_j}$, *for all* $j > i$.

Theorem 2.4.6. *The* orthogonal group $O(m_1, \ldots, m_\kappa, A_\infty)$ *is a subgroup of* $\mathrm{GL}_m(A_\infty)$. *In particular, the determinant of a matrix in* $O(m_1, \ldots, m_\kappa, K)$ *belongs to* U_∞.

Proof. The image of $T \in O(m_1, \ldots, m_\kappa, A_\infty)$ under the reduction homomorphism $A_\infty \to A_\infty/\mathfrak{m}_\infty \cong k$ is an invertible matrix; hence $\det T \in U_\infty$ and T is an invertible matrix. On the other hand, it is clear that $O(m_1, \ldots, m_\kappa, A_\infty)$ is stable under matrix multiplication and inversion. □

Theorem 2.4.7. $\mathrm{Aut}(\mathcal{K}^n) = \mathrm{GL}_n(A_\infty)$.

Proof. Denote $\| \ \|$ the norm of the normed space $\mathcal{K}^n$. Then, $\mathcal{K}^n = (K^n, \| \ \|)$ with $\|(\lambda_1, \ldots, \lambda_n)\| = \max_{1 \leq i \leq n}\{|\lambda_i|\}$. For $T \in \mathrm{GL}_n(K)$ the map $T : K^n \to K^n$ is an isomorphism. Denote by $\mathcal{B} = (e_1, \ldots, e_n)$ the standard basis of K^n. Since $\mathcal{B}$ is an orthonormal basis of $\mathcal{K}^n$, by Lemma 2.4.4, the map T is an isometry if and only if $\mathcal{B}' := (e_1T, \ldots, e_nT)$ is an orthonormal basis. That is, for an isometry T the rows built an orthonormal basis and have in particular length equal 0; hence $T \in \mathrm{GL}_n(K) \cap A_\infty^{n \times n}$. We apply Theorem 2.3.3 to the rows $T_1, \ldots, T_n$ of T. Then, T is an isometry if and only if the rows of T are linearly independent mod $\mathfrak{m}_\infty^n$. This is equivalent to the fact that $T_1 \bmod \mathfrak{m}_\infty^n, \ldots, T_n \bmod \mathfrak{m}_\infty^n$ are linearly independent over $A_\infty/\mathfrak{m}_\infty \cong k$. Clearly, the last statement holds if and only if $\det T \notin \mathfrak{m}_\infty$ or rather $|\det T| = 0$. Thus, we have shown that T is an isometry if and only if $T \in \mathrm{GL}_n(A_\infty)$. □

Corollary 2.4.8. *For $r \in \mathbb{R}$ it holds* $\mathrm{Aut}(\mathcal{K}^n(r)) = \mathrm{GL}_n(A_\infty)$.

Proof. Denote $\| \ \|$ the norm of the normed space $\mathcal{K}^n$ and $\| \ \|'$ the norm of $\mathcal{K}^n(r)$. By definition it holds $\| \ \|' = \| \ \| + r$. Then, we prove the statement analogously to the proof of Theorem 2.4.7, having in mind that an orthonormal basis of $\mathcal{K}^n(r)$ is $t^{-\lceil r \rceil}\mathcal{B}$, where $\mathcal{B}$ is the standard basis of $\mathcal{K}^n$. □

Theorem 2.4.9. *Let $-1 < r_1 < \cdots < r_\kappa \leq 0$ be a sequence of real numbers. Then, for $m_1, \ldots, m_\kappa \in \mathbb{Z}_{>0}$ it holds*

$$\mathrm{Aut}(\perp_{i=1}^{\kappa} \mathcal{K}^{m_i}(r_i)) = O(m_1, \ldots, m_\kappa, A_\infty).$$

Proof. Let $E' := \perp_{i=1}^{\kappa} \mathcal{K}^{m_i}(r_i)$ and denote by $\| \ \|$ the norm on E'. Note that the norm is defined by

$$\|(z_1, \ldots, z_n)\| = \max\{|z_1| + r_1, \ldots, |z_{m_1}| + r_1, \ldots, |z_{n-m_\kappa+1}| + r_\kappa, \ldots, |z_n| + r_\kappa\}. \tag{2.4}$$

By Lemma 2.4.4 $\mathrm{Aut}(E')$ consists of the matrices $T \in \mathrm{GL}_n(K)$ whose rows form an orthonormal basis of E'. Let us show that this property characterizes the matrices in $O(m_1, \ldots, m_\kappa, A_\infty)$. To this end, we will use the following:

Claim:

Let $i \in \{1, \ldots, \kappa\}$ and $b_1, \ldots, b_{m_i} \in E'$. It holds $\|b_1\| = \cdots = \|b_{m_i}\| = r_i$, and $\mathrm{red}_{r_i}(b_1), \ldots, \mathrm{red}_{r_i}(b_{m_i})$ are k-linearly independent if and only if the following two conditions are satisfied:

1. $b_l = (b_{1,l}, \ldots, b_{n,l}) \in A_\infty^n$, for all $1 \leq l \leq m_i$ and $b_{j,l} \in \mathfrak{m}_\infty$, for $m + m_i < j \leq n$ with $m := \sum_{j=1}^{i-1} m_j$.

2. $Q := (b_{j,l} \mid 1 \leq l \leq m_i, m < j \leq m + m_i) \in \mathrm{GL}_{m_i}(A_\infty)$.

The statement of the theorem follows immediately from the claim. In fact, for any $T \in \mathrm{Aut}(E')$, Lemma 2.3.2 and Theorem 2.3.3 show that the rows of T form an orthonormal basis of E' if and only if the κ subfamilies of the set of rows determined by the partition $n = m_1 + \cdots + m_\kappa$ satisfy the condition of the claim. By the claim this is equivalent to $T \in O(m_1, \ldots, m_\kappa, A_\infty)$ (cf. Definition 2.4.5).

We have to prove the claim. By (2.4), $\|b_l\| = r_i$, for $1 \leq l \leq m_i$, is equivalent to item 1, since $-1 < r_1 < \cdots < r_\kappa \leq 0$.

Note that $b_{j,l}e_j \in E_{<r_i}$, for all $1 \leq j \leq m$ (because $|b_{j,l}| \leq 0$, $\|e_j\| < r_i$) and for all $m + m_i < j \leq n$ (because $|b_{j,l}| \leq -1$, $\|e_j\| = r_i < r_i + 1$).

For $g \in U_\infty$, denote by $\mathrm{LC}(g) \in k^*$, the quotient of the leading coefficient of the numerator and denominator of g; for $g \in \mathfrak{m}_\infty$, we set $\mathrm{LC}(g) := 0$. Clearly, $g \in \mathrm{LC}(g) + \mathfrak{m}_\infty$, for all $g \in A_\infty$. The above remarks show that

$$b_l = \sum_{j=1}^{n} b_{j,l} e_j \in \sum_{j=m+1}^{m+m_i} \mathrm{LC}(b_{j,l}) e_j + E_{<r_i},$$

for $1 \leq l \leq m_i$. Clearly, $\mathrm{red}_{r_i}(b_1), \ldots, \mathrm{red}_{r_i}(b_{m_i})$ are k-linearly independent if and only if the determinant of $Q' := (\mathrm{LC}(b_{j,l})_{1 \leq l \leq m_i, m+1 \leq j \leq m+m_i})$ belongs to k^*. The last statement is equivalent to $Q \in \mathrm{GL}_{m_i}(A_\infty)$. This finishes the proof of the claim. □

Since every normed space $(E, \| \ \|)$ is isometric to some $\perp_{i=1}^{\kappa} \mathcal{K}^{m_i}(r_i)$ (Lemma 2.2.4), Theorem 2.4.9 reveals the general structure of $\mathrm{Aut}(E, \| \ \|)$.

Lemma 2.4.10. *Let $\mathcal{B}'$ be an orthonormal basis of E and let $m_1, \ldots, m_\kappa$ be the multiplicities of the lengths of the vectors of $\mathcal{B}'$. Then, a basis $\mathcal{B}$ of E is orthonormal if and only if the transition matrix from $\mathcal{B}$ to $\mathcal{B}'$ belongs to $O(m_1, \ldots, m_\kappa, A_\infty)$.*

Proof. Denote $E' := \perp_{i=1}^{\kappa} \mathcal{K}^{m_i}(r_i)$, where $r_1, \ldots, r_\kappa$ are the pairwise different lengths of the vectors in $\mathcal{B}'$. The transition matrix T from $\mathcal{B}$ to $\mathcal{B}'$ determines a K-isomorphism $T : E' \to E'$ fitting into the following commutative diagram:

$$\begin{array}{ccc} E & \xrightarrow{c_{\mathcal{B}}} & E' \\ & \searrow^{c_{\mathcal{B}'}} & \downarrow T \\ & & E' \end{array}$$

By Lemma 2.2.4, $c_{\mathcal{B}'}$ is an isometry. Hence, T is an isometry if and only if $c_{\mathcal{B}}$ is an isometry. By Theorem 2.4.9, T is an isometry if and only if $T \in O(m_1, \ldots, m_\kappa, A_\infty)$. Since $c_{\mathcal{B}}^{-1}$ sends the standard basis of K^n to $\mathcal{B}$, Lemma 2.4.4 shows that $c_{\mathcal{B}}^{-1}$ is an isometry if and only if $\mathcal{B}$ is an orthonormal basis. This proves the lemma. □

Definition 2.4.11. *Let $\mathcal{B}$ be an orthonormal basis of a normed space E. The* signature *of E is defined to be*

$$\mathrm{Sig}(E) := \{\|b\| + \mathbb{Z} \mid b \in \mathcal{B}\} \subset \mathbb{R}/\mathbb{Z}.$$

Clearly, this definition is independent of the choice of the orthonormal basis $\mathcal{B}$. Actually, $\mathrm{Sig}(E)$ is the underlying set of the multiset $\mathrm{sm}(E)$, as we saw in Lemma 2.3.6.

2.5 Determinant and orthogonal defect

In this section we define certain invariants for lattices and normed spaces, the determinant of a lattice and the orthogonal defect of a basis.

Definition 2.5.1 (Volume)**.** *Let E be a normed space and $\mathcal{B}$ be a basis of E. We define the* volume *of $\mathcal{B}$ as* $\mathrm{vol}(\mathcal{B}) := \sum_{b\in\mathcal{B}} \|b\|$.

We define the volume *of E as the volume of any orthonormal basis of E. The* volume *of a lattice L is defined to be the volume of a reduced basis of L. We use the notation* $\mathrm{vol}(E)$ *and* $\mathrm{vol}(L)$*, respectively.*

Definition 2.5.2 (Determinant)**.** *Let $\mathcal{B}$ be a basis of a normed space E. We define the* determinant *of $\mathcal{B}$ to be the index*

$$d(\mathcal{B}) := \left[\left\langle\, \mathcal{B}' \,\right\rangle_A : \left\langle\, \mathcal{B} \,\right\rangle_A\right] \in I_A,$$

where $\mathcal{B}'$ is an orthonormal basis of E.

Definition 2.5.3. *Let L be a lattice inside a normed space E. We define $d(L) \in I_A$ to be the determinant of any basis of L. We call $d(L)$ the* determinant *of L.*

Lemma 2.5.4 (Hadamard's inequality)**.** *Let $\mathcal{B}$ be a basis of E. Then,*

$$|d(\mathcal{B})| \leq \mathrm{vol}(\mathcal{B}) - \mathrm{vol}(E).$$

Proof. Let $\mathcal{B} = (b_1, \ldots, b_n)$ and let $\mathcal{B}' = (b'_1, \ldots, b'_n)$ be an orthonormal basis of E. Let $T = (t_{i,j})$ be the transition matrix from $\mathcal{B}$ to $\mathcal{B}'$. Since $\mathcal{B}'$ is reduced, for every $1 \leq i, j \leq n$, we have

$$\|t_{j,i} b'_i\| \leq \max_{1\leq k\leq n} \{\|t_{j,k} b'_k\|\} = \|b_j\|.$$

Hence, every summand of $\det T$, corresponding to a permutation τ of the set $\{1, \ldots, n\}$, has degree:

$$\begin{aligned} |t_{1,\tau(1)} \cdots t_{n,\tau(n)}| &= |t_{1,\tau(1)}| + \cdots + |t_{n,\tau(n)}| \\ &\leq \|b_1\| - \|b'_{\tau(1)}\| + \cdots + \|b_n\| - \|b'_{\tau(n)}\| \\ &= \mathrm{vol}(\mathcal{B}) - \mathrm{vol}(E). \end{aligned}$$

Thus, $|\det T| \leq \mathrm{vol}(\mathcal{B}) - \mathrm{vol}(E)$. □

Definition 2.5.5 (Orthogonal defect)**.** *The difference*

$$\mathrm{OD}(\mathcal{B}) := \mathrm{vol}(\mathcal{B}) - \mathrm{vol}(E) - |d(\mathcal{B})| \geq 0$$

is called the orthogonal defect *of $\mathcal{B}$.*

If $\mathcal{B}$ is orthonormal, then $\mathrm{vol}(B) = \mathrm{vol}(E)$ and $|d(\mathcal{B})| = 0$, so that $\mathrm{OD}(\mathcal{B}) = 0$.

Lemma 2.5.6. *Let $\mathcal{B} = (b_1, \dots, b_n)$ be a basis of E. Then, for any element $x = \sum_{i=1}^n a_i b_i \in E$, we have*

$$\|a_i b_i\| \leq \|x\| + \mathrm{OD}(\mathcal{B}), \text{ for all } 1 \leq i \leq n.$$

Proof. Let $\mathcal{B}' = (b'_1, \dots, b'_n)$ be an orthonormal basis of E, and T the transition matrix from $\mathcal{B}$ to $\mathcal{B}'$. We have $x = \sum_{i=1}^n c_i b'_i$, for

$$(a_1 \dots a_n)T = (c_1 \dots c_n).$$

Since $\mathcal{B}'$ is reduced, $\|x\| = \max_{1 \leq i \leq n}\{|c_i| + \|b'_i\|\}$. By Cramer's rule, $a_i = \det T' / \det T$, where T' is the matrix whose rows are the coordinates of $b_1, \dots, b_{i-1}, x, b_{i+1}, \dots, b_n$ with respect to $\mathcal{B}'$. Arguing as in the proof of Hadamard's inequality, we get

$$|\det T'| \leq \sum_{j \neq i} \|b_j\| + \|x\| - \mathrm{vol}(E).$$

Hence,

$$\begin{aligned} \|a_i b_i\| &= |a_i| + \|b_i\| = |\det T'| - |\det T| + \|b_i\| \\ &\leq \|x\| + \mathrm{vol}(\mathcal{B}) - \mathrm{vol}(E) - |\det T| \\ &= \|x\| + \mathrm{OD}(\mathcal{B}). \end{aligned}$$

□

Theorem 2.5.7. *A basis $\mathcal{B}$ is reduced if and only if $\mathrm{OD}(\mathcal{B}) = 0$.*

Proof. If $\mathrm{OD}(\mathcal{B}) = 0$, the lemma above shows that for any $x = \sum_{i=1}^n a_i b_i \in E$, we have $\|x\| \geq \|a_i b_i\|$, for all i. Hence, $\|x\| = \max_{1 \leq i \leq n}\{\|a_i b_i\|\}$, and $\mathcal{B}$ is reduced.

Suppose the basis $\mathcal{B}$ is reduced. Let $m_i = -\lceil \|b_i\| \rceil \in \mathbb{Z}$, so that the basis $\mathcal{B}' = (t^{m_1} b_1, \dots, t^{m_n} b_n)$ is orthonormal. If we take $m = \sum_{i=1}^n m_i$ then, clearly

$$\mathrm{vol}(\mathcal{B}') = m + \mathrm{vol}(\mathcal{B}), \quad |d(\mathcal{B}')| = m + |d(\mathcal{B})|.$$

Therefore, $\mathrm{OD}(\mathcal{B}) = \mathrm{OD}(\mathcal{B}') = 0$. □

Lemma 2.5.8. *Let E be a normed space, $L \subset E$ a lattice and $\mathcal{B} = (b_1, \dots, b_n)$ a reduced basis of L. Then, the determinant of L satisfies*

$$|d(L)| = \sum_{i=1}^n \lceil \|b_i\| \rceil.$$

Proof. Since $\mathcal{B}$ is a reduced basis, the family $\mathcal{B}' := (t^{m_1}b_1, \ldots, t^{m_n}b_n)$ with $m_i := -\lceil \|b_i\| \rceil$, for $1 \leq i \leq n$, is an orthonormal basis of E and $T := \mathrm{diag}(t^{-m_1}, \ldots, t^{-m_n})$ is a transition matrix from $\mathcal{B}$ to $\mathcal{B}'$. By definition, $|d(L)|$ satisfies

$$|d(L)| = |\det T| = -\sum_{i=1}^{n} m_i = \sum_{i=1}^{n} \lceil \|b_i\| \rceil.$$

□

2.6 Transition matrices between reduced bases

In this section we consider properties of transition matrices between reduced bases.

Definition 2.6.1. *The real numbers $r_1, \ldots, r_m$ are said to be ordered modulo $\mathbb{Z}$ if*

$$r_i - \lceil r_i \rceil \leq r_j - \lceil r_j \rceil,$$

for $1 \leq i \leq j \leq m$.

The next result is an immediate consequence of the definitions.

Lemma 2.6.2. *Let $\mathcal{B} = (b_1, \ldots, b_n)$ be a basis of E such that the sequence $r_1 = \|b_1\|, \ldots, r_n = \|b_n\|$ is ordered modulo $\mathbb{Z}$. Then, the family $\mathcal{B}$ is reduced if and only if $(t^{-\lceil r_1 \rceil}b_1, \ldots, t^{-\lceil r_n \rceil}b_n)$ is an orthonormal basis.*

Clearly, a family of real numbers $r_1, \ldots, r_m$ ordered modulo $\mathbb{Z}$ always induces a partition of m into a sum $m = m_1 + \cdots + m_\kappa$ of positive integers. If we denote $s_i := r_i - \lceil r_i \rceil$ for all $1 \leq i \leq m$, we have

$$-1 < s_1 = \cdots = s_{m_1} < s_{m_1+1} = \cdots = s_{m_2} < \cdots < s_{m_\kappa+1} = \cdots = s_m \leq 0,$$

where $\kappa = \#\{r_i + \mathbb{Z} \mid 1 \leq i \leq m\}$.

Corollary 2.6.3. *Let $r_1, \ldots, r_n$ be real numbers, which are ordered modulo $\mathbb{Z}$, and let $n = m_1 + \cdots + m_\kappa$ be the induced partition of n into a sum of positive integers. Then, it holds*

$$\mathrm{Aut}(\perp_{i=1}^{\kappa} \mathcal{K}^{m_i}(r_i)) = D \cdot O(m_1, \ldots, m_\kappa, A_\infty) \cdot D^{-1},$$

where $D := \mathrm{diag}(t^{\lceil r_1 \rceil}, \ldots, t^{\lceil r_n \rceil})$.

Proof. Denote $E := \perp_{i=1}^{\kappa} \mathcal{K}^{m_i}(r_i)$ and $E' := \perp_{i=1}^{\kappa} \mathcal{K}^{m_i}(s_i)$, where $s_j := r_j - \lceil r_j \rceil$. The matrix D determines an isometry $D : E \to E'$, and the result follows from Theorem 2.4.9. □

Proposition 2.6.4. *Let L be a lattice in a normed space E and let $\mathcal{B}' = (b'_1, \dots, b'_n)$ and $\mathcal{B} = (b_1, \dots, b_n)$ be bases of L, such that the two sequence of real numbers $r_1 := \|b'_1\|, \dots, r_n := \|b'_n\|$ and $\|b_1\|, \dots, \|b_n\|$ are ordered modulo $\mathbb{Z}$. Suppose $\mathcal{B}'$ is reduced and let $n = m_1 + \cdots + m_\kappa$ be the (by $r_1, \dots, r_n$) induced partition of n into a sum of positive integers. Then, $\mathcal{B}$ is reduced if and only if the transition matrix from $\mathcal{B}$ to $\mathcal{B}'$ belongs to $D \cdot O(m_1, \dots, m_\kappa, A_\infty) \cdot D^{-1}$, where $D := \operatorname{diag}(t^{\lceil r_1 \rceil}, \dots, t^{\lceil r_n \rceil})$.*

Proof. We consider $B' := (t^{-\lceil r_1 \rceil} b'_1, \dots, t^{-\lceil r_n \rceil} b'_n)$ and $B := (t^{-\lceil \|b_1\| \rceil} b_1, \dots, t^{-\lceil \|b_n\| \rceil} b_n)$ two bases of E. The vectors of B' and B have $\| \ \|$-value in the intervall $(-1, 0]$ and the basis B' is orthonormal. By Lemma 2.6.2, $\mathcal{B}$ is reduced if and only if B is orthonormal. Denote by T the transition matrix from B to B'. By Lemma 2.4.10 the basis B is orthonormal if and only if $T \in O(m_1, \dots, m_\kappa, A_\infty)$. Then, the proposition follows from the fact that $D \cdot T \cdot D^{-1}$ is the transition matrix from $\mathcal{B}$ to $\mathcal{B}'$. □

Lemma 2.6.5. *Let $\mathcal{B}' = (b'_1, \dots, b'_n)$ be an orthonormal basis of a normed space E and $\mathcal{B} = (b_1, \dots, b_n)$ be any basis of E such that $\|b'_i\| \equiv \|b_i\| \bmod \mathbb{Z}$, for $1 \leq i \leq n$. The transition matrix T from $\mathcal{B}$ to $\mathcal{B}'$ satisfies $|\det T| = \sum_{i=1}^n \lceil \|b_i\| \rceil$ if and only if $\mathcal{B}$ is reduced.*

Proof. Suppose $|\det T| = \sum_{i=1}^n \lceil \|b_i\| \rceil$. By the definition of the orthogonal defect, it holds:

$$\operatorname{OD}(\mathcal{B}) = \operatorname{vol}(\mathcal{B}) - \operatorname{vol}(E) - |\det T| = \sum_{i=1}^n \|b_i\| - \sum_{i=1}^n \|b'_i\| - \sum_{i=1}^n \lceil \|b_i\| \rceil = 0,$$

since $\|b_i\| - \lceil \|b_i\| \rceil = \|b'_i\|$ by assumption. Hence, by Theorem 2.5.7, the basis $\mathcal{B}$ is reduced. If $\mathcal{B}$ is reduced we are in the situation of Lemma 2.5.8. □

2.7 Reduction algorithm

A reduction algorithm is an algorithm, which transforms any family of nonzero vectors in a normed space into a reduced one, still generating the same A-module.

In the literature there are several reduction algorithms for particular normed spaces [16], [18] and [31]. In this section our goal is to describe such a reduction algorithm for arbitrary real-valued normed spaces. For the reader's commodity we assume that the initial family of nonzero vectors is a basis of the normed space.

Let $\mathcal{B} = (b_1, \dots, b_n)$ be a basis of a lattice L in a normed space E. The aim of a reduction algorithm is to compute a reduced basis of L. In practice, we work out this

problem by using coordinates with respect to an orthonormal basis $\mathcal{B}' = (b'_1, \ldots, b'_n)$ of E. Let

$$-1 < r_1 \leq r_2 \leq \cdots \leq r_n \leq 0,$$

be the lengths of $b'_1, \ldots, b'_n$, so that E is isometric to $\perp_{i=1}^n \mathcal{K}(r_i)$ through the map sending each $x \in E$ to its coordinate vector with respect to the basis $\mathcal{B}'$.

The image of L in $\perp_{i=1}^n \mathcal{K}(r_i)$ is the lattice generated by the rows of the transition matrix $T = T(\mathcal{B} \to \mathcal{B}') \in \mathrm{GL}_n(K)$ and the aim of the reduction algorithm is to find $R \in \mathrm{GL}_n(A)$ such that the rows of RT are a reduced set of vectors.

We may always assume that T has polynomial entries; that is,

$$T \in \mathrm{GL}_n(K) \cap A^{n \times n}.$$

In fact, for $1 \leq i \leq n$, let $g_i \in A$ be the least common multiple of the denominators of the entries in the i-th column of T, and denote $s_i = r_i - |g_i|$. We consider the isometry

$$\varphi\colon \perp_{i=1}^n \mathcal{K}(r_i) \longrightarrow \perp_{i=1}^n \mathcal{K}(s_i), \quad (x_1, \ldots, x_n) \mapsto (x_1 g_1, \ldots, x_n g_n).$$

This isometry sends the lattice generated by the rows of T to the lattice generated by the rows of $T' := T\,\mathrm{diag}(g_1, \ldots, g_n)$. The matrix T' belongs to $\mathrm{GL}_n(K) \cap A^{n \times n}$ because it is obtained from T by multiplying their columns by $g_1, \ldots, g_n$, respectively.

2.7.1 Reduction step

Our reduction algorithm is based on an iterated performance of a reduction step.

Definition 2.7.1 (Reduction step)**.** *Let $\mathcal{B} = (b_1, \ldots, b_n)$ be a basis of a normed space $(E, \| \ \|)$. A reduction step is a replacement of some $b_j \in \mathcal{B}$ by $\widetilde{b}_j := b_j + \alpha$ such that $\|\widetilde{b}_j\| < \|b_j\|$, where α is an appropriate A-linear combination of $b_1, \ldots, b_{j-1}, b_{j+1}, \ldots, b_n$.*

Clearly, $\widetilde{\mathcal{B}} := (b_1, \ldots, b_{j-1}, \widetilde{b}_j, b_{j+1}, \ldots, b_n)$ is still a basis of the lattice $\langle\, \mathcal{B} \,\rangle_A$ generated by $\mathcal{B}$. Any reduction step keeps invariant the value $|d(\mathcal{B})|$ and decreases the value $\mathrm{vol}(\mathcal{B}) = \sum_{b \in \mathcal{B}} \|b\|$ strictly. Since $OD(\mathcal{B}) = \sum_{b \in \mathcal{B}} \|b\| - \mathrm{vol}(E) - |d(\mathcal{B})|$ is bounded by 0 from below, after a finite number of reduction steps we obtain a reduced basis by Theorem 2.5.7 and Lemma 2.2.6.

In practice, we shall fix an orthonormal basis $\mathcal{B}'$ of E and work in coordinates with respect to $\mathcal{B}'$; thus, we represent the input basis $\mathcal{B}$ as the matrix $T = T(\mathcal{B} \to \mathcal{B}') \in \mathrm{GL}_n(K)$. The aim is to find $R \in \mathrm{GL}_n(A)$ such that $RT = T(\widetilde{\mathcal{B}} \to \mathcal{B}')$ is the matrix

of a reduced basis $\widetilde{\mathcal{B}}$. The matrix $R = T(\widetilde{\mathcal{B}} \to \mathcal{B})$ will be obtained as a product, $R = R_N \cdot R_{N-1} \cdots R_1$, where each R_i represents the concatenation of several reduction steps.

The following lemma is well known.

Lemma 2.7.2. *Let* $\mathrm{LT}_m(k) \subset \mathrm{GL}_m(k)$ *be the subset of all matrices which, up to permutation of its rows, are a lower triangular matrix with diagonal entries equal to* 1. *For any* $M \in k^{m\times n}$ *there exists a matrix* $P \in \mathrm{LT}_m(k)$*, such that* PM *is in row echelon form.*

2.7.2 The case $\mathcal{K}^n(r)$

For convenience, we deal at the beginning with the "simplest" normed space $E := \mathcal{K}^n(r)$ with $r \in \mathbb{R}$. Later we consider arbitrary normed spaces. Denote $\| \ \|$ the norm on E; that is, for $z \in K^n$ we have

$$\|z\| = \|(z_1, \ldots, z_n)\| := \max_{1\le i\le n} \{|z_i|\} + r.$$

Since a basis of E is reduced if and only if it is reduced as a basis of $\mathcal{K}^n$, we could assume that $r = 0$. Although there already exist several detailed descriptions of a reduction algorithm for this particular normed space (for instance [18], [24]), we want to review it in the case $r \neq 0$, which will be useful in regard to its generalization to arbitrary normed spaces. Since $\varphi : E \to E' := \mathcal{K}^n(r'),\ z \mapsto t^{\lceil r\rceil} \cdot z$ with $r' := r - \lceil r\rceil$ is an isometry, by Lemma 2.4.3 we can assume that $-1 < r \le 0$.

Reduceness criterion

We want to derive from Theorem 2.3.3 a reduceness criterion for this particular normed space. Recall that $\mathrm{sm}(E)$ is the multiset $\{r + \mathbb{Z}, \ldots, r + \mathbb{Z}\}$ of cardinality n and $V_r = E_{\le r}/E_{<r}$ has dimension n as a k-vector space (Corollary 2.3.4). By Theorem 2.3.3 the basis $\mathcal{B} = (b_1, \ldots, b_n)$ of E is reduced if and only if the vectors $\mathrm{red}_r(t^{-\lceil\|b_1\|\rceil}b_1), \ldots, \mathrm{red}_r(t^{-\lceil\|b_n\|\rceil}b_n) \in V_r$ are linearly independent. We are interested in a computational realization of $\mathrm{red}_r(z)$, for $z \in E_{\le r}$. Denote by $\mathcal{B}' := (e_1, \ldots, e_n)$ the standard basis of K^n, which is an orthonormal basis of E. For $z = (z_1, \ldots, z_n) \in E_{\le r}$, we obtain $z = \sum_{i=1}^n z_i e_i$ with $|z_i| \le 0$.

Definition 2.7.3. *Any $g \in A_\infty$ can be consider as an element in $K_\infty = k((t^{-1}))$. We write $g = \sum_{i=m}^{\infty} a_i t^{-i}$ with $m = v_\infty(g) \in \mathbb{Z}_{\geq 0}$ and $a_i \in k$ and define*

$$\mathrm{LC}(g) := \begin{cases} a_0 \in k & \text{if } m = 0, \\ 0 \in k & \text{if } m > 0. \end{cases}$$

Note that the leading coefficient of a polynomial $g \in A$ of degree m coincides with $\mathrm{LC}(g/t^m)$. If $|g| < m$, then $\mathrm{LC}(g/t^m) = 0$.

Any rational function $f \in A_\infty$ can be uniquely written as $f = \mathrm{LC}(f) + u_f$ with $u_f \in \mathfrak{m}_\infty$. In particular, $z_i = \mathrm{LC}(z_i) + u_i$ with $u_i \in \mathfrak{m}_\infty$ and

$$z = \sum_{i=1}^{n} \mathrm{LC}(z_i) e_i + \sum_{i=1}^{n} u_i e_i,$$

where $\sum_{i=1}^{n} u_i e_i \in E_{<r}$. Hence, $\mathrm{red}_r(z) = \mathrm{red}_r(\sum_{i=1}^{n} \mathrm{LC}(z_i) e_i) = \sum_{i=1}^{n} \mathrm{LC}(z_i)\, \mathrm{red}_r(e_i)$. By Corollary 2.3.4, the family $\mathrm{red}_r(e_1), \ldots, \mathrm{red}_r(e_n)$ is a k-basis of V_r. Hence, we may consider the k-isomorphism:

$$V_r \to k^n, \quad \mathrm{red}_r\Big(\sum_{i=1}^{n} z_i e_i\Big) \mapsto (\mathrm{LC}(z_1), \ldots, \mathrm{LC}(z_n)) \tag{2.5}$$

attaching to any element in V_r its coordinate vector with respect to that basis. Through this isomorphism, we may represent $\mathrm{red}_r(z)$ by the vector:

$$\big(\mathrm{LC}(z_1), \ldots, \mathrm{LC}(z_n)\big) \in k^n.$$

Therefore, the next statement follows directly from Theorem 2.3.3.

Corollary 2.7.4. *The basis $(b_1, \ldots, b_n)$ of E is reduced if and only if*

$$\mathrm{rank}((\mathrm{LC}(t^{-\lceil \|b_i\| \rceil} b_{i,j}))_{1 \leq i,j \leq n}) = n,$$

where $b_i = (b_{i1}, \ldots, b_{in})$, for $1 \leq i \leq n$.

Corollary 2.7.4 provides a comfortable criterion to decide whether a basis of E is reduced or not.

Example 2.7.5. Let $K = \mathbb{Q}(t)$ and $E = \mathcal{K}^2$. We consider $\mathcal{B} = (b_1, b_2)$ with

$$b_1 = (2t + 1, 1), \quad b_2 = (t^7 + 2, 2t^6).$$

Clearly, $\|b_1\| = \max\{|(2t+1)|, |1|\} = 1$ and $\|b_2\| = \max\{|t^7+2|, |2t^6|\} = 7$. We consider

$$M := \big(\mathrm{LC}(t^{-\lceil \|b_i\| \rceil} b_{i,j})\big)_{1 \leq i,j \leq 2} = \begin{pmatrix} \mathrm{LC}\left(\frac{2t+1}{t}\right) & \mathrm{LC}\left(\frac{1}{t}\right) \\ \mathrm{LC}\left(\frac{t^7+2}{t^7}\right) & \mathrm{LC}\left(\frac{2}{t}\right) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 1 & 0 \end{pmatrix} \in \mathbb{Q}^{2\times 2}.$$

Since $\mathrm{rank}(M) = 1 < 2$, Corollary 2.7.4 shows that the basis $\mathcal{B}$ is not reduced.

Realization of a reduction step

Our algorithm will realize several reduction steps at once. We order $b_1, \dots, b_n$ by increasing length, $\|b_1\| \leq \cdots \leq \|b_n\|$. For $1 \leq i \leq n$, let $b_{i1}, \dots, b_{in}$ be the coordinates of the vector b_i with respect to the orthonormal basis $(e_1, \dots, e_n)$, the standard basis of K^n. We set $T := (b_1 \dots b_n)^{\mathrm{tr}} = (b_{i,j})_{1 \leq i,j \leq n} = T(\mathcal{B} \to \mathcal{B}')$ and consider

$$T' = \mathrm{diag}(t^{-\lceil \|b_1\| \rceil}, \dots, t^{-\lceil \|b_n\| \rceil})T = (t^{-\lceil \|b_1\| \rceil} b_1 \dots t^{-\lceil \|b_n\| \rceil} b_n)^{\mathrm{tr}}.$$

The rows of T' are vectors in E and have by construction norm equal to r. We fix the matrix

$$M = (\mathrm{LC}(t^{-\lceil \|b_i\| \rceil} b_{i,j}))_{1 \leq i,j \leq n} \in k^{n \times n},$$

whose rows are representations of $\mathrm{red}_r(t^{-\lceil \|b_1\| \rceil} b_1), \dots, \mathrm{red}_r(t^{\lceil -\|b_n\| \rceil} b_n)$, and transform M into row echelon form $M' := PM$ with $P = (p_{i,j}) \in \mathrm{LT}_n(k)$, a lower triangular matrix with diagonal entries equal to 1, up to a permutation of its rows (Lemma 2.7.2). For convenience, we assume that P is already a lower triangular matrix.

The rows of P which correspond to the zero-rows of M', give us non-trivial expressions of the zero vector in k^n as k-linear combinations of the rows of M. Through the isomorphism $V_r \cong k^n$ from (2.5), this corresponds to non-trivial expressions of the zero vector in V_r as k-linear combinations of $\mathrm{red}_r(t^{-\lceil \|b_1\| \rceil} b_1), \dots, \mathrm{red}_r(t^{-\lceil \|b_n\| \rceil} b_n)$.

For any $1 \leq j \leq n$, let the j-th row P_j of P be:

$$P_j = (p_{j,1} \cdots p_{j,j-1}\ p_{j,j} = 1\ 0 \cdots 0),$$

so that, the j-th row of PT' is:

$$b'_j := \sum_{i<j} p_{j,i} t^{-\lceil \|b_i\| \rceil} b_i + t^{-\lceil \|b_j\| \rceil} b_j.$$

Let $m := \mathrm{rank}(M)$ and let P' be the lower triangular matrix with rows $P'_1, \dots, P'_n$ defined by

$$P'_j = \begin{cases} e_j & \text{if } j \leq m \\ P_j & \text{if } j > m. \end{cases}$$

For $1 \leq j \leq m$ we define $\widetilde{b}_j := b_j$ while for $m < j \leq n$ we take

$$\widetilde{b}_j := t^{\lceil \|b_j\| \rceil} b'_j = \sum_{i<j} p_{j,i} t^{\lceil \|b_j\| \rceil - \lceil \|b_i\| \rceil} b_i + b_j. \tag{2.6}$$

Thanks to our assumption $\|b_1\| \leq \cdots \leq \|b_n\|$, each $\widetilde{b}_j$ is equal to b_j plus an A-linear combination of $b_1, \ldots, b_m$. Clearly, the family $\widetilde{\mathcal{B}} := (\widetilde{b}_1, \ldots, \widetilde{b}_n)$ is a basis of the lattice $\left\langle \mathcal{B} \right\rangle_A$.

Clearly, the transition matrix $R = T(\widetilde{\mathcal{B}} \to \mathcal{B})$ is given by

$$R = \operatorname{diag}(t^{\lceil \|b_1\| \rceil}, \ldots, t^{\lceil \|b_n\| \rceil}) \cdot P' \cdot \operatorname{diag}(t^{-\lceil \|b_1\| \rceil}, \ldots, t^{-\lceil \|b_n\| \rceil}). \tag{2.7}$$

Note that R is a lower triangular matrix with diagonal entries equal to 1 and it belongs to $\mathrm{GL}_n(A)$, because $\|b_1\| \leq \cdots \leq \|b_n\|$.

By construction, through the isomorphism (2.5) $\operatorname{red}_r(b'_j)$ is represented by the j-th row of M', for $1 \leq j \leq n$. Hence, for $j > m$, we have $\operatorname{red}_r(b'_j) = 0$, so that $\|b'_j\| < r$ and $\|\widetilde{b}_j\| < \|b_j\|$. Therefore, (2.6) is a reduction step in that case. Thus, this procedure allows us to perform $n - \operatorname{rank}(M)$ reduction steps.

Example 2.7.6. We consider Example 2.7.5 again. Since $\mathcal{B} = (b_1, b_2)$ is not reduced, we want to apply a reduction step. With

$$P := \begin{pmatrix} 1 & 0 \\ -\frac{1}{2} & 1 \end{pmatrix} \text{ and } M' := \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$$

it holds $PM = M'$ and M' is in row echelon form. Then,

$$R := \operatorname{diag}(t^{\lceil \|b_1\| \rceil}, t^{\lceil \|b_2\| \rceil}) \cdot P \cdot \operatorname{diag}(t^{-\lceil \|b_1\| \rceil}, t^{-\lceil \|b_2\| \rceil}) = \begin{pmatrix} 1 & 0 \\ -\frac{t^6}{2} & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}[t]),$$

and $R \cdot (b_1 \ b_2)^{\mathrm{tr}} = (b_1 \ -t^6/2 \cdot b_1 + b_2)^{\mathrm{tr}}$ realizes a reduction step. We consider

$$\widetilde{b}_1 := b_1, \quad \widetilde{b}_2 := \frac{-t^6}{2} b_1 + b_2 = \left(-\frac{t^6}{2} + 2, \frac{3t^6}{2} \right).$$

Since $\|\widetilde{b}_2\| = 6$, we obtain

$$\left(\mathrm{LC}(t^{-\lceil \|\widetilde{b}_i\| \rceil} \widetilde{b}_{i,j})\right)_{1 \leq i,j \leq 2} = \begin{pmatrix} \mathrm{LC}\left(\frac{2t+1}{t}\right) & \mathrm{LC}\left(\frac{1}{t}\right) \\ \mathrm{LC}\left(-\frac{1}{2} + \frac{2}{t^6}\right) & \mathrm{LC}\left(\frac{3}{2}\right) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ -\frac{1}{2} & \frac{3}{2} \end{pmatrix} = M' \in \mathbb{Q}^{2 \times 2}.$$

As $\operatorname{rank}(M') = 2$, the basis $\widetilde{\mathcal{B}} := (\widetilde{b}_1, \widetilde{b}_2)$ is reduced by Corollary 2.7.4.

The algorithm

We denote by $T_1, \ldots, T_n$ the rows of a matrix $T \in K^{n \times n}$.

Algorithm 3: Basis reduction for $E = \mathcal{K}^n(r)$

Input: $\mathcal{B} = (b_1, \dots, b_n)$ basis of E.

Output: Reduced basis of the lattice $L = \langle \mathcal{B} \rangle_A$.

$T \leftarrow (b_1 \dots b_n)^{\mathrm{tr}} \in \mathrm{GL}_n(K), \quad s \leftarrow 1$
Compute $g_1, \dots, g_n \in A \backslash \{0\}$ of minimal degree s.t. $\widetilde{T} := T \cdot \mathrm{diag}(g_1, \dots, g_n) \in A^{n \times n}$ and set $(t_{i,j}) = T \leftarrow \widetilde{T}$
while $s < n$ **do**
    Sort rows of T increasingly ordered w.r.t. $\| \ \|$
    $M \leftarrow (\mathrm{LC}(t^{-\lceil \|b_i\| \rceil} t_{i,j}))_{1 \le i,j \le n} \in k^{n \times n}$
    Compute $P = (p_{i,j}) \in \mathrm{LT}_n(k)$ s.t. $M' := PM$ is in row echelon form
    $s \leftarrow \mathrm{rank}(M')$
    if $s < n$ **then**
        for $i = s+1, \dots, n$ **do**
            $u_i \leftarrow \max\{1 \le j \le n \mid p_{i,j} \neq 0\}$
            $T_{u_i} \leftarrow T_{u_i} + \sum_{j=1}^{u_i - 1} t^{\lceil \|T_{u_i}\| \rceil - \lceil \|T_j\| \rceil} \cdot p_{i,j} T_j$
        end for
    end if
end while
return $(b_1 \dots b_n)^{\mathrm{tr}} \leftarrow T \cdot \mathrm{diag}(g_1^{-1}, \dots, g_n^{-1})$

2.7.3 The general case

Let $(E, \| \ \|)$ be a normed space of dimension n and $\mathcal{B}' = (b'_1, \dots, b'_n)$ be an orthonormal basis of E. Denote by $-1 < r_1, \dots, r_\kappa \le 0$ the different lengths of the vectors in $\mathcal{B}'$ and $n_1, \dots, n_\kappa$ their multiplicities, respectively. Then,

$$E \cong \perp_{i=1}^{\kappa} \mathcal{K}^{n_i}(r_i),$$

where the isometry is given by the coordinate map $c_{\mathcal{B}'}$ with respect to $\mathcal{B}'$. Let $\mathcal{B} = (b_1, \dots, b_n)$ be a basis of E ordered by increasing length. Instead of working with the vectors $b_i \in \mathcal{B}$, we consider their coordinate vectors $c_{\mathcal{B}'}(b_i) = (b_{i,1} \dots b_{i,n}) \in K^n$,

which are vectors in $E' := \perp_{i=1}^{\kappa} \mathcal{K}^{n_i}(r_i)$.

