COMPUTING RIEMANN-ROCH SPACES IN ALGEBRAIC FUNCTION FIELDS AND RELATED TOPICS

F. HESS

Abstract. We develop a simple and efficient algorithm to compute Riemann-Roch spaces of divisors in general algebraic function fields which does not use the Brill-Noether method of adjoints nor any series expansions. The basic idea also leads to an elementary proof of the Riemann-Roch theorem. We describe the connection to the geometry of numbers of algebraic function fields and develop a notion and algorithm for divisor reduction. An important application is to compute in the divisor class group of an algebraic function field.

1. Introduction

Let F/k be an algebraic function field of transcendence degree one and D be a divisor of F/k. The construction of a k-basis of the Riemann-Roch space

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

is one of the fundamental tasks in algebraic function theory or the theory of algebraic curves because of the central position of the theorem of Riemann-Roch. Solutions to this task have been considered in many places for important applications such as, for example, the construction of algebraic geometric codes [16, 24, 26], the explicit addition in the divisor class group [21, 38, 39], symbolic parametrizations of curves [19, 20], integration of algebraic functions [11], the study of diophantine equations [7] or the computation of divisor class groups of global function fields and related problems [18].

These solutions can roughly be divided into *geometric* and *arithmetic* methods due to their origin or background. The geometric methods [16, 21, 24, 38, 39] use the Brill-Noether method of adjoints [2, 28] whereas the arithmetic methods [7, 11, 18, 26] use a strategy involving ideals of integral closures, the basic idea of which essentially dates back to Dedekind and Weber [12] (compare also [17]). These methods usually deal with series expansions of algebraic functions at special places which results in a number of technical problems: Assume, for example, that F/k is defined by some plane curve with a prescribed mapping to $\mathbb{P}^1$. Then in the case of wild ramification in characteristic $p > 0$, Puiseux series can no longer be used and have to be replaced by Hamburger-Noether series or P-adic series where singular points on the curve which defines F/k are (in effect) desingularized simultanously [4, 16, 30, 39]. Additionally, in order to compute these series intermediate constant field extensions seem to be necessary for places of degree greater than one and one has to take care that the series are computed to enough precision for subsequent computations. Finally, the computation of these series gets even more complicated if the function field is defined by a non-plane curve.

2. Results

In this paper we develop a simple and efficient algorithm for the computation of Riemann-Roch spaces to be counted among the arithmetic methods. The algorithm completely avoids series expansions and resulting complications, and instead relies on integral closures and their ideals only. It works for any "computable" constant field k of any characteristic as long as the required integral closures can be computed, and does not involve constant field extensions.

We explain the connection to the geometry of numbers of algebraic function fields which is used in [7, 32, 35, 36] and extend some of their results. In addition we develop an algorithm for the reduction of divisors. An important application of these algorithms is to compute efficiently in the divisor class group of a function field, especially in the global case.

The underlying theoretical idea dates back to [34] where a series expansion free proof of the theorem of Riemann-Roch is given. In the appendix we repeat this proof in a slightly improved and clarified way.

We mention that the method can be extended so that discrete valuations of the constant field are additionally taken into account [18].

The complexity of the algorithms of this paper is polynomial in the size of the input data. For the sake of simplicity we will however not develop explicit formulas. The algorithms have been implemented in Magma and Kash [1, 10, 22].

3. Preliminaries

3.1. **Algebraic function fields.** Throughout the paper F/k will denote an algebraic function field of transcendence degree one over a field k. This is an extension field F of k such that F is separable and of finite degree n over $k(x)$ for an element $x \in F$ transcendental over k. The element x is called a separating element. Every place P of F/k corresponds to a surjective valuation $v_P : F \to \mathbb{Z} \cup \{\infty\}$ which is zero on k. The divisor group $\mathcal{D}(F/k)$ of F/k is the free abelian group generated by the set of places of F/k. A divisor is an element of $\mathcal{D}(F/k)$. For $D \in \mathcal{D}(F/k) \otimes_{\mathbb{Z}} \mathbb{Q}$ ("divisors with rational coefficients") we define $\mathcal{L}(D)$ as in the introduction and $\dim_k(D) := \dim_k(\mathcal{L}(D))$ to be the dimension of $\mathcal{L}(D)$ as a k-vector space. The principal divisor generated by $a \in F^\times$ is denoted by (a). We write its zero and pole divisor $(a)_0$ and $(a)_\infty$ respectively.

For a non-empty set of places S, the ring of elements of F/k being integral at all places of S is denoted by $\mathfrak{o}_S$. It is thus the ring of those elements $a \in F$, for which $v_P(a) \geq 0$ holds for all $P \in S$. Complementarily $\mathfrak{o}^S$ is defined as the ring of all elements being integral at all places outside of S. From [9, pp. 58, p. 64] it follows that both rings are Dedekind domains. Their ideal groups are denoted by $\mathfrak{I}_S$ resp. by $\mathfrak{I}^S$. For $\mathfrak{o}^S$ it furthermore holds that the prime ideals of $\mathfrak{I}^S$ correspond to the places outside S in a unique and valuation preserving way such that the unit group $(\mathfrak{o}^S)^\times$ precisely consists of the S-units of F/k and that the quotient field of $\mathfrak{o}^S$ equals F.

The degree valuation v_∞ corresponding to the "infinite" place ∞ of the rational function field $k(x)$ is defined by $v_\infty(f/g) := \deg(g) - \deg(f)$, $f, g \in k[x]$. By defining $\deg := -v_\infty$ we extend the degree function to $k(x)$. The elements of $k(x)$ with non-positive degree form the discrete valuation ring $\mathfrak{o}_\infty$. This ring is strictly larger than $k[1/x]$. It has only one prime ideal which is generated by the prime element $1/x$.

For a unitary ring extension of entire rings $A \subseteq B$ we define $\mathrm{Cl}(A, B)$ to be the ring of all elements of B which are integral over A.

We will later especially consider the integral closures $\mathrm{Cl}\big(k[x], F\big)$ and $\mathrm{Cl}\big(\mathfrak{o}_\infty, F\big)$. If we choose S to be the set of the "infinite places" of $F/k(x)$, that means the set of the places of F/k over the infinite place ∞ of $k(x)$, then it holds that $\mathfrak{o}^S = \mathrm{Cl}\big(k[x], F\big)$ and $\mathfrak{o}_S = \mathrm{Cl}\big(\mathfrak{o}_\infty, F\big)$. Furthermore we have $S = \mathrm{supp}\big((x)_\infty\big)$. As $k[x]$ and $\mathfrak{o}_\infty$ are principal ideal domains, $\mathrm{Cl}\big(k[x], F\big)$ and $\mathrm{Cl}\big(\mathfrak{o}_\infty, F\big)$ have integral bases consisting of $[F : k(x)]$ elements and the same is true for their (fractional) ideals. Such bases are uniquely determined modulo unimodular transformations over $k[x]$ or $\mathfrak{o}_\infty$.

3.2. **Representation of algebraic function fields and algorithms.** We briefly discuss the representation of function fields and some basic algorithms that we will use in this paper.

Let k be a field. We assume that we can do basic computations in k, in polynomial rings and in rational function fields over k. For running times we will count the required number of operations in k plus the number of bit operations for computations in $\mathbb{Z}$.

We can in principle realize an algebraic function field F/k over the constant field k as the quotient field of the coordinate ring of a given irreducible affine curve over k. For our algorithms to work we will however need a special representation which can be obtained from the general one by a change of variable. Namely, we will realize F as the quotient field of a $k[x]$-order $\mathfrak{o}$ for some separating element $x \in F$. Upon dividing the generators of $\mathfrak{o}$ by suitable positive powers of x we obtain generators of an $\mathfrak{o}_\infty$-order of F (beause they become integral over $\mathfrak{o}_\infty$). These orders are free $k[x]$- resp. $\mathfrak{o}_\infty$-modules of rank $n = [F : k(x)]$. One advantage of using orders is that we can apply techniques from linear algebra.

As the main example we consider the "finite equation order" $k[x, y]\,/\langle f(x, y)\rangle$ where $f(x, y) = y^n + a_1 y^{n-1} + \cdots + a_n \in k[x][y]$ is an irreducible polynomial being monic and separable in y. Such a representation exists for every algebraic function field over a perfect constant field k, [37, p. 128], but it might not be best suited for computations. Expressed in another way $F = k(x, \rho)$ with $f(x, \rho) = 0$ holds. Let $C_f := \max\{\lceil \deg(a_i)/i\rceil \mid 1 \le i \le n\}$. As ρ/x^{C_f} is integral over $\mathfrak{o}_\infty$ we get the "infinite equation order" $\mathfrak{o}_\infty[y]/\langle x^{-nC_f} f(x, x^{C_f} y)\rangle$. For simplicity we will give all complexity statements only with respect to this representation of F/k by a single f.

As already mentioned we will especially consider the integral closures $\mathrm{Cl}\big(k[x], F\big)$ and $\mathrm{Cl}\big(\mathfrak{o}_\infty, F\big)$. We will assume that we are able to compute integral bases and that we have an element and ideal arithmetic for $\mathrm{Cl}\big(k[x], F\big)$ and $\mathrm{Cl}\big(\mathfrak{o}_\infty, F\big)$ including valuation computation with respect to given prime ideals. All this we can, for example, carry out in the case of k a finite field, a number field and other suitable fields, implementations can be found in Magma and Kash [1, 10, 22]. We remark that for the computation of prime ideals from given prime elements of $k[x]$ resp. $\mathfrak{o}_\infty$ and for ideal factorization we need factorization algorithms for polynomials over k (and over extensions of k). We only have to use factorization to generate non-trivial input for the algorithms described in this paper. Information about the above mentioned algorithms can be found in [8, 13, 31, 33] in general and in [32, 36] for the function field situation in particular.

In the case of global function fields ($k = \mathbb{F}_q$) it is shown in [6] that the running time required for the determination of an integral basis of $\mathrm{Cl}\big(k[x], F\big)$ or $\mathrm{Cl}\big(\mathfrak{o}_\infty, F\big)$

requires polynomial time in C_f and n. Using a variant of the Round-2 algorithm [3] one can see that this is true even for rather general k. Namely, only if $0 < p := \mathrm{char}(k) \leq n$ one seems to need additional properties of k, for example k perfect and the ability to compute p-th roots in k suffice. In particular no polynomial factorization over k is required. In the sequel we assume that k is such that bases for the above integral closures can be computed in time polynomial in C_f and n.

