TECHNISCHE UNIVERSITÄT WIEN

Unterschrift des Betreuers

Diplomarbeit

Algebraic Function Fields, Algebraic Curves and Goppa Codes

Ausgeführt am Institut für
Diskrete Mathematik und Geometrie
der Technischen Universität Wien

unter der Anleitung von
Ao.Univ.Prof. Dipl.-Ing. Dr.techn. Gerhard Dorfer

durch
Peter Michael Kuleff
Lambrechtgasse 10/29
1040 Wien

Datum

Unterschrift

Abstract

This thesis gives an introduction into the theory of algebraic function fields and algebraic curves with an application to Goppa codes. The first two chapters focus on function fields in a purely algebraic setting and have the Riemann-Roch Theorem as their main result. Algebraic curves are approached from the perspective of function fields. Two kinds of Goppa codes are defined via places and local components of differentials, respectively. An example of how to construct Goppa codes from algebraic curves is given. In the last chapter a standard decoding scheme as well as a list decoding algorithm for Goppa codes are presented.

Preface

I was always fascinated when I heard how a piece of abstract discrete mathematics could be used to solve "real word" problems. When diving deeper into the subject matter of such a solution, it is even more astonishing to see in what elegant ways results from algebra or number theory can be used to tackle problems in information technology. A particularly beautiful example of this are Goppa codes, also called algebraic geometry codes. Since their theoretical fundament involves field theory, algebraic geometry and the theory of algebraic function fields – subjects that I am greatly interested in – this topic felt like the right choice for the thesis when I first came across it.

I wrote this thesis from June 2016 onwards. Originally, I planned to put more emphasis on decoding algorithms of Goppa codes. However, I felt that elaborating the underlying theory was indispensable. Especially when it comes to providing concrete examples of Goppa codes, a profound knowledge of the function field of an algebraic curve is very important. Therefore, the theoretical part given in Chapters 1 to 3 became more extensive than I intended it to be. In chapter 5, besides the well-known decoding scheme of Vlăduţ and Skorobogatov, I focused on the list decoding algorithm developed by Sudan, Shokrollahi and Wasserman. In my opinion, the list decoding approach is itself interesting since it is a contrast to the "standard" approach of nearest neightbour decoding. In particular, list decoding of Goppa codes revealed an interesting result about the number of code words in a Hamming ball of a given radius.

I would like to thank a few people who made it possible for me to complete this thesis. First of all, I would like to thank my advisor, Prof. Gerhard Dorfer. He supported me constantly throughout the writing process, read drafts and paid attention to every detail. He suggested studying the books of Stichtenoth [14] and Pretzel [11], which shaped the Chapters 1 to 3, and encouraged me to look into list decoding of Goppa codes, an approach I was not aware of. My thanks also go to my friends Isaak Granzer, who corrected the text and gave me valuable comments on it, and Jordy van Velthoven, for discussing and suggesting various books. I am most grateful to my parents, Peter and Ursula, for supporting me my whole life, for their constant encouragement and for enabling my studies.

Vienna, February 2017 Peter Michael Kuleff

Contents

Chapter 1

Algebraic Function Fields

In this chapter we will give an introduction to the theory of algebraic function fields. An algebraic function field is a field extension F/K of transcendence degree one. This concept naturally arises in the theory of algebraic curves. More precisely, the set of rational functions on an algebraic curve is an algebraic function field (see Chapter 3). However, it is possible to study these objects in a purely algebraic setting. We shall follow this approach in this chapter. We will develop basic results about algebraic function fields as in the book [1] by Chevalley and [14] by Stichtenoth. The reader interested in the theory of algebraic function fields with applications to algebraic curves may be refered to [10] or [11] which treat this subject in the context of coding theory or to classic books about algebraic geometry such as [19] or [6].

1.1 Places and Valuation Rings

Definition 1.1.1. Let K be an arbitrary field. An *algebraic function field* F over K is an extension F/K with the following properties: There is an element $x \in F$ which is trancendental over K and the extension $F/K(x)$ is finite (hence algebraic).

By $\widetilde{K}$ we denote those elements of F which are algebraic over K. Since sums, products and quotients of algebraic elements are algebraic as well, $\widetilde{K}$ is a subfield of F. We call $\widetilde{K}$ the *field of constants* of F.

Lemma 1.1.2. *Let F/K be an algebraic function field. Then $z \in F$ is transcendental over K if and only if $[F : K(z)] < \infty$.*

Proof. For the whole proof fix an element $x \in F$ which is transcendental over K and satisfies $[F : K(x)] < \infty$. If z is algebraic over K then $[K(z) : K]$ is finite. Since

$$[F : K(z)] \cdot [K(z) : K] = [F : K] \geq [K(x) : K] = \infty$$

we see that $[F : K(z)] = \infty$.

Let z be transcendental over K. Since $[F : K(x)] < \infty$ the extension $F/K(x)$ is algebraic. Hence there is a polynomial $f(x, \zeta) \in K(x)[\zeta]$ such that $f(x, z) = 0$. Wlog we may assume that the coefficients are elements of $K[x]$. We can interpret f as a polynomial of the form $f(\xi, z)$ with coefficents in $K(z)$ in the independent variable ξ. x is a root of this polynomial and so $[K(x, z) : K(z)] < \infty$. Therefore

$$[F : K(z)] = [F : K(x, z)] \cdot [K(x, z) : K(z)] \leq [F : K(x)] \cdot [K(x, z) : K(z)]$$

and since both factors of the right hand side are finite we conclude $[F : K(z)] < \infty$.

□

Remark. The lemma above shows that the element x in the definition of an algebraic function field does not play a special role among the elements of F which are trancendetal over K.

The easiest example of a function field that one can think of is $K(x)/K$ where K is an arbitrary field and $K(x)$ denotes the field of rational functions in some indeterminate x. As a motivation for our next definition we will consider an irreducible polynomial $f(x)$ with coefficients in K and the set

$$\mathcal{O}_f := \left\{ \frac{g(x)}{h(x)} \,\middle|\, g(x), h(x) \in K[x], f(x) \nmid h(x) \right\}.$$

If $f(x)$ divides a product it has to divide one of its factors, so $\mathcal{O}_f$ is closed under addition and multiplication. Therefore it is a subring of $K(x)$ which obviously contains K. For any element $z \in K(x)$, $\mathcal{O}_f$ contains z itself or z^{-1}. The following definition generalises this notion:

Definition 1.1.3. Let F/K be a function field. A *valuation ring* of F/K is a subring $\mathcal{O} \subsetneq F$ which has K as a subset and for any $z \in F^\times$ contains z or its inverse. We denote the units of $\mathcal{O}$ by $\mathcal{O}^\times$ and the non-units by $\mathcal{P}$. We call $\mathcal{P}$ a *place* of F/K.

The following lemma summarises some basic properties of valuation rings.

Lemma 1.1.4. *A valuation ring $\mathcal{O}$ of a function field F/K has the following properties:*

1.) $\mathcal{P}$ is the unique maximal ideal of $\mathcal{O}$.

2.) *Take some arbitrary $z \in F^\times$. Then z is an element of $\mathcal{O}$ if and only if $z^{-1} \notin \mathcal{P}$.*

3.) *If some $z \in F$ satisfies an equation of the form $z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0 = 0$ where $a_0, \ldots, a_{n-1} \in \mathcal{O}$ then $z \in \mathcal{O}$.*[1]

4.) $\widetilde{K} \subseteq \mathcal{O}$.

5.) $\widetilde{K} \cap \mathcal{P} = \{0\}$.

Proof.

1.) It is sufficient to show that $\mathcal{P}$ is an ideal. Since a proper ideal of $\mathcal{O}$ must not contain units, any such ideal is a subset of $\mathcal{P}$. For arbitrary $u \in \mathcal{O}$, $z \in \mathcal{P}$ the product uz cannot be invertible in $\mathcal{O}$ since otherwise $u(uz)^{-1} = z^{-1} \in \mathcal{O}$. If $y, z \in \mathcal{P}$ and one of them is zero then clearly $y - z \in \mathcal{P}$. If both are non-zero then y/z or z/y is in $\mathcal{O}$. In the first case we have $z - y = z(1 - y/z) \in \mathcal{P}$, the other case follows similarly.

2.) Assume $z \in \mathcal{O}$ but $z^{-1} \in \mathcal{P}$. Then z is the inverse of z^{-1} in $\mathcal{O}$. So $z^{-1} \in \mathcal{O}^\times = \mathcal{O} \setminus \mathcal{P}$ which is a contradiction. Conversely, assume $z^{-1} \notin \mathcal{P}$ but $z \notin \mathcal{O}$. By the definition of a valuation ring $z^{-1} \in \mathcal{O}$. So z^{-1} is not invertible in $\mathcal{O}$, i.e. $z^{-1} \in \mathcal{P}$, contradicting the assumption.

3.) Let us assume that $z \notin \mathcal{O}$. The definition of a valuation ring then states that $z^{-1} \in \mathcal{O}$. Using the assumption gives

$$0 = z^{-(n-1)}(z^n + \sum_{i=0}^{n-1} a_i z^i) = z + \sum_{k=0}^{n-1} a_{n-1-k}(z^{-1})^k.$$

Thus $z \in \mathcal{O}$ which is a contradiction.

4.) An arbitrary $z \in \widetilde{K}$ fulfils an equation of the form $p(z) = 0$ were p is a polynomial with coefficients in $K \subseteq \mathcal{O}$. By *3.)* this means $z \in \mathcal{O}$.

5.) This follows from the last point. All non-zero elements of $\widetilde{K}$ lie in $\mathcal{O}$ and thus are units of this ring.

□

[1] Satisfying this condition, $\mathcal{O}$ is said to be *integrally closed* .

Remark. Point *2.)* of the previous lemma shows that a valuation ring $\mathcal{O}$ may be reconstructed from its place $\mathcal{P}$. In particular $\mathcal{O} = \{z \in F^\times : z^{-1} \notin \mathcal{P}\} \cup \{0\}$. Hence there is a one-to-one correspondence between the places and the valuation rings of F. We will make use of this fact frequently.

Example 1.1.5. *Let us return to our previous example, the field $K(x)$. We wish to find the place $\mathcal{P}_f$ associated with $\mathcal{O}_f$. Consider a non-zero element $g(x)/h(x)$ of $\mathcal{O}_f$, i.e. $g(x) \neq 0$ and $f(x)$ does not divide $h(x)$. This is invertible if and only if $h(x)/g(x) \in \mathcal{O}_f$, that is, if and only if $f(x)$ is not a divisor of $g(x)$. Therefore $\mathcal{P}_f$ can be described by means of*

$$\mathcal{P}_f = \left\{ \frac{g(x)}{h(x)} \,\middle|\, g(x), h(x) \in K[x], f(x) | g(x), f(x) \nmid h(x) \right\}.$$

It is easy to verify that

$$\mathcal{O}_\infty := \left\{ \frac{g(x)}{h(x)} \,\middle|\, g(x), h(x) \in K[x], \deg g(x) \leq \deg h(x) \right\}$$

is another valuation ring of $K(x)$. We use the convention $\deg(0) := -\infty$ such that $0 \in \mathcal{O}_\infty$. The corresponding place $\mathcal{P}_\infty$ consists of those rational functions $g(x)/h(x)$ with $\deg g(x) < \deg h(x)$. $\mathcal{P}_\infty$ may be interpreted in the following way: If $g(x) = g_m x^m + \ldots + g_1 x + g_0$, $h(x) = h_n x^n + \ldots + h_1 x + h_0$, $m \leq n$ then

$$\frac{g(x)}{h(x)} = \frac{g_m x^m + g_{m-1} x^{m-1} + \ldots + g_1 x + g_0}{h_n x^n + h_{n-1} x^{n-1} + \ldots + h_1 x + h_0} = \frac{(1/x)^{n-m}(g_0 (1/x)^m + g_1 (1/x)^{m-1} + \ldots + g_{m-1}(1/x) + g_m)}{h_0 (1/x)^n + h_1 (1/x)^{n-1} + \ldots + h_{n-1}(1/x) + h_n} = \frac{(1/x)^{n-m} \tilde{g}(1/x)}{\tilde{h}(1/x)}$$

where $\tilde{g}(x), \tilde{h}(x)$ are polynomials, $\tilde{h}(0) = h_n \neq 0$. Conversely, if we start with $\tilde{g}(x), \tilde{h}(x)$, $\tilde{h}(0) \neq 0$ then a similar calculation transforms $\tilde{g}(1/x)/\tilde{h}(1/x)$ into a fraction $g(x)/h(x)$, $g(x), h(x)$ polynomials, $\deg g \leq \deg h$. This shows that the automorphism of $K(x)$ that fixes K and takes x to $1/x$ maps $\mathcal{O}_\infty$ to $\mathcal{O}_x$. Thus $\mathcal{O}_\infty$ is not essentially different from the other places. We may think of $\mathcal{O}_\infty$ as the set of all rational functions "without a pole" at ∞.

Indeed, the aforementioned $\mathcal{O}_f$ together with $\mathcal{O}_\infty$ are all places of $K(x)$:

Proposition 1.1.6. *Let $\mathcal{O}$ be a valuation ring of $K(x)$. Then $\mathcal{O} = \mathcal{O}_f$ for some irreducible $f(x) \in K[x]$ or $\mathcal{O} = \mathcal{O}_\infty$.*

Proof. Let us first assume that $x \in \mathcal{O}$ such that $K[x] \subseteq \mathcal{O}$ holds. Since $\mathcal{P}$ is a prime ideal in $\mathcal{O}$, $\mathcal{P} \cap K[x]$ is a prime ideal in $K[x]$. If $\mathcal{P} \cap K[x]$ is the zero ideal, then every non-zero element of $K[x]$ is invertible in $\mathcal{O}$. It follows that $\mathcal{O} = K(x)$ which contradicts the definition of a valuation ring. So $\mathcal{P} \cap K[x]$ is generated by an irreducible $f(x) \in K[x]$. Take an element $u = g/h \in \mathcal{O}_f$ where g and h are polynomials in x. Then we may assume that f does not divide h and thus $h \in \mathcal{O} \setminus \mathcal{P} = \mathcal{O}^\times$. This yields $h^{-1} \in \mathcal{O}$ and thus $u = h^{-1}g \in \mathcal{O}$, so we see $\mathcal{O}_f \subseteq \mathcal{O}$. Now assume that there is a $u = g/h \in \mathcal{O} \setminus \mathcal{O}_f$ with polynomials g and h that are relatively prime. Then $f|h$, $f \nmid g$ so $1/g \in \mathcal{O}_f \subseteq \mathcal{O}$. Therefore $1/h = u/g \in \mathcal{O}$ which implies that $h \notin \mathcal{P}$. This is clearly contradicting $f|h$, so $\mathcal{O} = \mathcal{O}_f$.

Let us turn to the case where $x \notin \mathcal{O}$. We conclude that $1/x \in \mathcal{P}$ and therefore $K[1/x] \subseteq \mathcal{O}$. Similar to the first case one may derive the existence of an irreducible polynomial $\tilde{f} \in K[1/x]$ such that $\mathcal{P} \cap K[1/x]$ consists of all multiples of $\tilde{f}$ and $\mathcal{O} = \mathcal{O}_{\tilde{f}}$. But this time $1/x \in \mathcal{P}$ so $\tilde{f}(1/x)$ divides $1/x$. Therefore we can choose $\tilde{f}(1/x) = 1/x$ so $\mathcal{O} = \mathcal{O}_\infty$. □

1.2 Existence of Places

We will now show that any algebraic function field F admits infinitely many places. If $F = K(x)$ then this can be easily seen: Two essentially different[2] irreducible polynomials $f, g \in K[x]$ define two different places $\mathcal{P}_f$ and $\mathcal{P}_g$. This holds since $f \in \mathcal{P}_f$ and $f \notin \mathcal{P}_g$. Furthermore, there are infinitely many essentially different irreducible polynomials in $K[x]$. For an infinite field K one can consider $x - a$, $a \in K$. For a finite field it is well known that for any positive integer n there is an irreducible polynomial of degree n.

The following theorem will help us to prove this result for arbitrary function fields.

Theorem 1.2.1. *Let F/K be an algebraic function field. Take a subring R with the property $K \subseteq R \subseteq F$ and a proper ideal $I \neq \{0\}$ of R. Then there is a valuation ring $\mathcal{O}$ with associated place $\mathcal{P}$ such that $I \subseteq \mathcal{P}$ and $R \subseteq \mathcal{O}$.*

Proof. We consider the family

$$\mathcal{F} := \{S \mid S \text{ is a subring of } F, R \subseteq S, IS \neq S\}$$

where we denote by IS the ideal in S generated by I, i.e. all elements of the form $a_1 s_1 + \ldots + a_k s_k$ with $a_i \in I, s_i \in S$. We want to use Zorn's Lemma

[2]We call two polynomials essentially different if one is not a constant multiple of the other polynomial.

to show that there is a maximal element in $\mathcal{F}$, where we assume the usual set theoretic order. Since $R \in \mathcal{F}$ this set is not empty. Let $\mathcal{K} \subseteq \mathcal{F}$ be a linear ordered set. Define $T := \bigcup \mathcal{K}$. Then T is a ring containing R. We want to verify that IT is properly contained in T. Assume that $IT = T$. Then there are elements $a_1, \ldots, a_k \in I$, $t_1, \ldots, t_k \in T$ with the property $1 = a_1t_1 + \ldots + a_kt_k$. But then there is a ring S_0 in $\mathcal{K}$ which contains all t_i and therefore $1 \in IS_0$. This yields $IS_0 = S_0$ which contradicts the choice of $\mathcal{K}$. Hence $\mathcal{K}$ has an upper bound in $\mathcal{F}$ and due to Zorn's Lemma there is a maximal element $\mathcal{O}$ in $\mathcal{F}$.

Next we want to show that $\mathcal{O}$ is a valuation ring of F/K. We immediately see that $K \subseteq R \subseteq \mathcal{O}$. A consequence of $I\mathcal{O} \neq \mathcal{O}$ is that $\mathcal{O}$ is properly contained in F. To complete the proof assume that there is a $z \in F$ with $z, z^{-1} \notin \mathcal{O}$. Then $\mathcal{O} \subsetneq \mathcal{O}[z]$ and therefore $(I\mathcal{O})[z] = I(\mathcal{O}[z]) = \mathcal{O}[z]$ and, analogously, $(I\mathcal{O})[z^{-1}] = I(\mathcal{O}[z^{-1}]) = \mathcal{O}[z^{-1}]$. Hence we find $a_0, \ldots, a_k, b_0, \ldots, b_\ell \in I\mathcal{O}$ such that

$$\begin{aligned} 1 &= a_0 + a_1z + \ldots + a_kz^k \\ 1 &= b_0 + b_1z^{-1} + \ldots + b_\ell z^{-\ell} \end{aligned}$$

with $a_k, b_\ell \neq 0$. Observe that $k, \ell \geq 1$ since $1 \notin I\mathcal{O}$. We may assume that k and ℓ are chosen minimally and that $k \geq \ell$. If we multiply the first equation with $(1 - b_0)$ and the second one with a_kz^k we get

$$\begin{aligned} 1 - b_0 &= (1 - b_0)a_0 + (1 - b_0)a_1z + \ldots + (1 - b_0)a_kz^k \\ 0 &= a_k(b_0 - 1)z^k + a_kb_1z^{k-1} + \ldots + a_kb_\ell z^{k-\ell}. \end{aligned}$$

Adding the two equations yields an equation of the form $c_{k-1}z^{k-1} + \ldots + c_1z + c_0 = 1$ with $c_i \in I\mathcal{O}$. Obviously not all c_i can be zero, so let $j \leq k-1$ be maximal with $c_j \neq 0$. $1 \notin I\mathcal{O}$ and therefore $j \geq 1$. This equation contradicts the choice of k. So z or z^{-1} has to be an element of $\mathcal{O}$ which concludes the proof. □

Corollary 1.2.2. *There are infinitely many places of an algebraic function field F/K.*

Proof. Let $x \in F$ be an element that is transcendental over K. We take an arbitrary irreducible polynomial $f(x) \in K[x]$ and use the previous theorem with $I = f(x)K[x]$, $R = K[x]$. This shows the existence of a place $\mathcal{P}$ containing $f(x)$. Two essentially distinct irreducible polynomials $f(x)$ and $g(x)$ cannot be elements of the same place. This is due to the fact that for

such polynomials we find $u(x), v(x) \in K[x]$ with $u(x)f(x) + v(x)g(x) = 1$ and so 1 would be an element of that place. Since there are infinitely many essentially distinct polynomials, there are infinitely many places. □

1.3 Zeros, Poles and Valuations

Given a function field F/K we already saw in Lemma 1.1.4 that a place $\mathcal{P}$ is a maximal ideal of its valuation ring $\mathcal{O}$. Thus $\mathcal{O}/\mathcal{P}$ is a field. Let us consider the map $z \mapsto z + \mathcal{P}$ which maps the elements of $\mathcal{O}$ to their residue class. We call it the *residue class map* . Since Lemma 1.1.4 states that $\widetilde{K} \subseteq \mathcal{O}$ and $\widetilde{K} \cap \mathcal{P} = \{0\}$, the mapping is injective on the field of constants. Thus we can consider $\widetilde{K}$ as a subfield of $\mathcal{O}/\mathcal{P}$.

Definition 1.3.1. Let F be a function field, $\mathcal{P}$ one of its places and $\mathcal{O}$ the corresponding valuation ring. $\mathcal{O}/\mathcal{P}$ is the *residue class field* of $\mathcal{P}$. The *degree* of $\mathcal{P}$ is the dimension

$$\deg(\mathcal{P}) := [\mathcal{O}/\mathcal{P} : K].$$

The degree is always finite. This will easily follow from the next lemma if we choose $R = \mathcal{O}$ and $I = \mathcal{P}$.

Lemma 1.3.2. *Let F/K be an algebraic function field, R a subring with $K \subseteq R \subseteq F$ and $I \subsetneq R$ a proper ideal. Let z be a non-zero element of I. Assume that $t_0, \ldots, t_k \in R$ fulfill $t_0 = z$, $t_i/t_{i+1} \in I$ for $0 \leq i \leq k-1$, $t_k = 1$. Take $u_1, \ldots, u_n \in R$ such that their residue classes modulo I are linearly independent over K. Then the $k \cdot n$ elements $t_i u_j$, $1 \leq i \leq k$, $1 \leq j \leq n$ are linearly independent over $K(z)$.*

Proof. Assume that the $t_i u_j$ are not linearly independent. I.e. there is a relation of the form

$$\sum_{i=1}^{k} \sum_{j=1}^{n} q_{ij}(z) t_i u_j = 0$$

with $q_{ij}(z) \in K(z)$. We may assume that the $q_{ij}(z)$ are polynomials in z and that not all of them are divisible by z. This can be achieved by multiplying with the least common multiple of the denominators and by cancelling through a power of z if necessary. Let $k' \leq k$ be the largest integer such that $q_{k'j}(0) \neq 0$ for some j but $q_{ij}(0) = 0$ for all $i > k'$ and all $j \leq n$. Then we can rewrite the equation as

$$\sum_{i=1}^{k'} \sum_{j=1}^{n} q_{ij}(z) t_i u_j = zw$$

where w is some element of R. Subtracting the first $k'-1$ summands of the outer sum and dividing by $t_{k'}$ gives

$$\sum_{j=1}^{n} q_{k'j}(z) u_j = \frac{z}{t_{k'}} w - \sum_{i=1}^{k'-1} \sum_{j=1}^{n} q_{ij}(z) \frac{t_i}{t_{k'}} u_j.$$

For $i < k'$ the quotients of the form $t_i/t_{k'} = (t_i/t_{i+1}) \cdot \ldots \cdot (t_{k'-1}/t_{k'})$ are elements of $I^{k'-i}$ and hence of I since this is an ideal. This holds in particular for $z/t_{k'} = t_0/t_{k'}$. Therefore the right hand side is congruent zero modulo I. z is an element of I by assumption so $q_{k'j}(z) \equiv q_{k'j}(0)$ modulo I. This yields

$$\sum_{j=1}^{n} q_{k'j}(0) u_j \equiv 0 \mod I$$

where not all scalars are zero, thus contradicting our assumption. □

Using the same notation as in the previous lemma we obtain

Corollary 1.3.3. *The degree of a place $\mathcal{P}$ is finite. The degree $[\widetilde{K} : K]$ is finite. In particular*

$$[\widetilde{K} : K] \leq [\mathcal{O}/\mathcal{P} : K] \leq [F : K(z)]$$

for an arbitrary non-zero element $z \in \mathcal{P}$.

Proof. The right inequality follows by setting $R = \mathcal{O}$, $I = \mathcal{P}$, $k = 1$, $t_0 = z$, $t_1 = 1$ and taking $u_1, \ldots, u_n$ to be linearly independent in $\mathcal{O}/\mathcal{P}$ over K. The right hand side is finite by Lemma 1.1.2 and the fact that a non-zero element of $\mathcal{P}$ is transcendental. □

To study the residue class map in the case $F = K(x)$ take a place $\mathcal{P}_f$ consisting of all elements g/h with g divisible and h not divisible by some irreducible polynomial f. In this case $K[x] \subseteq \mathcal{O}_f$ and two elements of $K[x]$ are identified if their difference is divisible by f. Thus the image of $K[x]$ under the residue class map can be considered as $K[x]/f$ which is a field. Since $\mathcal{O}_f$ consists of certain quotients of elements of $K[x]$ this is already the image of the whole valuation ring $\mathcal{O}_f$. Thus $\mathcal{O}_f/\mathcal{P}_f$ can be considered as an algebraic extension of degree $\deg(f)$ of K. More precisely, $\mathcal{O}_f/\mathcal{P}_f$ can be obtained by adjoining an element ξ to K that satisfies $f(\xi) = 0$. To

understand $\mathcal{O}_\infty/\mathcal{P}_\infty$ we can use Example 1.1.5. We saw that there is an isomorphism of $K(x)$, fixing K and mapping $\mathcal{O}_\infty$ to $\mathcal{O}_x$ and $\mathcal{P}_\infty$ to $\mathcal{P}_x$. Thus $\mathcal{O}_\infty/\mathcal{P}_\infty \cong \mathcal{O}_x/\mathcal{P}_x \cong K$.

In the case where $f(x) = x - a$ it is convenient to write $\mathcal{P}_a := \mathcal{P}_{x-a}$ and $\mathcal{O}_a := \mathcal{O}_{x-a}$, respectively. We can interpret the residue class map as follows: For some $u = g/h$, $h(a) \neq 0$

$$u(x) - u(a) = \frac{g(x)h(a) - h(x)g(a)}{h(a)h(x)}$$

holds. Since $x-a$ divides the numerator of the right side we conclude $u(x) + \mathcal{P}_a = u(a) + \mathcal{P}_a$. Keeping our interpretation $\widetilde{K} \subseteq \mathcal{O}_a/\mathcal{P}_a$ in mind, $u + \mathcal{P}_a$ may be interpreted as the value of u at a. If u is a quotient as above but $h(a) = 0$, $g(a) \neq 0$, u does not lie in $\mathcal{O}_a$. In fact $x-a$ divides h and therefore a may be seen as pole of h. The following definition generalises this notion to arbitrary function fields and places:

Definition 1.3.4. Let F/K be a function field and $\mathcal{P}$ a place of F. Denote by $\mathcal{O}$ its valuation ring. For $u \in \mathcal{O}$ we write $u(\mathcal{P})$ for the residue class of u modulo $\mathcal{P}$ and call this the *value of u taken by $\mathcal{P}$* . If $u(\mathcal{P}) = 0$, i.e. $u \in \mathcal{P}$, then $\mathcal{P}$ is called a zero of u. If $u \notin \mathcal{O}$ the place $\mathcal{P}$ is said to be a *pole* of u.

Remark. $\mathcal{P}$ is a pole of u if and only if $\mathcal{P}$ is a zero of u^{-1}. This is just a reformulation of the fact that $u^{-1} \in \mathcal{P}$ if and only if $u \notin \mathcal{O}$.

Proposition 1.3.5. *Let F/K be an algebraic function field, $z \in F$ an element which is transcendental over K. Then z has at least one zero and one pole.*

Proof. $zK[z]$ is a proper ideal of $K[z]$ since z is transcendental over K. Therefore Theorem 1.2.1 applies to $K[z]$ and $zK[z]$. Thus there is a place $\mathcal{P}$ of F with $z \in \mathcal{P}$. Hence $\mathcal{P}$ is a zero of z. Similarly we find a zero $\mathcal{Q}$ of z^{-1}. So $\mathcal{Q}$ is a pole of z. □

For $F = K(x)$ each place $\mathcal{P}$ is a principal ideal, i.e. there is a generating element $t \in \mathcal{O}$ such that $\mathcal{P} = t\mathcal{O}$. In fact, if $\mathcal{P} = \mathcal{P}_f$ ($f \in K[x]$ irreducible) one can choose $t = f$. If $\mathcal{O} = \mathcal{O}_\infty$ a possible choice is $t = 1/x$. In the case $\mathcal{O} = \mathcal{O}_f$ suppose that there is an element $u = g/h$ which belongs to $f^n\mathcal{O}$ for all $n \geq 0$. Then $u = f^n g_n/h_n$ with g_n and h_n relatively prime and their quotient lying in $\mathcal{O}$. So $gh_n = hf^n g_n$ and since f does not divide h_n, f^n must divide g. So $g = 0$ and therefore $u = 0$. The same holds in the case $\mathcal{O} = \mathcal{O}_\infty$. We thus found an element $t \in \mathcal{O}$ with the properties

1.) $\mathcal{P} = t\mathcal{O}$

2.) $\bigcap_{n=0}^{\infty} t^n\mathcal{O} = \{0\}$.

From now on F/K may be an arbitrary function field and $\mathcal{P}$ one of its places. We assume that there is an element $t \in \mathcal{O}$ with the properties above. Indeed this is always the case as will be shown later. For any $u \in F$ there is some integer n with $u \in t^n\mathcal{O}$: If $u \in \mathcal{O}$ one can choose $n = 0$. If $u \notin \mathcal{O}$ then $u^{-1} \in \mathcal{O}$. Hence there is an integer m such that $u^{-1} \in t^m\mathcal{O}$, $u^{-1} \notin t^{m+1}\mathcal{O}$. Therefore $t^{-m}u^{-1} \in \mathcal{O}$ and $t^{-m}u^{-1} \notin t\mathcal{O} = \mathcal{P}$. So this element is invertible in $\mathcal{O}$ and thus $u = t^{-m}(t^{-m}u^{-1})^{-1} \in t^{-m}\mathcal{O}$. We conclude that for any non-zero element u of F there is a largest integer n such that $u \in t^n\mathcal{O}$. If $\tilde{t}$ is another element with the above two properties then $\tilde{t} \in \mathcal{P} = t\mathcal{O}$. So $\tilde{t}/t \in \mathcal{O}$ and by symmetry $t/\tilde{t} \in \mathcal{O}$. These quotients (and therefore all its powers) are invertible in $\mathcal{O}$. Consequently $t^m\mathcal{O} = \tilde{t}^m(t/\tilde{t})^m\mathcal{O} = \tilde{t}^m\mathcal{O}$. So the definition of n does not depend on the choice of t but only on $\mathcal{P}$. Thus we will denote the largest integer n with $u \in t^n\mathcal{O}$ by $v_{\mathcal{P}}(u) := n$.

We now consider the rational function field $\mathbb{C}(x)/\mathbb{C}$. For $u \in \mathbb{C}(x)$ there is the following interpretation of $v_a(u) := v_{\mathcal{P}_a}(u)$, $a \in \mathbb{C}$. If $u(a) = 0$ then $v_a(u)$ is the multiplicity of a as a zero of u. If a is a pole then $-v_a(u)$ is the multiplicity of this pole. And $v_a(u) = 0$ if and only if a is neither a pole nor a zero of u.

Proposition 1.3.6. *Let F/K be an algebraic function field and $\mathcal{P}$ one of its places. Then $\mathcal{P}$ is a principal ideal of the corresponding valuation ring $\mathcal{O}$. In particular there exists an element $t \in \mathcal{P}$ with $\mathcal{P} = t\mathcal{O}$ and $\bigcap_{n=0}^{\infty} t^n\mathcal{O} = \{0\}$.*

Proof. Fix an arbitrary non-zero element $z_0 \in \mathcal{P}$. We use Lemma 1.3.2 where we set $n = 1$, $u_1 = 1$. If we have $k+1$ elements t_i with the properties $t_0 = z_0$, $t_i/t_{i+1} \in \mathcal{P}$, $t_k = 1$ the lemma states that $k \leq [F : K(z_0)]$. Assume that k is chosen maximally and define $t := t_{k-1}$. We shall see that t is a generator of $\mathcal{P}$.

First assume that there is a $z \in \mathcal{P}$ which is not an element of $t\mathcal{O}$. I.e. $z/t \notin \mathcal{O}$, hence $t/z \in \mathcal{P}$. But then $t_0, t_1, \ldots, t_{k-1} = t, t/z, t_k = 1$ is a sequence with $k + 1$ elements that fulfils the above properties which contradicts the choice of k. This shows the inclusion $\mathcal{P} \subseteq t\mathcal{O}$. Since $t \in \mathcal{P}$ and $\mathcal{P}$ is an ideal we conclude that $\mathcal{P} = t\mathcal{O}$.

Assume $z \in t^m\mathcal{O}$ for a non-zero element $z \in \mathcal{P}$ and some $m \in \mathbb{N}$. Then we may write $z = t^0w_0 = t^1w_1 = \ldots = t^mw_m$ with elements $w_i \in \mathcal{O}$. Since $w_i/w_{i+1} = t \in \mathcal{P}$ and $w_{m-1} = w_mt \in \mathcal{P}$ we may use Lemma 1.3.2 (again with $n = 1$) for the sequence $z = w_0, w_1, \ldots, w_{m-1}, 1$. This shows $m \leq [F : K(z)]$. Thus we see $z \notin \cap_{n=0}^{\infty} t^n\mathcal{O}$. □

The generator t is sometimes called a *prime element* for $\mathcal{P}$. The above proposition shows that for any $u \in F^\times$ the notion of the largest integer $v_\mathcal{P}(u)$ such that $u \in t^{v_\mathcal{P}(u)}\mathcal{O}$ is well-defined in any function field.

Definition 1.3.7. Let F/K be a function field, $\mathcal{O}$ a valuation ring and $\mathcal{P}$ its place. Take a prime element t for $\mathcal{P}$. For $u \in F^\times$ we define

$$v_\mathcal{P}(u) := \max\{m \in \mathbb{Z} \colon u \in t^m\mathcal{O}\}.$$

$v_\mathcal{P}$ is called the *valuation at the place* $\mathcal{P}$. This definition does not depend on the choice of the generating element t but only on $\mathcal{P}$. If $u = 0$ we set $v_\mathcal{P}(u) := \infty$. If $n = v_\mathcal{P}(u) > 0$ we call $\mathcal{P}$ a *zero of order* n of u. If $n = v_\mathcal{P}(u) < 0$ we call $\mathcal{P}$ a *pole of order* $-n$ of u.