Definition 2.7.7. *For $r \in \mathbb{R}$ and any basis $\mathcal{B} = (b_1, \ldots, b_n)$ of E we define the index set*

$$I_{\mathcal{B}}(r) := \{1 \leq i \leq n \mid \|b_i\| \equiv r \bmod \mathbb{Z}\}.$$

Note that $I_{\mathcal{B}'}(r)$ does not depend on the choice of the orthonormal basis $\mathcal{B}'$ and Lemma 2.3.6 shows that $\#I_{\mathcal{B}'}(r_i) = n_i$, for $1 \leq i \leq \kappa$. We can generalize Corollary 2.7.4 as follows:

Theorem 2.7.8. *The basis $\mathcal{B}$ is reduced if and only if for all $r \in \{r_1, \ldots, r_\kappa\}$ the matrix*

$$M_r := (\mathrm{LC}(t^{-\lceil \|b_i\| \rceil} b_{i,j}))_{i \in I_{\mathcal{B}}(r), j \in I_{\mathcal{B}'}(r)}$$

has rank n_i.

Proof. We fix one $r \in \{r_1, \ldots, r_\kappa\}$ and consider b_i with length congruent to r modulo $\mathbb{Z}$ (i.e. $i \in I_{\mathcal{B}}(r)$). We have $t^{-\lceil \|b_i\| \rceil} b_i = \sum_{j=1}^{n} t^{-\lceil \|b_i\| \rceil} b_{i,j} b'_j$. Since $\|t^{-\lceil \|b_i\| \rceil} b_i\| = r$ with $-1 < r \leq 0$, the coefficients $t^{-\lceil \|b_i\| \rceil} b_{i,j}$ belong to A_∞ and $\| \sum_{j \notin I_{\mathcal{B}'}(r)} t^{-\lceil \|b_i\| \rceil} b_{i,j} b'_j \| < r$. We write $t^{-\lceil \|b_i\| \rceil} b_{i,j} = \mathrm{LC}(t^{-\lceil \|b_i\| \rceil} b_{i,j}) + r_j$ with $r_j \in \mathfrak{m}_\infty$, for $j \in I_{\mathcal{B}'}(r)$. Then,

$$\begin{aligned} t^{-\lceil \|b_i\| \rceil} b_i &= \sum_{j=1}^{n} t^{-\lceil \|b_i\| \rceil} b_{i,j} b'_j \\ &= \sum_{j \in I_{\mathcal{B}'}(r)} \mathrm{LC}(t^{-\lceil \|b_i\| \rceil} b_{i,j}) b'_j + \sum_{j \in I_{\mathcal{B}'}(r)} r_j b'_j + \sum_{j \notin I_{\mathcal{B}'}(r)} t^{-\lceil \|b_i\| \rceil} b_{i,j} b'_j \end{aligned}$$

with $\| \sum_{j \in I_{\mathcal{B}'}(r)} \mathrm{LC}(t^{-\lceil \|b_i\| \rceil} b_{i,j}) b'_j \| = r$ and $\sum_{j \in I_{\mathcal{B}'}(r)} r_j b'_j + \sum_{j \notin I_{\mathcal{B}'}(r)} t^{-\lceil \|b_i\| \rceil} b_{i,j} b'_j \in E_{<r}$. Clearly, $\sum_{j \in I_{\mathcal{B}'}(r)} \mathrm{LC}(t^{-\lceil \|b_i\| \rceil} b_{i,j}) b'_j$ is a representative of $\mathrm{red}_r(t^{-\lceil \|b_i\| \rceil} b_i)$. Since $\dim_k V_r = n_r$ with $n_r := \#I_{\mathcal{B}'}(r)$ by Corollary 2.3.4, the vector $(\mathrm{LC}(t^{-\lceil \|b_i\| \rceil} b_{i,j}))_{j \in I_{\mathcal{B}'}(r)}$ is a representation of $\mathrm{red}_r(t^{-\lceil \|b_i\| \rceil} b_i)$. Then, the statement is a direct consequence of Theorem 2.3.3. □

In order to apply a reduction step in $E' = \perp_{i=1}^{\kappa} \mathcal{K}^{n_i}(r_i)$ we will restrict our observation to the i-th part $\mathcal{K}^{n_i}(r_i)$ of E'. The next corollary ensures that a reduction step which is detected in $\mathcal{K}^{n_i}(r_i)$ corresponds to a reduction step in E' and therefore in E.

Corollary 2.7.9. *Denote $E^i := \mathcal{K}^{n_i}(r_i)$, for $1 \leq i \leq \kappa$. Then, the canonical projection $E' \to E^i$ induces a k-isomorphism*

$$E'_{\leq r_i} / E'_{<r_i} \to E^i_{\leq r_i} / E^i_{<r_i},$$

for $1 \leq i \leq \kappa$. In particular: For any i and $b = \sum_{j=1}^{n} \lambda_j b'_j \in E$ with $\|b\| = r_i$ the vector $(\mathrm{LC}(t^{-\lceil \|b\| \rceil}\lambda_j))_{j \in I_{\mathcal{B}'}(r_i)} \in k^{n_i}$ is up to isomorphism a representation of $\mathrm{red}_{r_i}(t^{-\lceil \|b\| \rceil}b)$, $\mathrm{red}'_{r_i}(t^{-\lceil \|b\| \rceil}(\lambda_1, \ldots, \lambda_n))$ and $\mathrm{red}^i_{r_i}(t^{-\lceil \|b\| \rceil}(\lambda_j)_{j \in I_{\mathcal{B}'}(r_i)})$, where $\mathrm{red}_r, \mathrm{red}'_r$ and red^i_r denote the reduction maps induced by $E_{\leq r_i}/E_{<r_i}$, $E'_{\leq r_i}/E'_{<r_i}$, and $E^i_{\leq r_i}/E^i_{<r_i}$, respectively.

Proof. The map $E'_{\leq r_i}/E'_{<r_i} \to E^i_{\leq r_i}/E^i_{<r_i}$ is clearly onto; hence it is an isomorphism because the vector spaces have dimension n_i by Corollary 2.3.4. For the second statement we consider the proof of the last theorem for the normed space E and b. □

Realization of a reduction step

Denote $T := (b_{i,j})_{1 \leq i,j \leq n} \in \mathrm{GL}_n(K)$ the transition matrix from $\mathcal{B}$ to $\mathcal{B}'$. The rows of T are the coordinate vectors $c_{\mathcal{B}'}(b)$ for $b \in \mathcal{B}$. Therefore, we can identify the basis $\mathcal{B}$ of E with the rows of T, which form a basis of $\perp_{i=1}^{\kappa} \mathcal{K}^{n_i}(r_i)$. A reduction step will be realized as explained in Subsection 2.7.2 by restricting our consideration to the normed spaces $E^i = \mathcal{K}^{n_i}(r_i)$, for $1 \leq i \leq \kappa$. We fix $1 \leq i \leq \kappa$ and consider $r_i, m_i := \#I_{\mathcal{B}}(r_i)$, and $n_i = \#I_{\mathcal{B}'}(r_i)$ with the submatrix of T given by

$$T_{r_i} := (b_{i,j})_{i \in I_{\mathcal{B}}(r_i), j \in I_{\mathcal{B}'}(r_i)} \in K^{m_i \times n_i}. \tag{2.8}$$

The rows of T_{r_i} are vectors in E^i. Therefore, we are in the situation of Subsection 2.7.2. We determine $R_{r_i} \in \mathrm{GL}_{n_i}(A)$ as defined in (2.7). Then, by Corollary 2.7.9 the product

$$R_{r_i}(b_j)^{\mathrm{tr}}_{j \in I_B(r_i)}$$

realizes $m_i - \mathrm{rank}(M_{r_i})$ reduction steps, where M_{r_i} is defined in Theorem 2.7.8. That is, the relations for a reduction step are detected by considering the normed space E^i. By Corollary 2.7.9 this relations also realize a reduction step in E. We will consider this circumstance in the next example explicitly.

Example 2.7.10. Let $K = \mathbb{F}_3(t)$ be the rational function field over $\mathbb{F}_3$, the finite field of three elements. We consider the normed space $E = \mathcal{K}(-1/2) \perp \mathcal{K}(-1/3) \perp \mathcal{K}(-1/4)$ and consider the standard basis $\mathcal{B}' = (e_1, e_2, e_3)$ of K^3 as an orthonormal basis of E. We have $r_1 = -1/2$, $r_2 = -1/3$, and $r_3 = -1/4$ with multiplicities $n_i = 1$ for $1 \leq i \leq 3$ and deduce $I_{\mathcal{B}'}(r_i) = \{i\}$. Consider $\mathcal{B} = (b_1, b_2, b_3)$ the basis of E with

$$b_1 := \left(t^2, t^2+1, 0\right), b_2 := \left(t(t^2+1), t, t^4+1\right), \text{ and } b_3 := \left(0, t^4(t+1), t^4\right).$$

The norm on E is given by $\|(z_1, z_2, z_3)\| = \max\{|z_1| - 1/2, |z_2| - 1/3, |z_3| - 1/4\}$; hence, $\|b_1\| = 5/3$, $\|b_2\| = 15/4$, and $\|b_3\| = 14/3$. The vectors b_1 and b_3 have the same length

congruent to r_2 modulo $\mathbb{Z}$. Thus, $I_{\mathcal{B}}(r_2) = \{1, 3\}$ and $m_2 := \#I_{\mathcal{B}}(r_2) = 2$. The basis $\mathcal{B}$ is not reduced, as $\mathcal{B}$ contains no vector of length in $r_1 + \mathbb{Z}$. We apply a reduction step. As defined in (2.8) we consider

$$T_{r_2} = \begin{pmatrix} t^2+1 \\ t^4(t+1) \end{pmatrix} \in K^{m_2 \times n_2}.$$

The rows of T_{r_2} are vectors in the normed space $\mathcal{K}(r_2)$. We obtain

$$M_{r_2} = \begin{pmatrix} \mathrm{LC}\big(t^{-\lceil 5/3 \rceil}(t^2+1)\big) \\ \mathrm{LC}\big(t^{-\lceil 14/3 \rceil}t^4(t+1)\big) \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in \mathbb{F}_3^{2\times 1} \tag{2.9}$$

and transform M_{r_2} into row echelon form to detect the relations for a reduction step. We deduce

$$P = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \text{ and } M'_{r_2} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ with } PM_{r_2} = M'_{r_2}.$$

Then, the matrix $R_{r_2} := \mathrm{diag}(t^{\lceil 5/3 \rceil}, t^{\lceil 14/3 \rceil}) \cdot P \cdot \mathrm{diag}(t^{-\lceil 5/3 \rceil}, t^{-\lceil 14/3 \rceil})$ as defined in (2.7) is given by

$$R_{r_2} = \begin{pmatrix} 1 & 0 \\ 2t^3 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_3[t])$$

and $R_{r_2} \cdot (b_1\ b_3)^{\mathrm{tr}} =: (\widetilde{b}_1\ \widetilde{b}_3)^{\mathrm{tr}}$ realizes a reduction step. In particular, we obtain $\widetilde{b}_1 = b_1$ and

$$\widetilde{b}_3 = 2t^3 \cdot b_1 + b_3 = \left(2t^5, t^3(t+2), t^4\right).$$

We deduce $\|\widetilde{b}_3\| = 7/2$. The basis $\widetilde{\mathcal{B}} := (\widetilde{b}_1, b_2, \widetilde{b}_3)$ is reduced, since $\|\widetilde{b}_1\|$, $\|b_2\|$, and $\|\widetilde{b}_3\|$ are different modulo $\mathbb{Z}$. Note that $\widetilde{b}_3$ and b_3 do not have the same length modulo $\mathbb{Z}$.

The algorithm

The idea of the algorithm can be explained easily: We split the basis $\mathcal{B} = (b_1, \ldots, b_n)$ of E into subsets $\mathcal{B}_r := \{b \in \mathcal{B} \mid \|b\| \equiv r \bmod \mathbb{Z}\}$ for any $r \in \{r_1, \ldots, r_\kappa\}$, and apply for each of these subsets reduction steps as mentioned before. Unfortunately, we can not ensure that the length of a reduced vector $b + \alpha$ lies in the same class as $\|b\|$ modulo $\mathbb{Z}$. Therefore, it may happen that the subsets $\mathcal{B}_r$ change after any reduction step.

Recall that $\mathrm{LT}_n(k)$ is the set of all $P \in \mathrm{GL}_n(k)$ which are lower triangular with 1 at the diagonal, up to row permutation.

Algorithm 4: Basis reduction

Input: $\mathcal{B}' = (b'_1, \ldots, b'_n)$ orthonormal basis of a normed space $(E, \| \ \|)$ and $\mathcal{B} = (b_1, \ldots, b_n)$ basis of E.

Output: Reduced basis of the lattice $L = \langle \mathcal{B} \rangle_A$.

$\mathcal{B}'\text{vals} \leftarrow [\|b'_1\|, \ldots, \|b'_n\|]$
vals $\leftarrow$ Sequence of pairwise distinct values in $\mathcal{B}'$vals
Compute $T = T(\mathcal{B} \to \mathcal{B}') \in \mathrm{GL}(n, K)$, $l \leftarrow 1$
Compute $g_1, \ldots, g_n \in A \backslash \{0\}$ of minimal degree s.t. $\widetilde{T} := T \cdot \mathrm{diag}(g_1, \ldots, g_n) \in A^{n \times n}$ and set $(t_{i,j}) = T \leftarrow \widetilde{T}$
while $l \leq \#\text{vals}$ **do**
    $\mathcal{B}\text{vals} \leftarrow [\max_{j=1}^{n}\{|t_{1,j}| + \|b'_j\|\}, \ldots, \max_{j=1}^{n}\{|t_{n,j}| + \|b'_j\|\}]$
    Sort $\mathcal{B}$vals increasingly ordered and apply changes to the rows of T
    Determine all $1 \leq e_1, \ldots, e_f \leq n$ with $\mathcal{B}\text{vals}[e_i] \equiv \text{vals}[l] \bmod \mathbb{Z}$
    Determine all $1 \leq c_1, \ldots, c_g \leq n$ with $\mathcal{B}'\text{vals}[c_i] \equiv \text{vals}[l] \bmod \mathbb{Z}$
    $M \leftarrow (\mathrm{LC}(t^{-\lceil \mathcal{B}\text{vals}[e_i] \rceil} t_{e_i,c_j}))_{1 \leq i \leq f, 1 \leq j \leq g} \in k^{f \times g}$
    Compute $P = (p_{i,j}) \in \mathrm{LT}_f(k)$ s.t. $M' := PM$ is in row echelon form
    $s \leftarrow \mathrm{rank}(M')$
    if $s = f$ **then**
        if $f < g$ and $\text{vals}[l] \notin \{\text{vals}[\iota] \mid \iota > l\}$ **then**
            Append(vals, vals[l])
        end if
    else
        for $i = s + 1, \ldots, f$ **do**
            $u_i \leftarrow \max\{1 \leq j \leq f \mid p_{i,j} \neq 0\}$
            $T_{e_{u_i}} \leftarrow T_{e_{u_i}} + \sum_{j=1}^{u_i - 1} t^{\lceil \mathcal{B}\text{vals}[e_{u_i}] \rceil - \lceil \mathcal{B}\text{vals}[e_j] \rceil} p_{i,j} T_{e_j}$
            $\mathcal{B}\text{vals}[e_{u_i}] \leftarrow \max_{j=1}^{n}\{|t_{e_{u_i},j}| + \|b'_j\|\}$
            if $\mathcal{B}\text{vals}[e_{u_i}] - \lceil \mathcal{B}\text{vals}[e_{u_i}] \rceil \notin \{\text{vals}[\iota] \mid \iota > l\}$ **then**
                Append(vals, $\mathcal{B}\text{vals}[e_{u_i}] - \lceil \mathcal{B}\text{vals}[e_{u_i}] \rceil$)
            end if
        end for

26: **end if**

27: $l \leftarrow l + 1$

28: **end while**

29: **return** $(b_1 \dots b_n)^{\mathrm{tr}} \leftarrow T \cdot \mathrm{diag}(g_1^{-1}, \dots, g_n^{-1}) \cdot (b'_1 \dots b'_n)^{\mathrm{tr}}$

Comments on Algorithm 4

Line	Comment
1-4	Initialization
6-11	Computation of T_r and M_r with $r := \mathrm{vals}[l]$ as in (2.8) and Theorem 2.7.8, and transforming M_r into row echelon form.
13	Check if a reduction step can be applied.
14-16	If no reduction step can be a applied but the number of vectors in $\mathcal{B}$ of length r mod $\mathbb{Z}$ does not coincide with the number of vectors in $\mathcal{B}'$ of length r mod $\mathbb{Z}$, we have not found "enough" vectors in $\mathcal{B}$ with length congruent to r modulo $\mathbb{Z}$. Later, there will occur (after several reduction steps) "new" vectors with length r modulo $\mathbb{Z}$. Therefore, we must reconsider the value $r = \mathrm{vals}[l]$ afterwards.
20	Apply reduction steps.
21	Computation of the length of the "new" vectors.
22-24	As mentioned above, here we deal with the case, in which the length r of the reduced vector does not coincide with the length of the original vector modulo $\mathbb{Z}$. Then, we have to reconsider the class r mod $\mathbb{Z}$ later.

Note that the reduction Algorithms 3 and 4 can easily be generalized to an arbitrary subset $\mathcal{B} = \{b_1, \dots, b_m\}$ of a normed space.

Remark 2.7.11. *By Proposition 2.2.5, for a reduced basis $\mathcal{B} = (b_1, \dots, b_n)$ the values $\|b_i\|$, $1 \leq i \leq n$, are the successive minima of L. Moreover, for a real number r, Proposition 2.2.5 shows that the k-vector space $L_{\leq r}$ admits the basis*

$$\{b_i t^{j_i} \mid 1 \leq i \leq n, \quad 0 \leq j_i \leq \lfloor r - \|b_i\| \rfloor\}.$$

Hence, Algorithm 4 can also be adapted to compute these objects.

2.7.4 Complexity

We are interested in the complexity of Algorithms 3 and 4. All estimations are expressed in the number of necessary operations in k (cf. Section 1.3). Recall that $\mathrm{Sig}(E)$ denotes the set of different lengths modulo $\mathbb{Z}$ of all nonzero vectors in the normed space $(E, \| \ \|)$.

Lemma 2.7.12. *Let $\mathcal{B}$ be a basis of an n-dimensional normed space E. The number of reduction steps to transform $\mathcal{B}$ into a reduced basis is bounded by*

$$\#\,\mathrm{Sig}(E) \cdot \lfloor OD(\mathcal{B}) \rfloor + (\#\,\mathrm{Sig}(E) - 1)n.$$

Proof. Let $\mathcal{B} = (b_1, \ldots, b_n)$ and let $\widetilde{\mathcal{B}} = (\widetilde{b}_1, \ldots, \widetilde{b}_n)$ be a reduced basis obtained from $\mathcal{B}$. Each vector b_i is changed by several reduction steps until we obtain the vector $\widetilde{b}_i \in \widetilde{\mathcal{B}}$. Let us denote by R_i the number of these reduction steps; that is

$$b_i \to b_i^{(1)} \to \cdots \to b_i^{(R_i)} = \widetilde{b}_i.$$

If we denote $D_i := \|b_i\| - \|\widetilde{b}_i\|$, then $OD(\mathcal{B}) = D_1 + \cdots + D_n$.

Let $\kappa := \#\,\mathrm{Sig}(E)$. If we apply κ consecutive reduction steps to any vector $b \in \langle \mathcal{B} \rangle_A$:

$$b = b^{(0)} \to b^{(1)} \to \cdots \to b^{(\kappa)} \tag{2.10}$$

then, $\|b\| - \|b^{(\kappa)}\| \geq 1$. In fact, since the lengths of all nonzero vectors in E have only κ possibilities modulo $\mathbb{Z}$, among the $\kappa + 1$ vectors in (2.10) there must be a coincidence. If $0 \leq j < l \leq \kappa$ satisfy $\|b^{(l)}\| \equiv \|b^{(j)}\| \bmod \mathbb{Z}$ then:

$$\|b\| - \|b^{(\kappa)}\| \geq \|b^{(j)}\| - \|b^{(l)}\| \geq 1.$$

This argument shows that $R_i \leq \lfloor D_i \rfloor \kappa + \kappa - 1$. Therefore, the total number of reduction steps is:

$$R_1 + \cdots + R_n \leq \lfloor OD(\mathcal{B}) \rfloor \kappa + (\kappa - 1)n$$

□

Corollary 2.7.13. *Let $\mathcal{B}$ be a basis of the n-dimensional normed space $\mathcal{K}^n(r)$, for some $r \in \mathbb{R}$. The number of reduction steps to transform $\mathcal{B}$ into a reduced basis is at most $OD(\mathcal{B})$.*

Proof. Follows directly from the last lemma, since $\#\,\mathrm{Sig}(\mathcal{K}^n(r)) = \#\{r + \mathbb{Z}\} = 1$. □

We introduce heights of rational functions in order to measure the complexity of the reduction algorithms.

Definition 2.7.14. *For $g = f/h \in K$, with coprime polynomials $f, h \in K$, we define the* height *of g by*

$$h(g) := \max\{|f|, |h|\}.$$

The height *of a matrix $T = (t_{i,j}) \in K^{n\times m}$ is defined to be*

$$h(T) := \max\{h(t_{i,j}) \mid 1 \le i \le n, \quad 1 \le j \le m\}.$$

Clearly, $|g|, |g^{-1}| \le h(g)$ for all $g \in K \setminus \{0\}$. The next lemma presents some more properties of the height, which will be useful for the complexity analyses of several algorithms.

Lemma 2.7.15. *Let $T, T' \in K^{n\times n}$ and let $\widetilde{T} \in A^{n\times n}$ be the matrix obtained by multiplying the columns of T by polynomials $g_1, \ldots, g_n \in A \setminus \{0\}$ of minimal degree.*

1. $h(T \cdot T') \le h(T) + h(T')$.
2. $h(\widetilde{T}) \le nh(T)$.
3. *If T is invertible, then*
   (a) $|\det T|, |\det T^{-1}| \le nh(T)$.
   (b) $h(T^{-1}) \le nh(T)$.

Proof. The first statement is obvious. For the second item, let us show that every column $\widetilde{T}_j$ of $\widetilde{T}$ has height bounded by $nh(T)$. In fact, if g_j is the product of all denominators of the entries of the j-th column of T, then each product $g_j t_{i,j}$ is equal to the product of n polynomials of degree less than or equal to $h(T)$.

Suppose that T is invertible. For any permutation σ of $\{1, 2, \ldots, n\}$ we have

$$\pm|t_{1,\sigma(1)} \cdots t_{n,\sigma(n)}| = \pm \sum_{i=1}^{n} |t_{i,\sigma(i)}| \le \sum_{i=1}^{n} h(t_{i,\sigma(i)}) \le nh(T).$$

This shows that $\pm|\det(T)| \le nh(T)$, which proves item *(a)* because $|\det(T^{-1})| = -|\det(T)|$.

Denote by $T_{i,j}$ the matrix which arises from deleting the i-th row and the j-th column in T. The entries $s_{i,j}$ of T^{-1} may be computed as

$$s_{i,j} = (-1)^{i+j} \frac{\det(T_{j,i})}{\det(T)}.$$

Hence, $h(s_{i,j}) \le nh(T)$ because numerator and denominator have degree bounded by $nh(T)$; this proves *(b)*. □

Lemma 2.7.16. *Let $\mathcal{B}$ and $\mathcal{B}'$ be bases of the n-dimensional normed space E and let $\mathcal{B}'$ be orthonormal. Denote by T the transition matrix from $\mathcal{B}$ to $\mathcal{B}'$. Then, $OD(\mathcal{B}) < n(2h(T)+1)$.*

Proof. Let $\mathcal{B} = (b_1, \ldots, b_n)$ and $\mathcal{B}' = (b'_1, \ldots, b'_n)$. By definition,

$$OD(\mathcal{B}) = \sum_{i=1}^{n} \|b_i\| - \mathrm{vol}(E) - |\det(T)|. \tag{2.11}$$

With $T = (t_{i,j})$ we obtain, for $1 \leq i \leq n$:

$$\|b_i\| = \max_{1\leq j\leq n}\{|t_{i,j}| + \|b'_j\|\} \leq \max_{1\leq j\leq n}\{|t_{i,j}|\} \leq h(T).$$

Hence, $\sum_{i=1}^{n} \|b_i\| \leq nh(T)$.

On the other hand, $\mathrm{vol}(E) = \sum_{i=1}^{n} \|b'_i\| > -n$, since $-1 < \|b'_i\| \leq 0$ for all i, as $\mathcal{B}'$ is orthonormal. Finally *(b)* of item *3* from the last lemma shows that $-|\det(T)| \leq nh(T)$. Therefore, from (2.11) we deduce $OD(\mathcal{B}) < nh(T) + n + nh(T) = n(2h(T)+1)$. □

Lemma 2.7.17. *Let $\widetilde{T} \in A^{n\times n}$ be the matrix obtained by multiplying the columns of $T \in K^{n\times n}$ by polynomials of minimal degree $g_1, \ldots, g_n \in A \setminus \{0\}$, respectively. The computation of $\widetilde{T}$ has a cost of $O(n^3 h(T)^2)$ operations in k.*

Proof. It suffices to show that the computation of the j-th column $\widetilde{T}_j$ of $\widetilde{T}$ has a cost of $O(n^2 h(T)^2)$ operations in k.

The computation of $\mathrm{lcm}(h_1, \ldots, h_n)$ for polynomials $h_i \in A$ of degree $|h_i| \leq N$ has a cost of $O(n^2N^2)$ operations in k, if we use the brute procedure:

$$\begin{array}{cc} l_1 = \mathrm{lcm}(h_1, h_2) & O(N^2) \\ l_2 = \mathrm{lcm}(l_1, h_3) & O(2N^2) \\ \vdots & \vdots \\ l_{n-1} = \mathrm{lcm}(l_{n-2}, h_n) & O((n-1)N^2) \end{array}$$

The sum of all these costs is $O(n^2N^2)$. Hence, the computation of g_j has a cost of $O(n^2h(T)^2)$ operations in k. Since $|g_j| \leq nh(T)$ and the product $g_j t_{i,j}$ has a cost of $nh(T)^2$ operations in k, the n products which are necessary to compute $\widetilde{T}_j$ require $O(n^2h(T)^2)$ operations in k. □

Lemma 2.7.18. *Let $\mathcal{B}'$ be an orthonormal basis of an n-dimensional normed space $(E, \|\ \|)$ and $\mathcal{B}$ be a basis of a lattice L in E. Denote by T the transition matrix from $\mathcal{B}$ to $\mathcal{B}'$. Then, Algorithm 4 takes at most*

$$O\big(\#\,\mathrm{Sig}(E) \cdot n^5 \cdot h(T)^2\big)$$

arithmetic operations in k to transform $\mathcal{B}$ into a reduced basis. If T has only polynomial entries the cost of Algorithm 4 is $O(\#\operatorname{Sig}(E)(n^4 \cdot h(T) + n^3 \cdot h(T)^2))$ operations in k.

Proof. By any reduction step in Algorithm 4 the value $OD(\mathcal{B})$ is decreased strictly. If $\kappa = \#\operatorname{Sig}(E)$, according to Lemma 2.7.12 and Theorem 2.5.7, after at most $\lfloor OD(\mathcal{B})\rfloor\kappa + (\kappa-1)n$ steps, the set $\mathcal{B}$ is reduced and the algorithm terminates.

Clearly, the runtime of the algorithm is dominated by the computation of $\widetilde{T}$, the transformation of matrices into row echelon form (cf. line 11 of Algorithm 4), and the realization of reduction steps (cf. line 20 of Algorithm 4).

At first we analyze the complexity of the transformation of matrices into row echelon form along Algorithm 4. Denote by $r_1, \ldots, r_\kappa$ the different length of vectors in $\mathcal{B}'$ and $n_1, \ldots, n_\kappa$ its multiplicities, respectively. Note that $n = n_1 + \cdots + n_\kappa$. Suppose, that after $i-1$ steps in Algorithm 4 we have transformed the basis $\mathcal{B}$ of L into $\mathcal{B}_i = (b_{i_1}, \ldots, b_{i_n})$. Note that $T = \widetilde{T}$ and $(b_{i_1} \ldots b_{i_n})^{\mathrm{tr}} = T \cdot \operatorname{diag}(g_1^{-1}, \ldots, g_n^{-1}) \cdot (b'_1 \ldots b'_n)^{\mathrm{tr}}$. We can split $\mathcal{B}_i$ into disjoint subsets

$$\mathcal{B}_i = \mathcal{B}_{r_1} \cup \cdots \cup \mathcal{B}_{r_\kappa},$$

where $\mathcal{B}_{r_j} := \{b \in \mathcal{B}_i \mid \|b\| \equiv r_j \bmod \mathbb{Z}\}$, for $1 \le j \le \kappa$. Assume $\mathcal{B}_i$ is not reduced. For $r \in \{r_1 \ldots, r_\kappa\}$, we consider the matrix $M_r \in k^{\#I_{\mathcal{B}_i}(r) \times \#I_{\mathcal{B}'}(r)}$ as in Theorem 2.7.8. Then, by Theorem 2.7.8, for at least one r, the matrix M_r has not full rank.

In the worst case, we have to transform all matrices $M_{r_1}, \ldots, M_{r_\kappa}$ into row echelon form until we detect at least one reduction step (i.e. one zero row). The number of rows and columns in M_{r_j} satisfy $\#I_{\mathcal{B}_i}(r_j) = \#\mathcal{B}_{r_j}$ and $\#I_{\mathcal{B}'}(r_j) = n_j$, for $1 \le j \le \kappa$, by Definition 2.7.7. Hence, $\sum_{j=1}^{\kappa} \#I_{\mathcal{B}'}(r_j) = \sum_{j=1}^{\kappa} n_j = n$ and $\sum_{j=1}^{\kappa} \#I_{\mathcal{B}_i}(r_j) = n$. Then, the cost for transforming all M_{r_j}, $1 \le j \le \kappa$, into row echelon form is less or equal than the cost of transforming one $n \times n$ matrix over k into row echelon form (which is equal to $O(n^3)$ operations in k, cf. [6]). Hence, the cost of all transformations of matrices into row echelon form along Algorithm 4 is bounded by $O((OD(\mathcal{B})\kappa + (\kappa-1)n) \cdot n^3)$ operations in k. According to Lemma 2.7.16 the last complexity bound can be estimated by $O(\kappa n^4 h(\widetilde{T}))$.

Additionally, we compute A-linear combinations of the rows of $\widetilde{T}$ (line 20 of Algorithm 4), where the coefficients are of the form αt^m with $\alpha \in k$ and a nonnegative integer m. After any reduction step the degree of the entries in $\widetilde{T}$ is less or equal than before; that is, at any level the value of $h(\widetilde{T})$ is not increased. Since the multiplication of a polynomial by a t-power is just a shift of the exponents, we can consider the latter A-linear combinations of rows of $\widetilde{T}$ as k-linear combinations.

The cost of any reduction step applied to the rows of $\widetilde{T}$ is $O(n^2 h(\widetilde{T}))$ operations in k. Thus, the total cost of performing all reduction steps of Algorithm 4 is $O(\kappa n^3 h(\widetilde{T})^2)$ by Lemma 2.7.12 and 2.7.16. Therefore, the total cost of Algorithm 4 is

$$O(\kappa(n^4 h(\widetilde{T}) + n^3 h(\widetilde{T})^2) + n^3 h(T)^2) = O(\kappa(n^4 h(\widetilde{T}) + n^3 h(\widetilde{T})^2)) \tag{2.12}$$

by Lemma 2.7.17. In terms of the input matrix T we get a cost of

$$O(\kappa n^5 h(T)^2)$$

by Lemma 2.7.15. For an input matrix $T \in A^{n \times n}$ the complexity bound (2.12) becomes

$$O(\kappa(n^4 h(T) + n^3 h(T)^2)).$$

□

In Subsection 2.8.1 we will present an optimized version of the reduction algorithm (cf. Lemma 2.8.17).

Corollary 2.7.19. *Let $\mathcal{B} = (b_1, \ldots, b_n)$ be a basis of the normed space $E := \mathcal{K}^n(r)$, $r \in \mathbb{R}$, and $T := (b_1 \ldots b_n)^{\mathrm{tr}}$. Algorithm 3 takes $O(n^5 h(T)^2)$ arithmetic operations in k to transform $\mathcal{B}$ into a reduced basis. If the input matrix T belongs to $A^{n \times n}$ the cost of Algorithm 3 is $O(n^4 h(T) + n^3 h(T)^2)$ operations in k.*

Proof. Clearly, $\mathrm{Sig}(\mathcal{K}^n(r)) = \{r + \mathbb{Z}\}$ and therefore $\#\,\mathrm{Sig}(E) = 1$. Then, Algorithm 4 coincides with Algorithm 3. Hence, the complexity bounds follow immediately from Lemma 2.7.18. □

If the transition matrix T has only polynomial entries, the complexity of Algorithm 3 can be split into two parts. On the one hand, we obtain $O(n^4 h(T))$ operations in k for the transformation of matrices into row echelon form, and on the other hand $O(n^3 h(T)^2)$ operations for the reduction steps. In practice, the runtime of Algorithm 3 (and Algorithm 4) is dominated by the realization of the reduction steps. The reason for this is that, $h(T) \geq n$ in most of the cases. Under this assumption the complexity of Algorithm 3 for transforming $\mathcal{B}$ into a reduced basis is equal to $O(n^3 h(T)^2)$ operations in k by the last corollary. In that context our reduction algorithm is one magnitude better than the reduction algorithms described in [18, 35] and its complexity coincides with the one in [24]. Note that the reduction algorithm in [24] is based on the computation of Popov forms of matrices over polynomial rings, whereas in [18, 35] the

approaches are similar to the presented one. However, in the contrast to Algorithm 4 the mentioned reduction algorithms do not determine a reduced basis for a real-valued lattice.

2.8 Classes of lattices and semi-reduceness

In this chapter denote by E an n-dimensional K-vector space. We consider a norm $\| \ \|$ on E and a lattice $(L, \| \ \|)$ in $(E, \| \ \|)$. Our aim is to construct a so-called "semi-reduced basis" (cf. Definition 2.8.10) $\mathcal{B}$ of L, which "nearly" behaves as a reduced one. By introducing an equivalence relation on the set of norms on E, we can consider instead of the real-valued lattice $(L, \| \ \|)$ an integer-valued lattice $(L, \| \ \|')$, which almost coincides with the original one. For instance, for the computation of the vector spaces $(L, \| \ \|)_{\leq r}$, for $r \in \mathbb{Z}$, it is sufficient to determine a reduced basis $\mathcal{B}$ of the lattice $(L, \| \ \|')$. Moreover, the computation of the reduced basis $\mathcal{B}$ of $(L, \| \ \|')$ can be used as a precomputation for the reduction algorithm in order to determine a reduced basis of $(L, \| \ \|)$. Thus, the reduction algorithm can be accelerated.

Definition 2.8.1. *We define the* norm space $\mathrm{Norm}(E)$ *of E as the set of all norms $\| \ \|$ on E such that $(E, \| \ \|)$ becomes a normed space. For a multiset $R = \{r_1 + \mathbb{Z}, \ldots, r_n + \mathbb{Z}\} \subset \mathbb{R}/\mathbb{Z}$, we define the R-*norm space *of E by*

$$\mathrm{Norm}(E, R) := \{\| \ \| \in \mathrm{Norm}(E) \mid \mathrm{sm}(E, \| \ \|) = R\}.$$

The space of lattices *of E is defined to be*

$$\mathrm{LS}(E) := \{(L, \| \ \|) \text{ a lattice in } (E, \| \ \|) \mid \| \ \| \in \mathrm{Norm}(E)\},$$

the set of all lattices $(L, \| \ \|)$, for all $\| \ \| \in \mathrm{Norm}(E)$. Moreover, we set $\mathrm{LS}(E, R) := \{(L, \| \ \|) \in \mathrm{LS}(E) \mid \overline{\mathrm{sm}}(L, \| \ \|) = R\}$ *and call it the R-*space of lattices *of E.*

We introduce an equivalence class on $\mathrm{Norm}(E)$.

Definition 2.8.2. *We call two norms $\| \ \|$ and $\| \ \|'$ in* $\mathrm{Norm}(E)$ equivalent*, and we write $\| \ \| \sim \| \ \|'$, if $\lceil \|z\| \rceil = \lceil \|z\|' \rceil$, for all $z \in E$.*

We call two normed spaces $(E, \| \ \|)$ and $(E, \| \ \|')$ equivalent*, and we write $(E, \| \ \|) \sim (E, \| \ \|')$, if $\| \ \| \sim \| \ \|'$.*

We call two lattices $(L, \| \ \|)$ and $(L, \| \ \|')$ equivalent*, and we write $(L, \| \ \|) \sim (L, \| \ \|')$, if $\| \ \| \sim \| \ \|'$.*

Lemma 2.8.3. *Let $(E, \| \|)$ be a normed space. Then, $(E, \lceil \| \| \rceil)$ is a normed space.*

Proof. The norm properties of $\lceil \| \| \rceil$ are inherited from $\| \|$. □

The following result follows easily from the definitions.

Lemma 2.8.4. *The relation $\sim$ is an equivalence relation on* $\mathrm{Norm}(E)$*. We denote the class of $\| \|$ in* $\mathrm{Norm}(E)/\sim$ *by* $[\| \|]$*.*

In each equivalence class there is a unique integer-valued norm, defined by $z \mapsto \lceil \|z\| \rceil$, for any $\| \|$ in the class. Hence, there are as many equivalence classes of norms as integer-valued norms

Definition 2.8.5. *A basis $\mathcal{B}$ of E is called a* semi-orthonormal *basis of $(E, \| \|)$, if it is, up to ordering, an orthonormal basis of a normed space $(E, \| \|')$, which is equivalent to $(E, \| \|)$.*

Note that a semi-orthonormal basis of $(E, \| \|)$ is a semi-orthonormal basis of $(E, \| \|')$, for all norms $\| \|'$ in the class of $\| \|$. In particular, an orthonormal basis is semi-orthonormal.

Lemma 2.8.6. *A basis $\mathcal{B}$ of a normed space $(E, \| \|)$ is semi-orthonormal if and only if*

$$\left\lceil \left\| \sum_{b \in \mathcal{B}} a_b b \right\| \right\rceil = \max_{b \in \mathcal{B}} \{|a_b|\}, \text{ for all } a_b \in K. \tag{2.13}$$

Proof. If $\mathcal{B}$ is semi-orthonormal, there exists $\| \|' \in \mathrm{Norm}(E)$ with $\| \|' \sim \| \|$ such that $\mathcal{B}$ is an orthonormal basis of $(E, \| \|')$. Hence,

$$\left\| \sum_{b \in \mathcal{B}} a_b b \right\|' = \max_{b \in \mathcal{B}} \{\|a_b b\|'\}, \text{ for all } a_b \in K.$$

As $-1 < \|b\|' \leq 0$, for all $b \in \mathcal{B}$, we obtain $\lceil \|b\|' \rceil = 0$ and $\lceil \max_{b \in \mathcal{B}} \{\|a_b b\|'\} \rceil = \max_{b \in \mathcal{B}} \{|a_b|\}$. Since $\lceil \|z\| \rceil = \lceil \|z\|' \rceil$, for all $z \in E$, the statement holds.

Conversely, if $\| \|$ satisfies (2.13) then $\lceil \|b\| \rceil = 0$ for all $b \in \mathcal{B}$, and $\mathcal{B}$ is an orthonormal basis of $(E, \| \|')$, where $\| \|'$ is the integer-valued norm defined by: $\|z\|' = \lceil \|z\| \rceil$. □

Theorem 2.8.7. *Let $\| \|, \| \|' \in \mathrm{Norm}(E)$. It holds $\| \| \sim \| \|'$ if and only if the transition matrix from a semi-orthonormal basis of $(E, \| \|)$ to a semi-orthonormal basis of $(E, \| \|')$ belongs to* $\mathrm{GL}_n(A_\infty)$*.*

In order to proof the theorem we will use the following lemma.

Lemma 2.8.8. *A matrix $T = (t_{i,j}) \in K^{n\times n}$ belongs to $\mathrm{GL}_n(A_\infty)$ if and only if*

$$\max_{1\le i\le n}\Big\{\Big|\sum_{j=1}^{n} t_{j,i}a_j\Big|\Big\} = \max_{1\le i\le n}\{|a_i|\},$$

for all $a_1,\dots,a_n \in K$.

Proof. The matrix T belongs to $\mathrm{GL}_n(A_\infty)$ if and only if T is an isometry on $\mathcal{K}^n$ by Theorem 2.4.7. Clearly, T is an isometry if and only if

$$\max_{1\le i\le n}\Big\{\Big|\sum_{j=1}^{n} t_{j,i}a_j\Big|\Big\} = \|(a_1\dots a_n)T\| = \|(a_1\dots a_n)\| = \max_{1\le i\le n}\{|a_i|\},$$

for all $a_1,\dots,a_n \in K$. □

Proof of Theorem 2.8.7. Denote by $\mathcal{B} = (b_1,\dots,b_n)$ and by $\mathcal{B}' = (b'_1,\dots,b'_n)$ semi-orthonormal bases of $(E,\|\ \|)$ and $(E,\|\ \|')$, respectively. Let $T = (t_{i,j})$ be the transition matrix from $\mathcal{B}$ to $\mathcal{B}'$. We write for an arbitrary element $z \in E$, $z = \sum_{i=1}^n a_i b_i$ and $z = \sum_{i=1}^n a'_i b'_i$ with coefficients in K and obtain $a'_i = \sum_{j=1}^n t_{j,i}a_j$. Then, by (2.13) it holds that

$$\lceil\|z\|\rceil = \max_{1\le i\le n}\{|a_i|\} = \max_{1\le i\le n}\Big\{\Big|\sum_{j=1}^{n} t_{j,i}a_j\Big|\Big\} = \max_{1\le i\le n}\{|a'_i|\} = \lceil\|z\|'\rceil$$

if and only if $T \in \mathrm{GL}_n(A_\infty)$, by Lemma 2.8.8. □

Lemma-Definition 2.8.9. *Let $\mathcal{B}$ be a semi-orthonormal basis of $(E,\|\ \|)$. Then, we define $L_\infty := \langle\mathcal{B}\rangle_{A_\infty} = (E,\|\ \|)_{\le 0}$. Moreover, any A_∞-basis of L_∞ is a semi-orthonormal basis of $(E,\|\ \|)$.*

Proof. By Lemma 2.8.6 it holds for $z = \sum_{i=1}^n a_i b_i \in E$ with coefficients a_i in K that $\lceil\|z\|\rceil = \max_{1\le i\le n}\{|a_i|\}$. Clearly, $\|z\| \le 0$ if and only if $|a_i| \le 0$, for $1 \le i \le n$; hence $L_\infty = (E,\|\ \|)_{\le 0}$.