We note that the complexity of the other cited algorithms above except factorization is polynomial in C_f, n and the maximal degree of the polynomials of $k[x]$ occuring in the representations of the involved ideals. The factorization of ideals or the computation of prime ideals is polynomial time in C_f, n and in the time required for factoring the occuring polynomials of $k[x]$.

4. Lattices and basis reduction over $k[x]$

For the computation of Riemann-Roch spaces we need a reduction algorithm for matrices in $k(x)^{n\times n}$. This algorithm can be interpreted in a broader context in terms of lattices and lattice basis reduction the essential statements about which we now describe. The particular connection to our algebraic function field F/k will be explained in section 7. For more detailed infomation about Lemma 1 we refer for example to the (somewhat different) descriptions in [25, 29, 32, 36].

By $k((t^{-1}))$ we denote the field of formal Laurent series in t^{-1}. Let the degree of an element be the exponent of the largest t-power occuring. For $v \in k((t^{-1}))^n$ we denote the column degree of v, that is the maximum of the degrees of the entries of v, by $\deg(v)$. By $\mathrm{hc}(v) \in k^n$ we denote the vector resulting from the coefficients of the $\deg(v)$-th power of t of the entries of v (that means the coefficients of the largest powers, the others are zero).

Now fix an $x \in k((t^{-1}))$ of positive degree which is transcendental over k. Let $\Lambda \subseteq k((t^{-1}))^n$ be a free $k[x]$-module of rank m and let $v_1, \ldots, v_m$ be a basis of Λ. We assume furthermore that the basis elements are $k((t^{-1}))$-linearly independent (this means that if k is a finite field, Λ is discrete regarding deg in the sense that there are always only finitely many vectors with bounded deg-values). Λ is then a "non-Archimedian" *lattice*. The maximum of the degrees of the determinants of $m \times m$-submatrices of $(v_j)_j$ is an invariant of Λ that we can regard as a lattice discriminant. By a reduction step we mean the addition of a $k[x]$-linear combination of the v_j to a v_i, $i \neq j$, so that the column degree of v_i decreases. This is a $k[x]$-unimodular transformation. The basis $v_1, \ldots, v_m$ of Λ, ordered with rising column degrees, is called *reduced* if one of the following equivalent conditions is fulfilled:

Lemma 1. *The following conditions are equivalent:*

- (*i*) $\{\ \mathrm{hc}(v_i) \mid 1 \leq i \leq m$ *and* $\deg(v_i) \equiv j \bmod \deg(x)\ \}$ *is a set of linearly independent elements of* k^n *for all* $0 \leq j < \deg(x)$,
- (*ii*) $\deg(\sum_{i=1}^m \lambda_i v_i) = \max_{i=1}^m \deg(\lambda_i v_i)$ *for all* $\lambda_i \in k[x]$, $1 \leq i \leq m$,
- (*iii*) $v_1, \ldots, v_m$ *realize the successive minima of* Λ,
- (*iv*) *if additionally* $\deg(x) = 1$ *holds:* $\sum_{i=1}^m \deg(v_i)$ *equals the lattice discriminant.*

Proof. For the proof see also [29, 32, 36]. The situation in (*i*) represents a point of view of (*ii*) and (*iv*) which only takes the leading terms into account; the linear independence means that no leading terms can be cancelled. With these remarks

one can work out the equivalence of $(i), (ii), (iv)$. The equivalence of (iii) with (ii) follows inductively. □

If a basis satisfies these conditions then no reduction step can be carried out. For a non-reduced basis we can therefore always perform a reduction step that decreases the sum of the column degrees of the v_i. For this sum the lattice discriminant represents a lower bound so that after finitely many reduction steps we necessarily come to a reduced basis. From this follows the *reduction algorithm*, a reduced basis can therefore always be constructed. For a more precise description of the reduction algorithm we refer to [29, 32, 36]. A matrix with non-zero columns forming a reduced basis is called reduced.

The property (iv) can be regarded as an orthogonality property of a reduced basis if $\deg(x) = 1$. The concept of orthogonality can be pursued in this case: We look at "orthogonal" or "isometric" maps of $k((t^{-1}))^n$, given by unimodular matrices $T \in k[[t^{-1}]]^{n\times n}$ with power series entries: $v \mapsto Tv$. For these $\deg(v) = \deg(Tv)$ holds. Two lattices Λ_1, Λ_2 are now called *isometric* if there is such a T with $\Lambda_1 = T\Lambda_2$. Reduced bases are transformed under T into reduced bases. Two isometric lattices have the same successive minima and the same lattice discriminant, as we can see using Lemma 1 and the definitions. We define the *orthogonal lattice* of rank m in $k((t^{-1}))^n$ with the succesive minima $-d_1 \leq \cdots \leq -d_m \in \mathbb{Z}$ as the uniquely determined lattice with a basis of the shape $(t^{-d_j}\delta_{i,j})_i \in k((t^{-1}))^n$ for $1 \leq j \leq m$ ($\delta_{i,j} = 1$ if $i = j$, $\delta_{i,j} = 0$ otherwise). Now the following "classification lemma" holds:

Lemma 2. *Assume* $\deg(x) = 1$ *and let* $\Lambda \subseteq k((t^{-1}))^n$ *be a lattice of rank* m*. Then* Λ *is isometric to exactly one orthogonal lattice in* $k((t^{-1}))^n$*.*

Proof. First we notice that $k[[t^{-1}]]$ is a Euclidean ring for deg and that elements of smaller degree are always divisible by elements of larger degree. Therefore an arbitrary basis of Λ can be put into an upper triangular shape by $k[[t^{-1}]]$-unimodular row operations where the entries over the diagonal are zero or have a proper larger degree than the diagonal entries below and the diagonal entries are powers of t (Hermite normal form). The lattice Λ' generated by this basis is isometric to Λ. If we start with a reduced basis of Λ the resulting basis of Λ' is also reduced because of the isometry. Because of (i) from Lemma 1 this basis of Λ' must already have a diagonal shape otherwise it would not be reduced. A reduced basis of Λ, however, always exists.

For the uniqueness one can easily see that two different orthogonal lattices cannot be isometric. □

Corollary 3. *Let* $M \in k(x)^{n\times n}$*. There exist unimodular matrices* $T_1 \in \mathfrak{o}_\infty^{n\times n}$ *and* $T_2 \in k[x]^{n\times n}$ *and uniquely determined rational integers* $d_1 \geq \cdots \geq d_n$ *such that*

$$T_1 M T_2 = (x^{-d_j}\delta_{i,j})_{i,j}.$$

The matrix T_2 *is the basis transformation matrix obtained by the reduction algorithm applied to the columns of* M*. The column degree of the* j*-th column of* MT_2 *is equal to* $-d_j$*.*

Proof. Let $t = x$ and consider the lattice spanned by the columns of M. We apply Lemma 2 and get unimodular matrices $T_1 \in k[[x^{-1}]]^{n\times n}$ and $T_2 \in k[x]^{n\times n}$ with $T_1 M T_2$ diagonal as required. Notice that $T_1 \in \mathfrak{o}_\infty^{n\times n}$ holds because of $M \in k(x)^{n\times n}$. The last assertions follow from the proof of Lemma 2 and the above comments. □

The matrix M is given in $k(x)^{n\times n}$ and can hence be written as M_0/d with $M_0 \in k[x]^{n\times n}$ and $d \in k[x]$. It suffices to perform the reduction algorithm on the columns of M_0 so that series and approximation errors can be avoided completely.

Corollary 4. *Let a $k[x]$-module M_1 and an $\mathfrak{o}_\infty$-module M_2 both free of rank n be given within a $k(x)$-vector space V. Then there are bases $v_1,\dots,v_n$ of M_1 and $b_1,\dots,b_n$ of M_2 such that*

$$(b_1,\dots,b_n)N = (v_1,\dots,v_n)$$

holds with a unique matrix N of the shape $N = (x^{-d_j}\delta_{i,j})_{i,j}$ and rational integers $d_1 \geq \cdots \geq d_n$.

Proof. Follows from Corollary 3 applied to the transformation matrix of arbitrary bases of M_1 and M_2. □

Example 5. *We give an example for the reduction algorithm and the matrix normal form of Corollary 3. We consider the matrix M:*

$$\begin{pmatrix} x^3-x & x^2-2 \\ 0 & x \end{pmatrix}.$$

This matrix is not reduced because the sum of the column degrees is 5 and the determinant degree is 4. We substract x times the second column from the first column and we get the reduced matrix

$$\begin{pmatrix} x & x^2-2 \\ -x^2 & x \end{pmatrix}.$$

For the calculation of the normal form we negate the last row, swap it with the first row and substract from the now last row $1/x$ times the first row. We obtain

$$\begin{pmatrix} x^2 & -x \\ 0 & x^2-1 \end{pmatrix}.$$

Now we add $x/(x^2-1)$ times the last row to the first row and scale the last row by $x^2/(x^2-1)$. The final result is

$$\begin{pmatrix} x^2 & 0 \\ 0 & x^2 \end{pmatrix}.$$

Remark 6. *The reduction algorithm is a generalized polynomial division, operating on columns. According to that we can also interpret it as a Gröbner reduction. For function fields the reduction algorithm takes on the role that the LLL-algorithm plays in the case of number fields.*

5. Bases of the k-spaces $\mathcal{L}(D)$

Let x denote a separating element of F/k, $S := \operatorname{supp}\big((x)_\infty\big)$ and $n := [F : k(x)]$. The main result of this section and the fundamental statement for the algorithm to be described is the following theorem together with its constructive proof:

Theorem 7. *For every divisor D of F/k there exist uniquely determined rational integers $d_1 \geq \cdots \geq d_n$ and elements $v_1,\dots,v_n \in F$ such that the set*

$$\{\, x^j v_i \mid 1 \leq i \leq n,\, 0 \leq j \leq d_i + r \}$$

represents a k-basis of $\mathcal{L}\big(D + r(x)_\infty\big)$ for all $r \in \mathbb{Z}$. The elements $v_1,\dots,v_n$ are $k(x)$-linearly independent.

