Brill-Noether Algorithm

Construction of Geometric Goppa Codes

and

Absolute Factorization of Polynomials

Paweł Wocjan
Universität Karlsruhe
Institut für Algorithmen und
Kognitive Systeme
Am Fasanengarten 5
76128 Karlsruhe
Germany

February 15, 1999

Contents

Chapter 1

Introduction

In this diploma thesis we present the Brill-Noether algorithm and show how it can be used for effective construction of geometric Goppa codes and for the absolute factorization of bivariate polynomials.

Let $\mathcal{C}$ be a projective plane curve defined over a field K and having only ordinary singular points. The classical Brill-Noether algorithm gives a construction of a basis of the vector space $\mathcal{L}(D)$ associated to a divisor D of the function field $\overline{K}(\mathcal{C})$ of the curve $\mathcal{C}$ where $\overline{K}$ denotes an algebraic closure of K. A generalization of the classical Brill-Noether algorithm to projective plane curves having non-ordinary singularities is presented in [BR88]. In the frame work of code theory this generalization gives a construction of "good" codes associated with curves having many rational points over a given finite field. G. Haché's presentation of the algorithms in a strictly algebraic manner using the theory of algebraic function fields in [Hac96] (preceding papers [BH95] and [Hac95]) permits an easy translation of the theory into any computer algebra language. It is easy to compute the genus of any singular plane curve $\mathcal{C}$, to find a basis of $\mathcal{L}(D)$, where D is a divisor of the function field $\overline{K}(\mathcal{C})$, and to evaluate functions at any place $\mathfrak{P}$ of degree one. We need all this for the construction of a geometric Goppa code. All the algorithms have been implemented by G. Haché in AXIOM. The Brill-Noether algorithm is polynomial in the degree of the curve and the degree of the divisor. This complexity has been proved in [Lau97].

In the second part we show that the Brill-Noether algorithm is also valid for non-irreducible projective plane curves. We generalize the concepts defined for algebraic function fields to a structure that is isomorphic to the direct product of function fields of the irreducible components. It is the ring of global functions defined on the non-irreducible curve. We can now apply the Brill-Noether algorithm for the absolute factorization of bivariate polynomials using the geometric approach proposed in [Duv91]. The Brill-Noether algorithm has been adapted to the non-irreducible case in [LB89]. However, in [Hac98] it has been shown that the Brill-Noether algorithm is also valid for non-irreducible curves without any modifications. This results in a better complexity.

Some new proofs concerning the Brill-Noether algorithm are presented in this diploma thesis. All the necessary algorithms for the construction of geometric Goppa codes and the absolute factorization have been implemented by the author in MuPAD. An implementation in MAGMA is planned.

Chapter 2

Algebraic Function Fields

In this chapter we first review the basic definitions and results of the theory of algebraic function fields: *valuations*, *places*, *divisors*, the *genus* of a function field and the *Riemann-Roch theorem*. Then we describe briefly the construction of geometric Goppa codes. For a thorough treatment of algebraic function fields and codes we refer the reader to [Sti93].

Throughout the whole report, K denotes a perfect field.

2.1 Places

Definition 2.1 *An* algebraic function field F/K of one variable over K *is an extension field $F \supset K$ such that F is a finite algebraic extension of $K(x)$ for some element $x \in F$ which is transcendental over K.*

For brevity, we simply refer to F/K as a *function field*. The set $\overline{K}^c := \{z \in F \mid z \text{ is algebraic over } K\}$ is a subfield of F, since sums, products and inverses of algebraic elements are also algebraic. $\overline{K}^c$ is called the *field of constants of F/K*. We have $K \subseteq \overline{K}^c \subset F$, and it is easily verified that $F/\overline{K}^c$ is a function field over $\overline{K}^c$. We say that K is *algebraically closed in F* (or K is the *full constant field of F*) if $K = \overline{K}^c$.

Remark 2.1 *The elements of F which are transcendental over K can be characterized as follows: $z \in F$ is transcendental over K if and only if $[F : K(z)] < \infty$.*

Proposition 2.1 *Let F/K be a function field where K is a perfect*[1] *field. Then there exist $x, y \in F$ such that $F = K(x, y)$.*

Proof: [Sti93], Proposition III.9.2 □

Let us recall that a non-constant polynomial $C \in K[X, Y]$ is called *absolutely irreducible* if it is irreducible in $\overline{K}[X, Y]$ where $\overline{K}$ is an algebraic closure of K.

Proposition 2.2 *Let F/K be a function field and $\overline{K}^c$ be the field of constants of F/K. Let $x, y \in F$ such that $F = K(x, y)$ and $C(X, Y) \in K[X, Y]$ be an irreducible polynomial such that $C(x, y) = 0$. Then*

$$K = \overline{K}^c \iff C \text{ is absolutely irreducible.}$$

[1] A field is called perfect if all its algebraic extensions are separable. For example, fields of characteristic 0, all finite fields and all algebraically closed fields are perfect

Proof: [Sti93] Corollary III.6.7 □

Definition 2.2 *A* valuation ring *of the function field F/K is a ring $\mathcal{O} \subset F$ with the following properties:*

1. $K \subsetneq \mathcal{O} \subsetneq F$,
2. *for any $z \in F$, $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.*

Proposition 2.3 *Let $\mathcal{O}$ be a valuation ring of F/K. Then*

1. *$\mathcal{O}$ is a local ring, i.e. $\mathcal{O}$ has a unique maximal ideal $\mathfrak{P} = \mathcal{O} \setminus \mathcal{O}^*$, where $\mathcal{O}^*$ is the group of units of $\mathcal{O}$.*
2. *For $0 \neq x \in F$, $x \in \mathfrak{P} \Longleftrightarrow x^{-1} \notin \mathcal{O}$.*
3. *For the field of constants of F/K we have $\overline{K}^c \subseteq \mathcal{O}$ and $\overline{K}^c \cap \mathfrak{P} = \{0\}$.*

Proof: [Sti93], I.1.5. Proposition □

Definition 2.3 *A* place *of the function field F/K is the maximal ideal of some valuation ring $\mathcal{O}$ of F/K. We denote the set of all places of F/K by $\mathbb{P}_F$.*

If $\mathcal{O}$ is a valuation ring of F/K and $\mathfrak{P}$ its maximal ideal, then $\mathcal{O}$ is uniquely determined by $\mathfrak{P}$ (the preceding proposition), namely $\mathcal{O} = \{z \in F \mid z^{-1} \notin \mathfrak{P}\}$. Hence $\mathcal{O}_\mathfrak{P} := \mathcal{O}$ is called the *valuation ring of the place* $\mathfrak{P}$.

Theorem 2.4 *Let $\mathcal{O}$ be a valuation ring of the function field F/K and $\mathfrak{P}$ the unique maximal ideal of $\mathcal{O}$. Then*

1. *$\mathfrak{P}$ is a principal ideal.*
2. *If $\mathfrak{P} = t\mathcal{O}_\mathfrak{P}$ then any element $z \in F \setminus \{0\}$ has a unique representation $z = t^n u$ for some element $n \in \mathbb{Z}$ and $u \in \mathcal{O}_\mathfrak{P}^*$. The number n does not depend on the choice of t.*

Proof: [Sti93] Theorem I.1.6 □

A ring having the above properties is called a *discrete valuation ring.*

Definition 2.4 *Let $\mathfrak{P}$ be a place of the function field F/K. Any element $t \in \mathfrak{P}$ such that $\mathfrak{P} = t\mathcal{O}_\mathfrak{P}$ is called a* local parameter *(or a* uniformizing variable*).*

A second useful description of places is given in terms of valuations.

Definition 2.5 *A* discrete valuation *of F/K is a function $\nu : F \to \mathbb{Z} \cup \{\infty\}$ with the following properties:*

1. *$\nu(x) = \infty \Longleftrightarrow x = 0$.*
2. *$\nu(xy) = \nu(x) + \nu(y)$ for any $x, y \in F$.*
3. *$\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$ for any $x, y \in F$.*
4. *There exists an element $z \in F$ with $\nu(z) = 1$.*

5. $\nu(a) = 0$ *for any* $0 \neq a \in K$.

A stronger version of the inequality 3 of the Definition 2.5 can be derived from the axioms and is often very useful:

Lemma 2.5 (Strict Triangle Inequality) *Let* ν *be a discrete valuation of* F/K *and* $x, y \in F$ *with* $\nu(x) \neq \nu(y)$. *Then* $\nu(x+y) = \min\{\nu(x), \nu(y)\}$.

Proof: [Sti93], I.1.10. Lemma □

Definition 2.6 *To any place* $\mathfrak{P} \in \mathbb{P}_F$ *we associate a function* $\nu_{\mathfrak{P}} : F \to \mathbb{Z} \cup \{\infty\}$ *that turn out to be a discrete valuation of* F/K*: Choose a local parameter* t *of* $\mathfrak{P}$. *Then every* $0 \neq z \in F$ *has a unique representation* $z = t^n u$ *with* $u \in \mathcal{O}_{\mathfrak{P}}^*$ *and* $n \in \mathbb{Z}$. *Define* $\nu_{\mathfrak{P}}(z) := n$ *and* $\nu_{\mathfrak{P}}(0) := \infty$.

Theorem 2.6 *Let* F/K *be a function field.*

1. *For any place* $\mathfrak{P} \in \mathbb{P}_F$, *the function* $\nu_{\mathfrak{P}}$ *defined above is a discrete valuation of* F/K. *Moreover, we have*

$$\begin{aligned} \mathcal{O}_{\mathfrak{P}} &= \{z \in F \mid \nu_{\mathfrak{P}}(z) \geq 0\}, \\ \mathcal{O}_{\mathfrak{P}}^* &= \{z \in F \mid \nu_{\mathfrak{P}}(z) = 0\}, \\ \mathfrak{P} &= \{z \in F \mid \nu_{\mathfrak{P}}(z) > 0\}. \end{aligned}$$

   An element $z \in F$ *is a local parameter for* $\mathfrak{P}$ *if and only if* $\nu_{\mathfrak{P}}(z) = 1$.

2. *Conversely, suppose that* ν *is a discrete valuation of* F/K. *Then the set* $\mathfrak{P} := \{z \in F \mid \nu(z) > 0\}$ *is a place of* F/K, *and* $\mathcal{O}_{\mathfrak{P}} = \{z \in F \mid \nu(z) \geq 0\}$ *is the corresponding valuation ring.*

3. *Any valuation ring* $\mathcal{O}$ *of* F/K *is a maximal proper subring of* F.

Proof: [Sti93], I.1.12 Theorem □

According to this theorem *places*, *valuation rings* and *discrete valuations* of a function field essentially amount to the same thing.

Let $\mathfrak{P}$ be a place of F/K and $\mathcal{O}_{\mathfrak{P}}$ its valuation ring. Since $\mathfrak{P}$ is a maximal ideal, the residue class ring $\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$ is a field. For $x \in \mathcal{O}_{\mathfrak{P}}$ we define $x(\mathfrak{P}) \in \mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$ to be the residue class of x modulo $\mathfrak{P}$, for $x \in F \setminus \mathcal{O}_{\mathfrak{P}}$ we put $x(P) := \infty$ (note that the symbol ∞ is used here in a different sense as in Definition 2.5). By Proposition 2.3 we know that $K \subset \mathcal{O}_{\mathfrak{P}}$ and $K \cap \mathfrak{P} = \{0\}$, so the residue map $\mathcal{O}_{\mathfrak{P}} \to \mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$ induces a canonical embedding of K into $\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$. Henceforth we shall always consider K as a subfield of $\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$ via this embedding. Observe that this argument also applies to $\overline{K}^c$ instead of K; so we can consider $\overline{K}^c$ as a subfield of $\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$ as well.

Definition 2.7 *Let* $\mathfrak{P} \in \mathbb{P}_F$.

1. $F_{\mathfrak{P}} := \mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$ *is the* residue class field *of* $\mathfrak{P}$. *The map* $x \mapsto x(\mathfrak{P})$ *from* F *to* $F_{\mathfrak{P}} \cup \{\infty\}$ *is called the* residue class map *with respect to* $\mathfrak{P}$. *Sometimes we shall also use the notation* $x + \mathfrak{P} := x(\mathfrak{P})$ *for* $x \in \mathcal{O}_{\mathfrak{P}}$.

2. $\deg \mathfrak{P} := [F_{\mathfrak{P}} : \mathfrak{P}]$ *is called the* degree *of* $\mathfrak{P}$.

The degree of a place is always finite; more precisely, the following holds.

Proposition 2.7 *If $\mathfrak{P}$ is a place of F/K and $0 \neq x \in \mathfrak{P}$ then*

$$\deg \mathfrak{P} \leq [F : K(x)] \leq \infty.$$

Proof: [Sti93], I.1.14 Proposition □

Since $\overline{K}^c$ is a subfield of $F_{\mathfrak{P}}$, we have the following Corollary.

Corollary 2.8 *Let $\overline{K}^c$ be the constant field of F/K. Then*

$$[\overline{K}^c : K] < \infty.$$

Remark 2.2 *For the case when $\deg \mathfrak{P} = 1$ we have $F_{\mathfrak{P}} = K$, and the residue class map maps F to $K \cup \{\infty\}$. In particular, if K is an algebraically closed field, any place has degree one, so we can interpret an element $z \in F$ as a function*

$$z : \begin{cases} \mathbb{P}_F & \to & K \cup \{\infty\} \\ \mathfrak{P} & \mapsto & z(\mathfrak{P}) \end{cases} .$$

This is why F/K is called a function field. *The elements of K, interpreted as functions in this sense are constant functions. For this reason K is called the* constant field *of F. Also, the following terminology is justified.*

Definition 2.8 *Let $z \in F \setminus \{0\}$ and $\mathfrak{P} \in \mathbb{P}_F$. We say that $\mathfrak{P}$ is a* zero *of z if $\nu_{\mathfrak{P}}(z) > 0$; $\mathfrak{P}$ is a* pole *of z if $\nu_{\mathfrak{P}}(z) < 0$.*

Proposition 2.9 *Let F/K be a function field. Let R be a ring such that $K \subsetneq R \subsetneq F$ and I a proper ideal of R. Then there exits a place $\mathfrak{P} \in \mathbb{P}_F$ such that $R \subseteq \mathcal{O}_{\mathfrak{P}}$ and $I \subseteq \mathfrak{P}$. Moreover, if I is a prime ideal then $I = \mathfrak{P} \cap R$.*

Proof: [Sti93], Theorem I.1.18. and [Che51], Remark 2 on page 8 □

Corollary 2.10 *Let F/K be a function field and $z \in F$ transcendental over K. Then z has at least a zero and a pole.*

Proof: To find a zero of z, we apply the preceding proposition to the ring $K[z] \subset F$ and to the ideal $I := zK[z]$. To find a pole, we use the same argument with z^{-1}. □

Remark 2.3 *Let F/K be a function field and $z \in F \setminus \{0\}$. Then*

$$z \in \overline{K}^c \setminus \{0\} \Longleftrightarrow z \text{ has neither a zero nor a pole.}$$

The implication ($\Rightarrow$) follows from the fact that $\overline{K}^c \cap \mathfrak{P} = \{0\}$ for any place $\mathfrak{P} \in \mathbb{P}_F$ and the converse is true since by the corollary 2.10 $z \notin \overline{K}^c$ implies that z is transcendental over K. □

Proposition 2.11 *In a function field F/K any element $z \in F \setminus \{0\}$ has only finitely many zeros and places.*

Proof: [Sti93], I.3.4 Corollary □

2.2 Divisors

The field $\overline{K}^c$ of constants of a function field F/K is a finite extension field of K, and F can be regarded as a function field over $\overline{K}^c$. Moreover, since any valuation ring $\mathcal{O}$ of F/K contains the field $\overline{K}^c$ of constants, the set of all valuation rings of $F/\overline{K}^c$ is the same as the set of all valuation rings of F/K.

From here on, F/K will always denote an algebraic function field of one variable such that K is the full constant field of F/K.

Definition 2.9 *The (additively written) free abelian group which is generated by the places of F/K is denoted by $\mathcal{D}_F$, the* divisor group *of F/K. The elements of $\mathcal{D}_F$ are called* divisors *of F/K. In other words, a divisor is a formal sum*

$$D = \sum_{\mathfrak{P} \in \mathbb{P}_F} n_{\mathfrak{P}} \mathfrak{P}$$

with $n_{\mathfrak{P}} \in \mathbb{Z}$, almost all $n_{\mathfrak{P}} = 0$.

The *support* of D is defined by

$$\mathrm{supp} D := \{\mathfrak{P} \in \mathbb{P}_F \mid n_{\mathfrak{P}} \neq 0\}.$$

Two divisors $D = \sum_{\mathfrak{P} \in \mathbb{P}_F} n_{\mathfrak{P}} \mathfrak{P}$ and $D' = \sum_{\mathfrak{P} \in \mathbb{P}_F} n'_{\mathfrak{P}} \mathfrak{P}$ are added coefficientwise:

$$D + D' := \sum_{\mathfrak{P} \in \mathbb{P}_F} (n_{\mathfrak{P}} + n'_{\mathfrak{P}}) \mathfrak{P}.$$

We define $\nu_{\mathfrak{P}}(D) := n_{\mathfrak{P}}$. A partial ordering on $\mathcal{D}_F$ is defined by

$$D_1 \leq D_2 :\Longleftrightarrow \nu_{\mathfrak{P}}(D_1) \leq \nu_{\mathfrak{P}}(D_2) \text{ for any } \mathfrak{P} \in \mathbb{P}_F.$$

A divisor $D \geq 0$ is called *positive* (or *effective*). The *degree* of a divisor is defined by

$$\deg D := \sum_{\mathfrak{P} \in \mathbb{P}_F} \nu_{\mathfrak{P}}(D) \cdot \deg \mathfrak{P}$$

and yields a group homomorphism $\deg : \mathcal{D}_F \to \mathbb{Z}$. By proposition 2.11, any nonzero element $x \in F$ has only finitely many zeros and poles in $\mathbb{P}_F$. Thus the following definition makes sense.

Definition 2.10 *Let $0 \neq x \in F$ and denote by $\mathcal{Z}$ (resp. $\mathcal{N}$) the set of zeros (poles) of x in $\mathbb{P}_F$. Then we define*

$$\begin{array}{rcll} (x)_0 & := & \sum_{\mathfrak{P} \in \mathcal{Z}} \nu_{\mathfrak{P}}(x) \mathfrak{P}, & \textit{the} \text{ zero divisor } \textit{of } x, \\ (x)_\infty & := & \sum_{\mathfrak{P} \in \mathcal{N}} -\nu_{\mathfrak{P}}(x) \mathfrak{P}, & \textit{the} \text{ pole divisor } \textit{of } x, \textit{ and} \\ (x) & := & (x)_0 - (x)_\infty, & \textit{the} \text{ principal divisor } \textit{of } x. \end{array}$$

The elements $0 \neq x \in F$ which are constants are characterized by

$$x \in K \Longleftrightarrow (x) = 0.$$

This follows immediately from remark 2.3 (note the general assumption made previously that $K = \overline{K}^c$).

Definition 2.11

$$\mathcal{P}_F := \{(x) \mid 0 \neq x \in F\}$$

is called the group of principal divisors *of F/K. This is a subgroup, since for $x, y \in F \setminus \{0\}$, $(xy) = (x) + (y)$.*

Two divisors are $D, D' \in \mathcal{D}_F$ are called *equivalent*, denoted by $D \equiv D'$, if $D - D' \in \mathcal{P}_F$.

Roughly speaking, the next proposition states that an element $0 \neq x \in F$ has many zeros as poles, provided the zeros and poles are counted properly.

Proposition 2.12 *Let $x \in F \setminus K$. Then*

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

Proof: [Sti93], Theorem I.4.11 □

2.3 The vector space $\mathcal{L}(D)$

Our next definition plays a fundamental role in the theory of algebraic function fields.

Definition 2.12 *For a divisor $D \in \mathcal{D}_F$ we set*

$$\mathcal{L}(D) = \{z \in F \setminus \{0\} \mid (z) \geq -D\} \cup \{0\}.$$

The elements of $\mathcal{L}(D)$ may have poles only at the places of the support of D; more precisely, if $x \in \mathcal{L}(D)$ and $\mathfrak{P}$ is a pole of x, then $\mathfrak{P} \in \text{supp}D$ and $\nu_{\mathfrak{P}}(x) \geq -\nu_{\mathfrak{P}}(D)$. Moreover, x has at most $\deg D$ zeros outside of supp$D$.

Lemma 2.13 *Let $D \in \mathcal{D}_F$. Then $\mathcal{L}(D)$ is a vector space over K.*

Proof: [Sti93], I.4.6 Lemma □

Proposition 2.14 *Let $D \in \mathcal{D}_F$. Then the dimension $\dim_K \mathcal{L}(D)$ of the vector space $\mathcal{L}(D)$ is finite. We will denote $\dim D := \dim_K \mathcal{L}(D)$.*

Proof: [Sti93], I.4.9 Proposition □

Proposition 2.15 *There exists a constant $\gamma \in \mathbb{Z}$ such that, for all divisors $D \in \mathcal{D}_F$, the following holds:*

$$\deg D - \dim D \leq \gamma.$$

Proof: [Sti93] I.4.14. Proposition □

Therefore the following definition makes sense.

Definition 2.13 *The* genus *of F/K is defined by*

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

The genus is the most important invariant of a function field.

Remark 2.4 *The genus of F/K is a non-negative integer.*

Proof: In the definition of g, put $D = 0$. Then $\deg(0) - \dim(0) + 1 = 0$, hence $g \geq 0$. □

Theorem 2.16 (Riemann) *Let F/K be a function field of genus g.*

1. *For any divisor $D \in \mathcal{D}_F$,*
$$\dim D \geq \deg + 1 - g.$$
2. *There is an integer c, depending on F/K, such that*
$$\dim D = \deg D + 1 - g$$
whenever $\deg D \geq c$.

Proof: [Sti93], I.4.17 Theorem □

The Riemann-Roch Theorem

Theorem 2.17 *Let W be a canonical divisor of F/K. Then, for any $D \in \mathcal{D}_F$,*
$$\dim D = \deg D + 1 - g + \dim(W - D).$$

Proof: [Sti93], I.5.15 Theorem □

Corollary 2.18 *For a canonical divisor W, we have*
$$\deg W = 2g - 2 \text{ and } \dim W = g.$$

Proof: [Sti93], I.5.16 Corollary □

Theorem 2.19 *If D is a divisor of F/K of degree $\geq 2g - 1$ then*
$$\dim D = \deg D + 1 - g.$$

Proof: [Sti93], I.5.17 Corollary □

Corollary 2.20 *Let $\mathfrak{P} \in \mathbb{P}_F$. Then there exists $u \in F$ such that $\mathfrak{P}$ is the unique zero (pole) of u.*

Proof: By the preceding theorem we know that there exists an integer n such that $\dim(n\mathfrak{P}) \geq 2$ and consequently there exists $v \in \mathcal{L}(n\mathfrak{P})$ such that $v \notin K$. Now $\mathfrak{P}$ is the unique place of v by the definition of $\mathcal{L}(n\mathfrak{P})$. It is obvious that $\mathfrak{P}$ is the unique pole of v^{-1}. □

2.4 Geometric Goppa Codes

In this section, we describe Goppa's construction of error-correcting codes using algebraic function fields. Let us fix some notation valid for the entire section.

- $F/\mathbb{F}_q$ is an algebraic function field of genus g over the finite field $\mathbb{F}_q$ with q elements,
- $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ are pairwise distinct places of $F/\mathbb{F}_q$ of degree 1,
- $\mathcal{P} = \mathfrak{P}_1 + \ldots + \mathfrak{P}_n$,

- D is a divisor of $F/\mathbb{F}_q$ such that $\mathrm{supp}D \cap \mathrm{supp}\mathcal{P} = \emptyset$.

Definition 2.14 *The* geometric Goppa code $\mathcal{C}_{\mathcal{L}}(\mathcal{P}, D)$ *associated with the divisors* $\mathcal{P}$ *and* D *is defined by*

$$\mathcal{C}_{\mathcal{L}}(\mathcal{P}, D) := \{(x(\mathfrak{P}_1), \ldots, x(\mathfrak{P}_n)) \mid x \in \mathcal{L}(D)\} \subseteq \mathbb{F}_q^n.$$

Note that this definition makes sense: for $x \in \mathcal{L}(D)$, we have $\nu_{\mathfrak{P}_i}(x) \geq 0$ $(i = 1, \ldots, n)$ because $\mathrm{supp}\mathcal{P} \cap \mathrm{supp}D = \emptyset$. The residue class $x(\mathfrak{P}_i)$ of x modulo $\mathfrak{P}_i$ is an element of the residue class field of $\mathfrak{P}_i$. As $\deg \mathfrak{P}_i = 1$, this residue field is $\mathbb{F}_q$, so $x(\mathfrak{P}_i) \in \mathbb{F}_q$.

The geometric Goppa code $\mathcal{C}_{\mathcal{L}}(\mathcal{P}, D)$ is the image of $\mathcal{L}(D)$ under the *evaluation map*

$$ev_{\mathcal{P}} : \left\{ \begin{array}{ccc} \mathcal{L}(D) & \rightarrow & \mathbb{F}_q^n \\ x & \mapsto & (x(\mathfrak{P}_1), \ldots, x(\mathfrak{P}_n)) \end{array} \right.$$

which is $\mathbb{F}_q$-linear.

Proposition 2.21 *The* geometric Goppa code $\mathcal{C}_{\mathcal{L}}(\mathcal{P}, D)$ *is a* $[n, k, d]$ *code with parameters*

$$k = \dim D - \dim(D - \mathcal{P})$$

and

$$d \geq n - \deg D.$$

Especially if $2g - 1 \leq \deg D < n$, *then*

$$k = \deg D - g + 1.$$

Proof: Since the mapping $ev_{\mathcal{P}}$ is a $\mathbb{F}_q$-linear we have

$$k := \dim_{\mathbb{F}_q} ev_{\mathcal{P}}(\mathcal{L}(D)) = \dim_{\mathbb{F}_q}(\mathcal{L}(D)) - \dim_{\mathbb{F}_q} \ker ev_{\mathcal{P}}.$$

We have $ev_{\mathcal{P}}(z) = 0$ if and only if $z \in \mathcal{L}(D - \mathcal{P})$. Therefore $k = \dim D - \dim(D - \mathcal{P})$. Let now $u \in \mathcal{L}(D)$. By the definition of $\mathcal{L}(D)$ u has at most $\deg D$ zero outside the support of D. It is now clear that there exist at most $n - \deg D$ places of the support of D which are zeros of u. Consequently the weight $w := w(ev_{\mathcal{P}}(u))$ of the code word $ev_{\mathcal{P}}(u)$ is such that $w \geq n - \deg D$. This shows that $d \geq n - \deg D$. Let now $2g - 1 \leq \deg D < n$. Since $\deg D < n = \deg \mathcal{P}$ we have $\mathcal{L}(D - \mathcal{P}) = \{0\}$ and therefore $k = \dim D = \deg D - g + 1$ by the Riemann-Roch theorem since $\deg D \geq 2g - 1$. □

Construction of Goppa-Codes

If $\{x_1, x_2, \ldots, x_l\}$ is a basis of $\mathcal{L}(D)$ then the matrix

$$G := \begin{pmatrix} x_1(\mathfrak{P}_1) & x_1(\mathfrak{P}_2) & \ldots & x_1(\mathfrak{P}_l) \\ x_2(\mathfrak{P}_1) & x_2(\mathfrak{P}_2) & \ldots & x_2(\mathfrak{P}_l) \\ \vdots & \vdots & \ddots & \vdots \\ x_n(\mathfrak{P}_1) & x_n(\mathfrak{P}_2) & \ldots & x_n(\mathfrak{P}_l) \end{pmatrix}$$

is a generator matrix for the geometric Goppa code $\mathcal{C}_{\mathcal{L}}(\mathcal{P}, D)$. It is now obvious what we need to construct geometric Goppa codes for a given algebraic function field $F/\mathbb{F}_q$:

1. Find the places of degree 1 and construct the divisor $\mathcal{P}$,
2. Construct a divisor D such that supp$D$ and supp$\mathcal{P}$ are disjoint,
3. Compute a basis $B := \{x_1, x_2, \ldots, x_l\}$ of the vector space $\mathcal{L}(D)$,
4. Evaluate the functions $x_i \in B$ at every place of the support of $\mathcal{P}$.

Chapter 3

Algebraic curves

In this chapter we describe briefly some elementary objects which arise in the study of algebraic geometry and present some basic facts about algebraic curves. We will see that the function field $\overline{K}(\mathcal{C})$ of a curve $\mathcal{C}$ is a an algebraic function field of one variable. This fact permits us to use several concepts of algebraic geometry to get more information about our algebraic function field of one variable.

3.1 Affine curves

Definition 3.1 *Affine n-space over K is the set of n-tuples*

$$\mathbb{A}^n = \mathbb{A}^n(\overline{K}) = \{P = (a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in \overline{K}\}.$$

Similarly, the set of K-rational points *in $\mathbb{A}^n$ is the set*

$$\mathbb{A}^n(K) = \{P = (a_1, \ldots, a_n) \in \mathbb{A}^n \mid a_1, \ldots, a_n \in K\}.$$

Notice that the Galois group $\mathcal{G}_{\overline{K}/K}$ acts on $\mathbb{A}^n$; for $\sigma \in \mathcal{G}_{\overline{K}/K}$ and $P \in \mathbb{A}^n$,

$$P^\sigma = (a_1^\sigma, \ldots, a_n^\sigma).$$

Then $\mathbb{A}^n(K)$ may be characterized by

$$\mathbb{A}^n(K) = \{P \in \mathbb{A}^n \mid P^\sigma = P \text{ for all } \sigma \in \mathcal{G}_{\overline{K}/K}\}.$$

Let $\overline{K}[\underline{X}] = \overline{K}[X_1, \ldots, X_n]$ be the polynomial ring in n variables, and let $I \subset \overline{K}[\underline{X}]$ be an ideal. To each such ideal I we associate a subset of $\mathbb{A}^n$,

$$\mathcal{V}(I) = \{P \in \mathbb{A}^n \mid G(P) = 0 \text{ for all } G \in I\}.$$

Definition 3.2 *An (affine)* algebraic set *is any set of the form $\mathcal{V}(I)$. If $V \subset \mathbb{A}^n$ is an algebraic set then the ideal of V is given by*

$$\mathcal{I}(V) = \{F \in \overline{K}[\underline{X}] \mid F(P) = 0 \textit{ for all } P \in V\}.$$

An algebraic set V is set *defined over* K if its ideal $\mathcal{I}(V)$ can be generated by polynomials in $K[\underline{X}]$. We denote this by V/K. If V is defined over K, the *set of K-rational points of V* is the set

$$V(K) = V \cap \mathbb{A}^n(K).$$

Remark 3.1 *Note that by the Hilbert basis theorem, all ideals in $\overline{K}[\underline{X}]$ and $K[\underline{X}]$ are finitely generated (i.e. the rings $\overline{K}[\underline{X}]$ and $K[\underline{X}]$ are noetherian).*

Let V be an algebraic set, and consider the ideal

$$\mathcal{I}(V/K) = \{G \in K[\underline{X}] \mid G(P) = 0 \text{ for all } P \in V\} = \mathcal{I}(V) \cap K[\underline{X}].$$

Then we see that V is defined over K if and only if

$$\mathcal{I}(V) = \mathcal{I}(V/K)\overline{K}[\underline{X}].$$

Let V be an algebraic set and $\sigma \in \mathcal{G}_{\overline{K}/K}$. Consider the ideal

$$\mathcal{I}(V)^\sigma := \{G^\sigma \mid G \in \mathcal{I}(V)\}.$$

It is obvious that

$$V \text{ is defined over } K \iff \mathcal{I}(V) = \mathcal{I}(V)^\sigma \text{ for all } \sigma \in \mathcal{G}_{\overline{K}/K}.$$

Definition 3.3 *An affine algebraic set V is called an affine* variety *if $\mathcal{I}(V)$ is a prime ideal in $\overline{K}[\underline{X}]$. Note that if V is defined over K, it is not enough to check that $\mathcal{I}(V/K)$ is prime.*

Definition 3.4 *Let V be an affine variety. The* coordinate ring *of V is defined by*

$$\overline{K}[V] := \overline{K}[\underline{X}]/\mathcal{I}(V).$$

If V is defined over K, the coordinate ring *of V/K is defined by*

$$K[V] := K[\underline{X}]/\mathcal{I}(V/K).$$

Remark 3.2 *The coordinate ring of a variety V can be interpreted as a set of functions with values in $\overline{K}$ which are defined at all points of V. Let $f \in \overline{K}[\mathcal{C}]$ and $F \in \overline{K}[\underline{X}]$ such that $f = F + \mathcal{I}(V) \in \overline{K}[V]$. We call $f(P) := F(P)$ the* evaluation *of f at the point P. It is clear that the definition of the evaluation does not depend on choice of the representative F.*

Since the ideal $\mathcal{I}(V)$ of a variety V is a prime ideal the coordinate ring $\overline{K}[V]$ integer and we can construct the quotient field $Quot(\overline{K}[V])$ of $\overline{K}[V]$.

Definition 3.5 *Let V be an affine variety. The* function field *of V, denoted by $\overline{K}(V)$, is the quotient field $Quot(\overline{K}[\mathcal{C}])$. If V is defined over K, the* function field *of V/K, denoted by $K(V)$, is the quotient field $Quot(K[V])$.*

Definition 3.6 *Let $V \subseteq \mathbb{A}^m$ and $W \subseteq \mathbb{A}^n$ be two varieties. We say V and W are* birationally isomorphic *if their function fields $\overline{K}(V)$ and $\overline{K}(W)$ are $\overline{K}$-isomorphic.*

Remark 3.3 *Let V/K be an affine variety. It is clear that $K[V]$ and $K(V)$ can be embedded canonically in, respectively, $\overline{K}[V]$ and $\overline{K}(V)$. Therefore we will always consider $K[V]$ as a subring of $\overline{K}[V]$ and $K(V)$ as a subfield of $\overline{K}(V)$.*

Since V is defined over K, the Galois group $\mathcal{G}_{\overline{K}/K}$ takes $\mathcal{I}(V)$ into itself (by acting on the coefficients of the polynomials of the ideal) and we can extend the action of $\mathcal{G}_{\overline{K}/K}$ to $\overline{K}[V]$ and $\overline{K}(V)$. One can check easily that $K[V]$ and $K(V)$ are, respectively, the subsets of $\overline{K}[V]$ and $\overline{K}(V)$ fixed by $\mathcal{G}_{\overline{K}/K}$.

Definition 3.7 *Let V be an affine variety and $P \in V$. The* local ring of the point *P is the ring*

$$\mathcal{O}_P(V) := \{f/g \in \overline{K}(V) \mid f, g \in \overline{K}[V], g(P) \neq 0\}.$$

Let $u \in \mathcal{O}_P(V)$ and $f, g \in \overline{K}[V]$ such that $u = f/g$ where $g(P) \neq 0$. We call $u(P) := f(P)/g(P)$ the evaluation *of u at the point P.*

Remark 3.4 *We can consider $\mathcal{O}_P(V)$ as the set of all functions which are defined at the point P. Let M_P be the maximal ideal corresponding to the point $P \in \mathbb{A}^2$. Then $\mathcal{I}(V) \subseteq M_P$ and $\overline{M}_P := M_P + \mathcal{I}(V)$ is a maximal ideal of the coordinate ring $\overline{K}[V]$. We have*

$$\mathcal{O}_P(V) := \{f/g \mid f, g \in \overline{K}[V], g \notin \overline{M}_P\}.$$

The ring $\mathcal{O}_P(V)$ is the localization $\overline{K}[V]_{\overline{M}_P}$ of $\overline{K}[V]$ at the maximal ideal $\overline{M}_P$ and has the unique maximal ideal

$$\begin{aligned} \mathcal{M}_P(V) &:= \{f, g \in \overline{K}(V) \mid f, g \in \overline{K}[V], f \in \overline{M}_P, g \notin \overline{M}_P\} \\ &= \{f, g \in \overline{K}(V) \mid f, g \in \overline{K}[V], f(P) = 0, g(P) \neq 0\} \end{aligned}$$

The function field $\overline{K}(V)$ of a variety is an extension field of finite type (i.e. there exist $x_1, \ldots, x_n \in \overline{K}(V)$ such that $\overline{K}(V) = \overline{K}(x_1, \ldots, x_n)$). Especially the transcendence degree of $\overline{K}(V)$ over $\overline{K}$ is finite.