Since the transition matrix between two bases of L_∞ belongs to $\mathrm{GL}_n(A_\infty)$, the second statement holds by Theorem 2.8.7. In particular, L_∞ is well-defined. □

Definition 2.8.10. *A subset $\{b_1,\dots,b_m\}$ in a normed space $(E,\|\ \|)$ is called* semi-reduced *or* weakly reduced *if*

$$\Big\lceil\Big\|\sum_{i=1}^{m} a_i b_i\Big\|\Big\rceil = \max_{1\le i\le m}\{\lceil\|a_i b_i\|\rceil\},$$

for any $a_1,\dots,a_m \in K$. Or equivalently, the subset is reduced with respect to the unique integer-valued norm equivalent to $\|\ \|$.

Clearly, any reduced set is semi-reduced. In fact, many of the results concerning a reduced set can be adapted to semi-reduced sets. For instance, the next result follows immediately from the definitions.

Corollary 2.8.11.

1. *A basis $\mathcal{B}$ of a normed space $(E, \| \ \|)$ is semi-orthonormal if and only if $\mathcal{B}$ is semi-reduced with $-1 < \|b\| \leq 0$, for all $b \in \mathcal{B}$.*

2. *If $\mathcal{B} = (b_1, \ldots, b_n)$ is semi-reduced, then the family $(t^{-\lceil \|b_1\| \rceil} b_1, \ldots, t^{-\lceil \|b_n\| \rceil} b_n)$ is semi-orthonormal.*

Lemma 2.8.12. *Let $(L, \| \ \|)$ and $(L, \| \ \|')$ be two equivalent lattices. Then, any semi-reduced basis of $(L, \| \ \|)$ is a semi-reduced basis of $(L, \| \ \|')$.*

Proof. Let $\mathcal{B}$ be a semi-reduced basis of $(L, \| \ \|)$. For arbitrary coefficients $a_b \in K$, we deduce

$$\left\lceil \left\| \sum_{b \in \mathcal{B}} a_b b \right\|' \right\rceil = \left\lceil \left\| \sum_{b \in \mathcal{B}} a_b b \right\| \right\rceil = \max_{b \in \mathcal{B}} \{ \lceil \|a_b b\| \rceil \} = \max_{b \in \mathcal{B}} \{ \lceil \|a_b b\|' \rceil \},$$

by the definition of the equivalence relation. Hence, $\mathcal{B}$ be a semi-reduced basis of $(L, \| \ \|')$. □

The next theorem summarizes all data, which shares one equivalence class of a lattice $(L, \| \ \|)$.

Theorem 2.8.13. *For $i \in \{1, 2\}$, denote by $\mathcal{B}_i = (b_{1,i}, \ldots, b_{n,i})$ a semi-reduced basis of the lattice $(L, \| \ \|_i)$, which is ordered by increasing length. Then, the following statements are equivalent:*

1. *$\| \ \|_1 \sim \| \ \|_2$,*

2. *$\lceil \|b_{1,i}\|_1 \rceil = \lceil \|b_{2,i}\|_2 \rceil$, for $1 \leq i \leq n$,*

3. *$(L, \| \ \|_1)_{\leq r} = (L, \| \ \|_2)_{\leq r}$, for all $r \in \mathbb{Z}$, and*

4. *$(E, \| \ \|_1)_{\leq 0} = (E, \| \ \|_2)_{\leq 0}$, with $E := \langle \mathcal{B}_1 \rangle_K = \langle \mathcal{B}_2 \rangle_K$.*

Proof. 1. ⇒ 3. One can easily see that item *3* of Proposition 2.2.5 is correct for a semi-reduced basis and an integer r. Thus,

$$(L, \| \ \|_1)_{\leq r} = \langle \{ b_{1,i} t^{j_i} \mid 1 \leq i \leq n, 0 \leq j_i \leq -\lceil \|b_{1,i}\|_1 \rceil + r \} \rangle_k.$$

By Lemma 2.8.12 the set $\mathcal{B}_1$ is also a semi-reduced basis of $(L, \| \ \|_2)$. Hence,

$$(L, \| \ \|_2)_{\leq r} = \langle \{ b_{1,i} t^{j_i} \mid 1 \leq i \leq n, 0 \leq j_i \leq -\lceil \|b_{1,i}\|_2 \rceil + r \} \rangle_k.$$

By assumption $\lceil \|z\|_1 \rceil = \lceil \|z\|_2 \rceil$ holds, for all $z \in E$, and therefore $(L, \| \ \|_1)_{\leq r} = (L, \| \ \|_2)_{\leq r}$.

3. $\Rightarrow$ *2.* If $(L, \| \ \|_1)_{\leq r}$ and $(L, \| \ \|_2)_{\leq r}$ coincide, for all $r \in \mathbb{Z}$, then their dimensions too. Let $r_1 \leq \cdots \leq r_n$ and $s_1 \leq \cdots \leq s_n$ with $r_i := \lceil \|b_{1,i}\| \rceil$ and $s_i := \lceil \|b_{2,i}\| \rceil$. Assume that $r_1 = s_1, \ldots, r_i = s_i$; $r_{i+1} < s_{i+1}$. Then, Proposition 2.2.5 shows that $\dim_k (L, \| \ \|_1)_{\leq s_{i+1}-1} \neq \dim_k (L, \| \ \|_2)_{\leq s_{i+1}-1}$, a contradiction.

2. $\Rightarrow$ *1.* We fix $m_i := \lceil \|b_{1,i}\|_1 \rceil = \lceil \|b_{2,i}\|_2 \rceil$, for $1 \leq i \leq n$, and consider $\mathcal{B}'_i := (t^{-m_1} b_{1,i}, \ldots, t^{-m_n} b_{n,i})$ with $i \in \{1, 2\}$. By Corollary 2.8.11 $\mathcal{B}'_1$ and $\mathcal{B}'_2$ are semi-orthonormal bases of $(E, \| \ \|_1)$ and $(E, \| \ \|_2)$, respectively. In particular, $\langle \mathcal{B}'_i \rangle_{A_\infty} = (E, \| \ \|_i)_{\leq 0}$ holds, for $1 \leq i \leq 2$, by Lemma-Definition 2.8.9. Clearly, the transition matrix $R = (a_{i,j})$ from $\mathcal{B}'_2$ to $\mathcal{B}'_1$ belongs to $A_\infty^{n \times n}$. In fact $0 = \lceil \|b'_{2,i}\|_2 \rceil = \max_{1 \leq j \leq n} \{ \lceil \|a_{i,j} b'_{1,j}\|_1 \rceil \} = \max_{1 \leq j \leq n} \{ |a_{i,j}| \}$, where $\mathcal{B}'_i = (b'_{i,1}, \ldots, b'_{i,n})$ for $i \in \{1, 2\}$. By construction, the transition matrix from $\mathcal{B}_i$ to $\mathcal{B}'_i$ is given by $T = \operatorname{diag}(t^{m_1}, \ldots, t^{m_n})$. The transition matrix M from $\mathcal{B}_2$ to $\mathcal{B}_1$ belongs to $\mathrm{GL}_n(A)$, since both bases generate the A-module L. Thus, we obtain the commutative diagram of transition matrices:

$$\begin{array}{ccc} \mathcal{B}'_1 & \xrightarrow{T} & \mathcal{B}_1 \\ {\scriptstyle R}\uparrow & & \uparrow{\scriptstyle M} \\ \mathcal{B}'_2 & \xrightarrow{T} & \mathcal{B}_2 \end{array}$$

Hence, $\det R = \det T \det M \det T^{-1} = \det M$ and $|\det R| = |\det M| = 0$. Therefore, $R \in \mathrm{GL}_n(A_\infty)$ and Theorem 2.8.7 shows that $\| \ \|_1 \sim \| \ \|_2$.

Finally let us show that *1* $\Leftrightarrow$ *4*. By considering the semi-orthonormal bases $\mathcal{B}'_1$ and $\mathcal{B}'_2$ as above, the equivalence follows by Theorem 2.8.7 and Lemma-Definition 2.8.9. $\square$

As we have seen in the proof of the last theorem it is sufficient to compute a semi-reduced basis of $(L, \| \ \|)$ in order to determine a basis of $(L, \| \ \|)_{\leq r}$, for $r \in \mathbb{Z}$.

Corollary 2.8.14. *Let L be a lattice in the normed space $(E, \| \ \|)$ and denote by $s_1, \ldots, s_n$ its successive minima. Let $\mathcal{B} = (b_1, \ldots, b_n)$ be a semi-reduced family of vectors in L of minimal length; that is, up to ordering, $\lceil \|b_i\| \rceil = \lceil s_i \rceil$ holds. Then, $\mathcal{B}$ is a semi-reduced basis of $(L, \| \ \|)$.*

Proof. By Definition 2.8.10 $\mathcal{B}$ is a reduced family of the lattice $(L, \lceil \| \ \| \rceil)$ having the successive minima $\lceil s_1 \rceil, \ldots, \lceil s_n \rceil$. Then, Theorem 2.2.8 shows that $\mathcal{B}$ is a reduced basis of $(L, \lceil \| \ \| \rceil)$, and in particular a semi-reduced basis of $(L, \| \ \|)$. □

The last corollary gives us a criterion to check if a semi-reduced family of vectors is a basis of the A-module L. In Chapter 5 we will explain it in the context of the computation of bases of holomorphic rings in function fields in more detail.

We end this paragraph with a trivial remark.

Lemma 2.8.15. *For $r \in \mathbb{R}$ it holds*

$$L_{\leq r} = L \cap E_{\leq r} = L \cap t^r E_{\leq 0} = L \cap t^r L_\infty.$$

2.8.1 Computation of (semi-) reduced bases

Let $\mathcal{B}'$ be an orthonormal basis of $(E, \| \ \|)$ and L be a lattice in $(E, \| \ \|)$. In section 2.7 we already described an algorithm (cf. Algorithm 4), which computes a reduced basis of L. This algorithm takes as input a basis $\mathcal{B}$ of L and the orthonormal basis $\mathcal{B}'$. According to Lemma 2.7.18 the runtime of the computation of a reduced basis of L is minimal if $E \cong \mathcal{K}(r)^n$, i.e. $\#\operatorname{Sig}(E) = 1$.

The computation of a semi-reduced basis amounts to the computation of a reduced basis of a normed space in this favourable situation. In fact, by Lemmas 2.8.3 and 2.8.12, a reduced basis of $(E, \lceil \| \ \| \rceil)$ is a semi-reduced basis of $(E, \| \ \|)$ and since $(E, \lceil \| \ \| \rceil)$ is an integer-valued normed space, it is isometric to $\mathcal{K}^n$.

We may use this idea to describe an optimized version of Algorithm 4. Let $\mathcal{B}'$ be an orthonormal basis of the normed space $(E, \| \ \|)$ and let $\mathcal{B}$ be any basis of the lattice $(L, \| \ \|)$ in $(E, \| \ \|)$. Clearly, $\mathcal{B}'$ is an orthonormal basis of $(E, \lceil \| \ \| \rceil)$ too, and $c_{\mathcal{B}'} : E \to K^n$ an isometry between $(E, \lceil \| \ \| \rceil)$ and $\mathcal{K}^n$.

In order to transform $\mathcal{B}$ into a reduced basis, we consider $\mathcal{B}$ as a basis of $(E, \lceil \| \ \| \rceil)$ and call Algorithm 3 for $\{c_{\mathcal{B}'}(b) \mid b \in \mathcal{B}\}$. This results in a semi-reduced basis $\mathcal{B}_{\text{semi}}$ of $(L, \| \ \|)$. We will see that transforming $\mathcal{B}_{\text{semi}}$ into a reduced basis $\mathcal{B}_{\text{red}}$ of $(L, \| \ \|)$ by Algorithm 4 can be realized at minimal cost. We summarize the results by the following pseudocode:

Algorithm 5: Basis reduction II

Input: $\mathcal{B}'$ orthonormal basis of a normed space $(E, \| \ \|)$ and $\mathcal{B} = (b_1, \ldots, b_n)$ a basis of E.

Output: Reduced basis of the lattice $L = \langle \mathcal{B} \rangle_A$.

1: $\mathcal{D} \leftarrow \{c_{\mathcal{B}'}(b_1), \ldots, c_{\mathcal{B}'}(b_n)\}$
2: $\mathcal{B}_{\text{semi}} \leftarrow$Algorithm 3$(\mathcal{D})$
3: $\mathcal{B}_{\text{red}} \leftarrow$Algorithm 4$(c_{\mathcal{B}'}^{-1}(\mathcal{B}_{\text{semi}}), \mathcal{B}')$
4: **return** $\mathcal{B}_{\text{red}}$

Complexity

We determine the complexity of Algorithm 5. After transforming the basis $\mathcal{B}$ into a semi-reduced basis $\mathcal{B}_{\text{semi}}$, the orthogonal defect $OD(\mathcal{B}_{\text{semi}})$ is dominated by the dimension of E.

Lemma 2.8.16. *Let $\mathcal{B}$ be a semi-reduced basis of a lattice $(L, \| \ \|)$. Then, the orthogonal defect of $\mathcal{B}$ satisfies*

$$\mathrm{OD}(\mathcal{B}) < n.$$

Proof. Let $\mathcal{B} = (b_1, \ldots, b_n)$ and consider a reduced basis $\mathcal{B}' = (b'_1, \ldots, b'_n)$ of L. By definition $\mathcal{B}$ is a reduced basis of the lattice $(L, \lceil \| \ \| \rceil)$. Assume that both bases are increasingly ordered with respect to the length of their vectors. By Theorem 2.5.7, we obtain $\mathrm{OD}(\mathcal{B}') = 0$, since $\mathcal{B}'$ is reduced. According to Theorem 2.8.13 we obtain $\lceil \|b_i\| \rceil = \lceil \|b'_i\| \rceil$ and therefore $\|b_i\| < \|b'_i\| + 1$, for $1 \leq i \leq n$. Then, $0 = \mathrm{OD}(\mathcal{B}') = \mathrm{vol}(\mathcal{B}') - \mathrm{vol}(E) - |d(L)|$ and therefore

$$\mathrm{OD}(\mathcal{B}) = \mathrm{vol}(\mathcal{B}) - \mathrm{vol}(E) - |d(L)| = \mathrm{vol}(\mathcal{B}) - \mathrm{vol}(\mathcal{B}') < n.$$

□

According to Lemma 2.7.12, the last lemma shows that at most $O(\#\,\mathrm{Sig}(E)n)$ reduction steps are necessary to transform a semi-reduced basis of $(L, \| \ \|)$ into a reduced one.

Lemma 2.8.17. *Let the notation be the same as in Lemma 2.7.18. Then, Algorithm 5 takes $O(n^5 h(T)^2)$ arithmetic operations in k to transform $\mathcal{B}$ into a reduced basis. If T has only polynomial entries the complexity can be estimated by*

$$O(n^4(h(T) + \#\operatorname{Sig}(E)) + n^3 h(T)^2)$$

operations in k. In particular, the complexity is equal to $O(n^3 h(T)^2)$ for $h(T) \geq n$ and $T \in A^{n\times n}$.

Proof. The bounds of the statement can be easily deduced by considering Corollary 2.7.19 and the proof of Lemma 2.7.18, having in mind that $\#\operatorname{Sig}(E) \leq n$ and $OD(\mathcal{B}) < n$ by the last lemma. □

3. Riemann-Roch theory on lattices

The concept of divisors and the theory of Riemann-Roch in functions fields play a significant role in number theory and algebraic geometry. In Chapter 4 we will see that a divisor D of a function field F/k can be interpreted as a lattice $(L_D, \| \|_D)$ by considering F as a K-vector space. Under this point of view, the Riemann-Roch space of D coincides with the k-vector space $(L_D, \| \|_D)_{\leq 0}$.

In this chapter we will generalize the notion of a divisor and certain invariants in algebraic function fields to lattice spaces (cf. Definition 2.8.1). Surprisingly, many of these concepts can be defined without any divisor or ideal arithmetic.

We fix for this chapter an n-dimensional K-vector space E and consider $\mathrm{Norm}(E)$, the set of all norms $\| \|$ on E, which determine a normed space $(E, \| \|)$. In the sequel we will describe properties of lattices in $\mathrm{LS}(E)$, the lattice space of E, in relation to a fixed one. The fixed lattice is determined by a bilinear form on E.

For the rest of the chapter we fix one non-degenerated symmetric bilinear form B on E.

3.1 Lattices and norms supported by E

Any basis of E provides a norm on E.

Lemma-Definition 3.1.1. *Any basis $\mathcal{B}$ of E determines a norm, which is defined as*

$$\| \|_{\mathcal{B}} : E \to \mathbb{Z}, \quad \left\| \sum_{b \in \mathcal{B}} \lambda_b b \right\| := \max_{b \in \mathcal{B}} \{|\lambda_b|\}.$$

We call $\| \|_{\mathcal{B}}$ the by $\mathcal{B}$ induced norm. *The norm $\| \|_{\mathcal{B}}$ belongs to* $\mathrm{Norm}(E)$ *and does not depend on the ordering of the basis $\mathcal{B}$.*

Proof. Clearly, E is isomorphic to K^n, where an isomorphism is given by the coordinate map $c_{\mathcal{B}}$. Since the norm $\| \ \|_{\mathcal{B}}$ is the pull-back of the norm of $\mathcal{K}^n = (K^n, \| \ \|)$ with $\|(\lambda_b)_{b\in\mathcal{B}}\| = \max_{b\in\mathcal{B}}\{|\lambda_b|\}$, the statement holds. □

By construction $\mathcal{B}$ is an orthonormal basis of the integer-valued normed space $(E, \| \ \|_{\mathcal{B}})$. The following statements are trivial and their proofs are left to the reader.

Lemma 3.1.2. *Let $\| \ \| \in \mathrm{Norm}(E)$ and let $\mathcal{B}$ and $\mathcal{B}'$ be two bases of E.*

1. *$\| \ \|_{\mathcal{B}} = \| \ \| \iff \| \ \|$ is integer-valued and $\mathcal{B}$ is an orthonormal basis of $\| \ \|$ (up to ordering).*
2. *$\| \ \|_{\mathcal{B}} \sim \| \ \| \iff \mathcal{B}$ is an orthonormal basis of $\lceil \| \ \| \rceil \iff \| \ \|_{\mathcal{B}} = \lceil \| \ \| \rceil$.*
3. *$\| \ \|_{\mathcal{B}} = \| \ \|_{\mathcal{B}'} \iff T(\mathcal{B} \to \mathcal{B}') \in \mathrm{GL}_n(A_\infty)$.*

Any equivalence class $[\| \ \|]$ in $\mathrm{Norm}(E)/\sim$ contains exactly one integer-valued norm, namely $\lceil \| \ \| \rceil$. As we have seen in Subsection 2.8.1, in same cases it is sufficient to work with this "simplest" representative of $[\| \ \|]$. Later, we will define the degree and dimension of a lattice $(L, \| \ \|)$ (cf. Definition 3.1.7 and Definition 3.1.8) and see that these invariants are the same for any lattice equivalent to $(L, \| \ \|)$. Thus, for the computation of these invariants it is sufficient to consider only the norm $\lceil \| \ \| \rceil$.

Note that any basis $\mathcal{B}$ of E determines the class $[\| \ \|_{\mathcal{B}}]$, where $\| \ \|_{\mathcal{B}}$ is the unique integer-valued representative. In particular, $\mathcal{B}$ is a semi-orthonormal basis of any normed space $(E, \| \ \|)$ with $\| \ \| \sim \| \ \|_{\mathcal{B}}$ and it holds by Lemma-Definition 2.8.9 that $(E, \| \ \|)_{\leq 0} = \langle \mathcal{B} \rangle_{A_\infty}$.

For the sequel we will fix an A-submodule $\mathcal{O}_E \subset \{z \in E \mid \mathrm{B}(z,z) \in A\}$ and an A_∞-submodule $\mathcal{O}_{E,\infty} \subset \{z \in E \mid \mathrm{B}(z,z) \in A_\infty\}$ both of rank n.

These modules will play the same role as the finite and infinite maximal orders $\mathcal{O}_F$ and $\mathcal{O}_{F,\infty}$ do in the case of an algebraic function field.

Lemma 3.1.3. *The modules $\mathcal{O}_E$ and $\mathcal{O}_{E,\infty}$ are free. Moreover, it holds $B(z,z') \in A$ for $z, z' \in \mathcal{O}_E$, and $B(z,z') \in A_\infty$ for $z, z' \in \mathcal{O}_{E,\infty}$.*

Proof. The modules $\mathcal{O}_E$ and $\mathcal{O}_{E,\infty}$ are free because they are torsion free and A is a principal ideal domain.

For the second statement we consider $\mathcal{O}_E$. The case $\mathcal{O}_{E,\infty}$ can be treated analogously. Let $z, z' \in \mathcal{O}_E$, then $\mathrm{B}(z+z', z+z') = \mathrm{B}(z,z) + 2\mathrm{B}(z,z') + \mathrm{B}(z'z') \in A$ with $\mathrm{B}(z,z), \mathrm{B}(z'z') \in A$ by definition; hence, $\mathrm{B}(z,z') \in A$. □

Definition 3.1.4. *The* zero norm *on E is given by $\| \ \|_0 := \| \ \|_{\mathcal{B}}$, where $\mathcal{B}$ denotes any basis of the A_∞-modul $\mathcal{O}_{E,\infty}$. The class of $\| \ \|_0$ in* $\mathrm{Norm}(E)/\sim$ *is called the* zero class.

By Lemma 3.1.2, for another basis $\mathcal{B}'$ of $\mathcal{O}_{E,\infty}$ we have $\| \ \|_{\mathcal{B}} = \| \ \|_{\mathcal{B}'}$. Therefore, the norm $\| \ \|_0$ is independent of the choice of the basis.

The zero norm is a canonical object in that setting. The next observation shows that $\| \ \|_0$ is "compatible" with the bilinear form B.

Lemma 3.1.5. *For $z, z' \in E$, we have $|\mathrm{B}(z,z')| \leq \|z\|_0 + \|z'\|_0$. Moreover, it holds that $\mathcal{O}_E \subseteq (E, \| \ \|_0)_{\geq 0}$ and $\mathcal{O}_{E,\infty} = (E, \| \ \|_0)_{\leq 0}$.*

Proof. Let $\mathcal{B} = (b_1, \ldots, b_n)$ be a basis of $\mathcal{O}_{E,\infty}$. Let $z = \sum_{i=1}^n \lambda_i b_i$ and $z' = \sum_{i=1}^n \lambda_i' b_i$ with $\lambda_i, \lambda_i' \in K$ for all i. Lemma 3.1.3 shows that $\mathrm{B}(b_i, b_j) \in A_\infty$, for $1 \leq i, j \leq n$. Hence,

$$|\mathrm{B}(z,z')| = \Big| \sum_{i,j} \lambda_i \lambda_j' \mathrm{B}(b_i, b_j) \Big| \leq \max_{i,j} \{|\lambda_i| + |\lambda_j'| + |\mathrm{B}(b_i,b_j)|\} \leq \max_{i,j} \{|\lambda_i| + |\lambda_j'|\}$$
$$\leq \max_i \{|\lambda_i|\} + \max_j \{|\lambda_j'|\} = \|z\|_0 + \|z'\|_0.$$

As $\mathcal{O}_E \subset \{z \in E \mid \mathrm{B}(z,z) \in A\}$ we obtain $|\mathrm{B}(z,z)| \geq 0$, for all $z \in \mathcal{O}_E$. By the last statement this implies $\|z\|_0 \geq 0$ and therefore $\mathcal{O}_E \subset (E, \| \ \|_0)_{\geq 0}$.

The last identity follows from Lemma-Definition 2.8.9, having in mind that any basis $\mathcal{B}$ of $\mathcal{O}_{E,\infty}$ is an orthonormal basis of $(E, \| \ \|_0)$ by construction. □

Corollary 3.1.6.

1. $(\mathcal{O}_E, \| \ \|_0)_{\leq 0} = \mathcal{O}_E \cap \mathcal{O}_{E,\infty} \subseteq \{z \in E \mid \mathrm{B}(z,z) \in k\}$.
2. $\mathrm{B}(z,z') \in k$, *for all* $z, z' \in (\mathcal{O}_E, \| \ \|_0)_{\leq 0}$.
3. $(\mathcal{O}_E, \| \ \|_0)_{\leq 0} \subseteq \{z \in E \mid \|z\|_0 = 0\}$.

Proof. It holds that $(\mathcal{O}_E, \| \ \|_0)_{\leq 0} = \mathcal{O}_E \cap \mathcal{O}_{E,\infty}$ by Lemma 2.8.15, since $\mathcal{O}_{E,\infty} = (E, \| \ \|_0)_{\leq 0}$ by the last lemma. By definition $\mathrm{B}(z,z) \in A \cap A_\infty = k$, for all $z \in \mathcal{O}_E \cap \mathcal{O}_{E,\infty}$. This proves item *1.* Item *2* follows from Lemma 3.1.3 and item *3* from the last lemma. □

The k-vector space $(\mathcal{O}_E, \| \ \|_0)_{\leq 0}$ is a subset of the set of all vectors in $(E, \| \ \|_0)$ having length 0. This vector space can be considered as the units in $\mathcal{O}_E$ with respect to $\| \ \|_0$. In the function field case F/k, the latter k-vector space coincides with $\mathcal{L}(0) = k_0$, the full constant field of F (cf. (4.9)).

We are going to define basic invariants of lattices with respect to the fixed lattice $(\mathcal{O}_E, \| \|_0)$. Recall that $\mathrm{LS}(E)$ is the set of all lattices in $(L, \| \|)$, for all $\| \| \in \mathrm{Norm}(E)$. Clearly, $(\mathcal{O}_E, \| \|_0)$ belongs to $\mathrm{LS}(E)$.

Definition 3.1.7 (Degree)**.** *The* degree *of a lattice* $(L, \| \|)$ *with respect to* $(\mathcal{O}_E, \| \|_0)$ *is defined by* $\deg(L, \| \|) := |d(\mathcal{O}_E, \| \|_0)| - |d(L, \| \|)|$. *For convenience, we write* $\deg L = |d(\mathcal{O}_E)| - |d(L)|$ *and we refer to this number as the degree of* L.

Definition 3.1.8 (Dimension)**.** *The* dimension *of a lattice* $(L, \| \|)$ *is defined by* $\dim L := \dim(L, \| \|)_{\leq 0}$.

Note that the degree and the dimension depend only on the class of $(L, \| \|)$: Let $(L, \| \|) \sim (L, \| \|')$, then $|d(L, \| \|)| = |d(L, \| \|')|$ and $\dim(L, \| \|) = \dim(L, \| \|')$ by Lemma 2.5.8 and Theorem 2.8.13.

Corollary 3.1.9. *For any lattice* $(L, \| \|) \in \mathrm{LS}(E)$ *we have*

$$\dim L = \sum_{\lceil \|b_i\| \rceil \leq 0} (-\lceil \|b_i\| \rceil + 1), \quad |d(L)| = \sum_{i=1}^{n} \lceil \|b_i\| \rceil,$$

for any semi-reduced basis $\mathcal{B} = (b_1, \ldots, b_n)$ *of* $(L, \| \|)$. *If* $\mathcal{B}$ *is ordered by increasing lengths and* $s_1 \leq \cdots \leq s_n$ *are the successive minima of* $(L, \| \|)$, *then* $\lceil s_i \rceil = \lceil \|b_i\| \rceil$, *for* $1 \leq i \leq n$.

Proof. By Proposition 2.2.5 item *3* and Lemma 2.5.8 the statements hold for any reduced basis. Since the formulae just apply the integer part of the norm of the vectors b_i, both identities hold for semi-reduced bases by Theorem 2.8.13. □

Assumption:
We assume for the rest of this chapter that $\dim(\mathcal{O}_E, \| \|_0) > 0$. In other words, we require that there exist vectors of $\| \|_0$-length 0 in $\mathcal{O}_E$.

Note that the following definition always depend on the bilinear form B and the chosen submodules $\mathcal{O}_E$ and $\mathcal{O}_{E,\infty}$.

Definition 3.1.10 (Genus)**.** *The* genus *of* $\mathrm{LS}(E)$ *with respect to* $(\mathcal{O}_E, \| \|_0)$ *is defined by*

$$g_E := \frac{\dim \mathcal{O}_E - n + |d(\mathcal{O}_E)|}{\dim \mathcal{O}_E}.$$

In Chapter 4 we will see that the genus of an algebraic function field is determined by the latter formula (cf. (4.8)).

Lemma 3.1.11. *The genus g_E is a nonnegative rational number.*

Proof. Clearly, g_E belongs to $\mathbb{Q}$, since $\dim \mathcal{O}_E, n$, and $|d(\mathcal{O}_E)|$ are integers. We show that $\dim \mathcal{O}_E - n + |d(\mathcal{O}_E)| \geq 0$. Denote by $\mathcal{B} = (b_1, \ldots, b_n)$ a reduced basis of $(\mathcal{O}_E, \| \|_0)$. Note that $\| \|_0$ is integer-valued; then, we have by Corollary 3.1.9

$$\begin{aligned} \dim \mathcal{O}_E - n + |d(\mathcal{O}_E)| &= \sum_{\|b_i\|_0 \leq 0} (-\|b_i\|_0 + 1) + \sum_{i=1}^{n} (\|b_i\|_0 - 1) \\ &= \sum_{\|b_i\|_0 > 0} (\|b_i\|_0 - 1) \geq 0. \end{aligned} \tag{3.1}$$

□

Theorem 3.1.12. *For any lattice $(L, \| \|) \in \mathrm{LS}(E)$, it holds that*

$$\dim L \geq \deg L + \dim(\mathcal{O}_E)(1 - g_E).$$

Proof. Denote by $\mathcal{B} = (b_1, \ldots, b_n)$ a semi-reduced basis of $(L, \| \|)$. Then, by Corollary 3.1.9 and the genus formula we obtain

$$\begin{aligned} \dim L &= \sum_{\lceil \|b_i\| \rceil \leq 0} (-\lceil \|b_i\| \rceil + 1) \geq \sum_{i=1}^{n} (-\lceil \|b_i\| \rceil + 1) \\ &= -|d(L)| + n = \deg L - |d(\mathcal{O}_E)| + n = \deg L + \dim(\mathcal{O}_E)(1 - g_E). \end{aligned}$$

□

3.2 Dual and complementary lattices

Definition 3.2.1 (Dual basis)**.** *Let $\mathcal{B} = (b_1, \ldots, b_n)$ be a basis of E. The* dual basis *$\mathcal{B}^\# = (b_1^\#, \ldots, b_n^\#)$ of $\mathcal{B}$ (with respect to the bilinear form* B*) is defined by*

$$\mathrm{B}(b_i, b_j^\#) = \delta_{i,j}, \quad \text{for } 1 \leq i, j \leq n.$$

If $\mathcal{B}'$ is another basis of E and $R = T(\mathcal{B} \to \mathcal{B}')$, then it is well-known that $R^{\mathrm{tr}} = T(\mathcal{B}'^\# \to \mathcal{B}^\#)$.

Let $\| \| \in \mathrm{Norm}(E)$. Denote by $\mathcal{B}$ a semi-orthonormal basis of $(E, \| \|)$ and $\mathcal{B}^\#$ its dual one. We define the *dual norm* of $\| \|$ to be $\| \|^\# := \| \|_{\mathcal{B}^\#}$, the by $\mathcal{B}^\#$ induced norm from Lemma-Definition 3.1.1, hence $\| \|^\# \in \mathrm{Norm}(E)$. By Theorem 2.8.7 and Lemma 3.1.2, any norm $\| \|'$ equivalent to $\| \|$ determines the same dual norm. We call the class of $\| \|^\#$ the *dual class* of the class $[\| \|]$.

Definition 3.2.2 (Dual Lattice)**.** *Let* $(L, \| \ \|)$ *be a lattice. We fix* $L^{\#} := \{z \in E \mid \mathrm{B}(z, z') \in A$, *for all* $z' \in L\}$, *and define the* dual lattice *by* $(L^{\#}, \| \ \|^{\#})$. *The dual lattice of* $(\mathcal{O}_E, \| \ \|_0)$ *is called the* different lattice *of* $\mathrm{LS}(E)$ *and its class the* different class *of* $\mathrm{LS}(E)$.

The next result follows immediately from the definitions.

Lemma 3.2.3. *The dual lattice* $(L^{\#}, \| \ \|^{\#})$ *is a lattice in* $(E, \| \ \|^{\#})$ *and for any basis* $\mathcal{B}$ *of* L, *the set* $\mathcal{B}^{\#}$ *is a basis of* $L^{\#}$.

Proposition 3.2.4. *Let* $\mathcal{B} = (b_1, \ldots, b_n)$ *be a semi-reduced basis of* $(L, \| \ \|) \in \mathrm{LS}(E)$. *Then,* $\mathcal{B}^{\#} = (b_1^{\#}, \ldots, b_n^{\#})$ *is a reduced basis of* $(L^{\#}, \| \ \|^{\#})$. *Moreover, it holds that* $|d(L, \| \ \|)| = -|d(L^{\#}, \| \ \|^{\#})|$ *and* $\lceil \|b_i\| \rceil = -\lceil \|b_i^{\#}\|^{\#} \rceil$, *for* $1 \leq i \leq n$.

Proof. The semi-reduced basis $\mathcal{B}$ induces the semi-orthonormal basis $\mathcal{D} := (t^{-\lceil \|b_1\| \rceil} b_1, \ldots, t^{-\lceil \|b_n\| \rceil} b_n)$. Hence, $\| \ \|^{\#} = \| \ \|_{\mathcal{D}^{\#}}$ and $\mathcal{D}^{\#}$ is an orthonormal basis of $(E, \| \ \|^{\#})$. Since $T := T(\mathcal{B} \to \mathcal{D}) = \mathrm{diag}(t^{\lceil \|b_1\| \rceil}, \ldots, t^{\lceil \|b_n\| \rceil})$, the transition matrix $T^{\#} := T(\mathcal{B}^{\#} \to \mathcal{D}^{\#})$ is given by $(T^{-1})^{\mathrm{tr}} = \mathrm{diag}(t^{-\lceil \|b_1\| \rceil}, \ldots, t^{-\lceil \|b_n\| \rceil})$. Hence, $\mathcal{B}^{\#}$ is a reduced basis of $(L^{\#}, \| \ \|^{\#})$.

Clearly, $|d(L, \| \ \|)| = |\det T| = -|\det T^{\#}| = -|d(L^{\#}, \| \ \|^{\#})|$. Since $\mathcal{D}^{\#} = (d_1^{\#}, \ldots, d_n^{\#})$ is an orthonormal basis of $(L^{\#}, \| \ \|^{\#})$ and $\| \ \|^{\#}$ is integer-valued, we have $\|b_i^{\#}\| = \|t^{-\lceil \|b_i\| \rceil} d_i^{\#}\|^{\#} = -\lceil \|b_i\| \rceil$, for $1 \leq i \leq n$. □

Definition 3.2.5 (Complementary Lattice)**.** *For a lattice* $(L, \| \ \|) \in \mathrm{LS}(E)$, *we define the* complementary lattice $(L^*, \| \ \|^*)$ *of* $(L, \| \ \|)$ *by* $L^* := L^{\#}$ *and* $\| \ \|^* := \| \ \|^{\#} + 2$.

Clearly, $(L^*, \| \ \|^*)$ is a lattice, since $(L^{\#}, \| \ \|^{\#})$ is a lattice.

Equivalent lattices determine the same complementary lattice.

Lemma 3.2.6. *For* $\| \ \| \in \mathrm{Norm}(E)$ *it holds* $(\| \ \|^{\#})^{\#} = \lceil \| \ \| \rceil$ *and* $(\| \ \|^*)^* = \lceil \| \ \| \rceil$.

Proof. Let $\mathcal{B} = (b_1, \ldots, b_n)$ be a semi-orthonormal basis of $(E, \| \ \|)$. Then, $\mathcal{B}^{\#} = (b_1^{\#}, \ldots, b_n^{\#})$ is an orthonormal basis of $(E, \| \ \|^{\#})$ by Proposition 3.2.4. Since $(\mathcal{B}^{\#})^{\#} = \mathcal{B}$ we have $(\| \ \|^{\#})^{\#} = \| \ \|_{\mathcal{B}}$ by definition. Then, Lemma 3.1.2 shows that $\| \ \|_{\mathcal{B}} = \lceil \| \ \| \rceil$.

Since $\mathcal{B}^{\#}$ is an orthonormal basis of $(E, \| \ \|^{\#})$, $\mathcal{B}^{\#}$ is reduced with respect to $\| \ \|^*$ with $\|b_i^{\#}\|^* = 2$, for $1 \leq i \leq n$. Then, the family $\mathcal{B}^* := t^{-2}\mathcal{B}^{\#}$ is an orthonormal basis of $(E, \| \ \|^*)$. By definition we have $(\| \ \|^*)^* = (\| \ \|^*)^{\#} + 2$, where $(\| \ \|^*)^{\#} = \| \ \|_{(\mathcal{B}^*)^{\#}}$. Since $\mathcal{B}$ is the dual basis of $\mathcal{B}^{\#}$, the basis $(\mathcal{B}^*)^{\#}$ coincides with $t^2\mathcal{B}$. Hence, $\| \ \|_{(\mathcal{B}^*)^{\#}} = \| \ \|_{t^2\mathcal{B}} = \lceil \| \ \| \rceil - 2$ and therefore $(\| \ \|^*)^* = \lceil \| \ \| \rceil - 2 + 2 = \lceil \| \ \| \rceil$. □

Lemma 3.2.7.

1. *For* $(L, \| \,\|) \in \mathrm{LS}(E)$*, it holds that* $\dim L = \dim L^* - |d(L)| + n$.

2. *The genus satisfies* $g_E = \dim \mathcal{O}_E^* / \dim \mathcal{O}_E$.

Proof. By Proposition 3.2.4 a semi-reduced basis $\mathcal{B} = (b_1, \ldots, b_n)$ of $(L, \| \,\|)$ induces a reduced basis $\mathcal{B}^\# = (b_1^\#, \ldots, b_n^\#)$ of the dual lattice $(L^\#, \| \,\|^\#)$, which is also a reduced basis of $(L^*, \| \,\|^*)$, since $\| \,\|^* = \| \,\|^\# + 2$. In particular, we have $\|b_i^\#\|^* = \|b_i^\#\|^\# + 2$ and $\|b_i^\#\|^\# = -\lceil \|b_i\| \rceil$, for $1 \leq i \leq n$. Then, by Corollary 3.1.9, it holds

$$\dim L^* = \sum_{\|b_i^\#\|^* \leq 0} (-\|b_i^\#\|^* + 1) = \sum_{\|b_i^\#\|^\# + 2 \leq 0} (-\|b_i^\#\|^\# - 1) = \sum_{\lceil \|b_i\| \rceil \geq 2} (\lceil \|b_i\| \rceil - 1).$$

Since $\dim L = \sum_{\lceil \|b_i\| \rceil \leq 0} (-\lceil \|b_i\| \rceil + 1)$, we obtain $\dim L - \dim L^* = \sum_{i=1}^n (-\lceil \|b_i\| \rceil + 1) = -|d(L)| + n$. This proves item one.

For the second statement we consider (3.1) and deduce that $\dim \mathcal{O}_E - n + |d(\mathcal{O}_E)| = \sum_{\|b_i\|_0 > 0} (\|b_i\|_0 - 1)$, where $(b_1, \ldots, b_n)$ is a reduced basis of the lattice $(\mathcal{O}_E, \| \,\|_0)$. For $1 \leq i \leq n$, it holds $-\|b_i\|_0 = \|b_i^\#\|^\#$ and $-\|b_i\|_0 + 2 = \|b_i^\#\|^*$. Since $(b_1^\#, \ldots, b_n^\#)$ is a reduced basis of $(\mathcal{O}_E^*, \| \,\|^*)$, by Corollary 3.1.9 we obtain

$$\dim(\mathcal{O}_E^*, \| \,\|^*) = \sum_{\|b_i^\#\|^* \leq 0} (-\|b_i^\#\|^* + 1) = \sum_{\|b_i\|_0 > 0} (\|b_i\|_0 - 1) = \dim \mathcal{O}_E - n + |d(\mathcal{O}_E)|.$$

Hence, by the genus formula yields $g_E = \dim \mathcal{O}_E^* / \dim \mathcal{O}_E$. □

3.3 Isometry classes in lattice spaces

Two lattices $(L, \| \,\|)$ and $(L', \| \,\|')$ in $\mathrm{LS}(E)$ are called isometric if $\mathrm{sm}(L, \| \,\|) = \mathrm{sm}(L', \| \,\|')$. In that case we write $(L, \| \,\|) \simeq (L', \| \,\|')$.

Definition 3.3.1. *Let* $(L, \| \,\|)$ *be a lattice in* $\mathrm{LS}(E)$*. The set of all lattices* $(L', \| \,\|') \in \mathrm{LS}(E)$ *with* $(L, \| \,\|) \simeq (L', \| \,\|')$ *is called the isometry class of* $(L, \| \,\|)$.

