The Abdus Salam International Centre for Theoretical Physics

United Nations Educational, Scientific and Cultural Organization

IAEA International Atomic Energy Agency

1958-10

# Summer School and Conference Mathematics, Algorithms and Proofs

*11 - 29 August 2008*

## Algorithms and Algebraic Geometry

Gert-Martin Greuel
*Universitaet Kaiserslautern and Mathematisches Forschungsinstitut Oberwolfach, Germany*

# Algorithms and Algebraic Geometry

Gert-Martin Greuel
Universität Kaiserslautern
and
Mathematisches Forschungsinstitut Oberwolfach

May 31, 2008

## Contents

# 1 Gröbner Basics

## 1.1 Rings and Ring Maps

**Definition 1.1.1.** Let $A$ be a ring, always commutative with 1.

(1) A **monomial** in $n$ variables (or indeterminates) $x_1, \dots, x_n$ is a power product

$$x^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}, \qquad \alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n .$$

The set of monomials in $n$ variables is denoted by

$$\mathbf{Mon}(\mathbf{x_1}, \dots, \mathbf{x_n}) = \mathbf{Mon_n} := \{x^\alpha \mid \alpha \in \mathbb{N}^n\} .$$

$\mathrm{Mon}(x_1, \dots, x_n)$ is a semigroup under multiplication, with neutral element $1 = x_1^0 \cdot \ldots \cdot x_n^0$.

$x^\alpha \mid x^\beta$ ($x^\alpha$ **divides** $x^\beta$) $\iff \alpha_i \le \beta_i$ for all $i$.

(2) A **term** is a monomial times a coefficient (an element of $A$),

$$ax^\alpha = ax_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}, \quad a \in A .$$

(3) A **polynomial over** $A$ is a finite sum of terms,

$$f = \sum_\alpha a_\alpha x^\alpha = \sum_{\alpha \in \mathbb{N}^n}^{\text{finite}} a_{\alpha_1 \ldots \alpha_n} x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} ,$$

with $a_\alpha \in A$. For $\alpha \in \mathbb{N}^n$, let $|\alpha| := \alpha_1 + \cdots + \alpha_n$.

$\deg(f) := \max\{|\alpha| \mid a_\alpha \ne 0\}$ is called the **degree** of $f$ if $f \ne 0$; $\deg(f) = -1$ for $f = 0$.

(4) The **polynomial ring** $A[x] = A[x_1, \dots, x_n]$ in $n$ variables over $A$ is the set of all polynomials together with the usual addition and multiplication:

$$\sum_\alpha a_\alpha x^\alpha + \sum_\alpha b_\alpha x^\alpha := \sum_\alpha (a_\alpha + b_\alpha) x^\alpha,$$

$$\left(\sum_\alpha a_\alpha x^\alpha\right) \cdot \left(\sum_\beta b_\beta x^\beta\right) := \sum_\gamma \left(\sum_{\alpha+\beta=\gamma} a_\alpha b_\beta\right) x^\gamma.$$

**Definition 1.1.2.** A **morphism** of rings is a map $\varphi : A \to B$ satisfying $\varphi(a + a') = \varphi(a) + \varphi(a')$, $\varphi(aa') = \varphi(a)\varphi(a')$, for all $a, a' \in A$, and $\varphi(1) = 1$. We call a morphism of rings also a **ring map**, and $B$ is called an $A$–**algebra**.

**Lemma 1.1.3.** *Let $A[x_1, \dots x_n]$ be a polynomial ring, $\psi : A \to B$ a ring map, $C$ a $B$–algebra, and $f_1, \dots, f_n \in C$ (e.g. $B = A$ and $\psi = id$). Then there exists a unique ring map*

$$\varphi : A[x_1, \dots, x_n] \longrightarrow C$$

*satisfying $\varphi(x_i) = f_i$ for $i = 1, \dots, n$ and $\varphi(a) = \psi(a) \cdot 1 \in C$ for $a \in A$.*

In SINGULAR one can define polynomial rings over the following fields:

(1) the field of rational numbers $\mathbb{Q}$,

(2) finite fields $\mathbb{F}_p$, $p$ a prime number $< 2^{31}$,

(3) finite fields $\mathbf{GF}(p^n)$ with $p^n$ elements, $p$ a prime, $p^n \leq 2^{15}$,

(4) **transcendental extensions of** $\mathbb{K} \in \{\mathbb{Q}, \mathbb{F}_p\}$, $\mathbb{K}(a_1, \ldots, a_n)$,

(5) simple **algebraic extensions of** $\mathbb{K} \in \{\mathbb{Q}, \mathbb{F}_p\}$, $\mathbb{K}[a]/\text{minpoly}$,

(6) arbitrary precision **real floating point numbers**,

(7) arbitrary precision **complex floating point numbers**.

## 1.2 Monomial Orderings

Monomial orderings are necessary for constructive ideal and module theory.

**Definition 1.2.1.** A **monomial ordering** or **semigroup ordering** is a total (or linear) ordering $>$ on $\text{Mon}(x_1, \ldots, x_n)$ satisfying

$$x^\alpha > x^\beta \implies x^\gamma x^\alpha > x^\gamma x^\beta$$

for all $\alpha, \beta, \gamma \in \mathbb{N}^n$. We say also $>$ is a *monomial ordering* on $A[x_1, \ldots, x_n]$.
A monomial ordering is a total ordering on $\mathbb{N}^n$, which is compatible with the semigroup structure on $\mathbb{N}^n$ given by addition.

*Example* 1.2.2. The **lexicographical ordering** on $\mathbb{N}^n$:
$x^\alpha > x^\beta$ if and only if the first non–zero entry of $\alpha - \beta$ is positive.

**Definition 1.2.3.** Let $>$ be a fixed monomial ordering. Write $f \in A[x]$, $f \neq 0$, in a unique way as a sum of non–zero terms

$$f = a_\alpha x^\alpha + a_\beta x^\beta + \cdots + a_\gamma x^\gamma, \quad x^\alpha > x^\beta > \cdots > x^\gamma\,,$$

and $a_\alpha, a_\beta, \ldots, a_\gamma \in K$. We define:

(1) $\text{LM}(f) :=$ `leadmonom(f)`$:= x^\alpha$, the **leading monomial** of $f$,

(2) $\text{LE}(f) :=$ `leadexp(f)`$:= \alpha$, the **leading exponent** of $f$,

(3) $\text{LT}(f) :=$ `lead(f)`$:= a_\alpha x^\alpha$, the **leading term** or **head** of $f$,

(4) $\text{LC}(f) :=$ `leadcoef(f)`$:= a_\alpha$, the **leading coefficient** of $f$,

(5) $\text{tail}(f) := f -$ `lead(f)`$= a_\beta x^\beta + \cdots + a_\gamma x^\gamma$, the **tail** of $f$.

The most important distinction is between global and local orderings.

**Definition 1.2.4.** Let $>$ be a monomial ordering on $\{x^\alpha \mid \alpha \in \mathbb{N}^n\}$.

(1) $>$ is called a **global ordering** if $x^\alpha > 1$ for all $\alpha \neq (0, \ldots, 0)$,

(2) $>$ is called a **local ordering** if $x^\alpha < 1$ for all $\alpha \neq (0, \ldots, 0)$,

(3) $>$ is called a **mixed ordering** if it is neither global nor local.

Local and global (and mixed) orderings have quite different properties.

**Lemma 1.2.5.** *Let $>$ be a monomial ordering, then the following conditions are equivalent:*

*(1)* $>$ *is a well–ordering.*

*(2)* $x_i > 1$ *for* $i = 1, \ldots, n$.

*(3)* $x^\alpha > 1$ *for all* $\alpha \neq (0, \ldots, 0)$, *that is,* $>$ *is global.*

*(4)* $\alpha \geq_{nat} \beta$ *and* $\alpha \neq \beta$ *implies* $x^\alpha > x^\beta$.