The following lemma will summarize some of the properties of $v_\mathcal{P}$. Indeed in the case of the function field $\mathbb{C}(x)/\mathbb{C}$, keeping the interpretation of $v_a(u)$ as the order of the pole or zero a of u in mind, these are well known.

Lemma 1.3.8. *Let $\mathcal{P}$ be a place of a function field F/K and $v_\mathcal{P}$ be defined as above. Take $u, w \in F^\times$, then the following properties hold.*

1.) *Fix a prime element t for $\mathcal{P}$. Then u has a unique representation of the form $u = t^{v_\mathcal{P}(u)}s$ with $s \in \mathcal{O}^\times$.*

2.) *Whenever there is a representation $u = t^n s$ with $s \in \mathcal{O}^\times$ we have $n = v_\mathcal{P}(u)$.*

3.) $v_\mathcal{P}(uw) = v_\mathcal{P}(u) + v_\mathcal{P}(w)$

4.) $v_\mathcal{P}(u + w) \geq \min(v_\mathcal{P}(u), v_\mathcal{P}(v))$

5.) $v_\mathcal{P}(a) = 0$ *for all* $a \in \widetilde{K} \setminus \{0\}$

6.) *If* $v_\mathcal{P}(u) \neq v_\mathcal{P}(w)$ *then* $v_\mathcal{P}(u + w) = \min(v_\mathcal{P}(u), v_\mathcal{P}(w))$.

Proof.

1.) Set $n := v_\mathcal{P}(u)$. By definition there is a representation of the form $u = t^n z$ where $z \in \mathcal{O}$. But z cannot be an element of $\mathcal{P} = t\mathcal{O}$ since otherwise $z = tz'$ for some $z' \in \mathcal{O}$ and thus $u \in t^{n+1}\mathcal{O}$. Clearly, z is unique.

2.) By assumption $u \in t^n\mathcal{O}$. Suppose $u = t^n s \in t^m\mathcal{O}$ for some $m > n$. Then $s \in t^{m-n}\mathcal{O} \subseteq t\mathcal{O} = \mathcal{P}$ so s is not invertible in $\mathcal{O}$ which is a contradiction. Hence $n = v_\mathcal{P}(u)$.

3.) Set $m := v_{\mathcal{P}}(u)$, $n := v_{\mathcal{P}}(w)$. Then there are $s_1, s_2 \in \mathcal{O}^\times$ such that $u = t^m s_1$, $w = t^n s_2$. Therefore $uw = t^{m+n} s_1 s_2$. Since $s_1 s_2 \in \mathcal{O}^\times$ the second point yields $v_{\mathcal{P}}(uw) = m + n$.

4.) Set m, n, s_1, s_2 as before. Wlog suppose $m \leq n$. Then $u + w = t^m(s_1 + t^{n-m} s_2) \in t^m \mathcal{O}$ and consequently $v_{\mathcal{P}}(u + w) \geq m = \min(m, n)$.

5.) Since $\widetilde{K} \subseteq \mathcal{O}$ we have $a \in \mathcal{O}$. But a is invertible in $\mathcal{O}$, so $a \notin \mathcal{P} = t\mathcal{O}$. Hence $v_{\mathcal{P}}(a) = 0$.

6.) Wlog we may assume $v_{\mathcal{P}}(u) < v_{\mathcal{P}}(w)$. Suppose the claim is not true, i.e. $v_{\mathcal{P}}(u + w) > v_{\mathcal{P}}(u)$. Note that $v_{\mathcal{P}}(w) = v_{\mathcal{P}}(-w)$ by *3.)* and *5.)*. Together with *4.)* this leads to

$$v_{\mathcal{P}}(u) = v_{\mathcal{P}}((u + w) - w) \geq \min(v_{\mathcal{P}}(u + w), v_{\mathcal{P}}(w)) > v_{\mathcal{P}}(u)$$

which clearly is a contradiction.

□

Statement *6.)* is sometimes called the *strict triangle inequality* .

Remark. The function $v_{\mathcal{P}}$ determines $\mathcal{O}$ uniquely. It is easily seen from the definition of $v_{\mathcal{P}}$ that

$$\begin{aligned} \mathcal{O} &= \{z \in F \colon v_{\mathcal{P}}(z) \geq 0\} \\ \mathcal{P} &= \{z \in F \colon v_{\mathcal{P}}(z) > 0\} \\ \mathcal{O}^\times &= \{z \in F \colon v_{\mathcal{P}}(z) = 0\}\,. \end{aligned}$$

The next lemma will turn out to be helpful. It shows that if a valuation ring contains another they have to be equal.

Lemma 1.3.9. *A valuation ring $\mathcal{O}$ of a function field F/K is a maximal subring of F.*

Proof. Take an element $z \in F \setminus \mathcal{O}$. We have to show that $F = \mathcal{O}[z]$. If we write $\mathcal{P}$ for the place of $\mathcal{O}$ then $v_{\mathcal{P}}(z) < 0$. For an arbitrary $y \in F$

$$v_{\mathcal{P}}(yz^{-k}) = v_{\mathcal{P}}(y) - k v_{\mathcal{P}}(z) \geq 0$$

if we choose k large enough. Therefore $u := yz^{-k} \in \mathcal{O}$ and so $y = uz^k \in \mathcal{O}[z]$ which concludes the proof. □

1.4 Independence of Valuations

In this section we will develop a fundamental theorem about the possible behaviour of an element u of a function field. To get an idea of what it is about let us consider the rational function field $\mathbb{C}(x)/\mathbb{C}$. Fix an element $a \in \mathbb{C}$ and two elements $u, w \in \mathbb{C}(x)$. Then the Laurent series expansion of their difference at a is of the form

$$u(x) - w(x) = \sum_{k=r}^{\infty} (u_k - w_k)(x-a)^k$$

where $u_k, w_k \in \mathbb{C}$ and r is the least integer such that $u_k \neq 0$ or $w_k \neq 0$. From this we see that $u_r = w_r, u_{r-1} = w_{r-1}, \ldots, u_{m-1} = w_{m-1}, u_m \neq w_m$ if and only if $(x-a)^m$ divides $u(x) - w(x)$, but $(x-a)^{m+1}$ does not, which is equivalent to $v_a(u-w) = m$.

Consider now the following problem: Given distinct complex numbers a_i, rational functions $w_i \in \mathbb{C}(x)$ and integers m_i for $1 \leq i \leq n$. Is there a function $u \in \mathbb{C}(x)$ with the property that its Laurent series expansion coincides with that of w_i at a_i up to the index m_i for all i? I.e. is there some $u \in \mathbb{C}(x)$ that fulfils the n conditions

$$v_a(u - w_i) = m_i$$

simultaneously? The main result of this section states that this is indeed possible. It is formulated in the much wider sense of an arbitrary function field. It is called "independence of valuations" since it states that the behaviour of a function at a given finite set of places does not imply anything about the behaviour at another place. In the literature it is also refered to as "weak approximation theorem".

Theorem 1.4.1 (Independence of Valuations)**.** *Let F/K be a function field and $n > 0$ an integer. For $1 \leq i \leq n$ fix arbitrary elements $w_i \in F$, distinct places $\mathcal{P}_i$ and integers m_i. We abbreviate $v_{\mathcal{P}_i}$ as v_i. Then there is an element $u \in F$ with the property*

$$v_i(u - w_i) = m_i$$

for all $i \leq n$.

Proof. The proof is rather technical and therefore divided into four steps:

1.) There exists some $y \in F$ such that $v_1(y) > 0$, $v_i(y) < 0$ for $i = 2, \ldots, n$.

2.) There is some $w \in F$ with the properties $v_1(w-1) > m_1$ and $v_i(w) > m_i$ for $i = 2, \ldots, n$.

3.) Given $y_1, \ldots, y_n \in F$ then there is a $z \in F$ such that $v_i(z - y_i) > m_i$ for all $i \leq n$.

4.) Final proof.

Proof of 1.) Denote by $\mathcal{O}_i$ the valuation ring of $\mathcal{P}_i$. We proof this step by induction on n. For $n = 2$ there are elements $y_1 \in \mathcal{O}_1 \setminus \mathcal{O}_2$ and $y_2 \in \mathcal{O}_2 \setminus \mathcal{O}_1$ by Lemma 1.3.9. So $v_1(y_1) \geq 0, v_1(y_2) < 0, v_2(y_2) \geq 0, v_2(y_1) < 0$. Therefore $y := y_1/y_2$ has the desired property. For $n > 2$ we start with the induction hypothesis $v_1(w) > 0, v_2(w) < 0, \ldots, v_{n-1}(w) < 0$ for some $w \in F$. Choose $z \in F$ such that $v_1(z) > 0, v_n(z) < 0$ and an integer $r \geq 1$ such that $rv_i(w) \neq v_i(z)$ for all $i \leq n-1$. If we set $y := z + w^r$ then of course $v_1(y) > 0$ and for $2 \leq i \leq n$

$$v_i(y) = v_i(z + w^r) = \min(v_i(z), rv_i(w)) < 0$$

by the strict triangle inequality stated in Lemma 1.3.8 and the choice of w and z.

Proof of 2.) Choose y with the properties stated in *1.)* and set $w := (1 + y^s)^{-1}$ for some $s \in \mathbb{N}$. Then

$$\begin{aligned} v_1(w-1) = v_1(-y^s(1+y^s)^{-1}) = sv_1(y) - v_1(1+y^s) = \\ sv_1(y) - \min(\underbrace{v_1(1)}_{=0}, \underbrace{sv_1(y)}_{>0}) = sv_1(y) \\ v_i(w) = -v_i(1+y^s) = -\min(\underbrace{v_i(1)}_{=0}, \underbrace{sv_i(y)}_{<0}) = -sv_i(y) \end{aligned}$$

for $2 \leq i \leq n$. If we choose s sufficiently large, w fulfils the required properties.

Proof of 3.) Take $s \in \mathbb{Z}$ with $v_i(y_j) \geq s$ for all $i, j \leq n$. Using step *2.)* n times we find $\hat{w}_1, \ldots, \hat{w}_n$ such that

$$\begin{aligned} v_i(\hat{w}_i - 1) &> m_i - s \\ v_i(\hat{w}_j) &> m_i - s \quad \text{for all } j \neq i. \end{aligned}$$

For arbitrary $i, j \leq n$, $j \neq i$ this choice leads to

$$v_i(\hat{w}_j y_j) = v_i(\hat{w}_j) + v_i(y_j) > (m_i - s) + s = m_i.$$

An analogous calculation shows $v_i((\hat{w}_i - 1)y_i) > m_i$. Define $z := \sum_{j=1}^{n} \hat{w}_j y_j$, then

$$v_i(z - y_i) = v_i(\sum_{j=1}^{n} \hat{w}_j y_j - y_i) \geq \min(\hat{w}_1 y_1, \ldots, (\hat{w}_i - 1)y_i, \ldots, \hat{w}_n y_n) > m_i.$$

Proof of 4.) To finish the proof choose $z \in F$ with $v_i(z - w_i) > m_i$ as in the previous step. We also find $z_i \in F$ such that $v_i(z_i) = m_i$ (simply set $z_i := t_i^{m_i}$ for a generating element t_i of $\mathcal{P}_i$). Using step *3.)* a second time gives $z' \in F$ such that $v_i(z' - z_i) > m_i$. Now we obtain

$$v_i(z') = \min(v_i((z' - z_i), v_i(z_i)) = m_i.$$

By setting $u := z + z'$ we see that

$$v_i(u - w_i) = v_i((z - w_i) + z') = \min(v_i(z - w_i), v_i(z')) = m_i.$$

Thus we found an element $u \in F$ with the desired features. □

1.5 Divisors

Theorem 1.5.1. *Let $\mathcal{P}_1, \ldots, \mathcal{P}_r$ be zeros of some $u \in F^\times$, F/K being a function field. Then*

$$\sum_{i=1}^{r} v_{\mathcal{P}_i}(u) \deg(\mathcal{P}_i) \leq [F : K(u)].$$

Thus u can only have finitely many poles and zeros.

Proof. In order to prove this set $v_i := v_{\mathcal{P}_i}$, $e_i := v_i(u)$ and denote by $\mathcal{O}_i$ the valuation ring of $\mathcal{P}_i$ for $1 \leq i \leq r$. Choose elements of F in the following way:

- For $1 \leq i \leq r$ choose t_i such that $v_i(t_i) = 1$ and $v_k(t_i) = 0$ for $k \neq i$. This is possible due to the Theorem of Independence of Valuations.
- For $1 \leq i \leq r$ we choose $u_{i,1}, \ldots, u_{i,d_i}$ such that their residue classes modulo $\mathcal{P}_i$ form a basis of $\mathcal{O}_i/\mathcal{P}_i$ as a K-vector space (i.e. $d_i = \deg \mathcal{P}_i$).
- For $1 \leq i \leq r$, $1 \leq j \leq d_i$ choose elements $z_{i,j} \in F$ such that $v_i(u_{i,j} - z_{i,j}) > 0$ and $v_k(z_{i,j}) \geq e_k$ for $k \neq i$. Note that $z_{i,j} \equiv u_{i,j}$ modulo $\mathcal{P}_i$.

We claim that the elements $t_i^\ell z_{i,j}$, $1 \le i \le r$, $1 \le j \le d_i$, $0 \le \ell \le e_i - 1$ are linearly independent over $K(u)$. This will proof our claim since there are $\sum_{i=1}^r e_i d_i = \sum_{i=1}^r v_i(u) \deg \mathcal{P}_i$ of these elements.

Assume that there exist $q_{i,j,\ell}(u) \in K(u)$ such that

$$\sum_{i=1}^{r} \sum_{j=1}^{d_i} \sum_{\ell=0}^{e_i-1} q_{i,j,\ell}(u) t_i^\ell z_{i,j} = 0.$$

Wlog we may assume that $q_{i,j,\ell}(u) \in K[u]$ and not all of these polynomials are divisible by u. Choose k, m such that $1 \le k \le r$, $0 \le m \le e_k - 1$ and

$$\begin{aligned} u | q_{k,j,\ell}(u) \text{ for all } j \le d_k, \ell < m \\ u \nmid q_{k,j,m}(u) \text{ for some } j \le d_k. \end{aligned}$$

Since $u \in \mathcal{O}_k$ we have $K[u] \subseteq \mathcal{O}_k$ and thus $v_k(q_{i,j,\ell}(u)) \ge 0$. Multiplying the above equation with t_k^{-m} and evaluating v_k at the summands shows the following: If $i \ne k$ we have

$$v_k(q_{i,j,\ell}(u) t_i^\ell t_k^{-m} z_{i,j}) = \underbrace{v_k(q_{i,j,\ell}(u))}_{\ge 0} + \underbrace{v_k(t_i^\ell)}_{=0} + \underbrace{v_k(t_k^{-m})}_{=-m} + \underbrace{v_k(z_{i,j})}_{\ge e_k} \ge e_k - m > 0.$$

Now consider the case $i = k$, $\ell \ne m$. If $\ell < m$ then $u | q_{k,j,\ell}(u)$ and thus $v_k(q_{k,j,\ell}(u)) = v_k(u \tilde{q}_{k,j,\ell}(u)) = v_k(u) + v_k(\tilde{q}_{k,j,\ell}(u)) \ge v_k(u)$, which gives

$$\begin{aligned} v_k(q_{k,j,\ell}(u) t_k^{\ell-m} z_{k,j}) = v_k(q_{k,j,\ell}(u)) + v_k(t_k^{\ell-m}) + v_k(z_{k,j}) \ge \\ v_k(q_{k,j,\ell}(u)) + v_k(t_k^{\ell-m}) \ge \begin{cases} v_k(u) + \ell - m \ge e_k - m > 0, & \ell < m \\ 0 + \ell - m > 0, & \ell > m \end{cases} \end{aligned}$$

Consequently for all $(i, \ell) \ne (k, m)$ we have $q_{i,j,\ell}(u) t_i^\ell t_k^{-m} z_{i,j} \in \mathcal{P}_k$. Therefore

$$\sum_{j=1}^{d_k} q_{k,j,m}(u) z_{k,j} \in \mathcal{P}_k.$$

Since $u \in \mathcal{P}_k$ we have $q_{k,j,m}(u) \equiv q_{k,j,m}(0)$ modulo $\mathcal{P}_k$ for $1 \le j \le d_k$. From $z_{k,j} \equiv u_{k,j}$ modulo $\mathcal{P}_k$ we see

$$\sum_{j=1}^{d_k} q_{k,j,m}(0) u_{k,j} \in \mathcal{P}_k.$$

So $q_{k,j,m}(0) = 0$ and thus $u | q_{k,j,m}(u)$ for all $j \le d_k$, contradicting our choice of k and m. □

Definition 1.5.2.

- A *divisor* of a given function field F/K is a formal product of the form

$$\mathcal{D} = \prod_{\mathcal{P}\in\mathfrak{P}} \mathcal{P}^{d_\mathcal{P}}$$

where $\mathfrak{P}$ denotes the set of all places of F, $d_\mathcal{P} \in \mathbb{Z}$ and $d_\mathcal{P} \neq 0$ for only finitely many $\mathcal{P} \in \mathfrak{P}$. Divisors are multiplied by the rule

$$\prod_{\mathcal{P}\in\mathfrak{P}} \mathcal{P}^{d_\mathcal{P}} \cdot \prod_{\mathcal{P}\in\mathfrak{P}} \mathcal{P}^{e_\mathcal{P}} := \prod_{\mathcal{P}\in\mathfrak{P}} \mathcal{P}^{d_\mathcal{P}+e_\mathcal{P}}.$$

This makes the set of all divisors an abelian group. It is called the *divisor group* of F. The neutral element is the product where all exponents are zero and is referred to as the *unit divisor* . It is denoted by $\mathfrak{o}$. We interpret $\mathcal{P}_0 \in \mathfrak{P}$ as a divisor by setting $d_{\mathcal{P}_0} = 1$ and $d_\mathcal{P} = 0$ for $\mathcal{P} \neq \mathcal{P}_0$. For a divisor $\mathcal{D}$ we denote by $\mathcal{D}^{-1}$ the inverse element. Exponentiation of the form $\mathcal{D}^n$, $n \in \mathbb{Z}$, is defined in the obvious way.

- For a given $x \in F^\times$ we define the *zero divisor* and the *pole divisor* by

$$(x)_0 := \prod_{\mathcal{P}\in Z} \mathcal{P}^{v_\mathcal{P}(x)}$$
$$(x)_\infty := \prod_{\mathcal{P}\in N} \mathcal{P}^{-v_\mathcal{P}(x)}$$

where Z denotes the set of zeros of x and N the set of poles. We use the convention that places not occurring in the product have exponents equal to zero. The *principal divisor* of x is defined by $(x) := (x)_0 \cdot (x)_\infty^{-1}$. *A principal divisor* is a divisor of the form $\mathcal{D} = (z)$ for some $z \in F^\times$. By Lemma 1.3.8, $(xy) = (x) \cdot (y)$, so $x \mapsto (x)$ is a homomorphism from $(F^\times, \cdot)$ to the divisor group. So the set of principal divisors is a subgroup of the divisor group.

- For a divisor $\mathcal{D}$ with exponents $d_\mathcal{P}$ we will also write $v_\mathcal{P}(\mathcal{D}) := d_\mathcal{P}$ in analogy to the notation for the order function at $\mathcal{P}$. Thus we may write

$$\mathcal{D} = \prod_{\mathcal{P}\in\mathfrak{P}} \mathcal{P}^{v_\mathcal{P}(\mathcal{D})} \quad \text{as well as}$$
$$(x) = \prod_{\mathcal{P}\in\mathfrak{P}} \mathcal{P}^{v_\mathcal{P}(x)}.$$

We shall refer to $\mathcal{P}$ as a *zero of* $\mathcal{D}$ if $v_{\mathcal{P}}(\mathcal{D}) > 0$ and call $\mathcal{P}$ a *pole of* $\mathcal{D}$ if $v_{\mathcal{P}}(\mathcal{D}) < 0$.

- Let $\mathcal{D}_1, \mathcal{D}_2$ be divisors with associated exponents $v_{\mathcal{P}}(\mathcal{D}_1)$ and $v_{\mathcal{P}}(\mathcal{D}_2)$. We say that $\mathcal{D}_1$ devides $\mathcal{D}_2$ and write $\mathcal{D}_1 \leq \mathcal{D}_2$ if $v_{\mathcal{P}}(\mathcal{D}_1) \leq v_{\mathcal{P}}(\mathcal{D}_2)$ for all $\mathcal{P} \in \mathfrak{P}$. A *positive divisor* $\mathcal{D}$ is a divisor with the property $\mathcal{D} \geq \mathfrak{o}$, i.e. a divisor without poles.

- The *support* of a divisor $\mathcal{D}$ is the set of places $\mathcal{P}$ where $v_{\mathcal{P}}(\mathcal{D})$ is non-zero, i.e.
$$\operatorname{supp} \mathcal{D} := \{\mathcal{P} \in \mathfrak{P} \colon v_{\mathcal{P}}(\mathcal{D}) \neq 0\}.$$

Remark. The divisor group can be interpreted as the free abelian group with generating set $\mathfrak{P}$.

Remark. If $\mathcal{P}$ is a place of degree one and $\mathcal{O}$ is the corresponding valuation ring then $\widetilde{K} = \mathcal{O}/\mathcal{P}$. So for $z \in \mathcal{O}$ the residue class $z(\mathcal{P}) := z + \mathcal{P}$ is an element of $\widetilde{K}$. If $z \notin \mathcal{O}$ we set $z(\mathcal{P}) := \infty$. If K is an algebraically closed field then $\widetilde{K} = K$ and there is the following interpretation for the elements of F: Since $\mathcal{O}/\mathcal{P}$ is an algebraic extension of K, it must be of dimension one, i.e. all places are of degree one. So identifying z with the map
$$\begin{cases} \mathfrak{P} \to K \cup \{\infty\} \\ \mathcal{P} \mapsto z(\mathcal{P}) \end{cases}$$
all elements of the function field are seen to be functions from $\mathfrak{P}$ (the set of places) to K. Therefore, elements of an arbitrary function field F/K are often refered to as *functions* .

Every divisor $\mathcal{D}$ of a function field F gives rise to a certain subset of F. This set may be interpreted as the set of all functions with prescribed zeros and allowed poles of a certain order described by the divisor. This set is called the *Riemann-Roch space*. It is one of the fundamental definitions of this chapter and will be object of further investigation.

Definition 1.5.3. Let F/K be a function field and $\mathcal{D}$ one of its divisors. The *Riemann-Roch space* is defined by
$$\begin{aligned} \mathfrak{L}(\mathcal{D}) :&= \{z \in F \,|\, v_{\mathcal{P}}(z) \geq -v_{\mathcal{P}}(\mathcal{D}) \quad \text{for all} \quad \mathcal{P} \in \mathfrak{P}\} \\ &= \left\{z \in F^{\times} \middle| (z) \geq \mathcal{D}^{-1}\right\} \cup \{0\} \\ &= \left\{z \in F^{\times} \middle| \mathcal{D} \cdot (z) \text{ is positive}\right\} \cup \{0\}. \end{aligned}$$

$\mathfrak{L}(\mathcal{D})$ is the set of all elements $z \in F$ such that $\mathcal{D} \cdot (z)$ has no pole. In other words: If

$$\mathcal{D} = \mathcal{P}_1^{a_1} \dots \mathcal{P}_m^{a_m} \mathcal{Q}_1^{-b_1} \dots \mathcal{Q}_n^{-b_n}$$

with $a_i, b_j > 0$ and places $\mathcal{P}_i, \mathcal{Q}_j$ of F then $\mathfrak{L}(\mathcal{D})$ consists of those elements that have zeros of order at least b_j at $\mathcal{Q}_j$ and poles only in $\mathcal{P} = \mathcal{P}_i$ with maximal order a_i. Since multiplication with non-zero elements of $\widetilde{K}$ does not change anything about poles and zeros of some $z \in F$ the Riemann-Roch space $\mathfrak{L}(\mathcal{D})$ is closed under multiplication by elements of $\widetilde{K}$. *4.)* of Lemma 1.3.8 shows that it is also closed under addition. So $\mathfrak{L}(\mathcal{D})$ is a subspace of F as a vector space over the base field K.

Definition 1.5.4. Let F/K be a function field and $\mathcal{D}$ a divisor. We define the *degree* of $\mathcal{D}$ by

$$\deg(\mathcal{D}) := \sum_{\mathcal{P} \in \mathfrak{P}} v_{\mathcal{P}}(\mathcal{D}) \deg(\mathcal{P}).$$

This sum is well defined since there are only finitely many summands not equal to zero. The *dimension* of $\mathcal{D}$ is the dimension of the associated Riemann Roch space

$$\ell(\mathcal{D}) := \dim_K(\mathfrak{L}(\mathcal{D})).$$

As a consequence of the following lemma we shall see that the dimension of a divisor is always finite.

Lemma 1.5.5. *Let F/K be a function field, $\mathcal{D}_1, \mathcal{D}_2$ divisors such that $\mathcal{D}_1 \leq \mathcal{D}_2$. Then $\mathfrak{L}(\mathcal{D}_1)$ is a subspace of $\mathfrak{L}(\mathcal{D}_2)$ and*

$$\dim_K(\mathfrak{L}(\mathcal{D}_2)/\mathfrak{L}(\mathcal{D}_1)) \leq \deg(\mathcal{D}_2) - \deg(\mathcal{D}_1).$$

Proof. For any $z \in \mathfrak{L}(\mathcal{D}_1)$ we have $v_{\mathcal{P}}(z) \geq -v_{\mathcal{P}}(\mathcal{D}_1) \geq -v_{\mathcal{P}}(\mathcal{D}_2)$, hence $z \in \mathfrak{L}(\mathcal{D}_2)$. To prove the second statement it is convenient to consider the special case $\mathcal{D}_2 = \mathcal{D}_1 \cdot \mathcal{P}$ for a place $\mathcal{P}$ of F (with corresponding valuation ring $\mathcal{O}$). Let $u \in F$ be an element with $v_{\mathcal{P}}(u) = v_{\mathcal{P}}(\mathcal{D}_2) = v_{\mathcal{P}}(\mathcal{D}_1) + 1$. Such a choice is possible by Theorem 1.4.1. Consider the K-linear map

$$f\colon \begin{cases} \mathfrak{L}(\mathcal{D}_2) \to \mathcal{O}/\mathcal{P} \\ z \mapsto (uz)(\mathcal{P}) \end{cases}.$$

This is well defined since $v_{\mathcal{P}}(uz) = v_{\mathcal{P}}(\mathcal{D}_2) + v_{\mathcal{P}}(z) \geq 0$, so $uz \in \mathcal{O}$. $z \in \ker(f)$ if and only if $uz \in \mathcal{P}$ or equivalently $v_{\mathcal{P}}(uz) \geq 1$. This holds if and only if $v_{\mathcal{P}}(z) \geq 1 - v_{\mathcal{P}}(u) = -v_{\mathcal{P}}(\mathcal{D}_1)$. Hence $\ker(f) = \mathfrak{L}(\mathcal{D}_1)$. Therefore there is

a linear, injective map from $\mathfrak{L}(\mathcal{D}_2)/\mathfrak{L}(\mathcal{D}_1)$ into the residue class field of $\mathcal{O}$. This shows

$$\dim_K(\mathfrak{L}(\mathcal{D}_2)/\mathfrak{L}(\mathcal{D}_1)) \leq \dim_K(\mathcal{O}/\mathcal{P}) = \deg(\mathcal{P}) = \deg(\mathcal{D}_2) - \deg(\mathcal{D}_1).$$

Now the general case follows easily by induction on the sum of exponents of $\mathcal{D}_2 \cdot \mathcal{D}_1^{-1}$: Assume that the inequality is already proven for the case $\mathcal{D}_1 \cdot \mathcal{P} \leq \mathcal{D}_2$. Using the well-known fact $W/V \cong (W/U)/(V/U)$ for arbitrary vector spaces $U \leq V \leq W$ we obtain

$$\begin{aligned}\dim_K(\mathfrak{L}(\mathcal{D}_2)/\mathfrak{L}(\mathcal{D}_1)) = \dim_K(\mathfrak{L}(\mathcal{D}_2)/\mathfrak{L}(\mathcal{D}_1\mathcal{P})) + \dim_K(\mathfrak{L}(\mathcal{D}_1\mathcal{P})/\mathfrak{L}(\mathcal{D}_1)) \leq \\ \deg(\mathcal{D}_2) - \deg(\mathcal{D}_1\mathcal{P}) + \deg(\mathcal{D}_1\mathcal{P}) - \deg(\mathcal{D}_1) = \deg(\mathcal{D}_2) - \deg(\mathcal{D}_1).\end{aligned}$$

□

Corollary 1.5.6. *For a function field F/K and a divisor $\mathcal{D}$ the dimension $\ell(\mathcal{D})$ is always finite. In particular*

$$\ell(\mathcal{D}) \leq \deg(\mathcal{D}_+) + [\widetilde{K} : K]$$

where $\mathcal{D}_+$ is defined by $v_\mathcal{P}(\mathcal{D}_+) = v_\mathcal{P}(\mathcal{D})$ if this integer is positive and $v_\mathcal{P}(\mathcal{D}_+) = 0$ otherwise.

Proof. The definition shows $\mathcal{D} \leq \mathcal{D}_+$ and the latter is a positive divisor. By Proposition 1.3.5 every element of F that is transcendental over K has a pole, so $\mathfrak{L}(\mathfrak{o}) = \widetilde{K}$. Thus the previous lemma yields

$$\ell(\mathcal{D}_+) = \dim_K(\mathfrak{L}(\mathcal{D}_+)/\mathfrak{L}(\mathfrak{o})) + \dim_K(\mathfrak{L}(\mathfrak{o})) \leq \deg(\mathcal{D}_+) + [\widetilde{K} : K] < \infty$$

and the inequality follows from $\mathfrak{L}(\mathcal{D}) \subseteq \mathfrak{L}(\mathcal{D}_+)$. □

We already saw that in the case $F = K(x)$ the degrees of the places are of the form

$$\begin{aligned}\deg(\mathcal{P}_f) &= \deg(f), \quad \text{for } f \in K[x] \text{ irreducible} \\ \deg(\mathcal{P}_\infty) &= 1.\end{aligned}$$

Any non-zero element $u \in K(x)$ may be written in the form

$$u = f_1^{a_1} \cdot \ldots \cdot f_m^{a_m} g_1^{-b_1} \cdot \ldots \cdot g_n^{-b_n}$$

with distinct irreducible polynomials $f_i, g_j \in K[x]$ and positive integers a_i, b_j. Let us denote the numerator by u_1 and the denominator by u_2. Wlog assume

that $a_1 + \ldots + a_m \geq b_1 + \ldots + b_n$. For the zero divisor of u this implies

$$\deg((u)_0) = \sum_{i=1}^{m} \deg(\mathcal{P}_{f_i}) v_{f_i}(u) = \sum_{i=1}^{m} \deg(f_i) a_i = \deg(u_1).$$

Using $v_\infty(f/g) = \deg(g) - \deg(f)$ for polynomials f, g we see that

$$\deg((u)_\infty) = \sum_{j=1}^{n} (-\deg(\mathcal{P}_{g_j})) v_{g_j}(u) - \deg(\mathcal{P}_\infty) v_\infty(u) = \sum_{j=1}^{n} \deg(g_j) b_j - (\deg(u_2) - \deg(u_1)) = \deg(u_1)$$

where $\deg(u_i)$ is the degree of the polynomial u_i. Thus the degrees of $(u)_0$ and $(u)_\infty$ coincide and $\deg((u)) = \deg((u)_0) - \deg((u)_\infty) = 0$. This means that for elements of $K(x)$ there are always as much poles as zeros if we count them weighted by the degrees of poles and zeros. Indeed, this is also the case for arbitrary function fields.

Theorem 1.5.7. *Let F/K be a function field. For $z \in F$, z transcendental over K, the following formula holds:*

$$\deg((z)_0) = \deg((z)_\infty) = [F : K(z)]$$

Proof. Using Theorem 1.5.1 for z^{-1} yields $\deg((z)_\infty) = \deg((z^{-1})_0) \leq [F : K(z^{-1})] = [F : K(z)] =: n$. Therefore it remains to show that $n \leq \deg((z)_\infty)$. We use the abbreviation

$$\mathcal{B} := (z)_\infty = \prod_{i=1}^{m} \mathcal{P}_i^{-v_{\mathcal{P}_i}(z)}$$

where $\mathcal{P}_i$, $1 \leq i \leq m$, denote the poles of z. Then $\mathcal{B}$ is a positive divisor. Let $u_1, \ldots, u_n$ be a basis of $F/K(z)$ and fix a positive divisor $\mathcal{C}$ with the property $(u_j) \geq -\mathcal{C}$ for all $j \leq n$. Take an arbitrary integer $r \geq 0$. Then the elements $z^i u_j$, $0 \leq i \leq r, 1 \leq j \leq n$ are linearly independent over K since the z^i are linearly independent in $K(z)$ (as a K-vector space) and the u_j are linearly independent in F (as a $K(z)$-vector space). The $z^i u_j$ are elements of $\mathfrak{L}(\mathcal{B}^r \mathcal{C})$ since

$$v_\mathcal{P}(z^i u_j) = i v_\mathcal{P}(z) + v_\mathcal{P}(u_j) \geq -i v_\mathcal{P}(\mathcal{B}) - v_\mathcal{P}(\mathcal{C}) \geq -v_\mathcal{P}(\mathcal{B}^r \mathcal{C}).$$

So there are $(r+1)n$ linearly independent elements in $\mathfrak{L}(\mathcal{B}^r\mathcal{C})$. Since $\mathcal{B}^r\mathcal{C}$ is a positive divisor the last corollary gives $(r+1)n \leq \ell(\mathcal{B}^r\mathcal{C}) \leq r\deg(\mathcal{B}) + \deg(\mathcal{C}) + [\widetilde{K} : K]$. This is equivalent to

$$n \leq \deg(\mathcal{B}) - \frac{n - \deg(\mathcal{C}) - [\widetilde{K} : K]}{r}.$$

Since r may be chosen arbitrarily large we obtain $n \leq \deg(\mathcal{B})$ as desired.

The statement about $(z)_0$ easily follows from $\deg((z)_0) = \deg((z^{-1})_\infty) = [F : K(z^{-1})] = [F : K(z)]$. □

Corollary 1.5.8. *Let F/K be a function field and $z \in F^\times$. Then* $\deg((z)) = 0$.

We call two divisors $\mathcal{D}_1$, $\mathcal{D}_2$ *equivalent* if their quotient $\mathcal{D}_1\mathcal{D}_2^{-1}$ is a principal divisor. I.e. if there is a $z \in F^\times$ such that $\mathcal{D}_1 = (z) \cdot \mathcal{D}_2$.

Lemma 1.5.9. *If $\mathcal{D}_1$, $\mathcal{D}_2$ are equivalent then $\mathfrak{L}(\mathcal{D}_1)$ is isomorphic to $\mathfrak{L}(\mathcal{D}_2)$ (as a K-vector space) and* $\deg(\mathcal{D}_1) = \deg(\mathcal{D}_2)$.