We note that the above d_i and v_i do not only depend on the divisor D but also depend on the constant field k and the separating element x; more exactly: they depend on the polynomial ring $k[x] \subseteq F$.

Definition 8. *We define the d_i of Theorem 7 to be the $k[x]$-invariants of D, written $|D|_i$, for a fixed, given $k[x]$.*

In order to obtain a constructive proof of this theorem we transfer the above situation into an ideal-theoretical context:

Proposition 9. (*i*) *There is a natural and valuation preserving bijection between the set of places of F/k and the set of prime ideals of $\mathfrak{o}^S$ and $\mathfrak{o}_S$,*
(*ii*) *by this bijection, an isomorphism of the divisor group of F/k is induced to the direct product $\mathfrak{I}^S \times \mathfrak{I}_S$ of the ideal groups, $D \mapsto (D^S, D_S)$.*
(*iii*) *If D denotes a divisor and if D^S, D_S are the corresponding ideals in $\mathfrak{I}^S$ and $\mathfrak{I}_S$, then $\mathcal{L}(D) = (D^S)^{-1} \cap (D_S)^{-1}$ holds.*

Proof. We refer to section 3.1. For (*iii*) let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}^S$, P the corresponding place of F/k and r the exact power with which $\mathfrak{p}$ divides D^S. Thus $r = v_P(D)$ (the exponent of P in D) is fulfilled. As $\mathfrak{o}^S$ is a Dedekind domain, $a \in (D^S)^{-1}$ holds if and only if $a \in F$ and $v_P(a) \geq -r$ holds. Analogously we have the same situation for $(D_S)^{-1}$ so that $\mathcal{L}(D) = (D^S)^{-1} \cap (D_S)^{-1}$ follows. □

Remark 10. *Let D be a divisor represented by (D^S, D_S). Then $D + r(x)_0$ is represented by $(x^r D^S, D_S)$ and $D + r(x)_\infty$ by $(D^S, x^{-r} D_S)$.*

Because of Proposition 9, (*iii*) we are now interested in the relation of $(D^S)^{-1}$ and $(D_S)^{-1}$ in F. The ideals in $\mathfrak{I}^S$ and $\mathfrak{I}_S$ are free $k[x]$- resp. $\mathfrak{o}_\infty$-modules of rank n. Therefore we can choose bases $v_1, \ldots, v_n \in (D^S)^{-1}$ and $b_1, \ldots, b_n \in (D_S)^{-1}$ of $(D^S)^{-1}$ and $(D_S)^{-1}$. As F is a $k(x)$-vector space of dimension n there is a matrix $M \in k(x)^{n \times n}$ such that $(b_1, \ldots, b_n)\, M = (v_1, \ldots, v_n)$ holds. We see that M is unique except for multiplication by a unimodular $T_1 \in \mathfrak{o}_\infty^{n \times n}$ from the left and a unimodular $T_2 \in k[x]^{n \times n}$ from the right since any two bases of $(D^S)^{-1}$ or $(D_S)^{-1}$ differ by such transformations. Corollary 4 exactly fits this situation so that we obtain a proof for Theorem 7:

Proof of Theorem 7. We fix a D and firstly prove the existence. We choose a basis transformation matrix M from $(D_S)^{-1}$ to $(D^S)^{-1}$ as above. By application of Corollary 4 we see that there are ideal bases $(v_i)_i$ of $(D^S)^{-1}$ and $(b_i)_i$ of $(D_S)^{-1}$ which are related to each other by a unique diagonal transformation matrix $(x^{-d_i}\delta_{i,j})_{i,j}$, i.e. $x^{-d_i} b_i = v_i$ with unique rational integers $-d_i$ for $1 \leq i \leq n$.

Let now $r \in \mathbb{Z}$ be arbitrary. The divisor $D + r(x)_\infty$ is according to Remark 10 uniquely represented by the pair of ideals $(D^S, x^{-r} D_S)$. The ideal bases of $(D^S)^{-1}$ and $x^r (D_S)^{-1}$ are $(v_i)_i$ as before and $(b'_i)_i$ with $b'_i = x^r b_i$. They already are related by a diagonal transformation matrix. We now consider the intersection of $(D^S)^{-1}$ with $x^r (D_S)^{-1}$: The element $z = \sum_{i=1}^n \lambda_i v_i$ with arbitrary $\lambda_i \in k[x]$ lies in $(D^S)^{-1}$. As $z = \sum_{i=1}^n \lambda_i x^{-d_i - r} b'_i$ holds on the other hand we see that it is necessary and sufficient for the condition $z \in x^r (D_S)^{-1}$ that $\lambda_i x^{-d_i - r} \in \mathfrak{o}_\infty$ is true. But this precisely means that $\deg \lambda_i \leq d_i + r$ has to hold. Because of this conclusion and the $k(x)$-linear independence of the v_i the statement of Theorem 7 about the basis follows.

The last statement of the theorem is to be proved next: The $k(x)$-linear independence of elements v_i as given in the theorem follows from the basis property of the $x^j v_i$ for all $r \in \mathbb{Z}$. Namely, if there were a relation $\sum_{i=1}^n \lambda_i v_i = 0$ with $\lambda_i \in k[x]$ not all zero, the elements $x^j v_i$ were k-linearly dependent.

It remains to prove the uniqueness of any d_i for which Theorem 7 together with arbitrary v_i is true. We firstly assert that $v_1, \ldots, v_n$ is an ideal basis of $(D^S)^{-1}$ and secondly that $x^{d_1}v_1, \ldots, x^{d_n}v_n$ is an ideal basis of $(D_S)^{-1}$. Indeed, as for every $g \in (D^S)^{-1}$ there is an $r \in \mathbb{Z}$ such that $g \in \mathcal{L}\big(D + r(x)_\infty\big)$ holds, we can represent g by the v_i, and the first assertion is clear. For the second assertion we note that for every $g \in (D_S)^{-1}$ there is an $h \in k[x]$ such that $g \in \mathcal{L}\big(D + (h)_0\big)$ holds. If we put $r := \deg h$ then $r(x)_\infty = (h)_\infty$ and furthermore $D + (h)_0 = D + r(x)_\infty + (h)$ holds such that the elements $h^{-1}x^j v_i$ with $1 \le i \le n$, $0 \le j \le d_i + r$ represent a k-basis of $\mathcal{L}\big(D + (h)_0\big)$ (note that $\mathcal{L}\big(D + (a)\big) = a^{-1}\mathcal{L}(D)$ for $a \in F^\times$). Thus we see that g can be represented by an $\mathfrak{o}_\infty$-linear combination of $x^{d_i}v_i$, what had to be proved.

As the bases $v_1, \ldots, v_n$ of $(D^S)^{-1}$ and $x^{d_1}v_1, \ldots, x^{d_n}v_n$ of $(D_S)^{-1}$ are related by a diagonal transformation matrix to each other we can deduce the uniqueness of d_i from the uniqueness statement of Corollary 4. □

Because of Theorem 7 and the theorem of Riemann-Roch we expect a connection between the $k[x]$-invariants of a divisor D, the genus and the dimension of the exact constant field of F/k over k.

Corollary 11. *Let g denote the genus of F/k and let k_0 be the exact constant field of F/k. For the $k[x]$-invariants $|D|_i$ of a divisor D it then holds that*

$$\sum_{i=1}^{n} |D|_i = \deg_k D + [k_0 : k](1 - g) - n.$$

Proof. We choose $r \in \mathbb{Z}$ large enough such that the divisor $D + r(x)_\infty$ is not special, [37, p. 33], and that $r \ge |D|_i$ holds for all $1 \le i \le n$. Because of the theorem of Riemann-Roch we then know that $\dim_k(D + r(x)_\infty) = \deg_k(D + r(x)_\infty) + [k_0 : k](1 - g)$. By means of Theorem 7 we obtain the equations $\dim_k(D + r(x)_\infty) = \sum_{i=1}^n (|D|_i + r + 1) = rn + n + \sum_{i=1}^n |D|_i$. Because of $\deg_k(D + r(x)_\infty) = \deg_k D + rn$ we obtain the desired result by equating. □

The last result yields a concrete interpretation of the invariants g and $[k_0 : k]$ of the function field F/k and of the degree of a divisor D (for a fixed separating element x): Namely, they measure a kind of "distance" of the ideals D^S and D_S, representing the divisor, in F. With increasing degree D^S and D_S move away from each other whereas $(D^S)^{-1}$ and $(D_S)^{-1}$ approach (so that they eventually overlap according to the size of the degree of D).

For the proof of the corollary we applied the theorem of Riemann-Roch. In the appendix we give a constructive proof of the theorem of Riemann-Roch based on a suitable reformulation of this corollary. This will be Corollary 26 where we supply an alternative proof without assuming the theorem of Riemann-Roch.