Definition 3.8 *Let V be a variety. The* dimension *of the variety V, denoted by* $\dim(V)$*, is the transcendence degree of $\overline{K}(V)$ over $\overline{K}$.*

Definition 3.9 *An* affine curve *$\mathcal{C} \subset \mathbb{A}^n$ is an affine variety of dimension* 1.

Definition 3.10 *Let $C \in K[X, Y]$ be an absolutely irreducible polynomial and consider the variety*

$$\mathcal{C} := \{C = 0\} = \{P \in \mathbb{A}^2 \mid C(P) = 0\}.$$

It is clear that the function field $\overline{K}(\mathcal{C})$ is of transcendence degree one over $\overline{K}$. The variety $\mathcal{C}$ is therefore a curve and since it is contained in the affine plane $\mathbb{A}^2$, we say that it is an affine plane curve. *Since $C \in K[X, Y]$ the curve $\mathcal{C}$ is defined over K.*

In studying any geometric object, one is naturally interested in knowing whether it looks reasonably "smooth". The next definition formalizes this notion in terms of the usual Jacobian criterion for the existence of a tangent plane.

Definition 3.11 *Let V be a variety, $P \in V$, and $G_1, \ldots, G_m \in \overline{K}[\underline{X}]$ a set of generators for $\mathcal{I}(V)$. Then V is* non-singular *(or* smooth*)* at *P if the $m \times n$ matrix*

$$(\partial G_i / \partial X_j(P))_{1 \leq i \leq m, 1 \leq j \leq n}$$

has rank $n - \dim(V)$. If V is non-singular at every point, we say that V is non-singular *(or* smooth*).*

For an affine plane curve the situation is much simpler.

Proposition 3.1 *Let $\mathcal{C} := \{C = 0\}$ be an affine plane curve. Let C_X and C_Y denote the derivatives with respect to X and Y. Then*

$$P = (a, b) \in \mathcal{C} \text{ is simple } \iff C_X(a, b) \neq 0 \text{ or } C_Y(a, b) \neq 0.$$

We want to establish a correspondence between points of an affine plane curve $\mathcal{C} := \{C = 0\}$ and places of its function field $\overline{K}(\mathcal{C})$. To do this we study local rings of points. One of the most important properties of a point of $\mathcal{C} \subset \mathbb{A}^2$ is its *multiplicity*. Let $P := (0, 0) \in \mathbb{A}^2$. We can write

$$C = C_{m_1} + C_{m_2} + \ldots + C_{m_d}$$

where $m_1 < m_2 < \ldots < m_d$ and C_{m_i} is a homogeneous polynomial of degree m_i for $i = 1, 2, \ldots, d$. We call C_{m_1} the *initial form* of C and denote it by $\mathrm{Init}(C)$. The *multiplicity* of the point $P = (0, 0)$ of C, denoted by $m_P(C)$, is the degree of the initial form, $m_{(0,0)}(C) := \deg \mathrm{Init}(C)$. If $P = (a, b)$, the multiplicity of the point P of C is defined by $m_P(C) := m_{(0,0)}(C(X + a, Y + b))$. It is clear that $C(P) = 0$ if and only if $m_P(C) > 0$.

Recall that every homogeneous polynomial of $\overline{K}[X, Y]$ factors in linear forms. If $P = (0, 0)$ and $m_P(C) > 0$ then we have

$$\mathrm{Init}(C) = \prod_{i=1}^{m_P(C)} (\alpha_i X + \beta_i Y).$$

Geometrically speaking, the distinct factors $L_j = \alpha_j X + \beta_j Y$ of $\mathrm{Init}(C)$ define tangents in at the affine plane curve $\mathcal{C}$ at the point P.

Definition 3.12 *Let $\mathcal{C} := \{C = 0\}$ be an affine plane curve and $P \in \mathcal{C}$. We call $m_P(\mathcal{C}) := m_P(C)$ the* multiplicity *of the point P.*

Theorem 3.2 *Let $\mathcal{C} := \{C = 0\}$ be an affine plane curve and $P \in \mathcal{C}$. The point P is a simple point of $\mathcal{C}$ if and only if $\mathcal{O}_P(\mathcal{C})$ is a discrete valuation ring. In this case, if $T = \alpha X + \beta Y + \gamma$ is any line through P which is not tangent to $\mathcal{C}$ at P then the image t of T in $\mathcal{O}_P(\mathcal{C})$ is a local parameter of $\mathcal{O}_P(\mathcal{C}^*)$.*

Proof: [Ful69] Theorem 1 on page 70 □

Let $\mathcal{C} := \{C = 0\}$ be an affine plane curve and $P := (a, b) \in \mathcal{C}$. Let C_X and C_Y denote the derivatives of C with respect to X and Y. We have

$$m_P(\mathcal{C}) = 1 \iff C_X(a, b) \neq 0 \text{ or } C_Y(a, b) \neq 0.$$

The right side of this equivalence corresponds to the definition of a simple point of an affine plane curve. The following proposition summarizes the equivalent conditions for a simple point.

Proposition 3.3 *Let $\mathcal{C} := \{C = 0\}$ be an affine plane curve and $P := (a, b) \in \mathcal{C}$. Then the following assertions are equivalent*

1. *P is simple.*
2. *$C_X(a, b) \neq 0$ or $C_Y(a, b) \neq 0$.*
3. *$m_P(\mathcal{C}) = 1$.*
4. *$\mathcal{O}_P(\mathcal{C})$ is a discrete valuation ring.*

Proposition 3.4 *The multiplicity of a point $P \in \mathcal{C}$ depends uniquely on the local ring $\mathcal{O}_P(\mathcal{C})$. Indeed, it can be show that there exists a sufficiently large N such that for all $n \geq N$*

$$m_P(\mathcal{C}) = \dim_{\overline{K}} \mathcal{M}_P(\mathcal{C})^n / \mathcal{M}_P(\mathcal{C})^{n+1}$$

where $\mathcal{M}_P(\mathcal{C})$ is the maximal ideal of $\mathcal{O}_P(\mathcal{C})$.

Proof: [Per95] Proposition 4.6 on page 113 or [Ful69] Theorem 2 on page 71. □

3.2 Projective plane curves

On the set $\mathbb{A}^3 \setminus \{(0, 0, 0)\}$, an equivalence relation $\equiv$ is given by

$$(a_0, a_1, a_2) \equiv (b_0, b_1, b_2) \text{ if there exists } 0 \neq \lambda \in \overline{K} \text{ such that } a_i = \lambda b_i \text{ for } i = 0, 1, 2.$$

The equivalence class of (a_1, a_2, a_3) with respect to the equivalence relation $\equiv$ is denoted by $(a_1 : a_2 : a_3)$. The *projective plane* $\mathbb{P}^2$ is the set of equivalence classes

$$\mathbb{P}^2 := \{(a_1 : a_2 : a_3) \mid a_i \in \overline{K}, \text{ not all } a_i = 0\}.$$

An element $P = (a_1 : a_2 : a_3) \in \mathbb{P}^2$ is called a point, and a_0, a_1, a_2 are called its *homogeneous coordinates*. We say a point $P = (a : b : c)$ is at *infinity* if $a_2 = 0$. If $V \subset \mathbb{P}^2$ we denote by V_∞ the set $V_\infty := \{(a : b : c) \in V \mid c = 0\}$. For $i = 0, 1, 2$ we set

$$U_i := \{(a_0 : a_1 : a_2) \in \mathbb{P}^2 \mid a_i \neq 0\}.$$

We call the sets U_i the *standard open sets* of $\mathbb{P}^2$. For $i = 0, 1, 2$ we have the bijective maps

$$\pi_i : \begin{cases} \mathbb{A}^2 & \to & U_i \\ (a, b) & \mapsto & \begin{cases} (1 : a : b) & \text{if } i = 0, \\ (a : 1 : b) & \text{if } i = 1, \\ (a : b : 1) & \text{if } i = 2. \end{cases} \end{cases}$$

The plane $\mathbb{P}^2$ is covered by the standard open sets U_0, U_1 and U_2. They are canonically isomorphic to $\mathbb{A}^2$.

The elements of $\overline{K}[U, V, W]$ can not be considered as functions defined on the projective plane $\mathbb{P}^2$ since every point of $\mathbb{P}^2$ can be represented by infinitely many homogeneous polynomials. For $d \in \mathbb{N}$ we set

$$S_d := \{G \in \overline{K}[U, V, W] \mid G \text{ is a homogeneous polynomial of degree } d\}.$$

If $G \in S_d$ we say that $P = (a : b : c) \in \mathbb{P}^2$ is a *zero* of G, denoted by $G(P) = 0$, if $G(a, b, c) = 0$. Since G is homogeneous we have $G(\lambda a, \lambda b, \lambda c) = \lambda^d G(a, b, c)$ for all $\lambda \in \overline{K} \setminus \{0\}$ and it is now clear that the definition does not depend on the coordinates of P.

Definition 3.13 *A* projective plane curve $\mathcal{C}^* \subset \mathbb{P}^2$ *is the zero set of a homogeneous irreducible polynomial* $C^* \in \overline{K}[U,V,W]$. *If* $C^* \in K[U,V,W]$, *we say the curve* $\mathcal{C}^*$ *is* defined over K *and we write* $\mathcal{C}^*/K$.

Let $C^* \in \overline{K}[U,V,W]$ be a homogeneous irreducible polynomial. Let $\mathcal{I}(\mathcal{C}) := \langle C^* \rangle$. The *coordinate ring* of $\mathcal{C}^*$ is the ring

$$\overline{K}[\mathcal{C}^*] := \overline{K}[U,V,W]/\mathcal{I}(\mathcal{C}^*).$$

If $\mathcal{C}^*$ is defined over K, the *coordinate ring* of $\mathcal{C}^*/K$ is the ring

$$K[\mathcal{C}^*] := K[U,V,W]/\mathcal{I}(\mathcal{C}^*/K).$$

Definition 3.14 *Let* $\mathcal{C}^* := \{C^* = 0\}$ *be a projective plane curve. We say* $g \in \overline{K}[\mathcal{C}^*] \setminus \{0\}$ *is a* form of degree d *if there exists a homogeneous polynomial* $G \in S$ *of degree* d *such that* $g = G + \langle C^* \rangle$. *We define* $\deg g := d$ *and write* $g(P) \neq 0$ *if* $P \in \mathcal{C}^*$ *such that* $G(P) \neq 0$. *The same definitions apply to* $K[\mathcal{C}^*]$ *if* $\mathcal{C}^*$ *is defined over* K.

The degree of a form is well-defined: if G' and G are two non-zero homogeneous polynomials of different degrees such that $G - G' \in \langle C^* \rangle$ then $G \in \langle C^* \rangle$ and $G' \in \langle C^* \rangle$ since otherwise the polynomial C^* would not be homogeneous.

We can not consider the elements of $\overline{K}[\mathcal{C}^*]$ as functions defined on $\mathcal{C}^*$ since the value would depend on the representation of the equivalence class. On the contrary, let $d \in \mathbb{N}$ and $G, H \in S_d$. Let $P = (a : b : c) \in \mathcal{C}^*$ and suppose that $H(P) \neq 0$. Then for all $\lambda \in \overline{K} \setminus \{0\}$ we have

$$\frac{G(\lambda a, \lambda b, \lambda c)}{H(\lambda a, \lambda b, \lambda c)} = \frac{\lambda^d G(a,b,c)}{\lambda^d H(a,b,c)} = \frac{G(a,b,c)}{H(a,b,c)}.$$

and the map $G/H \to (G/H)(P) := \frac{G(a,b,c)}{H(a,b,c)}$ is well-defined.

Definition 3.15 *Let* $\mathcal{C}^*$ *be a projective curve. The* function field $\overline{K}(\mathcal{C}^*)$ *of the curve* $\mathcal{C}^*$ *is the subfield of the quotient field of* $\overline{K}[\mathcal{C}^*]$ *given by*

$$\overline{K}(\mathcal{C}^*) := \{f/g \mid f, g \in \overline{K}[\mathcal{C}^*] \text{ are forms of the same degree and } g \neq 0\}.$$

If $\mathcal{C}^*$ *is defined over* K, *the the* function field $K(\mathcal{C}^*)$ *of* $\mathcal{C}^*/K$ *is the field*

$$K(\mathcal{C}^*) := \{f/g \mid f, g \in K[\mathcal{C}^*] \text{ are forms of the same degree and } g \neq 0\}.$$

We say $u \in \overline{K}(\mathcal{C})$ is *defined* at the point $P \in \mathcal{C}^*$ if there exist two forms f and g of the same degree such that $u = f/g$ and $g(P) \neq 0$. If $G, H \in S_d$ are such that $g = G + \langle C^* \rangle$ and $h = H + \langle C^* \rangle$ we *evaluate* u at the point P by setting $u(P) := (G/H)(P)$.

Definition 3.16 *Let* $\mathcal{C}^*$ *be a plane projective curve and* $P \in \mathcal{C}^*$. *The* local ring of the point P *is defined by*

$$\mathcal{O}_P(\mathcal{C}^*) := \{f/g \mid f, g \in \overline{K}[\mathcal{C}^*] \text{ are forms of the same degree and } g(P) \neq 0\}.$$

The local ring $\mathcal{O}_P(\mathcal{C}^*)$ of a point P is the set of all functions defined at the point P. It is clear that $\mathcal{O}_P(\mathcal{C}^*)$ is a local ring and that its unique maximal ideal is

$$\mathcal{M}_P(\mathcal{C}^*) = \{f/g \in \mathcal{O}_P(\mathcal{C}^*) \mid f(P) = 0\}.$$

Definition 3.17 *Let $\mathcal{C}$ and $\mathcal{C}'$ be two plane curves (affine or projective). We say that $\mathcal{C}$ is* birational *to $\mathcal{C}'$ if their function fields are $\overline{K}$-isomorphic.*

We show that any projective plane curve is birational to some affine plane curve. Let $\mathcal{C}^* := \{C^* = 0\}$ be a projective plane curve and suppose that $\mathcal{C}^* \neq W$. Set $C := C^*(X, Y, 1)$. The corresponding curve is

$$\mathcal{C} := \pi_2^{-1}(\mathcal{C}^*) = \{Q \in \mathbb{A}^2 \mid C(Q) = 0\}.$$

The irreducibility of C follows from the irreducibility of C^*. Therefore $\mathcal{C}$ is an affine plane curve. Moreover, $\mathcal{C}^*$ is birational to $\mathcal{C}$. It is easy to show that

$$\varphi_2 : \begin{cases} \overline{K}(\mathcal{C}^*) & \to & \overline{K}(\mathcal{C}) \\ \frac{G(u,v,w)}{H(u,v,w)} & \mapsto & \frac{G(x,y,1)}{H(x,y,1)} \end{cases}$$

is a $\overline{K}$-isomorphism where u,v and w denote the residual images of, respectively, U,V and W in $\overline{K}[\mathcal{C}^*]$ and where x and y denote the residual images of, respectively, X and Y in $\overline{K}[\mathcal{C}]$. Similarly we define the $\overline{K}$-isomorphisms φ_i and conclude that $\mathcal{C}_i := \pi_i^{-1}(\mathcal{C}^*)$ is an affine plane curve birational to $\mathcal{C}^*$.

Conversely, let $\mathcal{C} := \{C = 0\}$ be an affine plane curve defined by the polynomial

$$C = \sum_{l=0}^{d} \sum_{l=i+j} \alpha_{i,j} X^i Y^j \in \overline{K}[X, Y].$$

We set

$$C^* := \sum_{l=0}^{d} \sum_{l=i+j} \alpha_{i,j} U^i V^j W^{(d-l)} \in \overline{K}[U, V, W]$$

and

$$\mathcal{C}^* := \{C^* = 0\}.$$

Since $C(X, Y) = C^*(X, Y, 1)$ it is clear that C^* is irreducible. We show now the isomorphism. Let $f/g \in \overline{K}(\mathcal{C})$ and $F, G \in \overline{K}[X, Y]$ with $f = F + \langle C \rangle$ and $g = G + \langle C \rangle$. Then

$$\begin{cases} \overline{K}(\mathcal{C}) & \longrightarrow & \overline{K}(\mathcal{C}^*) \\ f/g & \mapsto & w^{\deg G - \deg F} F^*(u, v, w)/G^*(u, v, w) \end{cases}$$

is the desired isomorphism. The projective plane curve $\mathcal{C}^*$ is called the *projective closure* of the affine plane of $\mathcal{C}$. For the relation between a curve and its projective closure see [Kun85] Lemma 2.12 on page 70.

Remark 3.5 *Let $\mathcal{C}^*$ be a projective plane curve. For $i = 0, 1, 2$ we have shown that $\mathcal{C}_i := \pi_i^{-1}(\mathcal{C}^*)$ is an affine plane curve which is birationally isomorphic to $\mathcal{C}^*$. Note that there is a bijective correspondence between $\mathcal{C}_i$ and $\mathcal{C}^* \cap U_i$. Moreover, if $P \in \mathcal{C}^* \cap U_i$ and $P_i \in \mathcal{C}_i$ is such that $\pi(P_i) = P$ then*

$$\varphi_i(\mathcal{O}_P(\mathcal{C}^*)) = \mathcal{O}_{P_i}(\mathcal{C}_i).$$

The local rings $\mathcal{O}_P(\mathcal{C}^*)$ and $\mathcal{O}_{P_i}(\mathcal{C}_i)$ are isomorphic. Thus questions about a projective plane curve $\mathcal{C}^*$ near a point P can be reduced to questions about the affine plane curve $\mathcal{C}$.

We observe that $\Gamma_2 := (u/w, v/w)$ is a coordinate pair of the function field $\overline{K}(\mathcal{C}^*)$ since $\varphi_2(u/w) = x$ and $\varphi_2(v/w) = y$ and $\overline{K}(x, y) = \overline{K}(\mathcal{C}) \cong \overline{K}(\mathcal{C}^*)$. Similarly, we verify that $\Gamma_1 := (u/v, w/v)$ and $\Gamma_0 := (v/u, w/u)$ are coordinate pairs of $\overline{K}(\mathcal{C}^*)$. We call the coordinate pairs Γ_i for $i = 0, 1, 2$ the standard coordinates pairs *of the function field $\overline{K}(\mathcal{C}^*)$.*

Since the function field of an affine plane curve is an algebraic function field in one variable we have the following proposition.

Proposition 3.5 *The function field of a projective plane curve is an algebraic function field in one variable.*

Chapter 4

Brill-Noether algorithm

The aim of this chapter is to present the Brill-Noether algorithm which computes a basis of the vector space $\mathcal{L}(D)$ associated to the divisor D of the function field of a plane curve.

Since K is a perfect field, there always exist $x, y \in F$ such that $F = K(x, y)$. Let $C \in K[X, Y]$ be the irreducible polynomial such that $C(x, y) = 0$. Since K is the full constant field of F, the polynomial C is absolutely irreducible. Let $\overline{F}$ be the composition field $\overline{F} := \overline{K}F$ where $\overline{K}$ is an algebraic closure of K. Let $\mathcal{C}/K$ be the affine curve $\mathcal{C} := \{C = 0\}$ which is defined over K. It is clear that the function field $\overline{K}(\mathcal{C})$ of $\mathcal{C}$ is isomorphic to the algebraic function field $\overline{F}$ and the function field $K(\mathcal{C})$ of $\mathcal{C}/K$ is isomorphic to the algebraic function field F. We see that an algebraic function field is always isomorphic to the function field of an affine plane curve. Given the function field of a curve $\mathcal{C} \subset \mathbb{A}^n$ with $n \geq 3$ it is not always easy to find a coordinate pair of this field. We will not treat this problem here. Our algebraic function field $\overline{F}$ will always be the function field of a projective plane curve defined over K. In this case we know the standard coordinate pairs. Much of the work of this section can be viewed as methods for finding new coordinate pairs from some already known coordinate pair (blowing up points). The defining polynomials of the new coordinate pair determine affine plane curves with function fields isomorphic to $\overline{F}$. The new coordinate pairs will give us new information on our function field $\overline{F}$.

> From both an algebraic and algorithmic point of view it will be very useful to identify the algebraic function field $\overline{F}$ with all function fields $\overline{K}(\mathcal{C})$ of affine plane curves $\mathcal{C}$ which are $\overline{K}$-isomorphic to $\overline{F}$ ($\overline{F} \cong \overline{K}(\mathcal{C})$). This will permit us to compare local rings of points of different curves. We will need this when we blow up singular points.

The Brill-Noether algorithm is only defined when the field K is algebraically closed. But, as we will see in section 4.8.1, "Constant field extensions", it is always possible to associate to a divisor D of the function field $K(\mathcal{C})$ a divisor $\overline{D}$ of the function field $\overline{K}(\mathcal{C})$ such that

1. $\dim_K \mathcal{L}(D) = \dim_{\overline{K}} \mathcal{L}(\overline{D})$,
2. there exists a basis of $\mathcal{L}(\overline{D})$ consisting of elements of $K(\mathcal{C})$, and
3. any basis of $\mathcal{L}(\overline{D})$ consisting of elements of $K(\mathcal{C})$ is a basis of $\mathcal{L}(D)$.

Thus to compute a basis of $\mathcal{L}(D)$ we apply the Brill-Noether algorithm to the divisor $\overline{D}$ and gurantee that the basis consists of elements of $K(\mathcal{C})$.

4.1 Points versus places

Definition 4.1 (Coordinate pair of $\overline{F}$) *A pair $\Gamma := (x, y) \subset \overline{F}$ such that $\overline{F} = \overline{K}(x, y)$ is called a* coordinate pair *of $\overline{F}$. The irreducible polynomial $C_\Gamma \in \overline{K}[X, Y]$ such that $C_\Gamma(x, y) = 0$ is called the* defining polynomial *of $\overline{F}$ with respect to Γ. We associate to the coordinate pair Γ the affine plane curve*

$$\mathcal{C}_\Gamma := \{(a, b) \in \mathbb{A}^2 \mid C_\Gamma(a, b) = 0\}.$$

We say that Γ is defined over *K, denoted by Γ/K, if and only if $C_\Gamma \in K[X, Y]$ and $F = K(x, y)$.*

Let $\mathcal{C} := \{C = 0\}$ be an affine plane curve such that $\overline{K}(\mathcal{C}) \cong \overline{F}$. There exist infinitely many isomorphisms from $\overline{K}(\mathcal{C})$ to $\overline{F}$. On the contrary, by choosing a coordinate pair $\Gamma := (x, y)$ of $\overline{F}/\overline{K}$ such that $\mathcal{C} = \mathcal{C}_\Gamma$, we fix the isomorphism

$$\varphi_\Gamma : \begin{cases} \overline{K}(\mathcal{C}) & \to & \overline{F} \\ \frac{F(\overline{X},\overline{Y})}{G(\overline{X},\overline{Y})} & \mapsto & \frac{F(x,y)}{G(x,y)} \end{cases}$$

which maps $\overline{X}$ and $\overline{Y}$ (the residual images of X and Y in the coordinate ring $\overline{K}[\mathcal{C}]$) to, respectively, x and y. If Γ is defined over K then we can restrict φ_Γ to the field $K(\mathcal{C})$ and obtain the isomorphism $\varphi_{\Gamma/K} : K(\mathcal{C}) \to F$.

As we have seen we can associate to a coordinate pair $\Gamma := (x, y)$ of $\overline{F}/\overline{K}$ the affine plane curve $\mathcal{C}_\Gamma$ and obtain thereby the isomorphism $\varphi_\Gamma : \overline{K}(\mathcal{C}_\Gamma) \to \overline{F}$. This permits us to carry over all concepts of curves to the algebraic function field $\overline{F}$.

Remark 4.1 *Let $\Gamma := (x, y)$ be a coordinate pair and $\mathcal{C} := \mathcal{C}_\Gamma$ the associated curve. Let $P := (a, b)$ be a point of $\mathcal{C}$ and $\mathcal{O}_P(\mathcal{C})$ be the local ring of P. Since*

$$\mathcal{O}_P(\mathcal{C}) := \overline{K}[\overline{X}, \overline{Y}]_{\langle \overline{X}-a, \overline{Y}-b \rangle},$$

it is clear that

$$\varphi_\Gamma(\mathcal{O}_P(\mathcal{C})) = \overline{K}[x, y]_{\langle x-a, y-b \rangle}.$$

We introduce now the notion of points of function fields.

Definition 4.2 (Point of the function field $\overline{F}/\overline{K}$) *A* point *of $\overline{F}/\overline{K}$ is a pair $P := (a, b; x, y)$ where $\Gamma = (x, y)$ is a coordinate pair of $\overline{F}/\overline{K}$ and (a, b) is a point of the curve $\mathcal{C}_\Gamma$ associated to Γ. The localization of $\overline{K}[x, y]$ at the maximal ideal $\langle x - a, y - b \rangle$*

$$\mathcal{O}_P = \overline{K}[x, y]_{\langle x-a, y-b \rangle}$$

is called the local ring *of P. Its maximal ideal is denoted by $\mathcal{M}_P$. It is generated by $x - a$ and $y - b$. We call the set*

$$\mathcal{Z}(\Gamma) := \{(a, b; x, y) \mid (a, b) \in \mathcal{C}_\Gamma\}$$

the point set of $\overline{F}/\overline{K}$ determined by the coordinate pair Γ.

Let $\Gamma = (x, y)$ be a pair of coordinates of $\overline{F}/\overline{K}$ and $P = (a, b; x, y) \in \mathcal{Z}(\Gamma)$. The point P inherits all definitions and all local properties of the point (a, b) of the curve $\mathcal{C}_\Gamma$ via the isomorphism φ_Γ. For example, the point P is simple if and only if $(a, b) \in \mathcal{C}_\Gamma$ is simple and the *multiplicity* of P, denoted

by m_P, is the multiplicity $m_{(a,b)}(\mathcal{C}_\Gamma)$ of $(a,b) \in \mathcal{C}_\Gamma$. If $u \in \mathcal{O}_P$ then there exist $F, G \in \overline{K}[X,Y]$ such that $u = F(x,y)/G(x,y)$ and $G(a,b) \neq 0$. We call $u(P) := F(a,b)/G(a,b)$ the *evaluation* of u at P. It is clear that this definition does not depend on the choice of the polynomials F and G.

Two distinct points $P_1 := (a_1, b_1; x, y)$ and $P_2 := (a_2, b_2; x, y)$ of $\mathcal{Z}(\Gamma)$ yield distinct local rings as they correspond to two different points (a_1, b_1) and (a_2, b_2) of the curve $\mathcal{C}_\Gamma$. The definition of a point of $\overline{F}/\overline{K}$ permits us to compare points corresponding to two points of different curves. Now if (x_1, y_1) and (x_2, y_2) are different coordinate pairs of $\overline{F}/\overline{K}$ then there may exist two different points $P_1 := (a_1, b_1; x_1, y_1) \in \mathcal{Z}((x_1, y_1))$ and $P_2 := (a_2, b_2; x_2, y_2) \in \mathcal{Z}((x_2, y_2))$ of $\overline{F}/\overline{K}$ such that $\mathcal{O}_{P_1} = \mathcal{O}_{P_2}$. Therefore we define the following equivalence relation.

Definition 4.3 (Equivalent points) *Let P_1 and P_2 be two points of $\overline{F}/\overline{K}$. We say that P_1 and P_2 are* equivalent, *denoted by $P_1 \equiv P_2$, if $\mathcal{O}_{P_1} = \mathcal{O}_{P_2}$.*

Remark 4.2 (Affine transformations) *Let $\Gamma := (x, y)$ be a coordinate pair of $\overline{F}/\overline{K}$ with the defining polynomial C. For any $\alpha, \beta \in \overline{K}$ we have $\overline{K}[x, y] = \overline{K}[x-\alpha, y-\beta]$. Therefore $(x-\alpha, y-\beta)$ is a coordinate pair of $\overline{F}/\overline{K}$ with the defining polynomial $C(X+\alpha, Y+\beta)$. If $P = (a, b; x, y) \in \mathcal{Z}((x, y))$ then $P' = (0, 0; x-\alpha, y-\beta) \in \mathcal{Z}((x-\alpha, y-\beta))$ and P is equivalent to P'. We obtain the point P' by* translation *of the point P to the* origin.

Let $\alpha_1, \beta_1, \alpha_2, \beta_2 \in \overline{K}$ with $\gamma := \alpha_1\beta_2 - \beta_1\alpha_2 \neq 0$. We obtain a new coordinate pair (x_1, y_1) of $\overline{F}/\overline{K}$ by setting

$$\begin{aligned} x_1 &:= \alpha_1 x + \beta_1 y, \\ y_1 &:= \alpha_2 x + \beta_2 y \end{aligned}$$

The defining polynomial of (x_1, y_1) is $C(\gamma\beta_2 X - \gamma\beta_1 Y, -\gamma\alpha_2 + \alpha_1\beta_2 Y)$.

Let A and B be local rings with the maximal ideals, respectively, $\mathcal{M}_A$ and $\mathcal{M}_B$. We say B *dominates* A if $B \supseteq A$ and $\mathcal{M}_B \supseteq \mathcal{M}_A$.

Definition 4.4 (Above relation) *Let P and Q be two points of $\overline{F}/\overline{K}$. We say Q is* above *P, denoted by $Q \mid P$, if $\mathcal{O}_Q$ dominates $\mathcal{O}_P$. If $\mathfrak{P}$ is a place of $\overline{F}/\overline{K}$ we say $\mathfrak{P}$ is* above *the point P, denoted by $\mathfrak{P} \mid P$, if $\mathcal{O}_\mathfrak{P}$ dominates $\mathcal{O}_P$. We say P is a* representative *of the place $\mathfrak{P}$, denoted by $P \equiv \mathfrak{P}$, if $\mathcal{O}_P = \mathcal{O}_\mathfrak{P}$.*

The relation $Q \mid P$ defines a partial order on the set of points of $\overline{F}/\overline{K}$. The simple points of $\overline{F}/\overline{K}$ are the maximal elements for this order since their local rings are discrete valuation rings which are maximal proper subrings of $\overline{F}$.

Let P be a point $\overline{F}/\overline{K}$ and $\mathfrak{P}$ a place above P. We will see in section 4.2, "Blowing-up points", how to compute a chain of points $P = Q_0, Q_1, Q_2, \ldots, Q_n$ such that $Q_{i+1} \mid Q_i$ for $i = 1, \ldots, n-1$ and $Q_n \equiv \mathfrak{P}$.

Lemma 4.1 *Let $P := (a, b; x, y)$ be a point of $\overline{F}/\overline{K}$ and $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ such that $\mathfrak{P} \mid P$. Suppose that $\nu_\mathfrak{P}(x-a) \leq \nu_\mathfrak{P}(y-b)$. Then*

$$\nu_\mathfrak{P}(x-a) = \min\{\nu_\mathfrak{P}(z) \mid z \in \mathcal{M}_P\}.$$

Proof: Let $z \in \mathcal{M}_P$. There exist $g, h \in \mathcal{O}_P$ such that $z = (x-a)g + (y-b)h$. We have $z/(x-a) = g + h(y-b)/(x-a)$ and $z/(x-a) \in \mathcal{O}_\mathfrak{P}$ since $\nu_\mathfrak{P}(x-a) \leq \nu_\mathfrak{P}(y-b)$ and $g, h \in \mathcal{O}_P \subseteq \mathcal{O}_\mathfrak{P}$. Hence $\nu_\mathfrak{P}(x-a) \leq \nu_\mathfrak{P}(z)$ for all $z \in \mathcal{M}_P$. □

Proposition 4.2 (Local parameter of a place) *Let $P = (a, b; x, y)$ be a simple point. Then $x - a$ or $y - b$ is a local parameter of the place $\mathfrak{P} \equiv P$.*

Proof: This follows from the preceding lemma and from the fact that t is a local parameter of $\mathfrak{P}$ if and only if $\nu_{\mathfrak{P}}(t) = 1$. □

Proposition 4.3 *Let $P := (a, b; x, y)$ be a point of the function field $\overline{F}/\overline{K}$. Let Q be a point of $\overline{F}/\overline{K}$ and $\mathcal{Q}$ a place of $\overline{F}/\overline{K}$. Then the following assertions are equivalent:*

1.	$Q \mid P$	$\mathcal{Q} \mid P$
2.	$\mathcal{O}_P \subseteq \mathcal{O}_Q$	$\mathcal{O}_P \subseteq \mathcal{O}_{\mathcal{Q}}$
3.	$\mathcal{M}_P \subseteq \mathcal{M}_Q$	$\mathcal{M}_P \subseteq \mathcal{Q}$
4.	$x - a \in \mathcal{M}_Q$ *and* $y - b \in \mathcal{M}_Q$	$x - a \in \mathcal{Q}$ *and* $y - b \in \mathcal{Q}$

Proof: We show the proposition for the point Q of $\overline{F}/\overline{K}$ (the proof for a place is similar). By definition we have (1) $\Leftrightarrow$ ((2) and (3)). We show (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (2).

- (2) $\Rightarrow$ (3) Suppose that $\mathcal{O}_P \subseteq \mathcal{O}_Q$ and consider the injection $\mathcal{O}_P \hookrightarrow \mathcal{O}_Q$ followed by the canonical projection $\mathcal{O}_Q \to \mathcal{O}_Q/\mathcal{M}_Q \cong \overline{K}$

  $$\varphi : \mathcal{O}_P \hookrightarrow \mathcal{O}_Q \to \mathcal{O}_Q/\mathcal{M}_Q \cong \overline{K}.$$

  The kernel of φ must be a maximal ideal as the image of φ is a field. Since $\mathcal{O}_P$ is a local ring, we have $\ker\varphi = \mathcal{M}_P$. We must have $\mathcal{M}_P \subseteq \mathcal{M}_Q$. Otherwise φ would not be surjective.

- (3) $\Rightarrow$ (4) This is trivial since $\mathcal{M}_P = \langle x - a, y - b\rangle\, \mathcal{O}_P$.

- (4) $\Rightarrow$ (2) Let $u \in \mathcal{O}_P$. Since $\mathcal{O}_P$ is the localization of $\overline{K}[x, y]$ in the maximal ideal $M_P = \langle x - a, y - b\rangle$, there exist $g, h \in \overline{K}[x, y]$ such that $u = g/h$ with $h \notin M_P$. By assumption $x - a, y - b \in \mathcal{M}_Q$. We have therefore $\overline{K}[x, y] \subseteq \mathcal{O}_Q$ and $M_P \subseteq \mathcal{M}_Q$. Consequently $M_P = \overline{K}[x, y] \cap \mathcal{M}_Q$ and we have $g, h \in \mathcal{O}_Q$ with $h \notin \mathcal{M}_Q$. Therefore $h^{-1} \in \mathcal{M}_Q$ so that $u = gh^{-1} \in \mathcal{O}_Q$.