Proof. By assumption $\mathcal{D}_1 = (z) \cdot \mathcal{D}_2$. Therefore we can consider the K-linear map $u \mapsto uz$ from $\mathfrak{L}(\mathcal{D}_2)$ to $\mathfrak{L}(\mathcal{D}_1)$. Similarly, $u \mapsto uz^{-1}$ sends elements from $\mathfrak{L}(\mathcal{D}_1)$ to $\mathfrak{L}(\mathcal{D}_2)$. Since the two mappings are inverse to each other the Riemann-Roch spaces are isomorphic.

The second claim follows from Corollary 1.5.8 since $\deg(\mathcal{D}_1) = \deg((z)) + \deg(\mathcal{D}_2) = \deg(\mathcal{D}_2)$. □

The following lemma will provide an upper bound for $\deg(\mathcal{D}) - \ell(\mathcal{D})$ where $\mathcal{D}$ is an arbitrary divisor of F. The important thing is that this bound is independent of the divisor $\mathcal{D}$.

Lemma 1.5.10. *Let F/K be a function field. Then there is an integer γ such that*

$$\deg(\mathcal{D}) - \ell(\mathcal{D}) \leq \gamma$$

for all divisors $\mathcal{D}$ of F/K.

Proof. Given divisors $\mathcal{D}_1 \leq \mathcal{D}_2$ recall that

$$\ell(\mathcal{D}_2) - \ell(\mathcal{D}_1) = \dim_K(\mathfrak{L}(\mathcal{D}_2)/\mathfrak{L}(\mathcal{D}_1)) \leq \deg(\mathcal{D}_2) - \deg(\mathcal{D}_1)$$

by Lemma 1.5.5, so $\deg(\mathcal{D}_1) - \ell(\mathcal{D}_1) \leq \deg(\mathcal{D}_2) - \ell(\mathcal{D}_2)$. Fix a transcendental element $z \in F$ and consider the divisor $\mathcal{B} := (z)_\infty$. In the proof of Theorem 1.5.7 we showed the existence of a positive divisor $\mathcal{C}$, depending on z such that $\ell(\mathcal{B}^r\mathcal{C}) \geq (r+1)\deg(\mathcal{B})$ for all positive integers r. Lemma 1.5.5 gives

$$\ell(\mathcal{B}^r\mathcal{C}) - \ell(\mathcal{B}^r) = \dim_K(\mathfrak{L}(\mathcal{B}^r\mathcal{C})/\mathfrak{L}(\mathcal{B}^r)) \leq \deg(\mathcal{C})$$

and thus

$$\deg(\mathcal{B}^r) - \overbrace{(\deg(\mathcal{C}) - \deg(\mathcal{B}))}^{\gamma:=} = (r+1)\deg(\mathcal{B}) - \deg(\mathcal{C}) \leq \ell(\mathcal{B}^r\mathcal{C}) - \deg(\mathcal{C}) \leq \ell(\mathcal{B}^r)$$

follows. Now we want to extend the inequality $\deg(\mathcal{B}^r) - \ell(\mathcal{B}^r) \leq \gamma$ for $\ell \geq 0$ to arbitrary divisors $\mathcal{D}$. For a given $\mathcal{D}$ we will show the existence of divisors $\widehat{\mathcal{D}}$, $\mathcal{D}'$ and an integer r such that $\mathcal{D} \leq \widehat{\mathcal{D}}$, $\mathcal{D}' \leq \mathcal{B}^r$ and $\widehat{\mathcal{D}}, \mathcal{D}'$ being equivalent. From that we obtain

$$\deg(\mathcal{D}) - \ell(\mathcal{D}) \leq \deg(\widehat{\mathcal{D}}) - \ell(\widehat{\mathcal{D}}) \stackrel{*}{=} \deg(\mathcal{D}') - \ell(\mathcal{D}') \leq \deg(\mathcal{B}^r) - \ell(\mathcal{B}^r) \leq \gamma$$

where * follows from Lemma 1.5.9. For a fixed $\mathcal{D}$ choose $\widehat{\mathcal{D}} \geq \mathcal{D}$ such that $\widehat{\mathcal{D}}$ is positive. Then $\mathcal{B}^r\widehat{\mathcal{D}}^{-1} \leq \mathcal{B}^r$ and thus $\ell(\mathcal{B}^r) - \ell(\mathcal{B}^r\widehat{\mathcal{D}}^{-1}) \leq \deg\widehat{\mathcal{D}}$ by Lemma 1.5.5. Therefore

$$\ell(\mathcal{B}^r\widehat{\mathcal{D}}^{-1}) \geq \ell(\mathcal{B}^r) - \deg(\widehat{\mathcal{D}}) \geq \deg(\mathcal{B}^r) - \gamma - \deg(\widehat{\mathcal{D}}).$$

The second inequality holds because of our choice of γ. If we choose r sufficiently large then the right hand side is positive and hence we may select a non-zero element $z \in \mathfrak{L}(\mathcal{B}^r\widehat{\mathcal{D}}^{-1})$. Setting $\mathcal{D}' := (z)^{-1}\widehat{\mathcal{D}}$ shows that $\mathcal{D}'$ and $\widehat{\mathcal{D}}$ are equivalent and that $\mathcal{D}' = (z)^{-1}\widehat{\mathcal{D}} \leq \mathcal{B}^r\widehat{\mathcal{D}}^{-1}\widehat{\mathcal{D}} = \mathcal{B}^r$ which concludes the proof. □

The previous lemma shows that the following definition makes sense.

Definition 1.5.11. Set $\kappa := [\widetilde{K} : K]$. The genus g of an algebraic function field F/K is the integer defined by

$$g := \max\{\deg(\mathcal{D}) - \ell(\mathcal{D}) + \kappa \,|\, \mathcal{D} \text{ is a divisor of } F\}.$$

The genus is a non-negative integer since $\deg(\mathfrak{o}) - \dim(\mathfrak{o}) + \kappa = 0 - \kappa + \kappa = 0$. The definition of the genus shows

Corollary 1.5.12 (Riemann's Theorem)**.** *Let F/K be an algebraic function field of genus g and $\mathcal{D}$ be a divisor. Then the inequality*

$$\deg(\mathcal{D}) + \kappa - g \leq \ell(\mathcal{D})$$

holds.

If $\mathcal{D}$ is a positive divisor this can be combined with Corollary 1.5.6 and thus

$$\deg(\mathcal{D}) + \kappa - g \leq \ell(\mathcal{D}) \leq \deg(\mathcal{D}) + \kappa.$$

The genus is an important invariant in a function field. The inequality in 1.5.12 can be used to show that there exist functions with certain prescribed zeros and poles only at allowed places: If one chooses the divisor $\mathcal{D}$ such that the left hand side is positive, this assures that there is a non-zero element in the associated Riemann-Roch space, i.e. there exists a non-trivial example fulfilling these properties. Note that this result is essentially different from Theorem 1.4.1 since in the latter prescribed zeros or poles at some places could lead to poles at other places.

Corollary 1.5.13. *For a function field F/K there is an integer c such that*

$$\ell(\mathcal{D}) = \deg(\mathcal{D}) + \kappa - g$$

for every divisor $\mathcal{D}$ with $\deg(\mathcal{D}) \geq c$.

Proof. We choose a divisor $\mathcal{D}_0$ such that $\ell(\mathcal{D}_0) = \deg(\mathcal{D}_0) - g + \kappa$ and set $c := \deg(\mathcal{D}_0) + g$. Then

$$\ell(\mathcal{D}\mathcal{D}_0^{-1}) \geq \deg(\mathcal{D}\mathcal{D}_0^{-1}) - g + \kappa \geq c - \deg(\mathcal{D}_0) - g + \kappa = \kappa.$$

So there is some non-zero element $z \in \mathfrak{L}(\mathcal{D}\mathcal{D}_0^{-1})$. Then $(z) \geq \mathcal{D}^{-1}\mathcal{D}_0$ and so $\mathcal{D}' := (z)\mathcal{D} \geq \mathcal{D}_0$. Using Lemma 1.5.9 we see

$$\deg(\mathcal{D}) - \ell(\mathcal{D}) = \deg(\mathcal{D}') - \ell(\mathcal{D}') \geq \deg(\mathcal{D}_0) - \ell(\mathcal{D}_0) = g - \kappa.$$

Since $\deg(\mathcal{D}) - \ell(\mathcal{D}) \leq \kappa - g$ always holds this shows the claim. □

Chapter 2

The Riemann-Roch Theorem

So far we have developed lower and upper bounds for $\ell(\mathcal{D})$. In the case where $\mathcal{D}$ is a positive divisor the gap between these bounds is equal to the genus g. In the general case where $\mathcal{D}$ is not assumed to be positive this gap could grow arbitrarily large. The next step is to develop an exact formula for $\ell(\mathcal{D})$. This is the Riemann-Roch Theorem. It is crucial in order to derive properties of Goppa codes.

The original Riemann-Roch Theorem was not formulated in the setting of algebraic function fields. It was a result in the context of Riemann surfaces. It can be shown that the field of meromorphic functions on a compact Riemann surface is an algebraic function field over $\mathbb{C}$ in the sense of our definition. In the 1920s the Riemann-Roch theorem was generalized by André Weil, replacing the field of meromorphic functions of a compact Riemann surface with a general function field (stemming from an arbitrary field). This approach needs to translate the analytic machinery of the original theorem in purely algebraic terms. It leads to rather technical definitions and proofs which seem to appear from nowhere if they are not related to their original counterparts. Therefore Section 2.1 tries to motivate some of the concepts from their origin, i.e. the theory of compact Riemann surfaces, without diving too deep into this subject. The only parts of the section required for the rest of the chapter are Definitions 2.1.1 and 2.1.2. Therefore the reader may as well omit the other parts.

2.1 Repartitions and Differentials

For this section a prior knowledge in complex analysis is assumed. However, the reader does not have to be familiar with the basic theory of Riemann surfaces. This section is based to a great extent on Chapter 12 of [11] which

tries to show the conceptual abstraction undertaken by Weil. Another attempt which assumes some previous knowledge about Riemann surfaces can be found at the beginning of Chapter 6 of [12]. A good and compact introduction to the theory of Riemann surfaces is [5]. To dive into the concepts required for the proof of the Riemann-Roch Theorem in its original form it is sufficient to read §1, §6, §9 and §16.

A Riemann surface is a connected topological Haussdorff space which is locally homeomorphic to $\mathbb{C}$. That is, there is a family of so called "charts", (U_i, φ_i) such that $\varphi_i(U_i) \subseteq \mathbb{C}$ and φ_i is a homeomorphism onto $\varphi_i(U_i)$. It carries a bit of extra structure to be able to define holomorphic and meromorphic functions. In particular, the compositions $\varphi_j \circ \varphi_i^{-1}|_{\varphi_i(U_i \cap U_j)}$ are assumed to be holomorphic whenever $U_i \cap U_j$ is not empty. In this section we will assume the Riemann surface to be compact. Examples of compact Riemann surfaces include the Riemann sphere $\mathbb{C} \cup \{\infty\}$ which is homeomorphic to the unit ball $\mathbb{S}^2$ and the complex torus $\mathbb{T} \times \mathbb{T}$.[1]

Let X be a compact Riemann surface. One can define holomorphic and meromorphic functions $X \to \mathbb{C}$ ($X \to \mathbb{C} \cup \{\infty\}$ respectively). There are many analogies to holomporphic and meromorphic functions on a subset of $\mathbb{C}$. For example two holomorphic functions are equal if they coincide on a set which has a limit point. It is also possible to define the order of a pole of a meromorphic function as well as the residue at a point. A meromorphic function has only finitely many poles. The set of all meromorphic functions on X, denoted by $M(X)$, is a field.

An advanced topic is the concept of a differential ω (also called meromorphic differential form of degree one, meromorphic 1-form or simply differential form). The definition of differentials is rather technical and not very illuminating for our purposes so we will just state some of their properties. The set of differentials is a one dimensional vector space over the field of meromorphic functions $M(X)$. It is possible to define zeros and poles of a differential. There is also the notion of a holomorphic differential which can be thought of a differential without poles. Further, one can consider the residue $\mathrm{Res}_a(\omega) \in \mathbb{C}$ at any point $a \in X$. A result about compact Riemann surfaces states that a differential has only finitely many poles on X and hence only finitely many points with non-zero residue. Differentials can be integrated along a path[2] γ on the Riemann surface. This produces a complex number denoted by

$$\int_\gamma \omega.$$

[1] Here $\mathbb{T} = \{z \in \mathbb{C} \colon |z| = 1\}$.

[2] Here *path* refers to a piece-wise continuously differentiable curve.

If $f \in M(X)$ then the product $f\omega$ is again a differential form. Let us consider a simply connected, open subset $U \subseteq X$ and assume that the boundary ∂U can be parameterised by a path. Hence the differential ω gives rise to a function that maps each pair of such a subset and a meromorphic function to a complex number[3]

$$r_\omega \colon (U, f) \mapsto \int_{\partial U} f\omega.$$

r_ω is $\mathbb{C}$-linear in its second argument. Furthermore – similar to the well known result from classical complex analysis – the integral has the property that if $f\omega$ is holomorphic on U, then $r_\omega(U, f) = 0$. It is possible to show that analogously to meromorphic functions on $\mathbb{C}$

$$r_\omega(U, f) = \sum_{a \in U} \mathrm{Res}_a(f\omega).$$

holds. The sum always makes sense since as mentioned before only finitely many summands are non-zero. This representation has the advantage that we can extend it to arbitrary subsets $U \subseteq X$. A result about Riemann surfaces states that the sum of all residues of a differential is equal to zero, i.e. $r_\omega(X, f) = 0$ for $f \in M(X)$. To avoid working with pairs (U, f) we define the set of repartitions:

Definition 2.1.1. Let F/K be an algebraic function field. A repartition is a map Γ assigning an element $f \in F$ to each place of F and which has only finitely many distinct values. The set of all repartitions is denoted by R. We write $\Gamma_\mathcal{P}$ for the value of Γ at $\mathcal{P}$ and define $v_\mathcal{P}(\Gamma) := v_\mathcal{P}(\Gamma_\mathcal{P})$. If $\mathfrak{S}$ is a set of places $f/\mathfrak{S}$ denotes the repartition which assigns f to every place in $\mathfrak{S}$ and which is zero elsewhere. If addition of two repartitions and multiplication with an element of F is defined pointwise, R becomes a vectorspace over F. Let $\mathcal{D}$ be a divisor of F. In analogy to the Riemann-Roch space we define $R(\mathcal{D})$ to consist of all repartitions Γ with $v_\mathcal{P}(\Gamma) + v_\mathcal{P}(\mathcal{D}) \geq 0$ for all places $\mathcal{P}$.

Remark. In the literature repartitions are also called *adèles* . They are usually defined in a slightly different way: Most authors consider all maps $\Gamma \colon \mathfrak{P} \to F$ with $\Gamma(\mathcal{P}) \in \mathcal{O}_\mathcal{P}$ for almost all $\mathcal{P} \in \mathfrak{P}$ as repartitions. In contrast, our space is strictly included in this space.

Remark. Every repartition can be written as $f_1/\mathfrak{S}_1 + \ldots + f_n/\mathfrak{S}_n$ with $f_i \in F$ and the $\mathfrak{S}_i$ forming a partition of the set of all places. We interpret each $f \in F$ as the constant repartition assigning f to each place of F.

[3]For this function to be well defined this mapping has to be independent of the choice of the parameterisation. We state without a proof that this is always the case.

In the case of the function field of meromorphic functions on a Riemann surface we identify each pair (U, f) with f/U. Using our new notation we summarise the above mentioned properties of r_ω:

- $r_\omega \colon R \to \mathbb{C}$ is linear
- $r_\omega(f/U) = 0$ whenever $f\omega$ has no poles in U
- $r_\omega(f) = r_\omega(f/X) = 0$ for any meromorphic function $f \in M(X)$

The second property simply states that r_ω vanishes on all repartitions in $R(\mathcal{D})$ where $\mathcal{D}$ is chosen appropriately.[4] The last two properties are equivalent to the single property $r_\omega(\Gamma + f) = 0$ for all $\Gamma \in R(\mathcal{D}), f \in M(X)$. Hence we define differentials of an arbitrary function field in the following way:

Definition 2.1.2. Let F be an algebraic function field over K. For an arbitrary divisor $\mathcal{D}$ define $Y(\mathcal{D}) := R(\mathcal{D}) + F \leq R$. A K-linear map $\omega \colon R \to K$ is called *differential* if there is a divisor $\mathcal{D}$ such that ω vanishes on $Y(\mathcal{D})$. We denote the set of all differentials by Ω and the set of all differentials vanishing on $Y(\mathcal{D})$ by $\Omega(\mathcal{D})$.

Remark. If $\mathcal{D}_1 \leq \mathcal{D}_2$ then $Y(\mathcal{D}_1) \subseteq Y(\mathcal{D}_2)$. Therefore, if ω vanishes on $Y(\mathcal{D}_2)$ it does so on $Y(\mathcal{D}_1)$, i.e. $\Omega(\mathcal{D}_2) \subseteq \Omega(\mathcal{D}_1)$. If we define multiplication $K \times \Omega \to \Omega$ and addition $\Omega \times \Omega \to \Omega$ pointwise, then Ω becomes a K-vector space with $\Omega(\mathcal{D}_1)$ as a subspace. Indeed, if $\mathcal{C}$, $\mathcal{D}$ are divisors, $\omega_1 \in \Omega(\mathcal{C})$, $\omega_2 \in \Omega(\mathcal{D})$, $\alpha \in K$, then $\alpha\omega_1$ vanishes on $Y(\mathcal{C})$ and $\omega_1 + \omega_2$ vanishes on $Y(\mathcal{B})$ if we define $\mathcal{B}$ by $v_\mathcal{P}(\mathcal{B}) := \min(v_\mathcal{P}(\mathcal{C}), v_\mathcal{P}(\mathcal{D}))$.

2.2 The Weak Riemann-Roch Theorem

In this section we will define the index[5] $j(\mathcal{D})$ of a divisor. We will derive a first formula for $\ell(\mathcal{D})$ which depends on $j(\mathcal{D})$, following the approach of [11, chapter 12]. In a sense this only shifts the problem since the index is in general hard to calculate. We shall express the index in a different way in the next section which will lead to the final Riemann-Roch Theorem.

Definition 2.2.1. Let F be an algebraic function field over K and $\mathcal{D}$ one of its divisors. As in the previous secion, R denotes the space of repartitions. The *index* of $\mathcal{D}$ is defined as $j(\mathcal{D}) := \dim_K(R/Y(\mathcal{D}))$.

[4] More precisely: If ω has a pole of order $n > 0$ at a point a and $\mathcal{P}$ is the place corresponding to a then $v_\mathcal{P}(\mathcal{D}) \stackrel{!}{=} -n$.

[5] In the literature the term *index of speciality* is also common.

Remark. Recall our definition $\kappa = [\widetilde{K} : K]$ from Section 1.5. Since both R and $Y(\mathcal{D})$ are vector spaces over $\widetilde{K}$, so is $R/Y(\mathcal{D})$. Hence if $j(\mathcal{D})$ is finite (as we shall see this is always the case) it is a multiple of κ. The index has the following interpretation: Since some differential $\omega\colon R \to K$ that vanishes on $Y(\mathcal{D})$ corresponds to a linear functional $R/Y(\mathcal{D}) \to K$ in a natural way, $\Omega(\mathcal{D})$ can be interpreted as the dual space of $R/Y(\mathcal{D})$. Hence if the dimension $j(\mathcal{D})$ is finite, $\dim_K(\Omega(\mathcal{D})) = \dim_K(R/Y(\mathcal{D})) = j(\mathcal{D})$.

If $\mathcal{C}$, $\mathcal{D}$ are divisors, $\mathcal{C} \leq \mathcal{D}$, then $R(\mathcal{C}) \subseteq R(\mathcal{D})$ and $Y(\mathcal{C}) \subseteq Y(\mathcal{D})$. As we will see, the corresponding factor spaces are always finite-dimensional. To investigate the index of a divisor it is necessary to develop formulas that express these relative dimensions in terms of the degree of the involved divisors. In order to do so we need the following generalisation of the Riemann-Roch space:

Definition 2.2.2. Let F/K be a function field, $\mathcal{D}$ a divisor and $\mathfrak{S} \subseteq \mathfrak{P}$ a set of places. Then $\mathfrak{L}(\mathcal{D}, \mathfrak{S})$ consists of those elements $z \in F$ with $v_{\mathcal{P}}(z) + v_{\mathcal{P}}(\mathcal{D}) \geq 0$ for all $\mathcal{P} \in \mathfrak{S}$.

With this definition $\mathfrak{L}(\mathcal{D}) = \mathfrak{L}(\mathcal{D}, \mathfrak{P})$.

Lemma 2.2.3. *Let F be an algebraic function field over K, $\mathfrak{S}$ be a finite set of places, $\mathcal{C}, \mathcal{D}$ divisors such that $\mathcal{C} \leq \mathcal{D}$. Then $\mathfrak{L}(\mathcal{C}, \mathfrak{S}) \subseteq \mathfrak{L}(\mathcal{D}, \mathfrak{S})$ and $\dim_K(\mathfrak{L}(\mathcal{D}, \mathfrak{S})/\mathfrak{L}(\mathcal{C}, \mathfrak{S})) = \sum_{\mathcal{P} \in \mathfrak{S}} (v_{\mathcal{P}}(\mathcal{D}) - v_{\mathcal{P}}(\mathcal{C})) \deg(\mathcal{P})$.*

Proof. The inclusion holds by definition. We show the inequality in the special case where $\mathcal{D} = \mathcal{C} + \mathcal{P}$ for some place $\mathcal{P} \in \mathfrak{S}$. The general case follows by induction similar to the proof of Lemma 1.5.5. Choose elements $v_1, \ldots, v_d \in \mathcal{O}_{\mathcal{P}}$ such that their residual classes modulo $\mathcal{P}$ form a basis of $\mathcal{O}_{\mathcal{P}}/\mathcal{P}$ (as a K-vector space), i.e. $d = \deg \mathcal{P}$. By Theorem 1.4.1 there is some $u \in F$ with $v_{\mathcal{P}'}(u) = -v_{\mathcal{P}'}(\mathcal{D})$ for all $\mathcal{P}' \in \mathfrak{S}$. For the same reason we find x_i, $i \leq d$, such that

$$\begin{aligned} v_{\mathcal{P}}(v_i - x_i) &\geq 1 \\ v_{\mathcal{P}'}(x_i) \geq 0 \text{ for } \mathcal{P}' &\in \mathfrak{S} \setminus \{\mathcal{P}\}. \end{aligned}$$

By the choice of the x_i, $v_{\mathcal{P}}(x_i) \geq 0$, hence $x_i u \in \mathfrak{L}(\mathcal{D}, \mathfrak{S})$. We will show that the $x_i u$ form a basis of $\mathfrak{L}(\mathcal{D}, \mathfrak{S})/\mathfrak{L}(\mathcal{C}, \mathfrak{S})$.

Take an arbitrary $z \in \mathfrak{L}(\mathcal{D}, \mathfrak{S})$. Then $v_{\mathcal{P}'}(zu^{-1}) \geq 0$ for all $\mathcal{P}' \in \mathfrak{S}$. In particular $zu^{-1} \in \mathcal{O}_{\mathcal{P}}$. Hence there is a representation $zu^{-1} = \sum_{i=1}^{d} a_i v_i + w$ with $a_i \in K, w \in \mathcal{P}$. Since $x_i \equiv v_i$ modulo $\mathcal{P}$ we may also write $zu^{-1} = \sum_{i=1}^{d} a_i x_i + \tilde{w}$, $\tilde{w} \in \mathcal{P}$. Multiplying this with u we get a representation of

z in the desired kind if we can show that $u\tilde{w} \in \mathfrak{L}(\mathcal{C}, \mathfrak{S})$. We already know that $v_{\mathcal{P}}(\tilde{w}) \geq 1$. For a place $\mathcal{P}' \in \mathfrak{S}$ not equal to $\mathcal{P}$, $v_{\mathcal{P}'}(zu^{-1}) \geq 0$ and $\tilde{w} = \sum_{i=1}^{d} a_i x_i - zu^{-1}$ imply $v_{\mathcal{P}'}(\tilde{w}) \geq 0$. Hence $\tilde{w}u \in \mathfrak{L}(\mathcal{C}, \mathfrak{S})$.

To show linear independence of the $x_i u$, suppose there is a linear combination of the form $\sum_{i=1}^{d} a_i x_i u \in \mathfrak{L}(\mathcal{C}, \mathfrak{S})$. Then $v_{\mathcal{P}}(\sum_{i=1}^{d} a_i x_i) + v_{\mathcal{P}}(u) \geq -v_{\mathcal{P}}(\mathcal{C})$. Since $v_{\mathcal{P}}(u) = -v_{\mathcal{P}}(\mathcal{D}) = -v_{\mathcal{P}}(\mathcal{C}) - 1$ this implies $v_{\mathcal{P}}(\sum_{i=1}^{d} a_i x_i) \geq 1$, i.e. $\sum_{i=1}^{d} a_i x_i \in \mathcal{P}$. But the x_i form a basis of $\mathcal{O}_{\mathcal{P}}/\mathcal{P}$, so $a_i = 0$ for all $i \leq d$. □

Corollary 2.2.4. *With the same assumptions as for the previous lemma suppose $\mathfrak{S}$ contains the support of both $\mathcal{C}$ and $\mathcal{D}$. Then*

$$\dim_K(\mathfrak{L}(\mathcal{D}, \mathfrak{S})/\mathfrak{L}(\mathcal{C}, \mathfrak{S})) = \deg(\mathcal{D}) - \deg(\mathcal{C})$$

Lemma 2.2.5. *Let F/K be a function field, $\mathcal{C}$, $\mathcal{D}$ divisors such that $\mathcal{C} \leq \mathcal{D}$.*

1.) $R(\mathcal{C}) \subseteq R(\mathcal{D})$ *and* $\dim_K(R(\mathcal{D})/R(\mathcal{C})) = \deg(\mathcal{D}) - \deg(\mathcal{C})$

2.) $Y(\mathcal{C}) \subseteq Y(\mathcal{D})$ *and* $\dim_K(Y(\mathcal{D})/Y(\mathcal{C})) = \deg(\mathcal{D}) - \deg(\mathcal{C}) - (\ell(\mathcal{D}) - \ell(\mathcal{C}))$

Proof. The set inclusions in *1.)* and *2.)* follow immediately from the definitions.

1.) Let $\mathfrak{S} \subseteq \mathfrak{P}$ be a finite set of places containing the supports of both $\mathcal{C}$ and $\mathcal{D}$. If we can show that $R(\mathcal{D})/R(\mathcal{C})$ and $\mathfrak{L}(\mathcal{D}, \mathfrak{S})/\mathfrak{L}(\mathcal{C}, \mathfrak{S})$ are isomorphic then the formula follows by the above corollary.

Define a map by taking $u \in \mathfrak{L}(\mathcal{D}, \mathfrak{S})$ to $u/\mathfrak{S}$. Clearly $u/\mathfrak{S} \in R(\mathcal{D})$ and the so defined map ψ is linear. $u/\mathfrak{S} \in R(\mathcal{C})$ if and only if $u \in \mathfrak{L}(\mathcal{C}, \mathfrak{S})$. So ψ gives rise to an injective linear map

$$\widehat{\psi}\colon \mathfrak{L}(\mathcal{D}, \mathfrak{S})/\mathfrak{L}(\mathcal{C}, \mathfrak{S}) \to R(\mathcal{D})/R(\mathcal{C}).$$

To show that $\widehat{\psi}$ is surjective take some $\Gamma \in R(\mathcal{D})$, i.e. $v_{\mathcal{P}}(\Gamma) \geq -v_{\mathcal{P}}(\mathcal{D})$ for all places. By the Theorem of Independence of Valuations there is some $w \in F$ with the property $v_{\mathcal{P}}(w - \Gamma_{\mathcal{P}}) \geq -v_{\mathcal{P}}(\mathcal{C})$ for all $\mathcal{P} \in \mathfrak{S}$. $v_{\mathcal{P}}(w) \geq \min(v_{\mathcal{P}}(w - \Gamma_{\mathcal{P}}), v_{\mathcal{P}}(\Gamma_{\mathcal{P}})) \geq -v_{\mathcal{P}}(\mathcal{D})$, so w is an element of $\mathfrak{L}(\mathcal{D}, \mathfrak{S})$. Γ has no poles outside $\mathfrak{S}$, so $v_{\mathcal{P}}(w/\mathfrak{S} - \Gamma) \geq -v_{\mathcal{P}}(\mathcal{C})$ for all places $\mathcal{P}$, i.e. $w/\mathfrak{S}$ is congruent Γ modulo $R(\mathcal{C})$.

2.) We will use the following two standard lemmas from linear algebra: If W is a vector space and U, V are subspaces of W then

$$U/U \cap V \cong (U+V)/V.$$

If $U \subseteq V \subseteq W$ then

$$W/V \cong (W/U)/(V/U).$$

Since $Y(\mathcal{D}) = R(\mathcal{D}) + F = R(\mathcal{D}) + Y(\mathcal{C})$ we obtain $Y(\mathcal{D})/Y(\mathcal{C}) \cong R(\mathcal{D})/R(\mathcal{D}) \cap Y(\mathcal{C})$ by the first relation. For $\Gamma \in R(\mathcal{C})$, $y \in F$ the definition shows that $\Gamma + y \in R(\mathcal{D})$ if and only if $y \in F \cap R(\mathcal{D}) = \mathfrak{L}(\mathcal{D})$. This leads to $R(\mathcal{D}) \cap Y(\mathcal{C}) = R(\mathcal{C}) + \mathfrak{L}(\mathcal{D})$. Using all this we obtain

$$\begin{gathered} Y(\mathcal{D})/Y(\mathcal{C}) \cong R(\mathcal{D})/R(\mathcal{D}) \cap Y(\mathcal{C}) = \\ R(\mathcal{D})/(R(\mathcal{C}) + \mathfrak{L}(\mathcal{D})) \cong \frac{R(\mathcal{D})/R(\mathcal{C})}{(R(\mathcal{C}) + \mathfrak{L}(\mathcal{D}))/R(\mathcal{C})} \cong \\ \frac{R(\mathcal{D})/R(\mathcal{C})}{\mathfrak{L}(\mathcal{D})/R(\mathcal{C}) \cap \mathfrak{L}(\mathcal{D})} = \frac{R(\mathcal{D})/R(\mathcal{C})}{\mathfrak{L}(\mathcal{D})/\mathfrak{L}(\mathcal{C})}. \end{gathered}$$

By *1.)* the dimension of the numerator is equal to $\deg(\mathcal{D}) - \deg(\mathcal{C})$. The dimension of the denominator equals $\ell(\mathcal{D}) - \ell(\mathcal{C})$ which completes the proof.

□

Corollary 2.2.6. *Let $\mathcal{C} \leq \mathcal{D}$ be divisors of F. Then $\dim_K(Y(\mathcal{D})/Y(\mathcal{C})) \leq \ell(\mathcal{C}) - \deg(\mathcal{C}) + g - \kappa$. If $\deg(\mathcal{D}) - \ell(\mathcal{D}) = g - \kappa$ then equality holds.*

Proof. By Riemann's Theorem $\deg(\mathcal{D}) - \ell(\mathcal{D}) \leq g - \kappa$. So this follows easily from the previous lemma. □

Theorem 2.2.7 (Weak Riemann-Roch Theorem)**.** *Let F/K be an algebraic function field. Then for any divisor $\mathcal{D}$ the formula*

$$\ell(\mathcal{D}) = \deg(\mathcal{D}) + j(\mathcal{D}) - g + \kappa$$

holds. In particular, $j(\mathcal{D})$ is finite.

Proof. By the definition of the genus there is some divisor $\mathcal{C}$ with the property $\deg(\mathcal{C}) - \ell(\mathcal{C}) = g - \kappa$. This equality is also true for any divisor $\mathcal{B} \geq \mathcal{C}$. If we define $\mathcal{B}$ by $v_{\mathcal{P}}(\mathcal{B}) := \max(v_{\mathcal{P}}(\mathcal{C}), v_{\mathcal{P}}(\mathcal{D}))$ Corollary 2.2.6 gives

$$j(\mathcal{D}) = \dim_K(R/Y(\mathcal{D})) \geq \dim_K(Y(\mathcal{B})/Y(\mathcal{D})) = \ell(\mathcal{D}) - \deg(\mathcal{D}) + g - \kappa.$$

Define $n := \ell(\mathcal{D}) - \deg(\mathcal{D}) + g - \kappa$ and choose $n+1$ elements $\Gamma_0, \ldots, \Gamma_n \in R$. Since each of the Γ_i has only finitely many zeros and poles, defining

$$v_{\mathcal{P}}(\mathcal{B}') := \max(v_{\mathcal{P}}(\mathcal{C}), v_{\mathcal{P}}(\mathcal{D}), -v_{\mathcal{P}}(\Gamma_0), \ldots, -v_{\mathcal{P}}(\Gamma_n)), \quad \mathcal{P} \in \mathfrak{P},$$

gives rise to a divisor $\mathcal{B}' \geq \mathcal{C}$. It has the properties $\Gamma_i \in R(\mathcal{B}')$ for all i. Using the above equality with $\mathcal{B}'$ instead of $\mathcal{B}$ yields $\dim_K(Y(\mathcal{B}')/Y(\mathcal{D})) = n$ and therefore the Γ_i are linearly dependent. □

Remark. Since $\dim_K(\Omega(\mathcal{D})) = j(\mathcal{D})$ we observe that this vector space is finite dimensional for every divisor $\mathcal{D}$.

If we set $\mathcal{D}$ to be the unit divisor $\mathfrak{o}$ the Weak Riemann-Roch Theorem yields

Corollary 2.2.8. $g = j(\mathfrak{o}) = \dim_K(R/Y(\mathfrak{o}))$.

2.3 The Riemann-Roch Theorem

In this section we will prove the final version of the theorem. We shall achieve this by assigning a certain divisor to each differential. We call divisors stemming from a differential *canonical divisors*. It is possible to express the index $j(\mathcal{D})$ of a divisor as the dimension of a certain Riemann-Roch space using both $\mathcal{D}$ and a fixed canonical divisor. Within this section we will follow [14, chapter 1.5].

