LATTICES OVER POLYNOMIAL RINGS AND APPLICATIONS TO FUNCTION FIELDS

JENS-DIETRICH BAUCH

Abstract. This paper deals with 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 discrete 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 $(L, \| \|)$. By identifying a divisor D of an algebraic function field with a lattice $(L, \| \|)$ over a polynomial ring, this reduction algorithm can be addressed to the computation of the Riemann-Roch space of D and the successive minima of $(L, \| \|)$, without the use of any series expansion.

Introduction

The theory of lattices over the integers is an important tool in algebraic number theory. Lattices over the polynomial ring $k[t]$ in an indeterminate t, over a field k, admit a similar development although the theory becomes simpler. For instance, a shortest vector in a lattice can be found in polynomial time, whereas this 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 [13]. Lattices over polynomial rings (or Puiseux series rings) are used to factorize multivariate polynomials [11] and to compute Riemann-Roch spaces in algebraic function fields [10], [16], [17]. The idea of constructing bases of Riemann-Roch spaces of a divisor D by computing vectors of short length in a lattice $(L, \| \|)$ corresponding to D is due to W. M. Schmidt [16]. His method is based on the computation of Puiseux series in the context of function fields in one variable over number fields. This idea was adopted by M. Schörnig [16] to global function fields, which are tamely ramified at the places at infinity. Both methods use series expansions, which result in several technical problems; e.g. constant field extension are necessary and it has to take care that the series are computed to enough precision. F. Hess [10] could solve these problems by identifying a divisor D with a simplified lattice $(L', \| \|')$, which yields an algorithm that avoids series expansions and applies to function fields over arbitrary ("computable") constant fields. However, the simplified lattice $(L', \| \|')$ (and therefore Hess' algorithm) does not carry out the successive minima of the original lattice attached to D, only approximations.

The theory of lattices over $k[t]$ plays an important role in coding theory and cryptanalysis in the context of convolutional codes [12] and in the computation of approximated common divisors over polynomial rings [5].

Key words and phrases. Lattices, polynomial ring, reduction algorithm,riemann-roch spaces.
This research was supported by MTM2013-40680-P from the Spanish MEC and by the Netherlands Organization for Scientific Research (NWO) under grant 613.001.011.

In all these settings it is necessary to determine a reduced basis (cf. Section 1.1) of a lattice. This led to several reduction algorithms [11, 20, 16, 17, 14], 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) and, applied to the computation of Riemann-Roch spaces, it fixes the flaw of Hess' algorithm; that is, we are able to compute the Riemann-Roch space of a divisor D and the successive minima of the corresponding lattice without any series expansions.

The article is divided in the following sections. In Section 1 we introduce general lattices, their successive minima, and normed spaces. We define the concept of reduced bases and prove their existence in any lattice (cf. Lemma 1.13). Moreover, we define length preserving maps between normed spaces (isometries) and compute the general structure of the isometry group of a normed space. In Section 2 we introduce a reduction algorithm, which transforms any basis of a non integral-valued lattice into a reduced one. It generalizes the classical approach of A. Lenstra for integral-valued lattices [11], to the non integral-valued case. In Section 3 we consider the computation of Riemann-Roch spaces of divisors of function fields (and their successive minima) as an application of the new reduction algorithm. In Section 4 we give a precise estimation of the complexity of this method.

1. Lattices and normed spaces

Let k be a field and denote by $A=k[t]$, $K=k(t)$, the polynomial ring and the rational function field in the indeterminate t over k, respectively.

For any rational function $x=a/b\in K$, where $a,b\in A$ and $b\neq 0$, we define

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

This is a discrete valuation on K, with valuation ring $A_\infty=k[t^{-1}]_{(t^{-1})}\subset K$ and maximal ideal $P_\infty=\mathfrak{m}_\infty=t^{-1}A_\infty$. We denote by $U_\infty=\{a\in K\mid v_\infty(a)=0\}$ the group of units of A_∞.

Let $K_\infty=k((t^{-1}))$ be the v_∞-adic completion of K. The valuation v_∞ extends in an obvious way to K_∞. Let $\hat{A}_\infty\subset K_\infty$ be the valuation ring of v_∞, and $\hat{\mathfrak{m}}_\infty$ its maximal ideal.

On K_∞ we may consider the *degree function* $|\ |:=-v_\infty$, which is an extension of the ordinary degree of polynomials: $|a|=\deg a$ for all $a\in A$.

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

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 1.1. *A* norm*, or* length function *on an R-module L is a mapping*

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

satisfying the following conditions:

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

For $r \in \mathbb{R}$ we define

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

Note that for any $x_1, x_2 \in L$ with $\|x_1\| \neq \|x_2\|$, it holds

$$\|x_1 + x_2\| = \max\{\|x_1\|, \|x_2\|\}. \tag{1}$$

Clearly, the degree function itself $|\ |$ is a norm on R.

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 1.4).

Definition 1.2. *Let L be a finitely generated R-module and $\|\ \|$ a norm on L. The pair $(L, \|\ \|)$ is said to be a* lattice *over R if $\dim_k L_{\leq r} < \infty$ for all $r \in \mathbb{R}$.*

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

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 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 finitely generated R-submodule M of full rank is a lattice with the norm obtained by restricting $\|\ \|$ to M.

In fact, let $L \subset E$ be a sub-R-submodule such that $(L, \|\ \|)$ is a lattice. Since there exists an $a \in K_R \setminus \{0\}$ with $aM \subset L$, we obtain

$$\dim_k M_{\leq r} = \dim_k (aM)_{\leq r+|a|} \leq \dim_k (L)_{\leq r+|a|} < \infty, \quad \text{for all } r \in \mathbb{R}.$$

Examples.

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

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. Section 3).

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 1.3. *A lattice homomorphism between the lattices $(L, \|\ \|)$ and $(L', \|\ \|')$ is an A-module homomorphism $\varphi \colon L \longrightarrow L'$ such that $\|\varphi(x)\|' = \|x\|$ for all $x \in L$.*

A lattice isomorphism is called an isometry *between $(L, \|\ \|)$ and $(L', \|\ \|')$.*

Definition 1.4. *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 1.5. *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 $\| \ \|' = \| \ \| + r$.*

Lemma 1.6. *Let $(L, \| \ \|)$ be an A-lattice of rank n. For $1 \le i \le n$, consider*

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

Then, $r_i := \inf(\mathcal{R}_i)$ exists and is attained by some vector in L. These numbers $r_1 \le \cdots \le r_n$ are called the successive minima *of L.*

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

$$L_{\le \lambda_1} \supsetneq L_{\le \lambda_2} \supsetneq \dots .$$

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

1.1. **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.

Definition 1.7. *Let $\mathcal{B} = \{b_1, \dots, b_m\}$ be a subset of $E \setminus \{0\}$. We say that $\mathcal{B}$ is* reduced *if for all $a_1, \dots, a_m \in K$, it holds*

$$\|a_1 b_1 + \cdots + a_m b_m\| = \max_{1 \le i \le m} \{\|a_i b_i\|\}. \tag{2}$$

Equivalently, it suffices to check (2) for all families $a_1, \dots, a_m \in A$.

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

Lemma 1.8.

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

For a basis $\mathcal{B} = (b_1, \dots, b_n) \in E^n$, 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 1.9. *Let $\mathcal{B} = (b_1, \dots, b_n) \in E^n$ be a basis of E with the vectors ordered by increasing length:*

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

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 $L = \langle \mathcal{B} \rangle_A$ 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 Definition 1.7. Also, the fact that the A-isomorphism $L \simeq A^n$ obtained by restricting $c_{\mathcal{B}}$ to L is an isometry between L and $\mathcal{O}(r_1) \perp \cdots \perp \mathcal{O}(r_n)$ is a reformulation of Definition 1.7 too. □

Proposition 1.10. *Let $\mathcal{B} = (b_1, \dots, b_n) \in E^n$ be a reduced basis of E with*

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

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

(1) $\|E\| := \{\|x\| \mid x \in E \setminus \{0\}\} = (r_1+\mathbb{Z}) \cup \cdots \cup (r_n+\mathbb{Z})$.
This set induces a finite subset of $\mathbb{R}/\mathbb{Z}$ called the signature *of E:*

$$\mathrm{Sig}(E) := \|E\|/\mathbb{Z} = \{r_1+\mathbb{Z}, \dots, r_n+\mathbb{Z}\} \subset \mathbb{R}/\mathbb{Z}.$$

(2) *$r_1 \le \cdots \le r_n$ are the successive minima of L.*
(3) *For any $r \in \mathbb{R}$, the following family is a k-basis of $L_{\le r}$:*

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

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

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

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

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

This proves the first item.

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

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

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

$$\max\{\|x_1\|, \dots, \|x_j\|\} \ge \|b_j\|.$$

This proves the second item.

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

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

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

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

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

The following observation is a direct consequence of item (*1*) of Proposition 1.10.

Corollary 1.11. *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 reduced bases.

Theorem 1.12. *Let $(L, \|\ \|)$ be a lattice and $r_1 \le \cdots \le r_n$ its successive minima. Let $\mathcal{B} = (b_1, \dots, b_n)$ be a family of A-linearly independent elements in L such that $\|b_i\| = r_i$, for all $1 \le i \le n$. Then, $\mathcal{B}$ is a reduced basis of L.*

Proof. Let us first show that $\mathcal{B}$ is reduced by induction on n. Reduceness being obvious for $n = 1$, assume the statement holds for lattices of rank $n-1$.

Take $a_1, \dots, a_n \in A$ and set $u = a_1 b_1 + \cdots + a_{n-1} b_{n-1}$. We want to show that

$$\|u + a_n b_n\| = \max\{\|u\|, \|a_n b_n\|\},$$

since by induction hypothesis it holds $\|u\| = \max_{1\le i<n}\{\|a_ib_i\|\}$. For $\|u\| \ne \|a_nb_n\|$ the statement follows from (1).

Suppose $\|u\| = \|a_nb_n\|$ and $\|u+a_nb_n\| < \max\{\|u\|, \|a_nb_n\|\} = \|u\|$. In particular, we have $a_n \ne 0$. We fix $I := \{1 \le j \le n \mid \|a_ib_i\| = \|u\|\}$; note that $n \in I$ by our assumption. For $i \in I$ we write $a_i = \lambda_i t^{d_i} + a_i'$, where $\lambda_i \in k$ and $d_i = |a_i| > |a_i'|$. Then, if we take $u_0 = \sum_{i\in I} \lambda_i t^{d_i} b_i$, it holds $u + a_nb_n = u_0 + u'$ with $u' \in L$ having $\|u'\| < \|u\|$. Hence,

$$\|u_0\| \le \max\{\|u + a_nb_n\|, \|u'\|\} < \|u\| = |a_i| + r_i = d_i + r_i,\ \forall i \in I. \tag{3}$$

Since $r_i \le r_n$, we have $d_n \le d_i$ for $i \in I$. By (3), the element $b = t^{-d_n}u_0$ belongs to L and has $\|b\| < r_n$. Since $b_1, \dots b_{n-1}, b \in L$ are linearly independent, this contradicts the minimality of r_n. This proves that $\mathcal{B}$ is reduced.