□

Corollary 4.4 *A place $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ can not be above two distinct points $P_1 = (a_1, b_1; x, y)$ and $P_2 = (a_2, b_2; x, y)$ of $\mathcal{Z}(\Gamma)$ for a fixed coordinate pair $\Gamma = (x, y)$ of $\overline{F}/\overline{K}$.*

Proof: Assume that $\mathfrak{P}$ is above P_1 and P_2. Then by the preceding lemma $x - a_1$, $x - a_2$, $y - b_1$, $y - b_2 \in \mathfrak{P}$ and consequently $a_1 - a_2$ or $b_1 - b_2$ is a non-zero constant contained in $\mathfrak{P}$ contradicting the fact that $\mathfrak{P} \cap \overline{K} = \{0\}$. □

Corollary 4.5 *Let P be a point of the function field $\overline{F}/\overline{K}$. Then at least one place and at most finitely many places $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ are above P.*

Proof: By proposition 2.9 we know that there exists at least one place $\mathfrak{P}$ above P. Now there can not be infinitely many places above P since by the preceding proposition every place above the point $P = (a, b; x, y)$ is a zero of $x - a$ and $y - b$. We know by proposition 2.11 that any element of $\overline{F} \setminus \{0\}$ has only finitely many zeros, and consequently $x - a$ and $y - b$ can have only finitely many common zeros. □

Corollary 4.6 (Point set $\mathcal{Z}(\Gamma)$ of $\overline{F}/\overline{K}$) *Let $\Gamma = (x, y)$ be coordinate pair of $\overline{F}/\overline{K}$. Then*

$$\mathcal{Z}(\Gamma) = \{(x(\mathfrak{P}), y(\mathfrak{P}); x, y) \mid \mathfrak{P} \in \mathbb{P}_{\overline{F}} \text{ such that } x \in \mathcal{O}_{\mathfrak{P}} \text{ and } y \in \mathcal{O}_{\mathfrak{P}}\}.$$

Proof: ($\subseteq$) : Let $P = (a, b; x, y) \in \mathcal{Z}(\Gamma)$, $\mathcal{O}_P$ its local ring and $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ such that $\mathfrak{P} \mid P$. Since $\mathcal{M}_P \subseteq \mathfrak{P}$, we have $x - a \in \mathfrak{P}$ and $y - b \in \mathfrak{P}$ and therefore $(a, b) = (x(\mathfrak{P}), y(\mathfrak{P}))$.
($\supseteq$) : Let C be the defining polynomial of Γ and $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ such that $x, y \in \mathcal{O}_{\mathfrak{P}}$. We have

$$C(x(\mathfrak{P}), y(\mathfrak{P})) = C(x, y)(\mathfrak{P}) = 0(\mathfrak{P}) = 0$$

and therefore $(x(\mathfrak{P}), y(\mathfrak{P}); x, y) \in \mathcal{Z}(\Gamma)$. □

Remark 4.3 *For a fixed coordinate pair $\Gamma = (x, y)$ of $\overline{F}/\overline{K}$ there exist at least one place and at most finitely many places of $\overline{F}/\overline{K}$ which do not dominate any point of $\mathcal{Z}(\Gamma)$. These places are exactly the places which are poles of x or y. We will have to work with projective plane curves to avoid this "imbalance" between points and places.*

4.2 Blowing-up points

Let P be a point of the function field $\overline{F}/\overline{K}$ and $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ a place above P. If P is a simple point then $\mathcal{O}_P = \mathcal{O}_{\mathfrak{P}}$. If P is a singular point then $\mathcal{O}_P \subsetneq \mathcal{O}_{\mathfrak{P}}$. We may now ask if there exists a point Q of $\overline{F}/\overline{K}$ such that $Q \equiv \mathfrak{P}$ and if this is the case how this point can be determined. These two questions are closely related to the *desingularization* problem which consists of finding a smooth curve birationally isomorphic to a given singular curve. The classical method for solving this problem uses the technique of "blowing-up points".

Let $\Gamma := (x, y)$ be a coordinate pair of $\overline{F}/\overline{K}$ an $\mathcal{C}$ an affine plane curve such that $\mathcal{C} = \mathcal{C}_\Gamma$. A point $P = (a, b; x, y) \in \mathcal{Z}(\Gamma)$ represents a place of $\overline{F}/\overline{K}$ if and only if P is a simple point. The point P corresponds to the simple point (a, b) of the curve $\mathcal{C}$. A place $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ can not be represented by a point $\mathcal{Z}(\Gamma)$ if and only $\mathfrak{P}$ is above a singular point of $\mathcal{Z}(\Gamma)$. We will change the coordinates (x, y) in order to find a representation of such a place as a point of $\overline{F}/\overline{K}$.

Let $C \in \overline{K}[X, Y]$ be the defining polynomial of the coordinate pair (x, y). Set $x_1 := x/y$ and $y_1 := y/x$. Then both (x_1, y) and (x, y_1) are coordinate pair of $\overline{F}/\overline{K}$ since $x \in \overline{K}(x_1, y)$ and $y \in \overline{K}(x, y_1)$. The process of passing from (x, y) to (x, y_1) (resp. (x_1, y)) is called the *monoidal transformation with respect to the exceptional coordinate* x (resp. y). Let $G \in \overline{K}[X, Y]$ and $m := \deg \mathrm{Init}(G)$. Then m is the biggest integer such that X^m divides $G(X, XY) \in \overline{K}[X, Y]$ and Y^m divides $G(XY, Y) \in \overline{K}[X, Y]$. We set

$$G^{[x]} := G(X, XY)/X^m \in \overline{K}[X, Y]$$

which we call the *strict transform* of G with respect to the *exceptional coordinate* x. Similarly, we set

$$G^{[y]} := G(XY, X)/X^m \in \overline{K}[X, Y]$$

which we call the *strict transform* of G with respect to the *exceptional coordinate* y.

Lemma 4.7 *Let $\Gamma := (x, y)$ be a coordinate pair of $\overline{F}/\overline{K}$ with the defining polynomial $C \in \overline{K}[X, Y]$. Then $C^{[x]}$ (resp. $C^{[y]}$) is the defining polynomial of the coordinate pair (x, y_1) (resp. (x_1, y)).*

Proof: It is clear that $C^{[x]}(x, y_1) = 0$. It suffices to show that $C^{[x]}$ is irreducible to conclude the proof. We write

$$C(X, Y) = C_m(X, Y) + C_{m+1}(X, Y) + \ldots + C_n(X, Y)$$

where $m := \deg \mathrm{Init}(C)$, $n := \deg C$ and C_i is a homogeneous polynomial of degree i for $m \leq i \leq n$. It is now easily seen that

$$C^{[x]}(X, Y_1) = C_m(1, Y_1) + XC_{m+1}(1, Y_1) + \ldots + X^{n-m}C_n(X, Y_1).$$

We have $C(X, Y) = X^m\, C^{[x]}(X, Y/X)$ and it is clear that $C^{[x]}$ must be irreducible. Otherwise C would not irreducible. □

Assume that $P = (0, 0; x, y)$ is a point of the function field $\overline{F}/\overline{K}$ and $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ a place above P.

1. If $y_1 := y/x \in \mathcal{O}_{\mathfrak{P}}$ then
$$Q := (0, y_1(\mathfrak{P}); x, y_1)$$
is a point of $\overline{F}/\overline{K}$ (by corollary 4.6) such that $\mathfrak{P} \mid Q$ and $Q \mid P$ (by proposition 4.3).

2. Similarly, if $x_1 := x/y \in \mathcal{O}_{\mathfrak{P}}$ then
$$Q' := (x_1(\mathfrak{P}), 0; x_1, y_1)$$
is a point of $\overline{F}/\overline{K}$ such that $\mathfrak{P} \mid Q'$ and $Q' \mid P$.

It is easily verified that if $x_1 \in \mathcal{O}_{\mathfrak{P}}$ and $y_1 \in \mathcal{O}_{\mathfrak{P}}$, then Q and Q' are above each other and therefore $Q \equiv Q'$.

Definition 4.5 *Let $P := (a, b; x, y)$ be a point of $\overline{F}/\overline{K}$ and $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ a place above the point P. Set $x_0 := x - a$ and $y_0 := y - b$.*

1. *If $y_1 := y_0/x_0 \in \mathcal{O}_{\mathfrak{P}}$, then we set*
$$P^{\mathfrak{P}} := (0, \beta, x_0, y_1)$$
where $\beta := y_1(\mathfrak{P})$. We call x_0 the exceptional coordinate *of the point $P^{\mathfrak{P}}$.*

2. *Otherwise, we have $x_1 := x_0/y_0 \in \mathfrak{P}$ and we set*
$$P^{\mathfrak{P}} := (0, 0, x_1, y_0).$$
We call y_0 the exceptional coordinate *of the point $P^{\mathfrak{P}}$.*

We set $P^{\mathfrak{P}^{(0)}} := P$ and $P^{\mathfrak{P}^{(n)}} := \left(P^{\mathfrak{P}^{(n-1)}}\right)^{\mathfrak{P}}$ for $n \geq 1$. The point $P^{\mathfrak{P}^{(n)}}$ is called the infinitely close point of order n towards the place $\mathfrak{P}$. *We call* blow up *of the point P the set*

$$\mathfrak{B}(P) := \{P^{\mathfrak{P}} \mid \mathfrak{P} \in \mathbb{P}_{\overline{F}} \text{ such that } \mathfrak{P} \mid P\}.$$

We note that by Corollary 4.5 the blow up of a point is a finite set.

Remark 4.4 *Let $P := (a, b; x, y)$ be a point of $\overline{F}/\overline{K}$ and $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ above P. We note that if we apply the preceding definition to the point $P_0 := (0, 0; x - a, y - b)$, then we have $P_0^{\mathfrak{P}} = P^{\mathfrak{P}}$.*

We determine now the coordinates of points of $\mathfrak{B}(P)$ as a function of the coordinates of P. Suppose that $P = (0, 0; x, y)$ and let $C(X, Y) \in \overline{K}[X, Y]$ be the defining polynomial of the coordinate pair (x, y). Let $\mathrm{Init}(C)$ be the initial form of C and $m := m_P > 0$ the degree of $\mathrm{Init}(C)$. Consider its factorization

$$\mathrm{Init}(C) = \prod_{i=1}^{m} (\alpha_i X + \beta_i Y).$$

Let (x, y_1) (resp. (x_1, y)) be the monoidal transform of (x, y) with respect to the exceptional coordinate x (resp. y) which have $C^{[x]}$ (resp. $C^{[y]}$) as defining polynomials. Let $H := C - \mathrm{Init}(C)$. Then $l := \deg \mathrm{Init}(H) > m$ and we can write

$$C^{[x]} = \prod_{i=1}^{m} (\alpha_i + \beta_i Y) + X^{(l-m)} H^{[x]}$$

and

$$C^{[y]} = \prod_{i=1}^{m} (\alpha_i X + \beta_i) + Y^{(l-m)} H^{[y]}.$$

Now let $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ be a place above P (recall that in this case $x, y \in \mathfrak{P}$ by proposition 4.3). By the definition of a valuation ring we have $y_1 = y/x \in \mathcal{O}_{\mathfrak{P}}$ or $x_1 = x/y \in \mathcal{O}_{\mathfrak{P}}$.

1. If $y_1 \in \mathcal{O}_{\mathfrak{P}}$, then

$$0 = 0(\mathfrak{P}) = C^{[x]}(x, y_1)(\mathfrak{P}) = \prod_{i=1}^{m} (\alpha_i + \beta_i y_1(\mathfrak{P})) = \mathrm{Init}(C)(1, y_1(\mathfrak{P}))$$

   and consequently there exists i such that $\beta_i \neq 0$ and $y_1(\mathfrak{P}) = -\alpha_i/\beta_i$. Therefore

$$P^{\mathfrak{P}} := (0, -\alpha_i/\beta_i; x, y_1).$$

2. If $y_1 \notin \mathcal{O}_{\mathfrak{P}}$, then $x_1 \in \mathfrak{P}$ and $x_1(\mathfrak{P}) = 0$. We have

$$0 = 0(\mathfrak{P}) = C^{[y]}(x_1, y)(\mathfrak{P}) = \prod_{i=1}^{m} (\alpha_i x_1(\mathfrak{P}) + \beta_i) = \prod_{i=1}^{m} \beta_i$$

   and consequently there exists i such that $\beta_i = 0$. Therefore

$$P^{\mathfrak{P}} := (0, 0; x_1, y).$$

Note that the values $-\alpha_i/\beta_i$ are the distinct roots of $\mathrm{Init}(C)(1, Y)$. There exists i such that $\beta_i = 0$ if and only if $\mathrm{Init}(C)(0, 1) = 0$ which is equivalent to say that X does not divides $\mathrm{Init}(C)$. More precisely, we have

$$\mathfrak{B}(P) := \{(0, \gamma; x, y_1) \mid \gamma \in \overline{K}, \mathrm{Init}(C)(1, \gamma) = 0\} \cup \mathfrak{B}_\infty(P)$$

where

$$\mathfrak{B}_\infty(P) = \begin{cases} \{(0, 0; x_1, y)\} & \text{if } \mathrm{Init}(C)(0, 1) = 0 \\ \emptyset & \text{otherwise} \end{cases}.$$

Remark 4.5 *Let $P = (0,0;x,y)$ and $\mathcal{C}_\Gamma$ be the affine plane curve associated to the coordinate pair $\Gamma := (x,y)$. Note that the points of $\mathfrak{B}(P)$ correspond bijectively to the distinct linear factors of* $\mathrm{Init}(C)$ *and consequently to the tangents of the curve $\mathcal{C}_\Gamma$ in the point $(0,0)$. More precisely, $Q := (0,\gamma;x,y_1) \in \mathfrak{B}(P)$ if and only if the line $\gamma X - Y = 0$ is a tangent of the curve $\mathcal{C}_\Gamma$ in the point $(0,0)$. Similarly, $Q' = (0,0;x_1,y) \in \mathfrak{B}(P)$ if and only if $X = 0$ is a tangent of the curve $\mathcal{C}_\Gamma$ in the point $(0,0)$. We construct the points of $\mathfrak{B}(P)$ by splitting ("blowing up") the singular point $(0,0)$ in several new points corresponding to the tangents of the curve $\mathcal{C}_\Gamma$ in $(0,0)$.*

Definition 4.6 *Let P be a point of $\overline{F}/\overline{K}$. We say (x,y) is an* exceptional coordinate pair *of the blow up $\mathfrak{B}(P)$ if*

1. *$P \equiv (0,0;x,y)$, and*
2. *$x/y \in \mathcal{O}_\mathfrak{P}$ and $y/x \in \mathcal{O}_\mathfrak{P}$ for all places $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ above P.*

Lemma 4.8 *Every blow up $\mathfrak{B}(P)$ of a point P of $\overline{F}/\overline{K}$ has a exceptional coordinate pair.*

Proof: We assume without loss of generality that $P = (0,0;x,y)$. Set $x' := x + \alpha y$ and $y' := x + \beta y$ where $\alpha, \beta \in \overline{K} \setminus \{0\}$. It is clear that if $\alpha \neq \beta$, then $\Gamma' := (x', y')$ is also a coordinate pair of $\overline{F}/\overline{K}$ and $P \equiv (0,0;x',y')$. Choose now α and β such that $X + \alpha Y$ and $X + \beta Y$ does not divide $\mathrm{Init}(C)$ and therefore $x'/y' \in \mathcal{O}_\mathfrak{P}$ and $y'/x' \in \mathcal{O}_\mathfrak{P}$ for all places $\mathfrak{P} \mid P$. □

Lemma 4.9 *Let $P := (0,0;x,y)$ be a point of $\overline{F}/\overline{K}$ and $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ a place above P. If x is the exceptional coordinate of $P^\mathfrak{P}$, then*

1. *$\nu_\mathfrak{P}(x) = \min\{\nu_\mathfrak{P}(z) \mid z \in \mathcal{M}_P\}$,*
2. *$z/x \in \mathcal{O}_{P^\mathfrak{P}}$ for all $z \in \mathcal{M}_P$.*

Proof: The assertion (1) follows directly from lemma 4.1 since $\nu_\mathfrak{P}(x) \leq \nu_\mathfrak{P}(y)$. The proof of (2) is similar to the proof of lemma 4.1 (replace $\mathcal{O}_\mathfrak{P}$ by $\mathcal{O}_{P^\mathfrak{P}}$ and use $y/x \in \mathcal{O}_{P^\mathfrak{P}}$). □

The definition of an infinitely close point towards a place depends on the coordinates of the point. On the contrary, the following proposition shows that the local ring of an infinitely close point towards a place only depends on the local ring of the point P and the place $\mathfrak{P}$.

Proposition 4.10 *Let P and R be two equivalent points of $\overline{F}/\overline{K}$ and $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ a place above them. For all $n \in \mathbb{N}$ we have*

$$P^{\mathfrak{P}^{(n)}} \equiv R^{\mathfrak{P}^{(n)}}.$$

Proof: It suffices to show the proposition for an infinitely close point of order 1. Suppose that $P := (0,0;x,y)$ and $R := (0,0;u,v)$ (see remark 4.4) and $\nu_\mathfrak{P}(x) \leq \nu_\mathfrak{P}(y)$ and $\nu_\mathfrak{P}(u) \leq \nu_\mathfrak{P}(v)$ (toggle (x,y) and (u,v) if necessary). By the preceding lemma we have $x/u, y/u \in \mathcal{O}_{R^\mathfrak{P}}$. Since $\mathcal{M}_P = \mathcal{M}_R$, we have $\nu_\mathfrak{P}(x) = \nu_\mathfrak{P}(u)$ by lemma 4.1 and consequently $\nu_\mathfrak{P}(x/u) = 0$. Therefore $x/u \in \mathcal{O}_{R^\mathfrak{P}}$ is invertible in $\mathcal{O}_{R^\mathfrak{P}}$. We have now $y/x = (y/u)(u/x) \in \mathcal{O}_{R^\mathfrak{P}}$. The ring $\mathcal{O}_{R^\mathfrak{P}}$ contains x and y/x and consequently $R^\mathfrak{P} \mid P^\mathfrak{P}$ by proposition 4.3. □

Proposition 4.11 *Let $\Gamma = (x,y)$ be a coordinate pair of $\overline{F}/\overline{K}$ with the defining polynomial $C \in \overline{K}[X,Y]$ such that X does not divide* $\mathrm{Init}(C)$*. Then the element $y_1 := y/x$ satisfies an algebraic equation of degree m over $\overline{K}[x,y]$ where the leading coefficient is not zero in $P = (0,0;x,y)$. We have therefore $x^{m-1}\,(\mathcal{O}_P[y_1]) \subseteq \mathcal{O}_P$.*

Proof: [Per95] Lemma 4.5 on page 191 □

Proposition 4.12 *Let $P := (0, 0; x, y)$ be a point $\overline{F}/\overline{K}$ and suppose that X does not divide* $\mathrm{Init}(C)$ *where C is the defining polynomial of the coordinate pair (x, y). Then $\mathcal{O}_P[y_1]$ is a semi-local ring and its maximal ideals correspond bijectively to the points of $\mathfrak{B}(P)$.*

Proof: Let $\mathcal{M}$ be a maximal ideal of $\mathcal{O}_P[y_1]$. By Proposition 2.9 we know that there is a place $\mathfrak{P}$ of $\overline{F}$ such that $\mathcal{M} = \mathfrak{P} \cap \mathcal{O}_P[y_1]$. Since by Corollary 4.5. □

Proposition 4.13 *Let $P := (0, 0; x, y)$ be a point $\overline{F}/\overline{K}$ and suppose that $y/x \in \mathcal{O}_\mathfrak{P}$ for all places $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ above the point P. Then*

$$\mathcal{O}_P[y_1] = \bigcap_{Q \in \mathfrak{B}(P)} \mathcal{O}_Q$$

and therefore

$$x^{m_P - 1} \left(\bigcap_{Q \in \mathfrak{B}(P)} \mathcal{O}_Q \right) \subseteq \mathcal{O}_P$$

Proof: Since the ring $\mathcal{O}_P[y_1]$ is integer it is equal to the intersection of all its localizations in its maximal ideals (see [Mat80] lemma 2 on page 8). These localizations are exactly the local rings $\mathcal{O}_Q$. □

4.3 Exceptional divisors

We define the *exceptional divisor* of a point of $\overline{F}/\overline{K}$. This divisor plays an important role in the computation of a basis of the vector space $\mathcal{L}(D)$ where $D \in \mathcal{D}_{\overline{F}}$. We deduce from the definition of the exceptional divisor and its properties a method for the computation of principal divisors.

Definition 4.7 (Local divisor) *Let P be a point of $\overline{F}/\overline{K}$ and $z \in \overline{F} \setminus \{0\}$. The* local divisor *of z at the point P, denoted by $(z)_P$, is defined by*

$$(z)_P := \sum_{\mathfrak{P}|P} \nu_\mathfrak{P}(z)\mathfrak{P}. \tag{4.1}$$

Is is clear that $(z_1 z_2)_P = (z_1)_P + (z_2)_P$ for all $z_1, z_2 \in \overline{F} \setminus \{0\}$ and all points P of $\overline{F}/\overline{K}$.

Definition 4.8 (Exceptional divisor) *Let P be a point of $\overline{F}/\overline{K}$. The* exceptional divisor *of the point P, denoted by E_P, is defined by*

$$E_P := \sum_{\mathfrak{P}|P} m_\mathfrak{P}\mathfrak{P} \tag{4.2}$$

where $m_\mathfrak{P}$ is defined by

$$m_\mathfrak{P} := \min\{\nu_\mathfrak{P}(z) \mid z \in \mathcal{M}_P\}.$$

for all places $\mathfrak{P}$ above P.

Lemma 4.14 *Let (x, y) be a pair of exceptional coordinates of $\mathcal{B}(P)$. Then*

$$(x)_P = (y)_P = E_P.$$

Proof: By proposition 4.1 we have $\nu_{\mathfrak{P}}(x)$ or $\nu_{\mathfrak{P}}(y)$ is $\min\{\nu_{\mathfrak{P}}(z) \mid z \in \mathcal{M}_P\}$ and $\nu_{\mathfrak{P}}(x) = \nu_{\mathfrak{P}}(y)$ (since $x/y \in \mathcal{O}_{\mathfrak{P}}$ and $y/x \in \mathcal{O}_{\mathfrak{P}}$ by the definition of an exceptional coordinate pair) for all places $\mathfrak{P}$ with $\mathfrak{P} \mid P$. □

Remark 4.6 *If P is a simple point, then $E_P = \mathfrak{P}$ where $\mathfrak{P}$ is the unique place such that $\mathfrak{P} \equiv P$. The converse is also true as we will see in 4.21.*

Suppose that $P := (0, 0; x, y)$ is a singular point of $\overline{F}/\overline{K}$ and let $g \in \overline{K}[x, y]$. Since any place above P is above only one point of $\mathfrak{B}(P)$ (see Corollary 4.4) we have

$$(g)_P = \sum_{Q \in \mathfrak{B}(P)} (g)_Q.$$

Let $G \in \overline{K}[X, Y]$ such that $g = G(x, y)$. Let l_Q denote the exceptional coordinate of $Q \in \mathcal{B}(P)$ and set $x_1 := x/y$, $y_1 := y/x$ and

$$g^{(l_Q)} := \begin{cases} G^{[x]}(x, y_1) & \text{if } l_Q = x \\ G^{[y]}(x_1, y) & \text{if } l_Q = y \end{cases}.$$

We have

$$\begin{aligned} (g)_P &= \sum_{Q \in \mathfrak{B}(P)} (l_Q^{m_P(G)} g^{(l_Q)})_Q \\ &= m_P(G) \sum_{Q \in \mathfrak{B}(P)} (l_Q)_Q + \sum_{Q \in \mathfrak{B}(P)} (g^{(l_Q)})_Q. \end{aligned}$$

Since l_Q is an exceptional coordinate of the point $Q \in \mathfrak{B}(P)$, we have

$$\nu_{\mathfrak{P}}(l_Q) = \min\{\nu_{\mathfrak{P}}(z) \mid z \in \mathcal{M}_P\}$$

for all places $\mathfrak{P}$ above the point Q. Consequently

$$E_P := \sum_{Q \in \mathfrak{B}(P)} (l_Q)_Q$$

and

$$(g)_P = m_P(G) E_P + \sum_{Q \in \mathfrak{B}(P)} (g^{(l_Q)})_Q.$$

Proposition 4.15 *Let $P := (a, b; x, y)$ be a point of $\overline{F}/\overline{K}$ and C the defining polynomial of (x, y). Let $g \in \overline{K}[x, y] \setminus \{0\}$ and $G \in \overline{K}[X, Y]$ such that $g = G(x, y)$. If the initial form of $G(X + a, Y + b)$ does not have a common factor with the initial form of $C(X + a, Y + b)$ then*

$$(g)_P = m_P(G) E_P.$$

Proof: Let $x_0 := x - a$ and $y_0 := y - b$ and $Q \in \mathfrak{B}(P)$. We assume without loss of generality that $Q = (0, \beta; x_0, y_0/x_0)$. It is clear that $G^{[x]}(0, \beta) \neq 0$ and therefore $g^{[x]} \in \mathcal{O}_Q^* \subseteq \mathcal{O}_{\mathfrak{P}}^*$ (equivalent to $\nu_{\mathfrak{P}}(g^{[x]}) = 0$) for all $\mathfrak{P} \mid Q$. □

4.4 Intersection divisors

Let now $\overline{K}(\mathcal{C}^*)$ and $K(\mathcal{C}^*)$ denote, respectively, the function field of a projective plane curve $\mathcal{C}^* := \{C^* = 0\}$ defined over K.

Let $\overline{K}[\mathcal{C}^*]$ denote the coordinate ring of the curve $\mathcal{C}^*$ and u, v and w the residual images of, respectively, U, V and W in $\overline{K}[\mathcal{C}^*]$. We call $\Gamma := (u, v, w)$ the *homogeneous coordinate triple*. The *standard coordinate pairs* $\Gamma_2 := (u/w, v/w)$, $\Gamma_1 := (u/v, w/v)$ and $\Gamma_0 := (v/u, w/u)$ are coordinate pairs of $\overline{K}(\mathcal{C}^*)$ defined over K. The corresponding defining polynomials are, respectively, $C^*(X, Y, 1)$, $C^*(X, 1, Y)$ and $C^*(1, X, Y)$.

Let $P = (a : b : c) \in \mathcal{C}^*$. By the definition of homogeneous coordinates there exists at least one coordinate that is not zero. Suppose that $c \neq 0$. Then $P_{*2} = (a/c, b/c; u/w, v/w)$ is a point of $\overline{F}/\overline{K}$. If $b \neq 0$ then $P_{*1} = (a/b, c/b; u/v, w/v)$ is also a point of $\overline{K}(\mathcal{C}^*)$ and $P_{*2} \equiv P_{*1}$. Therefore all points of $\mathcal{C}^*$ can be identified with points of point of $\overline{K}(\mathcal{C}^*)$. This corresponds to the fact that questions about a projective plane curve $\mathcal{C}^*$ near a point P can be reduced to questions about the affine plane curve $\mathcal{C}$. Even though $\mathcal{O}_{P_{*2}}$ and $\mathcal{O}_{P_{*1}}$ are equal some computations depend on the choice of the non-zero coordinate. We fix the following convention:

Definition 4.9 (Points of $\overline{K}(\mathcal{C}^*)$) *We associate to every point $P := (a : b : c) \in \mathcal{C}^*$ a point of $\overline{K}(\mathcal{C}^*)$ defined by:*

$$P_* := \begin{cases} (a/c, b/c; u/w, v/w) & \text{if } c \neq 0 \\ (a/b, 0; u/v, w/v) & \text{if } c = 0 \text{ and } b \neq 0 \\ (0, 0; v/u, w/u) & \text{if } P = (1 : 0 : 0) \end{cases} .$$

For every homogeneous polynomial $F \in \overline{K}[U, V, W]$ we set

$$\overline{F}^P := \begin{cases} F(u, v, w)/w^{\deg G} & \text{if } c \neq 0 \\ F(u, v, w)/v^{\deg G} & \text{if } c = 0 \text{ and } b \neq 0 \\ F(u, v, w)/u^{\deg G} & \text{if } P = (1 : 0 : 0) \end{cases} .$$

We have $\overline{F}^P \in \overline{K}(\mathcal{C}^*)$ for all $P \in \mathcal{C}^*$ and all homogeneous polynomial $F \in \overline{K}[U, V, W]$. If $z = F(u, v, w)/G(u, v, w) \in \overline{K}(\mathcal{C}^*)$ for some homogeneous polynomials $F, G \in \overline{K}[U, V, W]$ then $z = \overline{F}^P/\overline{G}^P$ for all $P \in \mathcal{C}^*$.

Proposition 4.16 *Let $\mathcal{C}^*$ be a projective plane curve.*

1. *If $\mathfrak{P} \in \mathbb{P}_{\overline{K}(\mathcal{C}^*)}$, then there exists a unique point $P \in \mathcal{C}^*$ such that $\mathfrak{P} \mid P_*$.*
2. *If $P \in \mathcal{C}^*$, then $\{\mathfrak{P} \in \mathbb{P}_{\overline{K}(\mathcal{C}^*)} \mid \mathfrak{P} \mid P_*\}$ is a non-empty finite set.*

Proof: We show that at least one of the standard coordinate pairs is contained in $\mathcal{O}_{\mathfrak{P}}$. Assume that $u/w \notin \mathcal{O}_{\mathfrak{P}}$. By the definition of a valuation ring we have $w/u \in \mathcal{O}_{\mathfrak{P}}$. Assume now that $v/u \notin \mathcal{O}_{\mathfrak{P}}$ and we have $u/v \in \mathcal{O}_{\mathfrak{P}}$. Consequently $(w/u)(u/v) = w/v \in \mathcal{O}_{\mathfrak{P}}$. The coordinate pair $(u/v, w/v)$ is contained in $\mathcal{O}_{\mathfrak{P}}$. We can now use corollary 4.6. The other cases are treated similarly. The second assertion is equivalent to corollary 4.5. □

Definition 4.10 (Local divisor) *Let $z \in \overline{K}(\mathcal{C}^*)$ and $P \in \mathcal{C}^*$. The* local divisor *of z in the point P, denoted by $(z)_P$, is defined by $(z)_P := (z)_{P_*}$.*

Definition 4.11 (Intersection divisor) *Let $P \in \mathcal{C}^*$ and $F \in \overline{K}[U,V,W] \setminus \{0\}$ such that C^* does not divide F. The* local intersection divisor *of F in P, denoted by $(F)_P$, is defined by*

$$(F)_P := (\overline{F}^P)_P.$$

The intersection divisor *of F and C^*, denoted by (F), is defined by*

$$(F) := \sum_{P \in \mathcal{C}^*} (F)_P.$$

If $F(P) \neq 0$ then $\overline{F}^P$ is invertible in $\mathcal{O}_{P_*} \subseteq \mathcal{O}_{\mathfrak{P}}$ for all places $\mathfrak{P} \mid P$. Therefore the divisor (F) is well-defined because by the Bézout theorem there exists only a finite number of points $P \in \mathcal{C}^*$ such that $F(P) = 0$ (the intersection points of the curves $\mathcal{C}^*$ and $\mathcal{F} = \{F = 0\}$). It is also clear that $(F)_P$ does not depend on the choice of the non-zero homogeneous coordinate in the definition 4.9.

The following proposition shows that we can always write the principal divisor of a function as a difference of two intersection divisors. We conclude from this that two homogeneous polynomials of equal degree have intersection divisors of equal degree.

Proposition 4.17 (Principal divisors) *Let $z \in \overline{K}(\mathcal{C}^*) \setminus \{0\}$ and $F, G \in \overline{K}[U,V,W]$ two homogeneous polynomials non-divisible by C^* such that* $\deg F = \deg G$ *and*

$$z = \frac{F(u,v,w)}{G(u,v,w)}.$$

Then

$$(z) = (F) - (G).$$

Proof: Let $\mathfrak{P} \in \mathbb{P}_{\overline{K}(\mathcal{C})}$. Recall that $F(u,v,w)/G(u,v,w) = \overline{F}^P/\overline{G}^P$ for all $P \in \mathcal{C}^*$. We have

$$\begin{aligned} \nu_{\mathfrak{P}}(z) &= \nu_{\mathfrak{P}}(F(u,v,w)/G(u,v,w)) \\ &= \nu_{\mathfrak{P}}(\overline{F}^P/\overline{G}^P) \\ &= \nu_{\mathfrak{P}}(\overline{F}^P) - \nu_{\mathfrak{P}}(\overline{G}^P), \end{aligned}$$

and

$$(z)_P := \sum_{\mathfrak{P} \mid P} \nu_{\mathfrak{P}}(z)\mathfrak{P} = (F)_P - (G)_P.$$

The proposition follows now from the fact that a place $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ dominates a unique point of $\mathcal{C}^*$. □

Definition 4.12 (Transverse) *Let $H \in \overline{K}[U,V,W]$ be a homogeneous polynomial and $P := (a : b : c) \in \mathbb{P}^2$. We define*

$$H^P(X,Y) := \begin{cases} H(X,Y,1) & \text{if } c \neq 0, \\ H(X,1,Y) & \text{if } c = 0 \text{ and } b \neq 0, \\ H(1,X,Y) & \text{otherwise} \end{cases}$$

We say two homogeneous polynomials $F, G \in \overline{K}[U,V,W]$ are transverse *at the point $P \in \mathbb{P}^2$ if*

1. *$F(P) = G(P) = 0$ and*

2. $\mathrm{Init}(F^P)$ *and* $\mathrm{Init}(G^P)$ *do not have a common factor.*

This means geometrically that the curves $\mathcal{F} := \{F = 0\}$ *and* $\mathcal{G} := \{G = 0\}$ *have no common tangent at the point* P*.*

Definition 4.13 (Intersection number) *Let* $F, G \in S := \overline{K}[U, V, W]$ *be two homogeneous polynomials of degree, respectively,* m *and* n*. The* intersection number *is a map*

$$\begin{array}{ccc} \mathbb{P}^2 \times S \times S & \longrightarrow & \mathbb{N} \cup \{\infty\} \\ (P, F, G) & \mapsto & I_P(F, G) \end{array}$$

satisfying the following properties

1. $I_P(F, G) = \infty$ *if and only if* F *and* G *have a common factor* F' *such that* $F'(P) = 0$*, otherwise* $I_P(F, G) \in \mathbb{N}$*,*
2. $I_P(F, G) = 0$ *if and only if* $P \notin \mathcal{F} \cap \mathcal{G}$*,*
3. $I_P(F, G) = I_P(G, F)$*,*
4. $I_P(F, G) = I_{T(P)}(F^T, G^T)$ *for any projective coordinate transformation* T*,*
5. $I_P(F, G) \geq m_P(F)m_P(G)$ *with equality occuring if and only if* F *and* G *are transverse at the point* P*,*
6. *if* $F = \prod F_i^{r_i}$ *and* $G = \prod G_j^{s_i}$*, then* $I_P(F, G) = \sum_{i,j} r_i s_j I_P(F_i, G_j)$*,*
7. *if* $\deg F \geq \deg G$*, then for any homogeneous polynomial* $B \in S$ *with* $\deg B = \deg F - \deg G$ *we have* $I_P(F, G) = I_P(F + BG, G)$*.*

Theorem 4.18 *There exists a unique map from* $\mathbb{P}^2 \times S \times S$ *to* $\mathbb{N} \cup \{\infty\}$ *satisfying the properties of the intersection number.*

Proof: [Ful69] Theorem 10 on page 75 □

Theorem 4.19 (Bézout) *Let* $F, G \in \overline{K}[U, V, W]$ *be two homogenous polynomials having no common factor. Then*

$$\sum_{P \in \mathcal{F} \cap \mathcal{G}} I_P(F, G) = \deg F \cdot \deg G.$$

Proof: [Ful69] page 112 □

Proposition 4.20 (Variant of the Bézout theorem) *Let* $F \in \overline{K}[U, V, W]$ *be a homogeneous polynomial such that* C^* *does not divide* F*. Then*

$$\deg(F) = m \cdot n$$

where n *and* m *are the degrees of* C^* *and* F*.*

Proof: We assume without loss of generality that $C^* \neq U$ and $C^* \neq W$ so that

$$\mathcal{C}^*_\infty := \mathcal{C}^* \cap \{(a:b:c) \in \mathbb{P}^2 \mid c = 0\} = \mathcal{V}(C^*, W)$$

is a finite set. Let G and G' be any homogeneous polynomials with the same degree and non-divisible by C^*. By proposition 4.17 we know that the divisor $(G) - (G')$ is a principal divisor and consequently $\deg(G) = \deg(G')$. Therefore the divisors (F) and (X^{degF}) have the same degrees[1] and it suffices to show the proposition for $F = U$ since $\deg(U^d) = d \cdot \deg(U)$. Now let $x := u/w \in \overline{K}(\mathcal{C}^*)$. Then $(x) = (U) - (W)$. Since $\mathcal{C}^*_\infty$ is finite we can transform the curve such that the algebraic set $\mathcal{V}(U, C^*, W) = \emptyset$ and consequently $\mathrm{supp}(U) \cap \mathrm{supp}(W) = \emptyset$. We have now $(x)_0 = (U)$ and

$$\deg(U) = \deg(x)_0 = [\overline{K}(\mathcal{C}^*) : \overline{K}(x)].$$

The coordinate pair $(x, y) := (u/w, v/w)$ is a standard coordinate pair of $\overline{K}(\mathcal{C}^*)$ with the defining polynomial $C(X, Y) = C^*(U, V, 1)$. Therefore $p(Y) := C(x, Y) \in \overline{K}(x)[Y]$ is the minimal polynomial of y over $\overline{K}(x)$. Now it suffices to show that $\deg p(Y) = n$ since $\deg p(Y) = [\overline{K}(\mathcal{C}^*) : \overline{K}(x)] = \deg(x)_0 = \deg(U)$. If this was not true, then all the monomials of $C^*(U, V, W)$ would have a degree less n in the variable V and consequently $C^*(0, 1, 0) = 0$ which contradicts the hypothesis that $\mathcal{V}(U, C^*, W) = \emptyset$. □

The following proposition is very important. It shows that an infinitely close point of sufficiently large order is a simple point.