When we defined the set of differentials Ω of a function field F/K, we saw that it is a K-vector space. Since the product of an element $z \in F$ and a repartition $\Gamma \in R$ is defined[6] we may introduce a multiplication $F \times \Omega \to \Omega$ by

$$z\omega(\Gamma) := \omega(z\Gamma).$$

Lemma 2.3.1. *Let F/K be an algebraic function field, $\mathcal{C}, \mathcal{D}$ be divisors, $\omega \in \Omega(\mathcal{C})$ and $z \in \mathfrak{L}(\mathcal{D})$. Then $z\omega \in \Omega(\mathcal{C}\mathcal{D}^{-1})$.*

Proof. We consider an arbitrary $\Gamma \in Y(\mathcal{C}\mathcal{D}^{-1})$ and claim that $z\Gamma \in Y(\mathcal{C})$. $\Gamma = \Delta + y$ for some $\Delta \in R(\mathcal{C}\mathcal{D}^{-1})$ and $y \in F$. For an arbitrary place $\mathcal{P}$

$$v_{\mathcal{P}}(z\Delta) + v_{\mathcal{P}}(\mathcal{C}) = \underbrace{v_{\mathcal{P}}(z) + v_{\mathcal{P}}(\mathcal{D})}_{\geq 0} + \underbrace{v_{\mathcal{P}}(\Delta) + v_{\mathcal{P}}(\mathcal{C}) - v_{\mathcal{P}}(\mathcal{D})}_{\geq 0} \geq 0$$

so $z\Delta \in R(\mathcal{C})$ and $z\Gamma \in Y(\mathcal{C})$. This shows $z\omega(\Gamma) = \omega(z\Gamma) = 0$. □

[6] In the canonical way $(z \cdot \Gamma)_{\mathcal{P}} = z \cdot \Gamma_{\mathcal{P}}$.

Corollary 2.3.2. *With the above defined multiplication Ω is an F-vector space.*

Proof. Take $\omega \in \Omega$ and $z \in F$. Then $\omega \in \Omega(\mathcal{D})$ for some divisor $\mathcal{D}$ and $z \in \mathfrak{L}((z^{-1}))$. By the above lemma $z\omega \in \Omega((z)\mathcal{D}) \subseteq \Omega$. □

Our next step is to prove that Ω as an F-vector space has a rather simple structure:

Theorem 2.3.3. *Let F/K be an algebraic function field, Ω be the space of differentials. Then Ω is one-dimensional as an F-vector space.*

Proof. First we will argue that Ω is not the zero space, i.e. that there is a non-trivial differential. By Theorem 2.2.7

$$j(\mathcal{D}) = \ell(\mathcal{D}) - \deg(\mathcal{D}) + g - \kappa \geq -\deg(\mathcal{D}) - \kappa$$

for an arbitrary divisor $\mathcal{D}$. So if $\deg(\mathcal{D}) \leq -1-\kappa$ then $j(\mathcal{D}) \geq 1$ and therefore $\Omega \supseteq \Omega(\mathcal{D}) \neq \{0\}$. This shows that there are non-trivial differentials.

Now take differentials ω_1, ω_2. We want to show that they are linearly dependent over F. Wlog we may assume both to be non-zero. For $i = 1, 2$ there is some divisor $\mathcal{D}_i$ such that $\omega_i \in \Omega(\mathcal{D}_i)$. We take a divisor $\mathcal{C}$ which we will specify later and consider the maps

$$\varphi_i := \begin{cases} \mathfrak{L}(\mathcal{C}\mathcal{D}_i) \to \Omega(\mathcal{C}^{-1}) \\ z \mapsto z\omega_i \end{cases} .$$

By Lemma 2.3.1 this function indeed maps into $\Omega(\mathcal{C}^{-1})$. φ_i is also injective: Since $\omega_i \neq 0$ there is some $\Gamma \in R$ with the propery $\omega_i(\Gamma) \neq 0$. Hence if $z \neq 0$ we see from $(z\omega_i)(z^{-1}\Gamma) \neq 0$ that $z\omega_i$ is non-zero.

A well known result from linear algebra is that if U_1 and U_2 are subspaces of a finite-dimensional vector space V then

$$\dim(U_1 \cap U_2) \geq \dim(U_1) + \dim(U_2) - \dim(V).$$

We will use this with $U_i := \varphi_i(\mathfrak{L}(\mathcal{C}\mathcal{D}_i))$ and $V := \Omega(\mathcal{C}^{-1})$ to show that $U_1 \cap U_2 \neq \{0\}$ if we choose $\mathcal{C}$ appropriately. Recall that $\mathcal{D} \mapsto \deg(\mathcal{D}) - \ell(\mathcal{D})$ is monotone. Therefore if $\mathcal{D}_0$ has the property that equality holds in Riemann's Theorem and $\mathcal{D} \geq \mathcal{D}_0$ then this is true for $\mathcal{D}$ as well. So it is possible to choose a positive divisor $\mathcal{C}$ such that

$$\ell(\mathcal{C}\mathcal{D}_i) = \deg(\mathcal{C}\mathcal{D}_i) - g + \kappa$$

for $i = 1, 2$. Since $\mathcal{C}$ is positive $\ell(\mathcal{C}^{-1}) = 0$ and hence

$$\dim_K(\Omega(\mathcal{C}^{-1})) = j(\mathcal{C}^{-1}) = \ell(\mathcal{C}^{-1}) - \deg(\mathcal{C}^{-1}) + g - \kappa = \deg(\mathcal{C}) + g - \kappa.$$

Combining these equations with the inequality above gives

$$\begin{aligned}\dim(U_1 \cap U_2) \geq \\ (\deg(\mathcal{C}\mathcal{D}_1) - g + \kappa) + (\deg(\mathcal{C}\mathcal{D}_2) - g + \kappa) - (\deg(\mathcal{C}) + g - \kappa) \\ = \deg(\mathcal{C}) + \deg(\mathcal{D}_1) + \deg(\mathcal{D}_2) + 3(\kappa - g)\end{aligned}$$

Since $\mathcal{D}_1$, $\mathcal{D}_2$, κ and g are fixed we may choose $\mathcal{C}$ in a way that makes the right hand side positive. This shows that the intersection $U_1 \cap U_2$ is not trivial. Therefore we can pick elements $z_1, z_2 \in F$ such that $z_1\omega_1 = z_2\omega_2 \neq 0$ and hence $\omega_2 = (z_1/z_2)\omega_1$. □

Lemma 2.3.4. *Let F be an algebraic function field and $\omega \neq 0$ a differential. Then there exists a unique divisor $\mathcal{W}$ with the properties:*

- *ω vanishes on $Y(\mathcal{W})$, i.e. $\omega \in \Omega(\mathcal{W})$.*
- *For any divisor $\mathcal{D}$ for which ω vanishes on $Y(\mathcal{D})$ we have $\mathcal{D} \leq \mathcal{W}$.*

Proof. By Corollary 1.5.13 we know that there is a constant c such that if $\deg(\mathcal{D}) \geq c$ for some divisor $\mathcal{D}$ then $\ell(\mathcal{D}) = \deg(\mathcal{D}) + \kappa - g$. This gives $j(\mathcal{D}) = 0$ or in other words $\Omega(\mathcal{D}) = \{0\}$. Therefore if $\omega \in \Omega(\mathcal{D})$ then $\deg(\mathcal{D}) < c$. So there are maximal elements in the set

$$\{\mathcal{D} \colon \mathcal{D} \text{ is a divisor}, \omega \in \Omega(\mathcal{D})\}.$$

Now for $\mathcal{D}_1$, $\mathcal{D}_2$ define a divisor $\mathcal{D}_1 \vee \mathcal{D}_2$ by

$$v_{\mathcal{P}}(\mathcal{D}_1 \vee \mathcal{D}_2) := \max(v_{\mathcal{P}}(\mathcal{D}_1), v_{\mathcal{P}}(\mathcal{D}_2))$$

for all places $\mathcal{P}$. Then from the definition it is straightforward to see that $R(\mathcal{D}_1 \vee \mathcal{D}_2) = R(\mathcal{D}_1) \cup R(\mathcal{D}_2)$. Thus $Y(\mathcal{D}_1 \vee \mathcal{D}_2) = Y(\mathcal{D}_1) \cup Y(\mathcal{D}_2)$, so ω vanishes on $Y(\mathcal{D}_1 \vee \mathcal{D}_2)$ if and only if it vanishes on both $Y(\mathcal{D}_1)$ and $Y(\mathcal{D}_2)$. This yields $\Omega(\mathcal{D}_1 \vee \mathcal{D}_2) = \Omega(\mathcal{D}_1) \cap \Omega(\mathcal{D}_1)$ which shows that the above defined set is closed under $\vee$. So there is exactly one maximal element $\mathcal{W}$ which is also the greatest element.

□

Definition 2.3.5. Let ω be a non-zero differential of a function field F/K. Then the unique maximal divisor $\mathcal{W}$ with the property that $\omega \in \Omega(\mathcal{W})$ is called *the divisor of* ω and denoted by (ω). Every divisor stemming from a differential is said to be a *canonical divisor* . The order function of a differential is defined by $v_{\mathcal{P}}(\omega) := v_{\mathcal{P}}((\omega))$.

Lemma 2.3.6. *Let F/K be a function field, $z \in F^\times$ and $\omega \neq 0$ a differential. Then $(z\omega) = (z)(\omega)$.*

Proof. In the proof of Corollary 2.3.2 we showed the following: If ω vanishes on $Y(\mathcal{D})$ then $z\omega$ vanishes on $Y((z)\mathcal{D})$. If we set $\mathcal{D} = (\omega)$ we see that $z\omega$ vanishes on $Y((z)(\omega))$, hence $(z)(\omega) \leq (z\omega)$. Substitution yields $(z^{-1})(z\omega) \leq (z^{-1}z\omega) = (\omega)$. Multiplying with (z) concludes the proof. □

Definition 2.3.7. If $\mathcal{D}_1, \mathcal{D}_2$ are divisors then they are said to be equivalent if there is some $z \in F^\times$ such that $\mathcal{D}_1 = (z)\mathcal{D}_2$. Since $\deg((z)) = 0$ equivalent divisors are of the same degree.

Corollary 2.3.8. *Any two canonical divisors are equivalent.*

Proof. Consider two non-zero differentials ω_1, ω_2. Then by Theorem 2.3.3 there is some $z \in F^\times$ such that $\omega_1 = z\omega_2$. By the previous lemma $(\omega_1) = (z)(\omega_2)$. □

From the next theorem the Riemann-Roch Theorem will follow easily. It basically states that the linear injection we already considered in the proof of Theorem 2.3.3 is surjective if the involved divisor $\mathcal{C}$ is a canonical divisor.

Theorem 2.3.9. *Let $\mathcal{D}$ be an arbitrary divisor and $\mathcal{W} = (\omega)$ be a canonical divisor. Then*

$$\varphi\colon \begin{cases} \mathfrak{L}(\mathcal{W}\mathcal{D}^{-1}) \to \Omega(\mathcal{D}) \\ z \mapsto z\omega \end{cases}$$

is an isomorphism. Therefore $j(\mathcal{D}) = \ell(\mathcal{W}\mathcal{D}^{-1})$.

Proof. We already saw that φ maps $\mathfrak{L}(\mathcal{W}\mathcal{D}^{-1})$ into $\Omega(\mathcal{D})$ and that it is injective. To prove surjectivity fix some element $\omega_0 \in \Omega(\mathcal{D}) \setminus \{0\}$. By Theorem 2.3.3, ω spans Ω as an F-vector space, so there is an element $z \in F$ such that $\omega_0 = z\omega$. Using the privious corollary yields $(z)\mathcal{W} = (z)(\omega) = (z\omega) = (\omega_0) \geq \mathcal{D}$. This shows $z \in \mathfrak{L}(\mathcal{W}\mathcal{D}^{-1})$ which proves the claim. □

Combining this with the weak Riemann-Roch Theorem gives:

Theorem 2.3.10 (Riemann-Roch Theorem)**.** *Let F/K be an algebraic function field. Fix some canonical divisor $\mathcal{W}$ of F/K. Then for an arbitrary divisor $\mathcal{D}$ the following formula holds:*

$$\ell(\mathcal{D}) = \deg(\mathcal{D}) + \ell(\mathcal{W}\mathcal{D}^{-1}) + \kappa - g$$

Corollary 2.3.11. *Let $\mathcal{W}$ be some canonical divisor. Then $\ell(\mathcal{W}) = g-\kappa+1$ and $\deg(\mathcal{W}) = 2g - 2\kappa$.*

Proof. For the first claim set $\mathcal{D} = \mathfrak{o}$ in the Riemann-Roch Theorem. This gives

$$1 = \ell(\mathfrak{o}) = \deg(\mathfrak{o}) + \ell(\mathcal{W}) + \kappa - g = \ell(\mathcal{W}) + \kappa - g.$$

The second claim follows by setting $\mathcal{D} = \mathcal{W}$:

$$g - \kappa + 1 = \ell(\mathcal{W}) = \deg(\mathcal{W}) + \ell(\mathfrak{o}) + \kappa - g = \deg(\mathcal{W}) + 1 + \kappa - g$$

Rearranging this equation concludes the proof. □

A direct consequence of Riemann's Theorem was Corollary 1.5.13. It showed the existence of a certain integer c, depending only on the function field F/K, such that $\ell(\mathcal{D}) = \deg(\mathcal{D}) + \kappa - g$ for all divisors $\mathcal{D}$ with degree greater than or equal to c. We are now able to specify this constant:

Corollary 2.3.12. *Let F/K be a function field and $\mathcal{D}$ a divisor such that $\deg(\mathcal{D}) > 2g - 2\kappa$. Then*

$$\ell(\mathcal{D}) = \deg(\mathcal{D}) + \kappa - g.$$

Proof. Let $\mathcal{W}$ be a canonical divisor. The last corollary and our assumption imply $\deg(\mathcal{W}\mathcal{D}^{-1}) < 0$. Thus $\ell(\mathcal{W}\mathcal{D}^{-1}) = 0$ and so our claim follows from the Riemann-Roch Theorem. □

Remark. The bound of the above corollary is the best possible, since for a canonical divisor $\mathcal{W}$ we have $\ell(\mathcal{W}) = g - \kappa + 1$, whereas $\deg(\mathcal{W}) + \kappa - g = (2g - 2\kappa) + \kappa - g = g - \kappa$.

2.4 Local Components of Differentials

For the definition of Goppa codes in Chapter 4 we will need the notion of the local component of some differential ω of F/K. In the previous section we considered an embedding of F into R, which mapped some $f \in F$ to the repartition that is constantly f. Now we shall define a different embedding $\iota_{\mathcal{P}} \colon F \to R$ for some place $\mathcal{P}$ of F/K, namely

$$\iota_{\mathcal{P}}(f)(\mathcal{Q}) := \begin{cases} f, \text{ if } \mathcal{Q} = \mathcal{P} \\ 0, \text{ if } \mathcal{Q} \neq \mathcal{P} \end{cases} .$$

Definition 2.4.1. For an algebraic function field F/K, a differential $\omega \in \Omega$ and a place $\mathcal{P}$ we define the local component $\omega_{\mathcal{P}} \colon F \to K$ by

$$\omega_{\mathcal{P}}(f) := \omega(\iota_{\mathcal{P}}(f)).$$

Since $\iota_{\mathcal{P}}$ and ω are K-linear, the local component is a linear functional.

Proposition 2.4.2. *Let F/K be an algebraic function field, $\omega \in \Omega$ and let $\Gamma \in R$ be a repartition. Then $\omega_{\mathcal{P}}(\Gamma_{\mathcal{P}}) \neq 0$ for only finitely many places $\mathcal{P}$. The following equation holds:*

$$\omega(\Gamma) = \sum_{\mathcal{P} \in \mathfrak{P}} \omega_{\mathcal{P}}(\Gamma_{\mathcal{P}})$$

Proof. Wlog assume $\omega \neq 0$ and set $\mathcal{W} := (\omega)$, the canonical divisor of ω. Since $v_{\mathcal{P}}(\mathcal{W}) \neq 0$ for only finitely many places $\mathcal{P}$, Γ has only finitely many values $f_1, \ldots, f_k \in F$, and each of these functions has only finitely many poles, we conclude $v_{\mathcal{P}}(\Gamma_{\mathcal{P}}) < 0$ for only finitely many places $\mathcal{P}$. Thus there is a finite set $\mathfrak{S} \subseteq \mathfrak{P}$ such that

$$v_{\mathcal{P}}(\mathcal{W}) = 0, v_{\mathcal{P}}(\Gamma) \geq 0 \quad \forall \mathcal{P} \notin \mathfrak{S}.$$

Define $\Delta_{\mathcal{P}} := \Gamma_{\mathcal{P}}$ for $\mathcal{P} \notin \mathfrak{S}$ and $\Delta_{\mathcal{P}} := 0$ else. Then $\Delta \in Y(\mathcal{W})$ since $\operatorname{supp} \mathcal{W} \subseteq \mathfrak{S}$. Thus we have

$$\omega(\Gamma) = \underbrace{\omega(\Delta)}_{=0} + \omega\left(\sum_{\mathcal{P} \in \mathfrak{S}} \iota_{\mathcal{P}}(\Gamma_{\mathcal{P}})\right) = \sum_{\mathcal{P} \in \mathfrak{S}} \omega_{\mathcal{P}}(\Gamma_{\mathcal{P}}).$$

If $\mathcal{P} \notin \mathfrak{S}$ then $v_{\mathcal{P}}(\Gamma_{\mathcal{P}}) \geq 0 = -v_{\mathcal{P}}(\mathcal{W})$ and so $\iota_{\mathcal{P}}(\Gamma_{\mathcal{P}}) \in Y(\mathcal{W})$. Thus $\omega_{\mathcal{P}}(\Gamma_{\mathcal{P}}) = \omega(\iota_{\mathcal{P}}(\Gamma_{\mathcal{P}})) = 0$, which shows the claimed equation. □

The following lemma gives an alternative description of the order of a differential at a place.

Lemma 2.4.3. *Let $\omega \colon R \to K$, $\omega \neq 0$ be a differential of F/K and $\mathcal{P}$ be a place. Then*

$$v_{\mathcal{P}}(\omega) = \max\{r \in \mathbb{Z} \colon \omega_{\mathcal{P}}(f) = 0 \text{ for all } f \in F \text{ with } v_{\mathcal{P}}(f) \geq -r\}.$$

Proof. By definition, $v_{\mathcal{P}}(\omega) = v_{\mathcal{P}}(\mathcal{W})$ where $\mathcal{W} := (\omega)$ is the divisor of ω. Set $s := v_{\mathcal{P}}(\omega)$. If $f \in F$, $v_{\mathcal{P}}(f) \geq -s$ then $\iota_{\mathcal{P}}(f) \in R(\mathcal{W}) \subseteq Y(\mathcal{W})$. ω vanishes on $Y(\mathcal{W})$, so $\omega_{\mathcal{P}}(f) = \omega(\iota_{\mathcal{P}}(f)) = 0$. Now assume that $\omega_{\mathcal{P}}(f) = 0$ for all $f \in F$ satisfying $v_{\mathcal{P}}(f) \geq -s - 1$. Take an arbitrary element $\Gamma \in R(\mathcal{W}\mathcal{P})$.

We have $\Gamma = (\Gamma - \iota_{\mathcal{P}}(\Gamma_{\mathcal{P}})) + \iota_{\mathcal{P}}(\Gamma_{\mathcal{P}})$ as well as $\Gamma - \iota_{\mathcal{P}}(\Gamma_{\mathcal{P}}) \in Y(\mathcal{W})$ and $v_{\mathcal{P}}(\Gamma_{\mathcal{P}}) \geq -s-1$, hence

$$\omega(\Gamma) = \omega(\Gamma - \iota_{\mathcal{P}}(\Gamma_{\mathcal{P}})) + \omega(\iota_{\mathcal{P}}(\Gamma_{\mathcal{P}})) = 0.$$

So ω vanishes on $R(\mathcal{WP})$ and thus also on $Y(\mathcal{WP}) = R(\mathcal{WP}) + F$. But this contradicts the definition of $\mathcal{W}$. Thus there is some $f \in F$, $v_{\mathcal{P}}(f) = -s-1$ such that $\omega(f) \neq 0$, which proves the claim. □

Chapter 3

Algebraic Curves

Each algebraic curve, defined over some field K, gives rise to the field of rational functions on the curve. This field is an algebraic function field over K in the sense of our definition. The theory of algebraic curves is closely related to the theory of algebraic function fields: In the case of a non-singular curve, certain groups of points (conjugated points, see Section 3.7) are in one-to-one correspondance to the places of the function field. The genus of the function field is related to the degree of the polynomial defining the curve via the Plücker Formula. The reason for our study of algebraic curves is twofold: On one hand, they provide interesting examples of algebraic function fields (actually, up to isomorphy, any algebraic function field is of this kind, see e.g. [14, Appendix B]). On the other hand, evaluating certain rational functions on a curve at a fixed set of points will provide a method of constructing concrete Goppa codes (see Section 4.3.2).

After defining affine and projective algebraic curves in the following sections we will investigate the associated function field. A brief summary of the basic definitions needed for the purpose of Goppa codes including helpful examples can be found in [8, Section 2.1]. A more involved discussion about algebraic curves with an emphasis on curves over finite fields is provided in [10].

3.1 Affine and Projective Space

To establish notation we state the well-known definitions of affine and projective spaces.

Definition 3.1.1. Let K be an arbitrary field. The n-dimensional affine space over K is the set of n-tuples $(a_1, \ldots, a_n)$, $a_i \in K$. It will be denoted by $\mathbb{A}_K^n$ or simply $\mathbb{A}^n$ if the underlying field is not in question.

To define the n-dimensional projective space $\mathbb{P}^n_K$ or $\mathbb{P}^n$ consider the following equivalence relation on $\mathbb{A}^{n+1} \setminus \{\vec{0}\}$:

$$(a_0, a_1, \ldots, a_n) \sim (b_0, b_1, \ldots, b_n) :\Leftrightarrow \exists \lambda \in K^\times : a_i = \lambda b_i,\ 0 \leq i \leq n$$

The n-dimensional projective space is defined by $(\mathbb{A}^{n+1} \setminus \{\vec{0}\})/_\sim$. We write the equivalence class of $(a_0, a_1, \ldots, a_n)$ as $(a_0 : a_1 : \ldots : a_n)$. Let us consider the map given by

$$\psi_i : \begin{cases} \mathbb{A}^n \to \mathbb{P}^n \\ (a_1, \ldots, a_n) \mapsto (a_1 : \ldots : a_i : 1 : a_{i+1} : \ldots : a_n) \end{cases}$$

for $0 \leq i \leq n$. It is injective and it is not hard to verify that $\mathbb{P}^n = \bigcup_{i=0}^n \psi_i(\mathbb{A}^n)$, i.e. the $n+1$ copies $\psi_i(\mathbb{A}^n)$ of $\mathbb{A}^n$ cover the projective space.

3.2 Absolutely Irreducible Polynomials

For the whole chapter we will use the following notation for polynomials: For a field K, $\dot{x}$, $\dot{y}$, $\dot{z}$ will denote independent variables. $K[\dot{x}]$, $K[\dot{x}, \dot{y}]$ and $K[\dot{x}, \dot{y}, \dot{z}]$ will denote the polynomials in one, two or three variables and we will write $f(\dot{x}), g(\dot{x}, \dot{y})$ or $h(\dot{x}, \dot{y}, \dot{z})$ for their elements. The reason for this convention will be clear from Section 3.3 on.

Irreducibility of a polynomial $f(\dot{x}, \dot{y}) \in K[\dot{x}, \dot{y}]$ depends on the field. If L is an extension field of K, $f(\dot{x}, \dot{y})$ may factor in $L[\dot{x}, \dot{y}]$ while it is irreducible in $K[\dot{x}, \dot{y}]$. We call $f(\dot{x}, \dot{y})$ *absolutely irreducible* if it is irreducible in $\overline{K}[\dot{x}, \dot{y}]$, where $\overline{K}$ is the algebraic closure of K. Constant polynomials are by definition neither reducible nor irreducible. Since the irreducible elements of $\overline{K}[\dot{x}]$ are exactly the polynomials of degree one, it is not clear whether there are non-trivial examples of absolutely irreducible polynomials in $K[\dot{x}, \dot{y}]$. Below we cite Eisenstein's criterion and show how to use it to prove the existence of such polynomials. For a proof of this well-known result see e.g. [16].

Proposition 3.2.1 (Eisenstein's Criterion)**.** *Let R be an integral domain and*

$$g(\dot{x}) = a_n \dot{x}^n + a_{n-1} \dot{x}^{n-1} + \ldots + a_1 \dot{x} + a_0$$

a polynomial in $R[\dot{x}]$. If there is a prime element $p \in R$ such that $p \nmid a_n$, $p | a_i$ for $0 \leq i \leq n-1$, $p^2 \nmid a_0$ then $g(\dot{x})$ is irreducible in $R[\dot{x}]$.

If we set $R = \overline{K}[\dot{y}]$ and choose p to be a linear polynomial in the independent variable $\dot{x}$, this proves the following

Corollary 3.2.2. *Take a polynomial*

$$f(\dot{x},\dot{y}) = \sum_{i=0}^{n} p_i(\dot{y})\dot{x}^i \in K[\dot{x},\dot{y}]$$

where $p_i(\dot{y}) \in K[\dot{y}]$. *If there is some* $\alpha \in \overline{K}$, *such that* $p_n(\alpha) \neq 0$, $p_i(\alpha) = 0$ *for* $0 \leq i \leq n-1$, α *is not a double root of* $p_0(\dot{y})$ *then* $f(\dot{x},\dot{y})$ *is absolutely irreducible.*

Example 3.2.3.

- *For every field* K *and an arbitrary integer* $n > 0$ *the polynomial* $y^n - x$ *is absolutely irreducible.*
- *If* $n > 0$, $\operatorname{char} K \nmid n$ *then* $x^n + y^n - 1$ *is absolutely irreducible.*

3.3 Affine Curves

For the rest of the chapter we shall assume that K is an arbitrary field. We will then consider the affine space $\mathbb{A}^n = \mathbb{A}^n_{\overline{K}}$ over the algebraic closure $\overline{K}$. An affine algebraic curve is the set of zeros of an absolutely irreducible polynomial in two variables:

Definition 3.3.1 (Affine Algebraic Curve)**.** Let $f(\dot{x},\dot{y})$ be an absolutely irreducible polynomial. Then the set of points $(a,b) \in \mathbb{A}^2_{\overline{K}}$ which are zeros of $f(\dot{x},\dot{y})$ is called an *affine algebraic curve*. To indicate that $f(\dot{x},\dot{y})$ defines a curve we will write C_f or $C\colon f(\dot{x},\dot{y}) = 0$.

Every affine algebraic curve gives rise to a field. As we shall see in the next paragraphs, this field is an algebraic function field over K. To motivate the definition let us first consider an example.

Example 3.3.2. *Let us consider the curve* $C\colon \dot{x}^2 + \dot{y}^2 - 1 = 0$ *over some field* K *with* $\operatorname{char} K \neq 2$. *Consider the rational function* $\varphi(\dot{x},\dot{y}) := \dot{x}/\dot{y}$. *It can be evaluated for all points* $(a,b) \in C \setminus \{(\pm 1, 0)\}$. *For such a point*

$$\frac{a}{b} = \frac{a^2}{ab} = \frac{1-b^2}{ab}$$

so φ *has the same values as* $\psi(\dot{x},\dot{y}) := (1-\dot{y}^2)/(\dot{x}\dot{y})$ *in those points of* C *where both are defined. In the general case of some irreducible* $f(\dot{x},\dot{y})$, *when it comes to evaluating two functions* $g_i(\dot{x},\dot{y})/h_i(\dot{x},\dot{y}), i = 1,2$, *at points of* C_f, *we do not want to distinguish between them if* $f(\dot{x},\dot{y})$ *divides* $g_1(\dot{x},\dot{y})h_2(\dot{x},\dot{y}) - g_2(\dot{x},\dot{y})h_1(\dot{x},\dot{y})$.

Definition 3.3.3 (Function Field of an Affine Curve)**.** Let C_f be an algebraic curve described by some absolutely irreducible polynomial $f(\dot{x}, \dot{y}) \in K[\dot{x}, \dot{y}]$. The ring $K[C_f] := K[\dot{x}, \dot{y}]/f(\dot{x}, \dot{y})$ is called the *coordinate ring* of C_f. It is an integral domain since $f(\dot{x}, \dot{y})$ is irreducible. Therefore $K[C_f]$ has a field of fractions which we denote by $K(C_f)$. The field $K(C_f)$ is called the *function field* of C_f.

Remark. We set $x := \dot{x} + (f(\dot{x}, \dot{y})) \in K[C_f]$ and $y := \dot{y} + (f(\dot{x}, \dot{y})) \in K[C_f]$. Then for any polynomial $g(\dot{x}, \dot{y})$ its class modulo $f(\dot{x}, \dot{y})$ is given by $g(x, y)$. In this notation $g(x, y) = 0$ in $K[C_f]$ if and only if $f(\dot{x}, \dot{y}) | g(\dot{x}, \dot{y})$.

Example 3.3.4. *Consider the function field given by the curve* $C : f(\dot{x}, \dot{y}) = \dot{x}^3 + \dot{y}^3 - 1 = 0$ *for some field* K *with* $\operatorname{char} K \neq 3$*. The element* $1/x$ *is the same as* $x^2/(1 - y^3)$*.* $y^3/(1 - x)$ *is equal to* $x^2 + x + 1$*.*

The following proposition justifies the name function field for $K(C_f)$.

Proposition 3.3.5. *Let* C_f *be an algebraic curve defined by* $f(\dot{x}, \dot{y})$ *and* $K(C_f)$ *be its function field. Then* $K(C_f)/K$ *is an algebraic function field in the sense of Definition 1.1.1.*

Proof. Since $f(\dot{x}, \dot{y})$ is not constant, the ring homomorphism

$$\begin{cases} K[\dot{x}, \dot{y}] \to K[C_f] \\ g(\dot{x}, \dot{y}) \mapsto g(x, y) \end{cases}$$

is injective on K. Therefore, if we identify K with its image, K is a subring of $K[C_f]$ and thus $K \leq K(C_f)$. Wlog we may assume that $\dot{y}$ occurs in $f(\dot{x}, \dot{y})$. Hence x cannot be algebraic over K: For no element $p(\dot{x}) \in K[\dot{x}]$, $p(\dot{x}) \neq 0$ is a multiple of $f(\dot{x}, \dot{y})$ and therefore $p(x) \neq 0$ in $K[C_f]$. Hence x is transcentental over K and $K(x) \subseteq K(C_f)$. y is algebraic over $K(x)$ since it is a zero of $h(\dot{y}) := f(x, \dot{y}) \in K(x)[\dot{y}]$. Since $K(C_f) = K(x, y) = K(x)(y)$ the extension $K(C_f)/K(x)$ is finite. □

3.4 Homogeneous Polynomials

In order to define projective algebraic curves we introduce *homogeneous polynomials* and mention some of their properties without proving them. Proofs of the cited facts can be found in [19, Chapter I, §10]. In the following definition the degree of a multivariate monomial $\dot{X}_0^{k_0} \cdots \dot{X}_n^{k_n}$ is the sum of its exponents $k_0 + \ldots + k_n$:

Definition 3.4.1. A polynomial $F(\dot{X}_0, \dot{X}_1, \ldots, \dot{X}_n) \in K[\dot{X}_0, \dot{X}_1, \ldots, \dot{X}_n]$ is said to be *homogeneous of degree* d if all of its monomials are of degree d.

A polynomial F is homogeneous of degree d if and only if

$$F(\dot{T}\dot{X}_0, \dot{T}\dot{X}_1, \ldots, \dot{T}\dot{X}_n) = \dot{T}^d F(\dot{X}_0, \dot{X}_1, \ldots, \dot{X}_n)$$

holds in $K[\dot{X}_0, \dot{X}_1, \ldots, \dot{X}_n, \dot{T}]$. If $f(\dot{x}_1, \ldots, \dot{x}_n) \in K[\dot{x}_1, \ldots, \dot{x}_n]$ is of degree d then

$$F(\dot{X}_0, \dot{X}_1, \ldots, \dot{X}_n) := \dot{X}_0^d f(\dot{X}_1/\dot{X}_0, \ldots, \dot{X}_n/\dot{X}_0) \tag{3.1}$$

is homogeneous of degree d. Conversely, if $F(\dot{X}_0, \ldots, \dot{X}_n)$ is homogeneous of degree d, $\dot{X}_i \nmid F$, then

$$f(\dot{x}_1, \ldots, \dot{x}_n) := F(\dot{x}_1, \ldots, \dot{x}_i, 1, \dot{x}_{i+1}, \ldots, \dot{x}_n) \tag{3.2}$$

is a polynomial of degree d. For $i = 0$ Equations (3.1) and (3.2) define a one-to-one correspondence between the polynomials in $K[\dot{x}_1, \ldots, \dot{x}_n]$ of degree d and the homogeneous polynomials in $K[\dot{X}_0, \ldots, \dot{X}_n]$ of degree d not divisible by $\dot{X}_0$. f is irreducible if and only if F is irreducible.

Let us return to the projective plane $\mathbb{P}^2$. An affine point (a_0, a_1, a_2) could be a zero of some polynomial in three variables while $(\lambda a_0, \lambda a_1, \lambda a_2)$, $\lambda \in K^\times$, is not a zero. For a homogeneous polynomial F this is impossible, since

$$F(\lambda a_0, \lambda a_1, \lambda a_2) = \lambda^3 F(a_0, a_1, a_2).$$

Therefore we can define a projective point $(a_0 : a_1 : a_2)$ to be a zero of some homogeneous polynomial $F(\dot{X}_0, \dot{X}_1, \dot{X}_2)$ if $F(a_0, a_1, a_2) = 0$.

3.5 Projective Curves

We are now able to define *projective algebraic curves* . We will see that every affine algebraic curve can be embedded in a projective curve in a canonical way.

Definition 3.5.1 (Projective Algebraic Curve)**.** Let K be an arbitrary field, $\overline{K}$ its algebraic closure and $F(\dot{X}, \dot{Y}, \dot{Z})$ be an absolutely irreducible, homogeneous polynomial. We define the *projective algebraic curve* C_F of F to be the set of all projective points $(a_0 : a_1 : a_2) \in \mathbb{P}^2_{\overline{K}}$ that are zeros of F. A point which has a representative with all coefficients a_i in K is called *rational*.

Remark. Let $f(\dot{x},\dot{y})$ be an absolutely irreducible polynomial of degree d. Then $F(\dot{X},\dot{Y},\dot{Z}) := \dot{Z}^d f(\dot{X}/\dot{Z},\dot{Y}/\dot{Z})$ is absolutely irreducible as well. The affine algebraic curve C_f defined by f is embedded in the projective algebraic curve C_F. To be more precise, the map $\psi_2\colon (a,b) \mapsto (a:b:1)$ we considered in Section 3.1 embeds C_f into C_F. $\psi_2(C_f)$ consists of those points $(b_0 : b_1 : b_2) \in C_F$ with $b_2 \neq 0$. Points $(b_0 : b_1 : 0)$ of C_F are called the *points at infinity*. C_F is called the *projective closure* of C_f . The sets $\psi_i^{-1}(C_F)$, $i = 0, 1, 2$, are the *affine components* of the projective curve. They $\psi_i^{-1}(C_F)$ are algebraic curves described by the equations

$$\begin{aligned}\psi_2^{-1}(C_F)\colon f_2(\dot{x},\dot{y}) &= F(\dot{x},\dot{y},1) = 0\\ \psi_1^{-1}(C_F)\colon f_1(\dot{x},\dot{z}) &= F(\dot{x},1,\dot{z}) = 0\\ \psi_0^{-1}(C_F)\colon f_0(\dot{y},\dot{z}) &= F(1,\dot{y},\dot{z}) = 0\end{aligned}$$

where $f_2(\dot{x},\dot{y}) = f(\dot{x},\dot{y})$, so the corresponding affine component is the original affine curve.