Finally, let us 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 $b = \sum_{i=1}^n a_ib_i$ with at least one $a_i \in K \setminus A$. We set $I = \{1 \le i \le n \mid a_i \notin A\}$ and consider

$$\sum_{i\in I} a_ib_i = b - \sum_{i\notin I} a_ib_i \in L. \tag{4}$$

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

$$\Big\|\sum_{i\in I} a_ib_i\Big\| = \max_{i\in I}\{\|a_ib_i\|\} = \|a_jb_j\|,$$

for some $j \in I$. If $|a_j| \ge 0$ we can write $a_j = a + a_j'$ with $a \in A$ and $a_j' \in \mathfrak{m}_\infty$ and subtract ab_j in (4) from both sides. Therefore, we can assume that $|a_j| < 0$ and get $\|\sum_{i\in I} a_ib_i\| < \|b_j\| = r_j$. By setting $b_j' = \sum_{i\in I} a_ib_i$, 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 $\|b_j\| = r_j$. □

From Lemma 1.6, it follows easily the existence of linearly independent elements in a given lattice, whose length attains the successive minima. By Theorem 1.12, this guarantees the existence of reduced bases in any normed space.

Corollary 1.13. *Every lattice admits a reduced basis.*

1.2. **Reduceness criteria.** In this section we define a reduction map, which leads 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 $E_{\le r} \supset E_{<r}$ are A_∞-submodules of E such that $\mathfrak{m}_\infty E_{\le r} \subset E_{<r}$. Their quotient,

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

is a k-vector space, admitting a kind of *reduction map*:

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

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

Definition 1.14. *For any $\mathcal{B} \subset E \setminus \{0\}$ and $\rho \in \mathbb{R}/\mathbb{Z}$, we denote*

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

Lemma 1.15. *Let $\mathcal{B} = (b_1, \dots, b_n)$ 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 $I=\{\rho\in\mathbb{R}/\mathbb{Z}\mid \mathcal{B}_\rho\ne\emptyset\}$. We have $E=\bigoplus_{\rho\in I}E_\rho$, where E_ρ is the subspace of E generated by $\mathcal{B}_\rho$. Take $a_1,\dots,a_n\in K$ and let $x=\sum_{i=1}^n a_ib_i$. This element splits as $x=\sum_{\rho\in I}x_\rho$, where $x_\rho=\sum_{b_i\in\mathcal{B}_\rho}a_ib_i$. Since all values $\|x_\rho\|$ are different (because $\|a_ib_i\|\equiv\|b_i\| \bmod \mathbb{Z}$), we have $\|x\|=\max_{\rho\in I}\{\|x_\rho\|\}$. On the other hand, since all $\mathcal{B}_\rho$ are reduced, we have $\|x_\rho\|=\max_{b_i\in\mathcal{B}_\rho}\{\|a_ib_i\|\}$. Thus, $\mathcal{B}$ is reduced. □

Definition 1.16. *For $a\in A_\infty$, consider the series expansion of a with respect to the local parameter t^{-1} at P_∞:*

$$a=\sum_{i=0}^{\infty}\lambda_i\,t^{-i},\qquad \lambda_i\in k.$$

We define the zero coefficient *of a as $\operatorname{zc}(a)=\lambda_0\in k$. It is uniquely determined by the condition $|a-\operatorname{zc}(a)|<0$. Clearly, $\operatorname{zc}(a)=0$ if and only if $a\in\mathfrak{m}_\infty$.*

The next result is inspired by a criterion of W.M. Schmidt [16, 17], which was developed in the context of Puiseux expansions of functions in function fields.

Theorem 1.17. *Let $\mathcal{B}$ 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 $\mathbb{Z}$. For each $\mathcal{B}_\rho\ne\emptyset$, 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 $\{\operatorname{red}_r(t^{m_b}b)\mid b\in\mathcal{B}_\rho\}\subset V_r$ are k-linearly independent for all $\mathcal{B}_\rho\ne\emptyset$.

Proof. By Lemma 1.15 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 1.8, $\mathcal{B}$ is reduced if and only if $\{t^{m_b}b\mid b\in\mathcal{B}\}$ is reduced. Thus, we may assume that $\|b\|=r$ for all $b\in\mathcal{B}$.

Let $(a_b)_{b\in\mathcal{B}}$ a family of elements in K, not all of them equal to zero. By multiplying these elements by the same (adequate) power of t we may assume that $\max\{|a_b|\}=0$, so that $\max\{\|a_bb\|\}=r$. Let $\mathcal{C}=\{b\in\mathcal{B}\mid |a_b|=0\}$. Clearly,

$$\Big\|\sum_{b\in\mathcal{B}}a_bb\Big\|=r\iff\Big\|\sum_{b\in\mathcal{C}}a_bb\Big\|=r\iff\Big\|\sum_{b\in\mathcal{C}}\operatorname{zc}(a_b)b\Big\|=r$$

$$\iff\operatorname{red}_r\left(\sum_{b\in\mathcal{C}}\operatorname{zc}(a_b)b\right)\ne0\iff\sum_{b\in\mathcal{C}}\operatorname{zc}(a_b)\operatorname{red}_r(b)\ne0.$$

Hence, the condition (2) of reduceness, for all families $(a_b)_{b\in\mathcal{B}}$ in K, is equivalent to $\{\operatorname{red}_r(b)\mid b\in\mathcal{B}\}$ being k-linearly independent. □

Corollary 1.18. *With the above notation, $(\operatorname{red}_r(t^{m_b}b)\mid b\in\mathcal{B}_\rho)$ is a k-basis of V_r. In particular, it holds $\dim_k V_r=\#\mathcal{B}_\rho$.*

Proof. By the previous theorem, this family is k-linearly independent. Let us show that it generates V_r as well. As in the proof of the theorem, we may assume that $\|b\|=r$ for all $b\in\mathcal{B}_\rho$.

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, we deduce

$$r = \|x\| = \max_{b\in\mathcal{B}}\{\|a_b b\|\} = \max_{b\in\mathcal{B}_\rho}\{\|a_b b\|\} = r + \max_{b\in\mathcal{B}_\rho}\{|a_b|\}.$$

Hence, $|a_b| \le 0$ for all $b \in \mathcal{B}_\rho$ and $\mathcal{C} := \{b \in \mathcal{B}_\rho \mid |a_b| = 0\} \ne \emptyset$. Clearly, $x \in \sum_{b\in\mathcal{C}} \mathrm{zc}(a_b)b + E_{<r}$, and $\mathrm{red}_r(x)$ is a k-linear combination of $\{\mathrm{red}_r(b) \mid b \in \mathcal{C}\}$. □

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

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

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

Lemma 1.19. *All lattices $L \subset E$ in a normed space have the same multiset $\overline{\mathrm{sm}}(L)$. We denote by $\mathrm{sm}(E)$ this common multiset*

Proof. By Corollary 1.13 there exists a reduced basis $\mathcal{B} = (b_1, \dots, b_n)$ of any lattice L in E. By Proposition 1.10, the underlying set of $\overline{\mathrm{sm}}(L)$ is the signature of E, which depends only on E. Finally, for each $\rho \in \mathbb{R}/\mathbb{Z}$, the multiplicity of ρ as an element of the multiset $\overline{\mathrm{sm}}(L)$ is the cardinality of the set $\mathcal{B}_\rho$. By Corollary 1.18 this multiplicity $\#\mathcal{B}_\rho$ is also independent of L. □

Corollary 1.20. *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. From $\mathrm{Aut}_A(A) = k^*$ and $\mathrm{Aut}_K(K) = K^*$, we deduce immediately:

$$\mathcal{O}(r) \text{ isometric to } \mathcal{O}(r') \iff r = r'$$
$$\mathcal{K}(r) \text{ isometric to } \mathcal{K}(r') \iff r + \mathbb{Z} = r' + \mathbb{Z},$$

for any given real numbers $r, r' \in \mathbb{R}$. The corollary follows from the existence of reduced bases and Lemma 1.9. □

1.3. **Orthonormal bases and isometry group.**

Definition 1.21. *Let E be a normed space and $\mathcal{B} = (b_1, \dots, b_n)$ a reduced basis of E. We say that $\mathcal{B}$ is* orthonormal *if $-1 < \|b_1\| \le \cdots \le \|b_n\| \le 0$.*

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 1.22. *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 *of the normed space $(E, \|\ \|)$.*

Lemma 1.23. *Every morphism of normed spaces is injective and maps a reduced set to a reduced one.*

Proof. A length-preserving map is injective because it must have a trivial kernel. Also, it clearly preserves condition (2) from Definition 1.7. □

Lemma 1.24. *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 1.23, and the second one implies trivially the third one.

We show that that that (3) implies (1). Since φ maps an orthonormal basis $\mathcal{B} = (b_1, \dots, b_n)$ 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

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

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

$$\|x\| = \max_{1\leq i\leq n} \{\|a_i b_i\|\} = \max_{1\leq i\leq n} \{\|a_i \varphi(b_i)\|'\} = \Big\| \sum_{i=1}^n a_i \varphi(b_i) \Big\|' = \|\varphi(x)\|',$$

so that φ preserves lengths. ☐

Theorem 1.25. *For* $r \in \mathbb{R}$ *it holds* $\mathrm{Aut}(\mathcal{K}^n(r)) = \mathrm{GL}_n(A_\infty)$*.*

Proof. Let us first take $r = 0$. Recall that $\mathcal{K}^n = (K^n, \| \ \|)$ with $\|(a_1, \dots, a_n)\| = \max_{1\leq i\leq n}\{|a_i|\}$. Let $(e_1, \dots, e_n)$ be the standard basis of K^n, which is an orthonormal basis of $\mathcal{K}^n$. By Lemma 1.24, for $T \in \mathrm{GL}_n(K)$ the map $T : K^n \to K^n$ is an isometry if and only if $(e_1T, \dots, e_nT)$ is an orthonormal basis. In particular, the rows of T have length 0, so that $T \in \mathrm{GL}_n(K) \cap A_\infty^{n\times n}$. By Theorem 1.17, the rows of T are reduced if and only if they are linearly independent $\bmod \mathfrak{m}_\infty^n$. Clearly, this holds if and only if $\det T \notin \mathfrak{m}_\infty$. Thus, T is an isometry if and only if $T \in \mathrm{GL}_n(A_\infty)$.