Proposition 4.21 *Let E_P be the exceptional divisor of a point P of $\overline{K}(\mathcal{C}^*)$. Then*

$$\deg E_P = m_P.$$

Proof: We assume that $\overline{K}$ has characteristic $p > 0$. If P is simple then $E_P = \mathfrak{P}$ where $\mathfrak{P} \equiv P$ and it is clear that $\deg E_P = m_P$. Now let P be singular. We assume that there exists $F \in \overline{K}[U, V, W]$ such that

1. $F(P) = 0$,
2. F and C^* are transverse in P, and
3. for all $P' \in V' := V \setminus \{P\}$ we have
   (a) P' is a simple point of $\mathcal{C}^*$, and
   (b) F and C^* are transverse in P'.

where $V := \mathcal{V}(F, C^*)$. Since F and C^* are transverse in all points $P' \in V'$ we have $(F)_{P'} = m_P(F) E_P$. Further, since the points P' are simple points we have

$$\deg(F)_{P'} = m_{P'}(F) \deg E_{P'} = m_{P'}(F) = I_{P'}(C^*, F).$$

Let $m := \deg F$ and $n := \deg C^*$. By the preceding proposition we know that

$$\begin{aligned} m \cdot n = \deg(F) &= \deg(F)_P + \sum_{P' \in V'} \deg(F)_{P'} \\ &= m_P(F) \deg E_P + \sum_{P' \in V'} \deg(F)_{P'} \\ &= m_P(F) \deg E_P + \sum_{P' \in V'} I_{P'}(C^*, F) \end{aligned}$$

[1] Note that $\deg(G)$ denotes the degree of the divisor (G) and $\deg G$ the degree of the polynomial G

By the Bézout theorem we have

$$\begin{aligned} m \cdot n &= I_P(C^*, F) + \sum_{P' \in V'} I_{P'}(C^*, F) \\ &= m_P(F) \cdot m_P(C^*) + \sum_{P' \in V'} I_{P'}(C^*, F). \end{aligned}$$

Combining these equations we obtain

$$m_P(F) \deg E_P = m_P(F) \cdot m_P(C^*) \Longleftrightarrow \deg E_P = m_P(C^*).$$

We must show now that there exists a polynomial F satisfying the conditions above. Without loss of generality we can assume that

1. $P = (0 : 0 : 1)$,
2. $C^*(0, 1, 0) \neq 0$,
3. $C_X \neq 0$ where $C(X, Y) = C^*(U, V, 1)$, and
4. Y does not divide $\mathrm{Init}(C)$.

Set $F_\alpha := \alpha U^p + VW^{p-1}$ where $\alpha \in \overline{K}$. For any $0 \neq \alpha \in \overline{K}$ the point $(0 : 1 : 0)$ is the only point of $\mathcal{V}(F_\alpha)$ at infinity. We have $\mathcal{V}(F_\alpha, C^*) \subset \mathcal{C}^* \setminus \mathcal{C}^*_\infty$. since $C^*(0, 1, 0) \neq 0$. Set $F'_\alpha := F_\alpha(X, Y, 1) = Y + \alpha X^p$. Since Y does not divide $\mathrm{Init}(C)$, F and C^* are transverse at P.

If $Q = (a : b : 1) \in \mathcal{C}^* \setminus \mathcal{C}^*_\infty$ is a simple point, then

$$\mathrm{Init}(C(X + a, Y + b)) = C_X(a, b)X + C_Y(a, b)Y \neq 0.$$

For all $Q = (a : b : 1)$ such that $F_\alpha(Q) = 0$ we have

$$\mathrm{Init}(F'_\alpha(X + a, Y + b)) = \mathrm{Init}((Y + b) + \alpha(X + a)^p) = \mathrm{Init}((Y + \alpha X^p)) = Y.$$

We conclude that if $Q = (a : b : 1) \in V$ is a simple point of $\mathcal{C}^*$, then F and C^* are transverse if and only if $C_X \neq 0$. Since $C_X \neq 0$ and $\gcd(C, C_X) = 1$

$$W := \{Q = (a : b : 1) \in \mathcal{C}^* \setminus \mathcal{C}^*_\infty \mid C'_X(a, b) = 0\} \cup \{Q \in \mathcal{C}^* \setminus \mathcal{C}^*_\infty \mid Q \text{ is singular}\}$$

is a finite set (by the Bézout theorem and the fact that an irreducible curve has only finitely many singular points). It is now sufficient to choose $0 \neq \alpha \in \overline{K}$ such that $F_\alpha(Q) \neq 0$ for $Q \in W \setminus \{P\}$ which is always possible. Then every $Q \in \mathcal{V}(F_\alpha, C^*) \setminus \{P\}$ is a simple point of $\mathcal{C}^*$ and F and C^* are transverse in Q. □

4.5 Desingularization trees

We associate to a point P of $\overline{K}(\mathcal{C}^*)$ a tree which is called *desingularization tree* of P (see [VT91] on page 230) and denoted by $\mathcal{T}_P$. The root of $\mathcal{T}_P$ is the point P and the sons of a knot of $\mathcal{T}_P$ are its infinitely close points of order 1. It will be useful to include the corresponding exceptional divisor in every knot of $\mathcal{T}_P$. The tree $\mathcal{T}_P$ is defined recursively by

1. if P is simple, the P corresponds to a place $\mathfrak{P}$ and

$$\mathcal{T}_P := [P, E_P]$$

where $E_P := \mathfrak{P}$,

2. if P is singular, then

$$\mathcal{T}_P := [[P, E_P], [\mathcal{T}_Q \mid Q \in \mathfrak{B}(P)]]$$

where E_P is the exceptional divisor of P.

The following proposition and theorem show that the desingularization tree of a point P of $\overline{F}/\overline{K}$ is always finite. This permits us to establish a bijective correspondence between the places $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ above the point P and the leaves of the tree $\mathcal{T}_P$.

Let $P := (0, 0; x, y)$ be a singular point of $\overline{F}/\overline{K}$ and

$$C(X, Y) = \prod_{i=1}^{n} (\alpha_i X + \beta_i Y)^{e_i} + H(X, Y)$$

be the defining polynomial of the coordinate pair (x, y). The degrees of the monomials of H are greater than $m := \deg \mathrm{Init}(C) = \sum_{i=1}^{n} e_i$. Assume that $\beta_1 \neq 0$. Then the strict transform $C^{[x]}$ of C with respect to x is

$$C^{[x]}(X, Y_1) = \prod_{i=1}^{n} (\alpha_i + \beta_i Y)^{e_i} + X^{n-m} H^{[x]}(X, Y_1).$$

The infinitely close point $Q_1 := (0, -\alpha_1/\beta_1; x, y_1)$ of P is equivalent to the point $(0, 0; x, y_1 - \alpha_1/\beta_1)$. The defining polynomial of the coordinate pair $(x, y_1 - \alpha_1/\beta_1)$ is

$$\begin{aligned} C^{[x]}(X, Y - \alpha_1/\beta_1) &= \prod_{i=1}^{l} (\alpha_i + \beta_i (Y - \alpha_1/\beta_1)^{e_i} + X^{n-m} H^{[x]}(X, Y_1 - \alpha_1/\beta_1) \\ &= (\beta_1 Y)^{e_1} \prod_{i=2}^{l} (\alpha_i + \beta_i (Y - \alpha_1/\beta_1)^{e_i} + X^{n-m} H^{[x]}(X, Y_1 - \alpha_1/\beta_1) \end{aligned}$$

We have $m_{Q_1} = \deg \mathrm{Init}(C^{[x]}(X, Y - \alpha_1/\beta_1))$ which is clearly at most e_1. Similiary, we show that for some $\beta_i = 0$ the multiplicity of the corresponding infinitely close point is at most e_i. Thus we have shown the following theorem.

Theorem 4.22 *Let P be a singular point of $\overline{F}/\overline{K}$ and $Q_1, \ldots, Q_l$ be its infinitely close points of order one. Let m_i be the multiplicity of Q_i for $i = 1, \ldots, l$. We have $m_P \geq \sum_{i=1}^{l} m_i$.*

If all singular points of the curve $\mathcal{C}^*$ are ordinary, i.e. all e_i are one, then only one blow up is necessary for each point to find the simple points above the singular points. It is clear that the desingularization algorithm stops in this case. The situation is more difficult when there are non-oridinary singular points. We need the following results to show that the desingularization algorithm stops.

Proposition 4.23 *Let P be a point of $\overline{K}(\mathcal{C}^*)$ and $\mathfrak{P} \in \mathbb{P}_{\overline{F}/\overline{K}}$ a place above the point P. For all $u \in \mathcal{O}_{\mathfrak{P}}$ there exists $N_u \in \mathbb{N}$ such that $u \in \mathcal{O}_{P^{\mathfrak{P}(n)}}$ for $n \geq N_u$.*

Proof: Set $P_0 := P$ and $P_i := P^{\mathfrak{P}^{(i)}}$ for $i \in \mathbb{N}_{\geq 0}$. Let $\Gamma_i := (x_i, y_i)$ be coordinate pairs of $\overline{K}(\mathcal{C}^*)$ such that $P_i \equiv (0, 0; x_i, y_i)$ and $\nu_{\mathfrak{P}}(x_i) \leq \nu_{\mathfrak{P}}(y_i)$. By lemma 4.9 we have

$$z/x_i \in \mathcal{O}_{P_{i+1}} \text{ for every } z \in \mathcal{M}_{P_i}$$

for all $i \in \mathbb{N}$. Let $u \in \mathcal{O}_{\mathfrak{P}}$. Since the algebraic function field $\overline{F}$ is equal to the quotient field of any local ring of a point of $\overline{K}(\mathcal{C}^*)$ we can always find $f, g \in \mathcal{O}_{P_0}$ such that $u = f/g$. If $g \notin \mathcal{M}_{P_0}$, then $u \in \mathcal{O}_{P_0}$ and the proof is finished. If $g \in \mathcal{M}_{P_0}$ then there exists a maximal n such that

$$g_n := g/(x_0 x_1 \cdots x_n) \in \mathcal{O}_{P_{n+1}}$$

because $\nu_{\mathfrak{P}}(x_i) > 0$ and $\mathcal{O}_{P_i} \subseteq \mathcal{O}_{\mathfrak{P}}$ for all $i \in \mathbb{N}$. We must have $\nu_{\mathfrak{P}}(g_n) = 0$. Otherwise $g_n \in \mathfrak{P} \cap \mathcal{O}_{P_{n+1}} = \mathcal{M}_{P_{n+1}}$ and again by lemma 4.9 $g_n/x_{n+1} \in \mathcal{O}_{P_{n+2}}$ contradicting that n is maximal. Consequently we have $g_n \in \mathcal{O}_{P_{n+1}} \setminus \mathcal{M}_{P_{n+1}}$ and g_n is invertible in $\mathcal{O}_{P_{n+1}}$. Set $f_n := f/(x_0 x_1 \cdots x_n)$. Since $\nu_{\mathfrak{P}}(f) \geq \nu_{\mathfrak{P}}(g)$ and $g_n \in \mathcal{O}_{P_{n+1}}$ we have $f_n \in \mathcal{O}_{P_{n+1}}$. This concludes the proof as $u = f_n g_n^{-1} \in \mathcal{O}_{P_{n+1}}$. □

Theorem 4.24 *Let P be a point of $\overline{K}(\mathcal{C}^*)$ and $\mathfrak{P} \in \mathbb{P}_{\overline{F}/\overline{K}}$ above the point P. There exists $N \in \mathbb{N}$ such that $P^{\mathfrak{P}^{(n)}} \equiv \mathfrak{P}$ for all $n \geq N$.*

Proof: By lemma 2.20 there exists $u \in \mathfrak{P}$ such that $\mathfrak{P}$ is the unique zero of u. By the preceding proposition there exist a $l \in \mathbb{N}$ such that $u \in \mathcal{O}_{P_l}$. Since $u \in \mathfrak{P} \cap \mathcal{O}_{P_l} = \mathcal{M}_{P_l}$ $\mathfrak{P}$ is the unique place above P_l. Let t be a local parameter of $\mathfrak{P}$. Then there exists a $n \geq l$ such that $t \in \mathcal{O}_{P_n}$ and in this case we have $E_{P_n} = \mathfrak{P}$ by the the definition of the exceptional divisor. Consequently P_n is a simple point since $m_{P_n} = \deg E_{P_n} = 1$. □

Remark 4.7 *Although differently formulated the preceding theorem is a well-known classical result of the blowing up theory (see [Per95] Proposition 5.8).*

In general, we need to blow up singular points on a projective curve. We can always reduce this to the affine case. The algorithm described above is called local *blow up since we always blow up the singular singular points independently from each other. We do not obtain a smooth curve in this way. But we do not need a smooth model of our plane singular curve. All we need are curves on which some of the missing places correspond to simple points. To describe this convienently we use the notion of a point of a function field. When we blow up a singular point we do not change the singularities of the other singular points. This is the reason why we can always work locally. We do not obtain a chain of blow ups like in [Per95] Proposition 5.8 (global blow up).*

Proposition 4.25 *Let $\mathcal{C}^* := \{C^* = 0\}$ be a plane projective curve and $\mathcal{S}$ be the set of singular points of $\mathcal{C}^*$. Let $\mathfrak{P} \in \mathbb{P}_{\overline{K}(\mathcal{C}^*)}$ be a place of $\overline{K}(\mathcal{C}^*)$ and $P \in \mathcal{C}^*$ be the unique point such that $\mathfrak{P} \mid P_*$. Then*

1. *$P \equiv \mathfrak{P}$ if P is simple,*
2. *otherwise there exists a unique leaf Q of $\mathcal{T}_P$ such that $Q \equiv \mathfrak{P}$.*

There is a bijective correspondence between the set

$$\{P_* \mid P \in \mathcal{C}^* \setminus \mathcal{S}\} \cup \{Q \mid Q \text{ is a leaf of } \mathcal{T}_P, P \in \mathcal{S}\}$$

and the set $\mathbb{P}_{\overline{K}(\mathcal{C}^*)}$ of places of $\overline{K}(\mathcal{C}^*)$.

Proof: This is a consequence of the preceding theorem and the fact any place is above a unique point of $\mathcal{C}^*$.

Theorem 4.26 *Let $\mathcal{C}^* := \{C^* = 0\}$ be a plane projective curve and $\mathcal{S}$ the set of singular points of $\mathcal{C}^*$. For all $P \in \mathcal{C}^*$ let $\mathcal{I}_P$ denote the set of all knots of $\mathcal{T}_P$ (including the point P). Let g be the genus of $\overline{K}(\mathcal{C}^*)$ and $n := \deg C^*$. Then*

$$g = \frac{(n-1)(n-2)}{2} - \frac{1}{2}\sum_{P\in\mathcal{S}}\sum_{Q\in\mathcal{I}_P} m_Q(m_Q - 1).$$

Proof: [Per95] Corollaire 5.12 □

4.6 Adjoint divisors

The adjoint divisor play an essential role in the study of plane curves. It permits to characterize canonical divisors of the function field of a plane projective curve. We deduce an important property of the adjoint divisor which plays a crucial role in the determination of a basis of the vector space associated to a divisor.

Definition 4.14 (Adjoint divisor of a point) *Let P be a point of $\overline{F}/\overline{K}$. The* adjoint divisor $\mathcal{A}_P$ of the point P *is defined recursively by*

$$\mathcal{A}_P := (m_P - 1)E_P + \sum_{Q\in\mathfrak{B}(P)} \mathcal{A}_Q$$

where m_P is the multiplicity of the point P and E_P is the exceptional divisors of the point P.

Definition 4.15 (Adjoint divisor of a curve) *Let $\mathcal{C}^* := \{C^* = 0\}$ be a projective curve and $P \in \mathcal{C}^*$. The adjoint divisor of the point P is the divisor*

$$\mathcal{A}_P := \mathcal{A}_{P_*}.$$

The adjoint divisor of the curve $\mathcal{C}^*$ *is the divisor*

$$\mathcal{A} := \sum_{P\in\mathcal{S}} \mathcal{A}_P$$

where $\mathcal{S}$ is the set of singular points of $\mathcal{C}^*$.

We have $\mathcal{A}_P \geq 0$ for every $P \in \mathcal{C}^*$ and $\deg \mathcal{A}_P = 0$ if and only if P is simple. The following proposition gives a sufficient condition that an element of $\overline{F}/\overline{K}$ is contained in a local ring of a point.

Proposition 4.27 *Let P be a point of $\overline{F}/\overline{K}$ and $z \in \overline{F}$. Then*

$$(z)_P \geq \mathcal{A}_P \Longrightarrow z \in \mathcal{O}_P.$$

Proof: We use induction on $N := \deg \mathcal{A}_P$. If $N = 0$ then P is a simple point and $(z)_P = \nu_{\mathfrak{P}}(z)\mathfrak{P}$ where $\mathfrak{P} \equiv P$. We have $\nu_{\mathfrak{P}}(z) \geq 0$ and consequently $u \in \mathcal{O}_{\mathfrak{P}} = \mathcal{O}_P$.

Let now P be a singular point and suppose that the proposition is true for all $n < N$. We suppose without loss of generality that $P = (0, 0; x, y)$ and that (x, y) is an exceptional coordinate pair of $\mathfrak{B}(P)$. Therefore

$$E_P = (x)_P = \sum_{Q \in \mathfrak{B}(P)} (x)_Q$$

and

$$\begin{aligned}(z)_P &= \sum_{Q \in \mathfrak{B}(P)} (x)_Q \\ &\geq \mathcal{A}_P \\ &= (m_P - 1)E_P + \sum_{Q \in \mathfrak{B}(P)} \mathcal{A}_Q \\ &= \sum_{Q \in \mathfrak{B}(P)} ((m_P - 1)(x)_Q + \mathcal{A}_Q).\end{aligned}$$

Since local divisors in different points of $\mathfrak{B}(P)$ have always disjoint supports, we have

$$(z)_Q \geq (m_P - 1)(x)_Q + \mathcal{A}_Q \text{ for all } Q \in \mathfrak{B}(Q).$$

This is equivalent to

$$\left(\frac{z}{x^{m_P - 1}}\right)_Q \geq \mathcal{A}_Q \text{ for every } Q \in \mathfrak{B}(Q).$$

Since $\deg \mathcal{A}_Q < \deg \mathcal{A}_P = N$ for all $Q \in \mathfrak{B}(P)$ we have

$$\frac{z}{x^{m_P - 1}} \in \bigcap_{Q \in \mathcal{B}(P)} \mathcal{O}_Q$$

by the induction hypothesis. The proposition is a consequence of the proposition 4.13 since

$$z \in x^{m_P - 1} \left(\bigcap_{Q \in \mathfrak{B}(P)} \mathcal{O}_Q \right) \subseteq \mathcal{O}_P.$$

□

Proposition 4.28 *Let $\mathcal{C}^* := \{C^* = 0\}$ be a projective plane curve and $\mathcal{A}(\mathcal{C}^*)$ its adjoint divisor. Then*

$$\deg \mathcal{A} = (n - 1)(n - 2) - 2g$$

where g is the genus of the curve and $n := \deg C^*$.

Proof: This is a consequence of the proposition 4.21 and theorem 4.26. □

Remark 4.8 *This formula for the degree of the adjoint divisor in function of the genus of a projective plane curve is well-know. In [Gor52] this formula is established by using the conductor of*

the local ring $\mathcal{O}_P$ in its integral closure $\overline{\mathcal{O}}_P$ taken in the field $\overline{K}(\mathcal{C}^*)$; the conductor of $\mathcal{O}_P$ is the ideal of $\mathcal{O}_P$ defined by

$$\mathfrak{C}_{\mathcal{O}_P}^{\overline{\mathcal{O}}_P} := \{z \in \mathcal{O}_P \mid z\overline{\mathcal{O}}_P \subseteq \mathcal{O}_P\}$$

which is also an ideal of $\overline{\mathcal{O}}_P$. We show that if

$$\mathcal{A}_P = \sum_{i=1}^{r} n_i \mathfrak{P}_i,$$

then

$$\mathfrak{C}_{\mathcal{O}_P}^{\overline{\mathcal{O}}_P} = \bigcap_{i=1}^{r} (\mathfrak{P}_i^{n_i} \cap \mathcal{O}_P).$$

Moreover, we have

$$\mathfrak{C}_{\mathcal{O}_P}^{\overline{\mathcal{O}}_P} = \{z \in \mathcal{O}_P \mid (z)_P \geq \mathcal{A}_P\}.$$

Lemma 4.29 *Let $P = (0, 0; x, y)$ be a point of $\overline{F}/\overline{K}$ such that X does not divide* $\mathrm{Init}(C)$ *where C is the defining polynomial of (x, y). Then we have*

$$\mathfrak{C}_{\mathcal{O}_P}^{\mathcal{O}_P[y/x]} = \mathcal{M}_P^{r-1}$$

where r is the multiplcity of the point P.

Proof: We show first $\mathcal{M}_P^{r-1} \subseteq \mathfrak{C}_{\mathcal{O}_P}^{\mathcal{O}_P[y/x]}$. Since the elements of $B := \{x^i y^j \mid i + j = r - 1\}$ generate $\mathcal{M}_P^{r-1}$ it suffices to show that $B \subset \mathfrak{C}_{\mathcal{O}_P}^{\mathcal{O}_P[y/x]}$. Let $u \in \mathcal{O}_P[y/x]$ and $x^i y^j$ with $i + j = r - 1$. Since X does not divide $\mathrm{Init}(C)$ we know that $x^{r-1}\mathcal{O}_P[y/x] \subseteq \mathcal{O}_P$. We have therefore

$$x^i y^j u = x^{r-1} \frac{y^j}{x^j} u \in x^{r-1}\mathcal{O}_P[y/x]$$

and by the definition of the conductor $x^i y^j \in \mathfrak{C}_{\mathcal{O}_P}^{\mathcal{O}_P[y/x]}$.

We show now $\mathfrak{C}_{\mathcal{O}_P}^{\mathcal{O}_P[y/x]} \subseteq \mathcal{M}_P^{r-1}$. Let $f \in \mathfrak{C}_{\mathcal{O}_P}^{\mathcal{O}_P[y/x]}$ and suppose without loss of generality that $f \in \overline{K}[x, y]$. We can write now

$$f := g_0 + g_1 x + g_2 x^2 + \ldots + g_l x^l$$

where $g_i \in \overline{K}[y]$ for $i = 0, 1, \ldots, l$. We show by induction that $g_i x^i \in \mathcal{M}_P^{r-1}$ for $i = 0, 1, \ldots, l$. We set for $k := 1, 2, \ldots, l$

$$f_k := g_k x^k + g_{k+1} x^{k+1} + \ldots + g_l x^l$$

and for $k > l$ $g_k := 0$ and $f_k := 0$. Note that

$$g_0 \frac{y}{x} = (f - f_1)\frac{y}{x} = f\frac{y}{x} - f_1 \frac{y}{x} \in \mathcal{O}_P.$$

There are polynomials $H_0, A_0 \in \overline{K}[X, Y]$ and $G_0 \in \overline{K}[Y]$ such that

$$G_0(y)\frac{y}{x} = \frac{A_0(x, y)}{H_0(x, y)}.$$

Let $B_0 \in \overline{K}[X,Y]$ be such that $H_0(0,0) \neq 0$ and

$$G_0 H_0 Y - X A_0 = B_0 C.$$

Since X does not divide $\mathrm{Init}(G_0 H_0 Y)$ we have $\mathrm{Init}(G_0 H_0 Y) \neq \mathrm{Init}(X A_0)$ and consequently $B_0 \neq 0$. We have $\deg \mathrm{Init}(G_0 H_0 Y) \geq \deg \mathrm{Init}(B_0 C) \geq r$ and therefore

$$\deg \mathrm{Init}(G_0) \geq r - \deg \mathrm{Init}(H_0) - \deg \mathrm{Init}(Y) = r - 1.$$

This shows $g_0 \in \mathcal{M}_P^{r-1}$. Since $\mathcal{M}_P^{r-1} \subset \mathfrak{c}_{\mathcal{O}_P}^{\mathcal{O}_P[y/x]}$ we have

$$f_1 = f - g_0 \in \mathfrak{c}_{\mathcal{O}_P}^{\mathcal{O}_P[y/x]}.$$

Suppose now that $g_i x^i \in \mathcal{M}_P^{r-1}$ for $i \leq n-1$. We have then

$$f_n = f - (g_0 + g_1 x + \ldots + g_{n-1} x^{n-1}) \in \mathfrak{c}_{\mathcal{O}_P}^{\mathcal{O}_P[y/x]}$$

and since $f_{n+1}/x^{n+1} \in \mathcal{O}_P$,

$$g_n \frac{y^{n+1}}{x} = g_n x^n \frac{y^{n+1}}{x^{n+1}} = (f_n - f_{n+1}) \frac{y^{n+1}}{x^{n+1}} = f_n \frac{y^{n+1}}{x^{n+1}} - f_{n+1} \frac{y^{n+1}}{x^{n+1}} \in \mathcal{O}_P.$$

By reasoning as previously we find $G_n \in \overline{K}[Y]$ such that $g_n = G_n(y)$ and $\deg \mathrm{Init}(G_n) \geq r-(n+1)$ and consequently $g_n x^n \in \mathcal{M}_P^{r-1}$ for $n = 0, 1, \ldots, l$. This proves $f \in \mathcal{M}_P^{r-1}$. □

Theorem 4.30 (Conductor $\mathfrak{c}_{\mathcal{O}_P}^{\overline{\mathcal{O}}_P}$ versus adjoint divisor $\mathcal{A}_P$) *Let $\overline{\mathcal{O}}_P$ be the integral closure of $\mathcal{O}_P$ in $\overline{F}$ and $\mathcal{A}_P$ be the adjoint divisor of P. Then we have*

$$\mathfrak{c}_{\mathcal{O}_P}^{\overline{\mathcal{O}}_P} = \{u \in \overline{F} \mid (u)_P \geq \mathcal{A}_P\}.$$

Proof: ($\supseteq$) : Let $v \in \overline{\mathcal{O}}_P$ and $u \in \overline{F}$ with $(u)_P \geq \mathcal{A}_P$. Since $\overline{\mathcal{O}}_P = \cap_{\mathfrak{P}|P} \mathcal{O}_{\mathfrak{P}}$ we have $(v)_P \geq 0$ and $(uv)_P \geq \mathcal{A}_P$. By Proposition 4.27 we have $uv \in \mathcal{O}_P$ and consequently $u \in \mathfrak{c}_{\mathcal{O}_P}^{\overline{\mathcal{O}}_P}$.
($\subseteq$) : We suppose without loss of generality that $P = (0,0;x,y)$ and that X does not divide the initial form of the defining polynomial C of (x,y). Then $\mathcal{O}_P[y/x] \subseteq \overline{\mathcal{O}}_P$ and consequently $\mathfrak{c}_{\mathcal{O}_P}^{\overline{\mathcal{O}}_P} \subseteq \mathfrak{c}_{\mathcal{O}_P}^{\mathcal{O}_P[y/x]}$. By the preceding lemma we have $\mathfrak{c}_{\mathcal{O}_P}^{\overline{\mathcal{O}}_P} \subseteq \mathcal{M}_P^{r-1}$. If $u \in \mathfrak{c}_{\mathcal{O}_P}^{\overline{\mathcal{O}}_P}$ and $v \in \overline{\mathcal{O}}_P$ then $u \in \mathcal{M}_P^{r-1}$ and also $uv \in \mathcal{M}_P^{r-1}$. Therefore $u/x^{r-1} \in \mathcal{O}_P[y/x]$ and $(u/x^{r-1})v \in \mathcal{O}_P[y/x]$ and consequently

$$w := \frac{u}{x^{r-1}} \in \mathfrak{c}_{\mathcal{O}_P[y/x]}^{\overline{\mathcal{O}}_P}.$$

To conclude the proof it suffices to show that

$$(w)_P \geq \sum_{Q \in \mathfrak{B}(P)} \mathcal{A}_Q = \mathcal{A}_P - (r-1)E_P$$

since then $(u)_P = (x^{r-1})_P = (r-1)E_P + (w)_P \geq \mathcal{A}_P$. We show this inequality by induction on $n := \deg \mathcal{A}_P$. If $n = 0$ then the point P is simple and the inequality is trivial. Suppose that $n > 0$. The induction hypothesis is that the theorem is true for all degrees smaller than n. Since the point P is singular we have $\deg \mathcal{A}_Q < \deg \mathcal{A}_P$ for any $Q \in \mathfrak{B}(P)$ and by using the induction hypothesis

it suffices to show that $w \in \mathfrak{C}_{\mathcal{O}_Q}^{\overline{\mathcal{O}}_Q}$. This is clear if P has only one infinitely close point since then $\mathcal{O}_P[y/x]$ is a local ring and consequently $\mathcal{O}_Q = \mathcal{O}_P[y/x]$ and $\overline{\mathcal{O}}_Q = \overline{\mathcal{O}}_P$. We suppose now that $\#\mathfrak{B}(P) \geq 2$ and let $Q \in \mathfrak{B}(P)$. Set

$$z := \prod_{Q' \in \mathfrak{B}(P) \setminus \{Q\}} \left(\frac{y}{x} - \frac{y}{x}(Q') \right).$$

The element $z \in \mathcal{O}_Q$ in such a way that

$$z^{-1} \in \mathcal{O}_Q \text{ and } z \in \mathcal{M}_{Q'} \text{ for all } Q' \in \mathfrak{B}(P) \setminus \{Q\}.$$

Let $v \in \overline{\mathcal{O}}_Q$. By the constuction of z there exist a sufficiently large integer n such that $(vz^m) \geq \mathcal{A}_{Q'}$ for all $Q' \in \mathfrak{B}(P) \setminus \{Q\}$ and consequently

$$vz^m \in \overline{\mathcal{O}}_Q \cap \left(\bigcap_{Q' \in \mathfrak{B}(P) \setminus \{Q\}} \mathcal{O}_{Q'} \right) \subseteq \overline{\mathcal{O}}_P.$$

Recall that $w \in \mathfrak{C}_{\mathcal{O}_P[y/x]}^{\overline{\mathcal{O}}_P}$ and consequently $wvz^m \in \mathcal{O}_P[y/x] \subset \mathcal{O}_Q$. Since z is invertible in $\mathcal{O}_Q$ we have $wv \in \mathcal{O}_Q$ and consequently $w \in \mathfrak{C}_{\mathcal{O}_Q}^{\overline{\mathcal{O}}_Q}$ and by the induction hypothesis $(w)_Q \geq \mathcal{A}_Q$. Repeating the construction for all $Q \in \mathfrak{B}(P)$ we obtain

$$(w)_P = \sum_{Q \in \mathfrak{B}(P)} (w)_Q \geq \sum_{Q \in \mathfrak{B}(P)} \mathcal{A}_Q.$$

See also [Mnu97]. □

Proposition 4.31 (Canonical divisor) *Let $\mathcal{C}^* := \{C^* = 0\}$ be a projective plane curve and $\mathcal{A}$ its adjoint divisor. If G is a homogeneous polynomial such that $\deg G = \deg C^* - 3$ and $(G) \geq \mathcal{A}$ then*

$$\mathcal{K} := (G) - \mathcal{A}$$

is a canonical divisor of the function field $\overline{K}(\mathcal{C}^*)$.

Proof: [Gor52] Theorem 9. □

Definition 4.16 (Noether condition) *Let $\mathcal{C}^* := \{C^* = 0\}$ be a projective plane curve. Let $F, G \in \overline{K}[U, V, W]$ be two homogeneous polynomials such that C^* does not divide G. We say the pair (F, G) satisfies the* Noether condition in the point $P \in \mathcal{C}^*$ *if*

$$\overline{F}^P / \overline{G}^P \in \mathcal{O}_{P_*}.$$

Theorem 4.32 (Max Noether's Fundamental Theorem) *Let $\mathcal{C}^* := \{C^* = 0\}$ a projective plane curve. Let $F, G \in \overline{K}[U, V, W]$ be two homogeneous polynomials such that C^* does not divide G. Then the following conditions are equivalent:*

1. *there exist two homogeneous polynomials $A, B \in \overline{K}[U, V, W]$ such that $\deg A + \deg G = \deg B + \deg C^* = \deg F$ and*

$$F = AG + BC^*.$$

2. the pair (F, G) satisfies the Noether condition in all points of $\mathcal{C}^*$.