Definition 3.3.2. *We call two lattices* $(L_1, \| \,\|_1)$ *and* $(L_2, \| \,\|_2)$ equivalent*, and write* $(L_1, \| \,\|_1) \cong (L_2, \| \,\|_2)$*, if there exist a norm* $\| \,\| \in \mathrm{Norm}(E)$ *with* $\| \,\| \sim \| \,\|_2$*, such that* $(L_1, \| \,\|_1) \simeq (L_2, \| \,\|)$.

Note that this definition is compatible with the equivalence relation from Definition 2.8.2; that is, if $L_1 = L_2$ with $\| \,\|_1 \sim \| \,\|_2$, then $(L_1, \| \,\|_1) \cong (L_2, \| \,\|_2)$. Clearly, $\cong$ defines an equivalence relation on $\mathrm{LS}(E)$.

All equivalent lattices have the same degree and same dimension. In fact, two isometric lattices have the same degree and dimension and two equivalent norms lead to the same degree and dimension on any concrete sub-A-module $L \subset E$ of full rank.

The concept of principal and canonical divisors in algebraic function fields has an analogy in lattice spaces.

Definition 3.3.3 (Principal lattice class)**.** *Any lattice* $(L, \| \ \|)$ *in* $\mathrm{LS}(E)$*, which is equivalent to* $(\mathcal{O}_E, \| \ \|_0)$*, is called a* principal lattice *of* $\mathrm{LS}(E)$*. The class of* $(\mathcal{O}_E, \| \ \|_0)$ *is called the* principal lattice class *in* $\mathrm{LS}(E)/\cong$*.*

By this definition we obtain immediately the following statement.

Lemma 3.3.4. *For a principal lattice* $(L, \| \ \|)$ *it holds* $\deg L = 0$ *and* $\dim L = \dim \mathcal{O}_E$*.*

Definition 3.3.5 (Canonical lattice class)**.** *Any lattice* $(L, \| \ \|)$ *in* $\mathrm{LS}(E)$*, which is equivalent to* $(\mathcal{O}_E^*, \| \ \|_0^*)$*, is called a* canonical lattice *of* $\mathrm{LS}(E)$*. The class of* $(\mathcal{O}_E^*, \| \ \|_0^*)$ *is called the* canonical lattice class *in* $\mathrm{LS}(E)/\cong$*.*

Lemma 3.3.6. *For a canonical lattice* $(L, \| \ \|)$*, it holds*

$$\deg L = 2\dim(\mathcal{O}_E)(g_E - 1) \text{ and } \dim L = \dim(\mathcal{O}_E) g_E.$$

Proof. Since equivalent lattices have the same degree and dimension, it is sufficient to show that $(\mathcal{O}_E^*, \| \ \|_0^*)$ satisfies the identities. We consider the second identity. By Lemma 3.2.7 we have $\dim \mathcal{O}_E^* = \dim \mathcal{O}_E + |d(\mathcal{O}_E)| - n = \dim(\mathcal{O}_E) g_E$.

For the first identity, let $\mathcal{B}$ be a reduced basis of $(\mathcal{O}_E^*, \| \ \|_0^*)$. Then, by Corollary 3.1.9 and $|d(\mathcal{O}_E^\#)| = -|d(\mathcal{O}_E)|$ (by Proposition 3.2.4), it holds

$$\begin{aligned}\deg \mathcal{O}_E^* = -|d(\mathcal{O}_E^*)| + |d(\mathcal{O}_E)| &= -\sum_{b \in \mathcal{B}} \|b\|_0^* + |d(\mathcal{O}_E)| = -\sum_{b \in \mathcal{B}} (\|b\|_0^\# + 2) + |d(\mathcal{O}_E)| \\ &= 2(|d(\mathcal{O}_E)| - n) = 2\dim(\mathcal{O}_E)(g_E - 1),\end{aligned}$$

where the last identity follows by the genus formula. □

We are going to introduce a partial ordering on $\mathbb{R}^n$.

Definition 3.3.7. *Let* $S = (s_1, \ldots, s_n)$ *and* $S' = (s_1', \ldots, s_n')$ *be in* $\mathbb{R}^n$*. We write* $S \leq S'$*, if* $s_i \leq s_i'$ *for* $1 \leq i \leq n$*.*

This definition allows us to compare two lattice $(L, \| \ \|)$ and $(L', \| \ \|')$ in $\mathrm{LS}(E)$ with respect to their successive minima.

We consider a collection of properties of lattices with respect to their successive minima. The goal of the next lemma is its last item, which will be applied in Chapter 4 in the context of algebraic function fields (cf. Theorem 4.3.6)

Lemma 3.3.8. *Let L, L' be two A-modules of full rank in E and $\| \ \|, \| \ \|'$ two norms in* $\mathrm{Norm}(E)$.

1. $(L, \| \ \|)$ *belongs to* $\mathrm{LS}(E)$.
2. *If $L \subseteq L'$, then* $\mathrm{sm}(L', \| \ \|) \leq \mathrm{sm}(L, \| \ \|)$.
3. *If $\|z\|' \leq \|z\|$, for all $z \in E$, then* $\mathrm{sm}(L, \| \ \|') \leq \mathrm{sm}(L, \| \ \|)$.
4. *It holds $(E, \| \ \|)_{\leq 0} \subseteq (E, \| \ \|')_{\leq 0}$ if and only if $\lceil \|z\|' \rceil \leq \lceil \|z\| \rceil$, for all $z \in E$.*
5. *For $(E, \| \ \|)_{\leq 0} \subseteq (E, \| \ \|')_{\leq 0}$ with $\mathrm{sm}(E, \| \ \|) = \mathrm{sm}(E, \| \ \|')$, it holds $\|z\|' \leq \|z\|$, for all $z \in E$.*
6. *For $L \subseteq L'$ and $(E, \| \ \|)_{\leq 0} \subseteq (E, \| \ \|')_{\leq 0}$ with $\mathrm{sm}(E, \| \ \|) = \mathrm{sm}(E, \| \ \|')$, it holds $\mathrm{sm}(L', \| \ \|') \leq \mathrm{sm}(L, \| \ \|)$.*

Proof. The first item is obvious by the definition of normed spaces and lattices.

The second and third items follow immediately from the definition of successive minima.

We consider the fourth statement. Assume $(E, \| \ \|)_{\leq 0} \subseteq (E, \| \ \|')_{\leq 0}$ and take any $z \in E$. There exists $m \in \mathbb{Z}$ such that $\lceil \|t^m z\| \rceil = 0$. By assumption, it holds $\lceil \|t^m z\|' \rceil \leq 0$; hence, $\lceil \|z\|' \rceil \leq -m = \lceil \|z\| \rceil$. Conversely, assume that $\lceil \|z\|' \rceil \leq \lceil \|z\| \rceil$, for all $z \in E$. Then, $\|z\| \leq 0$ implies that $\|z\|' \leq \lceil \|z\|' \rceil \leq \lceil \|z\| \rceil \leq 0$.

For the proof of item *5*, we fix two orthonormal bases $\mathcal{B} = (b_1, \ldots, b_n)$ and $\mathcal{B}' = (b'_1, \ldots, b'_n)$ of $(E, \| \ \|)$ and $(E, \| \ \|')$, respectively. As $\mathrm{sm}(E, \| \ \|) = \mathrm{sm}(E, \| \ \|')$, we have $\|b_i\| = \|b'_i\|'$, for $1 \leq i \leq n$. Denote $T = (t_{i,j})$ the transition matrix from $\mathcal{B}$ to $\mathcal{B}'$. Without loss of generality, let $z \in E$ with $\|z\|, \|z\|' \leq 0$ (otherwise we multiply z with an adequate t-power). We write $z = \sum_{i=1}^n \lambda_i b_i = \sum_{i=1}^n \lambda'_i b'_i$ with coefficients λ_i, λ'_i in K, which satisfy by construction $|\lambda_i|, |\lambda'_i| \leq 0$ and $(\lambda_1 \ldots \lambda_n)T = (\lambda'_1 \ldots \lambda'_n)$. Since $(E, \| \ \|)_{\leq 0} \subseteq (E, \| \ \|')_{\leq 0}$, it holds that $T \in A_\infty^{n \times n}$ and therefore

$$|\lambda'_i| = \Big| \sum_{j=1}^n t_{j,i} \lambda_j \Big| \leq \max_{1 \leq j \leq n} \{|t_{j,i}| + |\lambda_j|\} \leq \max_{1 \leq j \leq n} \{|\lambda_j|\}.$$

As $\|z\| = \max_{1 \leq j \leq n} \{|\lambda_j| + \|b_j\|\}$, $\|z\|' = \max_{1 \leq j \leq n} \{|\lambda'_j| + \|b'_j\|'\}$, and $\|b_j\| = \|b'_j\|'$, for $1 \leq j \leq n$, we deduce $\|z\|' \leq \|z\|$.

For the last statement, from $L \subseteq L'$ we deduce $\mathrm{sm}(L', \| \|') \leq \mathrm{sm}(L, \| \|')$ by item *2.* As $(E, \| \|)_{\leq 0} \subseteq (E, \| \|')_{\leq 0}$ with $\mathrm{sm}(E, \| \|) = \mathrm{sm}(E, \| \|')$, by item *5* it holds $\|z\|' \leq \|z\|$, for all $z \in E$. Thus, we obtain $\mathrm{sm}(L, \| \|') \leq \mathrm{sm}(L, \| \|)$ by item *3.* Hence, $\mathrm{sm}(L', \| \|') \leq \mathrm{sm}(L, \| \|)$. □

Definition 3.3.9. *Let $(L, \| \|)$ be a lattice and $s_1 \leq \cdots \leq s_n$ its successive minima. We define the* normalized successive minima *of $(L, \| \|)$ to be the vector*

$$\mathrm{sm}_0(L, \| \|) := (s_1 - \lceil s_1 \rceil, \ldots, s_n - \lceil s_1 \rceil).$$

Note that the normalized successive minima are real numbers, which are strictly greater than -1.

Lemma 3.3.10. *For any lattice $(L, \| \|) \in \mathrm{LS}(E)$, it holds that*

$$\mathrm{sm}_0(L, \| \|) = \mathrm{sm}(L, \| \| - \lceil s \rceil), \quad s := \min \mathrm{sm}(L, \| \|).$$

The successive minima of $(\mathcal{O}_E, \| \|_0)$ are already normalized. More precisely, if $\mathrm{sm}(\mathcal{O}_E, \| \|_0) = (s_1, \ldots, s_n)$, then $s_1 = \cdots = s_l = 0 < s_{l+1}$ where $l := \dim \mathcal{O}_E$.

Proof. The first statements are obvious. Let $\mathcal{B} = (b_1, \ldots, b_n)$ be a reduced basis of $(\mathcal{O}_E, \| \|_0)$ with $\|b_i\| = s_i$, for $1 \leq i \leq n$. Note that $\|z\|_0 \in \mathbb{Z}$, for all $z \in E$. If $\|b_i\|_0 < 0$, then tb_i belongs to $(\mathcal{O}_E, \| \|_0)_{\leq 0}$ and by Corollary 3.1.6 it holds $\mathrm{B}(tb_i, tb_i) = t^2 \mathrm{B}(b_i, b_i) \in k$, a contradiction, since $\mathrm{B}(b_i, b_i) \in k$. Thus, $s_1 = 0$ and $\dim \mathcal{O}_E = \max\{1 \leq l \leq n \mid s_l = 0\}$ by Proposition 2.2.5. □

Note in particular that $\dim \mathcal{O}_E \leq n$.

Definition 3.3.11 (Diameter)**.** *For a lattice $(L, \| \|)$, we define its* diameter *to be the nonnegative rational number*

$$\mathrm{diam}(L, \| \|) := \max \mathrm{sm}(L, \| \|) - \min \mathrm{sm}(L, \| \|).$$

We define the diameter *of $\mathrm{LS}(E)$ with respect to $\mathcal{O}_E$ to be the diameter of $(\mathcal{O}_E, \| \|_0)$ and write* $\mathrm{diam}(\mathrm{LS}(E))$.

Lemma 3.3.12. *If $\dim \mathcal{O}_E = n$, then $\mathrm{diam}(\mathrm{LS}(E)) = 0$. For $\dim \mathcal{O}_E < n$ we have $\mathrm{diam}(\mathrm{LS}(E)) \leq g_E \dim \mathcal{O}_E + 1$.*

Proof. For $\dim \mathcal{O}_E = n$ the statement follows immediately from Lemma 3.3.10.

Suppose $\dim \mathcal{O}_E < n$. Let $\mathcal{B} = (b_1, \ldots, b_n)$ be an ordered reduced basis of $(\mathcal{O}_E, \| \|_0)$. By Lemma 3.3.10 we have $\mathrm{diam}(\mathrm{LS}(E)) = \mathrm{diam}(\mathcal{O}_E, \| \|_0) = \|b_n\|_0$, and $\|b_i\|_0 = 0$, for

$1 \leq i \leq l$ with $l := \dim \mathcal{O}_E$. Since $\sum_{i=1}^{n} \|b_i\|_0 = |d(\mathcal{O}_E)|$ by Corollary 3.1.9, we can estimate $\|b_n\|_0$ by

$$\|b_n\|_0 - 1 \leq \sum_{i=1}^{n} \|b_i\|_0 - \sum_{\|b_i\|_0 > 0} 1 = |d(\mathcal{O}_E)| - \sum_{i=l+1}^{n} 1 = |d(\mathcal{O}_E)| - (n - \dim \mathcal{O}_E).$$

By the definition of the genus, we obtain $\|b_n\|_0 \leq |d(\mathcal{O}_E)| - (n - \dim \mathcal{O}_E) + 1 = g_E \dim \mathcal{O}_E + 1$. □

From now on we will consider a subset of the lattice space $\mathrm{LS}(E)$. The following restriction may seem curios, however according to Theorem 4.3.6 this situation occurs in the context of algebraic function fields.

Definition 3.3.13 (Bounded lattice space)**.** *For a vector $S = (s_1, \ldots, s_n) \in \mathbb{R}^n$ with $-1 < s_1 \leq \cdots \leq s_n$, we define the* lattice space of length S *to be the set*

$$\mathrm{LS}(E)_S := \{(L, \| \|) \in \mathrm{LS}(E) \mid \mathrm{sm}_0(L, \| \|) \leq S\}.$$

Let $R = \{r_1 + \mathbb{Z}, \ldots, r_n + \mathbb{Z}\}$ be a multiset in $\mathbb{R}/\mathbb{Z}$. Then, we define the R-lattice space of length S *by*

$$\mathrm{LS}(E, R)_S := \{(L, \| \|) \in \mathrm{LS}(E, R) \mid \mathrm{sm}_0(L, \| \|) \leq S\}.$$

Any norm $\| \|' \in \mathrm{Norm}(E)$ with $\| \|' \sim \| \|_0$ induces a R-lattice space $\mathrm{LS}(E, R)_S$ of length S by taking $S = (s_1, \ldots, s_n) = \mathrm{sm}(\mathcal{O}_E, \| \|')$ and $R = \mathrm{sm}(E, \| \|')$. We will see in Chapter 4 that the divisor group of an algebraic function field F/k, given by an defining polynomial of degree n, can be considered as a subset of $\mathrm{LS}(F, R)_S$ by choosing $\| \|' = -\min_{P \in \mathbb{P}_\infty(F)}\{v_P(\ )/e(P/P_\infty)\}$.

We are interested in $\mathrm{LS}(E)_S$, for $S := \mathrm{sm}(\mathcal{O}_E, \| \|_0)$, the set of lattices, whose normalized successive minima are bounded by $\mathrm{sm}(\mathcal{O}_E, \| \|_0)$.

The relation $\cong$ from Definition 3.3.2 restricted to $\mathrm{LS}(E)_S$ determines again an equivalence relation and therefore equivalence classes. Clearly, if the lattice $(L, \| \|)$ belongs to $\mathrm{LS}(E)_S$, then its class belongs to $\mathrm{LS}(E)_S/\cong$. The principal lattice class is contained in $\mathrm{LS}(E)_S/\cong$, since $S = \mathrm{sm}(\mathcal{O}_E, \| \|_0)$.

Note that all subsequent statements are still true in the latter setting, that is for the lattice space $\mathrm{LS}(E, R)_S$ induced by a norm $\| \|'$ equivalent to $\| \|_0$.

Lemma 3.3.14. *Let* $(L, \| \|) \in \mathrm{LS}(E)_S$*, where* $S = \mathrm{sm}(\mathcal{O}_E, \| \|_0)$*.*

1. $\mathrm{diam}(L, \| \|) < \mathrm{diam}(\mathcal{O}_E, \| \|_0) + 1$*.*
2. *If* $\deg L < 0$*, then* $\dim L = 0$*.*
3. $(L, \| \|)$ *is principal if and only if* $\deg L = 0$ *and* $\dim L > 0$*.*

Proof. Since $\mathrm{diam}(L, \| \|) = \mathrm{diam}(L, \| \| + r)$, for all $r \in \mathbb{R}$, the first statement follows from the definition of $\mathrm{LS}(E)_S$.

In order to proof the second item we denote by $l_1 \leq \cdots \leq l_n$ and $s_1 \leq \cdots \leq s_n$ the successive minima of $(L, \| \|)$ and $(\mathcal{O}_E, \| \|_0)$, respectively. By Corollary 3.1.9 it holds $|d(L, \| \|)| = \sum_{i=1}^n \lceil l_i \rceil$ and $|d(\mathcal{O}_E, \| \|_0)| = \sum_{i=1}^n \lceil s_i \rceil$. Then, the condition $\deg L < 0$ is equivalent to $\sum_{i=1}^n \lceil s_i \rceil < \sum_{i=1}^n \lceil l_i \rceil$ by the definition of the degree. Let $r := \lceil l_1 \rceil$. By hypothesis, $l_i - r \leq s_i$ for $1 \leq i \leq n$. Thus,

$$-nr + \sum_{i=1}^n \lceil l_i \rceil \leq \sum_{i=1}^n \lceil s_i \rceil < \sum_{i=1}^n \lceil l_i \rceil.$$

Hence, $r = \lceil l_1 \rceil > 0$ and this implies $\dim L = 0$ by Corollary 3.1.9.

One direction of the third statement follows directly from Lemma 3.3.4. For the other one we assume that $\deg L = 0$ and $\dim L > 0$. Since we are assuming that $\dim \mathcal{O}_E > 0$, this implies $\lceil l_1 \rceil \leq 0$ by Corollary 3.1.9. In particular, $(l_1, \ldots, l_n) = \mathrm{sm}(L, \| \|) \leq \mathrm{sm}_0(L, \| \|) \leq (s_1, \ldots, s_n)$. Since $\deg L = 0$, we obtain $|d(\mathcal{O}_E, \| \|_0)| = |d(L, \| \|)|$ and equivalently $\sum_{i=1}^n \lceil s_i \rceil = \sum_{i=1}^n \lceil l_i \rceil$. Thus, $\lceil l_i \rceil = \lceil s_i \rceil = s_i$, for $1 \leq i \leq n$, since $\| \|_0$ is integer valued. Since $\| \| \sim \lceil \| \| \rceil$, we obtain $\mathrm{sm}(L, \lceil \| \| \rceil) = (\lceil l_1 \rceil, \ldots, \lceil l_n \rceil) = (s_1, \ldots, s_n) = \mathrm{sm}(\mathcal{O}_E, \| \|_0)$; hence $(L, \| \|) \cong (\mathcal{O}_E, \| \|_0)$. □

Theorem 3.3.15 (Riemann's theorem)**.** *Let* $S = \mathrm{sm}(\mathcal{O}_E, \| \|_0)$*. For any lattice* $(L, \| \|) \in \mathrm{LS}(E)_S$ *with* $\deg L \geq |d(\mathcal{O}_E, \| \|_0)| - 2n + (n-1)\mathrm{diam}(\mathrm{LS}(E)) + 1$ *it holds*

$$\dim L = \deg L + \dim(\mathcal{O}_E)(1 - g_E).$$

Proof. Let $(L, \| \|) \in \mathrm{LS}(E)_S$ and $\mathcal{B} = (b_1, \ldots, b_n)$ be a reduced basis of $(L, \| \|)$ ordered by increasing length. By Theorem 3.1.12 it holds $\dim L \geq \deg L + \dim(\mathcal{O}_E)(1 - g_E)$. In the corresponding proof we have seen that this is equivalent to

$$\sum_{\lceil \|b_i\| \rceil \leq 0} (-\lceil \|b_i\| \rceil + 1) \geq \sum_{i=1}^n (-\lceil \|b_i\| \rceil + 1).$$

Equality holds if and only if $\lceil \|b_n\| \rceil \leq 1$, since $\lceil \|b_i\| \rceil \leq \lceil \|b_n\| \rceil$, for $1 \leq i \leq n-1$.

Let $(L', \| \|')$ be a lattice having the successive minima $l'_1 = \cdots = l'_{n-1} = 2 - \mathrm{diam}(\mathrm{LS}(E))$; $l'_n = 2$. By construction $(L', \| \|')$ belongs to $\mathrm{LS}(E)_S$ with $\dim L > \deg L + \dim(\mathcal{O}_E)(1 - g_E)$. For any $(L, \| \|) \in \mathrm{LS}(E)_S$ with successive minima $l_1 \leq \cdots \leq l_n$ satisfying $\deg L > \deg L'$ it holds $l_n = 1$, since otherwise $\mathrm{diam}(L, \| \|) > 2-(2-\mathrm{diam}(\mathrm{LS}(E))) = \mathrm{diam}(\mathrm{LS}(E))$, a contradiction. Hence, for any lattice $(L, \| \|) \in \mathrm{LS}(E)_S$ with

$$\begin{aligned}\deg L \geq \deg L' + 1 &= |d(\mathcal{O}_E, \| \|_0)| - \sum_{i=1}^{n} \lceil l'_i \rceil + 1 \\ &= |d(\mathcal{O}_E, \| \|_0)| - \left(\sum_{i=1}^{n-1} (2 - \mathrm{diam}(\mathrm{LS}(E))) + 2 \right) + 1 \\ &= |d(\mathcal{O}_E, \| \|_0)| - 2n + (n-1)\mathrm{diam}(\mathrm{LS}(E)) + 1,\end{aligned}$$

we obtain $\dim L = \deg L + \dim(\mathcal{O}_E)(1 - g_E)$.

□

Lemma 3.3.16. *Suppose $n = 2$.*

1. *For $\dim \mathcal{O}_E = 1$ it holds $g_E \leq \mathrm{diam}(\mathrm{LS}(E)) \leq g_E + 1$.*

2. *For $\dim \mathcal{O}_E = 2$ it holds $g_E = 0$, $\mathrm{diam}(\mathrm{LS}(E)) = 0$.*

Proof. Let $\mathrm{sm}(\mathcal{O}_E, \| \|_0) = (s_1, s_2)$. Clearly, $|d(\mathcal{O}_E, \| \|_0)| = \lceil s_1 \rceil + \lceil s_2 \rceil$ by Corollary 3.1.9. For $\dim \mathcal{O}_E = 1$, it holds $s_1 = 0 < s_2$ and therefore $g_E = -1 + |d(\mathcal{O}_E, \| \|_0)| = -1 + \lceil s_2 \rceil \leq s_2 = \mathrm{diam}(\mathrm{LS}(E)) \leq g_E + 1$.

By Lemma 3.3.10 we obtain $s_1 = s_2 = 0$, for $\dim \mathcal{O}_E = 2$. Hence, $\mathrm{diam}(\mathrm{LS}(E)) = 0, |d(\mathcal{O}_E, \| \|_0)| = 0$ and the formula for the genus yields $g_E = 0$. □

Corollary 3.3.17. *Suppose $\dim_K E = 2$. For any lattice $(L, \| \|) \in \mathrm{LS}(E)_S$ with $\deg L \geq 2g_E - 1$ it holds*

$$\dim L = \deg L + 1 - g_E.$$

Proof. We apply Theorem 3.3.15 to this case. We obtain

$$|d(\mathcal{O}_E, \| \|_0)| - 2n + (n-1)\mathrm{diam}(\mathrm{LS}(E)) + 1 = |d(\mathcal{O}_E, \| \|_0)| + \mathrm{diam}(\mathrm{LS}(E)) - 3, \tag{3.2}$$

since $n = 2$. If $\dim(\mathcal{O}_E, \| \|_0) = 1$, the genus formula shows that $g_E = -1 + |d(\mathcal{O}_E, \| \|_0)|$ and by the last lemma we obtain $\mathrm{diam}(\mathrm{LS}(E)) \leq g_E + 1$. Hence, (3.2) is less than or equal to $2(g_E + 1) - 3 = 2g_E - 1$.

For $\dim(\mathcal{O}_E, \| \ \|_0) = 2$ we have seen in the proof of Lemma 3.3.16 that $\operatorname{diam}(\mathrm{LS}(E)) = 0, g_E = 0$, and $|d(\mathcal{O}_E, \| \ \|_0)| = 0$. Therefore, (3.2) is lower than $2g_E - 1$. Thus, in both cases the statement of the corollary follows from Theorem 3.3.15. □

4. Lattices in algebraic function fields

Let F/k be a function field with defining polynomial f of degree n. Then, F can be considered as an n-dimensional vector space over the rational function field K. In this chapter we will see that any divisor D in $\mathcal{D}_F$ induces a norm $\| \ \|_D$ and a normed space $(F, \| \ \|_D)$. Hence, the results from Chapter 2 become available in the context of algebraic function fields.

On the one hand, the theory of lattices in function fields can be used to compute a k-basis of the Riemann-Roch space of a divisor D and the successive minima of its induced lattice (cf. Section 4.1 and Subsection 4.3.1), and on the other hand to derive a formula for the genus of F/k, which admits a fast computation of this invariant by the Montes algorithm. Afterwards, we translate the results from Chapter 3 to algebraic function fields.

Recall that $e(P/P_\infty)$ denotes the ramification index of P over P_∞. For a given divisor D, we consider a divisor

$$D + r(t)_\infty = \sum_{Q \in \mathbb{P}_0(F)} \alpha_Q \cdot Q + \sum_{P \in \mathbb{P}_\infty(F)} (\beta_P + re(P/P_\infty)) \cdot P,$$

with $\alpha_Q, \beta_P, r \in \mathbb{Z}$. According to Subsection 1.2.3 the places $Q \in \mathbb{P}_0$ and $P \in \mathbb{P}_\infty$ are in one-to-one correspondence with prime ideals $\mathfrak{q}$ of $\mathcal{O}_F$ and $\mathfrak{p}$ of $\mathcal{O}_{F,\infty}$, respectively. Hence, the ideal representation of $D + r(t)_\infty$ is given by $(I, t^r I_\infty)$, where $I := \prod_{Q \in \mathbb{P}_0} \mathfrak{q}^{-\alpha_Q}$ and $I_\infty := \prod_{P \in \mathbb{P}_\infty} \mathfrak{p}^{-\beta_P}$ are fractional ideals of $\mathcal{O}_F$ and $\mathcal{O}_{F,\infty}$, respectively. In particular, I and I_∞ are A- and A_∞-modules of rank n, respectively. We consider on F the norm:

$$\| \ \|_D : F \to \{-\infty\} \cup \mathbb{Q}, \quad \|z\|_D = -\min_{P \in \mathbb{P}_\infty(F)} \left\{ \frac{v_P(z) + v_P(D)}{e(P/P_\infty)} \right\}. \tag{4.1}$$

Clearly, any divisor D induces a norm $\| \ \|_D$. As our considerations are relative to a fixed divisor D, we write $\| \ \|$ instead of $\| \ \|_D$. Note that $v_P = v_{\mathfrak{p}}$, for all places P of F/k and their corresponding prime ideal $\mathfrak{p}$ of F (cf. Subsection 1.2.3).

Theorem 4.0.1.

1. $\mathcal{L}(D + r(t)_\infty) = I \cap t^r I_\infty = (I, \| \ \|)_{\leq r}$.

2. $(I, \| \ \|)$ *is a lattice and* $(F, \| \ \|)$ *is a normed space.*

Proof. We consider the first identity of item *1.* For $z \in \mathcal{L}(D + r(t)_\infty)$, we obtain $(z) \geq -(D + r(t)_\infty)$ and equivalently

$$v_Q(z) \geq -\alpha_Q, \forall Q \in \mathbb{P}_0(F), \qquad v_P(z) \geq -\beta_P - re(P/P_\infty), \forall P \in \mathbb{P}_\infty(F).$$

Clearly, this is equivalent to $z \in I \cap t^r I_\infty$.

In order to proof the second identity of the first item we consider $z \in (I, \| \ \|)_{\leq r}$. That is, $z \in I$ with $\|z\| \leq r$, which is equivalent to

$$\min_{P \in \mathbb{P}_\infty(F)} \left\{ \frac{v_P(z) + v_P(D)}{e(P/P_\infty)} \right\} \geq -r \iff v_P(z) + \beta_P \geq -re(P/P_\infty), \forall P \in \mathbb{P}_\infty(F),$$

as $\beta_P = v_P(D)$. This is equivalent to $z \in I \cap t^r I_\infty$, since $z \in I$.

We consider the second item. Regarding Definition 2.1.5, we have to show that $\dim_k(I, \| \ \|)_{\leq r} < \infty$, for all $r \in \mathbb{R}$. This follows directly from item *1.* Then, Lemma 2.1.7 shows that the pair $(F, \| \ \|)$ is a normed space. □

Corollary 4.0.2. *Let* $\mathcal{B} = (b_1, \ldots, b_n)$ *be a semi-reduced basis of* $(I, \| \ \|)$. *Then,*

1. $I_\infty = (F, \| \ \|)_{\leq 0}$,

2. *the set* $\{b_i t^{j_i} \mid 1 \leq i \leq n, \ 0 \leq j_i \leq -\lceil \|b_i\| \rceil + r\}$ *is a k-basis of* $\mathcal{L}(D + r(t)_\infty)$,

3. $\dim_k(D + r(t)_\infty) = \sum_{\lceil \|b_i\| \rceil \leq r} (-\lceil \|b_i\| \rceil + r + 1)$.

Proof. By the last lemma $(I, \| \ \|)$ is a lattice. Then, by Corollary 2.8.11, the family $(t^{m_1} b_1, \ldots, t^{m_n} b_n)$ with $m_i := -\lceil \|b_i\| \rceil$, for $1 \leq i \leq n$, is a semi-orthonormal basis of $(F, \| \ \|)$. Hence, Lemma-Definition 2.8.9 yields the first item of the theorem.

The second item follows from the last lemma, Corollary 3.1.9, and Proposition 2.2.5. The third one follows from the second one. □

4.1 Computation of Riemann-Roch spaces

By Corollary 4.0.2, in order to compute a k-basis of the Riemann-Roch space $\mathcal{L}(D) = I \cap I_\infty$, it suffices to compute a semi-reduced A-basis of I. According to Subsection 2.8.1 a (semi-) orthonormal basis of the normed space F is required. By Lemma-Definition 2.8.9 and Corollary 4.0.2 any A_∞-basis of the A_∞-module I_∞ is semi-orthonormal. We summarize the computation of a basis of a Riemann-Roch space of a divisor D:

Algorithm 6: Riemann-Roch computation

Input: A-basis $\mathcal{B}$ of I and A_∞-basis $\mathcal{B}'$ of I_∞, where $\mathcal{L}(D) = I \cap I_\infty$.
Output: k-basis of $\mathcal{L}(D)$.

1: $\mathcal{D} \leftarrow (c_{\mathcal{B}'}(b) \mid b \in \mathcal{B})$
2: $(b_1, \ldots, b_n) \leftarrow$Algorithm 3$(\mathcal{D})$
3: **return** $\{c_{\mathcal{B}'}^{-1}(b_i)t^{j_i} \mid 1 \leq i \leq n,\ 0 \leq j_i \leq -\lceil \|c_{\mathcal{B}'}^{-1}(b_i)\| \rceil\}$

The correctness of the algorithm follows from the last corollary.

Note that Algorithm 6 basically coincides with the algorithm described in [16]. We will extend the latter algorithm in Subsection 4.3 by Algorithm 5 (the optimized reduction algorithm) in order to determine the successive minima of the by D induced lattice $(I, \| \ \|)$. In Chapter 5 we will present an algorithm, which determines both a basis of I and a (semi-) orthonormal basis of I_∞.

4.1.1 Complexity

To estimate the complexity of the computation of a basis of a Riemann-Roch space by Algorithm 6, we fix a divisor D and denote by (I, I_∞) its ideal representation; that is, $\mathcal{L}(D) = I \cap I_\infty$. We assume that bases $\mathcal{B}$ and $\mathcal{B}'$ of the fractional ideals I and I_∞ are available. In Chapter 5 we analyze the complexity of the computation of these bases (cf. Corollary 5.3.14 and Theorem 5.3.19). Moreover, we assume that both $\mathcal{B}$ and $\mathcal{B}'$ are Hermite bases and denote by T the transition matrix from $\mathcal{B}$ to $\mathcal{B}'$. Then, the rows of T are given by the coordinate vectors $c_{\mathcal{B}'}(b)$ for $b \in \mathcal{B}$.

Let $g_1, \ldots, g_n \in A$ be nonzero polynomials of minimal degree such that $\widetilde{T} := T \cdot \mathrm{diag}(g_1, \ldots, g_n) \in A^{n \times n}$. Then, the following statement follows immediately from Corollary 2.7.19.

Lemma 4.1.1. *Denote by $C(T)$ the cost of the computation of the transition matrix T. Then, algorithm 6 needs at most*

$$C(T) + O(n^4 h(\widetilde{T}) + n^3 h(\widetilde{T})^2)$$

arithmetic operations in k to determine a basis of $\mathcal{L}(D)$.

We are interested in a complexity estimation, which only depends on the data n and C_f of the defining polynomial f of the function field and on the divisor D (cf. Corollary 4.1.5). Therefore, we estimate $h(\widetilde{T})$ and $C(T)$ in terms of n, C_f and $h(D)$ (see below).

Definition 4.1.2 (Divisor height)**.** *For $D \in \mathfrak{D}_F \setminus \{0\}$, we define* the height *of D by $h(D) := \deg D^*$, where*

$$D^* := \sum_{P \in \mathbb{P}_F} |v_P(D)| \cdot P.$$

Note that the height of a divisor is a nonnegative integer and $h(D) = 0$ if and only if $D = 0$.

We will now formulate some technical lemmas, which will be useful for further complexity estimations.

Lemma 4.1.3. *Let F/k be a function field of genus g with defining polynomial f of degree n. Then, $\delta := |\operatorname{disc} f|$ and $\delta_\infty := v_\infty(\operatorname{disc} f_\infty)$ satisfy*

$$\delta, \delta_\infty \leq \delta + \delta_\infty = C_f n(n-1) = O(n^2 C_f).$$

In particular, it holds $|[\mathcal{O}_F : A[\theta]]| \leq \delta$ and $-|[\mathcal{O}_{F,\infty} : A_\infty[\theta_\infty]]| \leq \delta_\infty$.

Proof. The discriminant of f_∞ belongs to $k[t^{-1}]$ and $\operatorname{disc} f$ belongs to A. Hence, $\delta_\infty = v_\infty(\operatorname{disc} f_\infty)$, $\delta = \deg(\operatorname{disc} f) \geq 0$, and $\delta, \delta_\infty \leq \delta + \delta_\infty$. As $f_\infty = t^{-nC_f} f(t, t^{C_f} x)$, the discriminant of f_∞ satisfies by [27, p. 13]

$$\operatorname{disc} f_\infty = t^{-nC_f(2n-2)} t^{C_f(n^2-n)} \operatorname{disc} f = t^{-C_f n(n-1)} \operatorname{disc} f.$$

Therefore, $\delta_\infty = v_\infty(\operatorname{disc} f_\infty) = C_f n(n-1) - |\operatorname{disc} f| = C_f n(n-1) - \delta$. □

Lemma 4.1.4.

1. $h(I) + h(I_\infty) \leq H(I) + H(I_\infty) = O(h(D) + n^2 C_f)$.
2. $h(\widetilde{T}) = O(nh(D) + n^3 C_f)$.

Proof. In order to prove the first item we consider $D = \sum_{P\in\mathbb{P}_F} a_P P$ and set $D_0 := \sum_{P\in\mathbb{P}_0(F)} a_P P$ and $D_\infty := \sum_{P\in\mathbb{P}_\infty(F)} a_P P$. The ideal representation of D is given by (I, I_∞) with

$$I = \prod_{P\in\mathbb{P}_0(F)} \mathfrak{p}^{-a_P}, \quad I_\infty = \prod_{P\in\mathbb{P}_\infty(F)} \mathfrak{p}^{-a_P},$$

where the prime ideals $\mathfrak{p}$ of F corresponds to the places P of F. We consider $D_0^* := \sum_{P\in\mathbb{P}_0(F)} |a_P|P$ and $D_\infty^* := \sum_{P\in\mathbb{P}_\infty(F)} |a_P|P$ and set $I^* := \prod_{P\in\mathbb{P}_0(F)} \mathfrak{p}^{-|a_P|}$ and $I_\infty^* := \prod_{P\in\mathbb{P}_\infty(F)} \mathfrak{p}^{-|a_P|}$ as in (1.1). Lemma 1.2.6 shows that

$$[\mathcal{O}_F : I^*] = N_{F/K}(I^*) = \prod_{P\in\mathbb{P}_0(F)} N_{F/K}(\mathfrak{p})^{-|a_P|}.$$

Since $\deg P = |N_{F/K}(\mathfrak{p})|$ [14], we obtain, $|[\mathcal{O}_F : I^*]| = \sum_{P\in\mathbb{P}_0(F)} -|a_P| \deg P = -\deg D_0^*$. As $|[\mathcal{O}_F : I^*]| = -|[I^* : \mathcal{O}_F]|$, we get

$$\deg D_0^* = |[I^* : \mathcal{O}_F]| = |[I^* : A[\theta]]| - |[\mathcal{O}_F : A[\theta]]|. \tag{4.2}$$

Analogously, one can show $\deg D_\infty^* = -|[I_\infty^* : A_\infty[\theta_\infty]]| + |[\mathcal{O}_{F,\infty} : A_\infty[\theta_\infty]]|$. Then, by the definition of the height of an ideal (cf. Definition 1.2.7) and of a divisor, we obtain $\deg D_0^* = h(D_0) = h(I) - |[\mathcal{O}_F : A[\theta]]|$ and $\deg D_\infty^* = h(D_\infty) = h(I_\infty) + |[\mathcal{O}_{F,\infty} : A_\infty[\theta_\infty]]|$. Since the supports of D_0 and D_∞ are disjoint, we obtain

$$h(D) = h(D_0) + h(D_\infty) = h(I) - |[\mathcal{O}_F : A[\theta]]| + h(I_\infty) + |[\mathcal{O}_{F,\infty} : A_\infty[\theta_\infty]]|$$

and therefore $h(I) + h(I_\infty) \leq h(D) + \delta + \delta_\infty$. Clearly, $H(I) \leq h(I) + \delta$ and $H(I_\infty) \leq h(I_\infty) + \delta_\infty$ (cf. Definition 1.2.7). Thus, we deduce $H(I) + H(I_\infty) \leq h(I) + \delta + h(I_\infty) + \delta_\infty \leq h(D) + 2(\delta + \delta_\infty) = O(h(D) + n^2 C_f)$ by Lemma 4.1.3.

For a matrix $N \in K^{n\times n}$ denote by $g_N \in A$ a nonzero polynomial of minimal degree such that $g_N N \in A^{n\times n}$. Then, by the definition of $\widetilde{T}$ we have $h(\widetilde{T}) \leq h(g_T T)$. Let us estimate the height of $g_T T$.

We consider the matrices $M, M' \in K^{n\times n}$ with $M(1\ \theta \dots \theta^{n-1})^{\mathrm{tr}} = (b_1 \dots b_n)^{\mathrm{tr}}$ and $M'(1\ \theta \dots \theta^{n-1})^{\mathrm{tr}} = (b'_1 \dots b'_n)^{\mathrm{tr}}$, where $\mathcal{B} = (b_1, \dots, b_n)$ and $\mathcal{B}' = (b'_1, \dots, b'_n)$. Then, $T = MM'^{-1}$ is the transition matrix from $\mathcal{B}$ to $\mathcal{B}'$. Clearly, $|g_T| \leq |g_M| + |g_{M'^{-1}}|$, since $g_M g_{M'^{-1}} T \in A^{n\times n}$ and $|g_T|$ is minimal. Then, Lemma 2.7.15 shows that

$$h(\widetilde{T}) \leq h(g_T T) = |g_T| + h(T) \leq |g_M| + h(M) + |g_{M'^{-1}}| + h(M'^{-1}). \tag{4.3}$$

As $\mathcal{B}$ is an Hermite basis, Corollary 1.2.13 shows that $|g_M| + h(M) = O(H(I))$. We estimate $|g_{M'^{-1}}| + h(M'^{-1})$ and consider

$$M'\mathrm{diag}(1, t^{C_f}, \dots, t^{(n-1)C_f})(1\ \theta_\infty \dots \theta_\infty^{n-1})^{\mathrm{tr}} = (b'_1 \dots b'_n)^{\mathrm{tr}}.$$

We set $Q := M'\mathrm{diag}(1, t^{C_f}, \ldots, t^{(n-1)C_f})$. As $M'^{-1} = \mathrm{diag}(1, t^{C_f}, \ldots, t^{(n-1)C_f})Q^{-1}$, we obtain

$$|g_{M'^{-1}}| + h(M'^{-1}) \leq |g_{M'^{-1}}| + (n-1)C_f + h(Q^{-1}). \tag{4.4}$$

As $g_{Q^{-1}}M'^{-1} \in A^{n\times n}$, we deduce $|g_{M'^{-1}}| \leq |g_{Q^{-1}}|$. Arguing as we did in the proof of item *3* of Lemma 2.7.15, we see that $(g_Q^n \det Q)Q^{-1} \in A^{n\times n}$ with $g_Q^n \det Q \in A$; hence $|g_{Q^{-1}}| \leq |g_Q^n \det Q| \leq n(g_Q + h(Q))$. Moreover, we have $h(Q^{-1}) \leq nh(Q)$. As Q is the transition matrix from $\mathcal{B}'$ to $(1, \theta_\infty, \ldots, \theta_\infty^{n-1})$, it holds $|g_Q| + h(Q) = O(H(I_\infty))$ by Corollary 1.2.13 and therefore $|g_{M'^{-1}}| + h(M'^{-1}) = O(nH(I_\infty) + nC_f)$ by (4.4). Finally, (4.3) and item *1* show that

$$h(\widetilde{T}) = O(H(I) + nC_f + nH(I_\infty)) = O(nh(D) + n^3 C_f).$$

□

Corollary 4.1.5. *Let D be a divisor with $\mathcal{L}(D) = I \cap I_\infty$ and $\mathcal{B}$ and $\mathcal{B}'$ Hermite bases of the fractional ideals I and I_∞, respectively. Then, Algorithm 6 needs at most*

$$O(n^5(h(D) + n^2 C_f)^2)$$

arithmetic operations in k to compute a k-basis of $\mathcal{L}(D)$.