The general case follows from the same argument, 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 K^n. ☐

Definition 1.26. *Let* $n = m_1 + \cdots + m_\kappa$ *be a partition of a positive integer* n *into a sum of positive integers. Let* T *be an* $n \times n$ *matrix with entries in* A_∞*. The partition of* n *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 $O(m_1, \dots, m_\kappa, A_\infty)$ *is the subgroup of* $\mathrm{GL}_n(A_\infty)$ *formed by all* $T \in A_\infty^{n\times n}$*, 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 1.27. *Let* $-1 < r_1 < \cdots < r_\kappa \leq 0$ *be a sequence of real numbers. Then, for* $m_1, \dots, m_\kappa \in \mathbb{Z}_{>0}$ *it holds*

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

Proof. For $1 \leq i \leq \kappa$, let $n_i = m_1 + \cdots + m_i$ and $n = n_\kappa$. Let $E = \perp_{i=1}^{\kappa} \mathcal{K}^{m_i}(r_i)$ and denote by $\| \ \|$ the norm on E; that is,

$$\|(a_1, \dots, a_n)\| = \max\left\{|a_j| + r_{i_j} \mid 1 \leq j \leq n, \ n_{i_j} < j \leq n_{i_j+1}\right\}. \tag{5}$$

Let $e_1, \dots, e_n$ be the standard basis of K^n, which is an orthonormal basis of E. By Lemma 1.24, $\mathrm{Aut}(E)$ 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 $O(m_1, \dots, m_\kappa, A_\infty)$. 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) $b_l = (b_{1,l}, \ldots, b_{n,l}) \in A_\infty^{n_i} \times \mathfrak{m}_\infty^{n-n_i}$, for all $1 \le l \le m_i$.
(2) $Q := (b_{j,l} \mid 1 \le l \le m_i,\ n_{i-1} < j \le n_i) \in \mathrm{GL}_{m_i}(A_\infty)$.

The statement of the theorem follows immediately from the claim. In fact, for any $T \in \mathrm{GL}_n(K)$, Theorem 1.17 shows 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 $T \in O(m_1, \ldots, m_\kappa, A_\infty)$.

We have to prove the claim. By (5), $\|b_l\| \le r_i$, for $1 \le l \le m_i$, is equivalent to item (1) of the claim, since $-1 < r_1 < \cdots < r_\kappa \le 0$.

Note that $b_{j,l} e_j \in E_{<r_i}$, for all $1 \le j \le n_{i-1}$ (because $|b_{j,l}| \le 0$, $\|e_j\| < r_i$) and for all $n_i < j \le n$ (because $|b_{j,l}| \le -1$, $\|e_j\| < r_i + 1$). Thus,

$$b_l = \sum_{j=1}^{n} b_{j,l} e_j \in \sum_{j=n_{i-1}+1}^{n_i} \mathrm{zc}(b_{j,l}) e_j + E_{<r_i}, \quad 1 \le l \le m_i.$$

Clearly, $\mathrm{red}_{r_i}(b_1), \ldots, \mathrm{red}_{r_i}(b_{m_i})$ are k-linearly independent if and only if the matrix $(\mathrm{zc}(b_{j,l})_{1 \le l \le m_i,\, n_{i-1} < j \le n_i})$ belongs to $\mathrm{GL}_{m_i}(k)$. This is equivalent to $Q \in \mathrm{GL}_{m_i}(A_\infty)$ and $\|b_l\| = r_i$ for $1 \le l \le m_i$. This ends 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 1.9), Theorem 1.27 reveals the general structure of $\mathrm{Aut}(E, \|\ \|)$.

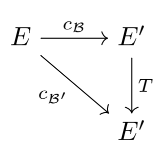
Let $\mathcal{B} = (b_1, \ldots, b_n)$ and $\mathcal{B}' = (b'_1, \ldots, b'_n)$ be two bases of E. The *transition matrix* from $\mathcal{B}$ to $\mathcal{B}'$ is the unique matrix $T = T(\mathcal{B} \to \mathcal{B}') \in \mathrm{GL}_n(K)$ such that

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

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

Lemma 1.28. *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. Let $E' := \perp_{i=1}^{\kappa} \mathcal{K}^{m_i}(r_i)$, 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:



By Lemma 1.9, $c_{\mathcal{B}'}$ is an isometry. Hence, T is an isometry if and only if $c_{\mathcal{B}}$ is an isometry. By Theorem 1.27, T is an isometry if and only if $T \in O(m_1, \ldots, m_\kappa, A_\infty)$. By Lemma 1.24, $c_{\mathcal{B}}$ is an isometry if and only if $\mathcal{B}$ is an orthonormal basis. □

1.4. **Determinant and orthogonal defect.**

Definition 1.29 (Volume)**.** *Let $\mathcal{B}$ be a basis of a normed space E. We define the* volume *of $\mathcal{B}$ as* $\operatorname{vol}(\mathcal{B}) := \sum_{b\in\mathcal{B}} \|b\|$.

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* $\operatorname{vol}(E)$ *and* $\operatorname{vol}(L)$*, respectively.*

Definition 1.30 (Determinant)**.** *Let $\mathcal{B}$ be a basis of a normed space E. We define the* determinant $d(\mathcal{B})$ *of $\mathcal{B}$ to be the fractional ideal of A generated by the determinant of the transition matrix from $\mathcal{B}$ to an orthonormal basis of E.*

The determinant $d(L)$ *of a lattice L is defined to be the determinant of any basis of L.*

By Lemma 1.28 the definition of the determinant is independent of the choice of the orthonormal basis of E.

For $h \in K$, we set $|hA| := |h|$ in order to extend the degree function $|\ |$ to fractional ideals of A.

Lemma 1.31 (Hadamard's inequality)**.** *Let $\mathcal{B}$ be a basis of E. Then,*

$$|d(\mathcal{B})| \le \operatorname{vol}(\mathcal{B}) - \operatorname{vol}(E).$$

Proof. Let $\mathcal{B} = (b_1, \dots, b_n)$ and let $\mathcal{B}' = (b'_1, \dots, b'_n)$ 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 $1 \le i, j \le n$, we have

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

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

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

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

Definition 1.32 (Orthogonal defect)**.** *The difference*

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

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

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

Lemma 1.33. *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*

$$\|a_i b_i\| \le \|x\| + \operatorname{OD}(\mathcal{B}), \ \text{for all } 1 \le i \le n. \tag{6}$$

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

If $a_i = 0$ the inequality (6) is obvious. Suppose $a_i \ne 0$. By Cramer's rule, we have $a_i = \det T' / \det T$, where T' is the transition matrix from the basis $b_1, \dots, b_{i-1}, x, b_{i+1}, \dots, b_n$ to $\mathcal{B}'$. By Hadamard's inequality, we get

$$|\det T'| \le \sum_{j\ne i} \|b_j\| + \|x\| - \operatorname{vol}(E).$$

Hence,

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

□

Theorem 1.34. *A basis $\mathcal{B}$ is reduced if and only if* $\mathrm{OD}(\mathcal{B}) = 0$.
In this case, $|d(\mathcal{B})| = \sum_{b\in\mathcal{B}} \lceil \|b\| \rceil$.

Proof. If $\mathrm{OD}(\mathcal{B}) = 0$, the lemma above shows that $\mathcal{B}$ is reduced.

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

$$\mathrm{vol}(\mathcal{B}') = m + \mathrm{vol}(\mathcal{B}), \quad 0 = |d(\mathcal{B}')| = m + |d(\mathcal{B})|.$$

Therefore, $\mathrm{OD}(\mathcal{B}) = \mathrm{OD}(\mathcal{B}') = 0$, and $|d(\mathcal{B})| = -m$. □

2. Reduction algorithm

A reduction algorithm 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 [14, 11, 17, 20]. 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. The reduction algorithm is based on an iterated performance of a reduction step.

Definition 2.1 (Reduction step)**.** *Let $\mathcal{B}$ be a basis of a normed space $(E, \|\ \|)$. A reduction step is a replacement of some $b \in \mathcal{B}$ by $\tilde{b} = b + \alpha$, for some A-linear combination α of $\mathcal{B} \setminus \{b\}$ such that $\|\tilde{b}\| < \|b\|$.*

Clearly, $(\mathcal{B} \setminus \{b\}) \cup \{\tilde{b}\}$ is still a basis of the lattice $L = \langle \mathcal{B} \rangle_A$. 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 $OD(\mathcal{B}) = \mathrm{vol}(\mathcal{B}) - \mathrm{vol}(E) - |d(\mathcal{B})|$ is bounded by 0 from below, after a finite number of reduction steps we obtain a reduced basis of L by Theorem 1.34 and Corollary 1.11.

In practice, we work out this problem by using coordinates with respect to an orthonormal basis of E. We have then an explicit isometry between E and the normed space $\perp_{i=1}^n \mathcal{K}(r_i)$, where $-1 < r_1 \leq r_2 \leq \cdots \leq r_n \leq 0$ are the lengths of the given orthonormal basis of E. Hence, we may assume that $E = \perp_{i=1}^n \mathcal{K}(r_i)$.

The initial basis $\mathcal{B}$ is given by the rows of some $T \in \mathrm{GL}_n(K)$, and the reduction algorithm finds $R \in \mathrm{GL}_n(A)$ such that the rows of RT are a reduced basis $\widetilde{\mathcal{B}}$. The matrix $R = T(\widetilde{\mathcal{B}} \to \mathcal{B})$ is obtained as a product, $R = R_m \cdot R_{m-1} \cdots R_1$, where each R_i represents the concatenation of several reduction steps.

2.1. The case $\#\,\mathrm{Sig}(E) = 1$.

Let $E = \mathcal{K}^n(r)$ for some $-1 < r \leq 0$, with norm:

$$\|(a_1, \ldots, a_n)\| = \max_{1\leq i\leq n} \{|a_i|\} + r.$$

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 exist several descriptions of a reduction algorithm for this particular normed space [11, 14], we review it in the case $r \neq 0$, in regard to its generalization to arbitrary normed spaces.

The standard basis $(e_1,\dots,e_n)$ of K^n is an orthonormal basis of E. A vector $(a_1,\dots,a_n)=\sum_{i=1}^n a_ie_i$ belongs to $E_{\le r}$ if and only if $|a_i|\le 0$ for all i. Hence, Corollary 1.18 shows that $(\operatorname{red}_r(e_1),\dots,\operatorname{red}_r(e_n))$ is a k-basis of $V_r=E_{\le r}/E_{<r}$, and the choice of this basis determines a k-linear isomorphism:

$$V_r\longrightarrow k^n,\quad \operatorname{red}_r(a_1,\dots,a_n)\ \mapsto\ \bigl(\operatorname{zc}(a_1),\dots,\operatorname{zc}(a_n)\bigr).$$

Therefore, Theorem 1.17 provides a comfortable criterion to decide whether a basis of E is reduced or not.

Corollary 2.2. *A basis $(b_1,\dots,b_n)$ of E is reduced if and only if the matrix*

$$\left(\operatorname{zc}\left(t^{-\lceil\|b_i\|\rceil}b_{i,j}\right)\right)_{1\le i,j\le n}\in k^{n\times n}$$

has rank n, where $b_i=(b_{i1},\dots,b_{in})$ for $1\le i\le n$.