Proof: See [Ful69] on page 120. □

Theorem 4.33 *Let $\mathcal{C}^* := \{C^* = 0\}$ be a projective plane curve, $\mathcal{A}$ be its adjoint divisor and $F, G \in \overline{K}[U, V, W]$ be two homogeneous polynomials such that C^* does not divide G. If*

$$(F) \geq \mathcal{A} + (G),$$

then there exist two homogeneous polynomials $A, B \in \overline{K}[U, V, W]$ such that $\deg A + \deg G = \deg B + \deg C^* = \deg F$ *and*

$$F = AG + BC^*.$$

Proof: If $(F) \geq \mathcal{A} + (G)$, then $(F)_P \geq \mathcal{A}_P + (G)_P$ and consequently we have $(\overline{F}^P/\overline{G}^P)_P = (F)_P - (G)_P \geq \mathcal{A}_P$ for all $P \in \mathcal{C}^*$. The theorem is now a consequence of proposition 4.27 and Max Noether's Fundamental theorem. □

Theorem 4.34 *Let $\mathcal{C}^* := \{C^* = 0\}$ be a projective plane curve and $\mathcal{A}$ be its adjoint divisor. Let D and D' be two divisors of $\overline{K}(\mathcal{C}^*)$ such that $D \equiv D'$ and suppose that D' is positive. If $G \in \overline{K}[U, V, W]$ is a homogeneous polynomial such that*

$$(G) = D + \mathcal{A} + R$$

for some positive divisor R, then there exists a homogeneous polynomial $G' \in \overline{K}[U, V, W]$ such that $\deg G' = \deg G$ *and*

$$(G') = D' + \mathcal{A} + R.$$

Proof: Since $D \equiv D'$ there exists $z \in \overline{K}(\mathcal{C}^*)$ such that

$$D = (z) + D'.$$

Let $H, H' \in \overline{K}[U, V, W]$ be two homogeneous polynomials such that $(z) = (H) - (H')$. We have

$$\begin{aligned} (H'G) &= (H') + (G) \\ &= (H') + D + \mathcal{A} + R \\ &= (H') + (z) + D' + \mathcal{A} + R \\ &= (H) + D' + \mathcal{A} + R. \end{aligned}$$

Since the divisors $(H), D', \mathcal{A}$ and R are positive we have

$$(H'G) \geq \mathcal{A} + (H).$$

By the preceding theorem there exist two homogeneous polynomials $G', B \in \overline{K}[U, V, W]$ such that $\deg G' + \deg H = \deg B + \deg C^* = \deg H'G$ and

$$H'G = G'H + BC^*$$

We have $(H'G) = (G'H)$ and consequently $(G') = (H'G) - (H) = D' + \mathcal{A} + R$. □

We can derive from the following theorem an algorithm which computes a basis of the vector space associated to a divisor of the function field of a plane curve.

Theorem 4.35 *Let $\mathcal{C}^* := \{C^* = 0\}$ be a projective plane curve, $\mathcal{A}$ be its adjoint divisor and D be a divisor of $\overline{K}(\mathcal{C}^*)$. Let $G_0 \in S_d$ such that C^* does not divide G_0 and*

$$(G_0) \geq D + \mathcal{A}.$$

Then

$$\mathcal{L}(D) := \{\overline{G}/\overline{G_0} \mid G \in S_d \text{ non-divisible by } C^* \text{ and } (G) \geq (G_0) - D\} \cup \{0\}$$

where $\overline{G}$ and $\overline{G_0}$ are the residual images of, respectively, G and G_0 in $\overline{K}[\mathcal{C}^*]$ and $S_d \subset \overline{K}[U, V, W]$ is the set of homogeneous polynomials of degree d.

Proof: ($\supseteq$) : Let $G \in \overline{K}[U, V, W]$ be a homogeneous polynomial such that $\deg G = \deg G_0$, C^* does not divide G and $(G) \geq (G_0) - D$. Set $z := \overline{G}/\overline{G_0}$. Then

$$(z) + D = (G) - (G_0) + D \geq 0$$

so that $z \in \mathcal{L}(D)$.
($\subseteq$) : Let $z \in \mathcal{L}(D) \setminus \{0\}$. Then $D' := D + (z) \geq 0$ by the definition of $\mathcal{L}(D)$. Since $D' \equiv D$ and $(G_0) \geq D + \mathcal{A}$ we can apply the preceding theorem with $R := (G_0) - (D + \mathcal{A}) \geq 0$ to find a $G' \in \overline{K}[U, V, W]$ such that $\deg G' = \deg G$ and

$$(G') = D' + \mathcal{A} + R.$$

We have

$$(G') - (G_0) = D' - D = (z).$$

Let $z' := \overline{G}/\overline{G_0}$. Then $(z/z') = 0$. Since only the constants have no zeros and no poles $\alpha := z/z' \in \overline{K}$ and consequently

$$z = \alpha z' := \alpha \overline{G'}/\overline{G_0}$$

which proves that z can be written in the above form. □

Let us remark that the theorem also applies to a divisor D which is not positive. It is clear that

$$(G_0) \geq \mathcal{A} + D \Longrightarrow (G_0) \geq (\mathcal{A} + D)_+.$$

The following algorithm is called *Brill-Noether algorithm* and uses exactly the preceding theorem to compute a basis of the vector space associated to a divisor of the function field of a plane curve.

Algorithm 1 Brill-Noether

- Input: A divisor of the function field $\overline{K}(\mathcal{C}^*)$ where $\mathcal{C}^*$ is a projective curve.
- Output: A basis of the vector space $\mathcal{L}(D)$.

1: Set $B := D + \mathcal{A}$ where $\mathcal{A}$ is the adjoint divisor of the curve $\mathcal{C}^*$.
2: Let $d \in \mathbb{N}$ be sufficiently big so that there exists a homogeneous polynomial $G \in S_d$ which is not divisible by C^* such that $(G) \geq B_+$ where B_+ is the positive part of B.
3: Compute a basis $\{G_1, G_2, \ldots, G_s\}$ of the $\overline{K}$-vector space

$$V := \{G \in S_d \mid C \text{ divides } G \text{ or } (G) \geq B_+\} \cup \{0\}.$$

4: If $d \geq \deg C^*$, then it is necessary to reduce the basis $\{G_1, G_2, \ldots, G_s\}$ modulo the vector space

$$W := \{A \in S_d \mid C^* \text{ divides } A\}.$$

It suffices to choose a basis $\{A_1, A_2, \ldots, A_k\}$ of W with $A_i \in S_d$ $(i = 1, 2, \ldots, k)$ and to supplement this basis to a basis

$$\{A_1, A_2, \ldots, A_k, G'_1, G'_2, \ldots, G'_{s'}\}$$

of the vector space V. Now the vector space $V' \subset S_d \cup \{0\}$ spanned by the elements $\{G'_1, G'_2, \ldots, G'_{s'}\}$ is such that $V' \setminus \{0\}$ is exactly the set of all homogeneous polynomials of degree d and non-divisible by C^* such that $(G) \geq B_+$.

5: Choose $G_0 \in V'$ and compute the intersection divisor (G_0).

6: Determine like in the two preceding steps a basis $\{G_1, G_2, \ldots, G_k\}$ of the vector space $V'' \subset S_d \cup \{0\}$ such that $V'' \setminus \{0\}$ is the set of all homogeneous polynomials of degree d and non-divisible by C^* such that $(G) \geq (G_0) - D$.

7: Set $\overline{G_i} := G_i + \langle C^* \rangle \in \overline{K}[\mathcal{C}^*]$ for $i := 0, 1, \ldots, k$ and return

$$\{\overline{G_i}/\overline{G_0} \mid i = 1, 2, \ldots, k\}$$

which is a basis of $\mathcal{L}(D)$.

Let us summarize what we need to know in order to apply the Brill-Noether algorithm:

1. Compute the *adjoint divisor* of a projective plane curve $\mathcal{C}^* := \{C^* = 0\}$.
2. For a divisor B and an integer d compute a basis of the subspace V of $S_d \cup \{0\}$ where

$$V := \{G \in S_d \mid C^* \text{ divides } G \text{ or } (G) \geq B\} \cup \{0\}.$$

3. For a homogeneous polynomial $G \in S_d \setminus \{0\}$ compute the *intersection divisor* G with C^*.

4.7 Interpolating forms

Definition 4.17 (Interpolating form) *Let $\mathcal{C}^* := \{C^* = 0\}$ be a projective curve and B a divisor of $\overline{K}(\mathcal{C}^*)$. An* interpolating form *for the divisor B is a homogeneous polynomial $G \in \overline{K}[U, V, W]$ such that one of the following properties is satisfied:*

1. *C^* divides G.*
2. *$(G) \geq B$ if C^* does not divide G.*

We will use the $\mathfrak{P}$-adic power series expansion (see section IV.2.2. in [Sti93]) to compute the interpolating forms. Let us summerize the facts we need.

A *valued field* (L, ν) is a field L equipped with a *discrete valuation* ν. We say a sequence $(s_n)_{n \geq 0}$ in L is *convergent* if there exists an element $s \in L$ (called the *limit* of the sequence) which satisfies: for any $c \in \mathbb{R}$ there exists an index $N_c \in \mathbb{N}$ such that $\nu(s - s_n) \geq c$ whenever $n \geq N_c$. The limit is unique and we write $s = \lim_{n \to \infty} s_n$.

A sequence $(s_n)_{n \geq 0}$ is called a *Cauchy sequence* if it has the following property: for any $c \in \mathbb{R}$ there exists an index $N_c \in \mathbb{N}$ such that $\nu(s_n - s_m) \geq c$ whenever $n, m \geq N_c$. Any convergent sequence is a Cauchy sequence. In general, it is not true that all Cauchy sequences are convergent. Hence we have the following notions.

Definition 4.18 (Completion) *Let (L, ν) be a valued field.*

1. *(L, ν) is said to be* complete, *if any Cauchy sequence in L is convergent.*
2. *A* completion *of (L, ν) is a valued field $(\hat{L}, \hat{\nu})$ with the following properties*
   (a) *$L \subseteq \hat{L}$ and ν is the restriction of $\hat{\nu}$ to L.*
   (b) *$(\hat{L}, \hat{\nu})$ is complete.*
   (c) *L is dense in $\hat{L}$, i.e. for any $s \in \hat{L}$ there exists a sequence $(s_n)_{n \geq 0}$ in L with $\lim_{n \to \infty} s_n = s$.*

Proposition 4.36 *For any valued field (L, ν) there exists a completion $(\hat{L}, \hat{\nu})$. It is unique in the following sense: if $(\tilde{L}, \tilde{\nu})$ is another completion of $(\hat{L}, \hat{\nu})$ then there exists an isomorphism $f : \hat{L} \to \tilde{L}$ such that $\hat{\nu} = \tilde{\nu} \circ f$.*

Proof: [Sti93] IV.2.3 Proposition □

Definition 4.19 ($\mathfrak{P}$-adic completion) *Let $\mathfrak{P}$ be a place of the function field F/K. The completion with respect to the valuation $\nu_{\mathfrak{P}}$ is called the* $\mathfrak{P}$-adic completion *of F. We denote the completion by $\hat{F}_{\mathfrak{P}}$ and the valuation of $\hat{F}_{\mathfrak{P}}$ by $\hat{\nu}_{\mathfrak{P}}$.*

Theorem 4.37 ($\mathfrak{P}$-adic power series expansion) *Let $\mathfrak{P} \in \mathbb{P}_F$ be a place of degree one and t be a local parameter of $\mathfrak{P}$. Then any element $z \in \hat{F}_{\mathfrak{P}}$ has a unique representation of the form*

$$z(t) := \sum_{i=n}^{\infty} c_i t^i$$

with $n \in \mathbb{Z}$ and $c_i \in K$. This representation is called the $\mathfrak{P}$-adic power series expansion *of z with respect to t.*

On the other hand, if $(c_i)_{i \geq n}$ is a sequence in K, then the series $\sum_{i=n}^{\infty} c_i t^i$ converges in $\hat{F}_P$, and we have

$$\hat{\nu}_{\mathfrak{P}} \left(\sum_{i=n}^{\infty} c_i t^i \right) = ord \left(\sum_{i=n}^{\infty} c_i t^i \right)$$

where $ord\left(\sum_{i=n}^{\infty} c_i t^i\right) = \min\{i \mid c_i \neq 0\}$.

Proof: [Sti93] IV.2.6. Theorem □

Remark 4.9 (Computation of the $\mathfrak{P}$-adic power series expansion) *Let $\mathfrak{P}$ be a place of F/K of degree one and t be a local parameter of $\mathfrak{P}$. We show how to compute the $\mathfrak{P}$-adic power series expansion of $z \in \hat{F}_{\mathfrak{P}}$ with respect to t. Since $\deg \mathfrak{P} = 1$ we can identify the residue class field $F_{\mathfrak{P}}$ with K.*

Let $n_1 := \hat{\nu}_{\mathfrak{P}}(z)$. There exists an element $y \in F$ with $\hat{\nu}_{\mathfrak{P}}(z - y) > n_1$ (since F is dense in $\hat{F}_{\mathfrak{P}}$). By the Triangle Inequality it follows that $\nu_{\mathfrak{P}}(y) > n_1$, hence $y = u_1 t^{n_1}$ for some $u_1 \in \mathcal{O}_{\mathfrak{P}}^*$. Then $c_i := u_1(\mathfrak{P}) \in K \setminus \{0\}$ and $\nu_{\mathfrak{P}}(u_1 - c_1) > 0$. We have

$$z = c_1 t^{n_1} + (u_1 - c_1) t^{n_1} + (z - u_1 t^{n_1}) = c_1 t^{n_1} + (u_1 - c_1) t^{n_1} + (z - y).$$

Set $z_1 := (u_1 - c_1)t^{n_1} + (z - y)$. *We have now*

$$\left\{ \begin{array}{rcl} z & = & c_1 t^{n_1} + z_1 \\ n_2 & := & \hat{\nu}_{\mathfrak{P}}(z_1) > n_1. \end{array} \right.$$

In the same manner, we find $a_2 \in K \setminus \{0\}$ *and* $z_2 \in \hat{F}_{\mathfrak{P}}$ *such that*

$$\left\{ \begin{array}{rcl} z & = & c_1 t^{n_1} + c_2 t^{n_2} + z_2 \\ n_2 & := & \hat{\nu}_{\mathfrak{P}}(z_2) > n_2. \end{array} \right.$$

Iterating this construction, we obtain a representation of z *in the form* $z = \sum_{i=1}^{\infty} a_i t^{n_i}$. *By the preceding theorem we know that the representation is unique and therefore* $z = \sum_{i=1}^{\infty} a_i t^{n_i}$ *is the* $\mathfrak{P}$*-adic power series expansion of* z *with respect to* t.

Moreover, using properties of convergence we can easily show that for all $x, y \in \hat{F}_{\mathfrak{P}}$ *we have* $(x+y)(t) = x(t) + y(t)$ *and* $xy(t) = x(t)y(t)$ *where the addition and multiplication are those of the Laurent series field*

$$K((t)) = \left\{ \sum_{i=n}^{\infty} c_i t^i \mid n \in \mathbb{Z}, c_i \in K \right\}.$$

Consequently $\hat{F}_{\mathfrak{P}}$ *is isomorphic to the field* $K((t))$.

Definition 4.20 (Local parameterization) *Let* $\mathcal{C}^* := \{C^* = 0\}$ *be a projective plane curve,* $\mathfrak{P}$ *a place of* $\overline{K}(\mathcal{C}^*)$ *and* $P = (a : b : c) \in \mathcal{C}^*$ *the unique point with* $\mathfrak{P} \mid P_*$. *Let* t *be a local parameter of* $\mathfrak{P}$ *and* $\Gamma := (x, y)$ *be one of the three standard coordinate pairs such that* $P_* \in \mathcal{Z}(\Gamma)$. *We associate to the place* $\mathfrak{P}$ *its* local parameterization $[\mathfrak{P}]$ *which is defined by*

$$[\mathfrak{P}] := \left\{ \begin{array}{ll} [x(t), y(t), 1] & \text{if } c \neq 0, \\ [x(t), 1, y(t)] & \text{if } c = 0 \text{ and } b \neq 0, \\ [1, x(t), y(t)] & \text{otherwise.} \end{array} \right.$$

Note that the definition of $[\mathfrak{P}]$ *is in accordance with the definition of* P_*. *Further we associate to a homogeneous polynomial* $G \in \overline{K}[U, V, W]$ *its* local parameterization in $\mathfrak{P}$, *denoted by* $G[\mathfrak{P}]$. *It is defined by*

$$G[\mathfrak{P}] := G(s_0, s_1, s_2)$$

where $[\mathfrak{P}] = [s_0, s_1, s_2]$ *is the local parameterization of the place* $\mathfrak{P}$.

We assume that $c \neq 0$. Then by definition s_0, s_1 and s_2 are the $\mathfrak{P}$-adic power series expansions of, respectively, u/w, v/w and $w/w = 1$. Let $G \in \overline{K}[U, V, W]$ be a homogeneous polynomial, $g := \overline{G}^P$ and $g(t) \in \overline{K}((t))$ be the $\mathfrak{P}$-adic power series expansion of g with respect to t. We have

$$g(t) = \frac{G(u, v, w)}{w^{\deg G}}(t) = G(u/w, v/w, 1)(t) = G(s_0, s_1, s_2) = G[\mathfrak{P}].$$

By the theorem 4.37 we have

$$\nu_{\mathfrak{P}}(g) = \operatorname{ord}(G[\mathfrak{P}])$$

and since $g \in \mathcal{O}_{\mathfrak{P}}$ we have $\nu_{\mathfrak{P}}(g) \geq 0$. Therefore we can write

$$G[\mathfrak{P}] = \sum_{i=0}^{\infty} c_i t^i \in \overline{K}((t)).$$

For $n \in \mathbb{N}$ we define the truncated power series

$$G[\mathfrak{P}]^{(n)} := (c_0, c_1, \ldots, c_{n-1}) \in \overline{K}^n$$

and the map

$$\Psi_{n\mathfrak{P}} : \left\{ \begin{array}{ccc} S_d \cup \{0\} & \rightarrow & \overline{K}^n \\ G & \mapsto & G[\mathfrak{P}]^{(n)}. \end{array} \right.$$

It is clear that $\Psi_{n\mathfrak{P}}$ is a $\overline{K}$-linear map and that its kernel is

$$\begin{aligned} \ker \Psi_{n\mathfrak{P}} &= \{G \in S_d \mid \mathrm{ord}(G[\mathfrak{P}]) \geq n\} \cup \{0\} \\ &= \{G \in S_d \mid \nu_{\mathfrak{P}}(\overline{G}^P) \geq n\} \cup \{0\}. \end{aligned}$$

We fix a basis $\{H_1, H_2, \ldots, H_l\}$[2] of the vector space $S_d \cup \{0\}$ and set

$$\Psi_{n\mathfrak{P}}(H_j) = (c_{j,0}, c_{j,1}, \ldots, c_{j,(n-1)})$$

for $j = 0, 1, \ldots, l$. Consider the matrix

$$M[n\mathfrak{P}]^{(d)} := \begin{bmatrix} c_{1,0} & c_{1,1} & \cdots & c_{1,(n-1)} \\ c_{2,0} & c_{2,1} & \cdots & c_{2,(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ c_{l,0} & c_{l,1} & \cdots & c_{l,(n-1)} \end{bmatrix}.$$

It is clear that

$$\nu_{\mathfrak{P}}\left(\sum_{i=1}^{l} \alpha_i \overline{H}^P\right) \geq n \Longleftrightarrow [\alpha_1, \alpha_2, \ldots, \alpha_l] M[n\mathfrak{P}]^{(d)} = 0.$$

To find a basis of the vector space of interpolating forms of degree d for a positive divisor

$$B := n_1\mathfrak{P}_1 + n_2\mathfrak{P}_2 + \ldots + n_k\mathfrak{P}_k$$

it suffices to calculate the left kernel of the matrix

$$M[B]^{(d)} = [M[n_1\mathfrak{P}_1]^{(d)} \mid M[n_2\mathfrak{P}_2]^{(d)} \mid \ldots \mid M[n_k\mathfrak{P}_k]^{(d)}]$$

since

$$(\sum_{i=1}^{l} \alpha_i H_i) \geq B \text{ or } C^* \text{ divides } \sum_{i=1}^{l} \alpha_i H_i \Longleftrightarrow [\alpha_1, \alpha_2, \ldots, \alpha_l] M[B]^{(d)} = 0.$$

It is clear that d must be sufficiently large if we want to find $G \in S_d$ with $(G) \geq B$ and C^* does not divide G.

Proposition 4.38 *Let $\mathcal{C}^* := \{C^* = 0\}$ be a projective plane curve and B a positive divisor of $\overline{K}(\mathcal{C}^*)$. If $d \in \mathbb{N}$ is such that*

$$d > \max\{n - 1, \frac{n}{2} + \frac{\deg B}{n} - \frac{3}{2}\},$$

where $n := \deg C^*$ then there exists $G \in S_d$ such that C^* does not divide G and $(G) \geq B$.

Proof : [Hac96], Corollaire 2.7.6 □

[2] We can take all the monomials of degree d. There are exactly $l = (d+1)(d+2)/2$ of them.

4.8 The Brill-Noether algorithm over a finite field

In this section we fix $K := \mathbb{F}_q$. Let $\mathcal{C}^* := \{C^*\}$ be a projective plane curve defined over K and $\overline{F}$ and F denote, respectively, the function fields $\overline{K}(\mathcal{C}^*)$ and $K(\mathcal{C}^*)$ of $\mathcal{C}^*$. We show how to use the Brill-Noether-Algorithm to compute a basis of $\mathcal{L}(D)$ where D is a divisor of F. To do that we study the properties of extensions F' with $F \subseteq F' \subseteq \overline{F}$.

4.8.1 Algebraic extensions of function fields

Any function field over K can be regarded as a finite extension of a rational function field $K(x)$. This is one of the reasons why it is of interest to investigate field extensions F'/F of algebraic function fields.

> In this section, we shall describe the relationship between places, divisors and the genera of F'/K' and F/K where $F' = K'F$ is a *constant field extension*. The study of constant field extensions reduces many problems to the case where the constant field is algebraically closed (which is often simpler because all places have degree one). This permits us to use the Brill-Noether algorithm for the construction of geometric Goppa codes over finite fields even though the algorithm is defined only for algebraically closed fields.

F/K denotes an algebraic function field of one variable with the full constant field K. We consider function fields F'/K' (where K' is the full constant field of F') such that $F' \supseteq F$ is an algebraic extension and $K' \supseteq K$. We consider only extensions $F' \supseteq F$ with $F' \subseteq \overline{F}$.

Definition 4.21 (Algebraic, finite and constant field extensions) *An algebraic function field F'/K' is called an* algebraic extension *(*finite extension*) of F/K if $F' \supseteq F$ is an algebraic field extension (finite field extension) and $K' \supseteq K$. The algebraic extension F'/K' of F/K is called a* constant field extension *if $F' = FK'$, the composite field of F and K'.*

A place $\mathfrak{P}' \in \mathbb{P}_{F'}$ is said to lie over *$\mathfrak{P} \in \mathbb{P}_F$ if $\mathfrak{P} \subseteq \mathfrak{P}'$. We also say that $\mathfrak{P}'$ is an extension of $\mathfrak{P}$, and we write $\mathfrak{P}' \mid \mathfrak{P}$.*

Proposition 4.39 *Let F'/K' be an algebraic extension of F/K. Then the following assertions are equivalent:*

1. $\mathfrak{P}' \mid \mathfrak{P}$.
2. $\mathcal{O}_{\mathfrak{P}} \subseteq \mathcal{O}_{\mathfrak{P}'}$.
3. *There exists an integer $e \geq 1$ such that $\nu_{\mathfrak{P}'}(x) = e \cdot \nu_{\mathfrak{P}}(x)$ for all $x \in F$.*

Proof: [Sti93], III.1.4 Proposition □

Definition 4.22 *Let F'/K' be an algebraic extension of F/K, and let $\mathfrak{P}' \in \mathbb{P}_{F'}$ be a place of F'/K' lying over $\mathfrak{P} \in \mathbb{P}_F$.*

1. *The integer $e(\mathfrak{P}' \mid \mathfrak{P}) := e$ with*

$$\nu_{\mathfrak{P}'}(x) = e \cdot \nu_{\mathfrak{P}}(x) \text{ for any } x \in F$$

is called the ramification index *of $\mathfrak{P}'$ over $\mathfrak{P}$. We say that $\mathfrak{P}' \mid \mathfrak{P}$ is* ramified *if $e(\mathfrak{P}' \mid \mathfrak{P}) > 1$, and $\mathfrak{P}' \mid \mathfrak{P}$ is* unramified *if $e(\mathfrak{P} \mid \mathfrak{P}') = 1$.*

2. $f(\mathfrak{P}' \mid \mathfrak{P}) := [F'_{\mathfrak{P}'} : F_{\mathfrak{P}}]$ *is called the* relative degree *of* $\mathfrak{P}'$ *over* $\mathfrak{P}$.

Note that $f(\mathfrak{P}' \mid \mathfrak{P})$ *can be finite or infinite; the ramification index, however, is always a natural number.*

Proposition 4.40 *Let* F'/K' *be an algebraic extension of* F/K.

1. *For any place* $\mathfrak{P}' \in \mathbb{P}_{F'}$ *there is exactly one place* $\mathfrak{P} \in \mathbb{P}_F$ *such that* $\mathfrak{P}' \mid \mathfrak{P}$, *namely* $\mathfrak{P} = \mathfrak{P}' \cap F$.
2. *Conversely, any place* $\mathfrak{P} \in \mathbb{P}_{F'}$ *has at least one, but finitely many, extensions* $\mathfrak{P}' \in \mathbb{P}_{F'}$.

Proof: [Sti93], III.1.7 Proposition □

Theorem 4.41 *Let* F'/K' *be a finite extension of* F/K. *For every place* $\mathfrak{P} \in \mathbb{P}_F$ *we have*

$$\sum_{\mathfrak{P}' \mid \mathfrak{P}} e(\mathfrak{P}' \mid \mathfrak{P}) f(\mathfrak{P}' \mid \mathfrak{P}) = [F' : F].$$

Proof: [Sti93], III.1.11 Theorem □

Definition 4.23 (Conorm) *Let* F'/K' *be an algebraic extension of* F/K. *For a place* $P \in \mathbb{P}_F$ *we define its* conorm *(with respect to* F'/K'*) by*

$$Con_{F'/F}(\mathfrak{P}) := \sum_{\mathfrak{P}' \mid \mathfrak{P}} e(\mathfrak{P}' \mid \mathfrak{P}) \mathfrak{P}',$$

where the sum runs over all places $\mathfrak{P}' \in \mathbb{P}_{F'}$ *lying over* $\mathfrak{P}$. *The conorm map is extended to a homomorphism from* $\mathcal{D}_F$ *to* $\mathcal{D}_{F'}$ *by setting*

$$Con_{F'/F}\left(\sum n_{\mathfrak{P}} \mathfrak{P}\right) := \sum n_{\mathfrak{P}} Con_{F'/F}(\mathfrak{P}).$$

4.8.2 Constant field extensions

We are especially interested in constant field extensions. The following theorem gives in a nutshell the most important properties of constant field extensions.

Theorem 4.42 *Let* F/K *be a function field,* $K \subseteq K' \subseteq \overline{K}$ *an algebraic extension of* K *and* $F' = FK'$.

1. K' *is the full constant field of* F'/K'.
2. F'/F *is unramified (i.e.* $e(\mathfrak{P}' \mid \mathfrak{P}) = 1$ *for all* $\mathfrak{P} \in \mathbb{P}_F$ *and all* $\mathfrak{P}' \in \mathbb{P}_{F'}$ *with* $\mathfrak{P}' \mid \mathfrak{P}$*).*
3. F'/K' *has the same genus as* F/K.
4. W *is a canonical divisor of* F/K *if and only if and only if* $Con_{F'/F}(W)$ *is a canonical divisor of* F'/K'.
5. *Let* $D \in \mathcal{D}_F$ *and set* $D' := Con_{F'/F}(D)$. *Then*

$$\deg D' = \deg D$$

and

$$\dim D' = \dim D.$$

Moreover,

(a) *a basis of the K-vector space $\mathcal{L}(D)$ is a basis of the K'-vector space $\mathcal{L}(D')$, and*

(b) *a basis of the K'-vector space $\mathcal{L}(D')$ containing only elements of F is a basis of the K-vector space $\mathcal{L}(D)$.*

Proof: [Sti93], proposition III.6.1 and theorem III.6.3 □

We compute a basis of the vector space $\mathcal{L}(D)$ where $D \in \mathcal{D}_F$ is a divisor of F by applying the Brill-Noether algorithm to the divisor $\overline{D} := \mathrm{Con}_{\overline{F}/F} D$ and making sure that the basis contains only elements of $K(\mathcal{C}^*)$. Consider the Frobenius map

$$\sigma : \left\{ \begin{array}{ccc} \overline{K} & \rightarrow & \overline{K} \\ \alpha & \mapsto & \alpha^q \end{array} \right. .$$

Let $f \in \overline{K}[\mathcal{C}^*]$ be a form and $F \in \overline{K}[U,V,W]$ a homogeneous polynomial with $f := F + \langle C^* \rangle$. We set

$$f^\sigma := F^\sigma + \langle C^* \rangle$$

where σ acts on the coefficients of F. Since $C^* \in K[U,V,W]$ it is clear that $f^\sigma = 0$ if and only if $f = 0$. We can therefore extend σ to the field $\overline{F}$ in the following way:

$$\sigma : \left\{ \begin{array}{ccc} \overline{F} & \rightarrow & \overline{F} \\ f/g & \mapsto & f^\sigma / g^\sigma \end{array} \right. .$$

It is easy to show that for any $z \in \overline{F}$ we have $z \in F \Longleftrightarrow \sigma(z) = z$, i.e. the automorphism σ fixes the field F.

The following definition is classic.

Definition 4.24 *Let E be a set to which the map σ is extended. We say $a \in E$ is* σ-conjugated *to $b \in E$ if there exists $i \in \mathbb{N}$ with $\sigma^i(a) = b$. We call the set*

$$\mathrm{Orb}_\sigma a := \{\sigma(a) \mid i \in \mathbb{N}\}$$

the σ-orbit *of a.*

Remark 4.10 *We show that σ can be extended to points P, local rings $\mathcal{O}_P$, places $\mathfrak{P}$ and divisors D of $\overline{F}/\overline{K}$, points of $\mathcal{C}^*$, desingularization trees $\mathcal{T}_P$ and powers series expansions $z(t)$. A σ-orbit can always be reconstructed from one element by applying σ. In the following we always choose an element to represent the σ-orbit.*

Proposition 4.43 *Let $K_r := \mathbb{F}_{q^r}$ and consider the constant field extension $F_r := FK_r$. If $\mathfrak{P}$ is any place of F of degree m, then there exist $d = \gcd(m,r)$ pairwise distinct places $\mathfrak{P}'_1, \mathfrak{P}'_2, \ldots, \mathfrak{P}'_d$ of F_r above $\mathfrak{P}$. These places are of degree m/d and mutually conjugated by the automorphism σ.*

Proof: [Sti93], lemma V.1.9 □

Proposition 4.44 *Let $\mathcal{Q} \in \mathbb{P}_{\overline{F}/\overline{K}}$.*

1. *$\nu_\mathcal{Q} \circ \sigma$ is a discrete valuation of $\overline{F}/\overline{K}$.*
2. *$\mathcal{Q}^\sigma := \sigma(\mathfrak{P})$ is a place of $\overline{F}/\overline{K}$, $\sigma(\mathcal{O}_\mathcal{Q}) = \mathcal{O}_{\mathcal{Q}^\sigma}$ and $\nu_\mathcal{Q} \circ \sigma = \nu_{\mathcal{Q}^\sigma}$.*

3. *Let* $\mathfrak{P} := \mathcal{Q} \cap F$ *and* $r := \deg \mathfrak{P}$. *Then* $\mathcal{Q}^{\sigma^r} = \mathcal{Q}$ *and*

$$\mathrm{Con}_{\overline{F}/F}\mathfrak{P} = \sum_{\mathcal{Q}' \in \mathrm{Orb}_\sigma \mathcal{Q}} \mathcal{Q}'.$$

Proof: The assertions (1) and (2) follow directly from the fact that σ is an automorphism of the field $\overline{F}$ such that $\sigma(\alpha) = \alpha$ for all $\alpha \in \overline{K}$. The assertion (3) follows from the preceding proposition. □

Remark 4.11 *By the preceding proposition it suffices to consider only one place in the support of* $\mathrm{Con}_{\overline{F}/F}\mathfrak{P}$ *since we can always determine the other places by the action of* σ. *The same argument is also valid for a divisor* $D = n_1\mathfrak{P}_1 + n_2\mathfrak{P}_2 + \ldots + n_k\mathfrak{P}_k$ *of the function field* F/K; *in this case it suffices to consider only one place of* $\mathrm{supp}\,\mathrm{Con}_{\overline{F}/F}\mathfrak{P}_i$ *for each place* $\mathfrak{P}_i \in \mathrm{supp}D$.

Recall that the Brill-Noether algorithm uses the adjoint divisor of the curve $\mathcal{C}^*$ and intersection divisors of homogeneous polynomials with the curve. If we want to take advantage of the preceding remark we must know if these divisors are the conorms of some divisors of the function field F/K. We introduce the following definition which facilitates the treatment of this question.

Definition 4.25 *Let* σ *be the Frobenius map extended to the field* $\overline{F}$.

1. *Let* $D := \sum n_{\mathcal{Q}}\mathcal{Q}$ *be a divisor of* $\overline{F}/\overline{K}$. *We call the divisor*

$$D^\sigma := \sum n_{\mathcal{Q}}\mathcal{Q}^\sigma$$

the conjugated divisor *of* D *by* σ. *We say* D *is* K-rational *if* $D = D^\sigma$.

2. *Let* $P := (a, b; x, y)$ *be a point of* $\overline{F}/\overline{K}$. *We call*

$$P^\sigma := (\sigma(a), \sigma(b); \sigma(x), \sigma(y))$$

the conjugated point *of* P *by* σ.

3. *Let* $\mathcal{T}_P$ *be the desingularization tree of the point* P. *The* conjugated tree *of* $\mathcal{T}_P$ *by* σ *is the tree defined recursively by*

   (a) $\mathcal{T}_P^\sigma := [P^\sigma, E_P^\sigma]$ *if* P *is a leaf.*
   (b) $\mathcal{T}_P^\sigma := [P^\sigma, \{\mathcal{T}_Q^\sigma \mid Q \in \mathfrak{B}(P)\}]$ *otherwise.*

Lemma 4.45 *Let* E *be a divisor of* $\overline{F}/\overline{K}$. *Then there exists a divisor* D *of* F/K *such that* $\mathrm{Con}_{\overline{F}/\overline{K}}D = E$ *if and only if* E *is* K*-rational. There is a bijective correspondence between the divisors of* F/K *and the* K*-rational divisors of* $\overline{F}/\overline{K}$.

Proof: This is a consequence of the proposition 4.44. □

The following lemma and its corollary are easily proved.

Lemma 4.46 *Let* P *be a point of* $\overline{F}/\overline{K}$, $\mathfrak{P}$ *be a place of* $\overline{F}/\overline{K}$, $\mathcal{T}_P$ *be a desingularization tree and* $z \in \overline{F}$.

1. *P^σ is a point of $\overline{F}/\overline{K}$.*
2. *$\mathfrak{P} \mid P$ if and only if $\mathfrak{P}^\sigma \mid P^\sigma$.*
3. *$\mathcal{T}_P^\sigma = \mathcal{T}_{P^\sigma}$.*
4. *$(z)_P^\sigma = (\sigma(z))_{P^\sigma}$ for $u \in \overline{F}$.*

Corollary 4.47 *Let $\mathcal{C}^* := \{C^* = 0\}$ be a projective curve defined over K.*

1. *$P := (a : b : c) \in \mathcal{C}^*$ if and only if $P^\sigma := (\sigma(a), \sigma(b), \sigma(c)) \in \mathcal{C}^*$. P is singular if and only if P^σ is singular. Moreover, we have $\sigma(\mathcal{O}_P) = \mathcal{O}_{P^\sigma}$ for all $P \in \mathcal{C}^*$.*
2. *The adjoint divisor $\mathcal{A}$ of the curve $\mathcal{C}^*$ is K-rational.*
3. *The intersection divisor (G) of a homogeneous polynomial $G \in K[U, V, W]$ and the curve $\mathcal{C}^*$ is K-rational.*

4.8.3 Computation of a basis of $\mathcal{L}(D)$

We show how to use the Brill-Noether algorithm to compute a basis of $\mathcal{L}(D)$ where D is a divisor of F/K. We fix a set $\mathfrak{D} \subset \mathbb{P}_{\overline{F}}$ defined by

1. for all places $\mathfrak{P} \in \mathbb{P}_F$ choose a unique place $\mathcal{Q} \in \operatorname{supp} \operatorname{Con}_{\overline{F}/\overline{F}}\mathfrak{P}$. This place is called the *distinguished place* and denoted by $\widehat{\mathfrak{P}} := \mathcal{Q}$.
2. we fix the set $\mathfrak{D} := \{\widehat{\mathfrak{P}} \mid \mathfrak{P} \in \mathbb{P}_F\}$.