Proof. We apply Lemma 4.1.4 to Lemma 4.1.1 and deduce that the complexity of Algorithm 6 is given by

$$C(T) + O(n^4 h(\widetilde{T}) + n^3 h(\widetilde{T})^2) = C(T) + O(n^5(h(D) + n^2 C_f)^2).$$

In order to estimate $C(T)$ we consider the proof of Lemma 4.1.4. There we have seen that $T = MM'^{-1}$. Clearly, the cost $C(T)$ for computing T is dominated by the cost of the inversion of M' and the realization of the matrix product MM'^{-1}.

Since $M' = Q\mathrm{diag}(1, t^{-C_f}, \ldots, t^{-(n-1)C_f})$, the cost for determining M'^{-1} is dominated by the inversion of Q. As $\mathcal{B}'$ is a Hermite basis of $\mathfrak{I}_\infty$, there exist $\beta \in \mathbb{Z}$ such that $t^\beta Q$ is in HNF. We can assume that $\beta = 0$. Hence, we have to invert a lower triangular matrix, whose entries $q_{i,j}$ satisfy $|q_{i,j}| = O(h(I_\infty))$ by Corollary 1.2.13. By Gaussian elimination this can be realized with at most $O(n^3 h(I_\infty))$ operations in k.

Since $h(g_M M) = O(h(I))$ and $h(g_{M'^{-1}}M'^{-1}) = O(nC_f + nh(I_\infty))$, the cost for computing MM'^{-1} is bounded by $O(n^3(nC_f + nh(I_\infty) + h(I))^2)$ operations in k. Hence, $C(T)$ is dominated by $O(n^5(h(D) + n^2 C_f)^2)$. □

For divisors D with large height, under certain conditions it is utile to apply a divisor reduction as explained in [16]. That is, one determines an effective divisor D' of F of "small" height, $a \in F^*$ and $r \in \mathbb{Z}$ such that

$$D = D' + r(t)_\infty - (a). \tag{4.5}$$

Then, $\mathcal{L}(D) = a \cdot \mathcal{L}(D' + r(t)_\infty)$. Let (I', I'_∞) be the ideal representation of D'. Then, according to Corollary 4.0.2 it is sufficient to determine a semi-reduced basis of $(I', \| \|)$ in order to compute a basis of $\mathcal{L}(D' + r(t)_\infty)$. Hence, the computation of $\mathcal{L}(D)$ can be restricted to the computation of $\mathcal{L}(D')$. For a divisor D, whose support only contains places of small degree, the height $h(D)$ enters the running time of the computation of $\mathcal{L}(D)$ logarithmically. For many applications, for instance the computation of the class group of a global function field, the divisor reduction leads to a remarkable speedup. However, for divisors carrying places of large degree, the divisor reduction is useless. Moreover, for many applications in function fields initially a basis of the zero divisor has to be computed. In that context no divisor reduction can be applied.

4.2 Genus computation

Let F/k be a function field of genus g over the field k, and denote by k_0 its full constant field. In this section we present an algorithm that computes the genus of a function field. Our algorithm is based on the repeated application of the Montes algorithm (i.e. Algorithm 1). Hence, it has an excellent practical performance for global function fields, that is, a function field with finite constant field k.

Corollary 4.2.1 ([16, Corollary 5.5])**.** *Let D be a divisor of F and (I, I_∞) its ideal representation. Then, it holds*

$$-|d(I)| = \deg D + [k_0 : k](1 - g) - n.$$

Proof. Let $(b_1, \ldots, b_n)$ be a reduced basis of I with respect to the norm $\| \| = \| \|_D$. For a sufficiently large $r \in \mathbb{Z}$, Corollary 4.0.2 shows that $\dim_k(D + r(t)_\infty) = (\sum_{i=1}^n -\lceil \|b_i\| \rceil) + nr + n$. Also, for large r we obtain by the Riemann-Roch theorem

$$\begin{aligned} \dim_k(D + r(t)_\infty) &= \deg(D + r(t)_\infty) + [k_0 : k](1 - g) \\ &= \deg D + rn + [k_0 : k](1 - g). \end{aligned} \tag{4.6}$$

So, finally we have $\deg D + [k_0 : k](1 - g) - n = -\sum_{i=1}^n \lceil \|b_i\| \rceil = -|d(I)|$, where the last equality follows from Lemma 2.5.8. □

Theorem 4.2.2. *Let F/k be a function field with defining polynomial f and let $\theta \in F$ be a root of f. Let D be a divisor and (I, I_∞) be its ideal representation. Then,*

$$|d(I)| = -|[I : A[\theta]]| + |[I_\infty : A_\infty[\theta_\infty]]| + C_f n(n-1)/2.$$

Proof. Let $\mathcal{B} = (b_1, \ldots, b_n)$ be any basis of I and $\mathcal{B}' = (b'_1, \ldots, b'_n)$ an orthonormal basis of I_∞. We consider $M, M' \in K^{n\times n}$ with $M(1\ \theta \ldots \theta^{n-1})^{\mathrm{tr}} = (b_1 \ldots b_n)^{\mathrm{tr}}$ and $M'(1\ \theta \ldots \theta^{n-1})^{\mathrm{tr}} = (b'_1 \ldots b'_n)^{\mathrm{tr}}$. Then, $T := MM'^{-1}$ is the transition matrix from $\mathcal{B}$ to $\mathcal{B}'$ and by definition,

$$|d(I)| = |\det(T)| = |\det(M)| + |\det(M'^{-1})| = -|[I : A[\theta]]| + |\det(M'^{-1})|. \tag{4.7}$$

Let $N := \mathrm{diag}(1, t^{-C_f}, \ldots t^{-C_f(n-1)})$. Clearly,

$$(1\ \theta_\infty \ldots \theta_\infty^{n-1})^{\mathrm{tr}} = N(1\ \theta \ldots \theta^{n-1})^{\mathrm{tr}} = NM'^{-1}(b'_1 \ldots b'_n)^{\mathrm{tr}}.$$

Hence, $|[I_\infty : A_\infty[\theta_\infty]]| = |\det(NM'^{-1})| = -C_f n(n-1)/2 + |\det(M'^{-1})|$, and therefore

$$|\det(M'^{-1})| = |[I_\infty : A_\infty[\theta_\infty]| + C_f n(n-1)/2.$$

Together with (4.7), we obtain the claimed formula for $|d(I)|$. □

We apply Corollary 4.2.1 to the zero divisor $D := (0)$. Then, I becomes $\mathcal{O}_F$ and $I_\infty = \mathcal{O}_{F,\infty}$. Therefore,

$$g = \frac{[k_0 : k] - n + |d(\mathcal{O}_F)|}{[k_0 : k]}. \tag{4.8}$$

Clearly, D induces the lattice $(\mathcal{O}_F, \| \ \|_0)$ with

$$\|z\|_0 := -\min_{P\in\mathbb{P}_\infty} \left\{ \frac{v_P(z)}{e(P/P_\infty)} \right\}, \quad \text{for all } z \in F. \tag{4.9}$$

Note that k_0 coincides with $\mathcal{L}(0) = (\mathcal{O}_F, \| \ \|_0)_{\leq 0}$. Moreover, $[k_0 : k] = \dim(\mathcal{O}_F, \| \ \|_0)_{\leq 0}$. Thus, in that context the genus formula (4.8) coincides with the one from Definition 3.1.10.

Corollary 4.2.3. *For a function field F/k with defining equation $f(t, \theta) = 0$, the genus may be computed as:*

$$g = \frac{[k_0 : k] - n - |[\mathcal{O}_F : A[\theta]]| + |[\mathcal{O}_{F,\infty} : A_\infty[\theta_\infty]]| + C_f n(n-1)/2}{[k_0 : k]}.$$

Moreover, let $g_k := -n - |[\mathcal{O}_F : A[\theta]]| + |[\mathcal{O}_{F,\infty} : A_\infty[\theta_\infty]]| + C_f n(n-1)/2 < 0$. Then, $g = 0$ if $g_k < 0$ and $g = 1$ if $g_k = 0$.

Proof. The first statement follows immediately from (4.8) and Theorem 4.2.2. For the second one we consider

$$0 \leq g = \frac{[k_0 : k] + g_k}{[k_0 : k]} = 1 + \frac{g_k}{[k_0 : k]} \leq 1.$$

Since $g \in \mathbb{Z}$, we obtain $g = 0$ if $g_k < 0$ and $g = 1$ if $g_k = 0$. □

A conventional way to compute the genus g of a function field F/k proceeds as follows: Consider the divisor $D := (r(t)_\infty)$ and the Riemann-Roch space $\mathcal{L}(D) = \mathcal{O}_F \cap t^r \mathcal{O}_{F,\infty}$. Determine the $\lceil \| \ \|_0 \rceil$-values of a $\| \ \|_0$-semi-reduced basis $(b_1, \ldots, b_n)$ of $\mathcal{O}_F$. For large r, Corollary 4.0.2 and (4.6) show that

$$\sum_{\lceil \|b_i\|_0 \rceil \leq r} (-\lceil \|b_i\|_0 \rceil + r + 1) = \dim_k D = rn + [k : k_0](1 - g). \tag{4.10}$$

Since $[k : k_0] = \dim_k \mathcal{L}(0) = \sum_{\lceil \|b_i\|_0 \rceil \leq 0} (-\lceil \|b_i\|_0 \rceil + 1)$, the genus g can be deduced easily from (4.10).

If $k_0 = k$, that is, the constant field k is algebraically closed in the function field F (for instance, when F is the function field of a geometrically irreducible curve over k), then Corollary 4.2.3 shows that the computation of the genus g of F can be reduced to the computation of the degree of the two indices $[\mathcal{O}_F : A[\theta]]$ and $[\mathcal{O}_{F,\infty} : A_\infty[\theta_\infty]]$. For a monic and irreducible polynomial $p(t) \in A$, the valuations

$$\mathrm{ind}_p := v_p([\mathcal{O}_F : A[\theta]]), \quad \mathrm{ind}_\infty := v_\infty([\mathcal{O}_{F,\infty} : A_\infty[\theta_\infty]])$$

of these two indices are computed by Algorithm 1, the Montes algorithm. Since $-v_\infty([\mathcal{O}_{F,\infty} : A_\infty[\theta_\infty]]) = |[\mathcal{O}_{F,\infty} : A_\infty[\theta_\infty]]|$ by definition and

$$|[\mathcal{O}_F : A[\theta]]| = \sum_{p(t)^2 | \operatorname{disc} f} v_p([\mathcal{O}_F : A[\theta]]) \cdot |p(t)|,$$

the computation of the genus can be restricted to the computation of the "local values" ind_p and ind_∞.

If k_0 is unknown we have to deduce $[k_0 : k]$ additionally as follows: Assume we have already computed the degree of the indices $[\mathcal{O}_F : A[\theta]]$ and $[\mathcal{O}_{F,\infty} : A_\infty[\theta_\infty]]$. Then, the degree of the places $P \in \mathbb{P}_\infty(F)$ and $P \in \mathbb{P}_0(F)$ with $P | P_p$, for $p(t)^2 | \operatorname{disc} f$, has been determined by the Montes algorithm as a by-product. Let $k = \mathbb{F}_q$ be the finite field with q elements. By [14, p. 367] the integer $l := [k_0 : k]$ is equal to the number of absolutely

irreducible factors of the defining polynomial f. That is, l coincides with the number of irreducible factors of f, considered as a polynomial in $\mathbb{F}_{q^{l'}}[t,x]$, where $l' := el$ and $e \in \mathbb{N}$ arbitrary. Since l is unknown, we have to factorize f over a certain extension $\mathbb{F}_{q^{l'}}$ of $\mathbb{F}_q$. Clearly, l divides n and the degree of any place of F. Hence, we can choose l' to be the gcd of n and the degrees of all places involved in the computation of $|[\mathcal{O}_F : A[\theta]]|$ and $|[\mathcal{O}_{F,\infty} : A_\infty[\theta_\infty]]|$. This leads us to an upper bound for l and determines a finite field $\mathbb{F}_{q^{l'}}$ over which f splits into absolutely irreducible factors. By factorizing $f \in \mathbb{F}_{q^{l'}}[t,x]$ we obtain l.

These ideas lead to the following algorithm.

Algorithm 7: Genus computation of global function fields

Input: A global function field $F/\mathbb{F}_q$ with defining polynomial f of degree n.
Output: Genus g of F.

1: $f_\infty \leftarrow t^{-C_f n} f(t, t^{C_f} x)$, FiniteIndex $\leftarrow 0$, $l' \leftarrow n$
2: Factorize d where $d = \gcd(\operatorname{disc} f, (\operatorname{disc} f)')$
3: **for** all irreducible factors $p(t)$ of d **do**
4: $\quad \operatorname{ind}_p \leftarrow$ Algorithm 1$(f, p(t))$
5: $\quad$ FiniteIndex $\leftarrow$ FiniteIndex $+|p(t)| \cdot \operatorname{ind}_p$
6: $\quad l' \leftarrow \gcd(\{\deg P \mid P | P_p\} \cup \{l'\})$
7: **end for**
8: $\operatorname{ind}_\infty \leftarrow$ Algorithm 1$(f_\infty, 1/t)$
9: $g_k \leftarrow -n -$FiniteIndex$- \operatorname{ind}_\infty + C_f n(n-1)/2$
10: **if** $g_k \leq 0$ **then**
11: $\quad$ **return** 0 if $g_k < 0$ or 1 if $g_k = 0$
12: **end if**
13: $l' \leftarrow \gcd(\{\deg P \mid P | P_\infty\} \cup \{l', g_k\})$
14: **if** $l' > 1$ **then**
15: $\quad$ Factorize f as a polynomial in $\mathbb{F}_{q^{l'}}[t,x]$
16: $\quad l' \leftarrow$ number of irreducible factors of f
17: **end if**
18: **return** $1 + g_k/l'$

Let us now fix an algorithm to factorize bivariate polynomials over finite fields. For a polynomial f in $\mathbb{F}_q[t,x]$ of degree n in x, let $C(f)$ be the expected number of operations in $\mathbb{F}_q$ of the algorithm applied to f over $\mathbb{F}_{q^n}$.

We admit fast multiplication techniques of Schönhage-Strassen [34].

Theorem 4.2.4. *The genus of a function field $F/\mathbb{F}_q$ with defining polynomial f of degree n in x can be computed in an expected number of*

$$C(f) + O(n^{5+\epsilon}{C_f}^{2+\epsilon}\log(q))$$

arithmetic operations in $\mathbb{F}_q$.

Remark 4.2.5. *In [3, 4] it is shown that f can be factorized over $\mathbb{F}_{q^n}$ in expected polynomial-time. In practice, the factorization of f over certain extensions of $\mathbb{F}_q$ (cf. line 15 in Algorithm 7) has an excellent performance (cf. Chapter 6).*

If k_0 is known or Algorithm 7 detects $g_k \leq 0$ or $l' = 1$ (in line 10 or 14), no bivariate polynomial must be factorized. In that context the expected number of operation in $\mathbb{F}_q$ is bounded by $O(n^{5+\epsilon}{C_f}^{2+\epsilon}\log(q))$.

Proof. Initially, Algorithm 7 computes $\operatorname{disc} f$ and factorizes its inseparable part. Since $\operatorname{disc} f = \operatorname{Res}(f, f')$, the cost of the computation of $\operatorname{disc} f$ is equal to the cost of computing the determinant of the Sylvester matrix M of f and f'. In [24] it is shown that the cost is $O(m^2n^3)$ field operations, where m denotes the maximal degree of the entries in M. Since $m = O(nC_f)$, the computation of $\operatorname{disc} f$ needs at most $O(n^5{C_f}^2)$ operations in k.

In the worst case we have to factorize $d = \operatorname{disc} f$. According to [35, Corollary 14.30] the factorization of $\operatorname{disc} f$ can be estimated by an expected number of $O((n^2C_f)^{2+\epsilon} + (n^2C_f)^{1+\epsilon}\log(q)) = O(n^{4+\epsilon}{C_f}^{2+\epsilon} + n^{2+\epsilon}{C_f}^{1+\epsilon}\log(q))$ operations in $\mathbb{F}_q$, since $\deg \operatorname{disc} f = |\operatorname{disc} f| = O(n^2C_f)$ (cf. Lemma 4.1.3).

Let $\delta_p := v_p(\operatorname{disc} f)$. Considering [1, theorem 5.14] the cost of one call of Algorithm 1 for the input $(f, p(t))$ and $(f_\infty, 1/t)$ is equal to

$$O((\deg p(t))^{1+\epsilon}(n^{2+\epsilon} + n^{1+\epsilon}\delta_p\log(q^{\deg p(t)}) + n^{1+\epsilon}\delta_p^{2+\epsilon}))$$

and $O\left(n^{2+\epsilon} + n^{1+\epsilon}\delta_\infty\log(q) + n^{1+\epsilon}\delta_\infty^{2+\epsilon}\right)$ operations in k, respectively. The worst case is that we have to call the Montes algorithm for all irreducible divisors $p(t)$ of $\operatorname{disc} f$. Therefore, the cost of the for-loop is

$$\begin{aligned}\sum_{p(t)|\operatorname{disc} f} & O((\deg p(t))^{1+\epsilon}(n^{2+\epsilon} + n^{1+\epsilon}\delta_p\log(q^{\deg p(t)})) + n^{1+\epsilon}\delta_p^{2+\epsilon}) \\ &= O(n^{2+\epsilon}\delta^{1+\epsilon} + n^{1+\epsilon}\delta^{2+\epsilon}\log(q) + n^{1+\epsilon}\delta^{2+\epsilon})\end{aligned}$$

operations in k. Adding the cost for applying Algorithm 1 for $(f_\infty, 1/t)$, we obtain for the computation of the degree of the two indices

$$\begin{aligned} & O(n^{2+\epsilon}\delta^{1+\epsilon} + n^{1+\epsilon}(\delta^{2+\epsilon} + \delta_\infty)\log(q) + n^{1+\epsilon}(\delta^{2+\epsilon} + \delta_\infty^{2+\epsilon})) \\ = & O(n^{4+\epsilon}{C_f}^{1+\epsilon} + n^{5+\epsilon}{C_f}^{2+\epsilon}\log(q) + n^{5+\epsilon}{C_f}^{2+\epsilon}) \\ = & O(n^{5+\epsilon}{C_f}^{2+\epsilon}\log(q)), \end{aligned}$$

field operations, where the first equality follows from Lemma 4.1.3. Clearly, the cost of the computation and factorization of disc f is dominated by $O(n^{5+\epsilon}{C_f}^{2+\epsilon}\log(q))$. □

Remark 4.2.6. *In [2, Lemma 1.29] is shown that for $g \geq 1$ the defining polynomial f of a global function field F/k can be chosen such that $C_f = O(g^2)$ holds. In that case algorithm 7 determines the genus of F in an expected number of $C(f) + O(n^{5+\epsilon}g^{4+\epsilon}\log(q))$ operations in $\mathbb{F}_q$.*

4.3 Isometry classes in function fields

As mentioned before any divisor D of a function field F/k induces the lattice $(I, \| \ \|_D)$ in the normed space $(F, \| \ \|_D)$, where F is being considered as an n-dimensional K-vector space and (I, I_∞) is the ideal representation of D. In particular, any lattice $(I, \| \ \|_D)$ belongs to $\mathrm{LS}(F)$, the space of lattices of F (cf. Definition 2.8.1).

The trace map $\mathrm{Tr}_{F/K} : F \to K$ with respect to F/K determines the non-degenerated symmetric bilinear form

$$\mathrm{B} : F \times F \to K, \quad \mathrm{B}(z, z') := \mathrm{Tr}_{F/K}(zz'),$$

the so-called *trace form* on F.

Lemma 4.3.1. $\mathcal{O}_F \subset \{z \in F \mid \mathrm{B}(z, z) \in A\}$ *and* $\mathcal{O}_{F,\infty} \subseteq \{z \in F \mid \mathrm{B}(z, z) \in A_\infty\}$.

Proof. We show the first inclusion, the second one can be treated analogously. For $\alpha \in \mathcal{O}_F$, let $g(x) = x^r + a_{r-1}x^{r-1} + \cdots + a_0$ the minimal polynomial of α^2. Since α is integral over A, α^2 is integral over A too. Therefore, the polynomial g belongs to $A[x]$. By [33, p. 333] it holds $\mathrm{Tr}_{F/K}(\alpha^2) = -[F : K(\alpha^2)]a_{r-1} \in A$; hence, $\mathcal{O}_F \subset \{z \in F \mid \mathrm{B}(z, z) \in A\}$. □

We define the zero norm $\| \ \|_0$ by (4.9) and the zero lattice of F by $(\mathcal{O}_F, \| \ \|_0)$. Therefore, the results of Chapter 3 become available in the context of an algebraic function field.

Lemma 4.3.2. *Let $\mathcal{B}$ be an A_∞-basis of $\mathcal{O}_{F,\infty}$, then $\| \ \|_{\mathcal{B}} \sim \| \ \|_0$.*

Proof. Lemma-Definition 2.8.9 and Corollary 4.0.2 show that $\mathcal{B}$ is a semi-orthonormal basis of $(F, \| \ \|_0)$. Then, by Lemma 3.1.2 it holds $\| \ \|_{\mathcal{B}} \sim \| \ \|_0$. □

Note that in the general setting from Chapter 3 the zero norm is integer valued, whereas $\| \ \|_0$ with $\|z\|_0 = -\min_{P \in \mathbb{P}_\infty}\{v_P(z)/e(P/P_\infty)\}$ has values in $\mathbb{Q}$. Since the results from Chapter 3 only depend on the class of the zero norm in $\mathrm{LS}(E)/\sim$ (resp. $\mathrm{LS}(E,R)/\sim$), we can choose any representative of this class. According to Definition 3.1.4 the last lemma shows that $\| \ \|_0$ as defined above is such an representative. The reader may choose $\lceil \| \ \|_0 \rceil$ instead of $\| \ \|_0$. However, for convenience we take $\| \ \|_0$ as defined in (4.9).

We summarize some of the results of Chapter 3 in the context of an algebraic function field.

Lemma 4.3.3. *Let F/k be function field of genus g and let $D \in \mathcal{D}_F$ with the ideal representation (I, I_∞). Denote by $(I, \| \ \|)$ the lattice induced by D.*

1. $\deg D = \deg(I, \| \ \|)$.
2. $\dim D = \dim(I, \| \ \|)_{\leq 0}$.
3. $g = g_F$.

Proof. We write $D = D_0 + D_\infty$ with $D_0 := \sum_{P \in \mathbb{P}_0(F)} a_P P$ and $D_\infty := \sum_{P \in \mathbb{P}_\infty(F)} a_P P$. According to (4.2) it holds $\deg D_0 = |[I : \mathcal{O}_F]|$. Analogously, one can show that $\deg D_\infty = -|[I_\infty : \mathcal{O}_{F,\infty}]|$. Hence, $\deg D = |[I : \mathcal{O}_F]| - |[I_\infty : \mathcal{O}_{F,\infty}]|$. By definition, we have $\deg(I, \| \ \|) = |d(\mathcal{O}_F, \| \ \|_0)| - |d(I, \| \ \|)|$. We apply Theorem 4.2.2 and deduce that $\deg(I, \| \ \|)$ is equal to

$$-|[\mathcal{O}_F : A[\theta]]| + |[\mathcal{O}_{F,\infty} : A_\infty[\theta_\infty]]| + C_f n(n-1)/2$$
$$-(-|[I : A[\theta]]| + |[I_\infty : A_\infty[\theta_\infty]]| + C_f n(n-1)/2) = |[I : \mathcal{O}_F]| - |[I_\infty : \mathcal{O}_{F,\infty}]|$$

The second statement follows immediately from Theorem 4.0.1.

Since $k_0 = \mathcal{O}_F \cap \mathcal{O}_{F,\infty} = (\mathcal{O}_F, \| \ \|_0)_{\leq 0}$ and $\dim \mathcal{O}_F = \dim_k k_0 = [k_0 : k]$, the last item is a consequence of Definition 3.1.10 and (4.8). □

The concept of Duality from Section 3.2 can be easily translated to this particular situation. We define the dual divisor $D^\#$ and the complementary divisor D^* exactly

as in Subsection 3.2 by taking $E := F, \mathcal{O}_F, \mathcal{O}_{F,\infty}$, and the trace form B. Then, we can define the lattices space $\mathrm{LS}(F)$ and the R-lattice space $\mathrm{LS}(F,R)$ of the function field F, where $R := \overline{\mathrm{sm}}(\mathcal{O}_F, \| \|_0)$. Hence, the divisor group of F becomes a subset of $\mathrm{LS}(F)$ and $\mathrm{LS}(F,R)$.

We define the *successive minima* $\mathrm{sm}(D)$ of D to be the successive minima of the by D induced lattice. We call two divisors D_1 and D_2 isometric if their induced lattices are isometric; that is, if $\mathrm{sm}(D_1) = \mathrm{sm}(D_2)$. Clearly, this determines an equivalence relation of the set of divisors of F/k.

Lemma 4.3.4. *Let D be a divisor of F/k and $a \in F^*$. Then, D and $D + (a)$ are isometric.*

Proof. Let (I, I_∞) the ideal representation of D. Then, $D + (a)$ is represented by $(a^{-1}I, a^{-1}I_\infty)$. In particular, D and $D+(a)$ induce the lattices $(I, \| \|)$ and $(a^{-1}I, \| \|')$, respectively, where

$$\| \| = -\min_{P\in\mathbb{P}_\infty}\left\{\frac{v_P(\ ) + v_P(D)}{e(P/P_\infty)}\right\}, \quad \| \|' = -\min_{P\in\mathbb{P}_\infty}\left\{\frac{v_P(\ ) + v_P(D) + v_P(a)}{e(P/P_\infty)}\right\}.$$

Then, the isometry is determined by the K-linear map $\mu_{a^{-1}}(z) = a^{-1}\cdot z$, for $z \in F$. □

The converse of Lemma 4.3.4 is false in general as the following example shows.

Example 4.3.5. Let $F/\mathbb{F}_3$ be the function field defined by the polynomial $f(t,x) = x^3 + t^2x + t \in \mathbb{F}_3[t,x]$. The places at infinity of F are P_1 and P_2, where $\deg P_1 = 1$ and $\deg P_2 = 2$. There exits only one place Q over P_t, the place of the rational function field $\mathbb{F}_3(t)$ induced by the irreducible polynomial $t \in A$. The degree of Q is equal 1. We consider the divisors

$$D = 2Q - 2P_2, \qquad D' = Q + P_1 - 2P_2,$$

both having degree -2 and successive minima $(1,2,2)$; hence $D \simeq D'$. On the other hand, $\dim(D - D') = 0$ ($\mathrm{sm}(D - D') = (1,1,1)$). Thus, D and D' are isometric but there exits no element $a \in F^*$ such that $D = D' + (a)$.

We define the normalized successive minima $\mathrm{sm}_0(D)$ and the diameter $\mathrm{diam}(D)$ of a divisor D by considering its induced lattice. Note that there exists an integer r such that $\mathrm{sm}_0(D) = \mathrm{sm}(D + r(t)_\infty)$. In particular, the divisor $D + r(t)_\infty$ induces the lattice $(I, \| \| - r)$, where $(I, \| \|)$ corresponds to D.

Theorem 4.3.6. *For any divisor D of F/k, it holds that* $\mathrm{sm}_0(D) \leq \mathrm{sm}(0)$.

Proof. We identify D with the lattice $(I, \| \|)$ and the zero divisor with $(\mathcal{O}_F, \| \|_0)$. We can assume that $\mathrm{sm}_0(D) = \mathrm{sm}(D)$, otherwise we shift D in the right class by considering $D + r(t)_\infty$, for an adequate $r \in \mathbb{Z}$. Denote by $d_1 \leq \cdots \leq d_n$ and $s_1 \leq \cdots \leq s_n$ the successive minima of D and 0, respectively. In particular, we have $\lceil d_1 \rceil = 0$. We consider a distinction of cases:

The case $\sum_{i=1}^n \lceil d_i \rceil > \sum_{i=1}^n \lceil s_i \rceil$ implies $\deg(I, \| \|) = \deg D < 0$ by Lemma 4.3.3 and Corollary 3.1.9, and therefore $\dim D = 0$. Since $\lceil d_1 \rceil = 0$, it holds $\dim D > 0$ by Corollary 3.1.9, a contradiction.

Let $\sum_{i=1}^n \lceil d_i \rceil \leq \sum_{i=1}^n \lceil s_i \rceil$. By construction we have $\dim D = \sum_{\lceil d_i \rceil \leq 0} (-\lceil d_i \rceil + 1) > 0$. Choose $a \in \mathcal{L}(D) \setminus k_0$ and consider $D' = D + (a) \geq 0$. By the last lemma, D' and D have the same successive minima. Denote by $(I', \| \|')$ the lattice which is induced by D' and let $I'_\infty := (F, \| \|')_{\leq 0}$. Then, (I', I'_∞) is the ideal representation of D', where $\mathcal{O}_F \subseteq I'$ and $(F, \| \|_0)_{\leq 0} = \mathcal{O}_{F,\infty} \subseteq I'_\infty$, since D' is effective. Thus, item *6* of Lemma 3.3.8 shows that $\mathrm{sm}(D) = \mathrm{sm}(D') \leq \mathrm{sm}(0)$. □

The last theorem allows us to interpret the divisor group $\mathcal{D}_F$ of F as a subset of $\mathrm{LS}(F, R)_S$, where $R = \overline{\mathrm{sm}}(\mathcal{O}_F, \| \|_0)$ and $S := \mathrm{sm}(0)$.

We summarize the results of Subsection 3.3 in the context of an algebraic function field.

Lemma 4.3.7.

1. *The isometry class of the zero divisor in $\mathcal{D}_F$ is given by the set of all principal divisors of F/k.*

2. *For all $D \in \mathcal{D}_F$ it holds* $\mathrm{diam}(D) < \mathrm{diam}(0) + 1 \leq g \cdot [k_0 : k] + 2$.

3. *For all $D \in \mathcal{D}_F$ with* $\deg D \geq |d(\mathcal{O}_F)| - 2n + (n-1)\mathrm{diam}(0) + 1$ *it holds*

$$\dim D = \deg D + [k_0 : k](1 - g).$$

Proof. Item *1* follows immediately from Lemma 3.3.14 item *3* and the fact that the principal divisors of F are characterized by divisor of F having positive dimension and degree equal to zero.

The second item yields by Lemma 3.3.14, Lemma 3.3.12, and the fact that $\dim 0 = \dim(\mathcal{O}_F, \| \|_0) = [k_0 : k]$. The third one is Theorem 3.3.15. □

Corollary 4.3.8. *For a function field of defining equation $f(t,\theta)=0$ with $\deg f = 2$, the genus satisfies*

$$g = \begin{cases} 0, & \text{if } |d(\mathcal{O}_F, \| \ \|_0)| = 0, \\ -1 - |d(\mathcal{O}_F, \| \ \|_0)|, & \text{if } |d(\mathcal{O}_F, \| \ \|_0)| > 0, \end{cases}$$

where $|d(\mathcal{O}_F, \| \ \|_0)| = -|[\mathcal{O}_F : A[\theta]]| + |[\mathcal{O}_{F,\infty} : A_\infty[\theta_\infty]]| + C_f$ by Theorem 4.2.2.

Proof. Let $s_1 \leq s_2$ be the successive minima of $(\mathcal{O}_F, \| \ \|_0)$. By Lemma 3.3.10 we know that $0 \leq \lceil s_i \rceil$, for $i = 1, 2$. Then, by Corollary 3.1.9 the fact $|d(\mathcal{O}_F, \| \ \|_0)| = 0$ implies $\dim(\mathcal{O}_F, \| \ \|_0) = [k_0 : k] = 2$. Thus, Lemma 3.3.16 shows that $g = 0$.

If $|d(\mathcal{O}_F, \| \ \|_0)| > 0$ the dimension of $\mathcal{O}_F$ is one and in particular $[k_0 : k] = 1$. Hence, $k_0 = k$ and the formula is deduced from (4.8). □

By the last corollary, for the computation of the genus of a function field of degree 2, one only needs to determine $|[\mathcal{O}_F : A[\theta]]|$ and $|[\mathcal{O}_{F,\infty} : A_\infty[\theta_\infty]]|$.

Corollary 4.3.9. *Let $D \in \mathcal{D}_F$ and denote by $d_1 \leq \cdots \leq d_n$ its successive minima. Then, $\lceil d_n \rceil - \lceil d_1 \rceil \leq g \cdot [k_0 : k] + 1$.*

Proof. Clearly, with $\mathrm{sm}_0(D) = (d_1', \ldots, d_n')$ it holds $(d_1', \ldots, d_n') = (d_1 + r, \ldots, d_n + r)$, for an adequate $r \in \mathbb{Z}$; hence, $\lceil d_n \rceil - \lceil d_1 \rceil = \lceil d_n' \rceil - \lceil d_1' \rceil$. Denote by $s_1 \leq \cdots \leq s_n$ the successive minima of $(\mathcal{O}_F, \| \ \|_0)$. By Theorem 4.3.6 we obtain $\lceil d_n' \rceil \leq \lceil s_n \rceil = \lceil \mathrm{diam}(0) \rceil$, as $\lceil s_1 \rceil = 0$. We deduce $\lceil d_n \rceil - \lceil d_1 \rceil = \lceil d_n' \rceil \leq \lceil \mathrm{diam}(0) \rceil$. Then, by Lemma 3.3.12 and the fact $\dim \mathcal{O}_F = [k_0 : k]$ the statement holds. □

Note that the last corollary improves the bound from [16, Lemma 2.15].

Denote by $\mathcal{P}_F$ the set of all principal divisors of F/k. Clearly, $\mathcal{P}_F$ is a subgroup of $\mathcal{D}_F$. The factor group $\mathcal{C}_F := \mathcal{D}_F/\mathcal{P}_F$ is called the *divisor class group* of F/k. The class of a divisor D in $\mathcal{C}_F$ is denoted by $[D]$. Since $\deg D' = \deg D$, for any $D' \in [D]$, we define the degree of $[D]$ by the degree of any of its representative. The *class group* of F/k is defined by $\mathcal{C}_F^0 := \{[D] \in \mathcal{C}_F \mid \deg[D] = 0\}$. The class group is an abelian group, which is finite if F/k is global; that is, if k is finite.

Clearly, divisors D and D', which belong to the same class in $\mathcal{C}_F$, are isometric by Lemma 4.3.4. Thus, the classes of $\mathcal{C}_F$ are contained in the isometry classes of $\mathcal{D}_F$. Moreover, we can define the (normalized) successive minima of a class in $\mathcal{C}_F$ by the successive minima of any of its representative.

We call $[D], [D'] \in \mathcal{C}_F$ isometric if $D \simeq D'$, and write $[D] \simeq [D']$.

Lemma 4.3.10. *The number of isometry classes in $\mathcal{C}_F^0$ is finite.*

Proof. Since all elements in an isometry class share the same successive minima, we only have to show that the number of different successive minima, which are attained by elements in $\mathcal{C}_F^0$, is finite.

Denote by $s_1 \leq \cdots \leq s_n$ the successive minima of 0, the zero divisor. By definition any $[D]$ with successive minima $d_1 \leq \cdots \leq d_n$ satisfies $\deg[D] = 0 = \deg 0$, and therefore

$$\sum_{i=1}^{n} \lceil d_i \rceil = \sum_{i=1}^{n} \lceil s_i \rceil = |d(\mathcal{O}_F, \| \ \|_0)|$$

by Corollary 3.1.9. Since $\mathrm{sm}_0(D) \leq \mathrm{sm}(0)$ by Theorem 4.3.6 and $\|E\| \cap [r, s]$ is a finite set, for any $r, s \in \mathbb{R}$, by Lemma 2.2.6, there are only finitely many values that can be attained by the $d_i \in \|F\|$; hence, the statement holds. □

Note that in general the group law of $\mathcal{C}_F^0$ does not respect the isometry classes of $\mathcal{C}_F^0$; that means for $D_1, D_1', D_2, D_2' \in \mathcal{C}_F^0$ the fact $D_1 \simeq D_1'$ and $D_2 \simeq D_2'$ does not imply $D_1 + D_2 \simeq D_1' + D_2'$. Moreover, $\mathcal{D}_F$ is (in general) a proper subset of $\mathrm{LS}(F, R)_S$. This fact is a direct consequence of Theorem 3.3.15. One can easily find a concrete function field F/k, for which $C := |d(\mathcal{O}_F)| - 2n + (n-1)\mathrm{diam}(0) + 1 > [k_0 : k](g-2) + 1$. For instance, the function field in Example 2 from Section 6.2 satisfies $C = 213 > [k_0 : k](g-2) + 1 = 157$. According to the proof of Theorem 3.3.15 the bound C was minimal with its property. However, in function fields a better bound is available by the theorem of Riemann-Roch. Hence, there exist a lattice $(L, \| \ \|)$ in $\mathrm{LS}(F, R)_S$ such that $\mathrm{sm}(L, \| \ \|)$ is not attained by the successive minima of any $D \in \mathcal{D}_F$.

4.3.1 Computation of the successive minima of a divisor

Let D be a divisor of F/k and denote by $(I, \| \ \|)$ the induced lattice. In order to compute the successive minima of D we apply Algorithm 5, the optimized reduction algorithm, to an A-basis $\mathcal{B}$ of I and an orthonormal basis $\mathcal{B}'$ of the normed space F. This results in a reduced basis of $(I, \| \ \|)$, where the length of its vectors realize the the successive minima of D by Proposition 2.2.5.

In Chapter 5 we present an algorithm, which computes $\mathcal{B}$ and $\mathcal{B}'$ as desired.

Theorem 4.3.11. *Given a divisor D of F/k with $\mathcal{L}(D) = I \cap I_\infty$, $\mathcal{B}$ an Hermite bases of the fractional ideal I, and $\mathcal{B}'$ an orthonormal basis of I_∞. Then, the computation of the successive minima of D takes at most*

$$O(n^5(h(D) + n^2 C_f)^2)$$

arithmetic operations in k.

Proof. In order to obtain the desired bound we only have to consider Subsection 4.1.1 and replace Algorithm 3 by Algorithm 5 in the observation. According to Lemma 2.8.17, one can easily see that the complexity of computing a reduced basis of $(I, \| \ \|)$ coincides with the complexity of the computation of a semi-reduced basis of the same lattice in that context. One only has to take care with the fact that an orthonormal basis in general can not be given by an Hermite basis. In Chapter 5 we will see that an orthonormal basis can be determined such that the size of its vectors satisfy the same condition as an Hermite basis in the context of Lemma 1.2.11 and Corollary 1.2.13. □

Note that this gives us an advantage over [16, Algorithm 2.25], which only determines a semi-reduced basis and therefore just an approximation of the successive minima. That is, instead of the successive minima $d_1, \ldots, d_n$ of D, the latter algorithm determines $\lceil d_1 \rceil, \ldots, \lceil d_n \rceil$. The algorithm presented in [31] can determine the rational numbers $d_1, \ldots, d_n$ in the context of a tamely ramified global function field. To this purpose, Puiseux expansions of certain function field elements must be computed. This leads to the technical problem of choosing the right precision of the expansions. Our algorithm for the computation of the successive minima of D mentioned above can be applied for arbitrary function fields and no Puiseux expansions are used.

Let $D = D' + r(t)_\infty - (a)$ as described in (4.5) and Denote by $d_1 \leq \cdots \leq d_n$ and $d'_1 \leq \cdots \leq d'_n$ the successive minima of D and D', respectively. Then, $d'_i = d_i - r$, for $1 \leq i \leq n$. Hence, the divisor reduction can be applied in order to accelerate the computation of the successive minima of a divisor with "large" height.

5. Reduceness

The results of Chapter 2 can be applied to compute several objects in function fields like integral bases of fractional ideals and holomorphic rings, and in particular an orthonormal basis of the normed space $(F, \| \ \|_D)$, where F is a function field and $\| \ \|_D$ is the norm induced by a divisor $D \in \mathcal{D}_F$. To this end, we introduce the notion of P reduceness, for a place P of a function field F/k, and S-reduceness, for a subset S of $\mathbb{P}_F$. By weaken the concept of reduceness we obtain as in Section 2.8 the notion of semi-reduceness. If S is the set of all places of F lying over P_p (reps. P_∞), where $p(t) \in A$ is monic and irreducible, then Theorem 5.3.3 provides a new description of being a local integral basis.

We consider a different kind of "norm" on a function field F/k. Let $\tau \in F \setminus k_0$ and denote by $k[\tau]$ and $k(\tau)$ the polynomial ring and the rational function field in τ, respectively. Clearly, F is a $\deg(\tau)_\infty$-dimensional $k(\tau)$-vector space. By

$$v : k[\tau]^* \to \mathbb{Z}, \quad v\Big(\sum_{i=0}^{m} \lambda_i \tau^i\Big) := \min_{1 \le i \le m} \{i \mid \lambda_i \neq 0\}$$

and $v(0) := \infty$ we obtain a discrete valuation, which can be naturally extended to $k(\tau)$. We define a v-compatible norm.

Definition 5.0.1. *A* τ-norm *on* F *is a mapping* $w : F \to \mathbb{R} \cup \{\infty\}$ *that satisfies:*

1. $w(x + y) \geq \min\{w(x), w(y)\}$, *for all* $x, y \in F$,
2. $w(ax) = v(a) + w(x)$, *for all* $a \in k(\tau)$ *and* $x \in F$, *and*
3. $w(x) = \infty$ *if and only if* $x = 0$.

In other words, a τ-norm is an extension of the valuation v to a function on F having all properties of a valuation except for the good behavior with respect to multiplication.

Clearly, if w is a t^{-1}-norm, then $-w$ is an ordinary norm function on F as it was defined in Definition 2.1.1.