Example 2.3. 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, $\|b_1\|=1$ and $\|b_2\|=7$. We consider

$$M=\begin{pmatrix}\operatorname{zc}\left(\frac{2t+1}{t}\right) & \operatorname{zc}\left(\frac{1}{t}\right)\\ \operatorname{zc}\left(\frac{t^7+2}{t^7}\right) & \operatorname{zc}\left(\frac{2}{t}\right)\end{pmatrix}=\begin{pmatrix}2&0\\1&0\end{pmatrix}\in\mathbb{Q}^{2\times 2}.$$

Since $\operatorname{rank}(M)<2$, Corollary 2.2 shows that the basis $\mathcal{B}$ is not reduced.

Let us describe a concrete procedure to perform the reduction steps.

We order by increasing length the vectors $b_1,\dots,b_n$ of the input basis $\mathcal{B}$. For $1\le i\le n$, let $b_i=(b_{i1},\dots,b_{in})$. We transform the matrix

$$M=\left(\operatorname{zc}(t^{-\lceil\|b_i\|\rceil}b_{i,j})\right)_{1\le i,j\le n}\in k^{n\times n},$$

into row echelon form, $M'=PM$, with $P=(p_{i,j})$ belonging to the set $\operatorname{LT}_n(k)$ of lower triangular matrices with diagonal entries equal to 1, up to a permutation of its rows. For commodity of the reader, we discuss only the case where 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. This corresponds to non-trivial expressions of the zero vector in V_r as k-linear combinations of $\operatorname{red}_r(t^{-\lceil\|b_1\|\rceil}b_1),\dots,\operatorname{red}_r(t^{-\lceil\|b_n\|\rceil}b_n)$.

Let $m=\operatorname{rank}(M)$. Let $P_1,\dots,P_n$ be the rows of P, and consider the lower triangular matrix P' with rows $P'_1,\dots,P'_n$ defined by

$$P'_j=\begin{cases}e_j, & \text{if } j\le m,\\ P_j=(p_{j,1}\cdots p_{j,j-1}\ p_{j,j}=1\ 0\cdots 0), & \text{if } j>m.\end{cases}$$

For $1\le j\le m$ we take $\tilde{b}_j=b_j$ while for $m<j\le n$ we consider

$$\tilde{b}_j=\sum_{i<j}p_{j,i}t^{\lceil\|b_j\|\rceil-\lceil\|b_i\|\rceil}b_i+b_j. \tag{7}$$

The family $\tilde{\mathcal{B}}=(\tilde{b}_1,\dots,\tilde{b}_n)$ is a basis of the lattice $\langle\,\mathcal{B}\,\rangle_A$, and the transition matrix $R=T(\widetilde{\mathcal{B}}\to\mathcal{B})$ is given by

$$R=\operatorname{diag}(t^{\lceil\|b_1\|\rceil},\dots,t^{\lceil\|b_n\|\rceil})\cdot P'\cdot\operatorname{diag}(t^{-\lceil\|b_1\|\rceil},\dots,t^{-\lceil\|b_n\|\rceil}). \tag{8}$$

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

By construction, $\mathrm{red}_r(t^{-\lceil \|b_j\| \rceil}\tilde{b}_j) = 0$, so that $\|\tilde{b}_j\| < \|b_j\|$ and (7) is a reduction step. Thus, this procedure performs $n - \mathrm{rank}(M)$ reduction steps at once.

Example 2.4. We consider Example 2.3 again. For the matrices

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

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

$$R = \mathrm{diag}(t, t^7) \cdot P \cdot \mathrm{diag}(t^{-1}, t^{-7}) = \begin{pmatrix} 1 & 0 \\ -\frac{t^6}{2} & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}[t])$$

realizes a reduction step $(\tilde{b}_1\ \tilde{b}_2)^{\mathrm{tr}} = R \cdot (b_1\ b_2)^{\mathrm{tr}}$. We get

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

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

$$\left(\mathrm{zc}(t^{-\lceil \|\tilde{b}_i\| \rceil} \tilde{b}_{i,j}) \right)_{1 \leq i,j \leq 2} = \begin{pmatrix} \mathrm{zc}\left(\frac{2t+1}{t}\right) & \mathrm{zc}\left(\frac{1}{t}\right) \\ \mathrm{zc}\left(-\frac{1}{2} + \frac{2}{t^6}\right) & \mathrm{zc}(\frac{3}{2}) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ -\frac{1}{2} & \frac{3}{2} \end{pmatrix}.$$

Since this matrix has rank 2, the basis $(\tilde{b}_1, \tilde{b}_2)$ is reduced by Corollary 2.2.

The algorithm. The initial basis is given by the rows $T_1, \ldots, T_n$ of a matrix $T \in \mathrm{GL}_n(K)$. We may always assume that T has polynomial entries. 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 $s_i = r_i - |g_i|$. The isometry

$$\perp_{i=1}^n \mathcal{K}(r_i) \longrightarrow \perp_{i=1}^n \mathcal{K}(s_i), \quad (a_1, \ldots, a_n) \mapsto (a_1 g_1, \ldots, a_n g_n)$$

sends the lattice generated by the rows of T to the lattice generated by the rows of $T\,\mathrm{diag}(g_1, \ldots, g_n)$, which has polynomial entries.

Algorithm 1 : Basis reduction for $E = \mathcal{K}^n(r)$

Require: $T \in \mathrm{GL}_n(K) \cap A^{n \times n}$.
Ensure: Reduced basis of the lattice generated by the rows of T.

$s \leftarrow 1$
while $s < n$ **do**
  Sort rows of T increasingly ordered w.r.t. $\| \ \|$
  $M \leftarrow (\mathrm{zc}(t^{-\lceil \|T_i\| \rceil} t_{i,j}))_{1 \leq i,j \leq n} \in k^{n \times n}$
  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 $i = s+1, \ldots, n$ **do**
      $u_i \leftarrow \max\{1 \leq j \leq n \mid p_{i,j} \neq 0\}$
      $T_{u_i} \leftarrow T_{u_i} + \sum_{j=1}^{u_i - 1} t^{\lceil \|T_{u_i}\| \rceil - \lceil \|T_j\| \rceil} \cdot p_{i,j} T_j$
    end for
  end if
end while
return T

2.2. **The general case.** Let $E = \perp_{l=1}^{\kappa} \mathcal{K}^{m_l}(r_l)$ for some $-1 < r_1 < \cdots < r_\kappa \le 0$. For all $1 \le l \le \kappa$, denote $n_k = m_1 + \cdots + m_l$, and let $n = n_\kappa = \dim E$.

The standard basis $(e_1, \dots, e_n)$ of K^n is an orthonormal basis of E. By Corollary 1.18, the vectors $(\mathrm{red}_{r_l}(e_j))_{n_{l-1} < j \le n_l}$ are a basis of V_{r_l} for each $1 \le l \le \kappa$. The choice of this basis yields a k-linear isomorphism:

$$V_{r_l} \longrightarrow k^{m_l}, \quad \mathrm{red}_{r_l}(t^{-\lceil \|b\| \rceil} b) \;\mapsto\; (\mathrm{zc}(t^{-\lceil \|b\| \rceil} a_j))_{n_{l-1} < j \le n_l},$$

where $b = (a_1, \dots, a_n) \in K^n$ has length $\|b\| \equiv r_l \pmod{\mathbb{Z}}$.

Therefore, we can reinterpret Theorem 1.17 as follows:

Corollary 2.5. *Let $\mathcal{B} = (b_1, \dots, b_n)$ be a basis of E ordered by increasing length, with $b_i = (b_{i,1}, \dots, b_{i,n}) \in K^n$ for all i. The basis $\mathcal{B}$ is reduced if and only if for all $1 \le l \le \kappa$ the following matrix has rank m_l:*

$$M_{r_l} := \left(\mathrm{zc}(t^{-\lceil \|b_i\| \rceil} b_{i,j})\right)_{i \in I_{\mathcal{B}}(r_l),\, n_{l-1} < j \le n_l},$$

where $I_{\mathcal{B}}(r_l) = \{1 \le i \le n \mid \|b_i\| \equiv r_l \bmod \mathbb{Z}\}$.

The algorithm. The initial basis $\mathcal{B}$ is given by the rows $T_1, \dots, T_n$ of a matrix $T \in \mathrm{GL}_n(K)$. As argued for Algorithm 1, we may always assume that T has polynomial entries.

We split the basis $\mathcal{B}$ of E into subsets $\mathcal{B}_r = \{b \in \mathcal{B} \mid \|b\| \equiv r \bmod \mathbb{Z}\}$ for any $r \in \{r_1, \dots, r_\kappa\}$, and apply for each of these subsets reduction steps as we did in Algorithm 1. Unfortunately, the length of a reduced vector $b + \alpha$ may not lie 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 2 Basis reduction for $E = \perp_{l=1}^{\kappa} \mathcal{K}^{m_l}(r_l)$

Require: $T \in \mathrm{GL}_n(K) \cap A^{n\times n}$.
Ensure: Reduced basis of the lattice generated by the rows of T.

1: vals $\leftarrow [r_1, \dots, r_\kappa]$
2: $\iota \leftarrow 1$
3: **while** $\iota \leq \#\mathrm{vals}$ **do**
4: $\mathcal{B}\mathrm{vals} \leftarrow [\|T_1\|, \dots, \|T_n\|]$
5: Sort $\mathcal{B}$vals increasingly ordered and apply changes to the rows of T
6: Determine $1 \leq l \leq \kappa$ with $\mathrm{vals}[\iota] \equiv r_l \bmod \mathbb{Z}$
7: Determine all $1 \leq e_1, \dots, e_f \leq n$ with $\mathcal{B}\mathrm{vals}[e_i] \equiv \mathrm{vals}[l] \bmod \mathbb{Z}$
8: $M \leftarrow (\mathrm{zc}(t^{-\lceil \mathcal{B}\mathrm{vals}[e_i]\rceil} t_{e_i,j}))_{1\leq i\leq f, n_{l-1}<j\leq n_l} \in k^{f\times m_l}$
9: Compute $P = (p_{i,j}) \in \mathrm{LT}_f(k)$ s.t. $M' := PM$ is in row echelon form
10: $s \leftarrow \mathrm{rank}(M')$
11: **if** $s = f$ **then**
12: **if** $f < m_l$ and $\mathrm{vals}[\iota] \notin \{\mathrm{vals}[s] \mid s > \iota\}$ **then**
13: Append(vals, vals[ι])
14: **end if**
15: **else**
16: **for** $i = s+1, \dots, f$ **do**
17: $u_i \leftarrow \max\{1 \leq j \leq f \mid p_{i,j} \neq 0\}$
18: $T_{e_{u_i}} \leftarrow T_{e_{u_i}} + \sum_{j=1}^{u_i-1} t^{\lceil \mathcal{B}\mathrm{vals}[e_{u_i}]\rceil - \lceil \mathcal{B}\mathrm{vals}[e_j]\rceil} p_{i,j} T_{e_j}$
19: $\mathcal{B}\mathrm{vals}[e_{u_i}] \leftarrow \|T_{e_{u_i}}\|$
20: **if** $\mathcal{B}\mathrm{vals}[e_{u_i}] - \lceil \mathcal{B}\mathrm{vals}[e_{u_i}]\rceil \notin \{\mathrm{vals}[s] \mid s > \iota\}$ **then**
21: Append(vals, $\mathcal{B}\mathrm{vals}[e_{u_i}] - \lceil \mathcal{B}\mathrm{vals}[e_{u_i}]\rceil$)
22: **end if**
23: **end for**
24: **end if**
25: $\iota \leftarrow \iota + 1$
26: **end while**
27: **return** T

Let us add some comments to clarify some parts of the algorithm.
Steps 12-14. If no reduction step can be a applied but the number of vectors in $\mathcal{B}$ of length r_l mod $\mathbb{Z}$ is lower than m_l, we have not found enough vectors in the set $\mathcal{B}_{r_l}$. Later, there will occur (after several reduction steps) new vectors with length r_l modulo $\mathbb{Z}$. Therefore, we must reconsider the value $r_l = \mathrm{vals}[\iota]$ afterwards.
Steps 20-22. If 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.