Note that there is a bijective correspondence between the places $\mathfrak{P}$ of F/K and the distinguished places $\widehat{\mathfrak{P}} \in \mathfrak{D}$. We can extend this bijective correspondence to divisors by associating to every divisor $D := \sum_{\mathfrak{P} \in \mathbb{P}_F} n_{\mathfrak{P}} \mathfrak{P}$ of F/K the divisor

$$\widehat{D} := \sum_{\mathfrak{P} \in \mathbb{P}_F} n_{\mathfrak{P}} \widehat{\mathfrak{P}}$$

which is called the *distinguished divisor* of D. Let $E := \sum_{\mathcal{Q} \in \mathbb{P}_{\overline{F}}} n_{\mathcal{Q}} \mathcal{Q}$ is a K-rational divisor of $\overline{F}/\overline{K}$. We associate to E the divisor

$$\widehat{E} := \sum_{\mathcal{Q} \in \mathfrak{D}} n_{\mathcal{Q}} \mathcal{Q}$$

which we call the *distinguished divisor* of E. We know that $\widehat{E}$ is the distinguished divisor $\widehat{D}$ of some divisor D of F/K.

Let $D \in \mathcal{D}_{F/K}$ be a divisor of F/K, $\overline{D} := \operatorname{Con}_{\overline{F}/F} D \in \mathcal{D}_{\overline{F}/\overline{K}}$ be the conorm of D and $\mathcal{A} \in \mathcal{D}_{\overline{F}/\overline{K}}$ be the adjoint divisor of the curve $\mathcal{C}^*$.

The Brill-Noether algorithm uses the divisors $\overline{D} + \mathcal{A}$, (G_0) and $(G_0) - \overline{D}$ where G_0 is a homogeneous polynomial such that $(G_0) \geq \overline{D} + \mathcal{A}$ to calculate a basis of $\mathcal{L}(\overline{D})$. We know that the divisor $\overline{D}$ is K-rational and so is the divisor $\overline{D} + \mathcal{A}$ since the adjoint divisor $\mathcal{A}$ is K-rational. Therefore the intersection divisor (G_0) such that $(G_0) \geq \overline{D} + \mathcal{A}$ can be K-rational. In this case we can choose the homogeneous polynomial $G_0 \in K[U, V, W]$. The intersection divisors (G_i) with $(G_i) \geq (G_0) - \overline{D}$ for $i = 1, \ldots, \dim_{\overline{K}} \mathcal{L}(\overline{D})$ can also be K-rational. It suffices to consider only distinguished divisors and to apply the Frobenius map only when necessary.

The following is very important. Let $\mathcal{Q} \in \mathcal{D}_{\overline{F}/\overline{K}}$ be a distinguished place ($\mathcal{Q} \in \mathfrak{D}$) and $r := |\mathrm{Orb}_\sigma(\mathcal{Q})|$. By the proposition 4.44 we know that the place $\mathfrak{P} := \mathcal{Q} \cap F$ of F/K is of degree r. Further by the proposition 4.43 we know that the place $\mathfrak{P}' = \mathcal{Q} \cap F_r$ of F_r/K_r ($F_r := K_r$ where $K_r := \mathbb{F}_{q^r}$) is of degree one, $r = |\mathrm{Orb}_\sigma(\mathfrak{P}')|$ and $\mathfrak{P}'^\sigma = \mathcal{Q}^\sigma \cap F_r$. Therefore it always suffices to consider finite extensions of K. By a *distinguished place* $\widehat{\mathfrak{P}}$ we mean in the following always a place $\mathfrak{P}'$ of the minimal finite extension F_r/K_r of F/K such that $\deg \mathfrak{P}' = 1$ and $\mathfrak{P} = \mathfrak{P}' \cap F$. This can be generalized to points, their local rings and divisors of function fields, points of $\mathcal{C}^*$, powers series expansions, blow up and desingularization trees. In the next chapter we will see how to make sure that the extensions are minimal.

The algorithm on the next page is a version of the Brill-Noether algorithm adapted for this situation.

Algorithm 2 Brill-Noether over a finite field

- Input: The distinguished divisor $\widehat{D}$ of a divisor D of the function field $K(\mathcal{C}^*)$ of a plane projective curve $\mathcal{C}^*$ defined over K.
- Output: A basis of the vector space $\mathcal{L}(D)$.

1: Let $\widehat{\mathcal{A}}$ be the distinguished adjoint divisor of the curve $\mathcal{C}^*$. Set $B := \widehat{D} + \widehat{\mathcal{A}}$ and

$$B_+ = n_1 + \mathcal{Q}_1 + n_2\mathcal{Q}_2 + \ldots + n_r\mathcal{Q}_r$$

the effective part of B where $\mathcal{Q}_i \in \mathfrak{D}$ and $\mathcal{Q}_i \neq \mathcal{Q}_j$ if $i \neq j$.

2: Let $d \in \mathbb{N}$ be sufficiently big so that there exists a homogeneous polynomial $G \in S_d(K)$ which is not divisible by C^* such that $\widehat{(G)} \geq B$.

3: Fix $\{H_1, H_2, \ldots, H_l\}$ a basis of $S_d(K) \cup \{0\}$.

4: Determine for each place $\mathcal{Q}_i \in \mathrm{supp}B_+$ the matrix $M_i := M[n_i\mathcal{Q}_i]^{(d)}$ in dependence on the fixed basis.

5: For each matrix M_i construct the matrix M_i' by the following algorithm:

6: $M_i' := M_i$

7: Let $c_1, c_2, \ldots, c_m$ be the m columns of the matrix M_i.

8: **for** $j = 1$ to m **do**

9: $\quad c := c_j$

10: $\quad$ **while** $c_j \neq c^\sigma$ **do**

11: $\quad\quad c := c^\sigma$

12: $\quad\quad$ attach the column c to the matrix M_i'

13: $\quad$ **end while**

14: **end for**

15: The vector space spanned by the columns of the matrix M_i' is invariant under the action of σ. Note: if $s \in \mathbb{N}$ such that $\mathcal{Q}_i^{\sigma^s}$ then the attachment of the columns corresponds to the attachment of linear conditions imposed by the places $\mathcal{Q}_i^{\sigma^k}$ for $k = 2, 3, \ldots, s-1$.

16: Compute $M_i^{(e)}$ the column echelon form of each matrix M_i'. Then the coefficients of all the matrices $M_i^{(e)}$ are in K.

17: Compute a basis $\{b_1, b_2, \ldots, b_s\}$ of the left kernel of the matrix

$$[M_1^{(e)} \mid M_2^{(e)} \mid \cdots \mid M_r^{(e)}].$$

We have

$$b_i = (\alpha_{i,1}, \alpha_{i,2}, \ldots, \alpha_{i,l})$$

where $l = \dim_K(S_d(K) \cup \{0\}) = (d+1)(d+2)/2$. Let

$$G_i := \sum_{j=1}^{l} \alpha_{i,j} H_j, \quad k = 1, 2, \ldots, s.$$

18: If $d \geq \deg C^*$, then it is necessary to reduce the basis $\{G_1, G_2, \ldots, G_s\}$ modulo the vector space

$$W := \{A \in S_d \mid C^* \text{ divides } A\}.$$

It suffices to choose a basis $\{A_1, A_2, \ldots, A_k\}$ of W with $A_i \in S_d(K)$ $(i = 1, 2, \ldots, k)$ and to supplement this basis to a basis

$$\{A_1, A_2, \ldots, A_k, G'_1, G'_2, \ldots, G'_{s'}\}$$

of the vector space V. Now the vector space $V' \subset S_d \cup \{0\}$ spanned by the elements $\{G'_1, G'_2, \ldots, G'_{s'}\}$ is such that $V' \setminus \{0\}$ is exactly the set of all homogeneous polynomials of degree d and non-divisible by C^* such that $\widehat{(G)} \geq B_+$.

19: Choose $G_0 \in V'$ and compute the intersection divisor $\widehat{(G_0)}$.

20: Determine like in the two preceding steps a basis $\{G_1, G_2, \ldots, G_k\}$ of the vector space $V'' \subset S_d \cup \{0\}$ such that $V'' \setminus \{0\}$ is the set of all homogeneous polynomials of degree d and non-divisible by C^* such that $\widehat{(G)} \geq \widehat{(G_0)} - D$.

21: Set $\overline{G_i} := G_i + \langle C \rangle \in \overline{K}[\mathcal{C}^*]$ for $i := 0, 1, \ldots, k$ and return

$$\{\overline{G_i}/\overline{G_0} \mid i = 1, 2, \ldots, k\}$$

which is a basis of $\mathcal{L}(D)$.

Remark 4.12 *Consider the matrices M_i and let K_i be minimal extension of K containing all the coefficients of M_i. A priori all computations with the matrices M_i are carried out in the minimal extension K' of K such that $K' \supseteq K$ for all i. But since all the computations with the matrix M_i can be carried out independently from the computations with the matrices M_j for $i \neq j$ it is advantageous to carry out the computations with each matrix M_i in the field K_i. We can do it since we always work with minimal extensions.*

Chapter 5

Algorithms

5.1 Algebraic sets

Let $I \subset K[X,Y]$ be an ideal such that its algebraic set $\mathcal{V}(I)$ is finite. Consider the set

$$\mathcal{V}_X(I) := \{a \in \overline{K} \mid \text{ there exists } b \text{ such that } (a,b) \in \mathcal{V}(I)\}$$

and set

$$p(Z) := \prod_{a \in \mathcal{V}_X(I)} (Z - a).$$

By Hilbert's Nullstellensatz there exists $n \in \mathbb{N}$ such that $q := p^n \in I$. We have

$$a \in \overline{K} \text{ is a root of } q \iff \text{ there exists } b \in \overline{K} \text{ such that } (a,b) \in \mathcal{V}(I).$$

We use this in the following algorithm to compute $\mathcal{V}(I)$:

Algorithm `algebraicSet`$(\{G_1, \ldots, G_r\})$

- Input: A generator set $\{G_1, \ldots, G_r\} \subset K[X,Y]$ of an ideal I.
- Output: The algebraic set $\mathcal{V}(I)$ if it is finite. Otherwise the algorithms stops with an error message.

1: $V := \emptyset$
2: If $1 \in I$, then return $\emptyset$
3: $A := K[X] \cap I$. If $A = \emptyset$, then $\mathcal{V}(I)$ is not finite and we return an error message.
4: choose $q \in A$ and compute the roots $\alpha_1, \ldots, \alpha_l$ of q.
5: **for** $i = 1, \ldots, l$ **do**
6: Set $H_j := G_j(\alpha_i, Y)$ for $j = 1, \ldots, r$. If $H_1 = \ldots = H_l = 0$, then $\mathcal{V}(I)$ is not finite and we return an error message.
7: $q_i(Y) := \gcd\{H_1, \ldots, H_r\}$
8: $V := V \cup \{(\alpha_i, \beta) \mid \beta \text{ is a root of } q_i\}$
9: **end for**
10: return V

Remark 5.1 *Let I be the ideal considered in preceding algorithm. We compute a Gröbner basis B of the ideal I with the lexicographical order $X < Y$. We have*

1. *$1 \in B$ if and only if $1 \in I$, and*
2. *if q is the generator of the principal ideal $A := \overline{K}[X] \cap I$, then $\{q\} = B \cap K[X]$.*

The following algorithm computes the intersection of the projective plane curve $\mathcal{C}^* := \{C^* = 0\}$ and an algebraic set $\mathcal{V}(J)$ where the homogeneous ideal $J \subset K[U, V, W]$ is generated by $\{G_1, \ldots, G_r\}$.

Algorithm `projectiveAlgebraicSet`$(\{G_1, \ldots, G_r\})$

- Input: A generator set $\{G_1, \ldots, G_r\} \subset S(K)$ of a homogeneous ideal $J \subset K[U, V, W]$.
- Output: The algebraic set $\mathcal{V}(J)$ if it is finite. Otherwise the algorithms stops with an error message.

1: we compute the points of the form $P = (a : b : 1)$
2: $V := \{(a : b : 1) \mid (a, b) \in$ `algebraicSet`$(G_1(X, Y, 1), \ldots, G_r(X, Y, 1))\}$
3: we compute the points of the form $P = (a : 1 : 0)$
4: Set $g_i := G_i(X, 1, 0)$ for $i = 1, \ldots, r$. If $g_1 = \ldots = g_r = 0$, then $\mathcal{V}(J)$ is not finite and we return an error message.
5: $p := \gcd(C^*(X, 1, 0), g_1, \ldots, g_r)$
6: $V := V \cup \{(a : 1 : 0) \mid a$ is a root of $q\}$
7: If $G_1(1, 0, 0) = \ldots = G_r(1, 0, 0)$, then $V := V \cup \{(1 : 0 : 0)\}$
8: return V

We could use the preceding algorithm to compute the singular points of the projective plane curve $\mathcal{C}^* := \{C^* = 0\}$; it suffices to apply it to the polynomials C^*_U, C^*_V and C^*_W (the derivatives of C^* with respect to the variables U,V and W). Notice that it is not necessary to consider the polynomial C^*_W to determine the singular points of the form $(a : b : 1)$, to consider the polynomial C^*_V to determine singular points of the form $(a : 1 : 0)$ and to consider C_W to determine if $(1 : 0 : 0)$ is a singular point since we can reduce the question to the affine case. Therefore it is more advantageous to use the following algorithm:

Algorithm `singularPoints`(C^*)

- Input: A homogeneous polynomial $C^* \in K[U, V, W]$.
- Output: the singular points of the curve $\mathcal{C}^* := \{C^* = 0\}$.

1: $C^*_U := \partial C^*/\partial U$, $C^*_V := \partial C^*/\partial V$, $C^*_W := \partial C^*/\partial W$
2: we compute the singular points of the form $P = (a : b : 1)$
3: $V := \{(a : b : 1) \mid (a, b) \in$ `algebraicSet`$(C^*(X, Y, 1), C^*_U(X, Y, 1), C^*_V)(X, Y, 1)\}$
4: we compute the singular points of the form $P = (a : 1 : 0)$
5: If $C^*(X, 1, 0) = C^*_U(X, 1, 0) = C^*_W(X, Y, 1) = 0$, then stop with an error message since in this case there are infinitely many singular points
6: $p := \gcd(C^*(X, 1, 0), C^*_U(X, 1, 0), C^*_W(X, Y, 1))$
7: $V := V \cup \{(a : 1 : 0) \mid a$ is a root of $p\}$

8: we check if $P = (1 : 0 : 0)$ is a singular point
9: If $C^*(1,0,0) = C^*_V(1,0,0) = C^*_W(1,0,0) = 0$, then $V := V \cup \{(1 : 0 : 0)\}$
10: return V

It is also easy to compute the points of $\mathcal{C}^* := \{C^* = 0\}$ of degree r:

Algorithm `pointsOfDegree`(C^*, r)

- Input: A homogeneous polynomial $C^* \in K[U, V, W]$ and a positive integer r.
- Output: The points the curve $\mathcal{C}^* := \{C^* = 0\}$ of degree r.

1: $q := \#K$
2: $p_X := X^{q^r} - X$
3: $p_Y := Y^{q^r} - Y$
4: we compute the points of the form $P = (a : b : 1)$
5: $V := \{(a : b : 1) \mid (a, b) \in$ `algebraicSet`$(C^*(X, Y, 1), p_X, p_Y)\}$
6: we compute the points of the form $P = (a : 1 : 0)$
7: $p := \gcd(C^*(X, 1, 0), p_X)$
8: $V := V \cup \{(a : 1 : 0) \mid a$ is a root of $p\}$
9: If $C^*(1,0,0) = 0$, then $V := V \cup \{(1 : 0 : 0)\}$
10: return V

5.2 Blowing up

It is not necessary to consider the coordinate pair (x, y) when computing the infinitely close points of order one of a point $P := (a, b; x, y)$ of $\overline{F}/\overline{K}$. We represent the point P by $[(\alpha, \beta), C]$ where C is the defining polynomial of (x, y).

Algorithm `blowUp`$([(a, b), C])$

- Input: A representation of a point $P := (a, b; x, y)$ of $\overline{F}/\overline{K}$.
- Output: P with multiplicity and $\mathfrak{B}(P)$.

1: $C_0(X, Y) := C(X + a, Y + b)$
2: $m := \deg \mathrm{Init}(C_0)$
3: If $m = 1$, then return$([P, \emptyset])$
4: $q := \mathrm{Init}(C_0)(1, Z)$. Compute $V := \{\alpha \mid \alpha$ is a root of $q\}$ and set

$$\mathfrak{B}(P) := \{[(0, \beta), C_0^{[x]}] \mid \beta \in V\}.$$

5: If $\mathrm{Init}(C_0)(0, 1) = 0$, then $\mathfrak{B}(P) := \mathfrak{B}(P) \cup \{[(0, 0), C_0^{[y]}]\}$

5.3 Desingularisation tree

It is easy to construct the desingularisation tree of a point by using the procedure `blowUp`.

Algorithm desingTreeOfPoint

```
desingTreeOfPoint := proc(infClsPt)

begin
  B := blowUp(infClsPt);
  infClsPtWithMult := B[1];

  if B[2] = [] then
    # simple point #
    return(createTree(infClsPtWithMult, []));
  else
    return(createTree(infClsPtWithMult, map(B[2], desingTreeOfPoint)));
  end_if;
end_proc;
```

To compute the desingularisation trees of all singular points of a curve we have the following

Algorithm desingTrees

```
desingTrees := proc()

begin
  ListOfSingPts       := singularPoints();
  ListOfSingInfClsPts := map(ListOfSingPts, createInfClsPointFromProjPoint);
  ListOfDesingTrees   := map(ListOfSingInfClsPts, desingTreeOfPoint);
  ListOfDesingTrees   := map(ListOfDesingTrees, TreeWithExceDiv);
end_proc;
```

5.4 Valuations and $\mathfrak{P}$-adic power series expansions

Let $P := (0, 0; x, y)$ be a simple point of $\overline{F}/\overline{K}$ and C the defining polynomial of the coordinate pair (x, y). We assume that X does not divide $\mathrm{Init}(C)$. In this case we have $\nu_{\mathfrak{P}}(x) \leq \nu_{\mathfrak{P}}(y)$ and by proposition 4.1 we know that $t := x$ is a local parameter of the place $\mathfrak{P}$ of $\overline{F}/\overline{K}$ with $\mathfrak{P} \equiv P$. Let $g := G(x, y) \in \overline{F}$ where $G \in \overline{K}[X, Y]$. We want to compute the valuation $\nu_{\mathfrak{P}}(g)$.

We suppose that $g \neq 0$ and therefore it is necessary that C does not divide G. Otherwise the algorithm enters into an infinite loops.

Algorithm Valuation(P, G)

- Input: A point $P = (0, 0; x, y)$ of $\overline{F}/\overline{K}$ where C is the defining polynomial of the coordinate pair (x, y) and $\nu_{\mathfrak{P}}(x) \leq \nu_{\mathfrak{P}}(y)$ and a polynomial $G \in \overline{K}[X, Y]$ representing $g := G(x, y) \in \overline{F}$. We suppose that C does not divide G. Otherwise the algorithm would end up in an infinite loop.

- Output: $e = \nu_{\mathfrak{P}}(g)$ and a where $g(t) = at^e + \sum_{i>e} a_i t^i$ is the power series expansion of g with respect to t.

1: $e := 0$
2: $a := G(0,0)$
3: **while** $a \neq 0$ **do**
4: $\quad e := e + m_{(0,0)}(G)$
5: $\quad b := -\alpha/\beta$ where $\mathrm{Init}(C) = \alpha X + \beta Y$ {remark $b = (y/x)(\mathfrak{P})$}
6: $\quad C := C^{[x]}$, $G := G^{[x]}$
7: $\quad C := C(X, Y + b)$, $G := G(X, Y + b)$
8: $\quad a := G(0,0)$
9: **end while**
10: return(e)

Proof of the algorithm: We use induction on $\nu_{\mathfrak{P}}(G(x,y))$. We have

$$\nu_{\mathfrak{P}}(G(x,y)) = 0 \Leftrightarrow G(x,y) \in \mathcal{O}_{\mathfrak{P}}^* = \mathcal{O}_P \Leftrightarrow G(0,0) \neq 0.$$

It is clear that in this case the algorithm return $e = 0$. We assume now that $\nu_{\mathfrak{P}}(G(x,y)) = n$. We have $\nu_{\mathfrak{P}}(x) = 1$ and

$$G(x,y) = x^{m_P(G)} G^{[x]}(x, y/x).$$

Consequently $\nu_{\mathfrak{P}}(G(x,y)) = m_P(G) + \nu_{\mathfrak{P}}(G^{[x]}(x,y/x))$. Since $\nu_{\mathfrak{P}}(G^{[x]}(x,y/x)) < n$ we can use the induction hypothesis. This proves the correctness of the algorithm. □

Remark 5.2 *Note that a in the above algorithm is the first nonzero coefficient of the power series expansion of g with respect to t.*

If $P = (a, b; x, y)$ is any simple point of $\overline{F}/\overline{K}$ all we have to do before using the above algorithm is:

1: $C := C(X + a, Y + b)$, $G := G(X + a, Y + b)$
2: **if** X divides $\mathrm{Init}(C)$ **then**
3: $\quad C := C(Y, X)$, $G := G(Y, X)$
4: **end if**

Now it is not difficult to develop an algorithm to compute the coefficients of the parameterization $[\mathfrak{P}]$ of $\mathfrak{P}$. We compute only as many coefficients of the infinite series as we need.

Algorithm `Parameterization`$(\mathfrak{P}, n)$

- Input: A place $\mathfrak{P}$ of $\overline{F}/\overline{K}$ which is represented by a point $Q = (0, 0; x, y)$ of $\overline{F}/\overline{K}$ where C is the defining polynomial of (x, y) and $\nu_{\mathfrak{P}}(x) \leq \nu_{\mathfrak{P}}(y)$ and an integer n.

  Let $P := (a : b : c)$ be the unique point of $\mathcal{C}^*$ with $\mathfrak{P} \mid P_*$ and $\Gamma := (x', y')$ a coordinate pair of $\overline{F}/\overline{K}$ such that $P_* \in \mathcal{Z}(\Gamma)$. Let $G_1, G_2 \in \overline{K}[X, Y]$ be two polynomials such that $x' = G_1(x, y)$ and $y' = G_2(x, y)$.

- Output: The parameterization $[\mathfrak{P}]$ of the place $\mathfrak{P}$ (only the n first coefficients of the power series extensions are computed).

1: $x(t) := t$

2: $param := 0$
3: **while** $order < n$ **do**
4: $b := -\alpha/\beta$ where $\mathrm{Init}(C) = \alpha X + \beta Y$
5: $C := C^{[x]}$
6: $C := C(X, Y + b)$
7: $order := order + 1$
8: $param := param + b * t^{order}$
9: **end while**
10: $y(t) := param$
11: return $G_1(x(t), y(t)), G_2(x(t), y(t), 1))$ (here we assume that $c \neq 0$; otherwise 1 must be inserted corresponding to the nonzero coordinate.)

Remark 5.3 *In our real implementation the truncated power series $x(t)$ and $y(t)$ are stored so that each time only new coefficients are computed if necessary.*

5.5 Divisors

Let $P := (a, b; x, y)$ be a point of $\overline{F}/\overline{K}$. We show how to compute local divisors $(g)_P$ of functions $g \in \overline{K}[x, y] \subset \overline{F}$. Let $G \in \overline{K}[X, Y]$ a polynomial with $g = G(x, y)$. Recall that the local divisor $(g)_P$ can be expressed as

$$(g)_P = m_P(G)E_P + \sum_{Q \in \mathcal{B}(P)} (g^{(l_Q)})_Q.$$

The following algorithm is based upon this equation.

Algorithm `localDivisor`$(G, \mathcal{T}_P)$

- Input: A polynomial $G \in \overline{K}[X, Y]$ and $\mathcal{T}_P$ the desingularisation tree of a point $P = (a, b; x, y)$.
- Output: The local divisor $(g)_P$ where $g = G(x, y)$.

1: **if** $G(a, b) \neq 0$ **then**
2: {g is invertible in the local ring $\mathcal{O}_P$ and therefore also in all $\mathcal{O}_\mathfrak{P}$ with $\mathfrak{P} \mid P$}
3: **return**(0)
4: **end if**
5: **if** P is a simple point **then**
6: $n :=$ `Valuation`(P, G)
7: return$(n \cdot \mathfrak{P})$ where $E_P = \mathfrak{P}$
8: **else**
9: **return**

$$m_P(G)E_P + \sum_{Q \in \mathfrak{B}(P)} \texttt{localDivisor}(G_Q, \mathcal{T}_Q)$$

where $G_Q := G(X + a, Y + b)^{(l_Q)}$ (E_P is the exceptional divisor of P and l_Q is the exceptional coordinate of the point $Q \in \mathfrak{B}(P)$)
10: **end if**

It is clear that we must first compute the exceptional divisors of points of the desingularisation tree before applying the `localDivisor` algorithm. To do this it suffices to use the `TreeWithExceDiv` algorithm which is based upon the equation

$$E_P = \sum_{Q \in \mathfrak{B}P} (l_Q)_Q.$$

Algorithm `TreeWithExceDiv`$(\mathcal{T}_P)$

- Input: A tree $\mathcal{T}_P$
- Output: The tree $\mathcal{T}_P$ with exceptional divisor attached to each knot

1: **if** P is a simple point **then**
2: create the place $\mathfrak{P} \equiv P$ and attach $E_P = \mathfrak{P}$ to the knot of P
3: **else**
4: $\mathcal{T}_Q :=$ `TreeWithExceDiv`$(\mathcal{T}_Q)$ for all $Q \in \mathfrak{B}(P)$
{we have computed the exceptional divisors of all infinitely close points of P; we can use the above equation the exceptional divisor E_P of P}
5: $E_P := \sum_{Q \in \mathfrak{B}(P)}$ `LocalDivisor`$(L_Q, \mathcal{T}_Q)$
{where $L_Q := X$ if x is the exceptional coordinate of the point Q, otherwise $L_Q := Y$}
6: attach the divisor E_P to the knot of P.
7: **end if**

It is simple to compute the adjoint divisor of a point.

Algorithm `adjointDivisorOfPoint`$(\mathcal{T}_P)$

- Input: The desingularisation tree of a point P
- Output: The adjoint divisor $\mathcal{A}_P$ of the point P.

1: **return**

$$(m_P - 1)E_P + \sum_{Q \in \mathfrak{B}(P)} \texttt{adjointDivisorOfPoint}(\mathcal{T}_Q).$$

It is also simple to compute the intersection divisor (G) of a homogeneous polynomial $G \in K[U, V, W]$.

Algorithm `intersectionDivisor`(G)

- Input: A homogeneous polynomial $G \in K[U, V, W]$.
- Output: The intersection divisor (G) of G.

1: **for all** points $P \in$ `projectiveAlgebraicSet`(C^*, G) **do**
2: **if** P_* is a simple point **then**
3: create a place $\mathfrak{P} \equiv P_*$ if this has not already been done
4: $n :=$ `Valuation`(P_*, G^P)
5: $(G) := (G) + n\mathfrak{P}$
6: **else**
7: $(G) := (G) +$ `localDivisor`$(G^P, \mathcal{T}_P)$
8: **end if**
9: **end for**

5.6 Constant field extensions

The Brill-Noether algorithm needs in theory an algebraically closed field or at least a sufficiently high extension of the ground field. We could use such an extension but this would not be very practical. Sometimes we want to work with a specific constant field extension. For example we are interested in the number of places that are rational over some constant field $\mathbb{F}_q$. Also for complexity reasons it is better to use the minimal extension which suffices to do the computations. This also permits us to choose a distinguished element.

Let $g(Z) = \prod_{i=1}^{k} g_i(Z) \in \mathbb{F}_q[Z]$ where g_i are irreducible factors for $i = 1, \ldots, k$. Assume that there is an irreducible factor g_i with $\deg g_i(Z) > 1$. The extension $\mathbb{F}_{q^{\deg g_i}}$ of $\mathbb{F}_q$ is the smallest extension in which we can express the roots of $g_i(Z)$. There are $\deg g_i$ roots of $g_i(Z)$ and they are mutually conjugated by $\alpha \mapsto \alpha^q$. It suffices to keep only one root of $g_i \in \mathbb{F}_q[Z]$.

```
>> groundField;
                                    F_4

>> groundField::minpoly;
                           2
                  poly(X1  + X1 + 1, [X1], IntMod(2))

>> q := poly(Z^3+Z+1,[Z],groundField);

                              3
                     poly(Z  + Z + 1, [Z], F_4)

> irreducible(q);

                                   TRUE
```

The ground field $\mathbb{F}_4$ (`F_4`) is represented as $\mathbb{F}_2[X_1]/\langle X_1^2 + X_1 + 1\rangle$. The polynomial $q(Z) := Z^3 + Z + 1$ is irreducible over $\mathbb{F}_4[Z]$. We can construct an extension in which we can represent a root of $q(Z)$:

```
>> exts := distRoots(q);

              -- table(                                      --
              |                                 2     4     |
              |    _embed = [F_64, X1, X2 + X2  + X2 ],     |
              |                         2                   |
              |    _distRoot = X2 + X2  + 1,                |
              |    _extDeg = 3                              |
              -- )

>> ext := exts[1]:

>> embeddedQ := embedPoly(q, ext[_embed]);
```

```
                                3
                       poly(Z  + Z + 1, [Z], F_64)

>> ext[_distRoot];
                                     2
                              X2 + X2  + 1

>> domtype(ext[_distRoot]);

                                  F_64

>> evalp(embeddedQ, Z=ext[_distRoot]);

                                   0
```

The entry `ext[_embed]` determines how `F_4` is embedded into `F_64`. We can embed an element into the new extension with `embedElem` and a polynomial into the polynomial ring over the new extension with `embedPoly`. We can concatenate two embeddings with `succEmbed`.

In the following we present the algorithms as if we calculated in the algebraically closed field $\overline{K}$ for simplicity. Actually we always work in the smallest extension and always choose a distinguished element.

5.7 Examples

Let us consider the projective plane curve $\mathcal{C}^*$ determined by the polynomial

```
>> projectiveCurve;

     8      5    3    4  5    4  2  3    9    6  3    3  6    9
poly(X  Y + X  Y Z  + X  Y  + X  Y  Z  + Y  + Y  Z  + Y  Z  + Z , [X,Y,Z], F_2)
```

over finite field $\mathbb{F}_2$

```
>> groundField;
                                  F_2
>> groundField::size;
                                   2
```

Let us determine the singular points of $\mathcal{C}^*$.

```
>> singPts := singularPoints():
>> nops(singPts);
                                   3
>> printProjPoint(singPts[1]);
                                [0, 1, 1]
>> printProjPoint(singPts[2]);
                                          2
                              [0, X2 + 1, 1]
```

```
>> printProjPoint(singPts[3]);
                                        2
                          [X2 + 1, 1, 0]
```

The point `singPts[1]` is rational over `F_2` and the points `singPts[2]` and `singPts[3]` are rational over `F_4` ($\mathbb{F}_{2^2}$). The index attached to a projective point is the degree of the minimal extension of the ground field `F_2` needed to represent the point. The field `F_4` was created to represent the points `singPts[2]` and `singPts[4]`. This index is also the length of the orbit under the Frobenius map. We always create only one point of each orbit. We see that the curve $\mathcal{C}^*$ has five singular points

$$P_1 := (0:1:1), \quad P_2 := (0:\beta:1), \quad P_3 := (\beta:1:0),$$
$$P_4 := (0:\beta^2:1), \quad P_5 := (\beta^2:1:0)$$

where β is a primitive element of $\mathbb{F}_{2^2}$. The points P_2 and P_4 are conjugated over $\mathbb{F}_2$ and so are P_3 and P_4.