As a demonstration of the technique we get the following bound for the genus, compare [37, p. 132], [14, p. 201] and [27, p. 169]:

Corollary 12. *Let the algebraic function field F/k with the exact constant field k_0 be given by the equation $f(x, y) = 0$ with an irreducible polynomial $f(x, y) \in k[x, y]$,*

separable and monic in y. Then for the genus of F/k it holds that

$$g \leq \frac{C_f(n-1)n - 2(n-[k_0:k])}{2[k_0:k]}.$$

For $C_f = 1$ and $k_0 = k$ this reduces to

$$g \leq \frac{(n-1)(n-2)}{2}.$$

Proof. Let $\rho \in F$ with $f(x,\rho) = 0$. We consider the equation orders $k[x,\rho] \subseteq \mathfrak{o}^S$ and $\mathfrak{o}_\infty[\rho/x^{C_f}] \subseteq \mathfrak{o}_S$ (note that ρ/x^{C_f} is integral over $\mathfrak{o}_\infty$). For the transformation matrix of the bases we get

$$(1, x^{-C_f}\rho, \ldots, x^{-C_f(n-1)}\rho^{n-1})\,(x^{C_f(i-1)}\delta_{i,j})_{i,j} = (1, \rho, \ldots, \rho^{n-1}).$$

Using a basis $\tilde{\omega}_1, \ldots, \tilde{\omega}_n$ of $\mathfrak{o}_S$ and $\omega_1, \ldots, \omega_n$ of $\mathfrak{o}^S$ we obtain

$$(\tilde{\omega}_1, \ldots, \tilde{\omega}_n)\, T_1 (x^{C_f(i-1)}\delta_{i,j})_{i,j} T_2^{-1} = (\omega_1, \ldots, \omega_n)$$

with suitable $T_1 \in \mathfrak{o}_\infty^{n\times n}$ and $T_2 \in k[x]^{n\times n}$. Now $\deg(\det(T_1)) \leq 0$ and $\deg(\det(T_2^{-1})) \leq 0$. Because of this and Corollary 3 applied to $(x^{C_f(i-1)}\delta_{i,j})_{i,j}$ and $T_1(x^{C_f(i-1)}\delta_{i,j})_{i,j}T_2^{-1}$, and because of the first paragraph of the proof of Theorem 7, we see that the sum $\sum_{i=1}^{n} C_f(i-1) = C_f n(n-1)/2$ is an upper bound for the sum of the negated $k[x]$-invariants of the zero divisor. Using Corollary 11 we now obtain $C_f n(n-1)/2 \geq [k_0:k](g-1)+n$ from which the statement follows by reordering the inequality. □

6. Computation of Riemann-Roch spaces

In this section we describe the basic method for the computation of the Riemann-Roch space of a divisor. We assume the maximal orders $\mathfrak{o}^S$ and $\mathfrak{o}_S$ to be computed (see section 3.2).

According to Proposition 9 we can represent places of F/k by prime ideals in either $\mathfrak{o}^S$ or $\mathfrak{o}_S$. For representing divisors there are essentially two ways. As already used D can be represented by two ideals D^S and D_S, but with regard to Proposition 9, (*iii*) we only use the inverses. We call this representation the *ideal representation*. The other representation simply means the sum of places or the power product of prime ideals. We call this the *free representation*.

For divisors in free representation the divisor arithmetic is carried out exponentwise, for divisors in ideal representation it is carried out by ideal arithmetic. We define the *height* of a divisor D as the sum of the degrees of the pole and zero divisors of D: $h(D) := \deg_k(D)_0 + \deg_k(D)_\infty$. In both cases the costs for the divisor arithmetic are polynomial in C_f, n and $\max\{\, h(D_1),\, h(D_2)\,\}$ for divisors D_1, D_2, because of section 3.2 (the size of the exponents has of course only a logarithmic influence on the arithmetic in free representation).

By multiplying out the prime ideal power products of a free representation the ideals D^S and D_S of the corresponding ideal representation can be determined. Conversely, these two ideals have to be factorized in order to get the places and their exponents occuring in the corresponding divisor. This change in representation requires a polynomial running time in C_f, n and $h(D)$ (and in the factorization costs), according to section 3.2. By using principal ideals we can thus also determine principal divisors of elements of $F^\times$ in free representation.

The computation of a Riemann-Roch space means the computation of a basis for it. We use Theorem 7 and distinguish bases in short representation (given by v_i, d_j) and long representation (given by all the $x^j v_i$).

Algorithm 13. *(Computation of Riemann-Roch spaces I)*
Input: *A divisor D of the algebraic function field F/k.*
Output: *A k-basis of $\mathcal{L}(D)$ in short or long representation.*

(1) *(Bases) Determine a $k[x]$-basis $v'_1, \ldots, v'_n$ of $(D^S)^{-1}$ and an $\mathfrak{o}_\infty$-basis $b'_1, \ldots, b'_n$ of $(D_S)^{-1}$.*
(2) *(Transformation) Determine $M \in k(x)^{n \times n}$ with $(b'_1, \ldots, b'_n)M = (v'_1, \ldots, v'_n)$.*
(3) *(Intersection) Compute the unimodular matrix $T_2 \in k[x]^{n \times n}$ and the d_i using Corollary 3 applied to M. The desired basis $v_1, \ldots, v_n$ with the $k[x]$-invariants d_j is now given by $(v_1, \ldots, v_n) = (v'_1, \ldots, v'_n)\, T_2$ according to Theorem 7 and its proof.*
(4) *(End) Output of the basis as in Theorem 7 in short or long representation. Terminate.*

Remark 14. *The algorithm requires a running time which is polynomial in C_f, n and $h(D)$: The size of the entries of the matrix M in the second step is polynomial in C_f, n and $h(D)$. Thus the reduction algorithm requires a running time polynomial in C_f, n and $h(D)$ as well.*

If we want to compute Riemann-Roch spaces of divisors of small height, i.e. approximately in the order of n or C_f, algorithm 13 is rather suitable. But especially in connection with the divisor class group of global function fields it can happen that the exponents of the divisors in free representation are of order q^g (while the degrees of the places are still small), where q is the number of elements of k and g is the genus of F/k. This implies an exponential running time for algorithm 13 according to the remark. The discussion about this problem will be continued in section 8.

Example 15. *In order to demonstrate the idea of the algorithm we consider a very simple example: We choose $k = \mathbb{Q}$, $f(x, y) = y^2 - x^3 - 1$ and $F = k(x, \rho)$ with $f(x, \rho) = 0$, i.e. an elliptic function field.*

We easily check that $\mathfrak{o}_F := \mathrm{Cl}(k[x], F) = k[x, \rho]$ holds. For the determination of $\mathfrak{o}_{F,\infty} := \mathrm{Cl}(\mathfrak{o}_\infty, F)$ we note that ρ/x^2 is integral over $\mathfrak{o}_\infty$. The corresponding minimal polynomial is $f_\infty(y) = y^2 - (x^3 + 1)/x^4 \in \mathfrak{o}_\infty[y]$, and here $\mathrm{Cl}(\mathfrak{o}_\infty, F) = \mathfrak{o}_\infty[\rho/x^2]$ also holds. Thus the general techniques from section 5 show that $\mathbb{Q}$ is the exact constant field and that the genus is one.

We want to factorize the principal ideal generated by $x - 2$ in $\mathfrak{o}_F$. According to the theorem of Kummer [37, p. 76] *we therefore factorize $f(x, y) \bmod (x - 2)k[x, y]$ in the shape $y^2 - 9 = (y - 3)(y + 3)$ and we get $(x - 2)\mathfrak{o}_F = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1 = (x - 2)\mathfrak{o}_F + (\rho - 3)\mathfrak{o}_F$ and $\mathfrak{p}_2 = (x - 2)\mathfrak{o}_F + (\rho + 3)\mathfrak{o}_F$. We conclude that there are two unramified places P_1 resp. P_2 of F/k with degree 1 above the place of $k(x)$ defined by $x - 2$, where x assumes the value 2 and ρ the value 3 resp. -3. We now examine the splitting of the infinite place ∞ of $k(x)$ in F. For this we have to factorize $(1/x)\mathfrak{o}_{F,\infty}$ since $1/x$ is a prime element of ∞. Again according to the theorem of Kummer and because of $f_\infty(x, y) \equiv y^2 \bmod (1/x)\mathfrak{o}_\infty[y]$ we have that $(1/x)\mathfrak{o}_\infty = \mathfrak{p}_3^2$ with $\mathfrak{p}_3 = (\rho/x^2)\mathfrak{o}_{F,\infty}$ holds. There is thus exactly one place of F above the infinite place of $k(x)$ which we denote by ∞ as well. It has degree 1 and is ramified. Therefore we can say that x has degree 2 and ρ degree 3.*

Finally the Riemann-Roch space of $D = 3\infty - P_1$, i.e. the intersection $\mathfrak{p}_1 \cap \mathfrak{p}_3^{-3}$, has to be computed. A $k[x]$-basis of $\mathfrak{p}_1$ is given by $(\alpha_1, \alpha_2) = (x-2, \rho-3)$ and an $\mathfrak{o}_\infty$-basis of $\mathfrak{p}_3^{-3}$ by $(\beta_1, \beta_2) = (x^3/\rho)\,(1, \rho/x^2)$. From this follows the basis relation

$$\begin{aligned}(\alpha_1, \alpha_2) &= (\beta_1, \beta_2) \begin{pmatrix} 0 & (x^3+1)/x^5 \\ 1/x & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & x^2 \end{pmatrix} \begin{pmatrix} x-2 & -3 \\ 0 & 1 \end{pmatrix} \\ &= (\beta_1, \beta_2) \begin{pmatrix} 0 & (x^3+1)/x^3 \\ (x-2)/x & -3/x \end{pmatrix}.\end{aligned}$$

The last matrix is already reduced so that the $k[x]$-invariants of D are both zero and a basis of the Riemann-Roch space is given by $x-2, y-3$. Explicitly this means that $\mathcal{L}(D)$ consists of the elements of $\mathfrak{p}_1$ with degree bounded by 3 so that the result is in accordance with the above remark about the degrees.

7. Connection to the geometry of numbers of algebraic function fields

The geometry of numbers of an algebraic function field F/k with separating element x provides means of computing Riemann-Roch spaces using series expansions [7, 32, 35, 36]. In this section we explain the connection to our ideal-theoretical method. With this aim in view we recall some notations and statements from [29, 32, 36] (in a somewhat different way).

We change from the logarithmic measure deg to an absolute value by means of the relation $\log_q |\cdot| = \deg(\cdot)$ which is not essential but emphasizes the analogy to the number field case: In the rational function field $k(x)$ we define the absolute value of $\lambda \in k(x)$ by $|\lambda| = q^{-v_\infty(\lambda)}$, where we choose some $q > 1$, preferably the number of elements of k if it is a finite field. The set of places over ∞ is written as $S = \{P_0, P_1, \ldots, P_s\}$, and we denote the surjective exponential valuation resp. the absolute value belonging to P_i by v_i resp. by $|\cdot|_i$ so that $|\alpha|_i = q^{-v_i(\alpha)}$ holds for an arbitrary $\alpha \in F^\times$. Let now D be a divisor of F/k. We define c_i to be the exponent of P_i in D and e_i to be the ramification index of P_i over ∞. The $k(x)$-vector space F is equipped with an ultrametric $|\cdot|$-linear norm $\|\cdot\|_D$ defined by $\|\alpha\|_D = \max_{i=0}^{s} q^{-c_i/e_i} |\alpha|_i^{1/e_i}$. The free $k[x]$-module $(D^S)^{-1}$ is discrete with respect to $\|\cdot\|_D$ and is called the *lattice* Λ_D belonging to D (and k, x).