Next we want to define the function field of a projective algebraic curve C_F. Consider all quotients $G(\dot{X},\dot{Y},\dot{Z})/H(\dot{X},\dot{Y},\dot{Z})$ with homogeneous polynomials $G(\dot{X},\dot{Y},\dot{Z}), H(\dot{X},\dot{Y},\dot{Z})$ of the same degree, $F(\dot{X},\dot{Y},\dot{Z}) \nmid H(\dot{X},\dot{Y},\dot{Z})$. Denote this set by R_F. It is a subring of $K(\dot{X},\dot{Y},\dot{Z})$. Denote the set of those quotients G/H in R_F where $F(\dot{X},\dot{Y},\dot{Z})$ divides $G(\dot{X},\dot{Y},\dot{Z})$ by I_F. This is as a maximal ideal of R_F.

Definition 3.5.2 (Function Field of a Projective Curve)**.** The field R_F/I_F is called the function field of the projective curve C_F. We denote it by $K(C_F)$. As in the case of the affine curve we denote the class of the homogeneous polynomial $G(\dot{X},\dot{Y},\dot{Z})$ modulo $F(\dot{X},\dot{Y},\dot{Z})$ by $G(X,Y,Z)$. An analogous notation will be used for quotients.

Example 3.5.3. *Consider the projective curve defined by* $C_F\colon \dot{X}^3+\dot{Y}^3-\dot{Z}^3 = 0$. *This is the homogeneous polynomial corresponding to* f *in Example 3.3.4.* $Y^3/(Z^3 - XZ^2)$ *is an element of the function field* $K(C_F)$ *since* F *does not divide* $\dot{Z}^3 - \dot{X}\dot{Z}^2$. *It is equal to*

$$\begin{aligned}&(Z^3 - X^3)/(Z^3 - XZ^2) =\\ &\qquad (Z - X)(Z^2 + XZ + X^2)/(Z^2(Z - X)) = (Z^2 + XZ + X^2)/Z^2.\end{aligned}$$

For an absolutely irreducible polynomial f and the corresponding homogeneous polynomial F we have seen that the algebraic curve C_f is embedded in C_F. Now we shall see how the function fields $K(C_f)$ and $K(C_F)$ are related.

Proposition 3.5.4. *Let $f(\dot{x},\dot{y}) \in K[\dot{x},\dot{y}]$ be absolutely irreducible and denote by $F(\dot{X},\dot{Y},\dot{Z})$ the homogeneous polynomial with $F(\dot{x},\dot{y},1) = f(\dot{x},\dot{y})$. Then there is an isomorphism from $K(C_F)$ to $K(C_f)$ that fixes K. In particular $K(C_F)$ is an algebraic function field in the sense of Definition 1.1.1.*

Proof. We consider the map

$$\Psi\colon \begin{cases} K(C_F) \to K(C_f) \\ \frac{G(X,Y,Z)}{H(X,Y,Z)} \mapsto \frac{G(x,y,1)}{H(x,y,1)} \end{cases} .$$

Here $G(X,Y,Z)$ and $H(X,Y,Z)$ are residue classes modulo $F(\dot{X},\dot{Y},\dot{Z})$ of homogeneous polynomials of the same degree. We will first show that this map is well-defined and afterwards argue that it is indeed a field isomorphism. Using the facts from Section 3.4 we see

$$\begin{aligned}
&\frac{G(X,Y,Z)}{H(X,Y,Z)} = \frac{G'(X,Y,Z)}{H'(X,Y,Z)} && \iff \\
&\frac{G(X,Y,Z)H'(X,Y,Z) - H(X,Y,Z)G'(X,Y,Z)}{H(X,Y,Z)H'(X,Y,Z)} = 0 && \iff \\
&F(\dot{X},\dot{Y},\dot{Z}) \,\Big|\, \Big(G(\dot{X},\dot{Y},\dot{Z})H'(\dot{X},\dot{Y},\dot{Z}) - H(\dot{X},\dot{Y},\dot{Z})G'(\dot{X},\dot{Y},\dot{Z})\Big) && \iff \\
&f(\dot{x},\dot{y}) = F(\dot{x},\dot{y},1) \,|\, (G(\dot{x},\dot{y},1)H'(\dot{x},\dot{y},1) - H(\dot{x},\dot{y},1)G'(\dot{x},\dot{y},1)) && \iff \\
&\frac{G(x,y,1)}{H(x,y,1)} = \frac{G'(x,y,1)}{H'(x,y,1)}
\end{aligned}$$

thus Ψ is well defined and injective. It is straightforward to check that Ψ is indeed a homomorphism. To show that Ψ is surjective take an element $g(x,y)/h(x,y)$ of $K(C_f)$ and consider

$$\Phi := \frac{Z^d g(X/Z, Y/Z)}{Z^d h(X/Z, Y/Z)} \tag{3.3}$$

where d is the maximum of the degrees of $g(\dot{x},\dot{y})$ and $h(\dot{x},\dot{y})$. Both numerator and denominator are homogeneous of degree d, so Φ is an element of $K(C_F)$. Obviously, Ψ maps Φ to $g(x,y)/h(x,y)$. □

3.6 Evaluating Functions

For a polynomial $p(\dot{x},\dot{y}) = \sum_{i=0}^{m}\sum_{j=0}^{n} p_{i,j}\dot{x}^i\dot{y}^j$ the formal partial derivative with respect to $\dot{x}$ is defined as

$$p_{\dot{x}}(\dot{x},\dot{y}) := \sum_{i=1}^{m}\sum_{j=0}^{n} i p_{i,j}\dot{x}^{i-1}\dot{y}^{j}.$$

$p_{\dot{y}}(\dot{x},\dot{y})$ is defined accordingly and the definition extends to polynomials with more than two variables in the obvious way. Consider the curve C_f defined by some absolutely irreducible $f(\dot{x},\dot{y})$. A point (a,b) of C_f is called *singular* if $f_{\dot{x}}(a,b) = f_{\dot{y}}(a,b) = 0$ and *non-singular* or *regular* otherwise. If $F(\dot{X},\dot{Y},\dot{Z})$ is a homogeneous polynomial the partial derivatives are again homogeneous and thus we can define a point $(a_0 : a_1 : a_2)$ of the projective curve C_F to be singular if all the partial derivatives vanish at this point. The curve C_f and C_F are said to be non-singular or regular if they have no singular points. The following lemma is a well known result about the formal partial derivative. For a proof see e.g. [19, Chapter I].

Lemma 3.6.1. *Let $p(\dot{x},\dot{y})$ be a polynomial with coefficients in some field K and take $a, b \in K$. Then*

$$p(\dot{x},\dot{y}) = p(a,b) + p_x(a,b)(\dot{x}-a) + p_y(a,b)(\dot{y}-b) + (\dot{x}-a)^2 p_1(\dot{x},\dot{y}) + (\dot{x}-a)(\dot{y}-b)p_2(\dot{x},\dot{y}) + (\dot{y}-b)^2 p_3(\dot{x},\dot{y})$$

for suitable polynomials $p_i(\dot{x},\dot{y})$, $i = 1,2,3$.

In the following paragraphs we shall discuss how to evaluate a function $\varphi \in K(C_f)$ at a point (a,b) of C_f. Note that for some $p(x,y) \in K[C_f]$ the evaluation $g(a,b)$ does not depend on the representative of $p(x,y)$ since $f(a,b) = 0$. For polynomials $g(\dot{x},\dot{y}), h(\dot{x},\dot{y})$ the formulation "$g(\dot{x},\dot{y})/h(\dot{x},\dot{y})$ is a representative of φ" means $\varphi = g(x,y)/h(x,y)$ in $K(C_f)$. Given a point (a,b) of the curve, such a quotient will have one of the three types:

(I) $h(a,b) \neq 0$

(II) $h(a,b) = 0$ and $g(a,b) \neq 0$

(III) $g(a,b) = h(a,b) = 0$

In case (I) we would like to say that φ has a value at (a,b). Case (II) should indicate a pole. It is allways possible to construct representatives of type (III) but they cannot be used to determine a value or a pole so we would like to avoid them. The following proposition shows that this intuitions are right. In Section 3.7 we will see that it is possible to avoid case (III) if the point (a,b) is regular.

Proposition 3.6.2. *Let C_f be an affine algebraic curve, (a, b) a point on the curve and $\varphi \in K(C_f)$ a function. Then the following properties hold*

- *It is impossible that φ has a representative of type* (I) *and type* (II).
- *If $g(\dot{x}, \dot{y})/h(\dot{x}, \dot{y})$ and $\hat{g}(\dot{x}, \dot{y})/\hat{h}(\dot{x}, \dot{y})$ are representatives of φ if type* (I) *then*

$$\frac{g(a,b)}{h(a,b)} = \frac{\hat{g}(a,b)}{\hat{h}(a,b)}.$$

  In this case we write $\varphi(a, b)$ for this value.

Proof.

- Assume $g(\dot{x}, \dot{y})/h(\dot{x}, \dot{y})$ is a representative of type (I) and $\hat{g}(\dot{x}, \dot{y})/\hat{h}(\dot{x}, \dot{y})$ is a representative of type (II). Then $f(\dot{x}, \dot{y})$ divides $g(\dot{x}, \dot{y})\hat{h}(\dot{x}, \dot{y}) - \hat{g}(\dot{x}, \dot{y})h(\dot{x}, \dot{y})$ and hence (a, b) is a zero of this difference. This yields

$$0 = g(a,b)\overbrace{\hat{h}(a,b)}^{=0} - \hat{g}(a,b)h(a,b) = -\hat{g}(a,b)h(a,b)$$

  contradicting $h(a, b), \hat{g}(a, b) \neq 0$ which holds by our assumption.

- The argument of the last point shows

$$g(a,b)\hat{h}(a,b) = \hat{g}(a,b)h(a,b)$$

  which proofs the claim.

□

Remark. It is possible to generalise these notions to polynomials $g(\dot{x_1}, \ldots, \dot{x_n})$ and points $(a_1, \ldots, a_n)$ for an arbitrary $n \geq 2$. Proposition 3.6.2 can be adapted in the obvious way.

Let us now turn to the case of a projective curve C_F. We would like to evaluate a function $\Phi \in K(C_F)$ at a point $(a_0 : a_1 : a_2)$ of the curve. Φ is given by a representative $G(\dot{X}, \dot{Y}, \dot{Z})/H(\dot{X}, \dot{Y}, \dot{Z})$ with homogeneous polynomials satisfying $\deg(G) = \deg(H) = d$ and $F \nmid H$. If $(a_0 : a_1 : a_2)$ is not a zero of H then the evaluation of G/H does not depend on the representative of $(a_0 : a_1 : a_2)$ because

$$\frac{G(\lambda a_0, \lambda a_1, \lambda a_2)}{H(\lambda a_0, \lambda a_1, \lambda a_2)} = \frac{\lambda^d G(a_0, a_1, a_2)}{\lambda^d H(a_0, a_1, a_2)} = \frac{G(a_0, a_1, a_2)}{H(a_0, a_1, a_2)}$$

for an arbitrary $\lambda \in \overline{K}^\times$ As above we can distiguish the cases:

(I) $H(a_0, a_1, a_2) \neq 0$

(II) $H(a_0, a_1, a_2) = 0$ and $G(a_0, a_1, a_2) \neq 0$

(III) $G(a_0, a_1, a_2) = H(a_0, a_1, a_2) = 0$.

If $(a_0 : a_1 : a_2)$ is not singular, together with the results from the next section we will see: Φ has either a representative of type (I) or of type (II). If $G(\dot{X}, \dot{Y}, \dot{Z})/H(\dot{X}, \dot{Y}, \dot{Z})$ is a representative of type (I) then we can define the value of Φ at $(a_0 : a_1 : a_2)$ as $G(a_0, a_1, a_2)/H(a_0, a_1, a_2)$. In the second case we define Φ to have a pole at $(a_0 : a_1 : a_2)$.

Remark. We saw that if $f(\dot{x}, \dot{y})$ is absolutely irreducible and $F(\dot{X}, \dot{Y}, \dot{Z})$ is its homogeneous counterpart then C_f is embedded in C_F via $(a_1, a_2) \mapsto (a_1 : a_2 : 1)$. Consider the isomorphism between $K(C_f)$ and $K(C_F)$ described in Proposition 3.5.4. Let $\varphi \in K(C_f)$ with the representative $g(\dot{x}, \dot{y})$ then its image Φ under the isomorphism has the representative as in (3.3). Therefore we see that (a_1, a_2) is a pole of φ if and only if $(a_1 : a_2 : 1)$ is a pole of Φ. If this is not the case, evaluating (a_1, a_2) at φ gives the same result as evaluating $(a_1 : a_2 : 1)$ at Φ:

$$\varphi(a_1, a_2) = \frac{g(a_1, a_2)}{h(a_1, a_2)} = \frac{G(a_1, a_2, 1)}{H(a_1, a_2, 1)} = \Phi((a_1 : a_2 : 1))$$

This shows that the interpretation of the function field $K(C_f)$ as "rational functions on C_f" extends naturally to $K(C_F)$. We may think of the elements of $K(C_F)$ as the rational functions on a projective curve.

3.7 Places and Points

Let $C_f \colon f(\dot{x}, \dot{y}) = 0$ be an affine algebraic curve. Every point (a, b) of the curve leads to a subring

$$\mathcal{O}_{(a,b)} = \left\{ \frac{g(x,y)}{h(x,y)} \middle| g(x,y), h(x,y) \in K[C_f],\, h(a,b) \neq 0 \right\}.$$

of $K(C_f)$. It is called the *local ring of* (a, b) . We shall see below that this ring has a unique maximal ideal. More generally, commutative rings with a unique

maximal ideal are called *local rings* . A quotient $g(x,y)/h(x,y) \in \mathcal{O}_{(a,b)}$ is invertible in this ring if and only if $g(a,b) \neq 0$. Thus the set of elements not invertible in $\mathcal{O}_{(a,b)}$ is given by

$$\mathcal{P}_{(a,b)} = \left\{ \frac{g(x,y)}{h(x,y)} \middle| g(x,y), h(x,y) \in K[C_f],\, g(a,b) = 0, h(a,b) \neq 0 \right\}.$$

Obviously $\mathcal{P}_{(a,b)}$ is an ideal of $\mathcal{O}_{(a,b)}$. Since proper ideals do not contain invertible elements, any proper ideal is a subset of $\mathcal{P}_{(a,b)}$, i.e. $\mathcal{P}_{(a,b)}$ is the unique maximal ideal of $\mathcal{O}_{(a,b)}$. It is possible to show that (a,b) is a regular point if and only if $\mathcal{O}_{(a,b)}$ is a valuation ring of $K(C_f)$. We shall prove this result in the case where (a,b) is a rational point. To do so we have to consider Noetherian rings:

Definition 3.7.1. Let R be an integral domain. R is called Notherian if for every ascending chain $I_1 \subseteq I_2 \subseteq \ldots$ of ideals there is an integer n such that $I_n = I_{n+1} = \ldots$

We are interested in Noetherian rings because of the following property: Assume R is a Noetherian ring and $t \in R$ is not invertible. For each $r \in R \setminus \{0\}$ there is a maximal $n \in \mathbb{N}$ such that $t^n | r$. Since otherwise $\ldots | \frac{r}{t^2} | \frac{r}{t} | r$ and thus $(r) \subsetneq (\frac{r}{t}) \subsetneq (\frac{r}{t^2}) \subsetneq \ldots$, contradicting the assumption. The following facts about Noetherian rings are not hard to proof. See e.g. [17]

- A ring is Noetherian if and only if every ideal is finitely generated.
- Homomorphic images (and hence factor rings) of Noetherian rings are Noetherian.
- If R is a Noetherian ring, $S \subseteq R \setminus \{0\}$ is closed under multiplication then the localisation $RS^{-1} := \{\frac{r}{s} \colon r \in R, s \in S\}$ is a Noetherian ring.

The proofs of the results from Lemma 3.7.2 to Corollary 3.7.8 go back to [11, Chapter 14].

Lemma 3.7.2. *Let (a,b) be an arbitrary point of the algebraic curve C_f then the local ring $\mathcal{O}_{(a,b)}$ is a Noetherian ring.*

Proof. $K[\dot{x},\dot{y}]$ is a Noetherian ring by Hilbert's Basis Theorem. Therefore $K[C_f] = K[\dot{x},\dot{y}]/f(\dot{x},\dot{y})$ is a Noetherian ring. Set $S := \{g(x,y) \in K[C_f] \colon g(a,b) \neq 0\}$ then $\mathcal{O}_{(a,b)}$ is isomorphic to the localisation $K[C_f]S^{-1}$. Thus $\mathcal{O}_{(a,b)}$ is a Noetherian ring. □

Lemma 3.7.3. *If (a,b) is a rational point of C_f, $f_{\dot{y}}(a,b) \neq 0$ then $\mathcal{P}_{(a,b)} = (x-a)\mathcal{O}_{(a,b)}$.*

Proof. The inclusion $(x-a)\mathcal{O}_{(a,b)} \subseteq \mathcal{P}_{(a,b)}$ is obvious. For the converse we will first show $(y-b)/(x-a) \in \mathcal{O}_{(a,b)}$ from which the rest will easily follow. By Lemma 3.6.1 we have the following expansion of $f(\dot{x},\dot{y})$:

$$f(\dot{x},\dot{y}) = \underbrace{f(a,b)}_{=0} + f_{\dot{y}}(a,b)(\dot{y}-b) + (\dot{x}-a)f_1(\dot{x},\dot{y}) + (\dot{y}-b)^2 f_2(\dot{x},\dot{y}).$$

By calculating modulo $f(\dot{x},\dot{y})$ and rearranging terms we obtain

$$\begin{aligned} 0 &= f_{\dot{y}}(a,b)(y-b) + (x-a)f_1(x,y) + (y-b)^2 f_2(x,y) \\ \frac{y-b}{x-a} &= \frac{f_1(x,y)}{-f_{\dot{y}}(a,b) - (y-b)f_2(x,y)}. \end{aligned}$$

Since the denominator of the right hand is non-zero at (a,b) this proves the claim. Now take some $\varphi \in \mathcal{P}_{(a,b)}$, $\varphi \neq 0$. Then $\varphi = g(x,y)/h(x,y)$, for polynomials $g(\dot{x},\dot{y}), h(\dot{x},\dot{y})$ with $g(a,b) = 0, h(a,b) \neq 0$. Write

$$g(x,y) = (x-a)g_1(x,y) + (y-b)g_2(x,y)$$

then $g(x,y)/(x-a) = g_1(x,y) + (y-b)/(x-a)g_2(x,y) \in \mathcal{O}_{(a,b)}$ and so $g(x,y) \in (x-a)\mathcal{O}_{(a,b)}$. Since $1/h(x,y) \in \mathcal{O}_{(a,b)}$ we have $\varphi \in (x-a)\mathcal{O}_{(a,b)}$ which concludes the proof. □

Proposition 3.7.4. *Let $C_f\colon f(\dot{x},\dot{y}) = 0$ be an algebraic curve and suppose (a,b) is a regular, rational point of C_f. Then $\mathcal{O}_{(a,b)}$ is a valuation ring of $K(C_f)/K$.*

Proof. Obviously $K \subsetneq \mathcal{O}_{(a,b)} \subsetneq K(C_f)$. Wlog assume that $f_{\dot{y}}(a,b) \neq 0$. Then we saw that $\mathcal{P}_{(a,b)}$ is a principal ideal with generator $(x-a)$. Take arbitrary elements $g(x,y), h(x,y) \in K[C_f]$. Since $\mathcal{O}_{(a,b)}$ is a Noetherian ring we can write $g(x,y) = (x-a)^m\varphi(x,y)$, $h(x,y) = (x-a)^n\psi(x,y)$, with $\varphi(x,y) = \varphi_1(x,y)/\varphi_2(x,y)$, $\psi(x,y) = \psi_1(x,y)/\psi_2(x,y)$ with polynomials φ_i, ψ_i such that $\varphi, \psi \in \mathcal{O}_{(a,b)}$ and $m,n \in N$ are maximal. We have $\varphi_1(a,b) \neq 0$, since otherwise $\varphi_1(x,y) = (x-a)\varphi_1'(x,y)$ for some $\varphi_1' \in \mathcal{O}_{(a,b)}$, which contradicts the choice of m. For the same reason $\psi_1(a,b) \neq 0$ and so $g(x,y)/h(x,y) = (x-a)^{m-n}(\varphi_1(x,y)\psi_2(x,y))/(\varphi_2(x,y)\psi_1(x,y))$. If $m \geq n$ this is an element of $\mathcal{O}_{(a,b)}$ and if $m < n$ we see that $h(x,y)/g(x,y) \in \mathcal{O}_{(a,b)}$. □

Remark. Proposition 3.7.4 is also true if we do not assume (a,b) to be a rational point. In this case the proof requires techniques from commutative algebra and gets much more involved. For this more general case see e.g. [10, Section 3.1] which in turn uses results from [4, Chapter 10]

In general these are not all valuation rings of $K(C_f)$. The function field $K(\dot{x})/K$ may be interpreted as the function field of the curve $\dot{y} = 0$. Assume that K is algebraically closed. As we have seen in Chapter 1 the places of $K(\dot{x})/K \cong K(C_{\dot{y}})/K$ are $\mathcal{P}_a$, $a \in K$, and $\mathcal{P}_\infty$. The places $\mathcal{P}_a$ are in one to one correspondence to the points $(a, 0)$ of $C_{\dot{y}}$, but there is no affine point corresponding to $\mathcal{P}_\infty$. Below we shall characterise those places of $K(C_f)$ corresponding to points of the affine algebraic curve. After that we can use these results to see how every place corresponds to a point on the projective closure of C_f.

Lemma 3.7.5. *Let L/K be a field extension, $\alpha, \beta \in L$. Then $K[\alpha, \beta]$ is a field if and only if α and β are algebraic over K.*

Proof. If α and β are algebraic over K then $K[\alpha]$ is a field and β is algebraic over $K[\alpha]$. Hence $K[\alpha, \beta] = K[\alpha][\beta]$ is a field. Conversely, assume that $K[\alpha, \beta]$ is a field. $K(\alpha)$ is a subfield and since $K(\alpha)[\beta] = K[\alpha, \beta]$, β is algebraic over $K(\alpha)$. If we assume that α is not algebraic over K then $K[\alpha, \beta]/K$ is an algebraic function field. In Chapter 1 we saw that any function field has infinitely many places. Further there are only finitely many places of $K[\alpha, \beta]/K$ that are poles of α or β. So there is some valuation ring $\mathcal{O}$ such that $\alpha, \beta \in \mathcal{O}$. Therefore we have $K[\alpha, \beta] \subseteq \mathcal{O}$ and thus $K[\alpha, \beta] = \mathcal{O}$. But this is a contradiction since valuation rings are proper subrings of their function field. □

Lemma 3.7.6. *Let C_f be an affine algebraic curve, (a, b) a point of C_f. Consider the evaluation map*

$$\Psi_{(a,b)} \colon \begin{cases} K[C_f] \to K[a, b] \\ g(x, y) \mapsto g(a, b) \end{cases} .$$

Then $\ker \Psi_{(a,b)}$ is a maximal ideal of $K[C_f]$. Any maximal ideal of $K[C_f]$ is of this kind.

Proof. Both a and b are algebraic over K, so $K[a, b]$ is a field. Since

$$K[C_f]/\ker \Psi_{(a,b)} \cong K[a, b],$$

$\ker \Psi_{(a,b)}$ must be a maximal ideal.

Conversely, assume that $I \lhd K[C_f]$ is maximal. Then $L := K[C_f]/I$ is a field and $L = K[\alpha, \beta]$ if we set $\alpha = x + I$, $\beta = y + I$. So by the previous lemma α and β are algebraic over K. There is a subfield L' of $\overline{K}$ isomorphic to L. Denote by $\psi \colon L \to L'$ an isomorphism that fixes K and set $a := \psi(\alpha), b := \psi(\beta)$, then $L' = K[a, b]$. We have $g(x, y) \in I$ if and only

if $g(\alpha, \beta) = 0$ which is equivalent to $g(a, b) = 0$. This shows $I = \ker \Psi_{(a,b)}$. Since $f(\alpha, \beta) = f(x, y) + I = 0 + I$ we see that $f(a, b) = 0$ and thus (a, b) is a point of C_f. □

Lemma 3.7.7. *Let C_f be an affine algebraic curve and $\mathcal{O}$ be a valuation ring of $K(C_f)$, such that $K[C_f] \subseteq \mathcal{O}$. Denote by $\mathcal{P}$ the place of $\mathcal{O}$. Then $\mathcal{P} \cap K[C_f]$ is a maximal ideal of $K[C_f]$.*

Proof. Note that $K \subseteq K[C_f]$ and $K \cap \mathcal{P} = \{0\}$. For $g(x, y) \in K[C_f]$ consider the map

$$\begin{cases} K[C_f]/\mathcal{P} \cap K[C_f] \to \mathcal{O}/\mathcal{P} \\ g(x, y) + \mathcal{P} \cap K[C_f] \mapsto g(x, y) + \mathcal{P} \end{cases}.$$

It is easily seen to be well-defined, injective and a ring homomorphism that fixes K. Thus up to isomorphy we have $K \subseteq K[C_f]/\mathcal{P} \cap K[C_f] \subseteq \mathcal{O}/\mathcal{P}$. In Corollary 1.3.3 we saw $[\mathcal{O}/\mathcal{P} : K] < \infty$. Hence $K[C_f]/\mathcal{P} \cap K[C_f] = K[\alpha_1, \ldots, \alpha_n]$ for elements $\alpha_i \in \mathcal{O}/\mathcal{P}$ that are algebraic over K. This shows that $K[C_f]/\mathcal{P} \cap K[C_f]$ is a field and hence $\mathcal{P} \cap K[C_f]$ is a maximal ideal in $K[C_f]$. □

The following corollary shows that every valuation ring of $K(C_f)$ that contains $K[C_f]$ is the local ring of some point:

Corollary 3.7.8. *Let C_f be an affine algebraic curve and $\mathcal{O}$ be a valuation ring of $K(C_f)$ with the property $K[C_f] \subseteq \mathcal{O}$. Then there is a point (a, b) of C_f such that $\mathcal{O} = \mathcal{O}_{(a,b)}$.*

Proof. Denote by $\mathcal{P}$ the place of $\mathcal{O}$. By the above lemma, $\mathcal{P} \cap K[C_f]$ is a maximal ideal of $K[C_f]$. By Lemma 3.7.6 there exists a point $(a, b) \in C_f$ such that $g(x, y) \in \mathcal{P} \cap K[C_f]$ if and only if $g(a, b) = 0$. We can now show that $\mathcal{O}_{(a,b)} \subseteq \mathcal{O}$: Take an element $g(x, y)/h(x, y) \in \mathcal{O}_{(a,b)}$. Then $h(a, b) \neq 0$, so $h(x, y) \notin \mathcal{P} \cap C[K_f]$ which implies that $h(x, y) \notin \mathcal{P}$. Therefore $1/h(x, y) \in \mathcal{O}$ and since $K[C_f] \subseteq \mathcal{O}$ we conclude $g(x, y)/h(x, y) \in \mathcal{O}$. By Lemma 1.3.9 valuation rings are maximal subrings of $K(C_f)$ which shows $\mathcal{O}_{(a,b)} = \mathcal{O}$. □

Remark. Obviously for any point $(a, b) \in C_f$ we have $K[C_f] \subseteq \mathcal{O}_{(a,b)}$. So the previous lemma characterises the valuations rings arising from points.

Analogous to the case of affine points every point $(a_0 : a_1 : a_2)$ of a projective curve C_F leads to the set

$$\mathcal{O}_{(a_0:a_1:a_2)} := \left\{ \frac{G(X, Y, Z)}{H(X, Y, Z)} \in K(C_F) \middle| H((a_0 : a_1 : a_2)) \neq 0 \right\} \subseteq K(C_F).$$

$\mathcal{O}_{(a_0:a_1:a_2)}$ is easily seen to be a subring of $K(C_F)$. If $(a_0 : a_1 : a_2)$ is non-singular then an arbitrary $\Phi \in K(C_F)$ has either a value at $(a_0 : a_1 : a_2)$ or a pole at $(a_0 : a_1 : a_2)$. In the first case $\Phi \in \mathcal{O}_{(a_0:a_1:a_2)}$ and in the second case $\Phi^{-1} \in \mathcal{O}_{(a_0:a_1:a_2)}$. In other words, if the point is non-singular then $\mathcal{O}_{(a_0:a_1:a_2)}$ is a valuation ring of $K(C_F)$. In this case Φ is not invertible in $\mathcal{O}_{(a_0:a_1:a_2)}$ if and only if it has a zero at $(a_0 : a_1 : a_2)$. Therefore, the place of this valuation ring is given by

$$\mathcal{P}_{(a_0:a_1:a_2)} = \left\{ \frac{G(X,Y,Z)}{H(X,Y,Z)} \in \mathcal{O}_{(a_0:a_1:a_2)} \middle| G((a_0 : a_1 : a_2)) = 0 \right\}.$$

Definition 3.7.9. Two points (a_1, a_2), (b_1, b_2) in $\mathbb{A}^2_{\overline{K}}$ are called *conjugated* if $g(a_1, a_2) = 0 \Leftrightarrow g(b_1, b_2) = 0$ for all $g(\dot{x}, \dot{y}) \in \overline{K}[\dot{x}, \dot{y}]$. Similiarly two projective points $(a_0 : a_1 : a_2)$, $(b_0 : b_1 : b_2) \in \mathbb{P}^2_{\overline{K}}$ are said to be conjugated if $G(a_0, a_1, a_2) = 0 \Leftrightarrow G(b_0, b_1, b_2) = 0$ for all homogeneous $G(\dot{X}, \dot{Y}, \dot{Z}) \in K[\dot{X}, \dot{Y}, \dot{Z}]$.

It follows directly from the definition that if $A = (a_0 : a_1 : a_2)$ and $B = (b_0 : b_1 : b_2)$ are conjugated, A is a point of C_F if and only if B is a point of C_F. Further, A is non-singular if and only if B is non-singular. In this case they lead to the same valuation ring, i.e. $\mathcal{O}_A = \mathcal{O}_B$, and hence to the same place. If A and B are not conjugated they lead to different valuation rings. This can be seen as follows: Take a homogeneous polynomial $G(\dot{X}, \dot{Y}, \dot{Z})$ such that A is a zero and B is not a zero. Wlog we can assume that $a_2 \neq 0$. Then $Z^{\deg G}/G(X, Y, Z)$ is an element of $\mathcal{O}_B$ but not of $\mathcal{O}_A$. Similiar considerations show that two non-singular points (a, b), (a', b') of some affine algebraic curve C_f are conjugated if and only if $\mathcal{O}_{(a,b)} = \mathcal{O}_{(a',b')}$.

Proposition 3.7.10. *Let $F(\dot{X}, \dot{Y}, \dot{Z})$ be an absolutely irreducible, homogeneous polynomial and $K(C_F)$ the function field of the corresponding projective curve. If $\mathcal{O}$ is a valuation ring of $K(C_F)$ then there is a point $A = (a_0 : a_1 : a_2)$ of C_F such that $\mathcal{O} = \mathcal{O}_A$.*

Proof. Let C_2, C_1 and C_0 denote the affine components of C_F, described by the polynomials

$$\begin{aligned} C_2 &: f_2(\dot{x}, \dot{y}) := F(\dot{x}, \dot{y}, 1) = 0 \\ C_1 &: f_1(\dot{x}, \dot{z}) := F(\dot{x}, 1, \dot{z}) = 0 \\ C_0 &: f_0(\dot{y}, \dot{z}) := F(1, \dot{y}, \dot{z}) = 0. \end{aligned}$$

Proposition 3.5.4 states that the map

$$\Psi_2 \colon \begin{cases} K(C_F) \to K(C_2) \\ \frac{G(X,Y,Z)}{H(X,Y,Z)} \mapsto \frac{G(x,y,1)}{H(x,y,1)} \end{cases}$$

is an isomorphism between the function fields $K(C_F)/K$ and $K(C_2)/K$. For $i = 0, 1$, defining Ψ_i analogously (i.e. substituting $Y = 1$ for $i = 1$ and $X = 1$ for $i = 0$) we get isomorphisms as well.

We would like to show that $\Psi_i^{-1}(K[C_i]) \subseteq \mathcal{O}$ for at least one i. It is not hard to check that the preimage of $K[C_2]$ is given by

$$\Psi_2^{-1}(K[C_2]) = K[X/Z, Y/Z]$$

Similiarly $\Psi_i^{-1}(K[C_i])$ is given by $K[X/Y, Z/Y]$ for $i = 1$ and $K[Y/X, Z/X]$ in the case $i = 0$. Consider the three sets

$$\{X/Y, Y/X\}, \{X/Z, Z/X\}, \{Z/Y, Y/Z\}.$$

Since $\mathcal{O}$ is a valuation ring, for every set at least one of its elements is contained in $\mathcal{O}$. We distinguish between two cases: In the first case among these three elements of $\mathcal{O}$ there are two with the same denominator, wlog $Y/X, Z/X \in \mathcal{O}$. Hence we see that $\Psi_0^{-1}(K[C_0]) = K[Y/X, Z/X] \subseteq \mathcal{O}$, showing our claim. In the second case all three denominators are different, wlog $X/Y, Y/Z, Z/X \in \mathcal{O}$. But then even all six elements are in $\mathcal{O}$ and with the same argument as before $\Psi_i^{-1}(K[C_i]) \subseteq \mathcal{O}$ for some i. Since Ψ_i is an isomorphism, $\Psi_i(\mathcal{O})$ is a valuation ring of $K(C_i)$ containing $K[C_i]$. By Corollary 3.7.8 there exists a point (a, b) of C_i such that $\Psi_i(\mathcal{O}) = \mathcal{O}_{(a,b)}$. Wlog we may assume that $i = 2$. To conclude the proof set $A = (a : b : 1)$. Take $G(X, Y, Z)/H(X, Y, Z) \in \mathcal{O}_A$, i.e. $H(a, b, 1) \neq 0$. So

$$\Psi_2(G(X, Y, Z)/H(X, Y, Z)) = G(x, y, 1)/H(x, y, 1) \in \mathcal{O}_{(a,b)}.$$

This shows $\Psi_2(\mathcal{O}_A) \subseteq \mathcal{O}_{(a,b)} = \Psi_2(\mathcal{O})$. Since Ψ_2 is a bijection and valuation rings are maximal subrings of $K(C_F)$ this yields $\mathcal{O}_A = \mathcal{O}$. □

3.8 Function Fields over Perfect Fields

We will now discuss the situation of a ground field K that is assumed to be perfect . This covers a lot of important cases, namely fields of characterisic zero, algebraically closed fields and – most important for our purposes – finite fields. Therefore we cite some definitions and results from field theory, which can be found in any book about general algebra, e.g. [16]. K is called a *perfect field* if any irreducible polynomial $p(x) \in K[x]$ splits into distinct

linear factors in its splitting field L. We summarise some properties of these fields:

Lemma 3.8.1. *All fields with characteristic zero are perfect. If* $\operatorname{char} K = p > 0$ *then* K *is perfect if and only if every element of* K *has a* p*-th root in* K*.*

Corollary 3.8.2. *Finite fields and algebraically closed fields are perfect.*

The next lemma will be used in the proof of Proposition 3.8.4.