Remark 2.6. *By Proposition 1.10, 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 1.10 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 2 can also be adapted to compute these objects.

Let us illustrate the algorithm with an example.

Example 2.7. 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

$$E = \mathcal{K}(-1/2) \perp \mathcal{K}(-1/3) \perp \mathcal{K}(-1/4).$$

We have $r_1 = -1/2$, $r_2 = -1/3$, and $r_3 = -1/4$ with multiplicities $m_l = 1$ for $1 \le l \le 3$. Consider the following basis $\mathcal{B} = (b_1, b_2, b_3)$ of E:

$$b_1 = \left(t^2, t^2+1, 0\right), \quad b_2 = \left(t(t^2+1), t, t^4+1\right), \quad b_3 = \left(0, t^4(t+1), t^4\right).$$

The norm on E is given by $\|(a_1, a_2, a_3)\| = \max\{|a_1| - 1/2, |a_2| - 1/3, |a_3| - 1/4\}$; hence, $\|b_1\| = 5/3$, $\|b_2\| = 15/4$ and $\|b_3\| = 14/3$.

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 focussing our attention on the set $\mathcal{B}_{r_2} = \{b_1, b_3\}$. We consider

$$M_{r_2} = \begin{pmatrix} \operatorname{zc}\left(t^{-\lceil 5/3 \rceil}(t^2+1)\right) \\ \operatorname{zc}\left(t^{-\lceil 14/3 \rceil} t^4 (t+1)\right) \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in \mathbb{F}_3^{2\times 1}$$

and transform M_{r_2} into row echelon form, $PM_{r_2} = M'$, with

$$P = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \quad M' = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

We perform the reduction step $(\tilde{b}_1 \ \tilde{b}_3)^{\mathrm{tr}} = R \cdot (b_1 \ b_3)^{\mathrm{tr}}$ with the transition matrix R defined as in (8):

$$R = \operatorname{diag}(t^2, t^5) \cdot P \cdot \operatorname{diag}(t^{-2}, t^{-5}) = \begin{pmatrix} 1 & 0 \\ 2t^3 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_3[t]).$$

We obtain $\tilde{b}_1 = b_1$ and $\widetilde{b_3} = 2t^3 \cdot b_1 + b_3 = \left(2t^5, t^3(t+2), t^4\right)$, with $\|\tilde{b}_3\| = 7/2$. Note that $\tilde{b}_3$ and b_3 do not have the same length modulo $\mathbb{Z}$.

The basis $(\tilde{b}_1, b_2, \tilde{b}_3)$ is reduced, since $\|\tilde{b}_1\|, \|b_2\|, \|\tilde{b}_3\|$ are different modulo $\mathbb{Z}$.

2.3. **Complexity.** We are interested in the complexity of Algorithms 1 and 2. All estimations are expressed in the number of necessary operations in k. Recall that $\operatorname{Sig}(E)$ denotes the set of different lengths modulo $\mathbb{Z}$ of all nonzero vectors in the normed space $(E, \| \ \|)$.

Lemma 2.8. *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*

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

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

$$b = b^{(0)} \to b^{(1)} \to \cdots \to b^{(\kappa)} \tag{9}$$

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

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

Definition 2.9. *For $g = f/h \in K$, with coprime polynomials $f, h \in A$, 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*

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

The next lemma presents some properties of the height, which will be useful for the complexity analyses of subsequent algorithms.

Lemma 2.10. *Let $T, T' \in K^{n\times n}$.*

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

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

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

This shows that $\pm|\det(T)| \leq nh(T)$; thus, $|\det(T^{-1})| = -|\det(T)| \leq nh(T)$.

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, $h(s_{i,j}) = \max\{|\det(T_{j,i})|, |\det(T)|\} \leq nh(T)$. □

Lemma 2.11. *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,

$$OD(\mathcal{B}) = \sum_{i=1}^{n} \|b_i\| - \mathrm{vol}(E) - |\det(T)|. \tag{10}$$

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, $-|\det(T)| \leq nh(T)$ by item (2) from Lemma 2.10. Therefore, from (10) we deduce $OD(\mathcal{B}) < nh(T) + n + nh(T) = n(2h(T) + 1)$. □

Lemma 2.12. *Let $\mathcal{B}'$ be an orthonormal basis of an n-dimensional normed space $(E, \| \ \|)$ and let $\mathcal{B}$ be a basis of E such that the transition matrix $T = T(\mathcal{B} \to \mathcal{B}')$ has polynomial entries. Then, Algorithm 2 takes at most*

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

arithmetic operations in k to transform $\mathcal{B}$ into a reduced basis.

Proof. By any reduction step in Algorithm 2 the value $OD(\mathcal{B})$ is decreased strictly. If $\kappa = \#\operatorname{Sig}(E)$, according to Lemma 2.8 and Theorem 1.34, the set $\mathcal{B}$ is reduced after at most $\lfloor OD(\mathcal{B}) \rfloor \kappa + (\kappa - 1)n$ steps.

Clearly, the runtime of the algorithm is dominated by the transformation of matrices into row echelon form and the realization of reduction steps.

At first we analyze the complexity of the transformation of matrices into row echelon form. Denote by $r_1, \dots, r_\kappa$ the different lengths of vectors in $\mathcal{B}'$ and $m_1, \dots, m_\kappa$ its multiplicities, so that $n = m_1 + \cdots + m_\kappa$. Suppose, that after $i - 1$ steps in Algorithm 2 we have transformed the basis $\mathcal{B}$ into $\mathcal{B}_i = (b_{i_1}, \dots, b_{i_n})$. We can split $\mathcal{B}_i$ into disjoint subsets

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

where $\mathcal{B}_{r_k} := \{b \in \mathcal{B}_i \mid \|b\| \equiv r_k \bmod \mathbb{Z}\}$, for $1 \le k \le \kappa$. Assume $\mathcal{B}_i$ is not reduced. By Corollary 2.5, for at least one r_k, the matrix $M_{r_k} \in k^{\# I_{\mathcal{B}_i}(r_k) \times m_k}$ has not full rank.

In the worst case, we have to transform all matrices $M_{r_1}, \dots, M_{r_\kappa}$ into row echelon form until we detect at least one reduction step (i.e. one zero row). The cost for transforming all M_{r_j}, $1 \le j \le \kappa$, into row echelon form is less than or equal to 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 [4]). Hence, the cost of all transformations of matrices into row echelon form along Algorithm 2 is bounded by $O((OD(\mathcal{B})\kappa + (\kappa - 1)n) \cdot n^3)$ operations in k. According to Lemma 2.11 the last complexity bound can be estimated by $O(\kappa n^4 h(T))$.

Additionally, we compute A-linear combinations of the rows of T (line 18 of Algorithm 2), 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 T is less or equal than before; that is, at any level the value of $h(T)$ 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 T as k-linear combinations.

The cost of any reduction step applied to the rows of T is $O(n^2 h(T))$ operations in k. Thus, the total cost of performing all reduction steps of Algorithm 2 is $O(\kappa n^3 h(T)^2)$. this ends the proof of the lemma. □

Remark 2.13. *If the transition matrix $T(\mathcal{B} \to \mathcal{B}')$ does not belong to $A^{n \times n}$, we must add the cost of finding the* lcm *of the entries of each column and the cost of multiplying by them to get rid of denominators. The total cost of the reduction algorithm is then $O\big(\#\operatorname{Sig}(E) \cdot n^4 \cdot h(T)^2\big)$ operations in k.*

In Subsection 2.5 we will present an optimized version of the reduction algorithm (cf. Lemma 2.26).

If $\#\operatorname{Sig}(E) = 1$, Algorithm 2 coincides with Algorithm 1. Hence, the complexity bounds for the latter follow immediately from Lemma 2.12.

Corollary 2.14. *For $r \in \mathbb{R}$, let $\mathcal{B} = (b_1, \dots, b_n)$ be a basis of the normed space $E = \mathcal{K}^n(r)$ such that $T = (b_1 \dots b_n)^{\mathrm{tr}}$ belongs to $A^{n\times n}$. Algorithm 1 takes $O(n^4 h(T) + n^3 h(T)^2)$ arithmetic operations in k to transform $\mathcal{B}$ into a reduced basis.*

In practice, the runtime of Algorithm 1 (and Algorithm 2) 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 1 is equal to $O(n^3 h(T)^2)$ operations in k. In this context, our reduction algorithm is one magnitude better than the reduction algorithms described in [11, 20] and its complexity coincides with the one in [14].

2.4. **Classes of lattices and semi-reduceness.** In the sequel 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 *semi-reduced basis* (cf. Definition 2.22) $\mathcal{B}$ of L, which "nearly" behaves as a reduced one.

To this end, we shall consider instead an integer-valued lattice $(L, \| \ \|')$, which almost coincides with $(L, \| \ \|)$. 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, a reduced basis $\mathcal{B}$ of $(L, \| \ \|')$ can be used as a precomputation for the reduction algorithm in order to determine a reduced basis of $(L, \| \ \|)$. In this way, the reduction algorithm can be accelerated.

Definition 2.15. *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. The* space of lattices *of E is defined to be*

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

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

Definition 2.16. *We say that two norms $\| \ \|$ and $\| \ \|'$ in* $\mathrm{Norm}(E)$ *are* equivalent, *and we write $\| \ \| \sim \| \ \|'$, if $\lceil \|z\| \rceil = \lceil \|z\|' \rceil$, for all $z \in E$.*

In this case, we write $(E, \| \ \|) \sim (E, \| \ \|')$ and $(L, \| \ \|) \sim (L, \| \ \|')$. We say too that these two normed spaces or lattices are equivalent.

The following results follow easily from the definitions.

Lemma 2.17. (1) *The relation $\sim$ is an equivalence relation on* $\mathrm{Norm}(E)$.