The term "lattice" is justified here with respect to section 4 because Λ_D and $k[x]$ can compatibly be embedded into $\bar{k}((t^{-1}))$ such that $\log_q \|\alpha\|_D = \deg(\bar{\alpha})/e$ hence $\deg(\bar{x}) = e$ with $e := \operatorname{lcm}(e_1, \ldots, e_s)$ holds for every $\alpha \in \Lambda_D$ and $\bar{\alpha}, \bar{x}$ the images of α, x in $\bar{k}((t^{-1}))$ respectively. If the places P_i are tamely ramified over $k(x)$ this can be done using $t = x^{-1/e}$ (Puiseux series), see for example [36] for k a finite field. In the wildly ramified case this can still be done using general P-adic series [5] or Hamburger-Noether series [4] where x will in general be represented by a proper series.

For the lattices Λ_D we can hence use the definitions and results of section 4 with respect to the embedding into $\bar{k}((t^{-1}))$. From there we recall (for our absolute value setting) that a basis $v_1, \ldots, v_n$ of Λ_D, ordered with increasing $\|\cdot\|_D$-values, is called *reduced* if $\|\sum_{i=1}^n \lambda_i v_i\|_D = \max_{i=1}^n \|\lambda_i v_i\|_D$ holds for all $\lambda_i \in k[x]$, $(1 \le i \le n)$. We introduce that it is called *weakly reduced* if only $\lceil \log_q \|\sum_{i=1}^n \lambda_i v_i\|_D \rceil = \max_{i=1}^n \lceil \log_q \|\lambda_i v_i\|_D \rceil$ holds for all $\lambda_i \in k[x]$, $(1 \le i \le n)$. It is clear that reduced bases are also weakly reduced.

Let D be a divisor of F/k, $v_1, \dots, v_n \in F$ and $d_1 \geq \dots \geq d_n$. For $R \in \{\mathbb{Z}, \mathbb{Q}\}$ let us call the v_i an *R-parametric basis of D* if all $d_i \in R$ and the set

$$\{ x^j v_i \mid 1 \leq i \leq n,\, 0 \leq j \leq d_i + r,\, j \in \mathbb{Z}\}$$

represents a k-basis of $\mathcal{L}\big(D + r(x)_\infty\big)$ for all $r \in R$. A $\mathbb{Q}$-parametric basis can clearly be used as $\mathbb{Z}$-parametric basis using $\lfloor d_i \rfloor$ but the converse is not possible in general.

The following theorem extends Theorem 7 and points out the connection to the geometry of numbers. It also generalizes the corresponding results from [7, 32, 35, 36]. The still constructive proof now relies on series expansions.

Theorem 16. *Let $R \in \{\mathbb{Z}, \mathbb{Q}\}$.*

- *(i) Every divisor D has an R-parametric basis. Every R-parametric basis of D has the same d_i and is $k(x)$-linearly independent.*
- *(ii) The elements $v_1, \dots, v_n \in F$ form an R-parametric basis of D if and only if they constitute a weakly reduced basis of Λ_D for $R = \mathbb{Z}$ and a reduced basis of Λ_D for $R = \mathbb{Q}$. In the first case $d_i = -\lceil \log_q \|v_i\|_D \rceil$ and in the second case $d_i = -\log_q \|v_i\|_D$ (the negated successive minima of Λ_D divided by e).*

Proof. Let D be a divisor of F/k and $r \in R$. Firstly we notice that for $\alpha \in F$ the conditions $\alpha \in \mathcal{L}(D + r(x)_\infty)$ and $\big(\alpha \in \Lambda_D \text{ and } \log_q \|\alpha\|_D \leq r\big)$ are equivalent, as a simple calculation shows. Secondly we notice that any given R-parametric basis of D has only one possible set of valid d_i because they uniquely determine (the size of) the dimension jumps of $\mathcal{L}\big(D + r(x)_\infty)\big)$ at $r = -d_1, \dots, -d_n$.

We consider the case $R = \mathbb{Z}$. Here (i) is just a repetition of Theorem 7. In order to prove (ii) let $v_1, \dots, v_n$ be a weakly reduced basis of Λ_D and $t_i := -\lceil \log_q \|v_i\|_D \rceil$. For an arbitrary $\alpha = \sum_{i=1}^n \lambda_i v_i$ with $\lambda_i \in k[x]$ and $r \in \mathbb{Z}$ we get the following equivalences since the v_i are weakly reduced:

$$\begin{aligned} \alpha \in \mathcal{L}(D + r(x)_\infty) &\Leftrightarrow \log_q \|\alpha\|_D \leq r \\ &\Leftrightarrow \lceil \log_q \|\lambda_i v_i\|_D \rceil \leq r, \text{ for } 1 \leq i \leq n, \\ &\Leftrightarrow \deg \lambda_i \leq t_i + r, \text{ for } 1 \leq i \leq n. \end{aligned}$$

Hence we obtain that the v_i form a $\mathbb{Z}$-parametric basis of D with $d_i = t_i$.

To show the converse we first note that the v_i constitute a basis of Λ_D because of $\Lambda_D = \bigcup_{r \in \mathbb{Z}} \mathcal{L}(D + r(x)_\infty)$, which follows from the equivalence mentioned at the beginning of the proof, and the parametric basis property. Now let $\alpha = \sum_{i=1}^n \lambda_i v_i$ be arbitrary and $r \in \mathbb{Z}$ minimal such that $\alpha \in \mathcal{L}(D + r(x)_\infty)$. From the parametric basis property we get that $\lambda_i v_i \in \mathcal{L}(D + r(x)_\infty)$. From the equivalence at the beginning of the proof we see $\log_q \|\alpha\|_D \leq r$ and $\log_q \|\lambda_i v_i\|_D \leq r$ for all $1 \leq i \leq n$. Because of the minimality of r we obtain $r = \lceil \log_q \|\alpha\|_D \rceil \leq \max_{i=1}^n \lceil \log_q \|\lambda_i v_i\|_D \rceil \leq r$ and the v_i are weakly reduced. The uniqueness of the d_i for any fixed $\mathbb{Z}$-parametric basis as stated at the beginning of the proof finally shows that $d_i = -\lceil \log_q \|v_i\|_D \rceil$ because of the first part of the proof of (ii).

We switch to the case $R = \mathbb{Q}$. In order to prove (ii) we can use the same reasoning as in the proof of (ii) for the case $R = \mathbb{Z}$ above but with $r \in \mathbb{Q}$ and without $\lceil \cdot \rceil$. From (ii) the existence statement in (i) is now seen to be true because there exists a reduced basis of Λ_D. We deduce the uniqueness of the d_i for any $\mathbb{Q}$-parametric basis and the $k(x)$-linear independence from (ii) as well because this

implies that the v_i constitute a reduced $k[x]$-basis of Λ_D and realize the successive minima (which are unique). □

8. Divisor reduction

We continue the discussion of section 6. In order to simplify the notation we now consider the degrees and the dimensions over the exact constant field k_0 and we assume $k = k_0$.

Definition 17. *Let A be a divisor with $\deg(A) \geq 1$. The divisor $\widetilde{D}$ is called* maximally reduced along A *if $\widetilde{D} \geq 0$ and $\dim(\widetilde{D} - rA) = 0$ holds for all $r \geq 1$. The representation of a divisor D as $D = \widetilde{D} + rA - (a)$ with a divisor $\widetilde{D}$ maximally reduced along A, $r \in \mathbb{Z}$, $a \in F^\times$ is called a* maximal reduction of D along A.

This generalizes the reduction strategy of [15]. Being reduced is not such an interesting property of a divisor per se, but because of its application for computations within the divisor class group it plays an important role. We note the following additional properties where the genus of F/k is denoted by g: $\dim(\widetilde{D}) \leq \deg(A)$ and $\deg(\widetilde{D}) < g + \deg(A)$ holds for divisors $\widetilde{D}$ maximally reduced along A.

For a maximal reduction $D = \widetilde{D}_1 + rA - (a)$ all other maximal reductions have the same degree and are formed by $\widetilde{D}_2 := (b) + \widetilde{D}_1$ for $b \in \mathcal{L}(\widetilde{D}_1)$. We thus see that maximal reductions along A are in a 1-1-relation to the points of the projective space $\mathbb{P}^{\dim(\widetilde{D}_1)}(k)$ by means of a basis of $\mathcal{L}(\widetilde{D}_1)$.

Proposition 18. *Let A be a divisor with $\deg(A) = 1$. The maximal reduction of a divisor D along A is then unique. In other words: For each divisor class $[D]$ there is exactly one divisor $\widetilde{D}$ maximally reduced along A and a uniquely determined $r \in \mathbb{Z}$ such that $[D] = [\widetilde{D} + rA]$.*

Proof. We take $[D - rA]$ with the maximal possible, uniquely determined $r \in \mathbb{Z}$ such that $\dim\big([D - rA]\big) = 1$ holds. The class $[D - rA]$ contains only one positive divisor $\widetilde{D}$ and this is maximally reduced along A. Thus $\widetilde{D} + rA$ is a unique representative of $[D]$. The uniqueness of (a) follows because of $(a) = \widetilde{D} + rA - D$. □

We now explain the steps for a reduction of divisors in free representation, similar to the proof of the proposition. This will be very helpful for the computation of Riemann-Roch spaces of divisors with large height or large degree.

Let A be an arbitrary divisor with small height and small degree; for example, a prime divisor of degree one (if there is one). A divisor D with large exponents can be "exhausted" by A: This means that we subtract from D a large (as large as possible) multiple of A such that $D - rA$ still has a dimension greater than zero. Here r can be negative itself for a divisor of negative degree. With this procedure we can achieve that $\widetilde{D} = (a) + D - rA$ becomes a divisor either maximally reduced along A or just a positive divisor with bounded degree. In particular we then have $D = \widetilde{D} + rA - (a)$ and $\mathcal{L}(D) = a \cdot \mathcal{L}(\widetilde{D} + rA)$.