Lemma 3.8.3. *Let* K *be a field,* $h(\dot{x}) \in K[\dot{x}]$ *be irreducible and* $L \geq K$ *be a splitting field of* $h(\dot{x})$*. For given roots* $\alpha_1, \alpha_2 \in L$ *of* $h(\dot{x})$ *there is an automorphism of* L *which fixes* K *and maps* α_1 *to* α_2*.*

Let us again consider the function field $K(C_f)/K$ of an affine algebraic curve C_f. We can now prove that if the ground field K is perfect then the field of constants $\widetilde{K}$ of $K(C_f)/K$ is equal to K.

Proposition 3.8.4. *Let* K *be a perfect field,* C_f *an algebraic curve defined by some absolutely irreducible polynomial* $f(\dot{x}, \dot{y}) \in K[\dot{x}, \dot{y}]$ *and* $K(C_f)/K$ *the algebraic function field arising from* C_f*. Then* $\widetilde{K} = K$*.*

Proof. Assume that there is an element $\varphi(x, y) = \varphi_1(x, y)/\varphi_2(x, y) \in K(C_f)$ which is algebraic over K but not an element of K, where $\varphi_i(\dot{x}, \dot{y})$ are assumed to be polynomials. Let $h(\dot{x}) \in K[\dot{x}]$ be the minimal polynomial of $\varphi(x, y)$ over K and denote by $L \geq K$ a splitting field of $h(\dot{x})$. Then we have

$$h(\varphi(\dot{x}, \dot{y})) = \prod_{k=1}^{n} (\varphi(\dot{x}, \dot{y}) - \alpha_i) =$$

$$\frac{1}{\varphi_2^n(\dot{x}, \dot{y})} \prod_{k=1}^{n} (\varphi_1(\dot{x}, \dot{y}) - \alpha_i \varphi_2(\dot{x}, \dot{y}))$$

in $L(\dot{x}, \dot{y})$, where the α_i are the roots of $h(\dot{x})$. They are all distinct since K is a perfect field by assumption. Since $h(\varphi(x, y)) = 0$ in $K(C_f)$, $f(\dot{x}, \dot{y})$ devides the numerator of $h(\varphi(\dot{x}, \dot{y}))$. $f(\dot{x}, \dot{y})$ is absolutely irreducible and therefore prime since $L[\dot{x}, \dot{y}]$ is a factorial ring. Thus $f(\dot{x}, \dot{y})$ must divide one of the factors $\varphi_1(\dot{x}, \dot{y}) - \alpha_i \varphi_2(\dot{x}, \dot{y})$, say the first one. Note that $n \geq 2$ since $\varphi(x, y) \notin K$. There is an automorphism σ of L that fixes K and takes α_1 to $\alpha_2 \neq \alpha_1$. Since $\sigma(f(\dot{x}, \dot{y})) = f(\dot{x}, \dot{y})$ and $\sigma(\varphi_i(\dot{x}, \dot{y})) = \varphi_i(\dot{x}, \dot{y})$ we conclude that $f(\dot{x}, \dot{y})$ divides also $\varphi_1(\dot{x}, \dot{y}) - \alpha_2 \varphi_2(\dot{x}, \dot{y})$. Hence $f(\dot{x}, \dot{y})$ divides $(\alpha_1 - \alpha_2)\varphi_2(\dot{x}, \dot{y})$. Since $\varphi_2(x, y) \neq 0$ in $K(C_f)$, $f(\dot{x}, \dot{y})$ must divide the first factor, which is an element of $L^\times$. But this is a contradiction since this implies that $f(\dot{x}, \dot{y})$ is constant. □

Remark. In Chapter 2 the integer $\kappa = [\widetilde{K} : K]$ occured in Riemann's Theorem and the Riemann-Roch Theorem. For perfect fields, in particular finite fields, which is the relevant case for our purposes, $\kappa = 1$. Hence the Riemann-Roch Theorem simplifies to

$$\ell(\mathcal{D}) = \deg(\mathcal{D}) - g + 1 + \ell(\mathcal{W}\mathcal{D}^{-1})$$

for a given divisor $\mathcal{D}$ and a fixed canonical divisor $\mathcal{W}$.

Chapter 4

Goppa Codes

4.1 Error-correcting Codes

In the following paragraphs we will briefly outline some of the basics of error-correcting codes . For a more detailed introduction to this subject we refer to the introductory chapters of [18] and [9].

We assume that we want to transmit k-tuples $(a_1, \ldots, a_k)$ of elements of some finite alphabet A over a noisy channel . In this context, noisy means that errors occure at random positions. Thus the received word might be different from the original one. To be able to recover the original word from the transmitted word one needs to add redundant information. This is achieved by an encoding function $f_C \colon A^k \to A^n$ which is assumed to be injective. It turns the original data $(a_1, \ldots, a_k)$ into a longer message $(b_1, \ldots, b_n)$ which will be transmitted over the channel. Transmission may result in errors, thus a different word $(b'_1, \ldots, b'_n)$ may be received. The goal is to reconstruct $(b_1, \ldots, b_n)$ from $(b'_1, \ldots, b'_n)$ which then gives $(a_1, \ldots, a_k)$.

Most applications are based on the approach that A is some finite field $\mathbb{F}_q$. Thus $(a_1, \ldots, a_k)$ is an element of $\mathbb{F}_q^k$ and $(b_1, \ldots, b_n) \in \mathbb{F}_q^n$, respectively. The encoding function f_C is assumed to be a linear injection $\mathbb{F}_q^k \to \mathbb{F}_q^n$. $C := f_C(\mathbb{F}_q^k)$ is called a (linear) *code* . It is a k-dimensional subspace of $\mathbb{F}_q^n$. k is the *rank* and n is the *length* of the code. We consider the elements of $\mathbb{F}_q^n$ as row vectors. They are called *words* and the elements of C are the *code words* . This way, after encoding message a to code word c, the transmission process adds an error $e \in \mathbb{F}_q^n$ to the word $c \in C$ that we wish to decode, i.e. reconstruct c from the received word

$$f = c + e \in \mathbb{F}_q^n.$$

The number of non-zero entries in e is called the *weight* of e and it is denoted

by $w(e)$. The *Hamming distance* between two words f_1, f_2 is defined by $d(f_1, f_2) := w(f_1 - f_2)$. It is easy to see that d is a metric on $\mathbb{F}_q^n$. We will always use the *nearest neighbour decoding* . This means that if there is a unique code word with least distance to the received word the decoding process chooses this one. The minimum weight of a non-zero codeword,

$$d := \min\{w(c) \colon c \in C \setminus \{0\}\} = \min\{d(c_1, c_2) \colon c_1, c_2 \in C,\, c_1 \neq c_2\}$$

is called the *minimum distance* of C. If $2t + 1 \leq d$ or equivalently $t \leq \lfloor (d - 1)/2 \rfloor$ the nearest neighbour decoding is correct for errors e with $w(e) \leq t$. In this case C is said to be t-error-correcting . The most important parameters of the code C are the length n, the rank k and the minimum distance d. We say that $C \subseteq \mathbb{F}_q^n$ is a linear $[n, k, d]_q$-code or simply linear $[n, k, d]$-code if it is clear that C is a code over $\mathbb{F}_q$. The following bound is a standard and easy to prove result.

Lemma 4.1.1 (Singleton Bound)**.** *Let C be a linear $[n, k, d]$-code, then the following inequality holds:*

$$d + k \leq n + 1$$

If we choose a basis $c_1, \ldots, c_k$ of C and define a matix G by setting the i-th row of G to be c_i, we obtain what is called a *generator matrix* of C. If we set $c_i = f_C(e_i)$, where e_i is the i-th unit vector in $\mathbb{F}_q^k$, then $f_C(a) = a \cdot G$. When the code words are characterised by their first k positions it is possible to choose the c_i in a way such that

$$G = \left(I_k \,\middle|\, \widehat{G} \right)$$

where I_k denotes the $k \times k$-unit matrix and $\widehat{G}$ is an appropriate $k \times (n - k)$-matrix. If $f_C(a) = a \cdot G$ and G has this particular shape then the encoding is said to be *systematic* . Systematic encoding is useful since the original message can be obtained from the corresponding code word by projecting on the first k coordinates.

A *parity check matrix* is an $(n - k) \times n$-matrix H such that for $c \in \mathbb{F}_q^n$

$$c \in C \Longleftrightarrow c \cdot H^T = 0.$$

It is always possible to find a parity check matrix for a code C. In the case of systematic encoding it is particularly easy. If $G = (I_k | \widehat{G})$ as above then $H = (-\widehat{G}^T | I_{n-k})$ is a parity check matrix for C.

For words $b = (b_1, \ldots, b_n)$, $b' = (b'_1, \ldots, b'_n)$ let $b \cdot b' = \sum_{i=1}^{n} b_i b'_i$ denote the inner product. For any linear $[n, k, d]_q$-code C with generator matrix G the dual space

$$C^{\perp} := \left\{ b \in \mathbb{F}_q^n \colon b \cdot c = 0 \text{ for all } c \in C \right\}$$

is an $(n-k)$-dimensional code with G as a parity check matrix. $C^{\perp}$ is called the *dual code* of C . Since we are dealing with finite dimensional vector spaces we have $(C^{\perp})^{\perp} = C$.

4.2 Goppa Codes

From now on we consider algebraic function fields F/K with $K = \mathbb{F}_q$. Thus K is a perfect field and the results of Section 3.8 hold. In particular $K = \widetilde{K}$, i.e. any element of $F \setminus K$ is transcendental over K. Further, for the constant κ which occurs in Riemann's Theorem and the Riemann-Roch Theorem, we have $\kappa = 1$. First we will define dual Goppa codes (which are also called *Goppa function codes* in the literature).

Definition 4.2.1 (Dual Goppa Code)**.** Let $F/\mathbb{F}_q$ be an algebraic function field and $\mathcal{P}_1, \ldots, \mathcal{P}_n$ distinct places of degree one. Define $\mathcal{B} := \mathcal{P}_1 \cdot \ldots \cdot \mathcal{P}_n$ and let $\mathcal{D}$ be a divisor with $\operatorname{supp} \mathcal{D} \cap \operatorname{supp} \mathcal{B} = \varnothing$. Then the *dual Goppa code* $C_L(\mathcal{B}, \mathcal{D})$ is defined as the set of all vectors $(\varphi(\mathcal{P}_1), \ldots, \varphi(\mathcal{P}_n))$ where $\varphi \in \mathfrak{L}(\mathcal{D})$.

This definition makes sense, since φ has no pole at $\mathcal{P}_i$. $C_L(\mathcal{B}, \mathcal{D}) \subseteq \mathbb{F}_q^n$ since all $\mathcal{P}_i$ are assumed to be of degree one, i.e. they are rational places and therefore $\mathcal{O}_i/\mathcal{P}_i = K$. In Section 3.7 we saw that there is a one-to-one correspondence between points of the curve and places of its function field. So in the case where $\mathcal{P}_i$ corresponds to a finite[1] point (a, b) of the curve the evaluation $\varphi(\mathcal{P}_i)$ in the above definition is actually an evaluation of the form $\varphi(a, b)$. In Section 4.3.2 we give an example of such a construction. This way a Goppa code can be constructed from a curve if a basis of $\mathfrak{L}(\mathcal{D})$ is known. The following lemma summarises some basic properties of dual Goppa codes.

Theorem 4.2.2. *Let $\mathcal{B}, \mathcal{D}$ be divisors with the above properties, then the dual Goppa code $C_L(\mathcal{B}, \mathcal{D})$ is a linear $[n, k, d]$-code with the following properties:*

1.) $n = \deg(\mathcal{B})$

[1] If C is given by $f(\dot{x}, \dot{y}) = 0$ the finite points are the zeros of f, i.e. the points that do not require the projective closure of the curve.

2.) $k = \ell(\mathcal{D}) - \ell(\mathcal{D}\mathcal{B}^{-1})$

3.) $d \geq n - \deg(\mathcal{D})$

Proof. Since $C_L(\mathcal{B}, \mathcal{D})$ is the image of the linear map $ev\colon \mathfrak{L}(\mathcal{D}) \to \mathbb{F}_q^n\colon \varphi \mapsto (\varphi(\mathcal{P}_1), \ldots, \varphi(\mathcal{P}_n))$, it is a subspace of $\mathbb{F}_q^n$. *1.)* holds by definition. To prove *2.)* we need to determine the kernel of ev. Observe that $\varphi(\mathcal{P}_i) = 0$ if and only if $v_{\mathcal{P}_i}(\varphi) \geq 1$. Thus an element $\varphi \in \mathfrak{L}(D)$ is in the kernel of ev if and only if $v_{\mathcal{P}_i}(\varphi) \geq 1$ for all $i = 1, \ldots, n$. This is the case if and only if $\varphi \in \mathfrak{L}(\mathcal{D}\mathcal{B}^{-1})$. This yields $k = \dim(ev(\mathfrak{L}(\mathcal{D}))) = \dim(\mathfrak{L}(\mathcal{D})) - \dim(\ker ev) = \ell(\mathcal{D}) - \ell(\mathcal{D}\mathcal{B}^{-1})$.

To show the last statement take a non-zero element $(\varphi(\mathcal{P}_1), \ldots, \varphi(\mathcal{P}_n))$ of the code and denote by m the number of zeros in the code word. By Corollary 1.5.8 the number of poles is equal to the number of zeros if weighted with the degrees of the involved places. Using $v_{\mathcal{P}}(\varphi) \geq -v_{\mathcal{P}}(\mathcal{D})$ for all places gives

$$0 = \sum_{\mathcal{P} \in \mathfrak{P}} v_{\mathcal{P}}(\varphi) \deg(\mathcal{P}) = \sum_{\mathcal{P} \in \operatorname{supp} \mathcal{B}} v_{\mathcal{P}}(\varphi) \deg(\mathcal{P}) + \sum_{\mathcal{Q} \notin \operatorname{supp} \mathcal{B}} v_{\mathcal{Q}}(\varphi) \deg(\mathcal{Q}) \geq$$
$$m + \sum_{\mathcal{Q} \notin \operatorname{supp} \mathcal{B}} v_{\mathcal{Q}}(\varphi) \deg(\mathcal{Q}) \geq m - \sum_{\mathcal{Q} \notin \operatorname{supp} \mathcal{B}} v_{\mathcal{Q}}(\mathcal{D}) \deg(\mathcal{Q}) = m - \deg(\mathcal{D}).$$

So $n - m \geq n - \deg(\mathcal{D})$. Since $n - m$ is the number of non-zero entries in $ev(\varphi)$ the weight of an arbitrary non-zero codeword is at least $n - \deg(\mathcal{D})$. □

The most important case is $\deg(\mathcal{D}) < n$. From this $\deg(\mathcal{D}\mathcal{B}^{-1}) = \deg(\mathcal{D}) - n < 0$ follows, so $\mathfrak{L}(\mathcal{D}\mathcal{B}^{-1}) = \{0\}$, i.e. $k = \ell(\mathcal{D})$. Combining this with Riemann's Theorem gives

Corollary 4.2.3. *Let F be an algebraic function field over $\mathbb{F}_q$ of genus g, $C_L(\mathcal{B}, \mathcal{D})$ a dual Goppa code with parameters $[n, k, d]$. If $\deg(\mathcal{D}) < n$ then $k \geq \deg(\mathcal{D}) - g + 1$ and $d \geq n - \deg(\mathcal{D})$. In particular $n - g + 1 \leq k + d \leq n + 1$.*

Remark. If $g = 0$ this gives $k + d = n + 1$, hence in this case Goppa codes meet the Singleton bound. Codes with this property are called *maximum distance seperable codes*, or *MDS codes* for short.

Let us now turn to the definition of primary Goppa codes (also know as *Goppa residue codes*). They are a generalisation of the original family of codes introduced by Goppa in 1981. Most decoding algorithms are based on them. To define these codes recall the definition of repartitions, differentials and local components of differentials for an algebraic function field F/K from Sections 2.2 and 2.4:

- A repartition Γ is a map that assigns an element of F to each place $\mathcal{P} \in \mathfrak{P}$ and takes only finitely many distinct values. We identify $f \in F$ with the repartition that is constantly f. The order of Γ at $\mathcal{P}$ is by definition $v_{\mathcal{P}}(\Gamma_{\mathcal{P}})$. The set of all repartitions of F/K is denoted by R. For a divisor $\mathcal{D}$, $R(\mathcal{D}) \subseteq R$ is the analogue of the Riemann-Roch space in R.

- A differential $\omega\colon R \to K$ is a linear map that vanishes on $Y(\mathcal{D}) := R(\mathcal{D}) + F$ for some divisor $\mathcal{D}$. The set

$$\{\mathcal{D}\colon \mathcal{D} \text{ is a divisor, } \omega \text{ vanishes on } Y(\mathcal{D})\}$$

  has a greatest element, denoted by (ω) and called the divisor of ω.

- $\Omega(\mathcal{D})$ is the K-vector space of all differentials vanishing on $Y(\mathcal{D})$. The index of a divisor $\mathcal{D}$ is given by

$$j(\mathcal{D}) = \dim_K(R/Y(\mathcal{D})) = \dim_K(\Omega(\mathcal{D})) = \ell(\mathcal{D}) - \deg(\mathcal{D}) + g - 1$$

- For $f \in F$, by definition, $\iota_{\mathcal{P}}(f)$ is the repartition which is f at $\mathcal{P}$ and zero elsewhere. For a differential ω the local component is $\omega_{\mathcal{P}}(f) := \omega(\iota_{\mathcal{P}}(f)) \in K$, i.e. the local component is a functional $\omega_{\mathcal{P}}\colon F \to K$. For a repartition Γ we have

$$\omega(\Gamma) = \sum_{\mathcal{P} \in \mathfrak{P}} \omega_{\mathcal{P}}(\Gamma_{\mathcal{P}})$$

  by Proposition 2.4.2.

Definition 4.2.4 (Primary Goppa Codes)**.** Let $\mathcal{B} = \mathcal{P}_1 \cdots \mathcal{P}_n$ be a divisor where $\mathcal{P}_i$, $1 \leq i \leq n$, are distinct places of degree one and let $\mathcal{D}$ be a divisor with support disjoint from $\operatorname{supp} \mathcal{B}$. Then

$$C_\Omega(\mathcal{B}, \mathcal{D}) := \{(\omega_{\mathcal{P}_1}(1), \ldots, \omega_{\mathcal{P}_n}(1))\colon \omega \in \Omega(\mathcal{D}\mathcal{B}^{-1})\}$$

is called the *primary Goppa code* of $\mathcal{B}$ and $\mathcal{D}$.

Since the local components $\omega_{\mathcal{P}_i}$ are functionals $F \to \mathbb{F}_q$ the set defined above is indeed a subspace of $\mathbb{F}_q^n$. We shall see how to express the dimension of $C_\Omega(\mathcal{B}, \mathcal{D})$ in terms of the indices $j(\mathcal{D})$ and $j(\mathcal{D}\mathcal{B}^{-1})$.

Lemma 4.2.5. *The dimension of $C_\Omega(\mathcal{B}, \mathcal{D})$ is equal to $j(\mathcal{D}\mathcal{B}^{-1}) - j(\mathcal{D})$.*

Proof. Consider the map

$$\Psi\colon \begin{cases} \Omega(\mathcal{D}\mathcal{B}^{-1}) \to C_\Omega(\mathcal{B},\mathcal{D}) \\ \omega \mapsto (\omega_{\mathcal{P}_1}(1),\dots,\omega_{\mathcal{P}_n}(1)) \end{cases}$$

We would like to show $\ker\Psi = \Omega(\mathcal{D})$ from which the rest will follow easily. First we argue that for an arbitrary place $\mathcal{P}$ of degree one and a differential $\omega \neq 0$ with $v_\mathcal{P}(\omega) \geq -1$ we have $\omega_\mathcal{P}(1) = 0$ if and only if $v_\mathcal{P}(\omega) \geq 0$. Recall that by Lemma 2.4.3 for a number $r \in \mathbb{Z}$

$$v_\mathcal{P}(\omega) \geq r \Leftrightarrow \omega_\mathcal{P}(f) = 0 \text{ for all } f \in F \text{ with } v_\mathcal{P}(f) \geq -r. \tag{4.1}$$

Assume that $\omega_\mathcal{P}(1) = 0$. Take an arbitrary $f \in F$, $v_\mathcal{P}(f) \geq 0$. We may write $f = f(\mathcal{P}) + (f - f(\mathcal{P}))$, where $v_\mathcal{P}(f - f(\mathcal{P})) \geq 1$ and $v_\mathcal{P}(\omega) \geq -1$. So by (4.1) we have $\omega_\mathcal{P}(f - f(\mathcal{P})) = 0$ and therefore

$$\omega_\mathcal{P}(f) = \omega_\mathcal{P}(f(\mathcal{P})) = f(\mathcal{P})\omega_\mathcal{P}(1) = 0.$$

Using (4.1) again, this yields $v_\mathcal{P}(\omega) \geq 0$. Now assume that $v_\mathcal{P}(\omega) \geq 0$. Then $v_\mathcal{P}(1) = 0 \geq -v_\mathcal{P}(\omega)$ and hence $\omega_\mathcal{P}(1) = 0$.

From the definition of the divisor (ω) it follows easily that $\Omega(\mathcal{D}) = \{\omega \in \Omega\colon \mathcal{D} \leq (\omega)\}$. So for an element $\omega \in \Omega(\mathcal{D}\mathcal{B}^{-1})$ we have $\omega \in \Omega(\mathcal{D})$ if and only if $v_{\mathcal{P}_i}(\omega) \geq 0$ for $1 \leq i \leq n$. By the above argument this is equivalent to $w_{\mathcal{P}_1}(1) = \ldots = w_{\mathcal{P}_n}(1) = 0$, i.e. $\omega \in \ker\Psi$. Since Ψ is surjective our claim follows from

$$\dim C_\Omega(\mathcal{B},\mathcal{D}) = \dim\Omega(\mathcal{D}\mathcal{B}^{-1}) - \dim(\ker\Psi) = \\ \dim\Omega(\mathcal{D}\mathcal{B}^{-1}) - \dim\Omega(\mathcal{D}) = j(\mathcal{D}\mathcal{B}^{-1}) - j(\mathcal{D}).$$

□

Now we are able to prove the surprising result that the two kinds of Goppa codes introduced before are dual to each other. More precisely, $C_L(\mathcal{B},\mathcal{D})$ is the dual code of $C_\Omega(\mathcal{B},\mathcal{D})$, which explains the terminology.

Theorem 4.2.6. *Let $\mathcal{P}_1,\dots,\mathcal{P}_n$ be places of degree one, $\mathcal{B} := \mathcal{P}_1\cdots\mathcal{P}_n$ and let $\mathcal{D}$ be a divisor,* $\operatorname{supp}\mathcal{B} \cap \operatorname{supp}\mathcal{D} = \varnothing$. *Then $C_\Omega(\mathcal{B},\mathcal{D}) = C_L(\mathcal{B},\mathcal{D})^\perp$.*

Proof. We start by proving the following fact: Let $\mathcal{P}$ be a place of degree one, ω a differential with divisor $\mathcal{W} := (\omega)$, $f \in F$ such that $v_\mathcal{P}(\omega) = v_\mathcal{P}(\mathcal{W}) \geq -1$, $v_\mathcal{P}(f) \geq 0$, then

$$\omega_\mathcal{P}(f) = f(\mathcal{P})\omega_\mathcal{P}(1).$$

We have $v_{\mathcal{P}}(\iota_{\mathcal{P}}(f - f(\mathcal{P}))) = v_{\mathcal{P}}(f - f(\mathcal{P})) \geq 1 \geq -v_{\mathcal{P}}(\mathcal{W})$. For a place $\mathcal{Q} \neq \mathcal{P}$, by definition of $\iota_{\mathcal{P}}$, $v_{\mathcal{Q}}(\iota_{\mathcal{P}}(f - f(\mathcal{P}))) = v_{\mathcal{Q}}(0) = \infty \geq -v_{\mathcal{Q}}(\mathcal{W})$ and hence $\iota_{\mathcal{P}}(f - f(\mathcal{P})) \in Y(\mathcal{W})$. ω vanishes on $Y(\mathcal{W})$, thus $\omega(\iota_{\mathcal{P}}(f - f(\mathcal{P}))) = 0$ and so

$$\omega_{\mathcal{P}}(f) = \omega(\iota_{\mathcal{P}}(f)) = \omega(\iota_{\mathcal{P}}(f(\mathcal{P}) \cdot 1)) = f(\mathcal{P})\omega(\iota_{\mathcal{P}}(1)) = f(\mathcal{P})\omega_{\mathcal{P}}(1).$$

Next we show the inclusion $C_\Omega(\mathcal{B}, \mathcal{D}) \subseteq C_L(\mathcal{B}, \mathcal{D})^\perp$. Take some differential $\omega \in \Omega(\mathcal{D}\mathcal{B}^{-1})$ and some $\varphi \in \mathfrak{L}(\mathcal{D})$ and consider the scalar product of the corresponding code words:

$$(\omega_{\mathcal{P}_1}(1), \ldots, \omega_{\mathcal{P}_n}(1)) \cdot (\varphi(\mathcal{P}_1), \ldots, \varphi(\mathcal{P}_n)) = \sum_{i=1}^{n} \varphi(\mathcal{P}_i)\omega_{\mathcal{P}_i}(1) = \sum_{i=1}^{n} \omega_{\mathcal{P}_i}(\varphi) \overset{(1)}{=} \sum_{\mathcal{P} \in \mathfrak{P}} \omega_{\mathcal{P}}(\varphi) \overset{(2)}{=} \omega(\varphi) = 0.$$

The last equation follows since by definition differentials vanish on F. To justify (1) take an arbitrary place $\mathcal{Q} \notin \{\mathcal{P}_1, \ldots, \mathcal{P}_n\}$. $v_{\mathcal{Q}}(\iota_{\mathcal{Q}}(\varphi)) = v_{\mathcal{Q}}(\varphi) \geq -v_{\mathcal{Q}}(\mathcal{D}) = -v_{\mathcal{Q}}(\mathcal{D}\mathcal{B}^{-1})$. For places $\mathcal{Q}' \neq \mathcal{Q}$ we have $v_{\mathcal{Q}'}(\iota_{\mathcal{Q}}(\varphi)) = v_{\mathcal{Q}'}(0) = \infty$, so $\iota_{\mathcal{Q}}(\varphi) \in Y(\mathcal{D}\mathcal{B}^{-1})$. Thus $\omega_{\mathcal{Q}}(\varphi) = \omega(\iota_{\mathcal{Q}}(\varphi)) = 0$. (2) holds by Proposition 2.4.2.

Now, using Theorem 4.2.2, Lemma 4.2.5 and the facts about the index of a divisor we obtain

$$\begin{aligned}
\dim C_\Omega(\mathcal{B}, \mathcal{D}) = j(\mathcal{D}\mathcal{B}^{-1}) - j(\mathcal{D}) = \\
\big(\ell(\mathcal{D}\mathcal{B}^{-1}) - \deg(\mathcal{D}\mathcal{B}^{-1}) + g - 1\big) - (\ell(\mathcal{D}) - \deg(\mathcal{D}) + g - 1) = \\
\deg(\mathcal{B}) + \ell(\mathcal{D}\mathcal{B}^{-1}) - \ell(\mathcal{D}) = n - (\ell(\mathcal{D}) - \ell(\mathcal{D}\mathcal{B}^{-1})) = \\
n - \dim C_L(\mathcal{B}, \mathcal{D}) = \dim C_L(\mathcal{B}, \mathcal{D})^\perp.
\end{aligned}$$

This shows that indeed $C_\Omega(\mathcal{B}, \mathcal{D}) = C_L(\mathcal{B}, \mathcal{D})^\perp$. □

Let us consider the dual Goppa code $C_L(\mathcal{B}, \mathcal{D})$ with parameters $[n, k, d]$. Assume further $\deg(\mathcal{D}) < n$ such that $\varphi \mapsto (\varphi(\mathcal{P}_1), \ldots, \varphi(\mathcal{P}_n))$ is injective. If we have a basis $\varphi_1, \ldots, \varphi_k$ of $\mathfrak{L}(\mathcal{D})$ then

$$G_L := \begin{pmatrix} \varphi_1(\mathcal{P}_1) & \varphi_1(\mathcal{P}_2) & \cdots & \varphi_1(\mathcal{P}_n) \\ \varphi_2(\mathcal{P}_1) & \varphi_2(\mathcal{P}_2) & \cdots & \varphi_2(\mathcal{P}_n) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_k(\mathcal{P}_1) & \varphi_k(\mathcal{P}_2) & \cdots & \varphi_k(\mathcal{P}_n) \end{pmatrix}$$

is a generator matrix of $C_L(\mathcal{B}, \mathcal{D})$. Hence $H_\Omega := G_L$ is a parity check matrix for $C_\Omega(\mathcal{B}, \mathcal{D})$. The following lemma shows how the parameters of a primary Goppa code can be computed from $\mathcal{B}$, $\mathcal{D}$ and the genus of the function field.

Theorem 4.2.7. *Let F/K be an algebraic function field of genus g and let the primary Goppa code $C_\Omega(\mathcal{B},\mathcal{D})$ be defined as in 4.2.4. If $2g-2<\deg(\mathcal{D})$ then $C_\Omega(\mathcal{B},\mathcal{D})$ is a linear $[n,k,d]$-code with parameters*

1.) $n=\deg(\mathcal{B})$

2.) $k=n-\deg(\mathcal{D})+g-1+\ell(\mathcal{D}\mathcal{B}^{-1})$

3.) $d\geq\deg(\mathcal{D})-(2g-2)$.

Proof. *1.)* follows directly from the definition. To prove *2.)* note that the code is the dual code of $C_L(\mathcal{B},\mathcal{D})$, hence Theorem 4.2.2 gives $n-k=\dim C_L(\mathcal{B},\mathcal{D})=\ell(\mathcal{D})-\ell(\mathcal{D}\mathcal{B}^{-1})$. By Corollary 2.3.12 (a corollary of the Riemann-Roch Theorem) $\ell(\mathcal{D})=\deg(\mathcal{D})+1-g$ since $\deg(\mathcal{D})>2g-2$. Putting this together gives the desired equality. To show *3.)* let $c=(c_1,\ldots,c_n)\neq 0$ be a code word with m non-zero entries. Assume that m is less than $\deg(\mathcal{D})-(2g-2)$. By reordering the places $\mathcal{P}_i$ we can assume that $c_i\neq 0$ for $1\leq i\leq m$ and $c_i=0$ otherwise. Define divisors $\mathcal{B}_j$ by $\mathcal{B}_j:=\mathcal{P}_1\cdot\ldots\cdot\mathcal{P}_j$ where $1\leq j\leq m$. Then, by assumption, $\deg(\mathcal{D}\mathcal{B}_j^{-1})\geq\deg(\mathcal{D})-m>2g-2$. Using Corollary 2.3.12 again, we obtain $\ell(\mathcal{D}\mathcal{B}_j^{-1})=\deg(\mathcal{D})-j+1-g$. In particular $\mathfrak{L}(\mathcal{D}\mathcal{B}_m^{-1})\subsetneq\mathfrak{L}(\mathcal{D}\mathcal{B}_{m-1}^{-1})$. Thus we may pick a function φ lying in $\mathfrak{L}(\mathcal{D}\mathcal{B}_{m-1}^{-1})\setminus\mathfrak{L}(\mathcal{D}\mathcal{B}_m^{-1})$. Due to our choice $\varphi(\mathcal{P}_1)=\ldots=\varphi(\mathcal{P}_{m-1})=0$, $\varphi(\mathcal{P}_m)\neq 0$. But since $\varphi\in\mathfrak{L}(\mathcal{D})$ this gives

$$\sum_{i=1}^{n}c_i\varphi(\mathcal{P}_i)=c_m\varphi(\mathcal{P}_m)\neq 0$$

contradicting the fact that c lies in $C_\Omega(\mathcal{B},\mathcal{D})=C_L(\mathcal{B},\mathcal{D})^\perp$.

□

4.3 Examples of Goppa Codes

4.3.1 Reed-Solomon Codes

First we consider so called Reed-Solomon codes . We will see how to interpret them as Goppa codes. To do so, we identify the words $c=(c_0,c_1,\ldots,c_{n-1})\in\mathbb{F}_q^n$ with polynomials $c(\dot{x})=c_0+c_1\dot{x}+\ldots+c_{n-1}\dot{x}^{n-1}$ of degree less than n.

Definition 4.3.1 (Reed-Solomon Code)**.** For a prime power q consider the finite field $\mathbb{F}_q$. Let α be a primitive element of $\mathbb{F}_q$. Set $n:=q-1$, choose integers i,k such that $0<k\leq n$. Define $g(\dot{x}):=(\dot{x}-\alpha^i)(\dot{x}-\alpha^{i+1})\cdots(\dot{x}-\alpha^{i+n-k-1})$, then the set

$$C_{RS}(k,i) := \{c(\dot{x}) \in \mathbb{F}_q[\dot{x}] \colon \deg c(\dot{x}) < n, g(\dot{x}) | \, c(\dot{x})\}$$

interpreted as a subset of $\mathbb{F}_q^n$ is called *Reed-Solomon code*.

It is not hard to show that $C_{RS}(k,i)$ is a linear subspace of $\mathbb{F}_q^n$, i.e. a code in the sense of our definition. A polynomial $c(\dot{x})$ of degree less than n is an element of $C_{RS}(k,i)$ if and only if $c(\alpha^i) = c(\alpha^{i+1}) = \ldots = c(\alpha^{i+n-k-1}) = 0$. Thus, if we denote by V_n the space of polynomials in $\mathbb{F}_q[\dot{x}]$ of degree less than n and define

$$\psi \colon \begin{cases} V_n \to \mathbb{F}_q^{n-k} \\ c(\dot{x}) \mapsto (c(\alpha^i), c(\alpha^{i+1}), \ldots, c(\alpha^{i+n-k-1})) \end{cases}$$

we have $C_{RS}(k,i) = \ker \psi$ and hence $\dim C_{RS}(k,i) = \dim \ker \psi = n - \dim \mathbb{F}_q^{n-k} = k$. We used the fact that ψ is surjective, which can be seen by using Lagrange interpolation: Since $n-k \leq n$ there is a polynomial $c(\dot{x})$, $\deg c(\dot{x}) \leq n-1$ such that $c(\alpha^i) = b_0, \ldots, c(\alpha^{i+n-k-1}) = b_{n-k-1}$ for given elements $b_j \in \mathbb{F}_q$.