(2) *If $(E, \| \ \|)$ is a normed space, then $(E, \lceil \| \ \| \rceil)$ is a normed space.*

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

Definition 2.18. *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 2.19. *A basis $\mathcal{B}$ of $(E, \| \ \|)$ is semi-orthonormal if and only if*

$$\left\lceil \left\| \sum_{b \in \mathcal{B}} a_b b \right\| \right\rceil = \max_{b \in \mathcal{B}} \{ \lceil |a_b| \rceil \}, \text{ for all } a_b \in K. \tag{11}$$

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,

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

As $-1 < \|b\|' \le 0$, 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 (11) 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 2.20. *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 $\mathrm{GL}_n(A_\infty)$.*

Proof. 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 $\mathcal{B}'$. For an arbitrary $z \in E$ we write $z = \sum_{i=1}^n a_i b_i = \sum_{i=1}^n a'_i b'_i$, with coefficients in K such that $a'_i = \sum_{j=1}^n t_{j,i} a_j$. By (11), the equality

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

holds for all $z \in E$ if and only if $T \in \mathrm{Aut}(\mathcal{K}^n)$, and this group coincides with $\mathrm{GL}_n(A_\infty)$ by Theorem 1.25. □

Lemma-Definition 2.21. *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 2.19 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 2.20. □

Definition 2.22. *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. 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.

Lemma 2.23.

(1) *A basis $\mathcal{B}$ of a normed space $(E, \| \|)$ is semi-orthonormal if and only if $\mathcal{B}$ is semi-reduced with $-1 < \|b\| \le 0$, for all $b \in \mathcal{B}$.*
(2) *If $\mathcal{B} = (b_1, \dots, b_n)$ is semi-reduced, then $(t^{-\lceil \|b_1\| \rceil} b_1, \dots, t^{-\lceil \|b_n\| \rceil} b_n)$ is semi-orthonormal.*

(3) *If* $\| \ \| \sim \| \ \|'$*, then, any semi-reduced basis of* $(L, \| \ \|)$ *is a semi-reduced basis of* $(L, \| \ \|')$*.*

The next theorem summarizes all data shared by all lattices in the equivalence class of $(L, \| \ \|)$.

Theorem 2.24. *For* $i \in \{1, 2\}$*, denote by* $\mathcal{B}_i = (b_{1,i}, \dots, b_{n,i})$ *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* $1 \le i \le n$,
(3) $(L, \| \ \|_1)_{\le r} = (L, \| \ \|_2)_{\le r}$ *for all* $r \in \mathbb{Z}$*, and*
(4) $(E, \| \ \|_1)_{\le 0} = (E, \| \ \|_2)_{\le 0}$*, 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 1.10 is correct for a semi-reduced basis and an integer r. Thus,

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

By Lemma 2.23, the set $\mathcal{B}_1$ is also a semi-reduced basis of $(L, \| \ \|_2)$. Hence,

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

Since $\lceil \|z\|_1 \rceil = \lceil \|z\|_2 \rceil$ holds for all $z \in E$, we get $(L, \| \ \|_1)_{\le r} = (L, \| \ \|_2)_{\le r}$.

(3) ⇒ (2). Let $r_1 \le \cdots \le r_n$; $s_1 \le \cdots \le s_n$, with $r_i = \lceil \|b_{1,i}\| \rceil$, $s_i = \lceil \|b_{2,i}\| \rceil$. Assume that $r_1 = s_1, \dots, r_i = s_i$, but $r_{i+1} < s_{i+1}$. Then, Proposition 1.10 shows that $\dim_k (L, \| \ \|_1)_{\le s_{i+1}-1} \ne \dim_k (L, \| \ \|_2)_{\le s_{i+1}-1}$, wich contradicts (3).

(2) ⇒ (1). This implication follows immediately from the definitions.

Finally let us show that (1) ⇔ (4). By Theorem 2.20, (1) is equivalent to the fact that the transition matrices between semi-orthonormal bases of the two normed spaces belong to $\mathrm{GL}_n(A_\infty)$. By Lemma-Definition 2.21, this condition is equivalent to $(E, \| \ \|_1)_{\le 0} = (E, \| \ \|_2)_{\le 0}$. □

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 $(L, \| \ \|)_{\le r}$, for $r \in \mathbb{Z}$.

2.5. **Computation of (semi-) reduced bases.** Let $\mathcal{B}'$ be an orthonormal basis of $(E, \| \ \|)$ and L be a lattice in $(E, \| \ \|)$. In section 2 we already described an algorithm (cf. Algorithm 2), which computes a reduced basis of L. According to Lemma 2.12 the runtime of the computation of a reduced basis of L is minimal if $E \cong \mathcal{K}(r)^n$, i.e. $\#\,\mathrm{Sig}(E) = 1$.

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 2.17 and 2.23, 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 2. Clearly, $\mathcal{B}'$ is an orthonormal basis of $(E, \lceil \| \ \| \rceil)$ too; hence, we may consider $\mathcal{B}$ as a basis of $(E, \lceil \| \ \| \rceil)$ and call Algorithm 1 for $T = T(\mathcal{B} \to \mathcal{B}')$. This results in a semi-reduced basis $\mathcal{B}_{\mathrm{semi}}$ of $(L, \| \ \|)$. We will see that transforming $\mathcal{B}_{\mathrm{semi}}$ into a reduced basis $\mathcal{B}_{\mathrm{red}}$ of $(L, \| \ \|)$ by Algorithm 2 can be realized at minimal cost. We summarize the results by the following pseudocode:

Algorithm 3 : Basis reduction

Require: $\mathcal{B}'$ orthonormal basis of a normed space $(E, \|\ \|)$ and $\mathcal{B}$ a basis of E.
Ensure: Reduced basis of the lattice $L = \langle \mathcal{B} \rangle_A$.

1: $T_{\mathrm{semi}} \leftarrow$Algorithm 1$(T(\mathcal{B} \to \mathcal{B}'))$
2: $T_{\mathrm{red}} \leftarrow$Algorithm 2$(T_{\mathrm{semi}})$
3: **return** T_{red}, transition matrix from a reduced basis of L to $\mathcal{B}'$

Lemma 2.25. *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 $\mathcal{B} = (b_1, \dots, b_n)$ and consider a reduced basis $\mathcal{B}' = (b'_1, \dots, b'_n)$ of L. Assume that both bases are increasingly ordered with respect to the length of their vectors. By Theorem 1.34, we obtain $\mathrm{OD}(\mathcal{B}') = 0$, since $\mathcal{B}'$ is reduced. Hence, $\mathrm{vol}(\mathcal{B}') = \mathrm{vol}(E) + |d(L)|$. According to Theorem 2.24 we obtain $\lceil \|b_i\| \rceil = \lceil \|b'_i\| \rceil$ and therefore $\|b_i\| < \|b'_i\| + 1$, for $1 \le i \le n$. 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 2.8, 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. Having in mind that $\#\,\mathrm{Sig}(E) \le n$, Corollary 2.14 and the proof of Lemma 2.12 yield the following complexity estimation.

Lemma 2.26. *Let the notation be the same as in Lemma 2.12. Then, Algorithm 3 takes $O(n^4 h(T) + n^3 h(T)^2)$ arithmetic operations in k to transform $\mathcal{B}$ into a reduced basis. In particular, for $h(T) \ge n$ the complexity is equal to $O(n^3 h(T)^2)$.*

If we use Remark 2.13, we get an estimation of $O(n^4 h(T)(\#\,\mathrm{Sig}(E) + h(T))$ operations in k, if we do not assume that the input matrix has polynomial entries.

3. Lattices in algebraic function fields

Let F/k be an *algebraic function field* of one variable over the constant field k and let k_0 be the *full constant field*. That is, F/K is a separable extension of finite degree n and k_0 is the algebraic closure of k in F.

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. Such a representation exists for every algebraic function field over a perfect constant field [19, p. 128]. We consider $\theta \in F$ with $f(t, \theta) = 0$, so that $F = k(t, \theta)$. We call $A[\theta]$ the *finite equation order* of f, and we define

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

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 another 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* $A_\infty[\theta_\infty]$.

A *place* P of F/k is the maximal ideal of the valuation ring of a surjective valuation $v_P : F \to \mathbb{Z} \cup \{\infty\}$, which vanishes on 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 denote $\mathbb{P}_0(F) = \mathbb{P}_F \setminus \mathbb{P}_\infty(F)$ the set of "finite" places.

A *divisor* D of F/k is a formal finite $\mathbb{Z}$-linear combination of the places of F. The set $\mathcal{D}_F$ of all divisors of F/k is an abelian group. For a divisor $D = \sum_{P\in\mathbb{P}_F} a_P P$, we set $v_P(D) = a_P$. A partial ordering on $\mathcal{D}_F$ is defined by: $D_1 \le D_2$ if and only if $v_P(D_1) \le v_P(D_2)$ for all $P \in \mathbb{P}_F$.

Every $z \in F^*$ determines a *principal divisor* $(z) = \sum_{P\in\mathbb{P}_F} v_P(z)P$.

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

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

Instead of $\dim_k \mathcal{L}(D)$, we write $\dim_k D$.

In this section we will see that any divisor D in $\mathcal{D}_F$ induces a norm $\| \|_D$ and a normed space $(F, \| \|_D)$. Hence, the results for lattices become available in the context of algebraic function fields.

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. In [17] an algorithm is presented, which covers this problem 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 can be applied for arbitrary function fields and no series expansions are used.

Let $\mathcal{O}_F = \mathrm{Cl}(A, F)$ and $\mathcal{O}_{F,\infty} = \mathrm{Cl}(A_\infty, F)$ be the integral closures of A and A_∞ in F, respectively. These 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. The nonzero prime ideals of $\mathcal{O}_F$ (respectively $\mathcal{O}_{F,\infty}$) are in 1-1 correspondence with the finite (respectively infinite) places of F/k. Hence, a divisor D admits a unique representation as a pair (I, I_∞) of fractional ideals I of $\mathcal{O}_F$ and I_∞ of $\mathcal{O}_{F,\infty}$. In particular, I and I_∞ are A- and A_∞-modules of full rank n, respectively.

More precisely, for a given divisor D, we consider a divisor

$$D + r(t)_\infty = \sum_{Q\in\mathbb{P}_0(F)} \alpha_Q \cdot Q + \sum_{P\in\mathbb{P}_\infty(F)} (\beta_P + r\, e(P/P_\infty)) \cdot P,$$

where $\alpha_Q, \beta_P, r \in \mathbb{Z}$ and $e(P/P_\infty)$ is the ramification index of P over P_∞. 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 $I_\infty = \prod_{P\in\mathbb{P}_\infty} \mathfrak{p}^{-\beta_P}$ constitute the ideal representation of D. The prime ideals $\mathfrak{Q}$ and $\mathfrak{p}$ of F are determined by the places Q, P of F through the identities $v_\mathfrak{Q} = v_Q$ and $v_\mathfrak{p} = v_P$, respectively.

We consider on F the norm:

$$\| \|_D : F \to \{-\infty\} \cup \mathbb{Q}, \quad \|z\|_D = -\min_{P\in\mathbb{P}_\infty(F)} \left\{ \frac{v_P(z) + v_P(D)}{e(P/P_\infty)} \right\}. \tag{12}$$

Clearly, any divisor D induces a norm $\| \|_D$. As our considerations are relative to a fixed divisor D, we write $\| \|$ instead of $\| \|_D$.