The theory of lattices and normed space can be adapted easily to this setting. For instance, the concept of reduceness with respect to a τ-norm can be defined as follows.

Definition 5.0.2. *Let w be a τ-norm. The set $\mathcal{B} \subset F$ is called w-reduced if*

$$w\Big(\sum_{b\in\mathcal{B}} \lambda_b b\Big) = \min_{b\in\mathcal{B}}\{w(\lambda_b b)\} \tag{5.1}$$

for all $\lambda_b \in k(\tau)$. Or equivalently, (5.1) holds for all $\lambda_b \in k[\tau]$. If we have additionally $0 \leq w(b) < 1$, for all $b \in \mathcal{B}$, then we call $\mathcal{B}$ w-orthonormal.

If we weaken condition (5.1) *to*

$$\Big\lfloor w\Big(\sum_{b\in\mathcal{B}} \lambda_b b\Big)\Big\rfloor = \min_{b\in\mathcal{B}}\{\lfloor w(\lambda_b b)\rfloor\},$$

we call $\mathcal{B}$ w-semi-reduced or w-semi-orthonormal, respectively.

If the τ-norm w is fixed we just say (semi-) reduced or (semi-) orthonormal, respectively.

Lemma 5.0.3. *The set $\mathcal{B} \subset F$ is (semi-) reduced with respect to the t^{-1}-norm w if and only if $\mathcal{B}$ is (semi-) reduced with respect to $\| \| := -w$. In particular, $-1 < \|b\| \leq 0$ if and only if $0 \leq w(b) < 1$, for all $b \in \mathcal{B}$.*

Clearly, any (semi-) reduced set $\mathcal{B} \subset F$ can be normalized to a (semi-) orthonormal set $\{\tau^{m_b} b \mid b \in \mathcal{B}\}$, where $m_b := -\lfloor w(b)\rfloor$.

5.1 P-reduceness

In this section we introduce the notion of P-reduceness, which can be seen as a "local" concept of reduceness. Let F/k be a function field and $P \in \mathbb{P}_0(F)$ be a place of F lying over P_p, where $p(t) \in A$ is a monic irreducible polynomial. Alternatively, one may choose a place $P \in \mathbb{P}_\infty(F)$, which lies over P_∞, the unique place at infinity of the rational function field K. Recall that $k_p = A/(p(t))$.

Definition 5.1.1. *For $a \in \mathbb{R}$ and $e \in \mathbb{Z}$ with $e \neq 0$, the mapping*

$$w_{P,e,a} : F \to \mathbb{R} \cup \{\infty\}, \quad w_{P,e,a}(z) := \frac{v_P(z) - a}{e}$$

is called the (P, e, a)-norm on F.

We fix an element $\tau \in F$ such that $v_P(\tau) = e$ and consider $F/k(\tau)$. Then, $w_{P,e,a}$ is a τ-norm on F.

The (P, e, a)-norm has a better behavior with respect to multiplications. In fact, we have

$$w_{P,e,a}(gh) = \frac{v_P(g)}{e} + w_{P,e,a}(h), \quad \forall g, h \in F. \tag{5.2}$$

Lemma 5.1.2. *Let $\mathcal{B} \subset F$ be $w_{P,e,a}$- (semi-) reduced. Then, $\mathcal{B}$ is $w_{P,e,a'}$- (semi-) reduced, for any $a' \in \mathbb{R}$.*

Proof. Since $w_{P,e,a'}(z) = w_{P,e,a}(z) + \frac{a-a'}{e}$, for all $z \in F$, the statement follows immediately from Definition 5.0.2. □

The next result is an immediate consequence of (5.2).

Lemma 5.1.3. *Let $\mathcal{B} \subset F$ be a $w_{P,e,a}$-reduced set and $c \in F^*$. Then, $c\mathcal{B}$ is $w_{P,e,a}$-reduced.*

In order to derive an adequate reduceness criterion for the concept of "local" reduceness, we are going to consider local fields. Therefore, we consider the completion of the function field F at a place P (details can be found in [26]).

Denote by $\hat{F}_P$ the completion of F at P. Let $\mathfrak{p}$ be a prime ideal of F corresponding to the place $P \in \mathbb{P}_F$ as in Subsection 1.2.3 and denote by $p(t)$ the monic irreducible polynomial in A lying under P. Regarding the notation from Section 1.4, for $P|P_p$ and $P|P_\infty$, we can realize the completions $\hat{F}_P$ by

$$\hat{F}_P = K_p(\theta_\mathfrak{p}), \quad \hat{F}_P = K_\infty(\theta_\mathfrak{p}), \tag{5.3}$$

respectively, where $K_p = k_p((p(t)))$, $K_\infty = k((t^{-1}))$, and $\theta_\mathfrak{p}$ denotes a root of $f_\mathfrak{p}$, the irreducible factor of f over $\hat{A}_p[x]$ (resp. f_∞ over $\hat{A}_\infty[x]$) corresponding to $\mathfrak{p}$.

The valuation v_p (resp. v_∞) extends in a unique way to a non-discrete valuation

$$\hat{v} : \overline{K}_p \to \mathbb{Q} \quad (\text{resp. } \hat{v} : \overline{K}_\infty \to \mathbb{Q}).$$

Note that $\hat{v}(\iota_P(z)) = v_P(z)/e(P/P_p)$ (resp. $\hat{v}(\iota_P(z)) = v_P(z)/e(P/P_\infty)$), for $z \in F$, where ι_P denotes the injection of F into $\hat{F}_P$ determined by $\theta \mapsto \theta_\mathfrak{p}$ (resp. $\theta_\infty \mapsto \theta_\mathfrak{p}$). In particular, it holds

$$\hat{v}(g(\theta_\mathfrak{p})) = v_P(g(\theta))/e(P/P_p), \quad \text{for all } g(x) \in A[x]. \tag{5.4}$$

The same yields for $g(x) \in A_\infty[x]$ with θ_∞ and $P|P_\infty$. We denote by $\hat{\mathcal{O}}_P \subset \hat{F}_P$ the valuation ring of the restriction of $\hat{v}$ to $\hat{F}_P$ and set $\hat{P} := \{z \in \hat{\mathcal{O}}_P \mid \hat{v}(z) > 0\}$ the maximal ideal of $\hat{\mathcal{O}}_P$.

The next lemma will play a fundamental role in the subsequent description of the computation of integral bases of fractional ideals. Any nonzero prime ideal $\mathfrak{p}$ of F (and therefore any place P) determines a set $\mathcal{B}_\mathfrak{p}$ of divisor polynomials (cf. Definition 1.4.11). In the sequel let P denote a place and $\mathfrak{p}$ the corresponding prime ideal. For a subset $\mathcal{B}$ of $A[x]$ denote $\mathcal{B}(\theta) := \{g(\theta) \mid g \in \mathcal{B}\}$. For convenience, we consider in what follows only prime ideals $\mathfrak{p}$ of $\mathcal{O}_F$. Clearly, all results can be translated to prime ideals of $\mathcal{O}_{F,\infty}$.

Lemma 5.1.4. *Let $\tau := p(t) \in A$ be a monic irreducible polynomial and let P be a place of F lying over P_p. Then, the set $\mathcal{B}_\mathfrak{p}(\theta)$ is $w_{P,e,a}$-reduced, for any $a \in \mathbb{R}$, where $e := e(P/P_p)$.*

Proof. By Lemma 5.1.2 we can assume that $a = 0$. Then, $w := w_{P,e,0} = e^{-1}v_P$ a discrete valuation, and $w(g(\theta)) = \hat{v}(g(\theta_\mathfrak{p}))$ for all $g \in A[x]$ by (5.4). Suppose that $\mathcal{B}_\mathfrak{p}(\theta) = \{1, g_1(\theta), \ldots, g_{n_\mathfrak{p}-1}(\theta)\}$ is not w-reduced. Let $\lambda_0, \ldots, \lambda_{n_\mathfrak{p}-1} \in k[p(t)]$ with

$$w\Big(\sum_{i=0}^{n_\mathfrak{p}-1} \lambda_i g_i(\theta)\Big) > \min_{0 \le i < n_\mathfrak{p}} \{w(\lambda_i g_i(\theta))\}. \tag{5.5}$$

By the strict triangle inequality we only have to consider all summands on the left hand side of (5.5), which have the same (minimal) w-value. In other words, we can assume that all summands on the left hand side of (5.5) have the same norm. According to Lemma 1.4.9 it holds $w(g_i(\theta)) \ge w(g_j(\theta))$, for all $0 \le j < i < n_\mathfrak{p}$. Since all summands in (5.5) have the same norm, we have $v_p(\lambda_j) \ge v_p(\lambda_i)$, for all $0 \le j < i < n_\mathfrak{p}$. Hence, $g(x) := \lambda_{n-1}^{-1} \sum_{i=0}^{n_\mathfrak{p}-1} \lambda_i g_i(\theta)$ is a monic polynomial of degree $n_\mathfrak{p} - 1$ with coefficients in $\hat{A}_p$ satisfying:

$$w(g(\theta)) > \min_{0 \le i < n_\mathfrak{p}} \{w(\lambda_{n-1}^{-1}\lambda_i g_i(\theta))\} = w(g_{n_\mathfrak{p}-1}(\theta)),$$

which is a contradiction, as $g_{n_\mathfrak{p}-1}$ is a divisor polynomial of $f_\mathfrak{p}$ (cf. Proposition 1.4.7). □

Henceforth we consider the τ-norm $w := w_{P,e,a}$ with $v_P(\tau) = e > 0$ and $a \in \mathbb{Z}$. We are interested in a criterion to check wether a set $\mathcal{B} \subset F$ is w-reduced or not. To this end, we consider P-adic expansions of elements in $\hat{F}_P$.

Let π_P be a prime element of P (i.e. $v_P(\pi_P) = 1$) and R be a system of representatives of F_P, the residue class field of P. By [26, Satz 4.4] any nonzero element z in $\hat{F}_P$ has a unique representation $z = \pi_P^m(\lambda_0 + \lambda_1\pi_P + \lambda_2\pi_P^2 + \cdots)$, where $\lambda_i \in R$ and $m = v_P(z) \in \mathbb{Z}$. In particular, for any $z \in F^*$ we can write

$$\iota_P(z) = \sum_{j=v_P(z)}^{\infty} \lambda_j \pi_P^j, \quad \lambda_j \in R.$$

Motivated by Section 2.3 we are interested in a kind of reduction map, which provides a reduceness-criterion analogous to Theorem 2.3.3.

For any $r \in \mathbb{R}$ the sets

$$F_{\geq r} := \{z \in F \mid w(z) \geq r\} \supset F_{>r} := \{z \in F \mid w(z) > r\}$$

are $k[\tau]$-submodules of F. Their quotient is a k-vector space $V_r := F_{\geq r}/F_{>r}$. For $r \notin w(F)$ it holds $V_r = 0$, whereas for $r \in w(F)$ there is a non-canonical isomorphism $V_r \cong F_P$, which we are going to describe. Suppose that $r \in w(F)$; that is, $er \in \mathbb{Z}$. Consider the division with remainder

$$er + a = qe + m, \quad 0 \leq m < e.$$

For $z \in F$ with $w(z) \geq r$, a reduction map is given by

$$\mathrm{red}^r_{(P,e,a)}(z) : F_{\geq r} \to F_P, \quad z \mapsto z\tau^{-q}\pi_P^{-m} + P,$$

Clearly, $\mathrm{red}^r_{(P,e,a)}$ is k-linear and it vanishes on $F_{>r}$. Thus, it induces a concrete isomorphism between V_r and F_P.

Theorem 5.1.5. *A set $\mathcal{B} \subset F$ is w-reduced if and only if for any $\rho \in \mathcal{R} := \{w(b) + \mathbb{Z} \mid b \in \mathcal{B}\}$ the vectors in*

$$\{\mathrm{red}^{w(b)}_{(P,e,a)}(b) \mid b \in \mathcal{B} \text{ with } w(b) + \mathbb{Z} = \rho\}$$

are k-linearly independent.

Proof. For $\rho \in \mathcal{R}$, we set $\mathcal{B}_\rho := \{b \in \mathcal{B} \mid w(b) + \mathbb{Z} = \rho\}$. The fact that $\mathcal{B}$ is w-reduced if and only if $\mathcal{B}_\rho$ is w-reduced, for all $\rho \in \mathcal{R}$, can be shown analogously to Lemma 2.3.2. Hence, we can assume that all vectors $b \in \mathcal{B}$ have the same length ρ modulo $\mathbb{Z}$.

Moreover, by an argument similar to that of Lemma 2.2.2 we may assume that all vectors $b \in \mathcal{B}$ have the same norm, by replacing each $b \in \mathcal{B}$ by $\tau^m b$ for an adequate choice of $m \in \mathbb{Z}$. Let us denote by $r := w(b)$ this common norm.

Let $\mathcal{B} = \{b_1, \dots, b_n\}$. We take $h_1(\tau), \dots, h_n(\tau) \in k[\tau]$ and consider $z := \sum_{i=1}^{n} h_i(\tau)b_i$. Let $m := \min_{1\le i\le n}\{v(h_i(\tau))\}$ and denote by I the set of all indices i for which $v(h_i(\tau)) = m$. For $i \in I$, we write $h_i(\tau) = \lambda_i\tau^m + h_i'(\tau)$ with $\lambda_i \in k^*$ and $v(h_i'(\tau)) > v(h_i(\tau))$. Denote $z' := \sum_{i\in I} \lambda_i b_i$. Since $w(a+b) = \min\{w(a), w(b)\}$, for all $a, b \in F$ with $w(a) \neq w(b)$, we obtain:

$$w(z) = w\Big(\sum_{i\in I} h_i(\tau)b_i\Big) = w\Big(\sum_{i\in I} \lambda_i\tau^m b_i\Big) = m + w(z').$$

On the other hand,

$$\min_{1\le i\le n}\{w(h_i(\tau)b_i)\} = \min_{i\in I}\{w(h_i(\tau)b_i)\} = w(h_i(\tau)b_i) = w(\lambda_i\tau^m b_i) = m + r.$$

Thus, $w(z') = r$ is equivalent to

$$0 \neq \operatorname{red}^r_{(P,e,a)}(z') = \sum_{i\in I} \lambda_i \operatorname{red}^r_{(P,e,a)}(b_i).$$

Hence, $w(\sum_{i=1}^{n} h_i(\tau)b_i) = \min\{w(h_i(\tau)b_i)\}$, for any $h_1(\tau), \dots, h_n(\tau) \in k[\tau]$ is equivalent to the fact that

$$\operatorname{red}^r_{(P,e,a)}(b_1), \dots, \operatorname{red}^r_{(P,e,a)}(b_n)$$

are k-linearly independent. □

In order to obtain an analogous criterion to test if a subset of F is w-semi-reduced we introduce another kind of reduction map. Recall that $w = w_{P,e,a}$ with $e, a \in \mathbb{Z}$ and $e > 0$.

Definition 5.1.6. *For $r \in \mathbb{R}$ and $z \in F_{\ge\lfloor r\rfloor}$, we have $v_P(z\pi_P^{-a}\tau^{-\lfloor r\rfloor}) = v_P(z) - a - e\lfloor r\rfloor \ge 0$. We write $\iota_P(z\pi_P^{-a}\tau^{-\lfloor r\rfloor}) = \lambda_0 + \lambda_1\pi_P + \cdots + \lambda_{e-1}\pi_P^{e-1} + \cdots$, and define*

$$\operatorname{sred}^r_{(P,e,a)}(z) := (\lambda_0 \dots \lambda_{e-1}) \in F_P^e.$$

Clearly, $\operatorname{sred}^r_{(P,e,a)}$ is k-linear.

Lemma 5.1.7. *For $r \in w(F)$ and $z \in F$ with $w(z) \ge \lfloor r\rfloor$, we have $\operatorname{sred}^r_{(P,e,a)}(z) \neq 0$ if and only if $\lfloor w(z)\rfloor = \lfloor r\rfloor$.*

Proof. If $\lfloor w(z)\rfloor = \lfloor r\rfloor$, we have $w(z) < r+1$; hence, $v_P(z\pi_P^{-a}\tau^{-\lfloor r\rfloor}) < e$, and in particular $\operatorname{sred}^r_{(P,e,a)}(z) \neq 0$. If $\lfloor w(z)\rfloor > \lfloor r\rfloor$, we have $w(z) \ge r+1$; hence, $v_P(z\pi_P^{-a}\tau^{-\lfloor r\rfloor}) \ge e$ and $\operatorname{sred}^r_{(P,e,a)}(z) = 0$. □

Theorem 5.1.8. *A set $\mathcal{B} \subset F$ is w-semi-reduced if and only if the vectors in*

$$\{\mathrm{sred}^{w(b)}_{(P,e,a)}(b) \mid b \in \mathcal{B}\}$$

are k-linearly independent.

Proof. The statement can be proven by considering the proof of Theorem 5.1.5 and replacing w by $\lfloor w \rfloor$ and $\mathrm{red}^r_{(P,e,a)}$ by $\mathrm{sred}^r_{(P,e,a)}$, respectively. □

5.2 S-reduceness

The concept of P-reduceness can be generalized to several places $P_1, \ldots, P_s$. Henceforth denote by $S = \{P_1, \ldots, P_s\}$ a finite set of places of F.

Definition 5.2.1. *Let $e = (e_1, \ldots, e_s) \in (\mathbb{Z}_{>0})^s$ and $a = (a_1, \ldots, a_s) \in \mathbb{Z}^s$. We define*

$$w_{e,a} : F \to \mathbb{Q} \cup \{\infty\}, \quad w_{e,a}(z) := \min_{1 \le i \le s} \{w_{P_i,e_i,a_i}(z)\}$$

An immediate consequence of this definition is the following observation.

Lemma 5.2.2. *Let $\tau \in F$ such that $v_{P_i}(\tau) = e_i$ for all $1 \le i \le s$. Then, $w_{e,a}$ is a τ-norm on F.*

Example 5.2.3. Let D be a Divisor of F, $e := (e(P/P_\infty) \mid P \in \mathbb{P}_\infty(F))$, and $a := (-v_P(D) \mid P \in \mathbb{P}_\infty(F))$. Then, $w_{e,a}$ is a τ-norm, for $\tau := t^{-1}$. In particular, $-w_{e,a}$ coincides with the norm $\| \ \|_D$ induced by D defined in (4.1).

Let again $e := (e_1, \ldots, e_s) \in (\mathbb{Z}_{>0})^s$ and $a := (a_1, \ldots, a_s) \in \mathbb{Z}^s$. We fix $\tau \in F$ with $v_{P_i}(\tau) = e_i$, for $1 \le i \le s$ and set $w := w_{e,a}$.

As in the last section we define "reduction maps" red and sred in order to generalize the reduceness-criterion from Theorem 5.1.5 and the semi-reduceness-criterion of Theorem 5.1.8 to this situation.

Definition 5.2.4. *For $r \in \mathbb{R}$ and $z \in F$, we define*

$$\mathrm{red}^r_{(e,a)}(z) := (\mathrm{red}^r_{(P_i,e_i,a_i)}(z))_{1 \le i \le s} \in F_{P_1} \times \cdots \times F_{P_s} \text{ and}$$
$$\mathrm{sred}^r_{(e,a)}(z) := (\mathrm{sred}^r_{(P_i,e_i,a_i)}(z))_{1 \le i \le s} \in F^{e_1}_{P_1} \times \cdots \times F^{e_s}_{P_s}.$$

The following properties are transmitted by the properties of the local mappings $\mathrm{red}^r_{(P_i,e_i,a_i)}$ and $\mathrm{sred}^r_{(P_i,e_i,a_i)}$, for $1 \le i \le s$, respectively.

Lemma 5.2.5. *The mappings* $\mathrm{red}^r_{(e,a)}$ *and* $\mathrm{sred}^r_{(e,a)}$ *are* k*-linear and vanish on* $F_{>r}$ *and* $F_{\geq \lfloor r \rfloor + 1}$*, respectively.*

Analogously to Theorem 5.1.5 and Theorem 5.1.8 one can prove the following statements.

Theorem 5.2.6. *A set* $\mathcal{B} \subset F$ *is* w*-reduced if and only if for any* $\rho \in \mathcal{R} := \{w(b) + \mathbb{Z} \mid b \in \mathcal{B}\}$ *the vectors in*

$$\{\mathrm{red}^{w(b)}_{(e,a)}(b) \mid b \in \mathcal{B} \text{ with } w(b) + \mathbb{Z} = \rho\}$$

are k*-linearly independent.*

Theorem 5.2.7. *A set* $\mathcal{B} \subset F$ *is* w*-semi-reduced if and only if the vectors in*

$$\{\mathrm{sred}^{w(b)}_{(e,a)}(b) \mid b \in \mathcal{B}\}$$

are k*-linearly independent.*

We are interested in the relation between P-reduced and S-reduced. Note that all considered norms are τ-norms, for a fixed τ as mentioned before.

Theorem 5.2.8. *For* $1 \leq i \leq s$*, let* $\mathcal{B}_i \subset F$ *be* w_{P_i,e_i,a_i}*-reduced and* $z_i \in F$ *such that, for all* $b \in \mathcal{B}_i$*,*

$$w_{P_i,e_i,a_i}(z_i b) < w_{P_j,e_j,a_j}(z_i b), \text{ for } j \in \{1, \ldots, s\} \setminus \{i\}. \tag{5.6}$$

Then, $\bigcup_{i=1}^s z_i \mathcal{B}_i$ *is* $w_{e,a}$*-reduced.*

Proof. We set $\mathrm{red}^r_i := \mathrm{red}^r_{(P_i,e_i,a_i)}$ and $w_i := w_{P_i,e_i,a_i}$, for $1 \leq i \leq s$ and $r \in \mathbb{R}$. By (5.6), for $1 \leq i, j \leq s$ and $b \in \mathcal{B}_i$, it holds $w(z_i b) = w(z_i b)_i$ and $w(z_i b) < w(z_i b)_j$, for $j \neq i$. Then, we obtain $\mathrm{red}^{w(z_i b)}_j(z_i b) = 0 \in F_{P_j}$, for all $j \neq i$, by the definition of red^r_j. Hence, $\mathrm{red}^{w(z_i b)}_{(e,a)}(z_i b)$ is given by

$$(0, \ldots, 0, \mathrm{red}^{w(z_i b)}_i(z_i b), 0, \ldots, 0).$$

By Lemma 5.1.3 the sets $z_i \mathcal{B}_i$ are w_i-reduced, for $1 \leq i \leq s$, and therefore $\{\mathrm{red}^{w(z_i b)}_{(e,a)}(z_i b) \mid b \in \mathcal{B}_i\}$ are k-linearly independent by Theorem 5.1.5. Hence, the set $\bigcup_{i=1}^s z_i \mathcal{B}_i$ is $w_{e,a}$-reduced by Theorem 5.2.6. □

Theorem 5.2.9. *For* $1 \leq i \leq s$*, let* $\mathcal{B}_i \subset F$ *be* w_{P_i,e_i,a_i}*-reduced and* $z_i \in F$ *such that for all* $b \in \mathcal{B}_i$

1. $\lfloor w_{P_i,e_i,a_i}(z_i b)\rfloor \leq \lfloor w_{P_j,e_j,a_j}(z_i b)\rfloor$ *for* $1 \leq i < j \leq s$

2. $\lfloor w_{P_i,e_i,a_i}(z_i b)\rfloor < \lfloor w_{P_l,e_l,a_l}(z_i b)\rfloor$ *for* $1 \leq l < i \leq s$.

Then, $\bigcup_{i=1}^{s} z_i\mathcal{B}_i$ *is* $w_{e,a}$*-semi-reduced.*

Proof. We set $w_i := w_{P_i,e_i,a_i}$ and $\mathrm{sred}_i^r := \mathrm{sred}^r_{(P_i,e_i,a_i)}$, for $1 \leq i \leq s$ and $r \in \mathbb{R}$. By the hypothesis, for $1 \leq l < i \leq s$ and $b \in \mathcal{B}_i$, we have $\lfloor w(z_i b)\rfloor = \lfloor w(z_i b)_i\rfloor < \lfloor w(z_i b)_l\rfloor$; hence, $\mathrm{sred}_l^{w(z_i b)}(z_i b) = 0 \in F_{P_l}^{e_l}$. In particular, with $r_i := w(z_i b)$ we deduce, for $1 \leq i \leq s$,

$$\mathrm{sred}^{r_i}_{(e,a)}(z_i b) = (0, \ldots, 0, \mathrm{sred}_i^{r_i}(z_i b), *, \ldots, *), \tag{5.7}$$

with some vectors $* \in F_{P_j}^{e_j}$, for $j > i$. Since $\lfloor w(z_i b)\rfloor = \lfloor w(z_i b)_i\rfloor$, we have $\mathrm{sred}_i^{w(z_i b)}(z_i b) = \mathrm{sred}_i^{w(z_i b)_i}(z_i b)$, for $b \in \mathcal{B}_i$. According to Lemma 5.1.3 the sets $z_i\mathcal{B}_i$ are w_i-reduced, and particularly w_i-semi-reduced. Then, by Theorem 5.1.8 the family $\{\mathrm{sred}_i^{w(z_i b)}(z_i b) \mid b \in \mathcal{B}_i\}$ is k-linearly independent. By (5.7), the family $\bigcup_{1\leq i\leq s}\{\mathrm{sred}^{w(z_i b)}_{(e,a)}(z_i b) \mid b \in \mathcal{B}_i\}$ is k-linearly independent. Thus, by Theorem 5.2.7 $\bigcup_{1\leq i\leq s} z_i\mathcal{B}_i$ is $w_{e,a}$-semi-reduced.

□

5.3 Computation of integral bases

Denote F/k a function field of degree n and $\mathcal{O}_F$ and $\mathcal{O}_{F,\infty}$ its finite and infinite maximal orders, respectively. We consider a fractional ideal I of $\mathcal{O}_F$ or $\mathcal{O}_{F,\infty}$. The goal of this section is to describe an algorithm, which computes a (reduced) integral basis of I; that is, an A-basis or an A_∞-basis of I, respectively.

Lemma-Definition 5.3.1. *Let* I *be a fractional ideal of* $\mathcal{O}_F$*,* $b_1, \ldots, b_n \in I$ *be* A*-linearly independent elements, and denote by* $M = \langle b_1, \ldots, b_n \rangle_A$ *the* A*-submodule of* I *that they generate. We fix a monic irreducible polynomial* $p(t) \in A$ *and denote by* A_p *the localization of* A *at the prime ideal* $p(t)A$*. The following conditions are equivalent:*

1. $v_p([I : M]) = 0$.

2. $b_1 \otimes 1, \ldots, b_n \otimes 1$ *are an* A_p*-basis of* $I \otimes_A A_p$.

3. $b_1 \otimes 1, \ldots, b_n \otimes 1$ *are a* k_p*-basis of* $I \otimes_A k_p$.

If these conditions are satisfied we call $(b_1, \ldots, b_n)$ *a* $p(t)$*-integral basis of* I*.*

Proof. The three conditions are equivalent by Nakayama's lemma, which can be found in [17]. □

For a fractional ideal I of $\mathcal{O}_{F,\infty}$ a t^{-1}-integral basis can be defined analogously by replacing A by $k[t^{-1}]$ and A_p by A_∞. Then, by item *2* a t^{-1}-integral basis is just an A_∞-basis of I.

We will restrict our consideration to fractional ideals of the finite maximal order, since the "infinite" case can be treated analogously.

In order to determine an A-basis of I (i.e. a global basis) of a fractional ideal of $\mathcal{O}_F$, we may compute $p(t)$-integral bases $\mathcal{B}_p$ of I for any irreducible polynomial $p(t)$ with $v_p([I : A[\theta]]) \neq 0$. Later we describe how to combine the "local" bases $\mathcal{B}_p$ to a global one by an easy application of the CRT.

5.3.1 Computation of $p(t)$-integral bases

We fix a monic and irreducible polynomial $p(t) \in A$ and denote by $\mathbb{P}_p(F)$ the set of all places lying over P_p. Any fractional ideal I of $\mathcal{O}_F$ has a unique factorization into nonzero prime ideals. By the identification of nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}_F$ and places $P \in \mathbb{P}_0(F)$ (cf. Subsection 1.2.3), we deduce

$$I = \prod_{P \in \mathbb{P}_0(F)} \mathfrak{p}^{a_P}.$$

Let $I_p := \prod_{P \in \mathbb{P}_p(F)} \mathfrak{p}^{a_P}$. Clearly, the ideal I_p induces a mapping $w_{I_p} : F \to \mathbb{Q} \cup \{\infty\}$,

$$w_{I_p}(z) := \min_{\mathfrak{p} \in \mathbb{P}_p(F)} \left\{ \frac{v_P(z) - a_P}{e(P/P_p)} \right\}.$$

We set $\tau := p(t)$. Then, the following observation is obvious.

Lemma 5.3.2. *The map w_{I_p} is a τ-norm. For $e := (e(P/P_p))_{P \in \mathbb{P}_p(F)}$ and $a := (a_P)_{P \in \mathbb{P}_p(F)}$ it holds $w_{I_p} = w_{e,a}$.*

For $\mathbb{P}_p(F) = \{P_1, \ldots, P_s\}$, we fix $e_i := e(P_i/P_p)$ and $a_i := a_{P_i}$ and set henceforth $e := (e_1, \ldots, e_s)$ and $a := (a_1, \ldots, a_s)$. For any $z \in F$ and $r \in \mathbb{R}$, we set $\mathrm{red}^r_{I_p}(z) := \mathrm{red}^r_{(e,a)}(z)$ and $\mathrm{sred}^r_{I_p}(z) := \mathrm{sred}^r_{(e,a)}(z)$.

Theorem 5.3.3. *Let $\mathcal{B}$ be subset of F with n elements. Then, $\mathcal{B}$ is a $p(t)$-integral basis of I if and only if $\mathcal{B}$ is w_{I_p}-semi-orthonormal.*

Proof. Suppose that $\mathcal{B}$ is w_{I_p}-semi-orthonormal. An easy computation shows that $w_{I_p}(z) \geq 0$ if and only if $z \in I$; hence, the set $\mathcal{B}$ is a subset of I. According to Lemma-Definition 5.3.1 it is sufficient to show that $\mathcal{B}$ is a set of k_p-linearly independent vectors in order to show that $\mathcal{B}$ is a $p(t)$-integral basis of I.

Assume $\sum_{b\in\mathcal{B}} \lambda_b b \in p(t)I \otimes_A A_p$ with $\lambda_b \in A_p$. Then, $w_{I_p}(\sum_{b\in\mathcal{B}} \lambda_b b) \geq 1$. Since $\mathcal{B}$ is w_{I_p}-semi-orthonormal, we deduce $w_{I_p}(\lambda_b b) \geq 1$, for all $b \in \mathcal{B}$, and therefore $v_p(\lambda_b) \geq 1$, for all $b \in \mathcal{B}$. That is, $\lambda_b \in p(t)A_p$, for $b \in \mathcal{B}$.

For the other direction we use the following claim.

Claim:
Let $\mathcal{B}' = (b'_1, \ldots, b'_n)$ be a w_{I_p}-semi-orthonormal basis, $T \in \mathrm{GL}_n(A_p)$, and $\mathcal{B} := (b_1, \ldots, b_n)$ determined by $T(b'_1, \ldots, b'_n)^{\mathrm{tr}} = (b_1, \ldots, b_n)^{\mathrm{tr}}$. Then, $\mathcal{B}$ is a w_{I_p}-semi-orthonormal basis.

After the claim, the statement of the lemma yields immediately. Let $\mathcal{B}$ be any $p(t)$-integral basis of I and $\mathcal{B}'$ a w_{I_p}-semi-orthonormal subset of I with n elements. As shown above, the family $\mathcal{B}'$ is also a $p(t)$-integral basis of I; hence, the transition matrix from $\mathcal{B}$ to $\mathcal{B}'$ belongs to $\mathrm{GL}_n(A_p)$. Thus, the claim states that $\mathcal{B}$ is w_{I_p}-semi-orthonormal too.

In order to prove the claim we consider Lemma 2.8.8. Analogously to its proof one can show that a matrix $T = (t_{i,j}) \in K^{n\times n}$ belongs to $\mathrm{GL}_n(A_p)$ if and only if

$$\min_{1\leq i\leq n} \Big\{ v_p\Big(\sum_{j=1}^{n} t_{j,i} a_j \Big) \Big\} = \min_{1\leq i\leq n} \{ v_p(a_i) \}, \tag{5.8}$$

for all $a_1, \ldots, a_n \in K$, having in mind that $|\ | = -v_\infty$. Let $a_1, \ldots, a_n \in K$ and set $a'_i := \sum_{j=1}^{n} t_{j,i} a_j$, for $1 \leq i \leq n$, where $(t_{i,j}) = T$. Since $\mathcal{B}'$ is w_{I_p}-semi-orthonormal and by (5.8) we obtain

$$\begin{aligned} \Big\lfloor w_{I_p}\Big(\sum_{i=1}^{n} a_i b_i \Big) \Big\rfloor = \Big\lfloor w_{I_p}\Big(\sum_{i=1}^{n} a'_i b'_i \Big) \Big\rfloor &= \min_{1\leq i\leq n} \{ v_p(a'_i) \} \\ &= \min_{1\leq i\leq n} \Big\{ v_p\Big(\sum_{j=1}^{n} t_{j,i} a_j \Big) \Big\} = \min_{1\leq i\leq n} \{ v_p(a_i) \}. \end{aligned}$$

Thus, $\mathcal{B}$ is w_{I_p}-semi-orthonormal .

□

Let f be a defining polynomial of the function field F/k and $\mathbb{P}_p(F) = \{P_1, \ldots, P_s\}$. For any place $P_j \in \mathbb{P}_p(F)$, corresponding to the prime ideal $\mathfrak{p}_j$, denote by $\Phi_j := \phi_{\mathfrak{p}_j}$ an

Okutsu approximation of the $p(t)$-adic irreducible factor $f_{\mathfrak{p}_j}$ of f in $\hat{A}_p[x]$ (cf. Subsection 1.4.3) and let $\mathcal{B}_j := \mathcal{B}_{\mathfrak{p}_j}(\theta)$, where $\mathcal{B}_{\mathfrak{p}_j}$ is defined in Definition 1.4.11.

We recall that the values $v_{P_j}(\Phi_i(\theta))$ for $j \neq i$ are computed by some closed formulas in terms of data collected by the Montes algorithm. When we improve Φ_i, the value $v_{P_i}(\Phi_i(\theta))$ increases, but the values $v_{P_j}(\Phi_i(\theta))$ for $j \neq i$ remain constant.

We set $n_{\mathfrak{p}_j} = \deg f_{\mathfrak{p}_j}$, for $1 \leq j \leq s$. Note that $n_{\mathfrak{p}_j} = e(P_j/P_p)f(P_j/P_p)$. By Lemma 5.1.4 the set $\mathcal{B}_j$ is $w_{P_j,e_j,a}$-reduced, for any $a \in \mathbb{R}$ and $1 \leq j \leq s$. By definition it holds $\#\mathcal{B}_j = \deg f_{\mathfrak{p}_j}$, for $1 \leq j \leq s$; hence, $\#\bigcup_{\kappa=1}^{s} \mathcal{B}_\kappa = \sum_{i=1}^{s} \deg f_{\mathfrak{p}_j} = \deg f = n$.

By applying Theorems 5.2.8, 5.2.9, and 5.3.3 we obtain the next two statements.

Theorem 5.3.4. *For $1 \leq \kappa \leq s$, we set*

$$z_\kappa := \prod_{\substack{j=1 \\ j\neq\kappa}}^{s} \Phi_j^{\epsilon_j}(\theta), \tag{5.9}$$

where $\epsilon_j \in \{0,1\}$ and the Okutsu approximation Φ_j are chosen in such a way that, for all $b \in \mathcal{B}_\kappa$,

1. $\lfloor w_{P_\kappa,e_\kappa,a_\kappa}(z_\kappa b)\rfloor \leq \lfloor w_{P_i,e_i,a_i}(z_\kappa b)\rfloor$, *for* $1 \leq \kappa < i \leq s$,
2. $\lfloor w_{P_\kappa,e_\kappa,a_\kappa}(z_\kappa b)\rfloor < \lfloor w_{P_i,e_i,a_i}(z_\kappa b)\rfloor$, *for* $1 \leq i < \kappa \leq s$.

Then, $\{b_1,\dots,b_n\} := \bigcup_{\kappa=1}^{s} z_\kappa \mathcal{B}_\kappa$ is w_{I_p}-semi-reduced. In particular, the family

$$\frac{b_i}{p(t)^{\lfloor w_{I_p}(b_i)\rfloor}}, \quad 1 \leq i \leq n,$$

is a $p(t)$-integral basis of I.

Theorem 5.3.5. *If we replace in Theorem 5.3.4 item 1 and 2 by the condition*

$$w_{P_\kappa,e_\kappa,a_\kappa}(z_\kappa b) < w_{P_i,e_i,a_i}(z_\kappa b), \text{ for } i \in \{1,\dots,s\} \setminus \{\kappa\},$$

then $(b_i/p(t)^{\lfloor w_{I_p}(b_i)\rfloor})_{1\leq i\leq n}$ is a w_{I_p}-orthonormal basis of I.

The idea of using multipliers to construct integral bases goes back to Ore (1925). In [10] a similar way of determining adequate multipliers is presented. An advantage of our choice is that in practice the multipliers z_κ are simple. That is, many exponents ϵ_j in (5.9) are zero. Often we may take

$$z_\kappa = \prod_{j<\kappa} \Phi_j(\theta), \quad 1 \leq \kappa \leq s.$$

Since $\deg \Phi_j = n_{\mathfrak{p}_j}$ and $\deg g_m = m$, for $g_m \in \mathcal{B}_{\mathfrak{p}_j}$ and $1 \leq j \leq s$, the degree of $\prod_{j<\kappa} \Phi_j(x) g_m$ is equal $\sum_{j<\kappa} n_{\mathfrak{p}_j} + m$, and the basis $\mathcal{B}$ is in that particular case triangular; that is, the transition matrix from $\mathcal{B}$ to $(1, \theta, \ldots, \theta^{n-1})$ is a triangular matrix. Even though, the multipliers z_κ are not always that simple, our choice leads in many cases to a partly triangular basis $\mathcal{B}$. Hence, the resulting $p(t)$-integral basis $\left(b_i/p(t)^{\lfloor w_{I_p}(b_i) \rfloor}\right)_{1 \leq i \leq n}$ can be transformed quickly into a Hermite basis.

At the end of this subsection we consider an alternative construction for the multiplier z_κ, $1 \leq \kappa \leq s$.

Algorithm 8: Computation of a $p(t)$-integral basis

Input: Defining polynomial f of a function field F/k, fractional ideal I of $\mathcal{O}_F$, irreducible polynomial $p(t) \in A$, and boolean variable red.

Output: A $p(t)$-integral basis of I, which is additionally w_{I_p}-orthonormal if red = TRUE.

1: Algorithm 1$(f, p(t))$
2: **for** $\mathfrak{p}_i | p$ **do**
3: Determine $\mathcal{B}_i = \mathcal{B}_{\mathfrak{p}_i}(\theta)$ with $\mathcal{B}_{\mathfrak{p}_i}$ as in Definition 1.4.11
4: Determine Φ_i by Algorithm 2 satisfying, if red = FALSE, the conditions of Theorem 5.3.4 and else the conditions of Theorem 5.3.5
5: **end for**
6: $\{b_1, \ldots, b_n\} \leftarrow \bigcup_{\kappa=1}^{s} z_\kappa \mathcal{B}_\kappa$
7: **return** $\left(b_i/p(t)^{\lfloor w_{I_p}(b_i) \rfloor}\right)_{1 \leq i \leq n}$

In order to determine the exponents ϵ_j and the precision of the approximations Φ_j so that z_κ satisfies the conditions of Theorem 5.3.4 or Theorem 5.3.5, we have to compute the values $w_{P_j, e_j, a_j}(z_\kappa b)$, for all $1 \leq \kappa, j \leq s$ and $b \in \mathcal{B}_\kappa$. That is, we need to determine the values $v_{P_\kappa}(\Phi_j(\theta))$ and $v_{P_j}(b)$, for $1 \leq \kappa, j \leq s$ and all $b \in \mathcal{B}_\kappa$. In [9, Proposition 4.7] concrete formulas can be found, which only depend on the data computed along Algorithm 1. Hence, these values can be computed as a by-product at cost zero. Thus, the cost of the determination of the integers ϵ_j and the precision of the approximations Φ_j can be neglected.

Remark 5.3.6. *Let $\mathbb{P}_\infty(F) = \{P_1, \ldots, P_s\}$. If we call Algorithm 8 for f_∞, t^{-1}, and the fractional ideal $I_\infty = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_s^{a_s}$ of $\mathcal{O}_{F,\infty}$, we obtain a t^{-1}-integral basis $\mathcal{B}$ of I_∞. We consider the t^{-1}-norm*

$$w_{I_\infty} := \min_{1 \le i \le s} \left\{ \frac{v_{P_i}(\ ) - a_i}{e(P_i/P_\infty)} \right\}.$$

As mentioned before $\mathcal{B}$ is an A_∞-basis of I_∞. Let D be a divisor of F/k and $-v_{P_i}(D) = a_i$, for $1 \le i \le s$. Then, $\| \ \|_D = -w_{I_\infty}$. In particular, a w_{I_∞}-orthonormal basis of I_∞ is a $\| \ \|_D$-orthonormal basis of F. Hence, Algorithm 8 determines, if red = TRUE*, an orthonormal basis of the normed space $(F, \| \ \|_D)$. If* red $\neq$ TRUE *the latter algorithm determines a semi-orthonormal basis of $(F, \| \ \|_D)$.*

Complexity

For a fractional ideal I of $\mathcal{O}_F$ or $\mathcal{O}_{F,\infty}$ let I^* be as in (1.1). Recall that $\delta_p = v_p(\mathrm{disc} f)$ and $\delta_\infty = v_\infty(\mathrm{disc} f_\infty)$.

Definition 5.3.7. *For a fractional ideal I of $\mathcal{O}_F$ and an irreducible polynomial $p(t) \in A$, we define*

$$h_p(I) := v_p([I^* : A[\theta]]), \quad H_p(I) := v_p([I^* : \mathcal{O}_F]) + \delta_p.$$

Recall that for a fractional I_∞ of $\mathcal{O}_{F,\infty}$ it holds $h(I_\infty) \le H(I_\infty) = -|[I_\infty^* : \mathcal{O}_{F,\infty}]| + \delta_\infty$. Clearly, $h_p(I) \le H_p(I)$, as $\delta_p \ge 0$.