We observe two things: Firstly, if a is known, we can determine $\widetilde{D}$ in ideal representation in order to avoid factorization. Secondly, the computation of a and $\widetilde{D}$ is still difficult since $h(D - rA)$ is in general not small compared to $h(D)$. This explicit representation of D by $\widetilde{D}$ as above is called *elementary reduction along A*, the choice of r will be determined later. The elementary reduction should only be performed for divisors of small height.

Next, there are unique divisors $D_0, \ldots, D_m$ such that $D = \sum_{i=0}^{m} 2^i D_i$ holds and the exponents in the D_i have absolute value 1. The number of places in D_i should not be too large. We evaluate this sum according to the Horner (or double-and-add) method, where an elementary reduction is performed before each multiplication. With $\widetilde{D}_{m+1} := 0$ we assume inductively for $-1 \leq j < m$ that

$$D = 2^{m-j}\widetilde{D}_{m-j} + \sum_{i=0}^{m-j-1} 2^i D_i + A \sum_{i=m-j}^{m} 2^i r_i - \sum_{i=m-j}^{m} 2^i (a_i)$$

holds. By an elementary reduction of $2\,\widetilde{D}_{m-j} + D_{m-j-1}$ we get the representation $2\,\widetilde{D}_{m-j} + D_{m-j-1} = \widetilde{D}_{m-j-1} + r_{m-j-1}A - (a_{m-j-1})$. By substituting this term we see that the representation of D with j also holds for $j+1$. Hence we get for $j = m$:

$$D = \widetilde{D}_0 + A\sum_{i=0}^{m} 2^i r_i - \sum_{i=0}^{m} 2^i (a_i) \tag{19}$$

The size of the exponents of D contributes only logarithmically to the costs whereas the number of places appearing in a single D_i is still a problem. We can sum up the places of D_i successively, and after each step we get subdivisors in ideal representation to which we apply the elementary reduction. The number of places then enters the running time in a linear way but an increase of the heights is avoided. We thus write $D_i = D_i' + l_i A - \sum_{j=1}^{t}(b_{i,j})$ where t is the number of places in D and D_i' is reduced. We substitute this into $\sum_{i=0}^{m} 2^i D_i$ and apply the procedure for (19) to $\sum_{i=0}^{m} 2^i D_i'$. In summary we get:

$$D = \widetilde{D}_0 + A\sum_{i=0}^{m} 2^i (r_i + l_i) - \sum_{i=0}^{m} 2^i \left((a_i) + \sum_{j=1}^{t} (b_{i,j}) \right) \tag{20}$$

We now discuss the choice of r in the elementary reduction. There are at least two strategies: degree reduction and maximal reduction along A. The degree reduction returns a positive divisor $\widetilde{D}$ of bounded degree whereas the maximal reduction results in a divisor $\widetilde{D}$ maximally reduced along A. In the degree reduction we determine $D - rA$ with a maximal $r \in \mathbb{Z}$ such that $g \leq \deg(D - rA) < g + \deg(A)$ holds. We get a positive, possibly rather large dimension, and $g \leq \deg(\widetilde{D}) < g + \deg(A)$ also holds for the reduced divisor $\widetilde{D}$. This reduction need not be unique. In the maximal reduction, similar to the proof of Proposition 18, we determine $D - rA$ with a maximal $r \in \mathbb{Z}$ such that $0 < \dim(D - rA) \leq \deg(A)$ holds. Several tries of values r might be neccessary but can be done, for example, using a binary search strategy. We then have $\deg(\widetilde{D}) < g + \deg(A)$, thus the degree can also be smaller than g. This reduction is unique for a divisor A of degree one. Both ways of reduction often give the same result for a given divisor.

We summarize the procedure in an algorithm:

Algorithm 21. *(Divisor reduction)*

Input: *Divisors A, D of the algebraic function field F/k, where D is in free representation and $\deg(A) > 0$, and a strategy for the elementary reduction.*

Output: *A positive divisor $\widetilde{D}$ with $\deg(\widetilde{D}) < g + \deg(A)$, given in ideal representation, an $r \in \mathbb{Z}$ and elements $a_i, b_{i,j} \in F^\times$ such that $D = \widetilde{D} + rA - \sum_{i=0}^{m} 2^i \big((a_i) + \sum_{j=1}^{t}(b_{i,j})\big)$ with $t := |\mathrm{supp}(D)|$ holds.*

(1) *(Decomposition of D) Compute $m \in \mathbb{Z}$ and divisors $D_0, \ldots, D_m$ whose exponents have absolute value 1 and for which $D = \sum_{i=0}^{m} 2^i D_i$ holds.*
(2) *(Support reduction) For each $i := 0, \ldots, m$ the divisors D'_i are successively computed in ideal representation, where an elementary reduction is performed after each addition resp. subtraction of a prime divisor of D_i. This provides $D_i = D'_i + l_i A - \sum_{j=1}^{t}(b_{i,j})$.*
(3) *(Exponent reduction) Let $\widetilde{D}_{m+1} := 0$. For $j := -1, \ldots, m-1$ compute a divisor $\widetilde{D}_{m-j-1}$ in ideal representation, an $r_{m-j-1} \in \mathbb{Z}$ and $a_{m-j-1} \in F$ by applying elementary reduction to $2\,\widetilde{D}_{m-j} + D'_{m-j-1}$ so that $2\,\widetilde{D}_{m-j} + D'_{m-j-1} = \widetilde{D}_{m-j-1} + r_{m-j-1}A - (a_{m-j-1})$ holds.*
(4) *(End) Let $\widetilde{D} := \widetilde{D}_0$ and $r := \sum_{i=0}^{m} 2^i(r_i + l_i)$. Output of $\widetilde{D}$, r and $a_i, b_{i,j}$. Terminate.*

Remark 22. *The size of the exponents enters the running time logarithmically, the number of places in D linearly. The last statement holds since the height of the D'_i is always bounded because of the reduction depending on* $\deg(A)$. *Altogether there is a constant $\alpha \in \mathbb{R}^{>0}$ such that the running time of algorithm 21 is less than or equal to $O\big(\log(h(D))\,|\mathrm{supp}(D)|\,(nC_f \deg(A)d)^{\alpha}\big)$, where d is the maximal degree of the places in D.*

If we have a divisor A with $\deg(A) = 1$ and apply the maximal reduction as strategy for the elementary reduction, algorithm 21 provides the unique maximal reduction of D along A for each divisor D (since a maximal reduction is performed in the last step). Thus we can compute unique representatives for divisor classes. If we choose an A of larger degree in the case of a global function field over the exact constant field with q elements, we get at most $(q^{\deg(A)} - 1)/(q-1)$ possibilities for a maximal reduction $\widetilde{D}$, resulting in a "bounded" ambiguity.

The maximal elementary reduction can particularly efficiently be performed in the case $A = (x)_\infty$ because the maximal possible $r \in \mathbb{Z}$ equals $|D|_1$ according to Theorem 7 resp. Theorem 16 and no tries over several r are neccessary.

Remark 23. *The divisor reduction can be generalized if we replace the set of possible reduction divisors $\{\, rA \mid r \in \mathbb{Z} \,\}$ by $\{\, \lceil rA \rceil \mid r \in \mathbb{Q} \,\}$ (apply $\lceil\cdot\rceil$ exponentwise). The maximal reduction then finds the largest $r \in \mathbb{Q}$ such that there is an $a \in \mathcal{L}(D - \lceil rA \rceil)$ and computes $\widetilde{D} := D - \lceil rA \rceil + (a)$. Here A is required to be known in free representation as well.*

The advantage of this generalization is that for $A = (x)_\infty$ we can still use the fast elementary reduction with $r = d_1$ according to Theorem 16, now using series expansions, but may get much smaller maximal reductions if $(x)_\infty$ is of a suitable form, most notably $(x)_\infty = eP$. Namely, the possible reduction divisors in $\{\, \lceil rA \rceil \mid r \in \mathbb{Q} \,\}$ are just integral multiplies of P so that reducing by $(x)_\infty$ in this case is the same as reducing by P.

By means of divisor reduction and with the relation $\mathcal{L}(D) = a \cdot \mathcal{L}(\widetilde{D} + rA)$ for $D = \widetilde{D} + rA - (a)$ we can now compute Riemann-Roch spaces also for "large" divisors. For this we consider two cases: If a divisor D has large exponents, but a small degree, the computation of $\mathcal{L}(\widetilde{D} + rA)$ for the divisor reduction $D = \widetilde{D} + rA - (a)$ should be no problem, since the dimension is small as well. If the degree of D is large, the dimension is also large and giving a basis could be difficult. But even

this is no problem according to Theorem 7, if we use $A = (x)_\infty$. Namely, in this case the basis elements can be given parametrically. From this results

Algorithm 24. *(Computation of Riemann-Roch spaces II)*
Input: *A divisor D of the algebraic function field F/k.*
Output: *A k-basis of $\mathcal{L}(D)$ in short representation as in Theorem 7 where the basis elements v_i are given by power products of elements from $F^\times$.*

(1) *(Reduction) Perform a divisor reduction of D according to algorithm 21 using $A = (x)_\infty$ and the degree reduction. Obtain $\widetilde{D}$, $r \in \mathbb{Z}$ and $a \in F^\times$ with $D = \widetilde{D} + rA - (a)$, where a is the power product of the a_i and $b_{i,j}$.*
(2) *(Riemann-Roch) Using algorithm 13 compute a basis of $\mathcal{L}(\widetilde{D})$ in short representation given by $v'_1, \ldots, v'_n$ and $d'_1, \ldots, d'_n$.*
(3) *(End) Let $v_j := av'_j$, $d_j := d'_j + r$ for $j := 1, \ldots, n$. Output of $v_1, \ldots, v_n$ and $d_1, \ldots, d_n$. Terminate.*

Remark 25. *According to Remark 22 the costs for this algorithm are of the same form as for algorithm 21.*

9. Applications

The theorem of Riemann-Roch dominates the whole theory of algebraic function fields. Thus constructive methods within the Riemann-Roch theory are applicable for many purposes. We mention some examples:

The construction of *algebraic-geometric codes* can be performed by means of bases of Riemann-Roch spaces and by bases of differential spaces related to divisors, [16, 24, 37].