*The last condition means that* $>$ *is a refinement of the natural partial ordering on* $\mathbb{N}^n$ *defined by*

$$(\alpha_1, \ldots, \alpha_n) \geq_{nat} (\beta_1, \ldots, \beta_n) :\Longleftrightarrow \alpha_i \geq \beta_i \text{ for all } i\,.$$

For the proof (which we leave as an exercise) one needs

**Lemma 1.2.6** (Dickson‘s Lemma)**.** *Let* $M \subset \mathbb{N}^n$ *be any subset. Then there is a* finite *set* $B \subset M$ *satisfying*

$$\forall\, \alpha \in M\; \exists\, \beta \in B \text{ such that } \beta \leq_{nat} \alpha\,.$$

*$B$ is sometimes called a* Dickson basis *of $M$.*

*Proof.* We write $\geq$ instead of $\geq_{\text{nat}}$ and use induction on $n$. For $n = 1$ we can take the minimum of $M$ as the only element of $B$.

For $n > 1$ and $i \in \mathbb{N}$ define

$$M_i = \{\alpha' = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{N}^{n-1} \mid (\alpha', i) \in M\}$$

and, by induction, $M_i$ has a Dickson basis $B_i$.

Again, by induction hypothesis, $\bigcup_{i\in\mathbb{N}} B_i$ has a Dickson basis $B'$. $B'$ is finite, hence $B' \subset B_1 \cup \cdots \cup B_s$ for some $s$.

We claim that

$$B := \{(\beta', i) \in \mathbb{N}^n \mid 0 \leq i \leq s,\ \beta' \in B_i\}$$

is a Dickson basis of $M$.

To see this, let $(\alpha', \alpha_n) \in M$. Then $\alpha' \in M_{\alpha_n}$ and, since $B_{\alpha_n}$ is a Dickson basis of $M_{\alpha_n}$, there is a $\beta' \in B_{\alpha_n}$ with $\beta' \leq \alpha'$. If $\alpha_n \leq s$, then $(\beta', \alpha_n) \in B$ and $(\beta', \alpha_n) \leq (\alpha', \alpha_n)$. If $\alpha_n > s$, we can find a $\gamma' \in B'$ and an $i \leq s$ such that $\gamma' \leq \beta'$ and $(\gamma', i) \in B_i$. Then $(\gamma', i) \in B$ and $(\gamma', i) \leq (\alpha', \alpha_n)$. ☐

*Example* 1.2.7 (the first two are global, the third is local).

(1) **lp** : $x^\alpha > x^\beta \Leftrightarrow \exists i : \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i$,
**lexicographical ordering (lex)**

(2) **dp** : $x^\alpha > x^\beta \Leftrightarrow |\alpha| > |\beta|$ or $|\alpha| = |\beta|$ and $\exists i : \alpha_i < \beta_i, \alpha_{i+1} = \beta_{i+1}, \ldots, \alpha_n = \beta_n$,
**degree reverse lexicographical ordering (degrevlex)**.

(3) **ds** : $x^\alpha > x^\beta \Leftrightarrow |\alpha| < |\beta|$ or $|\alpha| = |\beta|$ and $\exists i : \alpha_i < \beta_i, \alpha_{i+1} = \beta_{i+1}, \ldots, \alpha_n = \beta_n$,
**negative degree reverse lexicographical ordering**.
(mixed orderings will be considered later)

## 1.3 Ideal Operations

Ideals are in the centre of commutative algebra and algebraic geometry.
Let $A$ be a ring, as always, commutative and with 1.

**Definition 1.3.1.**

(1) A subset $I \subset A$ is called an **ideal** if it is an additive subgroup which is closed under scalar multiplication.