We analyze the complexity of Algorithm 8 step by step and admit fast multiplication techniques of Schönhage-Strassen [34]. Let R be a ring and let $g_1, g_2 \in R[x]$ be two polynomials, whose degrees are bounded by d_1 and d_2, respectively. Then, the multiplication $g_1 \cdot g_2$ needs at most $O(\max\{d_1, d_2\}^{1+\epsilon})$ operations in R. For the subsequent complexity analysis we assume that the field k is finite with q elements.

Step 1, Montes algorithm

According to [1, Theorem 5.14] the complexity of calling Algorithm $1(f, p(t))$ is

$$C_1 = O((\deg p(t))^{1+\epsilon}(n^{2+\epsilon} + n^{1+\epsilon}\delta_p \log(q^{\deg p(t)}) + n^{1+\epsilon}\delta_p^{2+\epsilon}))$$

operations in k.

Step 2, Computation of $\mathcal{B}_i$'s

We fix $i \in \{1, \ldots, s\}$ and set $\mathfrak{p} := \mathfrak{p}_i$. It holds $\mathcal{B}_i = \mathcal{B}_\mathfrak{p}(\theta)$, where $\mathcal{B}_\mathfrak{p} = \{1, \ldots, g_{n_\mathfrak{p}-1}(x)\}$

is a set of divisor polynomials as defined in Definition 1.4.11. For $0 \leq m < n_{\mathfrak{p}}$ the degree of g_m is $m < n_{\mathfrak{p}}$ and it holds

$$g_m(x) = \prod_{i=0}^{r} \phi_{\mathfrak{p},i}(x)^{c_i},$$

where $\phi_{\mathfrak{p},0} = x$, the polynomials $\phi_{\mathfrak{p},1}, \ldots, \phi_{\mathfrak{p},r} \in A[x]$ are taken from an optimal type $\mathbf{t}$ of order r corresponding to the irreducible factor $f_{\mathfrak{p}}$ of f in $\hat{A}_p[x]$, and the exponents $c_i \in \mathbb{Z}_{\geq 0}$ are defined in Theorem 1.4.10. We denote by m_j the degree of the polynomial $\phi_{\mathfrak{p},j}$, for $0 \leq j \leq r$. According to Subsection 1.4.1 we have $m_{r+1} = \deg \phi_{\mathfrak{p}} = n_{\mathfrak{p}}$. Since $\mathbf{t}$ is optimal, it holds $2m_j \leq m_{j+1}$, for $1 \leq j < r$ (cf. Definition 1.4.1 and (1.4)).

Lemma 5.3.8.

1. *For $0 \leq j \leq r$ the computation of $\phi_{\mathfrak{p},j}^{c_j}$ needs at most $O(m_{j+1}^{1+\epsilon})$ operations in A.*
2. *The computation of g_m can be realized with at most $O(n_{\mathfrak{p}}^{1+\epsilon})$ operations in A.*

Proof. For convenience, we assume that c_j is divisible by 2. The computation of $\phi_{\mathfrak{p},j}^{c_j} \in A[x]$ has a cost of $O\big(\sum_{j=1}^{\log c_j} (2^j n)^{1+\epsilon}\big)$ operations in A, if we use the brute procedure:

$$\begin{array}{cc} \phi_{\mathfrak{p},j}^2 & O(m_j^{1+\epsilon}) \\ (\phi_{\mathfrak{p},j}^2)^2 & O((2m_j)^{1+\epsilon}) \\ \vdots & \vdots \\ \big(\phi_{\mathfrak{p},j}^{c_j/2}\big)^2 & O((c_j m_j/2)^{1+\epsilon}) \end{array}$$

The sum of all these costs is bounded by

$$O\Big(\sum_{i=0}^{\log c_j} (2^i m_j)^{1+\epsilon}\Big) = O\Big(m_j^{1+\epsilon} \sum_{i=0}^{\log c_j} (2^i)^{1+\epsilon}\Big) = O((m_j c_j)^{1+\epsilon}).$$

According to Theorem 1.4.10 we have $c_j < m_{j+1}/m_j$, for $0 \leq j \leq r$; hence, the cost of the computation of $\phi_{\mathfrak{p},j}^{c_j}$ can be estimated by $O(m_{j+1}^{1+\epsilon})$ operations in A.

In order to estimate the complexity of the computation of g_m we fix $1 \leq j \leq r$ and assume that $h := \prod_{i=0}^{j-1} \phi_{\mathfrak{p},i}(x)^{c_i}$ and $\phi_{\mathfrak{p},j}(x)^{c_j}$ have already been computed. The cost of the realization of the product $h\phi_{\mathfrak{p},j}(x)^{c_j}$ is

$$O(\max\{\deg h, m_j c_j\}^{1+\epsilon}) = O(\max\{\deg h, m_{j+1}\}^{1+\epsilon}) \tag{5.10}$$

operations in A, since $c_j < m_{j+1}/m_j$. Moreover, we deduce $\deg h = \sum_{i=0}^{j-1} m_j c_j < \sum_{i=0}^{j-1} m_{j+1}$. As $2m_j \leq m_{j+1}$, for $1 \leq j < r$ we obtain

$$m_1 + \cdots + m_j \leq \frac{m_j}{2^{j-1}} + \frac{m_j}{2^{j-2}} + \cdots + \frac{m_j}{2} + m_j = O(m_j), \quad \text{for } 1 \leq j \leq r. \tag{5.11}$$

For $j = r+1$ we deduce $m_1 + \cdots + m_{r+1} = O(m_r + m_{r+1}) = O(m_{r+1})$, as $m_r < m_{r+1}$. By (5.10) and (5.11) we can estimate the cost of the multiplication $h\phi_{\mathfrak{p},j}(x)^{c_j}$ with $O(m_{j+1}^{1+\epsilon})$ operatons in A.

Then, the cost of the computation of the product $g_m = \prod_{i=0}^{r} \phi_{\mathfrak{p},i}(x)^{c_i}$ is equal to $O\big(\sum_{j=0}^{r} 2m_{j+1}^{1+\epsilon}\big)$ by item *1.* Since $m_{r+1} = n_{\mathfrak{p}}$ and by (5.11) we deduce $O\big(\sum_{j=0}^{r} m_{j+1}^{1+\epsilon}\big) = O(n_{\mathfrak{p}}^{1+\epsilon})$. This ends the proof. □

By the last lemma, the cost for determining $\mathcal{B}_{\mathfrak{p}}$ is equal to $O(\sum_{i=0}^{n_{\mathfrak{p}}-1} n_{\mathfrak{p}}^{1+\epsilon}) = O(n_{\mathfrak{p}}^{2+\epsilon})$ multiplications in A. In [1] it is shown that the degree of the coefficients of any g_m in $\mathcal{B}_{\mathfrak{p}}$ is less than or equal to $\deg p(t)\delta_p$. Thus, the cost of the computation of $\mathcal{B}_{\mathfrak{p}}$ can be estimated by

$$O(n_{\mathfrak{p}}^{2+\epsilon}(\deg p(t)\delta_p)^{1+\epsilon})$$

operations in k. As $\sum_{i=1}^{s} n_{\mathfrak{p}_i} = n$, the computation of all sets $\mathcal{B}_i$ can be realized by

$$C_2 := O\left(\sum_{i=1}^{s} n_{\mathfrak{p}}^{2+\epsilon}(\deg p(t)\delta_p)^{1+\epsilon}\right) = O(n^{2+\epsilon}(\deg p(t)\delta_p)^{1+\epsilon})$$

operations in k.

Step 3, Determining the Φ_i's

According to [1, Theorem 5.16], the cost of the computation of an Okutsu approximation Φ_i with precision ν at P_i; that is, $v_{P_i}(\Phi_i(\theta))/e_i \geq \nu$, is given by

$$O((\deg p(t))^{1+\epsilon}(nn_{\mathfrak{p}_i}\nu^{1+\epsilon} + n\delta_p^{1+\epsilon}))$$

operations in k.

The following technical lemmas provide concrete bounds for the precision ν of the Okutsu approximation Φ_i, for $1 \leq i \leq s$, which is sufficient in order to determine a $p(t)$-integral basis with Algorithm 5.3.5.

In the following observation we assume that the multipliers z_κ are given by

$$z_\kappa = \prod_{\substack{j=1 \\ j\neq\kappa}}^{s} \Phi_j^{\epsilon_j}(\theta), \quad \text{all } \epsilon_j = 1.$$

Although in practice many of the exponents ϵ_j are equal zero, for the complexity estimation we consider the worst case $\epsilon_j = 1$, for $j \neq \kappa$.

Lemma 5.3.9. *For $1 \leq i \leq s$, let $\mathcal{B}_i = \{b_{i,j} \mid 0 \leq j \leq n_{\mathfrak{p}_i} - 1\}$ and Φ_i such that*

$$v_{P_i}(\Phi_i(\theta))/e_i \geq \max\Big\{ \max_{1\leq\kappa<i\leq s}\{H_{i,\kappa}\}, \max_{1\leq i<\kappa\leq s}\{H_{i,\kappa}\}+1\Big\}, \tag{5.12}$$

where

$$H_{i,\kappa} := \max_{0\leq l<n_{\mathfrak{p}_\kappa}} \Big\{ w_{P_\kappa,e_\kappa,a_\kappa}\Big(b_{\kappa,l}\prod_{\substack{j=1\\ j\neq\kappa}}^{s}\Phi_j(\theta)\Big) - w_{P_i,e_i,a_i}\Big(b_{\kappa,l}\prod_{\substack{j=1\\ j\neq\kappa,i}}^{s}\Phi_j(\theta)\Big)\Big\}.$$

Then, $\{b_1,\ldots,b_n\} = \bigcup_{\kappa=1}^{s} z_i\mathcal{B}_\kappa$, with $z_\kappa := \phi_1(\theta)\cdots\phi_{\kappa-1}(\theta)\cdot\phi_{\kappa+1}(\theta)\cdots\phi_s(\theta)$ is w_{I_p}-semi-reduced. In particular, the family

$$\frac{b_i}{p(t)^{\lfloor w(b_i)_{I_p}\rfloor}}, \quad 1\leq i\leq n$$

is a $p(t)$-integral basis of I.

Proof. We show that the conditions on the Φ_i can be translated to the following statement: For $1\leq\kappa\leq s$ and for $0\leq l<n_{\mathfrak{p}_\kappa}$ it holds

1. $w_{P_\kappa,e_\kappa,a_\kappa}(z_\kappa b_{\kappa,l}) \leq w_{P_i,e_i,a_i}(z_\kappa b_{\kappa,l})$ for $1\leq\kappa<i\leq s$ and
2. $w_{P_\kappa,e_\kappa,a_\kappa}(z_\kappa b_{\kappa,l}) \leq w_{P_i,e_i,a_i}(z_\kappa b_{\kappa,l}) - 1$ for $1\leq i<\kappa\leq s$.

Then, the statement of the lemma follows from Theorem 5.3.4.

By (5.2), the inequality $v_{P_i}(\Phi_i(\theta))/e_i \geq H_{i,\kappa}$, for $\kappa<i$, implies that, for $0\leq l<n_{\mathfrak{p}_\kappa}$,

$$\begin{aligned} v_{P_i}(\Phi_i(\theta))/e_i &\geq w_{P_\kappa,e_\kappa,a_\kappa}\Big(b_{\kappa,l}\prod_{\substack{j=1\\ j\neq\kappa}}^{s}\Phi_j(\theta)\Big) - w_{P_i,e_i,a_i}\Big(b_{\kappa,l}\prod_{\substack{j=1\\ j\neq\kappa,i}}^{s}\Phi_j(\theta)\Big)\\ \iff w_{P_i,e_i,a_i}\Big(b_{\kappa,l}\prod_{\substack{j=1\\ j\neq\kappa}}^{s}\Phi_j(\theta)\Big) &\geq w_{P_\kappa,e_\kappa,a_\kappa}\Big(b_{\kappa,l}\prod_{\substack{j=1\\ j\neq\kappa}}^{s}\Phi_j(\theta)\Big), \end{aligned}$$

which proves the first item. Analogously, the inequality $v_{P_i}(\Phi_i(\theta))/e_i \geq H_{i,\kappa}+1$, for $\kappa>i$, implies the second item. □

Analogously to the last proof one can show with Theorem 5.3.5 the following statement.

Corollary 5.3.10. *If we require*

$$v_{P_i}(\Phi_i(\theta))/e_i > \max_{1\leq\kappa\leq s}\{H_{i,\kappa} \mid \kappa\neq i\},$$

for $1\leq i\leq s$, instead of (5.12), then the $p(t)$-integral basis from the last lemma is w_{I_p}-orthonormal.

By Lemma 5.3.9 we deduce a lower bound for the precision of the approximations Φ_i, for $1 \leq i \leq s$.

Lemma 5.3.11. *For $i \neq \kappa$ and $1 \leq i, \kappa \leq s$ we have*

$$H_{i,\kappa} = O(H_p(I)).$$

Proof. We keep the notation from Lemma 5.3.9. For $1 \leq \kappa, j \leq s$ and $0 \leq l < n_{\mathfrak{p}_\kappa}$ it holds $b_{\kappa,l},\ \Phi_i(\theta) \in \mathcal{O}_F$. Hence, for $0 \leq l < n_{\mathfrak{p}_\kappa}$, we obtain

$$\begin{aligned} & w_{P_\kappa,e_\kappa,a_\kappa}(b_{\kappa,l}z_\kappa) - w_{P_i,e_i,a_i}\Big(b_{\kappa,l} \prod_{\substack{j=1 \\ j\neq\kappa,i}}^{s} \Phi_j(\theta)\Big) \\ = {} & w_{P_\kappa,e_\kappa,0}(b_{\kappa,l}z_\kappa) - w_{P_i,e_i,0}\Big(b_{\kappa,l} \prod_{\substack{j=1 \\ j\neq\kappa,i}}^{s} \Phi_j(\theta)\Big) - \frac{a_\kappa}{e_\kappa} + \frac{a_i}{e_i} \\ \leq {} & w_{P_\kappa,e_\kappa,0}(b_{\kappa,l}z_\kappa) - \frac{a_\kappa}{e_\kappa} + \frac{a_i}{e_i}. \end{aligned}$$

Clearly, $-a_\kappa/e_\kappa + a_i/e_i \leq h_p(I)$ by the definition of h_p.

We estimate $w_{P_\kappa,e_\kappa,0}(b_{\kappa,l}z_\kappa)$. By definition, the elements $b_{\kappa,l} \in \mathcal{B}_\kappa$ are given by $b_{\kappa,l} = g_{\kappa,l}(\theta)$ with $g_{\kappa,l}(x) \in A[x]$ monic of degree $m < n_{\mathfrak{p}_\kappa}$. In [1, Proposition 1.3] it is shown that all monic polynomials $g \in A[x]$ of degree less than $n_{\mathfrak{p}_\kappa}$ satisfy $v_{P_\kappa}(g(\theta))/e_\kappa \leq \mu := \mu(f_{\mathfrak{p}_\kappa})$ for a certain constant μ which satisfies $\mu \leq \delta_p/n_{\mathfrak{p}_\kappa}$. Hence, $w_{P_\kappa,e_\kappa,0}(b_{\kappa,l}) \leq \delta_p/n_{\mathfrak{p}_\kappa}$, for all $0 \leq l < n_{\mathfrak{p}_\kappa}$.

We consider $w_{P_\kappa,e_\kappa,0}(z_\kappa) = \sum_{j=1,j\neq\kappa}^{s} v_{P_\kappa}(\Phi_j(\theta))/e_\kappa$. Let $f_{\mathfrak{p}_1}, \ldots, f_{\mathfrak{p}_s}$ be the irreducible factors of the defining polynomial f in $\hat{A}_p[x]$. As in (5.3), we identify the completion of F at P_κ with $K_p(\theta_{\mathfrak{p}_\kappa})$, for $1 \leq \kappa \leq s$, where $\theta_{\mathfrak{p}_\kappa}$ denotes a root of the irreducible factor $f_{\mathfrak{p}_\kappa}$. Let $\hat{v}$ be the extension of v_p to the algebraic closure of K_p.

Claim: It holds $v_{P_\kappa}(\Phi_j(\theta))/e_\kappa = \hat{v}(\Phi_j(\theta_{\mathfrak{p}_\kappa})) = \hat{v}(\mathrm{Res}(f_{\mathfrak{p}_j}, f_{\mathfrak{p}_\kappa}))/\deg f_{\mathfrak{p}_\kappa}$.

After the claim, the statement of the lemma follows immediately. In fact, since

$$\delta_p = \sum_{i=1}^{s} v_p(\mathrm{disc}(f_{\mathfrak{p}_i})) + 2 \sum_{1\leq i<j\leq s} v_p(\mathrm{Res}(f_{\mathfrak{p}_i}, f_{\mathfrak{p}_j}))$$

[32, III.§2-4], we deduce $w_{P_\kappa,e_\kappa,0}(z_\kappa) \leq \delta_p$. Together with the previous estimations, we obtain $H_{i,\kappa} = O(H_p(I))$, for $i \neq \kappa$ and $1 \leq i, \kappa \leq s$, since $h_p(I) + \delta_p = O(H_p(I))$.

In order to prove the claim we consider Z the set of roots of $f_{\mathfrak{p}_\kappa}$. Since $f_{\mathfrak{p}_\kappa}, f_{\mathfrak{p}_j} \in \hat{A}_p[x]$ are irreducible, $\hat{v}$ is constant on $f_{\mathfrak{p}_j}(Z)$. As

$$\hat{v}(\mathrm{Res}(f_{\mathfrak{p}_j}, f_{\mathfrak{p}_\kappa})) = \hat{v}\Big(\prod_{\alpha\in Z} f_{\mathfrak{p}_j}(\alpha)\Big),$$

we obtain $\hat{v}(\mathrm{Res}(f_{\mathfrak{p}_j}, f_{\mathfrak{p}_\kappa})) = \deg f_{\mathfrak{p}_\kappa} \hat{v}(f_{\mathfrak{p}_j}(\theta_{\mathfrak{p}_\kappa}))$. In [9, Prop. 7.4] there is a closed formula for $\hat{v}(\Phi_j(\theta_{\mathfrak{p}_\kappa}))$ which is valid for any Okutsu approximation Φ_j of $f_{\mathfrak{p}_j}$; in particular, $\hat{v}(\Phi_j(\theta_{\mathfrak{p}_\kappa})) = \hat{v}(f_{\mathfrak{p}_j}(\theta_{\mathfrak{p}_\kappa}))$. This ends the proof of the claim.

□

According to the last lemma, we compute in Algorithm 8 approximations Φ_i with a precision $\nu = O(H_p(I))$ at cost of

$$O((\deg p(t))^{1+\epsilon}(n n_{\mathfrak{p}_i} H_p(I)^{1+\epsilon} + n\delta_p^{1+\epsilon}))$$

operations in k. In the worst case we have to determine all approximations Φ_i with that precision. As $\sum_{i=1}^{s} n_{\mathfrak{p}_i} = n$ and $s \leq n$, the cost of computing the adequate approximations can be estimated by

$$\begin{aligned} C_3 :&= O\Big(\sum_{i=1}^{s} (\deg p(t))^{1+\epsilon}(n n_{\mathfrak{p}_i} H_p(I)^{1+\epsilon} + n\delta_p^{1+\epsilon})\Big) \\ &= O((\deg p(t))^{1+\epsilon} n^2 (H_p(I)^{1+\epsilon} + \delta_p^{1+\epsilon})) = O(n^2((\deg p(t)) H_p(I))^{1+\epsilon}) \end{aligned}$$

operations in k.

Step 4, Determining $z_\kappa \mathcal{B}_\kappa$

We have to multiply the elements b_{κ,j_κ}, $0 \leq j_\kappa < n_{\mathfrak{p}_\kappa}$, of $\mathcal{B}_\kappa$ with the multiplier z_κ. As mentioned before, the worst case occurs if any multiplier z_κ is given by

$$z_\kappa = \prod_{\substack{j=1 \\ j \neq \kappa}}^{s} \Phi_j(\theta).$$

Lemma 5.3.12. *Let $s \geq 2$. The multipliers $z_1, \ldots, z_s$ can be determined by $2(s-3)+s$ multiplications in $A[x]$.*

Proof. Initially we compute the products

$$\Phi_1\Phi_2, \Phi_1\Phi_2\Phi_3, \ldots, \Phi_1 \cdots \Phi_{s-2} \text{ and} \tag{5.13}$$

$$\Phi_{s-1}\Phi_s, \Phi_{s-2}\Phi_{s-1}\Phi_s, \ldots, \Phi_3 \cdots \Phi_s. \tag{5.14}$$

This can be realized by $2(s-3)$ multiplications. Every z_i can be written as a product of one element in the list (5.13) and one element in the list (5.14). Hence, to determine the multipliers $z_1, \ldots, z_s$ we have to apply exactly s additional multiplications. □

The complexity of any multiplication in the realization of the multipliers can be estimated by $O(n^{1+\epsilon})$ operations in A, since the degree of any product of approximations in (5.13) and (5.14) is less than n, for $1 \leq i \leq s$. As $s \leq n$, the complexity of the computation of $z_1, \ldots, z_s$ is equal to $O(sn^{1+\epsilon}) = O(n^{2+\epsilon})$ operations in A.

After all, we determine the products $z_\kappa b_{\kappa,j}$, for $1 \leq \kappa \leq s$ and $0 \leq j < n_{\mathfrak{p}_\kappa}$. Any $b_{\kappa,j}$ is given by $b_{\kappa,j} = g_{\kappa,j}(\theta)$, where $g_{\kappa,j}(x)$ is a monic polynomial in $A[x]$ of degree $j < n_{\mathfrak{p}_\kappa}$. For $1 \leq \kappa \leq s$, the multiplier z_κ is given by a polynomial in $A[x]$ of degree less than $n - n_{\mathfrak{p}_\kappa}$ evaluated in θ. As $\sum_{i=1}^{s} n_{\mathfrak{p}_i} = n$, the computation of $z_\kappa b_{\kappa,j}$ can be realized at cost of $O(n^{1+\epsilon})$ operations in A. In particular, we can compute all sets $z_\kappa \mathcal{B}_\kappa$ at the cost of $O(n^{2+\epsilon})$ operations in A.

Analogously to the proof of Lemma 5.3.11 one can show that $w_{P_i,e_i,a_i}(z_\kappa b_{\kappa,j}) = O(H_p(I))$ for $1 \leq i \leq s$ and $0 \leq j < n_{\mathfrak{p}_\kappa}$; hence, $w_{I_p}(z_\kappa b_{\kappa,j}) = O(H_p(I))$. Then, we can realize all the multiplications modulo $p(t)^\nu$ with $\nu = O(H_p(I))$ (cf. Lemma 5.3.17). Therefore, we can determine $z_\kappa \mathcal{B}_\kappa$, for $1 \leq \kappa \leq s$ with

$$C_4 := O(n^{2+\epsilon}(\deg(p(t))H_p(I))^{1+\epsilon})$$

operations in k.

Total cost:

Clearly, the cost of the normalization in the last step of Algorithm 8 can be neglected. Since C_2 and C_3 are dominated by C_4, we estimate the total cost of Algorithm 8 by $O(C_1 + C_4)$ operations in k.

Theorem 5.3.13. *Algorithm 8 needs at most*

$$O((\deg p(t))^{1+\epsilon}(n^{2+\epsilon}H_p(I)^{1+\epsilon} + n^{1+\epsilon}\delta_p \log(q^{\deg p(t)}) + n^{1+\epsilon}\delta_p^{2+\epsilon}))$$

arithmetic operations in k to determine a w_{I_p}-orthonormal basis of I. Moreover, the cost of computing a $p(t)$-integral Hermite basis of I is bounded by

$$O((\deg p(t))^{1+\epsilon}(n^3H_p(I)^2 + n^{1+\epsilon}\delta_p \log(q^{\deg p(t)}) + n^{1+\epsilon}\delta_p^{2+\epsilon}))$$

operations in k.

Proof. The first statement follows from the above considerations. In order to transform the basis $\mathcal{B} := (b_i/p(t)^{\lfloor w_{I_p}(b_i) \rfloor})_{1 \leq i \leq n}$, determined by Algorithm 8, into a Hermite basis, we only have to transform the matrix gM into HNF, where M is the transition matrix

from $(1, \theta, \ldots, \theta^{n-1})$ to $\mathcal{B}$ and g is the denominator of maximal degree in M. As mentioned above the coefficients of the b_i have degree equal to $O(H_p(I))$. Moreover, according to the proof of Lemma 5.3.11 one can deduce $w_{P_\kappa,e_\kappa,a_\kappa}(b_i) = O(H_p(I))$, for $1 \leq \kappa \leq s$ and $1 \leq i \leq n$. Hence, $w_{I_p}(b_i) = \min_{1\leq\kappa\leq s}\{w_{P_\kappa,e_\kappa,a_\kappa}(b_i)\} = O(H_p(I))$, and in particular the polynomial entries of gM have degree equal to $O(H_p(I))$. Then, by [24, Theorem 4.1] transforming gM into HNF can be realized with $O(n^3(H_p(I))^2)$ operations in k. This results in the second bound of the theorem. □

As mentioned in Remark 5.3.6 we can adopt Algorithm 8 for the computation of an (w_{I_∞}-orthonormal) A_∞-basis of a fractional ideal I_∞ of $\mathcal{O}_{F,\infty}$. Analogously to the last theorem one can deduce the following statement.

Corollary 5.3.14. *Algorithm 8 needs at most*

$$O(n^{2+\epsilon}H(I_\infty)^{1+\epsilon} + n^{1+\epsilon}\delta_\infty \log(q) + n^{1+\epsilon}\delta_\infty^{2+\epsilon})$$

arithmetic operations in k to determine a w_{I_∞}-orthonormal basis of I_∞. Moreover, the cost of computing a A_∞-Hermite basis of I_∞ is bounded by

$$O(n^3H(I_\infty)^2 + n^{1+\epsilon}\delta_\infty \log(q) + n^{1+\epsilon}\delta_\infty^{2+\epsilon})$$

operations in k.

At the end of this subsection we consider an alternative way of computing the multipliers z_κ, for $1 \leq \kappa \leq s$, in Algorithm 8. Although the complexity of the computation of the z_κ plays a minor role in the runtime of Algorithm 8, the computation of the Okutsu approximations Φ_j up to a certain precision has an important impact on the practical performance of the computation of a $p(t)$-integral basis.

According to Theorem 5.3.4 and Theorem 5.3.5 we have to construct elements z_κ with "large" valuation at P_j, for $j \in \{1, \ldots, s\} \setminus \{\kappa\}$, and "small" valuation at P_κ. In [9] a method is described, which produces elements $c_{P_i} \in F$, for $1 \leq i \leq s$, such that

$$v_{P_i}(c_{P_i}) > 0, \qquad v_{P_j}(c_{P_i}) = 0, \text{ for } j \neq i$$

as a by-product of the Montes algorithm. Then, for any $\kappa \in \{1, \ldots, s\}$, one can easily determine integers α_j, for $j \in \{1, \ldots, s\} \setminus \{\kappa\}$, so that

$$z_\kappa := \prod_{\substack{j=1 \\ j\neq\kappa}}^{s} c_{P_j}^{\alpha_j}$$

satisfies the conditions from Theorem 5.3.4 and Theorem 5.3.5, respectively. Note that $c_{P_j}^{\alpha_j}$ can be determined modulo $p(t)^\nu$ with $\nu = O(H_p(I))$. Hence, the computation of the multipliers z_κ is in practice extremely fast. On the other hand, by this choice of multipliers the resulting basis is far away from being triangular. Thus, the computation of an Hermite basis has a relatively high cost. This method may be applied for function fields of small degree and a fractional ideal I with large $H_p(I)$.

5.3.2 Computation of global integral bases

In the last subsection we presented an algorithm, which computes a $p(t)$-integral basis of an ideal I of $\mathcal{O}_F$ for a monic irreducible polynomial $p(t) \in A$. In the sequel we describe a method, which determines a global basis (i.e. an A-basis) of I by merging finitely many "local" bases. Recall that for any fractional ideal $I = \prod_{\mathfrak{p}\in \mathrm{Max}(\mathcal{O}_F)} \mathfrak{p}^{a_\mathfrak{p}}$, we denote $I_p := \prod_{\mathfrak{p}|p} \mathfrak{p}^{a_\mathfrak{p}}$.

A direct consequence of Theorem 5.3.3 is the following statement.

Theorem 5.3.15. *Let $\mathcal{B} \subset F$ be a set with n elements. Then, $\mathcal{B}$ is an A-basis of the ideal I if and only if $\mathcal{B}$ is w_{I_p}-semi-orthonormal, for all monic irreducible polynomials $p(t) \in A$.*

Lemma 5.3.16. *Let $p_1(t), \ldots, p_\kappa(t) \in A$ be all monic irreducible polynomials such that $v_{p_i}([I : A[\theta]]) \neq 0$. Denote by $\mathcal{B} = (b_0, \ldots, b_{n-1}) \subset F$ a family, which is $w_{I_{p_i}}$-semi-orthonormal, for all $1 \leq i \leq \kappa$ and whose elements are of the following form:*

$$b_l = \frac{g_l(\theta)}{\prod_{j=1}^{\kappa} p_j^{\alpha_{j,l}}}, \qquad \text{for } 0 \leq l < n \text{ and } \alpha_{j,l} \in \mathbb{Z},$$

where $g_l(x) \in A[x]$ monic and of degree l. Then, $\mathcal{B}$ is an A-basis of I.

Proof. Since the denominators of the b_l are the irreducible polynomials $p_1(t), \ldots, p_\kappa(t)$ and $\mathcal{B}$ is $w_{I_{p_i}}$-semi-orthonormal, for all $1 \leq i \leq \kappa$, we have $\mathcal{B} \subset I$. In particular, $\mathcal{B}$ is a $p_i(t)$-integral basis of I, for all $1 \leq i \leq \kappa$, by Theorem 5.3.3. Hence, we obtain $v_{p_i}([I : \left\langle \mathcal{B} \right\rangle_A]) = 0$, for all i. As the g_l are monic of degree l, it holds $[I : \langle \mathcal{B} \rangle_A] = A$ and therefore $\langle \mathcal{B} \rangle_A = I$ by Lemma 1.2.3. □

According to the last lemma, in order to determine an A-basis of a fractional ideal I we have to construct a triangular basis with monic numerators, which is "locally" semi-orthonormal, for any irreducible polynomial $p(t) \in A$ with $v_p([I : A[\theta]]) \neq 0$. This can be realized by an easy application of the CRT. To this end, the next lemma will

be helpful. For a monic irreducible polynomial $p(t) \in A$ and $I_p = \prod_{\mathfrak{p}|p} \mathfrak{p}^{a_\mathfrak{p}}$ we set for convenience $\operatorname{sred}^r_{I_p} := \operatorname{sred}^r_{(e,a)}$, $r \in \mathbb{R}$, where $e := (e(P/P_p))_{P|P_p}$ and $a := (a_\mathfrak{p})_{\mathfrak{p}|p}$.

Lemma 5.3.17. *Let I be a fractional ideal of $\mathcal{O}_F$, $p(t)$ be a monic irreducible polynomial in A, and $b = \sum_{j=0}^{n-1} \lambda_j \theta^j \in A[\theta]$. Let $b' = \sum_{j=0}^{n-1} \lambda'_j \theta^j \in A[\theta]$ with*

$$\lambda'_j \equiv \lambda_j \bmod p(t)^\nu, \quad \nu > \lfloor w_{I_p}(b) \rfloor, \quad \text{for all } j.$$

Then, it holds

$$\operatorname{sred}_{I_p}^{w_{I_p}(b)}(b) = \operatorname{sred}_{I_p}^{w(b')_{I_p}}(b').$$

Proof. We write $b' = b + p(t)^\nu r(t,\theta)$ with $r(t,\theta) \in A[\theta]$. Since $\lfloor w_{I_p}(p(t)^\nu r(t,\theta)) \rfloor = \lfloor \nu + w_{I_p}(r(t,\theta)) \rfloor > \lfloor w_{I_p}(b) \rfloor$, we have $w_{I_p}(b) = w_{I_p}(b')$. Then, the statement follows from Lemma 5.2.5. □

Now we are able to describe a method that allows us to construct a global basis of a fractional ideal I from the local bases of I.

Let $p_1, \ldots, p_\kappa$ be all monic irreducible polynomials in A with $v_{p_i}([I : A[\theta]]) \neq 0$ and denote, for $1 \leq i \leq \kappa$, by $\mathcal{B}_i = (b_{i,0}, \ldots b_{i,n-1})$ a $p_i(t)$-integral basis of I, where

$$b_{i,j} = \frac{g_{i,j}(t,\theta)}{p_i(t)^{\nu_{i,j}}}, \quad \nu_{i,j} := \lfloor w_{I_{p_i}}(g_{i,j}(t,\theta)) \rfloor \tag{5.15}$$

with $g_{i,j}(t,x) \in A[x]$ monic of degree j. For $j \in \{0, \ldots, n-1\}$ fixed, let $g_j(t,\theta) \in A[\theta]$ such that its coefficients coincide with the coefficients of $g_{i,j}(t,\theta)$ modulo $p_i(t)^{\beta_{i,j}}$, for $1 \leq i \leq \kappa$, where $\beta_{i,j} := \max\{\nu_{i,j}, 0\} + 1$. We set

$$b'_j := \frac{g_j(t,\theta)}{\prod_{i=1}^{\kappa} p_i(t)^{\nu_{i,j}}}. \tag{5.16}$$

Lemma 5.3.18. *The family $\mathcal{B}' := (b'_1, \ldots, b'_n)$ with b'_j defined in (5.16) is a $p_i(t)$-integral basis, for $1 \leq i \leq \kappa$.*

Proof. By Lemma 5.3.17 it holds

$$\operatorname{sred}_{I_{p_i}}^{w_{I_{p_i}}(g_j(t,\theta))}(g_j(t,\theta)) = \operatorname{sred}_{I_{p_i}}^{w_{I_{p_i}}(g_{i,j}(t,\theta))}(g_{i,j}(t,\theta))$$

and $w_{I_{p_i}}(g_j(t,\theta)) = w(g_{i,j}(t,\theta))_{I_{p_i}}$, for $1 \leq i \leq \kappa$. Then, according to Theorem 5.2.7 the family $\mathcal{B}'$ is $w_{I_{p_i}}$-semi-reduced, since $\mathcal{B}_i$ is $w_{I_{p_i}}$-semi-reduced, for $1 \leq i \leq \kappa$. Hence, $\mathcal{B}'$ is $w_{I_{p_i}}$-semi-orthonormal and a $p_i(t)$-integral basis of I by Theorem 5.3.3. □

By construction $\mathcal{B}' = (b'_1, \ldots, b'_n)$ is triangular with $b'_j = g_j(t,\theta)/\prod_{i=1}^{\kappa} p_i(t)^{\nu_{i,j}}$, where $g_j(x) \in A[x]$ is monic for $1 \leq j \leq n$; hence Lemmas 5.3.16 and 5.3.18 show that $\mathcal{B}'$ is an A-basis of I.

We summarize the procedure by the following pseudo code.

Algorithm 9: Computation of an A-basis

Input: Defining polynomial f of degree n of a function field F/k and a fractional ideal I of $\mathcal{O}_F$.

Output: An Hermite A-basis of I.

1: fac $\leftarrow$ list of all monic irreducible polynomials $p(t) \in A$ with $v_p([I : \mathcal{O}_F]) \neq 0$ or $v_p(\mathrm{disc} f) > 1$
2: **for** $p_i(t)$ in fac **do**
3: $\quad \widetilde{\mathcal{B}}_i \leftarrow$Algorithm 8$(f, I, p_i(t), \mathrm{FALSE})$
4: $\quad \mathcal{B}_i \leftarrow$ transform $\widetilde{\mathcal{B}}_i$ into a triangular basis, whose vectors satisfy (5.15)
5: **end for**
6: **for** $j = 0, \ldots, n-1$ **do**
7: $\quad$ Determine b'_i as in (5.16)
8: **end for**
9: Transform $(b'_0, \ldots, b'_{n-1})$ into Hermite basis $(b_0, \ldots, b_{n-1})$
10: **return** $(b_0, \ldots, b_{n-1})$

Complexity

Recall that $H(I) = |[I^* : \mathcal{O}_F]| + \delta$, where I^* is defined as in (1.1). For the estimation of the complexity, we assume that the factorization of I into a product of nonzero prime ideals is known. In [12] a factorization algorithm can be found.

Theorem 5.3.19. *Let F/k be a function field of degree n over the finite field k with q elements. Then, a basis of a fractional ideal I can be computed with*

$$O(n^3 H(I)^2 + n^{1+\epsilon}\delta^{2+\epsilon} \log q)$$

operations in k.

Proof. Clearly, the complexity of Algorithm 9 is dominated by:

- Computation and the factorization of disc f (cf. line 1).
- Computation of the local bases $\mathcal{B}_i$ by Algorithm 8 and their "normalization" (cf. line 3 and 4).
- Transformation of $(b'_0, \dots, b'_{n-1})$ into a Hermite basis (cf. line 9).

In the proof of Theorem 4.2.4 we have seen that the computation and factorization of disc f can be realized with

$$O(n^3 + \delta^{2+\epsilon} + \delta^{1+\epsilon} \log q)$$

operations in k

Let $p_1(t), \dots, p_\kappa(t)$ be all monic irreducible polynomials in A with $v_{p_i}([I : \mathcal{O}_F]) \neq 0$ or $v_{p_i}(\operatorname{disc} f) \neq 0$. Clearly, the cost of the computation of a "normalized" $p_i(t)$-integral basis $\widetilde{\mathcal{B}}_i$ of I, coincides with the cost of the computation of a $p_i(t)$-integral Hermite basis of I. Then, by Theorem 5.3.13 the cost of the computation of all "normalized" $p_i(t)$-integral bases $\widetilde{\mathcal{B}}_i$ of I is given by

$$\begin{aligned} &O\Big(\sum_{i=1}^{\kappa} (\deg p_i(t))^{1+\epsilon} (n^3 H_{p_i}(I)^2 + n^{1+\epsilon} \delta_{p_i} \log(q^{\deg p_i(t)}) + n^{1+\epsilon} \delta_{p_i}^{2+\epsilon})\Big) \\ &= O(n^3 H(I)^2 + n^{1+\epsilon} \delta^{2+\epsilon} \log q) \end{aligned}$$

operations in k.

In order to determine $(b_0, \dots, b_{n-1})$ we have to transform gM into HNF, where M denotes the transition matrix from $(1, \dots, \theta^{n-1})$ to $(b'_0, \dots, b'_{n-1})$ and $g \in A$ the denominator of maximal degree in M. We show that the entries in gM have degree equal to $O(H(I))$.

In the proof of Theorem 5.3.13 we have seen that the elements $b_{i,j}$ in the $p_i(t)$-integral basis $\mathcal{B}_i$ are given by

$$b_{i,j} = \frac{g_{i,j}(t, \theta)}{p_i(t)^{\nu_{i,j}}},$$

where $\nu_{i,j} = O(H_{p_i}(I))$. By the construction of $\mathcal{B}'$ (cf. (5.16)) its elements are given by

$$b'_j = \frac{g_j(t, \theta)}{\prod_{i=1}^{\kappa} p_i(t)^{\nu_{i,j}}},$$

where the degree of the coefficients of $g_j(t, \theta)$ are bounded by $O(\sum_{i=1}^{\kappa} \deg p_i(t) H_{p_i}(I)) = O(H(I))$. The same holds for the denominator. Hence, the entries in gM have degree equal to $O(H(I))$. According to [24, Theorem 4.1] transforming gM into HNF can be realized in $O(n^3 (H(I))^2)$ operations in k.

Then, the complexity of the computation of an A-basis of I is dominated by $O(n^3(H(I))^2 + n^{1+\epsilon}\delta^{2+\epsilon}\log q)$. □

Theorem 5.3.20. *Let F/k be a function field with defining polynomial f of degree n and let $D = \sum_{P\in\mathbb{P}_F} a_P P$ be a divisor of F/k. Then, a k-basis of $\mathcal{L}(D)$ can be determined with*

$$O((n^5(h(D) + n^2C_f)^2 + n^{5+\epsilon}{C_f}^{2+\epsilon}\log q)$$

operations in k.

Proof. Let (I, I_∞) be the ideal representation of D. In order to determine a k-basis of $\mathcal{L}(D)$ we compute a Hermite basis $\mathcal{B}$ of I, a Hermite basis $\mathcal{B}'$ of I_∞, and apply Algorithm 6.

By Lemma 4.1.3 we have $\delta + \delta_\infty = O(n^2C_f)$. Moreover, Lemma 4.1.4 shows that $H(I) + H(I_\infty) = O(h(D) + n^2C_f)$. Then, by the last theorem and Corollary 5.3.14 the complexity of the computation of $\mathcal{B}$ and $\mathcal{B}'$ is given by

$$\begin{aligned}
&O(n^3(H(I))^2 + n^{1+\epsilon}\delta^{2+\epsilon}\log q + n^3H(I_\infty)^2 + n^{1+\epsilon}\delta_\infty\log q + n^{1+\epsilon}\delta_\infty^{2+\epsilon})\\
&= O(n^3(H(I) + H(I_\infty))^2 + n^{1+\epsilon}(\delta + \delta_\infty)^{2+\epsilon}\log q)\\
&= O(n^3(h(D) + n^2C_f)^2 + n^{5+\epsilon}{C_f}^{2+\epsilon}\log q)
\end{aligned}$$

operations in k.

Additionally, we run Algorithm 6, which needs $O(n^5(h(D) + n^2C_f)^2)$ operations in k by Corollary 4.1.5. Together we can estimate the computation of a k-basis of $\mathcal{L}(D)$ by

$$O((n^5(h(D) + n^2C_f)^2 + n^{5+\epsilon}{C_f}^{2+\epsilon}\log q))$$

operations in k. □

Note that the computation of the successive minima of D has the same complexity.