The computation of *differential spaces* $\Omega(D) := \{\, \omega \in \Omega(F/k) \,|\, (\omega) \geq D \,\}$, compare [27, 37], can also be reduced to the computation of Riemann-Roch spaces. Let the function field F/k over the perfect field k be defined by $f(x, y) = 0$, where $f(x, y) \in k[x, y]$ is irreducible, separable and monic in y. We explain the procedure briefly. By application of the differential operator d to $f(x, y) = 0$ we get, according to the rules of differentiation, an F-linear relation between dy and dx:

$$dy = -\frac{f_x}{f_y} dx,$$

where the denominator is not zero due to the assumption on $f(x, y)$ being separable (f_x and f_y are the partial derivatives with respect to x and y). An arbitrary element a of F can be represented as a rational function in x, y. By applying d to a in this representation and observing the relation between x and y we get $b \in F$ with $da = b\,dx$. We know that each differential can be represented as $b\,dx$ for a suitable $b \in F$. The divisor of the differential $b\,dx$ is $(b\,dx) = (b) + (dx)$ where $(dx) = \mathcal{D}_{F/k(x)} - 2(x)_\infty$ holds, see [37, p. 156 (3.16)]. As usual, we can easily compute the different divisor by means of the trace matrix [8, p. 203, 4.8.18]. Summing up we are able to determine the divisor of an arbitrary differential. On the other hand, we see that the inequality $(b\,dx) \geq D$ holds for a divisor D if and only if $(b) + (dx) - D \geq 0$. This equivalence provides a k-vector space isomorphism $\Omega(D) \longrightarrow \mathcal{L}((dx) - D)$ by means of which we are finally able to compute a k-basis of $\Omega(D)$.

Another important application is the possibility to compute explicitly within the *divisor class group* of an algebraic function field, as previously described in [21,

38, 39]. Using our methods this can be performed in the very general setting of section 3.2. If two divisor classes $[D_1]$ and $[D_2]$ are given, $[D_1]+[D_2]=[D_1+D_2]$ and $k[D_1]=[kD_1]$ trivially hold. But there is the question if two classes are equal resp. if a class is the principal class. Now $[D_1]$ and $[D_2]$ are equal if and only if $\deg(D_1)=\deg(D_2)$ and $\dim(D_1-D_2)>0$, and this "principal divisor test" can easily and effectively be performed with the described methods. The logarithmic dependence of algorithm 21 on $h(D_1-D_2)$ is crucial for the global function field case. Additionally we note that also unique class representatives can be selected, as explained after algorithm 21.

Finally, the computation of Riemann-Roch spaces plays a central role in the generation of relations for the *computation of S-units, discrete logarithms in the divisor class group* and *the structure of the divisor class group* of a global function field [18], which will be described in a forthcoming paper.

10. Appendix: The theorem of Riemann-Roch

By applying the ideal-theoretical language from section 5 we now give a short, elementary and constructive proof of the theorem of Riemann-Roch (Theorem 29). Let again x denote a separating element of F/k, $S:=\operatorname{supp}\big((x)_\infty\big)$ and $n:=[F:k(x)]$.

We first need some further basic statements about the connection of divisors and ideals. We recall that the norm $\mathrm{N}_{F/k(x)}(\mathfrak{a})$ of a (fractional) ideal $\mathfrak{a}$ of $\mathfrak{o}^S$ or $\mathfrak{o}_S$ is defined to be the determinant of a transformation matrix of an integral basis to an ideal basis of $\mathfrak{a}$ (modulo units of $k[x]$ or $\mathfrak{o}_\infty$) and is multiplicative. From this one can see that for two ideals $\mathfrak{a},\mathfrak{b}$ of $\mathfrak{o}^S$ or $\mathfrak{o}_S$ the determinant of a transformation matrix of a basis of $\mathfrak{a}$ to a basis of $\mathfrak{ab}$ is given by $\mathrm{N}_{F/k(x)}(\mathfrak{b})$, up to the respective units again. For a prime ideal $\mathfrak{p}$ of $\mathfrak{o}^S$ and the corresponding place P of F/k we have $\deg(P)=\deg(\mathrm{N}_{F/k(x)}(\mathfrak{p}))$. Similarly, for a prime ideal of $\mathfrak{o}_S$ and the corresponding place P of F/k we have $\deg(P)=-\deg(\mathrm{N}_{F/k(x)}(\mathfrak{p}))$. This implies

$$\deg_k(D)=\deg\big(\mathrm{N}_{F/k(x)}(D^S)\big)-\deg\big(\mathrm{N}_{F/k(x)}(D_S)\big)$$

for any divisor D of F/k.

We now assume that we are in the situation exactly after the proof of Theorem 7. As the theorem of Riemann-Roch was used in its proof, Corollary 11 needs to be reformulated as follows:

Corollary 26. *For an algebraic function field F/k there exists a constant $c_{k,x}\in\mathbb{Z}$, depending only on the constant field k and on the chosen separating element x such that the following holds for the $k[x]$-invariants of a divisor D:*

$$\sum_{i=1}^{n}|D|_i \;=\; \deg_k D + c_{k,x} - n.$$

Proof. Let M_E, M_{D+E} be transformation matrices from $(E_S)^{-1}$ to $(E^S)^{-1}$ and from $(D_SE_S)^{-1}$ to $(D^SE^S)^{-1}$ respectively. From the first paragraph of the proof of Theorem 7 we see that $-\sum_{i=1}^{n}|E|_i=\deg(\det(M_E))$ and analogously $-\sum_{i=1}^{n}|D+E|_i=\deg(\det(M_{D+E}))$. Let M_1 be a transformation matrix from a basis of $(E_S)^{-1}$ to a basis of $(D_SE_S)^{-1}$. Analogously, let M_2 be a transformation matrix from a basis of $(E^S)^{-1}$ to a basis of $(D^SE^S)^{-1}$. We get $\det(M_1)=\mathrm{N}_{F/k(x)}(D_S)^{-1}$ and

$\det(M_2) = \mathrm{N}_{F/k(x)}(D^S)^{-1}$, up to units. For the matrices together we have

$$M_E = M_1 M_{D+E} M_2^{-1}.$$

Applying determinants and then the degree function we obtain

$$\deg(\det(M_E)) = \deg(\det(M_1)) + \deg(\det(M_{D+E})) - \deg(\det(M_2)).$$

From this we see

$$\begin{aligned} -\sum_{i=1}^{n} |E|_i &= -\sum_{i=1}^{n} |D+E|_i - \deg(\mathrm{N}_{F/k(x)}(D_S)) + \deg(\mathrm{N}_{F/k(x)}(D^S)) \\ &= \deg_k(D) - \sum_{i=1}^{n} |D+E|_i \end{aligned}$$

and finally

$$\sum_{i=1}^{n} |D+E|_i = \deg_k(D) + \sum_{i=1}^{n} |E|_i.$$

Substituting the zero divisor for E in this formula proves the assertion for $c_{k,x} := n + \sum_{i=1}^{n} |0|_i$. □

The sum of the $k[x]$-invariants of a divisor is equal to its degree plus a constant, only dependent on k, x and the function field F/k. According to Theorem 7 (for $r = 0$) we can now view the sum of the non-negative $|D|_i$ approximately as the dimension of $\mathcal{L}(D)$. In order to prove the theorem of Riemann-Roch we will show that there is a divisor D^* *dual* to D with non-negative $|D^*|_i$ approximately equal to $-|D|_i$ for $|D|_i < 0$. This means $\dim_k D - \dim_k D^* \approx \sum_{i=1}^{n} |D|_i = \deg_k D +$ a constant which already is the Riemann-Roch equation except for some inaccuracies.

In order to prove the existence of such a D^* we use complementary ideals, complementary divisors and their basic properties (see for example [23, pp. 88]): Let A be a principal ideal domain, K the quotient field of A, L/K a separable field extension of degree n and B the integral closure of A in L. If $\mathfrak{a}$ is a (fractional) ideal of B, then $\mathfrak{a}^{\#} := \{\alpha \in L \mid \mathrm{Tr}_{L/K}(\alpha\mathfrak{a}) \subseteq A\}$ is the *complementary* ideal of $\mathfrak{a}$. If $a_1, \ldots, a_n$ is an A-basis of $\mathfrak{a}$ then there are $a_1^{\#}, \ldots, a_n^{\#} \in \mathfrak{a}^{\#}$ with $\mathrm{Tr}_{L/K}(a_i^{\#} a_j) = \delta_{i,j}$ for $1 \le i, j \le n$, and they form an A-basis of $\mathfrak{a}^{\#}$. If $\mathfrak{b}$ is a further ideal of B, we have $(\mathfrak{a}\mathfrak{b})^{\#} = \mathfrak{a}^{\#}\mathfrak{b}^{-1}$. Back in our function field situation, let the divisor D be represented by $(\mathfrak{a}, \mathfrak{b})$. We define the $k(x)$-*complementary* divisor $D^{\#}$ to D to be the divisor represented by $\big(((\mathfrak{a}^{-1})^{\#})^{-1}, ((\mathfrak{b}^{-1})^{\#})^{-1}\big)$. We note that this definition actually depends only on the rational function field $k(x)$ and not on x itself. As above, the identity $(D+E)^{\#} = D^{\#} - E$ holds for divisors D and E. The *different divisor* $\mathcal{D}_{F/k(x)}$ of $F/k(x)$ is equal to the $k(x)$-complementary divisor of the zero divisor. Finally, for a divisor D we define the (k,x)-*dual divisor* D^* to be $D^{\#} - 2(x)_\infty$.

The following statements form the basis of the theorem of Riemann-Roch:

Lemma 27. *For the $k[x]$-invariants of the divisor $D^{\#}$, $k(x)$-complementary to D, we have*

$$|D^{\#}|_i = -|D|_i$$

for all $1 \le i \le n$.