Now consider a polynomial $f(\dot{x})$ of degree $\deg f(\dot{x}) < k$ and the word $c := (f(\alpha), f(\alpha^2), \ldots, f(\alpha^n)) \in \mathbb{F}_q^n$. We would like to show that $c \in C_{RS}(k,1)$. Due to linearity it is sufficient to show this for $f(\dot{x}) = \dot{x}^j$, $0 \leq j < k$. Thus we substitute $\dot{x} = \alpha^\ell$, $1 \leq \ell \leq n-k$, into the polynomial $\alpha^j + \alpha^{2j}\dot{x} + \ldots + \alpha^{nj}\dot{x}^{n-1}$. This yields

$$\alpha^j + \alpha^{2j}\alpha^\ell + \ldots + \alpha^{nj}\alpha^{(n-1)\ell} =$$

$$\alpha^j(1 + \alpha^{j+\ell} + \ldots + \alpha^{(n-1)(j+\ell)}) = \alpha^j \frac{1 - \alpha^{n(j+\ell)}}{1 - \alpha^{j+\ell}} = 0$$

since $n = q-1$ is the order of $(\mathbb{F}_q^\times, \cdot)$ and therefore $\alpha^n = 1$. Note that $1 \leq j + \ell \leq n-1$ and hence $\alpha^{j+\ell} \neq 1$. Thus

$$\big\{(f(\alpha), f(\alpha^2), \ldots, f(\alpha^n)) \colon f(\dot{x}) \in \mathbb{F}_q[\dot{x}], \deg f(\dot{x}) < k\big\} \subseteq C_{RS}(k,1).$$

Since $k \leq n$, a polynomial in $V_k \subseteq V_n$ has less than n zeros. So $\varphi \colon V_k \to \mathbb{F}_q^n \colon f(\dot{x}) \mapsto (f(\alpha), \ldots, f(\alpha^n))$ is injective. Thus the above defined subspace of $C_{RS}(k,1)$ is of dimension k and hence $\varphi(V_k) = C_{RS}(k,1)$. Hence we found an alternative description of Reed-Solomon codes.

The curve $C \colon \dot{y} = 0$ may be identified with the affine line $\mathbb{A}^1_K$, $K = \mathbb{F}_q$. The associated function field $K(C)$ is naturally isomorphic to the field of rational functions $K(\dot{x})$. The rational places of $K(\dot{x})$ are of the form $\mathcal{P}_a$, $a \in K$ (the set of rational functions having a zero at a) and $\mathcal{P}_\infty$ (the set

of rational functions $g(\dot{x})/h(\dot{x})$ with $\deg g(\dot{x}) < \deg h(\dot{x})$), see Proposition 1.1.6 and the paragraph after Corollary 1.3.3. An element $f(\dot{x}) \in K(\dot{x})$ is a polynomial of degree less than k if and only if it has no poles except $\mathcal{P}_\infty$ and this pole is of degree less than k. Hence $C_{RS}(k,1)$ can be rewritten as

$$\{(f(\mathcal{P}_\alpha), f(\mathcal{P}_{\alpha^2}), \ldots, f(\mathcal{P}_{\alpha^n}))\colon f(\dot{x}) \in \mathfrak{L}((k-1)\mathcal{P}_\infty)\}$$

i.e. $C_{RS}(k,1) = C_L(\mathcal{B}, (k-1)\mathcal{P}_\infty)$ if we set $\mathcal{B} = \mathcal{P}_\alpha \mathcal{P}_{\alpha^2} \cdots \mathcal{P}_{\alpha^n}$. Since $K(\dot{x})$ is of genus 0, the remark after Corollary 4.2.3 shows that Reed-Solomon codes are MDS codes.

A drawback of Reed-Solomon codes is that their length n is determined by the size of the alphabet q. An advantage of Goppa codes lies in the fact that the possible code length only depends on the number of rational places of the function field $K(C)/K$.

4.3.2 A Concrete Example of a Goppa Code

In this section we would like to construct a concrete Goppa code from an algebraic curve and determine the parameters n, k and d. Therefore we need to choose a finite field $\mathbb{F}_q$, a curve $C_f\colon f(\dot{x}, \dot{y}) = 0$ as well as rational points of the curve that lead to the divisors $\mathcal{B}$ and $\mathcal{D}$. We will consider the curve $C_f\colon f(\dot{x}, \dot{y}) := \dot{x}^3 + \dot{x}\dot{y}^2 + \dot{x}\dot{y} + \dot{y} = 0$ over $\mathbb{F}_{16}$ and the projective closure C_F. We will denote the elements of $\mathbb{F}_{16}$ according to the following table

element	minimal polynomial in $\mathbb{F}_2$
$0, 1$	$x, x+1$
α_0, α_1	$x^2 + x + 1$
$\beta_0, \beta_1, \beta_2, \beta_3$	$x^4 + x + 1$
$\gamma_0, \gamma_1, \gamma_2, \gamma_3$	$x^4 + x^3 + 1$
$\delta_0, \delta_1, \delta_2, \delta_3$	$x^4 + x^3 + x^2 + x + 1$

where $\beta_i^{-1} = \gamma_i$, $\beta_0^{2^i} = \beta_i$, $\gamma_0^{2^i} = \gamma_i$ and $\delta_0^{2^i} = \delta_i$ holds for $0 \leq i \leq 3$. γ_0 is a primitive element of $\mathbb{F}_{16}$ and $\gamma_0^5 = \alpha_0$, $\gamma_0^{-1} = \beta_0$, $\gamma_0^3 = \delta_0$. All calculations in this section were done using [3].

Corollary 3.2.2 shows that $f(\dot{x}, \dot{y})$ is absolutely irreducible. The corresponding homogeneous polynomial is $F(\dot{X}, \dot{Y}, \dot{Z}) = \dot{X}^3 + \dot{X}\dot{Y}^2 + \dot{X}\dot{Y}\dot{Z} + \dot{Y}\dot{Z}^2$. It is not hard to show that the projective algebraic curve has no singular points, i.e. that there is no common zero of $F(\dot{X}, \dot{Y}, \dot{Z})$ and all its partial derivatives. Thus C_F is indeed a non-singular, projective algebraic curve and every rational point (i.e. a point with coefficients in $\mathbb{F}_{16}$) defines a place. The table below lists all rational points of C_F:

$$\left.\begin{array}{l}\left.\begin{array}{l}(0:0:1)\\(0:1:0)\\(1:1:0)\\(1:1:1)\end{array}\right\}\mathbb{F}_2\\ \left.\begin{array}{l}(\alpha_0:1:1),(\alpha_1:1:1)\\(\alpha_0:\alpha_1:1),(\alpha_1:\alpha_0:1)\end{array}\right\}\mathbb{F}_4\\ (\gamma_0:\alpha_1:1),(\gamma_1:\alpha_0:1),(\gamma_2:\alpha_1:1),(\gamma_3:\alpha_0:1)\\ (\gamma_0:\beta_3:1),(\gamma_1:\beta_0:1),(\gamma_2:\beta_1:1),(\gamma_3:\beta_2:1)\end{array}\right\}\mathbb{F}_{16}$$

The points are grouped in a way such that conjugated points are in the same line.

To define a Goppa code we make the following choice: We set $\mathcal{Q} := (0 : 0 : 1)$ and we write $\mathcal{P}_i$, $1 \leq i \leq 8$, for the eight points in the last two rows where the index i increases from left to right. For the places corresponding to these points we shall write $\mathcal{Q}$ and $\mathcal{P}_i$ as well. Set $\mathcal{B} := \mathcal{P}_1 \cdots \mathcal{P}_8$ and consider the codes $C_L(\mathcal{B}, j\mathcal{Q})$, $1 \leq j < 8$. $C_L(\mathcal{B}, j\mathcal{Q})$ consists of the words $(\varphi(\mathcal{P}_1), \ldots, \varphi(\mathcal{P}_8))$ where φ is an arbitrary function having a pole only at $\mathcal{Q}$ with order at most j. To calculate the genus of C_F we need the so called Plücker Formula (see e.g. [11, Chapter 14]). It allows us to calculate the genus of the function field of $K(C_F)/K$ from the degree of the defining polynomial.

Theorem 4.3.2 (Plücker Formula)**.** *Let C_F: $F(\dot{X}, \dot{Y}, \dot{Z}) = 0$ be a projective algebraic curve over an arbitrary field K with at least one K-rational point. If C_F has no singular points and n is the degree of $F(\dot{X}, \dot{Y}, \dot{Z})$, then the genus of $K(C_F)/K$ is equal to*

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

Thus in our case the genus is $g = 1$. Therefore we may use Theorem 4.2.7. Note that $\deg(j\mathcal{Q}) = j < 8 = \deg(\mathcal{B})$ and hence $\ell(j\mathcal{Q}\mathcal{B}^{-1}) = 0$. Thus we see that $C_\Omega(\mathcal{B}, j\mathcal{Q})$ is a linear $[n, k, d]$-code with $n = 8$, $k = 8 - j$ and $d \geq j$. By the Singleton bound $d \in \{j, j + 1\}$.

A basis of $\mathfrak{L}(j\mathcal{Q})$ will lead to a basis of $C_L(\mathcal{B}, j\mathcal{Q})$ since by assumption $\ell(j\mathcal{Q}\mathcal{B}^{-1}) = 0$ and therefore the evaluation map $\varphi \mapsto (\varphi(\mathcal{P}_1), \ldots, \varphi(\mathcal{P}_8))$ is injective (see the proof of Theorem 4.2.2). This in turn will enable us to construct a check matrix of $C_\Omega(\mathcal{B}, j\mathcal{Q})$. Since $\deg(j\mathcal{Q}) = j > 0 = 2g - 2$, Corollary 2.3.12 tells us $\ell(j\mathcal{Q}) = \deg(j\mathcal{Q}) = j$. To find a basis of this

Riemann-Roch space it will be sufficient to find a non-constant element $\varphi \in \mathfrak{L}(\mathcal{Q})$. $f_{\dot{y}}(0,0) = (\dot{x}+1)|_{(\dot{x},\dot{y})=(0,0)} = 1$, so by Lemma 3.7.3, x is a generator of $\mathcal{P}_{(0,0)}$ and thus $v_{\mathcal{Q}}(x) = 1$. To calculate $v_{\mathcal{Q}}(y)$ we use

$$y = x^3 \frac{y}{x^3} = x^3 \frac{y^4 + x^2y^2 + x^2y + xy + x^2 + 1}{(x+1)^3}.$$

This follows from $f(\dot{x},\dot{y})(\dot{x}^2\dot{y}^2 + \dot{x}^2\dot{y} + \dot{x}^2 + \dot{x}\dot{y} + 1) = \dot{x}^3(\dot{y}^4 + \dot{x}^2\dot{y}^2 + \dot{x}^2\dot{y} + \dot{x}\dot{y} + \dot{x}^2 + 1) - (\dot{x}+1)^3\dot{y}$. Note that the above equation holds only for elements of $K(C_f)$, i.e. we are calculating modulo $f(\dot{x},\dot{y})$. The quotient on the right hand side is invertible in $\mathcal{O}_{\mathcal{Q}}$, thus $v_{\mathcal{Q}}(y) = 3$. Set $\psi := (y(y+\gamma_0))/x^2$. Then we have

$$v_{\mathcal{Q}}(\psi) = v_{\mathcal{Q}}(y) + v_{\mathcal{Q}}(y+\gamma_0) - 2v_{\mathcal{Q}}(x) = 3 + 0 - 2 = 1,$$

i.e. ψ has a zero of order 1 at $\mathcal{Q}$. Obviously ψ has no other zeros among the points of C_f. The element in $K(C_F)$ corresponding to ψ is $(Y(Y+\gamma_0 Z))/X^2$. Neither $(0:1:0)$ nor $(1:1:0)$ are zeros of this function. Thus $\varphi := \psi^{-1}$ has only a pole at $\mathcal{Q}$ which is of order one, i.e. $\varphi \in \mathfrak{L}(Q)$. Set $\varphi_i := \varphi^i$, then $v_{\mathcal{Q}}(\varphi_i) = -i$ and so $\{\varphi_1, \ldots, \varphi_j\}$ is a basis of $\mathfrak{L}(j\mathcal{Q})$. The matrix $(\varphi_i(\mathcal{P}_k))_{1\le i\le j, 1\le k\le n}$ is equal to the first j rows of

$$\begin{pmatrix}
\gamma_2 & \alpha_1 & \alpha_1 & \beta_3 & \gamma_0 & \delta_2 & \gamma_3 & \beta_0 \\
\gamma_3 & \alpha_0 & \alpha_0 & \beta_0 & \gamma_1 & \delta_3 & \gamma_0 & \beta_1 \\
\delta_2 & 1 & 1 & \delta_1 & \delta_0 & \delta_1 & \delta_3 & \delta_2 \\
\gamma_0 & \alpha_1 & \alpha_1 & \beta_1 & \gamma_2 & \delta_0 & \gamma_1 & \beta_2 \\
\alpha_0 & \alpha_0 & \alpha_0 & \alpha_0 & \alpha_0 & 1 & \alpha_1 & \alpha_1 \\
\delta_3 & 1 & 1 & \delta_2 & \delta_1 & \delta_2 & \delta_0 & \delta_3 \\
\beta_1 & \alpha_1 & \alpha_1 & \gamma_2 & \beta_3 & \delta_3 & \beta_2 & \gamma_3
\end{pmatrix}.$$

It is a parity check matrix for $C_\Omega(\mathcal{B}, j\mathcal{Q})$.

Chapter 5

Decoding Algorithms for Goppa Codes

5.1 Basic Error Correction

In this section we will consider primary Goppa codes, introduced in Section 4.2. We will develop a decoding algorithm going back to Skorobogatov and Vlăduţ, 1990. It was one of the first decoding algorithms for Goppa codes and is capable of decoding up to $\lfloor (d-g-1)/2 \rfloor$ errors where d is the minimum distance and g is the genus of the involved function field. Note that this is in general less than the error correction capacity $\lfloor (d-1)/2 \rfloor$ of the code. Our describtion of error locators and the Skorobogatov-Vlăduţ algorithm follows [11, chapter 6]. We fix the following notation:

- $F/\mathbb{F}_q$ is an algebraic function field of genus g
- $\mathcal{P}_1, \ldots, \mathcal{P}_n$ are places of degree one of $F/\mathbb{F}_q$
- $\mathcal{B} := \mathcal{P}_1 \cdots \mathcal{P}_n$ and $\mathcal{D}$ is a divisor with support disjoint from that of $\mathcal{B}$
- $C_\Omega(\mathcal{B}, \mathcal{D})$ is the primary Goppa code defined by $\mathcal{B}$ and $\mathcal{D}$
- $\mathcal{C}, \mathcal{Y}, \mathcal{Z}$ are divisors with properties that will be specified during this section

We use the notation

$$\varphi \cdot f := \sum_{i=1}^{n} \varphi(\mathcal{P}_i) f_i$$

for an arbitrary element $\varphi \in F$ without poles at $\mathcal{P}_i$ and an element $f = (f_1, \ldots, f_n) \in \mathbb{F}_q^n$ and call this product the syndrom of f with respect to φ. If φ has a pole among the places $\mathcal{P}_i$ then define $\varphi \cdot f := \infty$ where ∞ is not an element of $\mathbb{F}_q$. In this notation

$$C_\Omega(\mathcal{B}, \mathcal{D}) = \{c \in \mathbb{F}_q^n \colon \varphi \cdot c = 0 \text{ for all } \varphi \in \mathfrak{L}(\mathcal{D})\}.$$

Definition 5.1.1 (Error Locator)**.** Let $e = (e_1, \ldots, e_n) \in \mathbb{F}_q^n$ be an error word. A place $\mathcal{P}_j$ is called *error location* of e if $e_j \neq 0$. An element $\theta \in F^\times$ which has no poles among the $\mathcal{P}_i$ and has the property that $\theta(\mathcal{P}_i) = 0$ whenever $e_i \neq 0$ is called an *error locator* of e. In other words, an error locator of e is a function θ that vanishes at the error locations of e and therefore satifies $\theta \cdot e = 0$.

Note that the definition of an error locator is based on a fixed sequence $\mathcal{P}_1, \ldots, \mathcal{P}_n$. In the following paragraphs we will

1.) prove the existence of an error locator for a given error word e under certain conditions (Lemma 5.1.2),

2.) see how to use an error locator of e to determine e_i whenever $e_i \neq 0$ (Proposition 5.1.4) and

3.) show how to construct an error locator from an error word (Proposition 5.1.5).

Lemma 5.1.2. *Let t be a positive integer, $e \in \mathbb{F}_q^n$ be an arbitrary error word with $w(e) \leq t$, $\mathcal{C}$ a divisor such that $\ell(\mathcal{C}) > t$. Then there is an error locator of e in $\mathfrak{L}(\mathcal{C})$.*

Proof. Let $M \subseteq \{1, \ldots, n\}$ be the set of indices j where $e_j \neq 0$ and choose a basis $\varphi_1, \ldots, \varphi_m$ of $\mathfrak{L}(\mathcal{C})$, i.e. $m = \ell(\mathcal{C})$. Consider the following linear system of equations:

$$\sum_{i=1}^{m} a_i \varphi_i(\mathcal{P}_j) = 0,\ j \in M$$

The system consists of at most t equations with $m > t$ unknowns. This certainly has a non-trivial solution $(a_1, \ldots, a_m) \in \mathbb{F}_q^m$, i.e. $a_i \neq 0$ for some index i. Define $\theta := \sum_{i=1}^m a_i \varphi_i$. Then $\theta \in \mathfrak{L}(\mathcal{C})$ and $\theta(\mathcal{P}_j) = 0$ for all $j \in M$, i.e. θ is an error locator of e in $\mathfrak{L}(\mathcal{C})$. □

The next lemma seems to be somewhat technical. It will be clear in the subsequent corollary why it is useful.

Lemma 5.1.3. *Let t, r be integers, $t, r \geq 0$. Assume there are divisors $\mathcal{C}$, $\mathcal{Z}$ with support disjoint from $\mathcal{B}$ such that*

- *$\mathcal{C}$ is positive,* $\deg(\mathcal{C}) \leq t + r$
- $\deg(\mathcal{Z}) \geq t + r + 2g - 1$.

Fix an element θ of $\mathfrak{L}(\mathcal{C})$. Let $e^{(1)}, e^{(2)}$ be words in $\mathbb{F}_q^n$ such that $w(e^{(i)}) \leq t$ and θ is an error locator for $e^{(i)}$, $i = 1, 2$. If $\varphi \cdot e^{(1)} = \varphi \cdot e^{(2)}$ for all $\varphi \in \mathfrak{L}(\mathcal{Z})$ then $e^{(1)} = e^{(2)}$.

Proof. Denote by N the set of those indices $j \in \{1, \ldots, n\}$ where $\theta(\mathcal{P}_j) = 0$. Suppose N contains more than $t + r$ elements. Then, by Theorem 1.5.7

$$\deg((\theta)_\infty^{-1}\mathcal{C}) = \underbrace{-\deg((\theta)_0)}_{<-(t+r)} + \underbrace{\deg(\mathcal{C})}_{\leq(t+r)} < 0.$$

So $(\theta)_\infty^{-1}\mathcal{C}$ has a negative exponent at some place $\mathcal{P}$, i.e.

$$v_{\mathcal{P}}((\theta)\mathcal{C}) = v_{\mathcal{P}}((\theta)_0(\theta)_\infty^{-1}\mathcal{C}) = v_{\mathcal{P}}((\theta)_\infty^{-1}\mathcal{C}) < 0$$

But this contradicts the assumption $\theta \in \mathfrak{L}(\mathcal{C})$. Thus N has at most $r + t$ elements. Since θ is an error locator for the $e^{(i)}$, it is an error locator for $e^{(1)} - e^{(2)}$ and so $w(e^{(1)} - e^{(2)}) \leq t + r$.

Since the indices of the error locations of the $e^{(i)}$ are in N we have

$$\varphi \cdot e^{(i)} = \sum_{j \in N} \varphi(\mathcal{P}_j) e_j^{(i)}$$

for all $\varphi \in F$ without poles among the $\mathcal{P}_j$, $j = 1, \ldots, n$ and $i = 1, 2$. In particular this is true for all $\varphi \in \mathfrak{L}(\mathcal{Z})$. Since $\varphi \cdot e^{(1)} = \varphi \cdot e^{(2)}$ for all $\varphi \in \mathfrak{L}(\mathcal{Z})$, $e^{(1)} - e^{(2)}$ is a codeword of $C_\Omega(\mathcal{B}, \mathcal{Z})$. Due to our assumption on $\mathcal{Z}$ we have $2g - 2 < \deg(\mathcal{Z})$, so Theorem 4.2.7 is applicable to $C_\Omega(\mathcal{B}, \mathcal{Z})$, hence this code has minimum distance $d \geq \deg(\mathcal{Z}) - (2g-2) \geq t+r+2g-1-(2g-2) = t+r+1$. Since $e^{(1)} - e^{(2)}$ has weight at most $t + r$ we conclude $e^{(1)} - e^{(2)} = 0$. □

We are now able to describe how to find the error word e, given the received word $f = c + e$ and an error locator for e:

Proposition 5.1.4. *Let $r, t \geq 0$ be integers and suppose $\mathcal{C}$ and $\mathcal{Z}$ are divisors with the properties stated in the previous lemma. Assume further that $\mathcal{Z} \leq \mathcal{D}$. Fix some basis $\varphi_1, \ldots, \varphi_s$ of $\mathfrak{L}(\mathcal{Z})$. Suppose $c \in C_\Omega(\mathcal{B}, \mathcal{D})$ such that $f = c + e$ is the received word and $\theta \in \mathfrak{L}(\mathcal{C})$ is an error locator of e, $w(e) \leq t$. Consider the linear system*

$$\sum_{j\in N} \varphi_i(\mathcal{P}_j)x_j = \varphi_i \cdot f, \quad 1 \le i \le s \tag{5.1}$$

where N is the set of $j \in \{1,\dots,n\}$ with $\theta(\mathcal{P}_j) = 0$. Then $x_j = e_j, j \in N$, is the unique solution of (5.1).

Proof. We have $\varphi_i \in \mathfrak{L}(\mathcal{Z}) \subseteq \mathfrak{L}(\mathcal{D})$ and $e_k = 0$ whenever $k \notin N$, so

$$\sum_{j\in N} \varphi_i(\mathcal{P}_j)e_j = \varphi_i \cdot e = \varphi_i \cdot f - \varphi_i \cdot c = \varphi_i \cdot f, 1 \le i \le s.$$

Assume $(x_j)_{j\in N}$ is another solution of (5.1). Set $e'_i = x_i$ if $i \in N$ and $e'_i = 0$ else. Then θ is an error locator of $e' := (e'_1,\dots,e'_n)$. Since $\varphi_i \cdot e' = \varphi_i \cdot f = \varphi_i \cdot e$ for all $1 \le i \le s$ we see that $\varphi \cdot e' = \varphi \cdot e$ for all $\varphi \in \mathfrak{L}(\mathcal{Z})$. This implies $e = e'$ by the above lemma, showing that $x_i = e_i$ for all $i \in N$. □

We will now see how to find an error locator under certain conditions.

Proposition 5.1.5. *Consider an error word e with $w(e) \le t$. Let $\mathcal{C}$ and $\mathcal{Y}$ be divisors with support disjoint from* $\operatorname{supp}\mathcal{B}$, $\deg(\mathcal{Y}) \ge t + 2g - 1$. *Choose bases $\psi_1,\dots,\psi_\ell \in \mathfrak{L}(\mathcal{C})$ and $\chi_1,\dots,\chi_m \in \mathfrak{L}(\mathcal{Y})$. Then the system*

$$\begin{pmatrix} \psi_1\chi_1 \cdot e & \psi_2\chi_1 \cdot e & \dots & \psi_\ell\chi_1 \cdot e \\ \psi_1\chi_2 \cdot e & \psi_2\chi_2 \cdot e & \dots & \psi_\ell\chi_2 \cdot e \\ \vdots & \vdots & \ddots & \vdots \\ \psi_1\chi_m \cdot e & \psi_2\chi_m \cdot e & \dots & \psi_\ell\chi_m \cdot e \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_\ell \end{pmatrix} = \vec{0} \tag{5.2}$$

has a non-trivial solution $(a_1,\dots,a_\ell)^T \in \mathbb{F}_q^\ell$ if and only if $\sum_{i=1}^{\ell} a_i\psi_i$ is an error locator of e in $\mathfrak{L}(\mathcal{C})$.

Proof. We shall first prove the following result: $\theta \in \mathfrak{L}(\mathcal{C})$ is an error locator of e if and only if $\theta\chi \cdot e = 0$ for all $\chi \in \mathfrak{L}(\mathcal{Y})$. From this the rest will follow easily. If θ is an error locator then $\theta(\mathcal{P}_i)e_i = 0$ for all $i \le n$, hence $\sum_{i=1}^{n} \theta(\mathcal{P}_i)\chi(\mathcal{P}_i)e_i = 0$ for an arbitrary $\chi \in \mathfrak{L}(\mathcal{Y})$. For the converse consider the vector $c := (\theta(\mathcal{P}_1)e_1,\dots,\theta(\mathcal{P}_n)e_n)$. By assumtion $c \in C_\Omega(\mathcal{B},\mathcal{Y})$ and by Theorem 4.2.7 this code has minimum distance $d \ge t+1$. Since $w(e) \le t$ the vector c has at most t non-zero entries. Therefore it is the null vector which means that θ is an error locator of e.

If $(a_1,\dots,a_\ell)^T$ is a non-trivial solution of (5.2) and $\theta := \sum_{i=1}^{\ell} a_i\psi_i$ then $\theta\chi_j \cdot e = 0$ for $1 \le j \le m$. So $\theta\chi \cdot e = 0$ for all $\chi \in \mathfrak{L}(\mathcal{Y})$. Therefore $\theta \in \mathfrak{L}(\mathcal{C})$ is an error locator for e.

Conversely, if $\theta \in \mathfrak{L}(\mathcal{C})$ is an error locator for e then $\theta = \sum_{i=1}^{\ell} a_i\psi_i$, $a_i \neq 0$ for at least one index i. It is easy to check that $\theta\chi_j \cdot e$ is equal to the j-th component of the matrix-vector-product in (5.2). Since $\theta\chi_j \cdot e = 0$, $(a_1, \ldots, a_\ell)^T$ is a non-trivial solution. □

Using the previous results from this section we can now describe a decoding procedure for the Goppa code $C_\Omega(\mathcal{B}, \mathcal{D})$ and a fixed $t \geq 0$. We assume that $\mathcal{D}$ has degree $\deg(\mathcal{D}) > 2g - 2$ such that $C_\Omega(\mathcal{B}, \mathcal{D})$ has parameters as in Theorem 4.2.7. We assume that a divisor $\mathcal{C}$ exists that has the following properties: $\mathcal{C}$ is positive, $\operatorname{supp}\mathcal{C} \cap \operatorname{supp}\mathcal{B} = \varnothing$, $\ell(\mathcal{C}) > t$, $\deg\mathcal{C} \leq \deg\mathcal{D} - 2g + 1 - t$ After describing the algorithm we shall give conditions under which such a divisor $\mathcal{C}$ exists.

Algorithm 5.1.6. *The following steps will be performed only once: Set* $\mathcal{Y} := \mathcal{D} \cdot \mathcal{C}^{-1}$ *and select bases* $\{\varphi_1, \ldots, \varphi_s\}$ *of* $\mathfrak{L}(\mathcal{D})$, $\{\psi_1, \ldots, \psi_\ell\}$ *of* $\mathfrak{L}(\mathcal{C})$ *and* $\{\chi_1, \ldots, \chi_m\}$ *of* $\mathfrak{L}(\mathcal{Y})$, *respectively.*

Input *A word* $f = c + e$, $c \in C_\Omega(\mathcal{B}, \mathcal{D})$, $w(e) \leq t$.
Output *The error* e.
Step 1 *Find a non-trivial solution of the system*

$$\begin{pmatrix} \psi_1\chi_1 \cdot f & \psi_2\chi_1 \cdot f & \ldots & \psi_\ell\chi_1 \cdot f \\ \psi_1\chi_2 \cdot f & \psi_2\chi_2 \cdot f & \ldots & \psi_\ell\chi_2 \cdot f \\ \vdots & \vdots & \ddots & \vdots \\ \psi_1\chi_m \cdot f & \psi_2\chi_m \cdot f & \ldots & \psi_\ell\chi_m \cdot f \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_\ell \end{pmatrix} = \vec{0}$$

and set $\theta := \sum_{i=1}^{\ell} a_i\psi_i$.
Step 2 *Define* $N := \{j \colon 1 \leq j \leq n, \theta(\mathcal{P}_j) = 0\}$ *and solve*

$$\sum_{j \in N} \varphi_i(\mathcal{P}_j)x_j = \varphi_i \cdot f, 1 \leq i \leq s.$$

Step 3 *Set* $e_j = x_j$ *if* $j \in N$ *and* $e_j = 0$ *else. Return* $e := (e_1, \ldots, e_n)$.

Note the difference between the system in Step 1 and (5.2): The set of linear equations in this algorithm is solvable knowing only f. We will now prove that Algorithm 5.1.6 works.

Proposition 5.1.7. *Let* $t \geq 0$ *be an integer,* $C_\Omega(\mathcal{B}, \mathcal{D})$ *a primary Goppa code and* $\mathcal{C}$ *a divisor such that* $\mathcal{C}$ *is positive,* $\operatorname{supp}\mathcal{C} \cap \operatorname{supp}\mathcal{B} = \varnothing$, $\ell(\mathcal{C}) > t$ *and* $\deg\mathcal{C} \leq \deg\mathcal{D} - 2g + 1 - t$. *If* e *is an error word of weight at most* t, c *is a code word and* $f = c + e$ *then running Algorithm 5.1.6 with input* f *results in* e.

Proof. Note that $\deg \mathcal{Y} = \deg \mathcal{D} - \deg \mathcal{C} \geq t + 2g - 1$. The support of $\mathcal{Y}$ is contained in $\operatorname{supp} \mathcal{C} \cup \operatorname{supp} \mathcal{D}$ and thus disjoint to $\operatorname{supp} \mathcal{B}$. Thus $\mathcal{C}$ and $\mathcal{Y}$ fulfil the requirements of Lemma 5.1.2 and Proposition 5.1.5. To see that Proposition 5.1.4 may be applied set $\mathcal{Z} := \mathcal{D}$ and $r := \deg \mathcal{D} - 2g - 2t + 1 \geq \deg \mathcal{C} - t \geq \ell(\mathcal{C}) - 1 - t \geq 0$. Due to Lemma 5.1.2, e has an error locator in $\mathfrak{L}(\mathcal{C})$. Furthermore, $\psi_i \chi_j \in \mathfrak{L}(\mathcal{C}\mathcal{Y}) = \mathfrak{L}(\mathcal{D})$ and hence $\psi_i \chi_j \cdot f = \psi_i \chi_j \cdot e$ for $1 \leq i \leq \ell, 1 \leq j \leq m$, i.e. the system in Step 1 is equivalent to (5.2). By Proposition 5.1.5 the element θ computed in Step 1 is an error locator of e. Consequently, $e_k \neq 0$ is only possible if $\theta(\mathcal{P}_k) = 0$. The system in Step 2 computes the values of e_i by Proposition 5.1.4. □

The next lemma states some conditions such that a divisor $\mathcal{C}$ with the properties required to apply Proposition 5.1.7 exists.

Lemma 5.1.8.

- *If there is an integer c such that*

$$t + g \leq c \leq \deg(\mathcal{D}) - 2g + 1 - t$$

  and some place $\mathcal{Q}$ of degree one, $\mathcal{Q} \notin \operatorname{supp} \mathcal{B}$, then there is a divisor $\mathcal{C}$ fulfilling the requirements of Proposition 5.1.7.

- *In particular, such an integer c exists if* $\deg(\mathcal{D}) \geq 3g + 2t - 1$.

Proof.

- In this case choose $\mathcal{C}$ positive, with degree equal to c and support disjoint from $\mathcal{B}$. One possible choice is to set $\mathcal{C} := c\mathcal{Q}$. By Riemann's Theorem $\ell(\mathcal{C}) \geq \deg(\mathcal{C}) + 1 - g > t$. Hence both of the required inequalities hold.

- Under this assumption $t + g \leq \deg(\mathcal{D}) - 2g + 1 - t$.

□

Remark. The algorithm described above is called *Skorobogatov-Vlăduţ error processing algorithm* . Combining the second inequality from Lemma 5.1.8 with the inequality for the minimal distance d of $C_\Omega(\mathcal{B}, \mathcal{D})$ yields

$$d \geq g + 2t + 1$$

or equivalently $t \leq \lfloor (d - g - 1)/2 \rfloor$. This means that we cannot ensure that the algorithm is capable of correcting more than $\lfloor (d-g-1)/2 \rfloor$ errors, which is in general less than the general error correction capacity $\lfloor (d-1)/2 \rfloor$.

5.2 List Decoding

Usually, decoding of a linear $[n, k, d]_q$-code C assumes that if $f = c+e$, $c \in C$ and f is the received word, the error e is of weight $w(e) \leq \lfloor \frac{d-1}{2} \rfloor$. The reason for this is the following: If $w(e) > \lfloor \frac{d-1}{2} \rfloor$, then there could be a code word $c' \neq c$ such that $d(c', f) \leq d(c, f) = w(e)$, i.e. f is at least as close to c' as to c. Thus the nearest neighbour decoding could produce the wrong result. In this section we will drop this assumption and follow a different approach, known as *list decoding*. It differs from the standard decoding problem in that it asks for a list L of all code words with distance less than or equal to r to a given word f, where $r \geq 0$ is in general greater than $\lfloor \frac{d-1}{2} \rfloor$. Thus, if $d(f, c) = w(e) \leq r$, the original code word c will be in L.

Definition 5.2.1 (List Decoding Problem)**.** Let $C \subseteq \mathbb{F}_q^n$ be a linear code, r be a non-negative integer and $f \in \mathbb{F}_q^n$ be a word. The list decoding problem asks for all words in $B_r^n(f) \cap C$ where

$$B_r^n(f) := \{g \in \mathbb{F}_q^n \colon d(f, g) \leq r\}$$

is the Hamming ball in $\mathbb{F}_q^n$ of radius r around f.

We are particularly interested in list decoding of Goppa codes. In Section 5.2.1 we will discuss a list decoding algorithm for Reed-Solomon codes introduced by Sudan in [15]. This algorithm was generalised to Goppa codes by Shokrollahi and Wasserman in [13] and improved by Sudan and Guruswami in [7]. We shall discuss this generalisation in Section 5.2.2.