The point $P_1 \in \mathcal{C}^*$ (`singPts[1]`) is represented as

```
>> pt := singPts[1];

table(
  _embed = [F_2],
  _projCoords = [0, 1, 1],
  _deg = 1,
  _defCurve = poly(X^8*Y + X^5*Y*Z^3 + X^4*Y^5 + X^4*Y^2*Z^3 + Y^9 + Y^6*Z\
^3 + Y^3*Z^6 + Z^9, [X, Y, Z], F_2)
)
```

Let us blow up this point. To do that we must first create the point P_{1*} of $\overline{K}(\mathcal{C}^*)$.

```
>> icp0 := createInfClsPointFromProjPoint(pt);

table(
  _exceDiv = 0,
  _affCoords = [0, 1],
  _chart = 2,
  _prevEmbed = [F_2],
  _embed = [F_2],
  _exceCoord = None,
  _G1 = poly(X, [X, Y], F_2),
  _deg = 1,
  _G2 = poly(Y, [X, Y], F_2),
  _mult = 0,
  _defCurve = poly(X^8*Y + X^5*Y + X^4*Y^5 + X^4*Y^2 + Y^9 + Y^6 + Y^3 + 1\
, [X, Y], F_2)
)
```

Note that the multiplicity `icp0[_mult]` has not been computed. The procedure `blowUp` gives us the point with the multiplicity and a list of the infinitely close points.

```
>> [icp0, infClsPts_icp0] := blowUp(icp0):
>> icp0[_mult];
                                    3
>> nops(infClsPts_icp0);
                                    1

>> icp1 := infClsPts_icp0[1];
table(
  _exceDiv = 0,
  _affCoords = [0, 0],
  _chart = 2,
  _prevEmbed = [F_2],
  _embed = [F_2],
  _exceCoord = X,
  _G1 = poly(X, [X, Y], F_2),
  _deg = 1,
  _G2 = poly(X Y + 1, [X, Y], F_2),
  _mult = 0,
  _defCurve = poly(X^6*Y^9 + X^6*Y^5 + X^6*Y + X^5*Y^8 + X^5*Y^4 + X^5 + X\
^3*Y^6 + X^3*Y^2 + X^3*Y + X^2*Y + X^2 + X*Y^4 + Y^3, [X, Y], F_2)
)
```

We see that the multiplicity is of `icp0` is 3 and that there is only one infinitely close point `icp1` above `icp0`. Note that the entries `icp1[_G1]` and `icp1[_G2]` keep track of the coordinate transformations done when blowing up. Since `icp1[_affCoords]=[0,0]` the multiplicity of `icp1` is the degree of the initial form of `icp1[_defCurve]` (`icp1` is already in the origin).

```
>> initForm(icp1[_defCurve]);
                                  2
                          poly(X , [X, Y], F_2)
```

We know now that the multiplicity of `icp1` is 2 and that there is only one infinitely close. Its exceptional coordinate is Y. Let us check it.

```
>> [icp1, infClsPts_icp1] := blowUp(icp1):
>> icp1[_mult];
                                    2
>> icp2 := infClsPts_icp1[1];
table(
  _exceDiv = 0,
  _affCoords = [0, 0],
  _chart = 2,
  _prevEmbed = [F_2],
  _embed = [F_2],
  _exceCoord = Y,
  _G1 = poly(X Y, [X, Y], F_2),
  _deg = 1,
```

```
                2
  _G2 = poly(X Y  + 1, [X, Y], F_2),
  _mult = 0,
  _defCurve = poly(X^6*Y^13 + X^6*Y^9 + X^6*Y^5 + X^5*Y^11 + X^5*Y^7 + X^5\
*Y^3 + X^3*Y^7 + X^3*Y^3 + X^3*Y^2 + X^2*Y + X^2 + X*Y^3 + Y, [X, Y], F_2)
)
```

Since `icp2[_affCoords] = [0, 0]` and

```
>> initForm(icp2[_defCurve]);
                            poly(Y, [X, Y], F_2)
```

the point `icp2` is a simple point. Let us determine the exceptional divisors and the adjoint divisor.

```
>> desingTree_icp0 := desingTreeAtPointLocal(icp0):
>> desingTree_icp0 := TreeWithExceDiv(%):
>> drawTree(%);
                                  "UU(L1).."
```

We see that a symbol `L1` has been created. It represents the place corresponding to the simple point `icp2`. The exceptional divisors of `icp0` and `icp1` are respectively

```
>> desingTree_icp0[_knot][_exceDiv];
                                       3 L1
>> desingTree_icp0[_branches][1][_knot][_exceDiv];
                                       2 L1
```

The local adjoint divisor of `icp0` is

```
>> AdjDivOfTree(desingTreeOfIcp0);
                                       8 L1
```

We compute now all the desingularisation trees with `desing`. The adjoint divisor of the curve $\mathcal{C}^*$ is

```
>> adjointDivisor;
                          8 L1 + 8 L2 + 3 L3 + 3 L4
>> printDivisor(adjointDivisor);
                                    2       2       6
                        8 L1 + 8 L2  + 3 L4  + 3 L3
>> degOfDivisor(adjointDivisor);
                                      48
```

The genus of the function field $\overline{K}(\mathcal{C}^*)$ is $((n-1)(n-2) - \deg \mathcal{A})/2 = 4$ where $n = 9$ is the degree of the curve $\mathcal{C}^*$.

```
>> genus;
                                       4
```

We get a canonical divisor of $\overline{K}(\mathcal{C}^*)$ by

```
>> K := canonicalDivisor();
                              L1 + L2 + 3 S1
>> printDivisor(K);
                                     2
                              L1 + L2  + 3 S1
>> degOfDivisor(K);
                                     6
```

We know that the degree of a canonical divisor is $2g - 2 = 4$ where $g = 4$ is the genus of $\overline{K}(\mathcal{C}^*)$. The dimension of the vector space $\mathcal{L}(K)$ associated to a canonical divisor K is always g.

```
basis := brillnoether(K):
>> G0 := basis[1];
                           6  3    9
                    poly(Y  Z  + Z , [X, Y, Z], F_2)
>> [G1,G2,G3,G4] := basis[2]:

  9    6  3
[Z  + Y  Z ,

    8      6  2    3    5    6    2    2  2  5    2  5  2
 X Z  + X Y  Z  + X  Y Z  + X  Y Z  + X  Y  Z  + X  Y  Z ,

  8      2  7    2  7    6  2      2  3  4    3  2  4
 Y  Z + X  Z  + Y  Z  + X  Y  Z + X  Y  Z  + X  Y  Z ,

  9      8    3  6    5  4    6  3    3  6    3  6      2  6
 Y  + X Y  + X  Y  + X  Y  + X  Y  + X  Z  + Y  Z  + X Y  Z

    5    3    3  3  3
 + X  Y Z  + X  Y  Z ]

>> interDivG0 := intersectionDivisor(G0):
>> interDivG1 := intersectionDivisor(G1):
>> interDivG2 := intersectionDivisor(G2):
>> interDivG3 := intersectionDivisor(G3):
>> interDivG4 := intersectionDivisor(G4):
>> -K;
                             - L1 - L2 - 3 S1
>> interDivG1-interDivG0;
                                     0
>> interDivG2-interDivG0;
                            2 L4 - L1 - L2 - S1
>> interDivG3-interDivG0;
                       L4 - L1 - L2 - 2 S1 + S2 + S6
>> interDivG4-interDivG0;
                            L3 - L1 - L2 - 3 S1
```

```
>> degOfDivisor(%);
                                    0
```

We see that $\{G_1/G_0, \ldots, G_4/G_0\}$ is a basis of $\mathcal{L}(K)$.

Let us consider the curve over F_{2^2}.

```
>> groundField;
                                  F_4
>> projectiveCurve;
     8      5    3    4  5    4  2  3    9    6  3    3  6    9
poly(X  Y + X  Y Z  + X  Y  + X  Y  Z  + Y  + Y  Z  + Y  Z  + Z ,
  [X, Y, Z] , F_4)
```

The adjoint divisor is

```
>> printDivisor(adjointDivisor);
                                              3              3
            8 L1 + 8 L2 + 8 L3 + 3 L5 + 3 L4  + 3 L7 + 3 L6
```

With respect to the standard coordinate triple we have the following divisors:

```
>> printDivisor(intersectionDivisor(poly(X,[X,Y,Z],groundField)));
                           3 L1 + 3 L2 + 3 L3
>> printDivisor(intersectionDivisor(poly(Y,[X,Y,Z],groundField)));
                                 9 S1
>> printDivisor(intersectionDivisor(poly(Z,[X,Y,Z],groundField)));
                               3          3
                        L5 + L4  + L7 + L6  + S1
```

`S1` corresponds to the simple point

```
>> printProjPoint(ListOfSimplePts[1]);
                                [1, 0, 0]
```

of the curve $\mathcal{C}^*$. Consider the divisor `9*S1`. Regarding the intersection divisors (X), (Y) and (Z) above we see that X^3YZ^3 is an interpolating form for $\mathcal{A} + 9S_1$.

```
>> G0 := poly(X^3*Y*Z^3,[X,Y,Z],groundField):
>> interDivG0 := intersectionDivisor(G0);
         9 L1 + 9 L2 + 9 L3 + 3 L4 + 3 L5 + 3 L6 + 3 L7 + 12 S1
>> interDivG0 - (adjointDivisor + 9*S1);
                           L1 + L2 + L3 + 3 S1
>> denoms := interpolatingForms(interDivG0 - 9*S1, 7):
>> nops(denoms);
                                    6
>> map(denoms, expr);
  3  4   3    3   4  3   2  5    4    2    2  3  2    3  2  2
[X  Z , X  Y Z , X  Z , X  Z  + X  Y Z  + X  Y  Z  + X  Y  Z ,

    7    6      2    4    2  4      4  2
```

```
   Z  + Y  Z + X  Y Z  + X  Y  Z + X  Y  Z,

    7      6    6        6      6    3  4    5  2
   Y  + X Y  + X  Y + X Z  + Y Z  + X  Y  + X  Y ]
```

We see that the dimension of dim $\mathcal{L}(9S_1) = 6$, according to the Riemann-Roch theorem dim $\mathcal{L}(mS_1) = m - g + 1$ for all $m > 2g - 2 = 6$. The function field $\overline{K}(\mathcal{C}^*)$ has

```
>> plcs := placesOfDegreeOne();
       [S7, S8, S9, L1, L2, L3, L5, L7, S1, S2, S10, S3, S4, S5, S6]
>> nops(plcs);
                                    15
```

places of degree one. Let `P` be the list of all places of degree one except `S1`. We can construct the geometric Goppa-Code $C_{\mathcal{L}}(\mathcal{P}, 6S_1)$

```
>> P := [op({op(plcs)} minus {S1})];
         [S7, S8, S9, L1, L2, L3, L5, L7, S2, S3, S10, S4, S5, S6]
>> goppaCode([G0,denoms], P);
             +-                                                  -+
             |     1,   1, X1 + 1,   X1,   X1 + 1,   X1          |
             |    X1,   1,   X1,     X1,   X1 + 1, X1 + 1        |
             |     1,   1,    1,      0,      1,      1          |
             |     1,   1,    1,      1,      1,      1          |
             |    X1,   1,    1,   X1 + 1, X1 + 1,    1          |
             |  X1 + 1, 1,    1,     X1,     X1,      1          |
             |     1,   1, X1 + 1,    0,     X1,     X1          |
             |     1,   1,   X1,      0,   X1 + 1, X1 + 1        |
             |    X1,   1, X1 + 1,    1,      1,     X1          |
             |  X1 + 1, 1,    1,      0,   X1 + 1,    1          |
             |  X1 + 1, 1, X1 + 1, X1 + 1,   X1,     X1          |
             |     1,   1,   X1,   X1 + 1,   X1,   X1 + 1        |
             |  X1 + 1, 1,   X1,      1,      1,   X1 + 1        |
             |    X1,   1,    1,      0,     X1,      1          |
             +-                                                  -+

>> groundField::minpoly;
                          2
                 poly(X1  + X1 + 1, [X1], IntMod(2))
```

Chapter 6

Absolute factorization of bivariate polynomials

6.1 Introduction

We describe the algorithm for factoring bivariate polynomials over an algebraically closed field proposed by D. Duval in [Duv91]. Let K be a perfect field and $\overline{K}$ an algebraic closure of K. Let $C \in \overline{K}[X, Y]$ be a reducible square-free polynomial. Consider its factorization

$$C = \prod_{i=1}^{r} C^{(i)}, \tag{6.1}$$

where the polynomials $C^{(i)} \in \overline{K}[X, Y]$ are irreducible for $i = 1, 2, \ldots, r$. The irreducible components of the affine plane reduced curve [1]

$$\mathcal{C} := \left\{ P \in \mathbb{A}^2 \mid C(P) = 0 \right\}$$

are the irreducible curves

$$\mathcal{C}^{(i)} = \{ P \in \mathbb{A}^2 \mid C^{(i)}(P) = 0 \}$$

defined by the irreducible factors of the polynomial C:

$$\mathcal{C} = \mathcal{C}^{(1)} \cup \ldots \cup \mathcal{C}^{(r)}.$$

The geometric question of determining the irreducible components of the curve $\mathcal{C}$ is equivalent to the algebraic question of factoring the bivariate polynomial C over the algebraically closed field $\overline{K}$.

6.2 The function ring of a reduced curve

The algorithm is based on some geometric invariants of the curve $\mathcal{C}$. For the basic concepts of algebraic geometry see Chapter 3 "Regular and rational functions" in [Kun85]. Each irreducible factor $C^{(i)}$ of C defines a plane irreducible curve

$$\mathcal{C}^{(i)} := \{ P \in \mathbb{A}^2 \mid C^{(i)}(P) = 0 \}.$$

[1] By a curve we mean an equidimensional algebraic set whose irreducible components have dimension 1 (i.e. are irreducible curves).

with the *coordinate ring*

$$\overline{K}[\mathcal{C}^{(i)}] := \overline{K}[X,Y]/\left\langle C^{(i)}\right\rangle$$

and the *function field*

$$\overline{K}(\mathcal{C}^{(i)}) := \left\{ f/g \mid f,g \in \overline{K}[\mathcal{C}^{(i)}], g \neq 0 \right\}.$$

The square-free polynomial C defines an affine plane reduced curve

$$\mathcal{C} := \left\{ P \in \mathbb{A}^2 \mid C(P) = 0 \right\}$$

with the coordinate ring

$$\overline{K}[\mathcal{C}] := \overline{K}[X,Y]/\left\langle C\right\rangle.$$

As a rational function r on $\mathcal{C}$ is defined on a dense open subset U of $\mathcal{C}$ (domain of definition) it must have the form $r = f/g$ with $f \in \overline{K}[\mathcal{C}]$ and $g \in \overline{K}[\mathcal{C}]^*$ where $\overline{K}[\mathcal{C}]^*$ is the multiplicatively closed subset of non-zerodivisors of $\overline{K}[\mathcal{C}]$. The denominator g must not be a zerodivisor since otherwise the domain of definition would not be dense in $\mathcal{C}$. The *function ring* of $\mathcal{C}$ will be denoted by $\overline{K}(\mathcal{C})$. It is the total quotient ring of $\overline{K}[\mathcal{C}]$ [2] (see also Chapter 2 "Localization" in [Eis95])

$$\overline{K}(\mathcal{C}) := \overline{K}[\mathcal{C}]_{\overline{K}[\mathcal{C}]^*} = \left\{ f/g \mid f \in \overline{K}[\mathcal{C}] \text{ and } g \in \overline{K}[\mathcal{C}]^* \right\}.$$

It is the "biggest" localization such that the natural map ι

$$\iota : \left\{ \begin{array}{ccc} \overline{K}[\mathcal{C}] & \longrightarrow & \overline{K}(\mathcal{C}) \\ g & \mapsto & g/1 \end{array} \right.$$

is an injection. Let I be an ideal of $\overline{K}(\mathcal{C})$. The correspondence $I \mapsto \iota^{-1}(I)$ is a bijection between the prime ideals of $\overline{K}(\mathcal{C})$ and the prime ideals of $\overline{K}[\mathcal{C}]$ not meeting $\overline{K}[\mathcal{C}]^*$ (Proposition 2.2 [Eis95]). The latter are exactly the prime ideals $\overline{C}^{(i)} := C^{(i)} + \langle C\rangle \in \overline{K}[\mathcal{C}]$.

The function ring $\overline{K}[\mathcal{C}]$ has exactly r prime ideals which are

$$\mathfrak{C}^{(i)} := \iota(\overline{C}^{(i)}) = (\overline{C}^{(i)}/1)\overline{K}(\mathcal{C}).$$

Every ideal J of $\overline{K}[\mathcal{C}]$ with $J \supsetneq \overline{C}^{(i)}$ meets $\overline{K}[\mathcal{C}]^*$ so that $1 \in \iota(J)$ and consequently $\iota(J) = \overline{K}(\mathcal{C})$.

The ideals $\mathfrak{C}^{(i)}$ are therefore maximal so that $\mathfrak{C}^{(i)} + \mathfrak{C}^{(j)} = \overline{K}(\mathcal{C})$ for $i \neq j$ and their intersection $\bigcap_{i=1}^{r} \mathfrak{C}^{(i)}$ is the zero ideal as the intersection $\bigcap_{i=1}^{r} \overline{C}^{(i)} = \overline{C}^{(1)}\overline{C}^{(2)} \ldots \overline{C}^{(r)} = \overline{0}$ is the zero ideal in $\overline{K}[\mathcal{C}]$ and localization preserves finite intersections (Corollary 2.6 in [Eis95]). We are now in the situation of the Chinese Remainder Theorem which establishes the isomorphism

$$\overline{K}(\mathcal{C}) \cong \overline{K}(\mathcal{C})/\mathfrak{C}^{(1)} \times \ldots \times \overline{K}(\mathcal{C})/\mathfrak{C}^{(r)}.$$

We can also obtain this isomorphism directly (see page 85 in [Kun85]) as the coordinate ring $\overline{K}[\mathcal{C}] \neq 0$ is a reduced ring with finitely many minimal prime ideals $\overline{C}^{(1)}, \overline{C}^{(2)}, \ldots, \overline{C}^{(r)}$ which correspond to the irreducible components of $\mathcal{C}$.

[2] For the irreducibles curves $\mathcal{C}^{(i)}$ we obtain $\overline{K}(\mathcal{C}^{(i)}) = \left\{ f/g \mid f,g \in \overline{K}[\mathcal{C}^{(i)}], g \neq 0 \right\} = \overline{K}[\mathcal{C}^{(i)}]_{\overline{K}[\mathcal{C}^{(i)}]^*}$

Since the function fields $\overline{K}(\mathcal{C}^{(i)})$ are $\overline{K}$-isomorphic to the fields $\overline{K}(\mathcal{C})/\mathfrak{C}^{(i)}$ for $i = 1, \ldots, r$ we have the $\overline{K}$-algebra isomorphism

$$\varphi : \begin{cases} \overline{K}(\mathcal{C}) & \longrightarrow & \overline{K}(\mathcal{C}^{(i)}) \times \ldots \times \overline{K}(\mathcal{C}^{(i)}) \\ \frac{G(x,y)}{H(x,y)} & \mapsto & \left(\frac{G(x^{(1)},y^{(1)})}{H(x^{(1)},y^{(1)})}, \ldots, \frac{G(x^{(r)},y^{(r)})}{H(x^{(r)},y^{(r)})}\right) \end{cases} \tag{6.2}$$

where $G, H \in \overline{K}[X, Y]$ with $\gcd(H, C) = 1$ and where $x, x^{(1)}, \ldots, x^{(r)}$ and $y, y^{(1)}, \ldots, y^{(r)}$ are the images of X and Y in $\overline{K}[\mathcal{C}], \overline{K}[\mathcal{C}^{(1)}]), \ldots, \overline{K}[\mathcal{C}^{(r)}])$. We can also obtain the isomorphism φ directly using Proposition 4.23 in [Kun85].

6.3 Places and divisors of the function ring

Since the function ring of a reduced curve is isomorphic to the direct product of function fields of irreducibles curves we can generalize the notions of places and divisors of an algebraic function field in one variable to the function ring of a curve. More details on these notions can be found in chapter 1. Nevertheless let us repeat briefly some basic results.

A *valuation ring* of an algebraic function field in one variable F with ground field K is a ring $\mathcal{O}$ such that

1. $K \subsetneq \mathcal{O} \subsetneq F$,
2. if $x \in F \setminus \mathcal{O}$ then $x^{-1} \in \mathcal{O}$.

Every valuation ring is a local ring. A *place* of F is the unique maximal ideal of a valuation ring. The set of places is denoted by $\mathbb{P}_{F/K}$. For every $\mathfrak{P} \in \mathbb{P}_{F/K}$ there is a unique valuation ring which has $\mathfrak{P}$ as its maximal ideal. We will denote this valuation ring by $\mathcal{O}_{\mathfrak{P}}$. Every place $\mathfrak{P}$ has a remarkable element t such that $\mathfrak{P} = t\mathcal{O}_{\mathfrak{P}}$. This element is called a *local parameter*. Every element $v \in F$ can be written in the form

$$v = ut^n$$

where $n \in \mathbb{Z}$ and $u \in \mathcal{O}_{\mathfrak{P}}^* := \mathcal{O}_{\mathfrak{P}} \setminus \mathfrak{P}$. We can associate to every place $\mathfrak{P}$ the function $\nu_{\mathfrak{P}} : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ defined by

$$\nu_{\mathfrak{P}}(v) := \begin{cases} n & v \neq 0 \text{ and } v = t^n u \text{ where } u \in \mathcal{O}_{\mathfrak{P}}^*, \\ \infty & v = 0 \end{cases} . \tag{6.3}$$

The function $\nu_{\mathfrak{P}}$ is well defined and does not depend on the choice of the local parameter t. It is a *discrete valuation* of F because it is surjective and satisfies the following three conditions:

1. $\nu_{\mathfrak{P}}(u) = \infty \Leftrightarrow u = 0$,
2. $\nu_{\mathfrak{P}}(uv) = \nu_{\mathfrak{P}}(u) + \nu_{\mathfrak{P}}(v)$ for all $u, v \in F$,
3. $\nu_{\mathfrak{P}}(u + v) \geq \min\{\nu_{\mathfrak{P}}(u), \nu_{\mathfrak{P}}(v)\}$ for all $u, v \in F$ *(triangle inequality).*

We will consider the function fields of each irreducible component $\mathcal{C}^{(i)}$ of $\mathcal{C}$.

Definition 6.1 (Place) *A place of $\overline{K}(\mathcal{C})$ is a place of the function field $\overline{K}(\mathcal{C}^{(i)})$ of one irreducible component $\mathcal{C}^{(i)}$ of $\mathcal{C}$. The set of places of $\overline{K}(\mathcal{C})$ will be denoted by $\mathbb{P}$.*

Let $\mathfrak{P}$ be a place of $\overline{K}(\mathcal{C})$. Let $i_{\mathfrak{P}} \in \{1, \ldots, r\}$ be the unique index such that $\mathfrak{P}$ is a place of $\overline{K}(\mathcal{C}^{(i)})$ [3] and let us consider the corresponding discrete valuation:

$$\nu_{\mathfrak{P}}^{(i_{\mathfrak{P}})} : \overline{K}(\mathcal{C}^{(i)}) \longrightarrow \mathbb{Z} \cup \{\infty\}.$$

We can define a map

$$\nu_{\mathfrak{P}} : \begin{cases} \overline{K}(\mathcal{C}) & \longrightarrow & \mathbb{Z} \cup \{\infty\} \\ u & \mapsto & \nu_{\mathfrak{P}}^{(i_{\mathfrak{P}})}(u^{(i_{\mathfrak{P}})}) \end{cases} \tag{6.4}$$

by projecting $\overline{K}(\mathcal{C})$ onto $\overline{K}(\mathcal{C}^{(i)})$. This map is surjective and satisfies the following three properties:

1. $\nu_{\mathfrak{P}}(u) = \infty \Leftrightarrow u^{(i_{\mathfrak{P}})} = 0$,
2. $\nu_{\mathfrak{P}}(uv) = \nu_{\mathfrak{P}}(u) + \nu_{\mathfrak{P}}(v)$ for all $u, v \in \overline{K}(\mathcal{C})$,
3. $\nu_{\mathfrak{P}}(u+v) \geq \min\{\nu_{\mathfrak{P}}(u), \nu_{\mathfrak{P}}(v)\}$ for all $u, v \in \overline{K}(\mathcal{C})$.

The map $\nu_{\mathfrak{P}}$ does not satisfy all the properties of a discrete valuation because there is $u \in \overline{K}(\mathcal{C}) \setminus \{0\}$ with $u^{(i_{\mathfrak{P}})} = 0$ and therefore $\nu_{\mathfrak{P}}(u) = \infty$ even though $u \neq 0$. Nevertheless we will use the following definition:

Definition 6.2 (Discrete valuation) *A discrete valuation of $\overline{K}[C]$ is a surjective map*

$$\nu : \overline{K}(\mathcal{C}) \longrightarrow \mathbb{Z} \cup \{\infty\}$$

satisfying the following properties:

1. *there is an index $i \in \{1, \ldots, r\}$ such that $\nu(u) = \infty$ if and only if $u^{(i)} = 0$,*
2. *$\nu_{\mathfrak{P}}(uv) = \nu_{\mathfrak{P}}(u) + \nu_{\mathfrak{P}}(v)$ for all $u, v \in \overline{K}(\mathcal{C})$,*
3. *$\nu_{\mathfrak{P}}(u+v) \geq \min\{\nu_{\mathfrak{P}}(u), \nu_{\mathfrak{P}}(v)\}$ for all $u, v \in \overline{K}(\mathcal{C})$.*

Let ν be a discrete valuation of $\overline{K}(\mathcal{C})$. The index i for which $\nu(u) = \infty$ if and only if $u^{(i)} = 0$ is unique. Since ν is surjective there is $u \in \overline{K}(\mathcal{C})$ such that $\nu(u) \neq \infty$ and therefore $u^{(i)} \neq 0$. Let $j \neq i$, $1 \leq j \leq r$. We can always choose $u \in \overline{K}(\mathcal{C})$ such that $u^{(j)} = 0$ and $\nu(u) \neq \infty$. We know that a place of a function field is uniquely determined by a discrete valuation. The following proposition is therefore evident.

Proposition 6.1 *For every place $\mathfrak{P} \in \mathbb{P}$ the map $\nu_{\mathfrak{P}}$ is discrete valuation of $\overline{K}(\mathcal{C})$. Conversely if $\nu : \overline{K}(\mathcal{C}) \to \mathbb{Z} \cup \{\infty\}$ is a discrete valuation of $\overline{K}(\mathcal{C})$ then there is a unique place $\mathfrak{P} \in \mathbb{P}$ such that $\nu = \nu_{\mathfrak{P}}$.*

We can now generalize the notion of a divisor to the function ring of a reduced curve.

Definition 6.3 (Divisor) *A* divisor *of $\overline{K}(\mathcal{C})$ is a formal sum*

$$D := \sum_{\mathfrak{P} \in \mathbb{P}} n_{\mathfrak{P}} \mathfrak{P}$$

where $n_{\mathfrak{P}} \in \mathbb{Z} \cup \{\infty\}$. We denote the set of all divisor of $\overline{K}(\mathcal{C})$ by $\mathcal{D}_{\mathcal{C}}$.

[3] Every place $\mathfrak{P}$ of $\overline{K}(\mathcal{C})$ corresponds to a point of the function ring $\overline{K}(\mathcal{C})$ (see Definition 6.7). This determines the index $i_{\mathfrak{P}}$ in a unique way. The uniqueness here should be understood via this representation.

Contrary to a divisor of a function field the support of a divisor $D := \sum_{\mathfrak{P}\in\mathbb{P}} n_{\mathfrak{P}}$ of the function ring $\overline{K}(\mathcal{C})$ is not necessarily finite. This can also occur for the *degree* of D which is defined by

$$\deg D := \sum_{\mathfrak{P}\in\mathbb{P}} n_{\mathfrak{P}}$$

and which takes values from $\mathbb{Z}\cup\{\infty\}$. We allow this since the function ring $\overline{K}(\mathcal{C})$ contains zerodivisors.

The set of divisors $\mathcal{D}_{\mathcal{C}}$ is partially ordered by the relation

$$D \geq D' \Longleftrightarrow n_{\mathfrak{P}} \geq n'_{\mathfrak{P}} \text{ for all } \mathfrak{P} \in \mathbb{P}$$

where $D := \sum_{\mathfrak{P}\in\mathbb{P}} n_{\mathfrak{P}}$ and $D' := \sum_{\mathfrak{P}\in\mathbb{P}} n'_{\mathfrak{P}}$.

We define the sum of D and D' by

$$D + D' := \sum_{\mathfrak{P}\in\mathbb{P}} (n_{\mathfrak{P}} + n'_{\mathfrak{P}})\mathfrak{P}$$

where the addition in $\mathbb{Z}\cup\{\infty\}$ is the usual addition in $\mathbb{Z}$ if both $n_{\mathfrak{P}}, n'_{\mathfrak{P}} \in \mathbb{Z}$ and $n_{\mathfrak{P}} + n'_{\mathfrak{P}} = \infty$ if $n_{\mathfrak{P}} = \infty$ or $n'_{\mathfrak{P}} = \infty$. We denote the neutral element of the addition in $\mathcal{D}_{\mathcal{C}}$ by 0. We conclude from

$$\deg(D + D') = \deg(D) + \deg(D')$$

that D is invertible $\mathcal{D}_{\mathcal{C}}$ if and only if $\deg(D) < \infty$. The set $\mathcal{D}_{\mathcal{C}}$ endowed with this addition is not a group but only a monoid.

Remark 6.1 *The monoid $\mathcal{D}_{\mathcal{C}}$ contains elements which are not regular. Let A be a divisor such that $A+D = A+D'$. If $\deg(A) < \infty$ then $D = D'$. But if $\deg(A) = \infty$ it can happen that $D \neq D'$.*

It is now straightforward to generalize the concepts of principal divisors and of vector spaces associated to divisors to function rings.

Definition 6.4 (Principal divisor) *Let $u \in \overline{K}(\mathcal{C})$. We call*

$$(u) := \sum_{\mathfrak{P}\in\mathbb{P}} \nu_{\mathfrak{P}}(u)\mathfrak{P}$$

the principal divisor of the function u.

There are principal divisors of infinite degree: these are the principal divisor of zerodivisors of $\overline{K}(\mathcal{C})$. On the contrary, if $u \in \overline{K}(\mathcal{C})^*$, then $\deg(u) = 0$. Let D be a divisor of $\overline{K}(\mathcal{C})$. It is easily verified that

$$\mathcal{L}(D) := \{u \in \overline{K}(\mathcal{C}) \mid D \geq -(u)\} \tag{6.5}$$

is a finite-dimensional $\overline{K}$-vector space. The absolute factorization algorithm proposed in [Duv91] relies on the following proposition:

Proposition 6.2 *(See [Duv91]) Let r be the number of irreducible components $\mathcal{C}^{(i)}$ of $\mathcal{C}$ then*

1. $\dim_{\overline{K}} \mathcal{L}(0) = r$,

2. $\dim_{\overline{K}} \mathcal{L}(-n\mathfrak{P}) = r-1$ *for every place* $\mathfrak{P} \in \overline{K}(\mathcal{C})$ *and for every integer* $n > 0$.

Proof: Let D be a divisor of $\overline{K}(\mathcal{C})$ with $\deg(D) < \infty$. It is obvious that

$$\mathcal{L}(D) \cong \mathcal{L}(D^{(1)}) \times \ldots \times \mathcal{L}(D^{(r)})$$

via the $\overline{K}$-algebra isomorphism $\overline{K}(\mathcal{C}) \cong \overline{K}(\mathcal{C}^{(i)}) \times \ldots \times \overline{K}(\mathcal{C}^{(i)})$. The $\overline{K}$-vector spaces $\mathcal{L}(D^{(i)}) \subset \overline{K}(\mathcal{C}^{(i)})$ have all a finite dimension and $\dim_{\overline{K}} \mathcal{L}(D) = \sum_{i=1}^{r} \dim_{\overline{K}} \mathcal{L}(D^{(i)})$. Especially $\dim_{\overline{K}} \mathcal{L}(0) = \sum_{i=1}^{r} \dim_{\overline{K}} \mathcal{L}(0^{(i)}) = r$ because the dimension of the vector space associated to the zero divisor in a function field is 1. We can suppose without loss of generality that $\mathfrak{P}$ is a place of $\mathcal{C}^{(1)}$ and let $n > 0$. It is obvious that $u \in \mathcal{L}(-n\mathfrak{P})$ if and only if $u^{(1)} = 0$ and $u^{(i)} \in \overline{K}$ for $i \neq 1$ and therefore $\dim_{\overline{K}} \mathcal{L}(-n\mathfrak{P}) = r-1$. □

Remark 6.2 (Absolute factor) *Let* $F_i \in \overline{K}[X,Y]$ *for* $i = 1, \ldots, r-1$ *and* $G \in \overline{K}[X,Y]$ *be such that*

$$F_i/G \in \mathcal{L}(-\mathfrak{P}).$$

This means that $F \mod C^{(1)} = 0$ *and consequently* F_i *are multiples of* $C^{(1)}$. *By calculating* $\gcd(C, F_1, \ldots, F_{r-1})$ *we obtain an absolutely irreducible factor.*

6.4 Local rings of points of a reduced curve

Let $\mathcal{C} := \{C = 0\}$ be an affine plane reduced curve and $P \in \mathcal{C}$. We will study the local properties of $\mathcal{C}$, that is the intrinsic properties of points of the curve $\mathcal{C}$. It is evident that such properties should only depend on the components passing through P. At first glance it may seem that

$$\overline{K}[\mathcal{C}]_P := \{f/g \mid f \in \overline{K}[\mathcal{C}], g \in \overline{K}[\mathcal{C}]^* \text{ and } g(P) \neq 0\} \subset \overline{K}(\mathcal{C})$$

is the right choice for the local ring of the point P of the curve $\mathcal{C}$. If the curve $\mathcal{C}$ is irreducible, then the coordinate ring $\overline{K}[\mathcal{C}]$ is integer and $\overline{K}[\mathcal{C}]_P$ is its localization in the maximal ideal formed by elements $g \in \overline{K}[\mathcal{C}]$ such that $g(P) = 0$. But if $\mathcal{C}$ is a reducible curve then it turns out that the ring $\overline{K}[\mathcal{C}]_P$ is not necessarily local.

Proposition 6.3 *Let* $\mathcal{C}$ *be an affine plane reduced curve,* $\mathcal{C}^{(1)}, \ldots, \mathcal{C}^{(r)}$ *its irreducible components and* $P \in \mathcal{C}$. *Then* $\overline{K}[\mathcal{C}]_P$ *is a local ring if and only if* $P \in \bigcap_{i=1}^{r} \mathcal{C}^{(i)}$.

Proof: Consider the ideals $I^{(i)} := \overline{C}^{(i)}\overline{K}[\mathcal{C}]_P$ for $i = 1, \ldots, r$. Observe that the ideals $I^{(i)}$ are prime such that $\{0\} \subsetneq I^{(i)} \subsetneq \overline{K}[\mathcal{C}]_P$ and if $u \in \overline{K}[\mathcal{C}]_P \setminus \cup_{i=1}^{r} I^{(i)}$, then u is invertible in $\overline{K}[\mathcal{C}]_P$. Consider now the ideal

$$M_P := \{f/g \mid f, \in \overline{K}[\mathcal{C}], h \in \overline{K}[\mathcal{C}]^*, f(P) = 0 \text{ and } g(P) \neq 0\}.$$

The ideal M_P is maximal and for $i = 1, \ldots, r$ we have

$$P \in \mathcal{C}^{(i)} \Longrightarrow I^{(i)} \subset M_P$$

Suppose that $P \in \cap_{i=1}^{r} \mathcal{C}^{(i)}$ and let $u \in \overline{K}[\mathcal{C}]_P \setminus M_P$. Since $P \in \cap_{i=1}^{r} \mathcal{C}^{(i)}$ we have $u \notin I^{(i)}$ for $i = 1, \ldots, r$ and consequently u is invertible in $\overline{K}[\mathcal{C}]_P$. The ideal M_P is then maximal since it is exactly the set of elements which are not invertible in $\overline{K}[\mathcal{C}]_P$. Conversely, suppose that there exist i such that $P \notin \mathcal{C}^{(i)}$. Then $\overline{C}^{(i)} \notin M_P$ and consequently $I^{(i)} \not\subset M_P$, i.e. M_P is not the unique

maximal ideal. □

This is not unexpected when we recall that $\overline{K}(\mathcal{C})$ is the ring of "global" functions, that is functions defined on a dense subset of $\mathcal{C}$ which do not allow us to study the local properties of $\mathcal{C}$.

Let us introduce some notation which will be very useful in the following. We associate to a subset S of $\{1, 2, \ldots, r\}$ the polynomial

$$C^{(S)} = \prod_{i \in S} C^{(i)}$$

and the curve

$$\mathcal{C}^{(S)} := \{C^{(S)} = 0\}.$$

We also associate to S the $\overline{K}$-homomorphism

$$\varphi^{(S)} : \overline{K}(\mathcal{C}) \to \overline{K}[\mathcal{C}^{(S)}]$$

which is the projection of $\overline{K}(\mathcal{C})$ onto $\overline{K}[\mathcal{C}^{(S)}]$ defined via the isomorphism φ. To every point $P \in \mathcal{C}$ we associate the *support* of the point P

$$S_P := \{i \in \{1, 2, \ldots, r\} \mid P \in \mathcal{C}^{(i)}\}.$$

If $\#S_P = 1$, then P is the point of only one component of $\mathcal{C}$ and we say the point P is *isolated*. We denote $\mathcal{C}^{(\mathfrak{P})}$ the unique irreducible component such that $\mathfrak{P}$ is a place of $\overline{K}(\mathcal{C}^{(\mathfrak{P})})$.

Definition 6.5 *Let P be a point of $\mathcal{C}$ and S_P the support of P. The ring*

$$\mathcal{O}_P(\mathcal{C}) := \{f/g \mid f \in \overline{K}[\mathcal{C}^{(S_P)}], g \in \overline{K}[\mathcal{C}^{(S_P)}]^* \text{ and } g(P) \neq 0\}$$

is called the local ring of the point P.