Proof. We abbreviate $\mathfrak{a} = (D^S)^{-1}$ and $\mathfrak{b} = (D_S)^{-1}$. Then $D^{\#}$ is represented by $(\mathfrak{a}^{\#})^{-1}$ and $(\mathfrak{b}^{\#})^{-1}$. As in section 5 let $a_1, \ldots, a_n$ be a $k[x]$-basis of $\mathfrak{a}$ and $b_1, \ldots, b_n$ an $\mathfrak{o}_\infty$-basis of $\mathfrak{b}$ such that $b_i = x^{|D|_i} a_i$ holds for $1 \le i \le n$. It is sufficient to

prove $b_i^{\#} = x^{-|D|_i} a_i^{\#}$: There is $\lambda_{i,j} \in k(x)$ such that $a_j^{\#} = \sum_{i=1}^{n} \lambda_{i,j} b_i^{\#}$ holds. We thus get $\lambda_{i,j} = \mathrm{Tr}_{F/k(x)}(a_j^{\#} b_i) = x^{|D|_i} \mathrm{Tr}_{F/k(x)}(a_j^{\#} a_i) = x^{|D|_i} \delta_{i,j}$ where the first and the last identity follow because of the dual basis property, and the second identity follows because $b_i = x^{|D|_i} a_i$. □

Lemma 28. *For every divisor D of F/k and its (k,x)-dual divisor D^* the equation*

$$\dim_k D \;=\; \deg_k D + c_{k,x} + \dim_k D^*$$

holds.

Proof. We have $\sum_{|D|_i \geq 0}(|D|_i+1) + \sum_{|D|_i \leq -1}(|D|_i+1) = \sum_{i=1}^{n} |D|_i + n = \deg_k D + c_{k,x}$ because of Corollary 26. According to Theorem 7 the dimension $\dim_k D$ is equal to the first sum above. Because of Lemma 27 and Theorem 7 we can see that the $k[x]$-invariants of D^* correspond to $|D^*|_i = -|D|_i - 2$. Summing up for the dimension of D^* already results in $\dim_k D^* = \sum_{|D^*|_i \geq 0}(|D^*|_i+1) = -\sum_{|D|_i \leq -1}(|D|_i+1)$, the negative of the second sum above. □

Because of what was said above about complementary divisors, D^* can be written as $D^* = W_{k,x} - D$ where we define $W_{k,x}$ to be $\mathcal{D}_{F/k(x)} - 2(x)_\infty$. Furthermore, let l be the dimension of the exact constant field k_0 of F/k over k. With Lemma 28 we validate that $c_{k,x}$ is divisible by l and that (use the zero divisor) $c_{k,x} \leq l$ holds. We finally define the *genus* of F/k to be $g := 1 - c_{k,x}/l$ and we get

Theorem 29 (Riemann-Roch)**.** *The set of divisors W of F/k, for which the equation*

$$\dim_k D \;=\; \deg_k D + l(1-g) + \dim_k(W - D)$$

with arbitrary divisors D holds, forms a non-empty divisor class of F/k. Its elements W, the canonical divisors, are precisely characterized by $\dim_k W = lg$ and $\deg_k W = 2l(g-1)$ among all divisors of F/k.

Proof. The divisors $W_{k,x}$ are canonical divisors, since they satisfy the required equation for all divisors D because of the previous lemma. Furthermore, the definition of the genus does not depend on k or x, since for divisors D of large positive degree $\dim_{k_0}(W_{k,x} - D) = 0$, i.e. $1 - g = \dim_{k_0} D - \deg_{k_0} D$ holds, and the right hand side is certainly independent of D. If W_1 fulfills the above equation for all divisors D, we have $\dim_k W_1 = lg$ and $\deg_k W_1 = 2l(g-1)$, as we can see by substituting the zero divisor and W_1 for D. If the equations $\dim_k W_2 = lg$ and $\deg_k W_2 = 2l(g-1)$ hold for W_2 then we have $\dim_k(W_1 - W_2) = l$ and $\deg_k W_1 - W_2 = 0$ such that W_1 and W_2 belong to the same divisor class. This proves the last statement and shows that the canonical divisors indeed form a divisor class. □

11. Acknowledgments

The author would like to thank S. Galbraith, M. E. Pohst and N. P. Smart for helpful comments, and for the support by a NaFöG and EPSRC grant.

References

[1] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symbolic Comp.*, 24, 3/4:235–265, 1997.

[2] A. Brill and M. Noether. Über die algebraischen Functionen und ihre Anwendung in der Geometrie. *Math. Ann.*, 7:269–310, 1874.

[3] J. Buchmann and H. Lenstra. Approximating rings of integers in number fields. *J. Theor. Nombres Bordx.*, 6(2):221–260, 1994.
[4] A. Campillo. *Algebroid curves in positive characteristic*. LNM 813. Springer-Verlag, Berlin-Heidelberg-New York, 1980.
[5] C. Chevalley. *Introduction to the theory of algebraic functions of one variable*, volume 6 of *Mathematical Surveys*. American Mathematical Society, New York, 1951.
[6] A. L. Chistov. The complexity of constructing the ring of integers of a global field. *Soviet Math. Dokl.*, 39:597–600, 1989.
[7] J. Coates. Construction of rational functions on a curve. *Proc. Camb. Phil. Soc.*, 68:105–123, 1970.
[8] H. Cohen. *A course in Algebraic Number Theory*. 3rd corr. printing, GTM 138. Springer-Verlag, Berlin-Heidelberg-New York, 1996.
[9] P. M. Cohn. *Algebraic Numbers and Algebraic Functions*. Chapman & Hall, London, 1991.
[10] Comp. algebra group. Magma. `http://www.maths.usyd.edu.au:8000/u/magma/`, 2004.
[11] J. H. Davenport. *On the integration of algebraic functions*. LNCS 102. Springer-Verlag, Berlin-Heidelberg-New York, 1981.
[12] R. Dedekind and H. Weber. Theorie der algebraischen Functionen einer Veränderlichen. *J. Reine angew. Math.*, 92:181–290, 1882.
[13] C. Friedrichs. Berechnung relativer Ganzheitsbasen mit dem Round-2-Algorithmus. MSc Thesis, Technische Universität Berlin, 1997.
[14] W. Fulton. *Algebraic curves*. Benjamin, New York, 1969.
[15] S. Galbraith, S. Paulus, and N. P. Smart. Arithmetic on superelliptic curves. *Math. Comp.*, 71:393–405, 2002.
[16] G. Haché. Computation in algebraic function fields for effective construction of algebraic-geometric codes. In G. Cohen et al., editors, *Applied algebra, algebraic algorithms and error-correcting codes, AAECC-11*, LNCS 948, pages 262–278, Paris, 1995. Springer-Verlag, Berlin-Heidelberg-New York.
[17] K. Hensel and G. Landsberg. *Theorie der algebraischen Funktionen einer Variabeln und ihre Anwendung auf algebraische Kurven und Abelsche Integrale*. B. G. Teubner, Leipzig, 1902.
[18] F. Hess. *Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern*. PhD Thesis, Technische Universität Berlin, 1999.
[19] M. van Hoeij. An algorithm for computing the Weierstrass normal form. In A. H. M. Levelt, editor, *Proceedings of the International Symposium on Symbolic and Algebraic Computation, ISSAC '95*, pages 90–95, Montreal, Canada, 1995. ACM Press, New York.
[20] M. van Hoeij. Rational parametrizations of algebraic curves using a canonical divisor. *J. Symbolic Comp.*, 23, 2-3:209–227, 1997.
[21] M.-D. Huang and D. Ierardi. Counting points on curves over finite fields. *J. Symbolic Comp.*, 25:1–21, 1998.
[22] Kant group. Kash. `http://www.math.tu-berlin.de/~kant`, 2004.
[23] H. Koch. *Zahlentheorie*. Vieweg Verlag, Braunschweig, 1997.
[24] D. Le Brigand and J. J. Risler. Algorithme de Brill-Noether et codes de Goppa. *Bull. Soc. Math. France*, 116:231–253, 1988.
[25] A. K. Lenstra. Factoring multivariate polynomials over finite fields. *J. Comput. Syst. Sci.*, 30:235–248, 1985.
[26] R. Matsumoto and S. Miura. Finding a basis of a linear system with pairwise distinct discrete valuations on an algebraic curve. *J. Symbolic Comp.*, 30:309–323, 2000.
[27] C. Moreno. *Algebraic curves over finite fields*. Cambridge University Press, Cambridge, 1991.
[28] M. Noether. Rationale Ausführung der Operationen in der Theorie der algebraischen Functionen. *Math. Ann.*, 23:311–358, 1884.
[29] S. Paulus. Lattice basis reduction in function fields. In J. Buhler, editor, *Proceedings of the Third Symposium on Algorithmic Number Theory, ANTS-III*, LNCS 1423, pages 567–575, Portland, Oregon, 1998. Springer-Verlag, Berlin-Heidelberg-New York.
[30] L. Pecquet. Private communication, 1999.
[31] M. E. Pohst. *Computational algebraic number theory*. DMV-Seminar 21. Birkhäuser Verlag, Basel-Boston-Berlin, 1993.

[32] M. E. Pohst and M. Schörnig. On integral basis reduction in global function fields. In H. Cohen, editor, *Proceedings of the Second Symposium on Algorithmic Number Theory, ANTS-II*, LNCS 1122, pages 273–282, Talence, France, 1996. Springer-Verlag, Berlin-Heidelberg-New York.

[33] M. E. Pohst and H. Zassenhaus. *Algorithmic Algebraic Number Theory*. Cambridge University Press, Cambridge, 1st paperback edition, 1997.

[34] F. K. Schmidt. Analytische Zahlentheorie in Körpern der Charakteristik *p*. *Math. Z.*, 33:1–32, 1931.

[35] W. M. Schmidt. Construction and estimation of bases in function fields. *J. Number Th.*, 39:181–224, 1991.

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

[37] H. Stichtenoth. *Algebraic Function Fields and Codes*. Springer-Verlag, Berlin-Heidelberg-New York, 1993.

[38] E. Volcheck. Computing in the Jacobian of a plane algebraic curve. In L. Adleman et al., editors, *Proceedings of the First Symposium on Algorithmic Number Theory, ANTS-I*, LNCS 877, pages 221–233, Ithaca, New York, 1994. Springer-Verlag, Berlin-Heidelberg-New York.

[39] E. Volcheck. Addition in the Jacobian of a curve over a finite field. Computational Number Theory (Oberwolfach), conference manuscript, 1995.