5.4 Basis computation of holomorphic rings

The concept of reduceness, introduced in Chapter 2, has another field of application. In this section we consider a method to determine a basis of certain holomorphic rings. The idea is an generalization and an improvement of the algorithm described in [22]. Moreover, we present a alternative reduceness-criterion, which allows us to apply the reduction algorithm in more general situations.

Let $\tau \in F \setminus k_0$ and $S := \mathrm{supp}((\tau)_\infty)$. For a divisor D of F/k we define

$$\mathcal{O}(D) := \{z \in F \mid v_P(z) \geq -v_P(D), \quad \text{for } P \in \mathbb{P}_F \setminus S\}.$$

Lemma 5.4.1. *The set $\mathcal{O}(D)$ is a free $k[\tau]$-module of rank $\deg(\tau)_\infty$.*

Proof. The fact that $\mathcal{O}(D)$ is a $k[\tau]$-module is obvious. We consider $F/k(\tau)$. Clearly, $[F : k(\tau)] = \deg(\tau)_\infty$ and $k(\tau)$ is the field of fractions of the principal domain $k[\tau]$. In particular, $k[\tau]$ is integrally closed. Since $\mathcal{O}(0) = \mathrm{Cl}(k[\tau], F)$, by [33, Theorem III. 3.4] the set $\mathcal{O}(0)$ is a free $k[\tau]$-module of rank $\deg(\tau)_\infty$. By the strong approximation theorem we can choose an element $z' \in F$ with $v_P(z') = v_P(D)$, for all $\mathbb{P}_F \setminus S$. Then,

$$z'\mathcal{O}(D) = \{z \in F \mid v_P(z) \geq 0, \quad \text{for } P \in \mathbb{P}_F \setminus S\} = \mathcal{O}(0).$$

Hence, $\mathcal{O}(D)$ is a free $k[\tau]$-module of rank $\deg(\tau)_\infty$. □

The aim of this section is to develop a method to determine a $k[\tau]$-basis of the module $\mathcal{O}(D)$. Denote henceforth $n := \deg(\tau)_\infty$ the degree of the extension $F/k(\tau)$. Let $(\tau)_\infty = \sum_{i=1}^{s} e_i P_i$ and $a_i := v_{P_i}(D)$, for $1 \leq i \leq s$. We set $e := (e_i)_{1 \leq i \leq s}$ and $a := (a_i)_{1 \leq i \leq s}$. We define the mapping

$$\| \ \| : F \to \mathbb{Q}, \quad \|z\| := -w_{e,a}(z),$$

where $w_{e,a}(z)$ is defined as in Definition 5.2.1.

One can easily see that $-\| \ \|$ is a τ-norm. Moreover, for $\tau = t$ the norm $\| \ \|$ coincides with the norm $\| \ \|_D$ induced by D defined in (4.1). Hence, we can consider $\| \ \|$ as a generalization of $\| \ \|_D$ and adopt all results from Section 4 to our situation. In fact, the following lemma can be proven exactly as Theorem 4.0.1.

Lemma 5.4.2. *For $D \in \mathcal{D}_F$ and $r \in \mathbb{Z}$ it holds*

1. *$\mathcal{L}(D + r(\tau)_\infty) = (\mathcal{O}(D), \| \ \|)_{\leq r}$ and*
2. *$(\mathcal{O}(D), \| \ \|)$ is a lattice in the normed space $(F, \| \ \|)$.*

The next theorem provides the theoretical foundation for the computation of a $k[\tau]$-basis of $\mathcal{O}(D)$.

Theorem 5.4.3. *Let $\mathcal{B}'$ be a k-basis of $\mathcal{L}(D + r(\tau)_\infty)$ with*

$$r \geq \frac{2[k_0 : k](g-1) + 1 - \deg D}{n} + 1. \tag{5.17}$$

Then, there exists $\mathcal{B} \subset \langle \mathcal{B}' \rangle_k$ such that $\mathcal{B}$ is a semi-reduced $k[\tau]$-basis of $(\mathcal{O}(D), \| \ \|)$.

Proof. Let $\mathcal{B} = (b_1, \ldots, b_n)$ be a semi-reduced basis of $(\mathcal{O}(D), \| \ \|)$. If $\|b_i\| \leq r$ for $1 \leq i \leq n$, then $\mathcal{B} \subset (\mathcal{O}(D), \| \ \|)_{\leq r} = \mathcal{L}(D + r(\tau)_\infty) = \langle \mathcal{B}' \rangle_k$ by the last lemma.

We have to show that $\|b_i\| \leq r$, for $1 \leq i \leq n$, and r as in (5.17). We fix

$$r' := \frac{2[k_0 : k](g-1) + 1 - \deg D}{n}.$$

Analogously to Corollary 4.0.2 one can show that

$$\dim(D + r'(\tau)_\infty) = \sum_{\lceil \|b_i\| \rceil \leq r'} (-\lceil \|b_i\| \rceil + r' + 1).$$

On the other hand, by the theorem of Riemann-Roch we obtain

$$\dim(D + r'(\tau)_\infty) = \deg D + r'n + [k_0 : k](1-g),$$

since $r' = (2[k_0 : k](g-1) + 1 - \deg D)/n$ and equivalently $\deg(D + t(\tau)_\infty) = \deg D + nr' = 2[k_0 : k](g-1) + 1$. Thus,

$$\sum_{\lceil \|b_i\| \rceil \leq r'} (-\lceil \|b_i\| \rceil + r' + 1) = \deg D + r'n + [k_0 : k](1-g). \tag{5.18}$$

Clearly, Corollary 4.2.1 can be adopted to this situation, that is $-|d(\mathcal{O}(D))| = \deg D + [k_0 : k](1-g) - n$. Then, Lemma 2.5.8 shows that $-\sum_{i=1}^n \lceil \|b_i\| \rceil + n = \deg D + [k_0 : k](1-g)$. Hence, (5.18) is equivalent to

$$\begin{aligned} \sum_{\lceil \|b_i\| \rceil \leq r'} (-\lceil \|b_i\| \rceil + r' + 1) = -\sum_{i=1}^n \lceil \|b_i\| \rceil + n + r'n = \sum_{i=1}^n (-\lceil \|b_i\| \rceil + r' + 1) \\ \iff 0 = \sum_{\lceil \|b_i\| \rceil > r'} (-\lceil \|b_i\| \rceil + r' + 1). \end{aligned}$$

This implies that $\lceil \|b_i\| \rceil = r' + 1$, for all i with $\lceil \|b_i\| \rceil > r'$, and therefore $\|b_i\| \leq r' + 1$, for $1 \leq i \leq n$. Thus, for $r \geq r' + 1 = (2[k_0 : k](g-1) + 1 - \deg D)/n + 1$, it holds $\|b_i\| \leq r$, for $1 \leq i \leq n$. □

By the last theorem we only need to determine a semi-reduced basis in the k-vector space $\mathcal{L}(D + r(\tau)_\infty)$, where r satisfies (5.17). In particular, a k-basis $\mathcal{B}'$ of the latter vector space is a $k[\tau]$-generating system of $\mathcal{O}(D)$.

In order to transform $\mathcal{B}'$ into a $k[\tau]$-basis of $\mathcal{O}(D)$ we apply the reduction algorithm to $\mathcal{B}'$. That is, we apply reduction steps to the elements in $\mathcal{B}'$ until we have detect a semi-reduced family $\mathcal{B}$ in $\langle \mathcal{B} \rangle_k$ with n elements of minimal length. Then, Corollary 2.8.14 shows that $\mathcal{B}$ is a basis of $\mathcal{O}(D)$.

We want to adopt Algorithm 3 to this situation. Hence, we need an adequate (semi-) reduceness criterion.

Theorem 5.4.4. *A set $\mathcal{B} \subset F$ is reduced if and only if for any $\rho \in \mathcal{R} := \{\|b\| + \mathbb{Z} \mid b \in \mathcal{B}\}$ the vectors in*

$$\{\mathrm{red}_{(e,a)}^{-\|b\|}(b) \mid b \in \mathcal{B} \text{ with } \|b\| + \mathbb{Z} = \rho\}$$

are k-linearly independent. Moreover, $\mathcal{B}$ is semi-reduced if and only if the vectors in

$$\{\mathrm{sred}_{(e,a)}^{-\|b\|}(b) \mid b \in \mathcal{B}\}$$

are k-linearly independent.

Proof. Clearly, $\mathcal{B}$ is (semi-) reduced with respect to $\| \ \|$ if and only if $\mathcal{B}$ is (semi-) reduced with respect to the τ-norm $-\| \ \| = w_{(e,a)}$. Thus, the statements follows by Theorems 5.2.6 and 5.2.7. □

In order to compute the vectors $\mathrm{red}_{(e,a)}^r(z)$ and $\mathrm{sred}_{(e,a)}^r(z)$, for $r \in \mathbb{R}$ and $z \in F$, one has to determine the vectors $(\mathrm{red}_{(P_i,e_i,a_i)}^r(z))$ and $(\mathrm{sred}_{(P_i,e_i,a_i)}^r(z))$, for any $1 \leq i \leq s$; that is, approximations of the P_i-adic development of $\iota_{P_i}(z) \in \hat{F}_{P_i}$. We fix $P := P_i$. In [12] an algorithmic realization of the by P induced residue class map $z \mapsto z \bmod P \in F_P$ is presented. Let $R_P \subset A_p$ be system of representatives of F_P. Then, the class $z \bmod P$ is represented by an adequate element in R_P. Moreover, we can consider $z \bmod P$ as a vector in $k^{\deg P}$.

Now we present an algorithm, which determines for $r \in \mathbb{R}$, $P_i \in \mathbb{P}_F$, $e_i, a_i \in \mathbb{Z}$, $e_i > 0$, and $z \in F$ the vector $\mathrm{sred}_{(P_i,e_i,a_i)}^r(z)$. Thus, we obtain an algorithmic realization of $\mathrm{sred}_{(e,a)}^r(z)$. Analogously, one can develop an algorithm, which determines $\mathrm{red}_{(e,a)}^r(z)$.

Algorithm 10: P-adic development

Input: Element $z \in F$, real number r, place $P \in \mathbb{P}_F$, and $e, a \in \mathbb{Z}$ with $e > 0$.
Output: $\mathrm{sred}_{(P,e,a)}^r(z)$.

1: **if** $\lfloor r \rfloor < \lfloor w_{P,e,a}(z) \rfloor$ or $r \notin w_{P,e,a}(F)$ **then**
2: **return** 0
3: **end if**
4: $\pi \leftarrow$ prime element of P
5: $z \leftarrow z\pi^{-a}\tau^{-\lfloor r \rfloor}$, $z' \leftarrow 0$
6: $C \leftarrow (0)_{0 \leq i < v_P(z)}$
7: **for** $j = v_P(z), \ldots, e-1$ **do**

8: $a \leftarrow (z - z')/\pi^j \bmod P$

9: Append(C, a)

10: $z' \leftarrow z' + a\pi^j$

11: **end for**

12: **return** C

Clearly, the output of the last algorithm is a vector of elements in R_P. In the implementation we consider these elements as vectors in $k^{\deg P}$.

Now we have all ingredients to describe an algorithm, which determines a $k[\tau]$-basis of $\mathcal{O}(D)$.

Initially, we compute a k-basis $\mathcal{B}'$ of $\mathcal{L}(D + r(\tau)_\infty)$ by Algorithm 6, for $r := \lceil (2[k_0 : k](g-1) + 1 - \deg D)/n + 1 \rceil$. By Theorem 5.4.3 we have to transform $\mathcal{B}'$ into a semi-reduced basis of $\mathcal{O}(D)$. One possibility is to adapt Algorithm 3 straight forward. That is, we have to change in Algorithm 3 the way of detecting the relations for the reduction steps. Instead of determining M as in line 5 in Algorithm 3, we compute the matrix, whose rows are given by the vectors $\mathrm{sred}_{(e,a)}^{-\|b'\|}(b')$, for $b' \in \mathcal{B}'$.

Alternatively we can proceed as follows: According to Theorem 5.4.3 there exits a basis $\mathcal{B}$ of $\mathcal{O}(D)$, whose elements are k-linear combinations of the vectors in $\mathcal{B}'$. Thus, in any reduction step we only consider vectors $b_1, \ldots, b_m$ satisfying $\lceil \|b_i\| \rceil = \lceil \|b_j\| \rceil$, for $1 \leq i, j \leq m$. As we decrease by any reduction step the length of the considered vectors, we start with the maximal possible length $m_0 := \max\{\|b'\| \mid b' \in \mathcal{B}'\}$.

We apply the semi-reduceness criterion from Theorem 5.4.4 to $\mathcal{B}'_{m_0} := (b \in \mathcal{B}' \mid \lceil \|b\| \rceil = \lceil m_0 \rceil)$. In particular, we detect a family $\mathcal{B}_{m_0} \subset \mathcal{B}'_{m_0}$ such that the vectors in $\mathrm{sred}_{(e,a)}^{-m_0}(\mathcal{B}_{m_0})$ built a k-basis of the k-vector space $\langle \mathrm{sred}_{(e,a)}^{-m_0}(\mathcal{B}'_{m_0}) \rangle_k$. The lengths of the vectors in $\mathcal{B}'_{m_0} \setminus \mathcal{B}_{m_0}$ can be reduced by applying reduction steps; that is, we subtrac from any vector in $\mathcal{B}'_{m_0} \setminus \mathcal{B}_{m_0}$ an adequate k-linear combination of vectors in $\mathcal{B}_{m_0}$. According to Theorem 5.4.4 the family $\mathcal{B}_{m_0}$ is semi-reduced. We set $\mathcal{B}' := \mathcal{B}' \setminus \mathcal{B}_{m_0}$.

In the next step we repeat the procedure and obtain $m_1 := \max\{\|b'\| \mid b' \in \mathcal{B}'\}, \mathcal{B}'_{m_1}$ and $\mathcal{B}_{m_1}$, accordingly. The family $\mathcal{B}_{m_1}$ is semi-reduced, whereas $\mathcal{B}_{m_0} \cup \mathcal{B}_{m_1}$ is not necessarily semi-reduced. We check for any $b \in \mathcal{B}_{m_0}$ if $\{b\} \cup \mathcal{B}_{m_1}$ is semi-reduced and delete b in $\mathcal{B}_{m_0}$ if it is not the case. Then, after finitely many steps this leads to a semi-reduced family $\mathcal{B}_{m_0} \cup \mathcal{B}_{m_1}$. Moreover, the vectors in $\mathcal{B}_{m_0} \cup \mathcal{B}_{m_1}$ built a maximal

semi-reduced family of minimal length in

$$\langle \{ b \in \mathcal{B}' \mid \lceil \|b\| \rceil = \lceil m_0 \rceil \text{ or } \lceil \|b\| \rceil = \lceil m_1 \rceil \} \rangle_k .$$

Proceeding this way results in a maximal semi-reduced family $\mathcal{B} := \cup_{i=0}^{l} \mathcal{B}_{m_i}$ (with an adequate $l \in \mathbb{Z}$) of vectors of minimal length in $\langle \mathcal{B}' \rangle_k$; hence, by Corollary 2.8.14 the family $\mathcal{B}$ is a semi-reduced basis of $\mathcal{O}(D)$.

We summarize the algorithm by the following pseudocode.

Algorithm 11: Basis computation of holomorphic rings

Input: A divisor D of F/k and $\tau \in F \setminus k_0$ with $(\tau)_\infty = \sum_{i=1}^{s} e_i P_i$.
Output: A $k[\tau]$-basis of the holomorphic ring $\mathcal{O}(D)$.

Compute basis $\mathcal{B}'$ of $\mathcal{L}(D + r(\tau)_\infty)$, for $r = \lceil (2[k_0 : k](g-1) + 1 - \deg D)/n + 1 \rceil$
$l \leftarrow 0$, $n \leftarrow \deg(\tau)_\infty$, $\mathcal{B} \leftarrow (\ )$, $e \leftarrow (e_i)_{1 \le i \le s}$, $a \leftarrow (v_{P_i}(D))_{1 \le i \le s}$
while $l < n$ **do**
    mval $\leftarrow \max_{b \in \mathcal{B}'} \{\|b\|\}$, $I \leftarrow$ set of indices of vectors in $\mathcal{B}'$ having $\lceil \| \ \| \rceil$-value equal to $\lceil \text{mval} \rceil$
    $M \leftarrow (\text{sred}_{(e,a)}^{-\text{mval}}(b_i))_{i \in I} \in k^{m \times n}$, where $m := \#I$
    Compute $P = (p_{i,j}) \in \text{LT}_m(k)$ s.t. $M' := PM$ is in row echelon form
    $s \leftarrow \text{rank}(M')$
    if $s < m$ **then**
        for $i = s+1, \ldots, m$ **do**
            $u_i \leftarrow \max\{1 \le j \le n \mid p_{i,j} \neq 0\}$
            Denote b_j the j-th vector in $\mathcal{B}'$:
            $b_{u_i} \leftarrow b_{u_i} + \sum_{j=1}^{u_i - 1} p_{i,j} b_j$
        end for
    end if
    $I' \leftarrow$ set of indices of vectors in $\mathcal{B}'$ corresponding to nonzero rows in M'
    Let $\mathcal{B} = (b_{m_1}, \ldots, b_{m_l})$
    for $j = m_1, \ldots, m_l$ **do**
        if $\text{rank}((\text{sred}_{(a,b)}^{-\|b_i\|}(b_i))_{i \in I' \cup \{m_j\}}) = s$ **then**
            $\mathcal{B} \leftarrow \mathcal{B} \setminus (b_{m_j})$
        end if

20: **end for**

21: $\mathcal{B} \leftarrow \mathcal{B} \cup (b_i \mid i \in I')$, $\mathcal{B}' \leftarrow \mathcal{B}' \setminus (b_i \mid i \in I')$, $l \leftarrow \#\mathcal{B}$

22: **end while**

23: **return** $\mathcal{B}$

6. Experimental results

We have implemented the algorithms, presented in the previous chapters, in Magma [5]. Those algorithms concerning function fields have been implemented for global function fields. We will compare the runtime of our algorithms with that of the algorithms of Magma. All computations have been done in a Linux server, with two Intel Quad Core processors, running at 3.0 GHz, with 32 GB of RAM memory. Times are expressed in seconds. If an algorithm did not terminate after 24 hours we write "$-$" instead. At first we compare the running time for the computation of the genus and the Riemann-Roch space $\mathcal{L}(0)$ of the zero divisor. Later we present the running time for the computation of $\mathcal{L}(D)$ for randomly chosen divisors D.

6.1 Computation of the genus

In this section we consider the practical performance of Algorithm 7 for the computation of the genus of a global function field and that of Algorithms 6 and 5 for the computation of a semi-reduced basis and a reduced basis of the lattice $(\mathcal{O}_F, \| \ \|_0)$, respectively.

For each example we present the characteristic data of the function field F/k and its defining polynomial f and the time, which needed the algorithms mentioned above and that of Magma to determine the genus or a (semi-) reduced basis of $(\mathcal{O}_F, \| \ \|_0)$, respectively. Additionally, we give the number of seconds of the initial computation (I.C.) in Algorithm 7; that is, the time that costs the computation of $\operatorname{disc} f$ and the factorization of its inseparable part. We will see that in most of the cases the initial computation dominates Algorithm 7. In the column Algo 7 we display the total running time of Algorithm 7, including the initial computation.

Note that for the computation of the genus of a function field, Magma only determines a semi-reduced basis of the lattice induced by the zero divisor. We will compare

our algorithms with that of Magma; that is, we compute with Algorithm 9 and Algorithm 8 bases of $\mathcal{O}_F$ and $\mathcal{O}_{F,\infty}$, respectively, and call Algorithm 6 in order to determine a semi-reduced basis of $(\mathcal{O}_F, \| \ \|_0)$. We present the running time for the computation of a semi-reduced basis in the column Sred.

By determining an orthonormal basis with Algorithm 8 (cf. Remark 5.3.6) and replacing Algorithm 6 through Algorithm 5, the same procedure computes a reduced basis of $(\mathcal{O}_F, \| \ \|_0)$. In the column Red we display the running time for the computation of a reduced basis of $(\mathcal{O}_F, \| \ \|_0)$.

For the first examples we use families of global function fields, which cover all the computational difficulties of the Montes algorithm [12]. Later, we use randomly chosen global function fields.

We consider in all examples the function field F/k of genus g, with defining polynomial $f(t,x) \in k[t,x]$.

Example 1

Let $f = (x + p(t)^r + \cdots + 1)^n + p(t)^k \in \mathbb{F}_{37}[t,x]$, where $p(t) \in A$ is irreducible and k, r are nonnegative integers.

g	$p(t)$	n	k	r	I.C.	Algo 7	Magma	Sred	Red
0	t	5	7	10	0.0	0.02	0.39	0.03	0.05
22	t^3+2	23	30	10	0.04	9.40	66289.34	2.2	2.6
0	$t+1$	77	163	20	2.73	5.42	–	133.42	151.56

Example 2

Let $f = (\prod_{\alpha \in \mathbb{F}_3}(x + t\alpha)^m + tp(t)^k)^m + tp(t)^{3mk} \in \mathbb{F}_3[t,x]$, where $p(t) = t^2 + 1$ and m, k are nonnegative integers.

g	$\deg f$	k	m	I.C.	Algo 7	Magma	Sred	Red
50	12	2	2	0.01	0.05	0.82	0.10	0.12
528	48	5	4	0.21	1.17	1322.08	9.16	25.17
1136	75	7	5	3.32	24.30	15961.82	193.65	199.53
1198	147	1	7	2.60	80.3	–	1498.19	13745.52

Example 3

Let $f = (x^2 - 2x + 4)^3 + p^k \in \mathbb{F}_q[t, x]$, where $p(t) \in A$ is irreducible and k a nonnegative integer.

g	q	$p(t)$	k	I.C.	Algo 7	Magma	Sred	Red
0	7	$t+2$	7	0.00	0.01	0.04	0.05	0.06
60	7	$t+2$	122	0.02	0.03	0.36	0.02	0.03
450	101	$t+1$	901	0.00	0.03	15.76	0.02	0.02
3512	73	t^2+1	3511	6.59	9.15	1238.77	10.16	11.09

Example 4

Let $f = ((x^6 + 4(t^2+1)x^3 + 3(t^2+1)^2x^2 + 4(t^2+1)^2)^2 + (t^2+1)^6)^3 + p(t)^k \in \mathbb{F}_q[t, x]$ of degree 36, where $p(t) \in A$ is irreducible and k a nonnegative integer.

g	q	$p(t)$	k	I.C.	Algo 7	Magma	Sred	Red
85	13	t^2+1	11	0.05	0.19	122.6	0.80	3.00
519	101	$t+17$	112	0.83	4.59	1052.82	19.44	27.54
3379	53	t^2+2	323	19.58	234.65	4617.74	309.23	308.90

Example 5

Let $f = (x^{l-1} + \cdots + x + 1)^m + t^k \in \mathbb{F}_q[t, x]$, where m, l, k are nonnegative integers.

g	q	$\deg f$	m	l	k	I.C.	Algo 7	Magma	Sred	Red
6	101	8	4	3	13	0.00	0.01	0.10	0.03	0.03
0	13	42	7	7	13	0.01	0.17	292.9	3.77	4.31
2	3	260	13	21	2	0.02	0.82	–	31.39	32.48
36	13	420	21	21	5	1.45	3.81	–	85325.14	–

Example 6

For $1 \leq l \leq 6$ we take the family of polynomials $f_l \in \mathbb{F}_{13}[t, x]$ with:

$f_1(t, x) = x^2 + t$
$f_2(t, x) = f_1(x)^2 + (t-1)t^3x$
$f_3(t, x) = f_2(x)^3 + t^{11}$
$f_4(t, x) = f_3(x)^3 + t^{29}xf_2(x)$
$f_5(t, x) = f_4(x)^2 + (t-1)t^{42}xf_1(x)f_3(x)^2$
$f_6(t, x) = f_5(x)^2 + t^{88}xf_3(x)f_4(x)$

l	g	$\deg f_l$	I.C.	Algo 7	Magma	Sred	Red
1	0	2	0.0	0.0	0.0	0.02	0.02
2	3	4	0.0	0.01	0.01	0.03	0.03
3	9	12	0.01	0.02	1.66	0.04	0.18
4	40	36	0.09	0.12	707.06	8.84	44.00
5	133	72	1.37	1.61	60125.24	233.60	1922.65
6	329	144	22.06	24.67	–	9039.53	–

Example 7

We consider the function field $F/\mathbb{F}_q$ of genus $g = 140$ with the defining polynomial $x^{41} - (t^2+1)(x^2-1) - (t^8+2t^6+1)x$.

q	I.C.	Algo 7	Magma	Sred	Red
3	0.01	0.05	64.23	1.56	14.59
97	0.03	0.03	169.02	1.16	16.43
10007	0.08	0.10	171.98	5.82	31.31

Example 8

We consider the function field $F/\mathbb{F}_q$ of genus $g = 213$ with the defining polynomial $x^{62} + (t+1)x^{12} + t^8 + 1$.

q	I.C.	Algo 7	Magma	Sred	Red
7	0.03	0.23	765.12	0.25	0.46
113	0.01	0.13	2011.94	1.79	79.21
1013	0.04	0.12	2017.90	2.01	92.04

Example 9

We consider the function field $F/\mathbb{F}_q$ of genus $g = 325$ with the defining polynomial $x^{94} + (t+1)x^{12} + t^8 + 1$.

q	I.C.	Algo 7	Magma	Sred	Red
7	0.04	0.26	5990.76	0.60	0.74
103	0.04	0.38	23528.40	0.73	0.88
1009	0.08	0.32	24305.16	2.33	3556.87

Example 10

We consider the function field $F/\mathbb{F}_q$ of genus g with the defining polynomial $x^{40} + (t+1)x^{23} + t^9x + (t+1)x^{13} + (t^5 - 3t^2)x^7 + t^{62}x^3 + t + 1$.

g	q	I.C.	Algo 7	Magma	Sred	Red
1220	5	0.59	0.66	92.5	0.76	0.82
1220	125	1.05	1.07	98.02	1.34	1.39
1221	3137	1.64	1.71	212.37	1.81	1.87

Example 11

We consider the function field $F/\mathbb{F}_q$ of genus g with the defining polynomial $x^{68} + (t+1)^4x^{23} + (t^3+5)^9x + (t+1)x^{13} + (t^5 - 3t^2)x^7 + t^{62}x^3 + t + 1$.

g	q	I.C.	Algo 7	Magma	Sred	Red
2082	5	0.1	0.18	514.14	0.41	0.50
2082	125	0.21	0.33	598.40	0.47	0.55
2083	3137	7.39	7.45	1662.31	7.69	7.81

Example 12

We consider the function field $F/\mathbb{F}_q$ of genus $g = 3669$ with the defining polynomial $x^{120} + (t+1)^4x^{23} + (t^3+5)^9x + (t+1)x^{13} + (t^5 - 3t^2)x^7 + t^{62}x^3 + t + 1$.

q	I.C.	Algo 7	Magma	Sred	Red
5	7.77	7.84	15415.75	9.04	74.69
97	5.00	5.10	21610.17	8.00	139.59
529	33.93	33.83	16172.12	50.12	1170.70

Example 13

We consider the function field $F/\mathbb{F}_q$ of genus $g = 15154$ with the defining polynomial $x^{4330} - (t^2+1)(x^2-1) - (t^8 + 2t^6 + 1)x$.

q	I.C.	Algo 7	Magma	Sred	Red
3	1.69	9.93	–[a]	–[a]	–[a]
37	1.90	32.58	–[a]	–[a]	–[a]

[a] All virtual memory has been exhausted, so Magma cannot perform this statement.

Example 14

We consider the function field $F/\mathbb{F}_{101}$ of genus $g = 0$ with the defining polynomial $h^4 + 23h^3 + h^2 + 30h + 50$ and $k_0 = \mathbb{F}_{101^4}$, where $h := x^{101} + (t+1)x + t^{62} + t + 1$.

I.C.	Algo 7	Magma	Sred	Red
0.73	6.66[b]	–	12.45	13.58

[b]Algorithm 7 had to factorize f over $\mathbb{F}_{101^4}$. The factorization took 2.07 seconds.

Example 15

We consider the function field $F/\mathbb{F}_{13}$ of genus $g = 1221$ with the defining polynomial $h^3 + h^2 + 4h + 1$ and full constant field $k_0 = \mathbb{F}_{13^3}$, where $h := x^{40} + (t+1)x^{23} + t^9x + (t+1)x^{13} + (t^5 - 3t^2)x^7 + t^{62}x^3 + t + 1$.

I.C.	Algo 7	Magma	Sred	Red
127.82	129.45[c]	–	1511.61	25471.56

[c]Algorithm 7 had to factorize f over $\mathbb{F}_{13^3}$. The factorization took 0.24 seconds.

6.2 Computation of Riemann-Roch spaces

In this subsection we compare the runtime of our algorithms for the computation of Riemann-Roch spaces with that of Magma.

Let F/k be a global function field. Our algorithms are based on the OM-representation of prime ideals and places (cf. Subsection 1.4.1), whereas Magma uses the classical representation [5, 6]. In order to compare the routines in the context of the computation of $\mathcal{L}(D)$, for some divisor D of F/k, we create divisors in both settings as a free $\mathbb{Z}$-linear combination of places (free representation) and by a pole divisor of a nonzero element $a \in F$. Note that the timings of the subsequent computations include both generating a divisor D and computing $\mathcal{L}(D)$ in the OM-setting or the classical one, respectively.

By the computation of the Riemann-Roch space $\mathcal{L}(D)$ of a divisor D, we mean the computation of a (semi-) reduced basis of the lattice induced by D. In the rows Sred and Red we present the characteristic data regarding the computation of a semi-reduced basis and a reduced basis, respectively, as explained in the last section; that is, the timings for computing $\mathcal{L}(0)$ and $\mathcal{L}(D)$ for divisors D of height $h(D)$.

The routine of Magma, which determines such a semi-reduced basis is called *ShortBasis* and is based upon the algorithm presented in [16]. For all tests we do not apply any divisor reduction, except for the computation of the Riemann-Roch space of the

pole divisor of a nonzero function $a \in F$ by Magma. In that particular context Magma applies initially a divisor reduction, which can not be avoided.

The tests are distinguished into two different types; the computation of Riemann-Roch spaces of randomly chosen divisors given in free representation, and the computation of Riemann-Roch spaces of pole divisors of randomly chosen elements in F.

The randomly chosen divisors (in free representation) are again separated into two different types: For a divisor D of F/k, we denote by $\mathrm{md}(D)$ the maximal degree of all places contained in $\mathrm{supp}(D)$. At first we consider randomly chosen divisors D carrying places of "small" degree; that is, divisors D satisfying

$$\mathrm{md}(D) \leq \max\{\lceil 2\log_q(4g-2)\rceil, \lceil 2\log_q(2g)\rceil + 1\}, \quad h(D) \leq 10g,$$

where g denotes the genus of F/k and q is the number of elements in k. According to [16] this kind of divisors occur in the context of the class group computation of global function fields.

Later we consider divisors, which carry places of "large" degree and have "large" height. Note that we determine for all examples initially $\mathcal{L}(0)$.

Example 1

We consider the function field $F/\mathbb{F}_q$ of genus $g = 79$ with the defining polynomial $f := (x^2 - 2x + 4(t+1)^{12})^3 + (t+7)^{33} + 2$. The ramification indices of all places at infinity are equal 1; that is, any norm induced by a divisor D of F/k is integer-valued. Hence, any semi-reduced basis is automatically a reduced one. We consider 500 repetitions and the present the average values.

Computation of Riemann-Roch spaces of divisors in free representation:

$q = 13$	$\mathcal{L}(0)$	$\mathcal{L}(D)$	$h(D)$	$\mathrm{md}(D)$
Red	0.12	0.47	553	5
ShortBasis	0.03	1.13	557	5
Red		24.68	33161	213
ShortBasis		70.67	33022	214

Computation of Riemann-Roch spaces of pole divisors:

$q = 13$	$\mathcal{L}(D)$	$h(D)$	$\mathrm{md}(D)$
Red	0.16	551	98
ShortBasis	2.19	527	96

Computation of Riemann-Roch spaces of divisors in free representation:

$q = 13^5$	$\mathcal{L}(0)$	$\mathcal{L}(D)$	$h(D)$	$\mathrm{md}(D)$
Red	0.16	0.35	330	2
ShortBasis	0.05	1.35	324	2
Red		103.70	33229	213
ShortBasis		293.92	33136	214

Computation of Riemann-Roch spaces of pole divisors:

$q = 13^5$	$\mathcal{L}(D)$	$h(D)$	$\mathrm{md}(D)$
Red	1.64	535	94
ShortBasis	7.71	537	93

Example 2

We consider the function field $F/\mathbb{F}_q$ of genus $g = 765$ with the defining polynomial $f := x^9 + x^5(t^{23} + 12t^8) + t^{123}x^4 + (t^{12} + 1)^{12} + 2$. We consider 250 repetitions and the present the average values.

Computation of Riemann-Roch spaces of divisors in free representation:

$q = 17$	$\mathcal{L}(0)$	$\mathcal{L}(D)$	$h(D)$	$\mathrm{md}(D)$
Sred	0.29	18.72	4207	7
Red	0.30	19.82	4273	7
ShortBasis	2.78	40.28	4337	7
Sred		474.30	79679	126
Red		507.56	79112	128
ShortBasis		1415.67	77853	129

Computation of Riemann-Roch spaces of pole divisors:

$q = 17$	$\mathcal{L}(D)$	$h(D)$	$\mathrm{md}(D)$
Sred	1.83	2555	373
Red	1.74	2532	394
ShortBasis	99.28	2358	373

Computation of Riemann-Roch spaces of divisors in free representation:

$q = 17^4$	$\mathcal{L}(0)$	$\mathcal{L}(D)$	$h(D)$	$\mathrm{md}(D)$
Sred	0.43	29.44	2821	3
Red	0.50	25.63	2600	3
ShortBasis	5.35	107.36	2933	3
Sred		678.19	62171	96
Red		700.74	64270	98
ShortBasis		3104.04	60070	94

Computation of Riemann-Roch spaces of pole divisors:

$q = 17^4$	$\mathcal{L}(D)$	$h(D)$	$\mathrm{md}(D)$
Sred	139.57	3248	613
Red	114.80	3271	562
ShortBasis	560.32	3198	495

Example 3

We consider the function field $F/\mathbb{F}_q$ of genus $g = 1982$ with the defining polynomial $f := x^{11} + t^{13} + 3x^7 + (2(t+1)^8 + 2t)^7 x^6 + (2t^8 + t^6 + 2t)^{45} x^3 + (t+1)^5 t^4 (2x + x) + t^{12} + 2$. We consider 250 repetitions and the present the average values.

Computation of Riemann-Roch spaces of divisors in free representation:

$q = 7$	$\mathcal{L}(0)$	$\mathcal{L}(D)$	$h(D)$	$\mathrm{md}(D)$
Sred	1.57	16.66	3351	10
Red	6.33	34.29	3560	10
ShortBasis	180.25	160.84	3532	10
Sred		483.36	71027	251
Red		631.17	68904	242
ShortBasis		1468.05	66938	248

Computation of Riemann-Roch spaces of pole divisors:

$q = 7$	$\mathcal{L}(D)$	$h(D)$	$\mathrm{md}(D)$
Sred	0.37	4162	217
Red	1.59	4121	206
ShortBasis	1277.94	4142	212

Computation of Riemann-Roch spaces of divisors in free representation:

$q = 7^7$	$\mathcal{L}(0)$	$\mathcal{L}(D)$	$h(D)$	$\mathrm{md}(D)$
Sred	6.03	16.53	1433	3
Red	24.70	64.40	1468	3
ShortBasis	438.64	649.20	1450	3
Sred		163.88	16794	97
Red		257.79	15830	92
ShortBasis		1110.01	15708	93

Computation of Riemann-Roch spaces of pole divisors:

$q = 7^7$	$\mathcal{L}(D)$	$h(D)$	$\mathrm{md}(D)$
Sred	4.26	4155	203
Red	12.21	4104	181
ShortBasis	10910.44	4112	177

Example 4

We consider the function field $F/\mathbb{F}_q$ of genus $g = 4721$ with the defining polynomial $f^2 + x^4(t+2)^4 - t^{12}$, where f is defined as in Example 2. We consider 50 repetitions and the present the average values.

Computation of Riemann-Roch spaces of divisors in free representation:

$q = 5$	$\mathcal{L}(0)$	$\mathcal{L}(D)$	$h(D)$	$\mathrm{md}(D)$
Sred	28.98	104.71	3718	12
Red	386.27	428.97	3609	12
ShortBasis	65767.46	529.41	3281	12
Sred		1896.82	86562	357
Red		3510.66	91299	356
ShortBasis		20487.03	88076	361

Computation of Riemann-Roch spaces of pole divisors:

$q = 5$	$\mathcal{L}(D)$	$h(D)$	$\mathrm{md}(D)$
Sred	3.56	16239	358
Red	837.70	16296	466
ShortBasis	–		

Computation of Riemann-Roch spaces of divisors in free representation:

$q = 5^7$	$\mathcal{L}(0)$	$\mathcal{L}(D)$	$h(D)$	$\mathrm{md}(D)$
Sred	113.31	552.63	2875	3
Red	637.96	1729.12	2800	3
ShortBasis	–	2597.79	2813	3
Sred		3042.12	52867	183
Red		5451.88	48783	202
ShortBasis		18761.07	49858	194

Computation of Riemann-Roch spaces of pole divisors:

$q = 5^7$	$\mathcal{L}(D)$	$h(D)$	$\mathrm{md}(D)$
Sred	37.94	16123	383
Red	7686.77	16087	363
ShortBasis	–		

Bibliography

[1] J.-D. Bauch, E. Nart, H. Stainsby, *Complexity of OM factorizations of polynomials over local felds*, LMS J. Comput. Math. 16, 2013, 139-171.

[2] J.-D. Bauch, *Berechnung von Divisorenklassengruppen von globalen Funktionenkörpern mittels der Tate-Lichtenbaum Paarung*, Diplomarbeit, TU Berlin 2009.

[3] K. Belabas, M. van Hoeij, J. Klüners, A. Steel, *Factoring polynomials over global fields*, Journal de Théorie des Nombres de Bordeaux **21** (2009), 15-39, 2009.

[4] A. Bostan, G. Lecerf, B. Salvy, É. Schost, B. Wiebelt, *Complexity issues in bivariate polynomial factorization*, Proceedings of ISSAC, (2004).

[5] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Computation, 24 3/4:235265, 1997.

[6] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, Springer, 1993.

[7] J. Guàrdia, J. Montes, E. Nart, *Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields*, Journal de Théorie des Nombres de Bordeaux **23** (2011), no. 3, 667–696.

[8] J. Guàrdia, J. Montes, E. Nart, *Newton polygons of higher order in algebraic number theory*, Trans. Amer. Math. Soc. **364** (2012), no. 1, 361–416.

[9] J. Guàrdia, J. Montes, E. Nart, *A new computational approach to ideal theory in number fields*, Found Comput Math (2013) 13:, 729-762.

[10] J. Guàrdia, J. Montes, E. Nart, *Higher newton polygons and integral bases*, arXiv:0902.3428v2[math.NT]..

[11] J. Guàrdia, J. Montes, E. Nart, *Genetics of polynomials over local fields*, arXiv:1309.4340v1 [math.NT].

[12] J. Guàrdia, E. Nart, S. Pauli, *Single-factor lifting and factorization of polynomials over local fields*, Journal of Symbolic Computation 47 (2012), 1318-1346.

[13] J. Guàrdia, E. Nart, *Okutsu invariants and Newton polygons*, Acta Arith. **145**(1), 83-108, (2012).

[14] H. Hasse, *Number theory*, second Edition, Grundlehren der mathematischen Wissenschaften, Springer, 1980.

[15] K. Hensel, *Theorie der algebraischen Zahlen*, Teubner, Leipzig, Berlin, 1908.

[16] F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symbolic Computation, 11,1-000, 2001.

[17] S. Lang, *Algebra*, Graduate Texts in Mathematics, Springer New York, 2002.

[18] A. K. Lenstra, *Factoring Multivariate Polynomials over Finite Fields*, Journal of Computer and System Science **30** (1985), 235–248.

[19] H. W. Lenstra, JR. *Lattices*, Algorithmic Number Theory, MSRI Publications, Volume **44** (2008).

[20] S. Mac Lane, *A construction for absolute values in polynomial rings*, Transactions of the American Mathematical Society, **40** (1936), 363395.

[21] K. Mahler, *An analogue to Minkowski's geometry in a field of series*, Ann. of Math. (2) **42** (1941), 488522.

[22] G. Möhlmann, *Einbettungen globaler Funktionenkörper*, Diplomarbeit, TU Berlin 2008.

[23] J. Montes, *Polígonos de Newton de orden superior y aplicaciones aritméticas*, PhD Thesis, Universitat de Barcelona, 1999.

[24] T. Mulders, A. Storjohann, *On lattice reduction for polynomial matrices*, J. Symbolic Computation, 35,4,377–401 , 2003

[25] T. Mulders, A. Storjohann, *Rational Solution of Singular Linear Systems*, In Proceedings of ISSAC'2000, ACM Press, 24224–9 , 2000

[26] J. Neukirch, *Algebraische Zahlentheorie*, Springer Verlag, 1991.

[27] E. Nart, *Local computation of differents and discriminants*, Mathematics of Computation, 83 (2014), 1513-1534.

[28] K. Okutsu, *Construction of Integral Basis. I*, Proceedings of the Japan Academy, 58, Ser. A (1982), 47-49, 87-89.

[29] M. Pohst, H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1997.

[30] W. M. Schmidt, *Construction and Estimation of Bases in Function Fields*, Journal of Number Theory **39** (1991), 181–224.

[31] M. Schörnig, *Untersuchung konstruktiver Probleme in globalen Funktionenkörpern*, PhD Thesis, TU Berlin 1996.

[32] J.-P. Serre, *Corps locaux*, 4th corrected Edition, Hermann, Paris, 2004.

[33] H. Stichtenoth, *Algebraic Function Fields and Codes*, second Edition, Graduated Texts in Mathmatics, Springer, 2008.

[34] A. Schönhage, V. Strassen, *Schnelle Multiplikation großer Zahlen*, Computing 7 (1971) 281-292.

[35] J. von zur Gathen, J. Gerhard: *Modern Computer Algebra*, Second Edition. Cambridge University Press, Cambridge, 2003.