Assume that for some fixed $r \geq 0$ and an arbitrary word $f \in \mathbb{F}_q^n$ the number of code words with distance at most r to f is bounded by some integer ℓ. I.e. if $B_r^n(f) \cap C = \{c_1, \ldots, c_{m(f)}\}$ then $m(f) \leq \ell$. A good list decoding algorithm should work for arbitrarily large n in reasonable time, i.e. in polynomial time in n. A necessary condition for this is that the size of the output $m(f)$ is bounded polynomially in n for all $f \in \mathbb{F}_q^n$ which is true if ℓ can be bounded by some polynomial in n. To formalize this notion we make the following definition:

Definition 5.2.2. Let C be a linear code of length n. If there are integers $r, \ell \geq 0$ such that there are at most ℓ code words in $B_r^n(f)$ for all $f \in \mathbb{F}_q^n$, i.e. $|B_r^n(f) \cap C| \leq \ell$, then C is said to be (r, ℓ)-decodeable.

Every $[n, k, d]_q$-code is $(\lfloor \frac{d-1}{2} \rfloor, 1)$-decodeable as well as (n, q^k)-decodeable.

5.2.1 List Decoding for Reed-Solomon Codes

Recall that a Reed-Solomon code $C_{RS}(k,1)$ over the field $\mathbb{F}_q$, introduced in Section 4.3.1, is an $[n,k,d]_q$ code where $n = q-1$, $1 \leq k \leq n$ and $d = n-k+1$. It is given by

$$C_{RS}(k,1) = \{(f(\alpha), f(\alpha^2), \ldots, f(\alpha^n))\colon f(\dot{x}) \in \mathbb{F}_q[\dot{x}], \deg f(\dot{x}) < k\}$$

where α is a primitive element of $\mathbb{F}_q$. The list decoding problem for $C_{RS}(k,1)$, a given word $(b_1, \ldots, b_n) \in \mathbb{F}_q^n$ and $r \geq 0$ is the problem of finding all polynomials $f(\dot{x}) \in \mathbb{F}_q[\dot{x}]$, $\deg f(\dot{x}) < k$ such that $f(\alpha^i) \neq b_i$ for at most r indices $i \in \{1, \ldots, n\}$. Or, in other words, finding all $f(\dot{x})$ such that $f(\alpha^i) = b_i$ for at least $t := n - r$ indices. Hence we can reformulate the list decoding problem for $C_{RS}(k,1)$ as follows:

Definition 5.2.3 (List Decoding Problem for Reed-Solomon Codes)**.** Let $(x_1, b_1), \ldots, (x_n, b_n)$ be distinct points with components in $\mathbb{F}_q$ and t be an integer, $0 \leq t \leq n$. The list decoding problem for Reed-Solomon codes is the problem of finding all polynomials $f(\dot{x}) \in \mathbb{F}_q[\dot{x}]$, $\deg f(\dot{x}) \leq k-1 =: k'$ such that $f(x_i) = b_i$ for at least t indices $i \in \{1, 2, \ldots, n\}$.

The list decoding problem for Reed-Solomon codes can be solved in polynomial time in n under the assumption that t is bounded from below by a certain constant depending on n and k'. We will present an algorithm to solve it going back to [15].

To motivate the algorithm assume we are in possession of a list of all polynomials $f_1(\dot{x}), \ldots, f_m(\dot{x})$ that solve the list decoding problem for tuples $(x_1, b_1), \ldots, (x_n, b_n)$ and parameters $k' = k-1$ and t. Set $Q(\dot{x}, \dot{y}) := (\dot{y} - f_1(\dot{x})) \cdots (\dot{y} - f_m(\dot{x}))$. Then, if t is small enough, $Q(x_i, b_i) = 0$ for all $i \leq n$. In particular, if $t \leq k'$, then for any choice of t indices $i(1), \ldots, i(t)$ there is a polynomial $f(\dot{x})$ of degree at most k' such that $f(x_{i(j)}) = b_{i(j)}$, $1 \leq j \leq t$, by Lagrange interpolation and thus $Q(x_{i(j)}, b_{i(j)}) = 0$. If we factor $Q(\dot{x}, \dot{y})$ into irreducible factors (note that $\mathbb{F}_q[\dot{x}, \dot{y}]$ is a unique factorisation domain) then we are able to reconstruct the list of the $f_i(\dot{x})$ again. Thus we will pursue the following strategy:

- Find a bivariate polynomial $Q(\dot{x}, \dot{y}) \neq 0$ with coefficients in $\mathbb{F}_q$ such that $Q(x_i, b_i) = 0$ for all $i \leq n$.
- Decompose $Q(\dot{x}, \dot{y})$ into irreducible factors. For each factor that is a constant multiple of $\dot{y} - f(\dot{x})$ for some $f(\dot{x}) \in \mathbb{F}_q[\dot{x}]$, output $f(\dot{x})$ if $\deg f(\dot{x}) \leq k'$ and $f(x_i) = b_i$ for at least t indices $i \in \{1, \ldots, n\}$.

We will have to choose the degree of $Q(\dot{x}, \dot{y})$ sufficiently large to be able to satisfy the first point. We will see that if a certain quantity derived from the degree of $Q(\dot{x}, \dot{y})$ is smaller than t then the polynomials provided in the second point represent a complete list of solutions to the list decoding problem.

Definition 5.2.4 ((w_1, w_2)-weighted Degree)**.** Let K be an arbitrary field. For a monomial $a\dot{x}^i\dot{y}^j \in K[\dot{x}, \dot{y}]$, $a \in K^\times$, and positive integers w_1, w_2 the (w_1, w_2)-weighted degree is $w_1 i + w_2 j$. For a polynomial $Q(\dot{x}, \dot{y}) \in K[\dot{x}, \dot{y}]$ the (w_1, w_2)-weighted degree $\deg_{(w_1,w_2)} Q(\dot{x}, \dot{y})$ is the maximum of the (w_1, w_2)-weighted degrees of all monomials of $Q(\dot{x}, \dot{y})$ with non-zero coefficients.

We will be interested in the $(1, k')$-weighted degree of bivariate polynomials and start with a result showing that the second point in our strategy indeed leads to all polynomials $f(\dot{x})$ that fulfil $f(x_i) = b_i$ for at least t indices i.

Lemma 5.2.5. *Let $Q(\dot{x}, \dot{y})$ be a bivariate polynomial and $g(\dot{x})$ be a univariate polynomial with coefficients in an arbitrary field K. Then there are polynomials $q(\dot{x}, \dot{y})$ and $r(\dot{x})$ such that*

$$Q(\dot{x}, \dot{y}) = (\dot{y} - g(\dot{x}))q(\dot{x}, \dot{y}) + r(\dot{x}).$$

Proof. We consider $Q(\dot{x}, \dot{y}) = \sum_{i=0}^{m} Q_i(\dot{x})\dot{y}^i$ as a polynomial in the unknown $\dot{y}$ with coefficients in $K(\dot{x})$, i.e. as an element of $K(\dot{x})[\dot{y}]$. Since $K(\dot{x})$ is a field we can use univariate polynomial division to obtain

$$Q(\dot{x}, \dot{y}) = (\dot{y} - g(\dot{x}))q(\dot{x}, \dot{y}) + r(\dot{x})$$

with $q(\dot{x}, \dot{y}) \in K(\dot{x})[\dot{y}]$ and $r(\dot{x}) \in K(\dot{x})$. We want to show that actually $q(\dot{x}, \dot{y}) \in K[\dot{x}, \dot{y}]$ and $r(\dot{x}) \in K[\dot{x}]$. Write $q(\dot{x}, \dot{y}) = q_1(\dot{x}, \dot{y})/q_2(\dot{x})$ and $q_1(\dot{x}, \dot{y}) = \sum_{i=0}^{m-1} h_i(\dot{x})y^i$ with $q_2(\dot{x}), h_i(\dot{x}) \in K[\dot{x}]$, $0 \leq i \leq m-1$. Then comparing coefficients at $\dot{y}^j$, $0 \leq j \leq m$, yields

$$\begin{aligned} Q_m(\dot{x}) &= h_{m-1}(\dot{x})/q_2(\dot{x}) \\ Q_j(\dot{x}) &= h_{j-1}(\dot{x})/q_2(\dot{x}) - g(\dot{x})h_j(\dot{x})/q_2(\dot{x}), 1 \leq j \leq m-1 \\ Q_0(\dot{x}) &= -g(\dot{x})h_0(\dot{x})/q_2(\dot{x}) + r(\dot{x}) \end{aligned}$$

By induction we see that $h_j(\dot{x})/q_2(\dot{x}) \in K[\dot{x}]$ for $0 \leq j \leq m-1$. Therefore $q(\dot{x}, \dot{y}) \in K[\dot{x}, \dot{y}]$ and consequently $r(\dot{x}) \in K[\dot{x}]$.

□

Proposition 5.2.6. *Let K be a field, $Q(\dot{x}, \dot{y}) \in K[\dot{x}, \dot{y}]$ and $f(\dot{x}) \in K[\dot{x}]$. Then $Q(\dot{x}, f(\dot{x}))$ is the zero polynomial if and only if $\dot{y} - f(\dot{x})$ divides $Q(\dot{x}, \dot{y})$.*

Proof. The implication from right to left is obvious. Thus, assume that $Q(\dot{x}, f(\dot{x})) = 0$. We use the above lemma to decompose $Q(\dot{x}, \dot{y})$ and substitute $\dot{y} = f(\dot{x})$:

$$0 = Q(\dot{x}, f(\dot{x})) = (f(\dot{x}) - f(\dot{x}))q(\dot{x}, f(\dot{x})) + r(\dot{x}) = r(\dot{x}).$$

Thus we see that $r(\dot{x})$ is the zero polynomial and hence $Q(\dot{x}, \dot{y}) = (\dot{y} - f(\dot{x}))q(\dot{x}, \dot{y})$. □

Corollary 5.2.7. *Let $(x_1, b_1), \ldots, (x_n, b_n) \in \mathbb{F}_q^2$ be distinct pairs, $0 \leq k', t \leq n$ integers, $Q(\dot{x}, \dot{y}) \in \mathbb{F}_q[\dot{x}, \dot{y}]$ with $Q(x_i, b_i) = 0$ for all $i \leq n$ and $f(\dot{x}) \in \mathbb{F}_q[\dot{x}]$, $\deg f(\dot{x}) \leq k'$ such that $f(x_i) = b_i$ for at least t indices i. If $Q(\dot{x}, \dot{y})$ is of $(1, k')$-weighted degree $N < t$ then $\dot{y} - f(\dot{x})$ divides $Q(\dot{x}, \dot{y})$.*

Proof. Let $a\dot{x}^i\dot{y}^j$ be a monomial of $Q(\dot{x}, \dot{y})$. To evaluate the degree of this monomial after the substitution $\dot{y} = f(\dot{x})$ we calculate

$$\deg(a\dot{x}^i f(\dot{x})^j) = i + j \deg f(\dot{x}) \leq \deg_{(1,k')} a\dot{x}^i\dot{y}^j \leq \deg_{(1,k')} Q(\dot{x}, \dot{y}).$$

Therefore we have the following bound for the degree of $g(\dot{x}) := Q(\dot{x}, f(\dot{x}))$:

$$\deg g(\dot{x}) = \deg(Q(\dot{x}, f(\dot{x}))) \leq \deg_{(1,k')} Q(\dot{x}, \dot{y}) = N < t$$

Due to our assumption

$$g(x_i) = Q(x_i, f(x_i)) = Q(x_i, b_i) = 0$$

for at least t indices i. Note that if $f(x_i) = b_i$, $f(x_j) = b_j$ for distinct indices i, j then $(x_i, f(x_i)) = (x_i, b_i) \neq (x_j, b_j) = (x_j, f(x_j))$ and thus $x_i \neq x_j$. So $g(\dot{x})$ has at least t distinct zeros. But $g(\dot{x})$ is of degree less than t and hence equal to the zero polynomial. Therefore $Q(\dot{x}, f(\dot{x})) = 0$ and so by Proposition 5.2.6, $\dot{y} - f(\dot{x})$ divides $Q(\dot{x}, \dot{y})$. □

Lemma 5.2.8. *Let $(x_1, b_1), \ldots, (x_n, b_n)$ be distinct points with coordinates in $\mathbb{F}_q$. If $r, s \geq 0$ are integers such that $(r+1)(s+1) + k'(s+1)s/2 > n$ then there exists a polynomial $Q(\dot{x}, \dot{y}) \in \mathbb{F}_q[\dot{x}, \dot{y}]$, $Q(\dot{x}, \dot{y}) \neq 0$ with $(1, k')$-weighted degree at most $r + sk'$ such that $Q(x_i, b_i) = 0$ for all $i \leq n$.*

Proof. We start by setting

$$Q(\dot{x}, \dot{y}) := \sum_{j=0}^{s} \sum_{i=0}^{r+(s-j)k'} q_{ij}\dot{x}^i\dot{y}^j.$$

Note that the $(1, k')$-weighted degree of the inner sum is at most $r + (s - j)k' + k'j = r + sk'$ and hence $\deg_{(1,k')} Q(\dot{x}, \dot{y}) \leq r + sk'$. The n equations

$Q(x_i, b_i) = 0$ lead to a linear system of equations in the unknowns q_{ij}. There are exactly

$$\sum_{j=0}^{s}(r + (s-j)k' + 1) = (r+1)(s+1) + k'\sum_{j=0}^{s}(s-j)$$
$$= (r+1)(s+1) + k'(s+1)s/2 > n$$

unknowns. Therefore there is a non-trivial solution q_{ij}, $0 \leq j \leq s, 0 \leq i \leq r + (s-j)k'$ of this system. This solution leads to a polynomial $Q(\dot{x}, \dot{y})$ with the desired properties. □

Corollary 5.2.7 and Lemma 5.2.8 show that if we find integers r, s such that

$$r + k's < t \text{ and } (r+1)(s+1) + k'(s+1)s/2 > n \tag{5.3}$$

the approach of finding a polynomial $Q(\dot{x}, \dot{y})$ with all the (x_i, b_i) as zeros and factoring it into irreducible factors provides a solution of the list decoding problem. Note that under the conditions given above all solutions $f(\dot{x})$ of the list decoding problem lead to a factor $\dot{y} - f(\dot{x})$ of $Q(\dot{x}, \dot{y})$. There might be factors $\dot{y} - f(\dot{x})$ of $Q(\dot{x}, \dot{y})$ such that $f(\dot{x})$ is not a solution of the list decoding problem. But these can be ruled out easily by testing the conditions $\deg f(\dot{x}) < k$ and $f(x_i) = b_i$ for at least t indices $i \in \{1, \ldots, n\}$. What is left to do is to choose r and s in a way that guarantees the above inequalities. The following lemma provides sufficient conditions on n, k' and t under which such integers r and s can be found:

Lemma 5.2.9. *If n, k' and t are non-negative integers such that*

$$t \geq k' \left\lceil \sqrt{2(n+1)/k'} \right\rceil - \lfloor k'/2 \rfloor \tag{5.4}$$

then the choice $r := \lceil k'/2 \rceil - 1$, $s := \left\lceil \sqrt{2(n+1)/k'} \right\rceil - 1$ leads to integers satisfying (5.3).

Proof. Set $A := \left\lceil \sqrt{2(n+1)/k'} \right\rceil$, then $s = A - 1$. Substituting this and rearranging terms show

$$\begin{aligned} 2\lceil k'/2\rceil &\geq k' \Rightarrow \\ (2\lceil k'/2\rceil - k')A &\geq 0 \Rightarrow \\ \underbrace{k'A^2}_{\geq 2n+2} + (2\lceil k'/2\rceil - k')A - 2n - 2 &\geq 0 \Rightarrow \\ 2\lceil k'/2\rceil A + k'A(A-1) &\geq 2n+2 \Rightarrow \\ (r+1)(s+1) + k'(s+1)s/2 &\geq n+1 \end{aligned}$$

The other inequality follows by the assumption on t from

$$r + k's = \lceil k'/2\rceil - 1 + k'(A-1) = \underbrace{k'A - \lfloor k'/2\rfloor}_{\leq t} + \underbrace{\lfloor k'/2\rfloor - k' + \lceil k'/2\rceil}_{=0} - 1 < t$$

□

Thus, putting together Corollary 5.2.7, Lemma 5.2.8 and Lemma 5.2.9 we obtain an algorithm solving the list decoding problem for Reed-Solomon codes with parameters n, k' and t, provided inequality (5.4) holds:

Algorithm 5.2.10.

Input	*A list of n distinct pairs $(x_1, b_1), \ldots, (x_n, b_n) \in \mathbb{F}_q^2$, parameters k', t.*
Output	*A list of all polynomials $f(\dot{x}) \in \mathbb{F}_q[\dot{x}]$, $\deg f(\dot{x}) \leq k'$ with the property that $f(x_i) = b_i$ for at least t indices i.*
Initialisation	*$r := \lceil k'/2\rceil - 1$, $s := \left\lceil \sqrt{2(n+1)/k'} \right\rceil - 1$, an empty list L.*
Step 1	*Find $Q(\dot{x}, \dot{y}) \in \mathbb{F}_q[\dot{x}, \dot{y}]$ such that $Q(x_i, b_i) = 0$ for all $i \leq n$ and $\deg_{(1,k')} Q(\dot{x}, \dot{y}) \leq r + sk'$ by solving a linear system of equations.*
Step 2	*Factor $Q(\dot{x}, \dot{y})$ into irreducible elements. For each factor which is a constant multiple of $\dot{y} - p(\dot{x})$, check if $\deg p(\dot{x}) \leq k'$ and $p(x_i) = b_i$ for at least t indices $i \leq n$. If so add $p(\dot{x})$ to L.*

Since this section should motivate the solution of the list decoding problem for Goppa codes, we did not pay attention to every detail. In particular we skipped the problem of factoring polynomials in $\mathbb{F}_q[\dot{x}, \dot{y}]$ into irreducible factors. This problem is solveable in polynomial time in the degree of the bivariate polynomial. The degree of $Q(\dot{x}, \dot{y})$ in the above algorithm is bounded

by some polynomial in n. So the procedure still runs in polynomial time, although the factorisation of $Q(\dot{x}, \dot{y})$ is the bottle neck. When we consider list decoding of Goppa codes we will see how to generalise the approach of Algorithm 5.2.10.

Putting together the previous results we can prove that Reed-Solomon codes are (r, ℓ)-decodeable for fairly good parameters r and ℓ:

Corollary 5.2.11. *The Reed-Solomon code $C_{RS}(k, 1)$ over $\mathbb{F}_q$ of length $n = q - 1$ is (r, ℓ)-decodeable with*

$$r = n - (k-1)\left\lceil \sqrt{2(n+1)/(k-1)} \right\rceil, \ell = \left\lceil \sqrt{2(n+1)/(k-1)} \right\rceil.$$

Proof. Take an arbitrary word $b = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$. We must show that $|B_r(b) \cap C_{RS}(k, 1)| \leq \ell$. Let α be a primitive element of $\mathbb{F}_q$ such that the code words are $(f(\alpha), \ldots, f(\alpha^n))$, $f(\dot{x}) \in \mathbb{F}_q[\dot{x}]$, $\deg f(\dot{x}) < k$. Set $x_i := \alpha^i$, $1 \leq i \leq n$ and $t := n - r$. Then $(f(\alpha), \ldots, f(\alpha^n)) \in B_r(b)$ if and only if $f(x_i) = b_i$ for at least t indices $i \in \{1, \ldots, n\}$. By the choice of r, t fulfils the condition of Lemma 5.2.9 ($k' = k - 1$). Thus there is a polynomial $Q(\dot{x}, \dot{y})$ such that $Q(x_i, b_i) = 0$, $i \leq n$ and the $(1, k')$-weighted degree of $Q(\dot{x}, \dot{y})$ is less than t. Let $f_i(\dot{x})$, $1 \leq i \leq m$ be the polynomials of degree less than k corresponding to the code words in $B_r(b)$, i.e. $|B_r(b) \cap C_{RS}(k, 1)| = m$. Then by Corollary 5.2.7 the factors $\dot{y} - f_i(\dot{x})$ divide $Q(\dot{x}, \dot{y})$ and thus

$$mk' = \deg_{(1,k')}(\dot{y} - f_1(\dot{x})) + \ldots + \deg_{(1,k')}(\dot{y} - f_m(\dot{x})) \leq \deg_{(1,k')} Q(\dot{x}, \dot{y}) < t$$

and hence $m < t/k' = \left\lceil \sqrt{2(n+1)(k-1)} \right\rceil / (k-1) \leq \left\lceil \sqrt{2(n+1)/(k-1)} \right\rceil$. □

5.2.2 List Decoding for Goppa Codes

It is obvious how to reformulate the list decoding problem for dual Goppa codes. Recall that for divisors $\mathcal{B} = \mathcal{P}_1 \cdots \mathcal{P}_n$, $\mathcal{D}$ with $\operatorname{supp} \mathcal{B} \cap \operatorname{supp} \mathcal{D} = \varnothing$, where $\mathcal{P}_i$ are places of degree one, the dual Goppa code is defined by

$$C_L(\mathcal{B}, \mathcal{D}) = \{(\varphi(\mathcal{P}_1), \ldots, \varphi(\mathcal{P}_n)) \colon \varphi \in \mathfrak{L}(\mathcal{D})\}.$$

Thus the list decoding problem for $C_L(\mathcal{B}, \mathcal{D})$, analogous to the case of Reed-Solomon codes, will be solved if we find a solution to the following problem: Given an integer t, $0 \leq t \leq n$ and a word $b = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$, find all functions $\varphi \in \mathfrak{L}(\mathcal{D})$ such that $\varphi(\mathcal{P}_i) = b_i$ for at least t indices among $i = 1, \ldots, n$.

Since Reed-Solomon codes are a special case of Goppa codes, it is not surprising that it is possible to generalise the results of the previous section for the latter class of codes. For this purpose we define the following evaluation of polynomials $H(\dot{y}) \in F(\dot{y})$, where $F/\mathbb{F}_q$ is an algebraic function field: Take a place $\mathcal{Q}$ of $F/\mathbb{F}_q$ and an element $\varphi \in F$. Then $H(\varphi) \in F$ and thus $H(\mathcal{Q}, \varphi) := H(\varphi)(\mathcal{Q})$ is an element of some finite extension field of $\mathbb{F}_q$, if $\mathcal{Q}$ is not a pole of $H(\varphi)$. If $\mathcal{Q}$ is a place of degree one, $\beta \in \mathbb{F}_q$ then $H(\mathcal{Q}, \beta) \in \mathbb{F}_q \cup \{\infty\}$. If $H(\dot{y}) = \sum_{j=0}^{m} u_j \dot{y}^j$ then this evaluation is given by

$$H(\mathcal{Q}, \beta) = \sum_{j=0}^{m} u_j(\mathcal{Q}) \beta^j.$$

In analogy to the case of Reed-Solomon codes the solution to the list decoding problem is roughly the following:

- Find a polynomial $H(\dot{y}) \in F[\dot{y}]$ (this will play the role of $Q(\dot{x}, \dot{y})$ in the previous section), $H(\dot{y}) = \sum_{j=0}^{m} u_j \dot{y}^j$ such that $H(\mathcal{P}_i, b_i) = 0$ for $1 \leq i \leq n$.
- Find all roots $\varphi \in F$ of $H(\dot{y})$. For each root check if $\varphi \in \mathfrak{L}(\mathcal{D})$ and $\varphi(\mathcal{P}_i) = b_i$ for at least t indices $i \in \{1, \ldots, n\}$. In this case, φ is a solution to the list decoding problem.

We will first give conditions on $H(\dot{y})$ under which all solutions of the list decoding problem are roots of $H(\dot{y})$:

Lemma 5.2.12. *Consider the dual Goppa code $C_L(\mathcal{B}, \mathcal{D})$, $\mathcal{B} = \mathcal{P}_1 \cdots \mathcal{P}_n$ and a word $b = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$. Take some integer $0 \leq t \leq n$, an integer $m \geq 0$ and a divisor $\mathcal{F}$, $\deg \mathcal{F} = t - 1 - m \deg(\mathcal{D})$ with support disjoint from $\mathcal{B}$. If*

$$H(\dot{y}) = \sum_{j=0}^{m} u_j \dot{y}^j \in F[\dot{y}],$$

$u_j \in \mathfrak{L}(\mathcal{F}\mathcal{D}^{m-j})$, such that $H(\mathcal{P}_i, b_i) = 0$ for $1 \leq i \leq n$ and $\varphi \in \mathfrak{L}(\mathcal{D})$ is a solution to the list decoding problem then φ is a root of $H(\dot{y})$.

Proof. Due to our assumptions we have $u_j \varphi^j \in \mathfrak{L}(\mathcal{F}\mathcal{D}^m)$, hence $H(\varphi)$ is in this Riemann-Roch space as well.

$$H(\mathcal{P}_i, \varphi) = \sum_{j=0}^{m} u_j(\mathcal{P}_i) \varphi(\mathcal{P}_i)^j = \sum_{j=0}^{m} u_j(\mathcal{P}_i) b_i^j = 0$$

for at least t places $\mathcal{P}_i$ by the assumption on φ. Denote by $\mathcal{C}$ the product of those places $\mathcal{P}_i$ such that $H(\varphi)(\mathcal{P}_i) = H(\mathcal{P}_i, \varphi) = 0$, i.e. $\deg \mathcal{C} \geq t$.

So $H(\varphi) \in \mathfrak{L}(\mathcal{C}^{-1})$ and since $\operatorname{supp}\mathcal{C} \cap \operatorname{supp}\mathcal{F}\mathcal{D}^m = \varnothing$ we have $H(\varphi) \in \mathfrak{L}(\mathcal{F}\mathcal{D}^m\mathcal{C}^{-1})$. By the choice of the degree of $\mathcal{F}$ we obtain

$$\deg(\mathcal{F}\mathcal{D}^m\mathcal{C}^{-1}) = \deg(\mathcal{F}) + m\deg(\mathcal{D}) - \deg(\mathcal{C}) \leq (t - 1 - m\deg(\mathcal{D})) + m\deg(\mathcal{D}) - t < 0$$

This shows $\mathfrak{L}(\mathcal{F}\mathcal{D}^m\mathcal{C}^{-1}) = \{0\}$, so $H(\varphi) = 0$, which concludes the proof. □

Lemma 5.2.13. *With the notation of Lemma 5.2.12 assume that*

$$(m+1)(t-g) - \deg(\mathcal{D})\frac{m(m+1)}{2} > n. \tag{5.5}$$

Then there is a polynomial $H(\dot{y}) \in F[\dot{y}]$ with the properties stated in the lemma.

Proof. Let $\psi_{j1}, \ldots, \psi_{jr(j)}$ be a basis of $\mathfrak{L}(\mathcal{F}\mathcal{D}^{m-j})$ for $0 \leq j \leq m$, i.e. $r(j) = \ell(\mathcal{F}\mathcal{D}^{m-j})$. We make the ansatz $u_j = \sum_{k=1}^{r(j)} a_{jk}\psi_{jk}$ for unknowns $a_{jk} \in \mathbb{F}_q$. Substituting this into the equation for $H(\dot{y})$ and evaluating at $(\mathcal{P}_i, b_i)$ yield the n linear equations

$$H(\mathcal{P}_i, b_i) = \sum_{j=0}^{m}\sum_{k=1}^{r(j)} a_{jk}\psi_{jk}(\mathcal{P}_i)b_i^j = 0, \quad 1 \leq i \leq n. \tag{5.6}$$

By Riemann's Theorem $r(j) \geq \deg(\mathcal{F}\mathcal{D}^{m-j}) - g + 1 = (t - 1 - m\deg(\mathcal{D})) + (m-j)\deg(\mathcal{D}) - g + 1 = t - g - j\deg(\mathcal{D})$. There are exactly

$$\sum_{j=0}^{m} r(j) \geq \sum_{j=0}^{m} t - g - j\deg(\mathcal{D}) = (m+1)(t-g) - \deg(\mathcal{D})\frac{m(m+1)}{2} > n$$

unknowns. Thus the linear system (5.6) has a non-trivial solution, which leads to a polynomial $H(\dot{y})$ with the desired properties. □

Lemma 5.2.14. *Assume m, n, g and $\deg(\mathcal{D})$ are given. If we set*

$$t := \left\lceil \frac{n+1}{m+1} + \frac{m\deg(\mathcal{D})}{2} + g \right\rceil$$

then inequality (5.5) is satisfied.

Proof. According to our choice of t the left hand side of inequality (5.5) is greater than or equal to

$$(m+1)\left(\frac{n+1}{m+1}+\frac{m\deg(\mathcal{D})}{2}\right)-\deg(\mathcal{D})\frac{m(m+1)}{2}=n+1>n.$$

□

Lemma 5.2.15. *The dual Goppa code $C_L(\mathcal{B},\mathcal{D})$ is (r,m)-decodeable with $r=n-\lceil(n+1)/(m+1)+(m\deg(\mathcal{D}))/2+g\rceil$ for an arbitrary integer $m\geq 0$.*

Proof. Given an arbitrary word $b=(b_1,\ldots,b_n)\in\mathbb{F}_q^n$ the number of code words in $B_r(b)$ is bounded by the number of those $\varphi\in\mathfrak{L}(\mathcal{D})$ with the property $\varphi(\mathcal{P}_i)=b_i$ for at least $t:=n-r$ indices $i=1,\ldots,n$, i.e. the number of solutions to the associated list decoding problem. By our choice of r, Lemma 5.2.14 and Lemma 5.2.13 apply to t and thus there is a polynomial $H(\dot{y})\in F[\dot{y}]$ of degree at most m satisfying the conditions of Lemma 5.2.12. By this lemma, each solution of the list decoding problem is a root of $H(\dot{y})$. This shows $|B_r(b)\cap C_L(\mathcal{B},\mathcal{D})|\leq m$. □

Let us consider some consequences of Lemma 5.2.15: Note that under the standard assumption $\deg(\mathcal{D})<\deg(\mathcal{B})$ we have $k=\ell(\mathcal{D})\geq\deg(\mathcal{D})-g+1$ and hence $\deg(\mathcal{D})\leq k+g-1$. Thus we see that Goppa codes are $(n-\lceil(n+1)/(m+1)+m(k+g-1)/2+g\rceil,m)$-decodeable for an arbitrary $m\geq 0$. By choosing $\alpha:=g+k-1$, $m=\lceil\sqrt{2n/\alpha}\rceil$ a straight forward estimate shows that Goppa codes are

$$\left(n-\left\lceil\sqrt{2n\alpha}\right\rceil+g,\left\lceil\sqrt{2n/\alpha}\right\rceil\right)$$

-decodeable. For Reed-Solomon codes $g=0$, so $\alpha=k-1$ and this turns out to be almost the same result as Corollary 5.2.11 (actually it is even a slight improvement).

If we collect the results of this section, we obtain an algorithm similar to 5.2.10, that solves the list decoding problem. Of course we have to assume that the parameters n,g and $\deg(\mathcal{D})$ (stemming from $C_L(\mathcal{B},\mathcal{D})$) as well as t (stemming from the list decoding problem) and m fulfil inequality (5.5), e.g. by choosing t as suggested by Lemma 5.2.14.

Algorithm 5.2.16. *The following step has to be performed only once: Choose a divisor $\mathcal{F}$, $\deg\mathcal{F}=t-1-m\deg(\mathcal{D})$, $\operatorname{supp}\mathcal{F}\cap\operatorname{supp}\mathcal{B}=\varnothing$ and find bases $\psi_{j1},\ldots,\psi_{jr(j)}$ of $\mathfrak{L}(\mathcal{F}\mathcal{D}^{m-j})$ for $0\leq j\leq m$.*

Input	*Places* $\mathcal{P}_1, \ldots, \mathcal{P}_n$, *elements* $b_1, \ldots, b_n \in \mathbb{F}_q$, *parameters* $t, m, \deg(\mathcal{D}), g$.
Output	*A list* L *of all elements* $\varphi \in \mathfrak{L}(\mathcal{D})$ *with the property* $\varphi(\mathcal{P}_i) = b_i$ *for at least* t *indices* $i \in \{1, \ldots, n\}$.
Initialisation	*Empty list* L.
Step 1	*Find a polynomial* $H(\dot{y}) = \sum_{j=0}^{m} u_j \dot{y}^j \in F[\dot{y}]$, $H(\dot{y}) \neq 0$, $u_j \in \mathfrak{L}(\mathcal{F}\mathcal{D}^{m-j})$, $H(\mathcal{P}_i, b_i) = 0$ *for* $1 \leq i \leq n$ *by solving the linear system in (5.6) and setting* $u_j := \sum_{k=1}^{r(j)} a_{jk}\psi_{jk}$.
Step 2	*Factor* $H(\dot{y})$ *into irreducible factors in* $F[\dot{y}]$. *For each linear factor* $\dot{y} - \varphi$ *of* $H(\dot{y})$ *check if* $\varphi \in \mathfrak{L}(\mathcal{D})$ *and* $\varphi(\mathcal{P}_i) = b_i$ *for at least* t *indices* $i \in \{1, \ldots, n\}$. *If so add* φ *to* L.

Remark. This algorithm requires a subroutine to factor polynomials in $F(\dot{x})$ into irreducible factors. A possible solution to solve this problem is sketched in [13, Section III]. It is an adaption of a well-known procedure to factor univariate polynomials with coefficients in algebraic number fields, see e.g. [2, Section 3.6]

Bibliography

[1] Claude Chevalley. *Introduction to the Theory of Algebraic Functions of One Variable*. Mathematical Surveys, No. VI. American Mathematical Society, New York, N. Y., 1951.

[2] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[3] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 7.3)*, 2016. `http://www.sagemath.org`.

[4] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[5] Otto Forster. *Lectures on Riemann surfaces*, volume 81 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1981.

[6] William Fulton. *Algebraic curves*. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989.

[7] Venkatesan Guruswami and Madhu Sudan. Improved decoding of Reed-Solomon and algebraic-geometry codes. *IEEE Trans. Inform. Theory*, 45(6):1757–1767, 1999.

[8] Tom Høholdt, Jacobus H. van Lint, and Ruud Pellikaan. *Algebraic geometry codes*. 2011. `http://www.win.tue.nl/~ruudp/paper/31.pdf`.

[9] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes. I.* North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977. North-Holland Mathematical Library, Vol. 16.

[10] Harald Niederreiter and Chaoping Xing. *Algebraic geometry in coding theory and cryptography*. Princeton University Press, Princeton, NJ, 2009.

[11] Oliver Pretzel. *Codes and algebraic curves*, volume 8 of *Oxford Lecture Series in Mathematics and its Applications*. The Clarendon Press, Oxford University Press, New York, 1998.

[12] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[13] M. Amin Shokrollahi and Hal Wasserman. List decoding of algebraic-geometric codes. *IEEE Trans. Inform. Theory*, 45(2):432–437, 1999.

[14] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[15] Madhu Sudan. Decoding of Reed Solomon codes beyond the error-correction bound. *J. Complexity*, 13(1):180–193, 1997.

[16] B. L. van der Waerden. *Algebra. Vol. I.* Springer-Verlag, New York, 1991.

[17] B. L. van der Waerden. *Algebra. Vol. II.* Springer-Verlag, New York, 1991.

[18] J. H. van Lint. *Introduction to coding theory*, volume 86 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, third edition, 1999.

[19] Robert J. Walker. *Algebraic Curves*. Princeton Mathematical Series, vol. 13. Princeton University Press, Princeton, N. J., 1950.

Index