By preceding proposition we know that $\mathcal{O}_P(\mathcal{C})$ is a local ring. Its maximal ideal is

$$\mathcal{M}_P(\mathcal{C}) := \{f/g \mid f \in \overline{K}[\mathcal{C}^{(S_P)}], g \in \overline{K}[\mathcal{C}^{(S_P)}]^*, f(P) = 0 \text{ and } g(P) \neq 0\}.$$

It may seem that the above definition of a local ring $\mathcal{O}_P(\mathcal{C})$ is not useful since the factorization of C is not known. The following proposition shows that it is not necessary to know the factorization of C in order to describe the ring $\mathcal{O}_P(\mathcal{C})$. We can do it by passing from the local ring of a point $P \in \mathbb{A}^2$ defined by

$$\mathcal{O}_P(\mathbb{A}^2) := \{F/G \mid F, G \in \overline{K}[X, Y] \text{ and } G(P) \neq 0\}.$$

Proposition 6.4 *Let P be a point of the plane affine reduced curve $\mathcal{C} := \{C = 0\}$. Then*

$$\mathcal{O}_P(\mathcal{C}) \cong \mathcal{O}_P(\mathbb{A}^2)/C\mathcal{O}_P(\mathbb{A}^2).$$

Proof: Let us denote by $\overline{F}$ and $\overline{G}$ the residual images of, respectively, $F, G \in \overline{K}[X, Y]$ in $\overline{K}(\mathcal{C}^{(S_P)}) = \overline{K}[X, Y]/\left\langle C^{(S_P)} \right\rangle$. The map

$$\varphi : \left\{ \begin{array}{ccc} \mathcal{O}_P(\mathbb{A}^2) & \to & \mathcal{O}_P(\mathcal{C}) \\ F/G & \mapsto & \overline{F}/\overline{G} \end{array} \right.$$

is a $\overline{K}$-homomorphism. We have $\ker\varphi = C^{(S_P)}\mathcal{O}_P(\mathbb{A}^2)$. Set $C' := C/C^{(S_P)} \in \overline{K}[X, Y]$. Since $C'(P) \neq 0$ it is clear that $C' \in \mathcal{O}_P(\mathbb{A}^2)$ is invertible in $\mathcal{O}_P(\mathbb{A}^2)$ and consequently $\ker\varphi = C' \ker\varphi = C\mathcal{O}_P(\mathbb{A}^2)$. The homomorphism φ is surjective. Now we have $\mathcal{O}_P(\mathcal{C}) \cong \mathcal{O}_P(\mathbb{A}^2)/C\mathcal{O}_P(\mathbb{A}^2)$. □

One of the most important properties of a point $P \in \mathcal{C}$ is the *multiplicity*. The multiplicity of an affine plane reduced curve is defined like in the irreducible case.

Lemma 6.5 *Let $\mathcal{C}^{(1)}, \ldots, \mathcal{C}^{(r)}$ be the irreducible components of $\mathcal{C}$ and $P \in \mathcal{C}$. We have*

$$m_P(\mathcal{C}) = \sum_{i=1}^{r} m_P(\mathcal{C}^{(i)}).$$

Let C_X and C_Y denote the derivatives of C with respect to X and Y. It is clear that

$$m_P(\mathcal{C}) = 1 \Longleftrightarrow C_X(a,b) \neq 0 \text{ or } C_Y(a,b) \neq 0.$$

The right side of this equivalence corresponds to the definition of a *simple* point of an affine plane curve. If P is simple, then it is clear that only one component of $\mathcal{C}$ passes through P. In this case $\mathcal{C}^{(S_P)}$ is an irreducible curve and $\mathcal{O}_P(\mathcal{C})$ is a discrete valuation ring of the function field $\overline{K}(\mathcal{C}^{(S_P)})$.

Proposition 6.6 *The multiplicity of a point $P \in \mathcal{C}$ depends uniquely on the local ring $\mathcal{O}_P(\mathcal{C})$. Indeed, it can be show that there exists a sufficiently big N such that for all $n \geq N$*

$$m_P(\mathcal{C}) = \dim_{\overline{K}} \mathcal{M}_P(\mathcal{C})^n / \mathcal{M}_P(\mathcal{C})^{n+1}$$

where $\mathcal{M}_P(\mathcal{C})$ is the maximal ideal of $\mathcal{O}_P(\mathcal{C})$.

Proof: [Per95], Proposition 4.6 on page 113. □

6.5 Points of the function ring

We generalize in this section the notions *coordinate pair* and *point* to the function ring $\overline{K}(\mathcal{C})$ of a plane reduced curve.

Definition 6.6 (Coordinate pair of $\overline{K}(\mathcal{C})$) *Let $\overline{K}(\mathcal{C})$ be the function ring of the plane reduced curve $\mathcal{C}$. A* coordinate pair *of $\overline{K}(\mathcal{C})$ is a pair $\Gamma := (x, y)$ satisfying the following properties:*

1. *the regular elements of $\overline{K}[x, y]$ are invertible in $\overline{K}(\mathcal{C})$, and*
2. *the total quotient ring of $\overline{K}[x, y]$ is $\overline{K}(\mathcal{C})$.*

A defining polynomial *of $\Gamma = (x, y)$ is the polynomial $C_\Gamma \in \overline{K}[X, Y]$ of lowest degree such that $C_\Gamma(x, y) = 0$. We associate to the coordinate pair Γ the affine plane curve $\mathcal{C}_\Gamma := \{C_\Gamma = 0\}$.*

Definition 6.7 (Point of $\overline{K}(\mathcal{C})$) *Let $\overline{K}(\mathcal{C})$ be the function ring of the reduced curve $\mathcal{C}$. A* point *of $\overline{K}(\mathcal{C})$ is a pair $P := (a, b; x, y)$ such that*

1. *$\Gamma := (x, y)$ is a coordinate pair of $\overline{K}(\mathcal{C})$ with the defining polynomial C_Γ and*
2. *$(a, b) \in \mathcal{C}_\Gamma := \{C_\Gamma = 0\}$.*

If $\mathcal{C}^{(1)}, \ldots, \mathcal{C}^{(r)}$ are the irreducible components of $\mathcal{C}$ and $\mathcal{C}_\Gamma^{(1)}, \ldots, \mathcal{C}_\Gamma^{(r)}$ are the irreducible components of $\mathcal{C}_\Gamma$ such that $\mathcal{C}^{(i)} \longrightarrow \mathcal{C}_\Gamma^{(i)}$ [4] for $i = 1, \ldots, r$ we call

$$S_P := \{i \mid (a, b) \in \mathcal{C}_\Gamma^{(i)}\}$$

the support *of P. The* multiplicity *of P is multiplicity $m_{(a,b)}(\mathcal{C}_\Gamma)$ of the point $(a, b) \in \mathcal{C}_\Gamma$.*

[4] We mean by $\mathcal{C}^{(i)} \longrightarrow \mathcal{C}_\Gamma^{(i)}$ that we obtain $\mathcal{C}_\Gamma^{(i)}$ by a sequence of translations and strict transformations from $\mathcal{C}^{(i)}$ when we blow up a point of $\mathcal{C}$. Every point of $\overline{K}(\mathcal{C})$ which we work with corresponds either to a point of $\mathcal{C}$ or to a point obtained by blowing up. Therefore the notation $\mathcal{C}^{(i)} \longrightarrow \mathcal{C}_\Gamma^{(i)}$ is well-defined (every transformation can be "traced back").

This definition generalizes of the notion *point of a function field* to function ring of affine plane reduced curve. The notion of point of F of a given function field permits to fix F and to compare in F the local rings of points of different curves having a function field which is isomorphic to F. We will do the same for the function ring $\overline{K}(\mathcal{C})$. But this will be more delicate since the local ring of a point P of the reduced curve $\mathcal{C}$ is not necessarily a subring of $\overline{K}(\mathcal{C})$ but only of $\overline{K}(\mathcal{C}^{(S_P)})$ where S is the support of the point of P.

Definition 6.8 *Let $P := (a, b; x, y)$ be a point of $\overline{K}(\mathcal{C})$ and S_P the support of P. The* local ring $\mathcal{O}_P$ *of the point P is the subring of $\overline{K}(\mathcal{C}^{(S_P)})$ which is isomorphic to the local ring $\mathcal{O}_{(a,b)}(\mathcal{C}_\Gamma) \subset \overline{K}(\mathcal{C}_\Gamma^{S_P})$. We denote by $\mathcal{M}_P$ the maximal ideal of $\mathcal{O}_P$ where $\Gamma = (x, y)$.*

Let P be a point of $\overline{K}(\mathcal{C})$ and S_P be the support of P. It will be useful to consider the element $\varphi^{(S_P)}(u) \in \overline{K}(\mathcal{C}^{(S_P)})$. If $\varphi^{(S_P)}(u) \in \mathcal{O}_P$ we write $u \overline{\in} \mathcal{O}_P$. Similarly, if $\mathfrak{P}$ is a place of $\overline{K}(\mathcal{C})$ we write $u \overline{\in} \mathcal{O}_\mathfrak{P}$ (resp. $u \overline{\in} \mathfrak{P}$) when $\varphi^{(S_P)}(u) \in \mathcal{O}_\mathfrak{P}$ (resp. $\varphi^{(S_P)}(u) \in \mathfrak{P}$). If $u \overline{\in} \mathcal{O}_\mathfrak{P}$, then the unique $\alpha \in \overline{K}$ such that $u - \alpha \overline{\in} \mathfrak{P}$ is called the *evaluation* of u at the place $\mathfrak{P}$. It is denoted by $u(\mathfrak{P})$.

The following proposition is equivalent to the proposition 4.3 when the curve is irreducible.

Definition 6.9 *Let $P := (a, b; x, y)$ be a point of $\overline{K}(\mathcal{C})$. Let Q be a point (resp. $\mathfrak{P}$ a place) of $\overline{K}(\mathcal{C})$. We say Q (resp. $\mathfrak{P}$) is* above P, *denoted by $Q \mid P$ (resp. $\mathfrak{P} \mid P$) if*

$$x - a \overline{\in} \mathcal{M}_Q \text{ and } y - b \overline{\in} \mathcal{M}_Q \text{ (resp. } x - a \overline{\in} \mathfrak{P} \text{ and } y - b \overline{\in} \mathfrak{P} \text{).}$$

If the curve is irreducible we know there are at least one and at most finitely many places above P. It is also clear that this is also true when the curve is reduced.

6.6 Blowing-up points

Strict transforms, *exceptional coordinates*, and *monoidal transformations* are defined like in the irreducible case. If $C = \prod_{i=1}^r C^{(i)}$, then $C^{[x]} = \prod_{i=1}^r C^{(i)^{[x]}}$ and $C^{[y]} = \prod_{i=1}^r C^{(i)^{[y]}}$. We conclude that if C is not divisible by X (resp. Y), then C is irreducible if and only if $C^{[x]}$ (resp. $C^{[y]}$) is irreducible. Moreover, $\overline{K}(\mathcal{C}) \cong \overline{K}(C^{[x]})$ (resp. $\overline{K}(\mathcal{C}) \cong \overline{K}(C^{[y]})$. Moreover, we have the following proposition.

Proposition 6.7 *Let $\Gamma := (x, y)$ be a coordinate pair of $\overline{K}(\mathcal{C})$ and C the defining polynomial of Γ. If C is not divisible by X (resp. Y) then $(x, y/x)$ (resp. $(x/y, y)$) is coordinate pairs of $\overline{K}(\mathcal{C})$ with $C^{[x]}$ (resp. $C^{[y]}$) as defining polynomial.*

Proof: We show the proposition for $(x, y/x)$. Suppose that X does not divide C. It is clear that if $(x, y/x)$ is a coordinate pair then $C^{[x]}$ is the defining polynomial. Since $\overline{K}[x, y] \subset \overline{K}[x, y/x]$ it suffices to show that every regular element of $\overline{K}[x, y/x]$ is invertible in $\overline{K}(\mathcal{C})$ because it is clear that in this case the total quotient ring of $\overline{K}[x, y/x]$ is equal to $\overline{K}(\mathcal{C})$. Let g be a regular element of $\overline{K}[x, y/x]$. Then there exists $n \in \mathbb{N}$ such that $g' := x^n g \in \overline{K}[x, y]$. The element g' is regular in $\overline{K}[x, y]$ since x is regular in $\overline{K}[x, y]$. Therefore g' is invertible in $\overline{K}(\mathcal{C})$ and also $g = g'/x^n$. □

Suppose that $P = (0, 0; x, y)$ and let $C(X, Y) \in \overline{K}[X, Y]$ be the defining polynomial of the coordinate pair (x, y). Let $\mathrm{Init}(C)$ be the initial form of C and $m := m_P > 0$ the degree of $\mathrm{Init}(C)$. Consider its factorization

$$\mathrm{Init}(C) = \prod_{i=1}^{m} (\alpha_i X + \beta_i Y).$$

Let (x, y_1) (resp. (x_1, y)) be the monoidal transform of (x, y) with respect to the exceptional coordinate x (resp. y) which have $C^{[x]}$ (resp. $C^{[y]}$) as defining polynomials. Let $H = C - \mathrm{Init}(C)$. Then $l := \deg \mathrm{Init}(C) > m$ and we can write

$$C^{[x]} = \prod_{i=1}^{m}(\alpha_i + \beta_i Y) + X^{(l-m)}H^{[x]}$$

and

$$C^{[y]} = \prod_{i=1}^{m}(\alpha_i X + \beta_i) + Y^{(l-m)}H^{[y]}.$$

Now let $\mathfrak{P} \in \mathbb{P}_{\overline{F}}$ be a place dominating P (recall that in this case $x, y \in \mathfrak{P}$ by proposition 4.3). By the definition of a valuation ring we have $y_1 = y/x \in \mathcal{O}_{\mathfrak{P}}$ or $x_1 = x/y \in \mathcal{O}_{\mathfrak{P}}$.

1. If $y_1 \,\overline{\in}\, \mathcal{O}_{\mathfrak{P}}$, then

$$0 = 0(\mathfrak{P}) = C^{[x]}(x, y_1)(\mathfrak{P}) = \prod_{i=1}^{m}(\alpha_i + \beta_i y_1(\mathfrak{P})) = \mathrm{Init}(C)(1, y_1(\mathfrak{P}))$$

   and consequently there exists i such that $\beta_i \neq 0$ and $y_1(\mathfrak{P}) = -\alpha_i/\beta_i$. Therefore

$$P^{\mathfrak{P}} := (0, -\alpha_i/\beta_i; x, y_1).$$

2. If $y_1 \,\overline{\notin}\, \mathcal{O}_{\mathfrak{P}}$, then $x_1 \in \mathfrak{P}$ and $x_1(\mathfrak{P}) = 0$. We have

$$0 = 0(\mathfrak{P}) = C^{[y]}(x_1, y)(\mathfrak{P}) = \prod_{i=1}^{m}(\alpha_i x_1(\mathfrak{P}) + \beta_i) = \prod_{i=1}^{m}\beta_i$$

   and consequently there exists i such that $\beta_i = 0$. Therefore

$$P^{\mathfrak{P}} := (0, 0; x_1, y).$$

Note that the values $-\alpha_i/\beta_i$ are the distinct roots of $\mathrm{Init}(C)(1, Y)$. There exists i such that $\beta_i = 0$ if and only if $\mathrm{Init}(C)(0, 1) = 0$ which is equivalent to say that X divides $\mathrm{Init}(C)$. More precisely, we have

$$\mathfrak{B}(P) := \{(0, \gamma; x, y_1) \mid \gamma \in \overline{K}, \mathrm{Init}(C)(1, \gamma) = 0\} \cup \mathfrak{B}_\infty(P)$$

where

$$\mathfrak{B}_\infty(P) = \begin{cases} \{(0, 0; x_1, y)\} & \text{if } \mathrm{Init}(C)(0, 1) = 0 \\ \emptyset & \text{otherwise} \end{cases}.$$

Proposition 6.8 *Let P be a point of $\overline{K}(\mathcal{C})$. Then*

1. $\mathfrak{B}(P) = \{P^{\mathfrak{P}} \mid \mathfrak{P} \mid P\}$,
2. *for every place above the point P we have*

$$\mathfrak{P} \mid P^{\mathfrak{P}} \text{ and } P^{\mathfrak{P}} \mid P.$$

Proof: Let $Q \in \mathfrak{B}(P)$ and suppose without loss of generality that $P = (0, 0; x, y)$ and $Q = (0, \gamma; x, y)$ where $y_1 := y/x$. It is clear that $x \overline{\in} \mathcal{M}_Q$ and $y = xy_1$ and therefore Q is above P. We will show that there exists a place $\mathfrak{P}$ such that $Q = \mathfrak{P}$ to finish the proof. Let C be the defining polynomial of (x, y). By the definition of Q we have $\mathrm{Init}(C)(1, \gamma) = 0$. So there exists an irreducible factor C' of C such that $\mathrm{Init}(C')(1, \gamma) = 0$. Let $\mathcal{C}' := \{C' = 0\}$ which is an irreducible component of $\mathcal{C}$. Let us denote by x', y' and y'_1 the projections of, respectively, x, y and y_1 onto $\overline{K}(\mathcal{C}')$. Then $P' := (0, 0; x', y')$ and $Q' := (0, \gamma; x', y'_1) \in \mathfrak{B}(P')$ are points of the function field $\overline{K}(\mathcal{C}')$. There exists a place $\mathfrak{P}$ of $\overline{K}(\mathcal{C}')$ such that $\mathfrak{P} \subset \mathcal{M}_{Q'}$ and therefore $Q' := P'^{\mathfrak{P}}$. Since $\mathfrak{P}$ is a place of $\overline{K}(\mathcal{C})$ by definition it is clear that $Q' = P'^{\mathfrak{P}}$ implies $Q = P^{\mathfrak{P}}$. □

Proposition 6.9 *Let P be a point of $\overline{K}(\mathcal{C})$ and $\mathfrak{P}$ a place dominating the point P. Then there exists $N \in \mathbb{N}$ such that for $n \geq N$ the point $P^{\mathfrak{P}}$ is an isolated point of $\overline{K}(\mathcal{C})$.*

Proof: There is nothing to show if the curve $\mathcal{C}$ is irreducible. Let $\mathcal{C}^{(1)}, \ldots, \mathcal{C}^{(r)}$ be the $r \geq 2$ irreducible components of $\mathcal{C}$. Suppose that $P = (0, 0; x, y)$. Let C be the defining polynomial of (x, y) and $C^{(1)}, \ldots, C^{(r)}$ be the r irreducible factors of C (in the order corresponding to the irreducible components $\mathcal{C}^{(i)}$). Suppose that $\mathfrak{P}$ is a place of $\overline{K}(\mathcal{C}^{(i)})$ and set

$$G_1(X, Y) := C/C^{(1)} = \prod_{i=2}^{r} C^{(i)} \in \overline{K}[X, Y].$$

If $G_1(0, 0) \neq 0$ then it is clear that the point P is isolated and the proof is finished. Otherwise let $Q := P^{\mathfrak{P}}$ and suppose that $Q = (0, \gamma; x, y_1)$ where $y_1 := y/x$. Recall that $C^{[x]}$ is the defining polynomial of the coordinate pair (x, y). Set

$$G_2(X, Y) := G_1^{[x]} = C^{[x]}/C^{(1)\,[x]}.$$

If $G_2(0, \gamma) \neq 0$, then Q is isolated and the proof is finished. Otherwise consider the functions

$$g_1 := G_1(x, y) \text{ and } g_2 := G_2(x, y_1).$$

They are linked with each other by the relation

$$g_1 = x^m g_2$$

where $m := \deg \mathrm{Init}(G_1)$. Consequently $\nu_{\mathfrak{P}}(g_1) > \nu_{\mathfrak{P}}(g_2)$ since $m > 0$ and $\nu_{\mathfrak{P}}(x) > 0$. We replace P by Q which move to the origin and repeat the step. We find $g_3 \in \overline{K}(\mathcal{C})$ with $\nu_{\mathfrak{P}}(g_3) > \nu_{\mathfrak{P}}(g_2)$. After a finite number of iterations, say N, we find g_N such that $\nu_{\mathfrak{P}}(g_N) = 0$ and consequently the point $P^{\mathfrak{P}^{(n)}}$ is isolated for $n \geq N$. □

Corollary 6.10 *Let P be a point of $\overline{K}(\mathcal{C})$ and $\mathfrak{P}$ a place dominating the point P. Then there exists $N \in \mathbb{N}$ such that for $n \geq N$ the point $P^{\mathfrak{P}}$ is simple.*

Proof: We know that this is true when the curve $\mathcal{C}$ is irreducible. This already suffices to prove the corollary since by the preceding lemma we can suppose that P is isolated and in this case the local ring $\mathcal{O}_P$ is contained in the function field of the irreducible component passing through P. □

The desingularisation tree is defined like in the irreducible case.

6.7 Divisors

Exceptional, local, adjoint and intersection divisors are defined like in the irreducible case. The following proposition gives us a sufficient condition for applying the Max Noether's Fundamental Theorem which the Brill-Noether algorithm is based upon. We already know that this proposition is true for irreducible curves and the proof is much simpler than that for reducible curves. We consider a singular point P of a curve $\mathcal{C}$ to pinpoint this difference. If $\mathcal{C}$ is irreducible, then the local rings of all infinitely close points of P are contained in the function field. The proof is then based upon an element contained in the intersection of all these local rings. But if the curve $\mathcal{C}$ is reducible the point may not be isolated and then the local rings of the infinitely close points of P are not all necessarily contained in the same function ring and it is not possible to take the intersection of these local rings.

Proposition 6.11 *Let $P := (0, 0; x, y)$ be a point $\overline{F}/\overline{K}$ and suppose that X does not divide* $\mathrm{Init}(C)$ *where C is the defining polynomial of the coordinate pair (x, y). Then the ring $\mathcal{O}_P[y_1]$ is a semi-local ring and its maximal ideals correspond bijectively to the points of $\mathfrak{B}(P)$.*

Proof: We already know that this is true for the absolutely irreducible case (see proposition 4.12). By projecting on the function fields of the absolutely irreducible components it is not difficult to prove that this is also true for the reducible case. □

Proposition 6.12 *Let $\mathcal{C} := \{C = 0\}$ be a reduced curve, P be a point of $\overline{K}(\mathcal{C})$ and $u \in \overline{K}(\mathcal{C})$. Then*

$$(u)_P \geq \mathcal{A}_P \Longrightarrow u \,\overline{\in}\, \mathcal{O}_P.$$

Proof: We use induction on $N := \deg \mathcal{A}_P$. If $N = 0$ then P is a simple point and $(u)_P = \nu_{\mathfrak{P}}(u)\mathfrak{P}$ where $\mathfrak{P} \equiv P$. By assumption we have $\nu_{\mathfrak{P}}(u) \geq 0$ and consequently $u \in \mathcal{O}_{\mathfrak{P}} = \mathcal{O}_P$. Let P be singular. We assume that the proposition is true for all $n < N$. We suppose without loss of generality that all components of $\mathcal{C}$ pass through $P = (0, 0; x, y)$ and that X does not divide $\mathrm{Init}(C)$. In this case x is invertible in $\overline{K}(\mathcal{C})$ and

$$x^{m_P-1}\mathcal{O}_P[y_1] \subseteq \mathcal{O}_P$$

where m_P is the multiplicity of the point P and $y_1 := y/x$. It is sufficient to show that $v := u/x^{m_P-1} \in \mathcal{O}_P[y_1]$. Let $C' := C^{[x]}$ be the defining polynomial of (x, y_1) and $G, H \in \overline{K}[X, Y]$ such that

$$v = \frac{G(x, y_1)}{H(x, y_1)}.$$

If $H(Q) \neq 0$ for all $Q \in \mathfrak{B}(P)$ then the proof is finished since then we can show that $H(x, y_1)$ does not belong to any maximal ideal of $\mathcal{O}_P[y_1]$ (see proposition 6.11) and consequently v is invertible in $\mathcal{O}_P[y_1]$. Otherwise we must find $G', H' \in \overline{K}[X, Y]$ (another representation) such that $v = G'(x, y_1)/H'(x, y_1)$ and $H'(Q) \neq 0$ for all $Q \in \mathfrak{B}(Q)$. Observe that

$$(u)_P = \sum_{Q \in \mathfrak{B}(P)} (u)_Q \geq \mathcal{A}_P = (m_P - 1)E_P + \sum_{Q \in \mathfrak{B}(P)} \mathcal{A}_Q$$

and $E_P = (x)_P$. Now we can write

$$(v)_Q = (u)_Q - (x^{(m_P-1)})_Q \geq \mathcal{A}_Q \text{ for all } Q \in \mathfrak{B}(P).$$

Since $\deg \mathcal{A}_Q < \deg \mathcal{A}_P$ for all $Q \in \mathfrak{B}(P)$ we have

$$v \overline{\in} \mathcal{O}_Q \text{ for all } Q \in \mathfrak{B}(P).$$

Therefore there exist for every point $Q \in \mathfrak{B}(P)$ three polynomials $G_Q, H_Q, A_Q \in \overline{K}[X,Y]$ such that

$$H_Q(Q) \neq 0 \text{ and } GH_Q = G_Q H + A_Q C'^{(S_Q)}.$$

We set

$$\widehat{C}'_Q := C'/C'^{(S_Q)} \in \overline{K}[X,Y].$$

Since $\widehat{C}'_Q(Q) \neq 0$ and $H_Q(Q) \neq 0$ we can choose $\alpha_Q \in \overline{K}$ such that $H'(Q) \neq 0$ for all $Q \in \mathfrak{B}(Q)$ where

$$H' := \sum_{Q \in \mathfrak{B}(P)} \alpha_Q \widehat{C}'_Q H_Q.$$

We multiply the equation $GH_Q = G_Q H + A_Q C'^{(S_Q)}$ by $\alpha_Q \widehat{C}'_Q$ for each $Q \in \mathfrak{B}(Q)$ and sum up. We obtain

$$GH' = G'H + (\sum_{Q \in \mathfrak{B}(P)} \alpha_Q A_Q) C'$$

where

$$G' := \sum_{Q \in \mathfrak{B}(P)} \alpha_Q \widehat{C}'_Q G_Q.$$

Consequently we have

$$v = \frac{G'(x, y_1)}{H'(x, y_1)}$$

with $H'(Q) \neq 0$ for all $Q \in \mathfrak{B}(P)$. □

The Brill-Noether algorithm relies essentially on Max Noether's Fundamental Theorem which does not impose any constraint on the irreducibility of the curve $\mathcal{C}^*$.

Theorem 6.13 (Max Noether's Fundamental Theorem) *Let $\mathcal{C}^* := \{C^* = 0\}$ a projective plane curve. Let $F, G \in \overline{K}[U,V,W]$ be two homogeneous polynomials such that C^* does not divide G. Then the following conditions are equivalent:*

1. *there exist two homogeneous polynomials $A, B \in \overline{K}[U,V,W]$ such that* $\deg A + \deg G = \deg B + \deg C^* = \deg F$ *and*
$$F = AG + BC^*.$$
2. $\overline{F}^P / \overline{G}^P \overline{\in} \mathcal{O}_{P_*}$.

Proof: See [Ful69] on page 120 □

The following theorem gives us an algorithm which computes a basis of the vector space associated to a divisor.

Theorem 6.14 *Let $\mathcal{C}^* := \{C^* = 0\}$ be a projective plane curve, $\mathcal{A}$ be its adjoint divisor and D be a divisor of $\overline{K}(\mathcal{C}^*)$ with $\deg D < \infty$. Let $G_0 \in S_d$ such that C^* does not divide G_0 and*

$$(G_0) \geq D + \mathcal{A}.$$

Then

$$\mathcal{L}(D) := \{\overline{G}/\overline{G_0} \mid G \in S_d \text{ non-divisible by } C^* \text{ and } (G) \geq (G_0) - D\} \cup \{0\}$$

where $\overline{G}$ and $\overline{G_0}$ are the residual images of, respectively, G and G_0 in $\overline{K}[\mathcal{C}^*]$ and $S_d \subset \overline{K}[U, V, W]$ is the set of homogeneous polynomials of degree d.

Proof: ($\supseteq$) : Let $G \in \overline{K}[U, V, W]$ be a homogeneous polynomial such that $\deg G = \deg G_0$, C^* does not divide G and $(G) \geq (G_0) - D$. Set $z := \overline{G}/\overline{G_0}$. Then

$$(z) + D = (G) - (G_0) + D \geq 0$$

so that $z \in \mathcal{L}(D)$.
($\subseteq$) : Let $z \in \mathcal{L}(D) \setminus \{0\}$. Then $D' := D + (z) \geq 0$ by the definition of $\mathcal{L}(D)$. Since $D' \equiv D$ and $(G_0) \geq D + \mathcal{A}$ we can apply the theorem 4.34 with $R := (G_0) - (D + \mathcal{A}) \geq 0$ to find a $G' \in \overline{K}[U, V, W]$ such that $\deg G' = \deg G$ and

$$(G') = D' + \mathcal{A} + R.$$

We have

$$(G') - (G_0) = D' - D = (z).$$

Let $z' := \overline{G}/\overline{G_0}$. Then $(z/z') = 0$. Since z and z' have the same zeros and poles we have

$$z = \alpha z' := \alpha\overline{G'}/\overline{G_0}$$

which proves that z can be written in the above form. □

6.8 Examples

Consider the curve $\mathcal{C}^*$ determine by the polynomial

```
>> projectiveCurve;
         6    5      4  2    3  3    2  4      4      6
   poly(X  + X  Z + X  Z  + X  Z  + X  Y  + X Y  Z + Y , [X, Y, Z], F_2)
```

defined over

```
>> groundField;
                                     F_2
>> nops(ListOfSingPts);
                                      2
>> map(ListOfSingPts, printProjPoint);
                            [[1, 0, 1], [0, 0, 1]]
>> map(ListOfDesingTrees, drawTree);
                           ["UU(L1)..", "UU(L2).."]
```

```
>> printDivisor(adjointDivisor);
                                    3       3
                                4 L1  + 4 L2
>> nums := interpolatingForms(adjointDivisor,4);
      4                           2  2      2
[poly(Y , [X, Y, Z], F_2), poly(X  Y  + X Y  Z, [X, Y, Z], F_2),
        4    2  2
   poly(X  + X  Z , [X, Y, Z], F_2)]
>> G0 := nums[1];
                                4
                           poly(Y , [X, Y, Z], F_2)
>> interDivG0 := intersectionDivisor(G0);
                                 4 L1 + 4 L2
```

Since the intersection divisor of (G_0) and the adjoint divisor are the same, the denominators can be chosen as the interpolating forms for the adjoint divisor. We see that the polynomial has three absolutely irreductibel factors.

```
>> absFactor(4,L1);
                     2                    2
               poly(X  + X Z + (X2 + 1) Y , [X, Y, Z], F_8)
>> op(%, 3);
                                     F_8
>> (%)::minpoly;
                           3     2
                  poly(X2  + X2  + 1, [X2], IntMod(2))
```

Chapter 7

Conclusion

The aim of this diploma thesis has been the implementation of all algorithms necessary to construct geometric Goppa codes and to determine the absolutely irreducible factors of a bivariate polynomial in the computer algebra system MuPAD.

In the first part the geometric Goppa codes have been introduced using the language of algebraic function fields of one variable. It has been shown how the Brill-Noether algorithm can be used for the construction of geometric Goppa codes provided that we know a plane model of the algebraic function field. The main difficulty is here that we are working with a curve which may contain any singularities. Therefore we have used a generalization of the classical Brill-Noether algorithm to projective plane curves with any singularities. The presentation of the algorithms in a strictly algebraic manner using the theory of algebraic function fields has facilitated the translation from theory to implementation. We have shown how to obtain a representation of all places using the technique of blowing up. It is possible to determine places of any degree, to construct any divisor, to compute a basis of the vector space associated to any divisor, and to evaluate functions at any place of degree one. We need all this for the construction of a geometric Goppa code. Moreover, we can compute the genus and canonical divisors of the function field. Many results presented in [Sti93] can be verified by computing concrete examples.

The second part treats the absolute factorization of bivariate polynomials. It has been shown that the Brill-Noether algorithm is also valid for reduced curves. Here the function field of an absolutely irreducible curve is replaced by the function ring of a reduced curve and the concepts of algebraic function fields are carried over to function rings of reduced curves. A geometric approach for the absolute factorization has been described.

Some new proofs concerning the Brill-Noether algorithm have been presented in this diploma thesis. All the necessary algorithms for the construction of geometric Goppa codes and the absolute factorization have been implemented by the author in MuPAD. The Brill-Noether algorithm is defined over an algebraically closed field. It has been shown how an algebraic closure of the ground field can be simulated by using dynamic extensions. During the computations it is necessary to construct extension fields. Unfortunately MuPAD does not offer any methods for this. The necessary methods had to be implemented. An implementation in MAGMA is planned since MAGMA offers very efficient methods for constructing extension fields and for analyzing error-correcting codes (see [BCP97]). It would be interesting to study the properties of the codes in dependence on the choice of the divisors used for the construction.

Acknowledgements

I would like to express my gratitude first to my diploma thesis supervisor Prof. Calmet and also to my second supervisor Dr. Zimmermann who welcomed me into the PolKA project at LORIA in France.

I would like to extend my gratitude to Dr. Haché from the "Centre interuniversitaire en calcul mathématiques algébriques" of McGill University in Montréal for helping me understand the full scope of the theory of the Brill-Noether algorithm. My diploma work is substantially based on his Ph. D. thesis.

Bibliography

[BCP97] Wieb Bosma, John J. Cannon, and Catherine Playoust. The Magma Algebra System I: The User Language. *Journal of Symbolic Computation*, 24(3–4):235–266, 1997.

[BH95] D. Le Brigand and G. Haché. Effective construction of algebraic geometry codes. *IEEE Transations on Information Theory*, 41(6):1615–1628, November 1995.

[BR88] D. Le Brigand and J. J. Risler. Algorithme de Brill-Noether et codes de Goppa. *Bull. Soc. Math. France*, 116:231–253, 1988.

[Che51] Claude Chevalley. *Introduction to the theory of algebraic functions of one variable*. Mathematical survey. New-York, American Mathematical Society, 1951.

[Duv91] D. Duval. Absolute factorization of polynomials: a geometric approach. *SIAM Journal on computing*, 20(1):1–21, February 1991.

[Eis95] David Eisenbud. *Commutative Algebra with a View Towards Algebraic Geometry*. Graduate Texts in Mathematics. Springer-Verlag, 1995.

[Ful69] William Fulton. *Algebraic curves*. W.A. Benjamin, INC., 1969.

[Gor52] Daniel Gorenstein. An arithmetic theory of adjoint plane curves. *Trans. Amer. Math. Soc*, 72:414–436, 1952.

[Hac95] Gaétan Haché. Computation in algebraic function fields for effective construction of algebraic-geometric codes. *Lecture Notes in Computer Science*, 948:262–278, 1995.

[Hac96] Gaétan Haché. *Construction Effective des Codes Géométriques*. Ph.D. thesis, Université Paris 6, 1996.

[Hac98] Gaétan Haché. L'algorithme de Brill-Noether appliqué aux courbes réduites. Rapport de recherche du Laboratoire LACO, `http://www.unilim.fr/laco/rapports/index.html`, 1998.

[Kun85] E. Kunz. *Introduction to Commutative Algebra and Algebraic Geometry*. Birkhäuser, 1985.

[Lau97] K. S. Laursen. *Constructing Geometric Goppa Codes*. Ph.D. thesis, Aalborg university, 1997.

[LB89] D. Le Brigand. Polynomial Factorization Using Brill-Noether Algorithm. *Lecture Notes in Computer Science*, 388:37–46, 1989.

[Mat80] H. Matsumura. *Commutative Algebra*. Mathematics Lecture Note Series. The Benjamin/Cummings Publishing Company, second edition, 1980.

[Mnu97] Michal Mnuk. An Algebraic Approach to Computing Adjoint Curves. *J. Symbolic Computation*, 23:229–240, 1997.

[Per95] Daniel Perrin. *Géométrie algébrique - Une introduction*. InterÉditions/CNRS Éditions, 1995.

[Sti93] Henning Stichtenoth. *Algebraic function fields and codes*. Springer, 1993.

[VT91] S. G. Vladut and M. A. Tsfasman. *Algebraic-Geometric Codes*. Mathematics and Its Applications. Kluwer Academic Publishers, 1991.