Theorem 3.1.

(1) $\mathcal{L}(D + r(t)_\infty) = I \cap t^r I_\infty = (I, \| \|)_{\le r}$.

(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

$$v_Q(z) \geq -\alpha_Q, \forall Q \in \mathbb{P}_0(F), \qquad v_P(z) \geq -\beta_P - r\, e(P/P_\infty), \forall P \in \mathbb{P}_\infty(F).$$

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

$$\min_{P \in \mathbb{P}_\infty(F)} \left\{ \frac{v_P(z) + v_P(D)}{e(P/P_\infty)} \right\} \geq -r \iff v_P(z) + \beta_P \geq -re(P/P_\infty), \forall P \in \mathbb{P}_\infty(F).$$

This is equivalent to $z \in I \cap t^r I_\infty$, since $z \in I$.

We consider the second item. Regarding Definition 1.2, we have to show that $\dim_k (I, \| \,\|)_{\leq r} < \infty$, for all $r \in \mathbb{R}$. This follows directly from item *1*. □

By the last theorem we can identify any divisor D uniquely with the lattice $(I, \| \,\|)$. Hence, we can define the successive minima $\mathrm{sm}(D)$ of D to be the successive minima of the corresponding lattice. We call two divisors D_1 and D_2 *isometric* if they have the same successive minima, and we write then $D_1 \sim D_2$. Clearly $\sim$ is an equivalence relation on the set of divisors. The class of D in $\mathcal{D}_F/\sim$ is called the *isometry class* of D.

Corollary 3.2. *Let* $\mathcal{B} = (b_1, \dots, b_n)$ *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 Theorem 3.1, $(I, \| \,\|)$ is a lattice. Let $m_i = -\lceil \|b_i\| \rceil$, for $1 \leq i \leq n$. By Lemma 2.23, the family $(t^{m_1} b_1, \dots, t^{m_n} b_n)$ is a semi-orthonormal basis of $(F, \| \,\|)$. Hence, Lemma-Definition 2.21 yields the first item of the theorem.

Since $\mathcal{B}$ is a reduced basis of $(I, \lceil \| \,\| \rceil) \sim (I, \| \,\|)$, the second item follows from Theorem 2.24 and Proposition 1.10. The third one follows from the second one. □

The successive minima $\mathrm{sm}(D)$ determine the isometry class of a divisor D. For the computation of $\mathrm{sm}(D)$ we need a reduced basis $\mathcal{B}$ of the corresponding lattice $(I, \| \,\|)$. According to Subsection 2.5 an orthonormal basis $\mathcal{B}'$ of the normed space F is required. If $\mathrm{supp}(D) \cap \mathbb{P}_\infty(F) = \emptyset$, algorithms which determine a reduced basis of $(F, \| \,\|)$ can be found in [3], [8] and [18]. These ideas can be easily generalized to arbitrary divisors D, for instance see [1]. We assume that a basis $\mathcal{B}$ of I and an orthonormal basis $\mathcal{B}'$ of $(F, \| \,\|)$ are already available. Then, Algorithm 3 transforms $\mathcal{B}$ into a reduced basis of $(I, \| \,\|)$. Since every reduced basis is in particular semi-reduced by Corollary 3.2, Algorithm 3 determines a basis of the Riemann-Roch space $\mathcal{L}(D) = I \cap I_\infty$ too.

In [3, Theorem 3.2] it is shown that the semi-reduced bases of $(F, \| \,\|)$ are characterized by the A_∞-bases of the fractional ideal I_∞. For a basis $\mathcal{B}'$ of $I_\infty = (F, \| \,\|)_{\leq 0}$, which is not reduced, Algorithm 3 does compute a k-basis of $\mathcal{L}(D)$ but not the successive minima of D. If we call in that context the simplified reduction Algorithm 1 for the transition matrix $T(\mathcal{B} \to \mathcal{B}')$ then we are in the case of Hess' algorithm described in [10]. Hence, Algorithm 3 can be considered as a refinement of Hess' algorithm in that setting.

4. Appendix: Complexity of the computation of the successive minima

4.1. **Bases of fractional ideals.** Let R be either A or A_∞. We denote $\mathcal{O}_R = \mathcal{O}_F$, $\theta_R = \theta$, if $R = A$, and $\mathcal{O}_R = \mathcal{O}_{F,\infty}$, $\theta_R = \theta_\infty$, if $R = A_\infty$. We consider $\mathcal{B}_{\theta_R} = (1, \theta_R, \dots, \theta_R^{n-1})$, which is a basis of $R[\theta_R]$.

Let M and M' be two free R-modules of rank n. The *index* $[M : M']$ is the nonzero fractional ideal of R generated by the determinant of the transition matrix from a basis of M' to a basis of M.

In the sequel 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 determine concrete bounds for the entries of the transition matrix from such a canonical basis to $\mathcal{B}_{\theta_R}$.

Let $I = \prod_{\mathfrak{p}\in \mathrm{Max}(\mathcal{O}_R)} \mathfrak{p}^{a_\mathfrak{p}}$ be a nonzero fractional ideal of $\mathcal{O}_R$. We define

$$I^* := \prod_{\mathfrak{p}\in \mathrm{Max}(\mathcal{O}_R)} \mathfrak{p}^{-|a_\mathfrak{p}|}. \tag{13}$$

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

For $h \in K$ we set $|hR| := |h|$ and extend the degree function $|\ |$ to fractional ideals of R.

Definition 4.1. *The* height *of the fractional ideal I of $\mathcal{O}_F$ or I_∞ of $\mathcal{O}_{F,\infty}$ is defined to be the integer*

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

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

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

Lemma 4.2. *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. $h(I) \leq |[I^* : \mathcal{O}_F]| + \frac{1}{2}|\mathrm{Disc} f| \leq H(I)$,
3. $h(I_\infty) \leq -|[I_\infty^* : \mathcal{O}_{F,\infty}]| - \frac{1}{2}|\mathrm{Disc} f_\infty| \leq H(I_\infty)$.

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 $|\mathrm{Disc} f|,\ -|\mathrm{Disc} f_\infty| \geq 0$, 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 $\mathcal{B} = (b_0, \dots, b_{n-1})$ a basis of $\mathcal{O}_F$ and let $\mathcal{B}_\theta = (1, \theta, \dots, \theta^{n-1})$. By [15] it holds

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

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

Definition 4.3. *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 the matrix hT is in Hermite normal form (HNF), for any $h \in R \setminus R^*$ such that $hT \in R^{n\times n}$.*

Lemma 4.4. *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 $d_1, \dots, d_n \in K$ 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 $R[\theta_R]$, we obtain $d_1, \dots, d_n \in R$ 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 4.5. *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 4.6. *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,

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

According to the proof of Lemma 4.2 we have $|[\mathcal{O}_F : A[\theta]]| \le \frac{1}{2}|\mathrm{Disc} f|$; hence, $h(I_1) + h(I_2) = |[I^* : \mathcal{O}_F]| + 2|[\mathcal{O}_F : A[\theta]]| \le H(I)$. □

Proof of Lemma 4.5. 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 4.6.

As $[I_1 : A[\theta]] = rA$ with $r \in A$, we deduce $|g| \le |r| = |[I_1 : A[\theta]]| = h(I_1)$, 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 $|t_{i,j}| \le |t_{j,j}|$, for $j \le i \le n$. We consider the matrix $T^{-1} = T(\mathcal{B}_{\theta_R} \to \mathcal{B})$ which has the diagonal entries $t_{j,j}^{-1}$ for $1 \le j \le n$. 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, $|g't_{j,j}^{-1}| \ge 0$ and equivalently $|g'| \ge |t_{j,j}|$.

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

Finally, we deduce $|gt_{i,j}| \le h(I_1) + h(I_2) \le H(I)$, by Lemma 4.6. □

Corollary 4.7. *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 $1 \le i, j \le n$, we have*

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

Proof. For $R = A$ the statement is a direct consequence of Lemma 4.5.

Let $R = A_\infty$. We consider the elementary divisors $d_1, \dots, d_n$ of I, which satisfy $d_i = t^{\alpha_i}$ with $\alpha_i \in \mathbb{Z}$ and $\alpha_1 \le \cdots \le \alpha_n$, 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 4.5 shows that $v_\infty(g' t_{i,j}) \le H(I)$, 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 $\deg_{t^{-1}}(g't_{i,j}) \le H(I)$ 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 $|t^m h| \le m$. Thus, any entry of $g'T$ can be written as $f_{i,j}/t^{m_{i,j}}$ with $f_{i,j} \in A$, $|f_{i,j}| \le H(I)$, and $0 \le m_{i,j} \le H(I)$. Clearly, there exists $m \in \mathbb{Z}$, with $m \le H(I)$, such that $t^m f_{i,j}/t^{m_{i,j}} \in A$, for all $1 \le i, j \le n$. We set $g := t^m$ and $h_{i,j} := t^{m_{i,j}}$ and obtain $|g| + \max\{|f_{i,j}|, |h_{i,j}|\} \le 2H(I)$, for $1 \le i, j \le n$. □

4.2. **complexity.** In [6, 7] it is shown that the computation of a basis of a Riemann-Roch space $\mathcal{L}(D)$ by Hess' algorithm is polynomially bounded in n and the *height* $h(D)$ of D (see definition below). In the sequel we are going to give precise bounds for the complexity of the computation of the successive minima of a divisor D and therefore for the computation of a basis of $\mathcal{L}(D)$ by Algorithm 3. We fix a divisor D and denote by (I, I_∞) its ideal representation; that is, $\mathcal{L}(D) = I \cap I_\infty$. We need a basis $\mathcal{B}$ of the fractional ideal I and a reduced basis $\mathcal{B}'$ of the normed space $(F, \|\ \|)$. We assume that $\mathcal{B}$ is a Hermite basis and that $\mathcal{B}'$ is obtained by the algorithm explained in [18]; that is, $\mathcal{B}'$ is given by a triangular basis of the fractional ideal I_∞, which is a reduced basis of $(F, \|\ \|)$. Note that in [18] the basis $\mathcal{B}'$ is constructed such that the entries of the transition matrix $T(\mathcal{B} \to \mathcal{B}_{\theta_\infty})$ satisfy the bounds from Lemma 4.5. Thus, for the complexity estimation we can assume that $\mathcal{B}'$ is a Hermite basis of I_∞. Note that in general a Hermite basis of I_∞ is not reduced.

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 $g_1, \dots, g_n \in A$ be nonzero polynomials of minimal degree such that $\widetilde{T} := T{\cdot}\mathrm{diag}(g_1, \dots, g_n) \in A^{n\times n}$. Denote by $C(T)$ the cost of the computation of the transition matrix T. Then, the following statement follows immediately from Lemma 2.26.

Lemma 4.8. *Algorithm 3 needs at most*

$$C(T) + O(n^3 h(\widetilde{T})(n + h(\widetilde{T})))$$

arithmetic operations in k to determine the successive minima of D and 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 4.12). Therefore, we estimate $h(\widetilde{T})$ and $C(T)$ in terms of n, C_f and $h(D)$ (see below).

Definition 4.9 (Divisor height)**.** *For* $D \in \mathcal{D}_F$*, 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 4.10. *Let* F/k *be a function field with defining polynomial* f *of degree* n*. Then,* $\delta := |\mathrm{Disc} f|$ *and* $\delta_\infty := v_\infty(\mathrm{Disc} f_\infty)$ *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. See [2, Lemma 3.8]. □

Lemma 4.11.

(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 (13). It is well known that

$$[\mathcal{O}_F : I^*] = N_{F/K}(I^*) = \prod_{P\in\mathbb{P}_0(F)} N_{F/K}(\mathfrak{p})^{-|a_P|}.$$

Since $\deg P = |N_{F/K}(\mathfrak{p})|$ [9], 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

$$\deg D_0^* = |[I^* : \mathcal{O}_F]| = |[I^* : A[\theta]]| - |[\mathcal{O}_F : A[\theta]]|. \tag{14}$$

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 4.1) 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 4.1). 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 4.10.

We consider the second item: 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, $|g_T| \le |g_M| + |g_{M'^{-1}}|$, since $g_M g_{M'^{-1}} T \in A^{n\times n}$ and $|g_T|$ is minimal. Then, Lemma 2.10 shows that

$$h(\widetilde{T}) \le h(g_T T) = |g_T| + h(T) \le |g_M| + h(M) + |g_{M'^{-1}}| + h(M'^{-1}). \tag{15}$$

As $\mathcal{B}$ is an Hermite basis, Corollary 4.7 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 $Q := M'\mathrm{diag}(1, t^{C_f}, \dots, t^{(n-1)C_f})$. As $M'^{-1} = \mathrm{diag}(1, t^{C_f}, \dots, t^{(n-1)C_f})Q^{-1}$, we obtain

$$|g_{M'^{-1}}| + h(M'^{-1}) \le |g_{M'^{-1}}| + (n-1)C_f + h(Q^{-1}). \tag{16}$$

As $g_{Q^{-1}} M'^{-1} \in A^{n\times n}$, we deduce $|g_{M'^{-1}}| \le |g_{Q^{-1}}|$. Arguing as we did in the proof of item *3* of Lemma 2.10, we see that $(g_Q^n \det Q)Q^{-1} \in A^{n\times n}$ with $g_Q^n \det Q \in A$; hence $|g_{Q^{-1}}| \le |g_Q^n \det Q| \le n(g_Q + h(Q))$. Moreover, we have $h(Q^{-1}) \le nh(Q)$. As Q is the transition matrix from $\mathcal{B}'$ to $(1, \theta_\infty, \dots, \theta_\infty^{n-1})$, it holds $|g_Q| + h(Q) = O(H(I_\infty))$ by Corollary 4.7 and therefore $|g_{M'^{-1}}| + h(M'^{-1}) = O(nH(I_\infty) + nC_f)$ by (16). Finally, (15) and item *1* show that

$$h(\widetilde{T}) = O(H(I) + nC_f + nH(I_\infty)) = O(nh(D) + n^3 C_f). \tag{17}$$

□

Corollary 4.12. *Let D be a divisor with $\mathcal{L}(D) = I \cap I_\infty$ and $\mathcal{B}$ and $\mathcal{B}'$ as above. Then, Algorithm 3 needs at most*

$$O(n^5(h(D) + n^2 C_f)^2)$$

arithmetic operations in k to compute $\mathrm{sm}(D)$*.*

Proof. We apply Lemma 4.11 to Lemma 4.8 and deduce that the complexity of Algorithm 3 is given by

$$C(T) + O(n^3 h(\widetilde{T})(n + h(\widetilde{T}))) = C(T) + O(n^5(h(D) + n^2 C_f)^2).$$

In order to estimate $C(T)$ we consider the proof of Lemma 4.11. 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 $M' = Q\mathrm{diag}(1, t^{-C_f}, \dots, t^{-(n-1)C_f})$, the cost for determining M'^{-1} is dominated by the inversion of Q. As mentioned above we can assume that $\mathcal{B}'$ is a Hermite basis of $\mathcal{I}_\infty$; that is, 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 4.7. 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 $O(n^5(h(D) + n^2 C_f)^2)$. □

In the sequel we assume that the constant field k is finite with q elements and we admit fast multiplication techniques of Schönhage-Strassen [20]. 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.

Theorem 4.13. *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, the successive minima of D and a k-basis of $\mathcal{L}(D)$ can be determined with*

$$O(n^5(h(D) + n^2 C_f)^2 + n^{5+\epsilon} {C_f}^{2+\epsilon} \log q)$$

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 reduced basis $\mathcal{B}'$ of $(F, \|\ \|)$, and apply Algorithm 3.

By Lemma 4.10 we have $\delta + \delta_\infty = O(n^2 C_f)$. Moreover, Lemma 4.11 shows that $H(I) + H(I_\infty) = O(h(D) + n^2 C_f)$. By [1, Theorem 5.3.19, Corollary 5.3.14] the computation of $\mathcal{B}$ and $\mathcal{B}'$ takes $O(n^3 H(I)^2 + n^{1+\epsilon}\delta^{2+\epsilon} \log q)$ and $O(n^{2+\epsilon} H(I_\infty)^{1+\epsilon} + n^{1+\epsilon}\delta_\infty \log(q) + n^{1+\epsilon}\delta_\infty^{2+\epsilon})$ operations in k, respectively. Together we deduce

$$\begin{aligned} &O(n^3(H(I))^2 + n^{1+\epsilon}\delta^{2+\epsilon} \log q + n^{2+\epsilon} H(I_\infty)^{1+\epsilon} + n^{1+\epsilon}\delta_\infty \log(q) + n^{1+\epsilon}\delta_\infty^{2+\epsilon}) \\ = &O(n^3(H(I) + H(I_\infty))^2 + n^{1+\epsilon}(\delta + \delta_\infty)^{2+\epsilon} \log q) \\ = &O(n^3(h(D) + n^2 C_f)^2 + n^{5+\epsilon} {C_f}^{2+\epsilon} \log q) \end{aligned}$$

operations in k.

Additionally, we run Algorithm 3, which needs $O(n^5(h(D) + n^2 C_f)^2)$ operations in k by Corollary 4.12. Together we can estimate the computation of $\mathrm{sm}(D)$ and a k-basis of $\mathcal{L}(D)$ by

$$O((n^5(h(D) + n^2 C_f)^2 + n^{5+\epsilon} {C_f}^{2+\epsilon} \log q))$$

operations in k. □

Corollary 4.14. *For a divisor D, let $D = D_0 + D_\infty$ as defined in the proof of Lemma 4.11. If there exists an integer r such that $D_\infty = r(t)_\infty$, then the successive minima of D and a k-basis of $\mathcal{L}(D)$ can be determined with*

$$O(n^3(h(D) + n^3 C_f)^2 + n^{5+\epsilon} {C_f}^{2+\epsilon} \log q)$$

operations in k.

Proof. Denote by $(s_1, \dots, s_n)$ and $(s'_1, \dots, s'_n)$ the successive minima of D and D_0, respectively. Clearly, $D_\infty = r(t)_\infty$ implies $s_i = s'_i + r$ for $i = 1, \dots, n$. Moreover by Corollary 3.2 it is sufficient to determine a reduced basis of the lattice induced by D_0 in order to deduce a basis of $\mathcal{L}(D)$. Hence, we can assume that $r = 0$. Then, the ideal representation of D is given by (I, I_∞) with $I_\infty = \mathcal{O}_{F,\infty}$. Let $\widetilde{T}$ be defined as above. We consider (17) with $I_\infty = \mathcal{O}_{F,\infty}$. Then, $h(\widetilde{T}) = O(H(I) + nC_f + n\delta_\infty) = O(H(I) + n^3 C_f)$ by the definition of $H(I_\infty)$ and Lemma 4.10. We apply Lemma 4.11 and deduce $h(\widetilde{T}) = O(h(D) + n^3 C_f)$. If we replace the bound for $h(\widetilde{T})$ in the proof of Corollary 4.13 by the new one, we deduce the complexity bound from the statement.

□

References

[1] J.-D. Bauch, *Lattices over polynomial Rings and Applications to Function Fields*, PhD thesis, Universitat Aut'onoma de Barcelona, July 2014.

[2] J.-D. Bauch, *Genus computation of global function fields*, J. Symbolic Computation, **66** (2015), 8-20.

[3] J.-D. Bauch, *Computation of integral basis*, arXiv:1507.04058v3 [math.NT], November 2015.

[4] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, Springer, 1993.

[5] H. Cohn and N. Heninger, *Approximate common divisors via lattices*, Proceedings ANTS X, 271- 293, 2012.

[6] C. Diem. *On arithmetic and the discrete logarithm problem in class groups of curves*, Habilitationsschrift, Universität Leipzig. Available at `http://www.math.uni-leipzig.de/?diem/preprints/habil.pdf`, 2008.

[7] K. Eisentrger, S. Hallgren, *Computing the unit group, the class group and compact representations in algebraic function fields*, ANTS X. Proceedings of the tenth algorithmic number theory symposium, 335-358, 2013.

[8] J. Guardia, J. Montes, E. Nart, *Higher Newton polygons and integral bases*, J. Number Theory 147 (2015), 549589.

[9] H. Hasse, *Number theory*, second Edition, Grundlehren der mathematischen Wissenschaften, Springer, 1980.

[10] F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symbolic Computation, 11,1-000, 2011.

[11] A. Lenstra, *Factoring Multivariate Polynomials over Finite Fields*, J. Computer and System Science **30** (1985), 235-248.

[12] R. J. McEliece, *The algebraic theory of convolutional codes* In V. Pless and W. Huffman, editors, Handbook of Coding Theory, Vol. 1, p. 10651138. Elsevier, Amsterdam, 1998.

[13] K. Mahler, *An analogue to Minkowski's geometry of numbers in a field of series*, Ann. Math. (2) **42** (1941), 488-522.

[14] T. Mulders and A. Storjohann, *On lattice reduction for polynomial matrices*, J. Symbolic Computation **35** (2003), 377-401.

[15] M. Pohst, H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1997.

[16] W. M. Schmidt, *Construction and estimation of bases in function fields*, J. Number Theory **39** (1991), 181-224.

[17] M. Schörnig, *Untersuchung konstruktiver Probleme in globalen Funktionenkörpern*, Technische Universität Berlin, 1996.

[18] H. D. Stainsby, *Triangular bases of integral closures*, arXiv:1506.01904v2 [math.NT], June 2015.

[19] H. Stichtenoth, *Algebraic Function Fields and Codes*, second Edition, Graduated Texts in Mathmatics, Springer, 2008.

[20] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, Cambridge University Press (2003), ISBN=9780521826464.

Math Department - Simon Fraser University SCK 10502 - 8888 University Drive Burnaby, BC V6C 1A5, Canada

E-mail address: `j.bauch@sfu.ca`