(2) A family $(f_\lambda)_{\lambda\in\Lambda}$, $\Lambda$ any index set, and $f_\lambda \in I$, is called a **system of generators** of $I$ if every element $f \in I$ can be expressed as a finite sum $f = \sum_\lambda a_\lambda f_\lambda$ for suitable $a_\lambda \in A$. If $\Lambda$ is finite, say $\Lambda = \{1, \dots, k\}$, we say that $I$ is **finitely generated** and we write

$$I = \langle f_1, \dots, f_k \rangle_A = \langle f_1, \dots, f_k \rangle .$$

(3) If $G \subset A[x] = A[x_1, \dots, x_n]$ is any set we denote by

- $L(G) = \langle \mathrm{LT}(g) \mid g \in G \rangle_{A[x]}$, the **leading term ideal** of G,
- $LM(G) = \langle \mathrm{LM}(g) \mid g \in G \rangle_{A[x]}$, the **leading monomial ideal** of G,

For $A = K$ a field, $L(G) = LM(G)$, and we have for $\lambda \in K \setminus \{0\}$

$$\lambda x^\alpha \in L(G) \iff x^\alpha \in L(G) \iff \exists\, g \in G : \mathrm{LM}(g) \mid x^\alpha.$$

Often ideals are not given by generators.
If $\varphi : A \to B$ is a ring homomorphism and $J \subset B$ an ideal, then the **preimage**

$$\varphi^{-1}(J) = \{a \in A \mid \varphi(a) \in J\}$$

is an ideal. In particular, the **kernel**

$$\operatorname{Ker} \varphi = \{a \in A \mid \varphi(a) = 0\}$$

is an ideal in $A$. On the other hand, the **image**

$$\operatorname{Im} \varphi = \varphi(I) = \{\varphi(a) \mid a \in I\}$$

is, in general, only an ideal if $\varphi$ is surjective.

*Note* 1.3.2. Preimages (hence kernels) can be effectively computed (i.e. a generating set can be computed) which is, however, not easy. Images are generated by the images of the generators (for surjective $\varphi$), hence the computation is trivial.

**Definition 1.3.3.** A ring $A$ is called **Noetherian** if every ideal in $A$ is finitely generated.

**Theorem 1.3.4** (Hilbert Basis Theorem)**.** *If $A$ is a Noetherian ring then the polynomial ring $A[x_1, \dots, x_n]$ is Noetherian. In particular, if $K$ is a field, then $K[x_1 \dots, x_n]$ is Noetherian.*

For the proof of the Hilbert basis theorem we use

**Proposition 1.3.5.** *The following properties of a ring $A$ are equivalent:*

(1) *$A$ is Noetherian.*

(2) *Every ascending chain of ideals*

$$I_1 \subset I_2 \subset I_3 \subset \ldots \subset I_k \subset \ldots$$

*becomes stationary (that is, there exists some $j_0$ such that $I_j = I_{j_0}$ for all $j \geq j_0$).*

(3) *Every non–empty set of ideals in $A$ has a maximal element (with regard to inclusion).*

Condition (2) is called the *ascending chain condition* and (3) the *maximality condition*. We leave the proof of this proposition as an exercise.

*Proof of Theorem 1.3.4.* We need to show the theorem only for $n = 1$, the general case follows by induction.

We argue by contradiction. Let us assume that there exists an ideal $I \subset A[x]$ which is not finitely generated. Choose polynomials

$$f_1 \in I, \quad f_2 \in I \setminus \langle f_1 \rangle, \quad \ldots, \quad f_{k+1} \in I \setminus \langle f_1, \ldots, f_k \rangle, \quad \ldots$$

of minimal possible degree. If $d_i = \deg(f_i)$,

$$f_i = a_i x^{d_i} + \text{ lower terms in } x\,,$$

then $d_1 \leq d_2 \leq \ldots$ and $\langle a_1 \rangle \subset \langle a_1, a_2 \rangle \subset \ldots$ is an ascending chain of ideals in $A$. By assumption it is stationary, that is, $\langle a_1, \ldots, a_k \rangle = \langle a_1, \ldots, a_{k+1} \rangle$ for some $k$, hence, $a_{k+1} = \sum_{i=1}^k b_i a_i$ for suitable $b_i \in A$. Consider the polynomial

$$g = f_{k+1} - \sum_{i=1}^k b_i x^{d_{k+1} - d_i} f_i = a_{k+1} x^{d_{k+1}} - \sum_{i=1}^k b_i a_i x^{d_{k+1}} + \text{ lower terms}\,.$$

Since $f_{k+1} \in I \setminus \langle f_1, \ldots, f_k \rangle$, it follows that $g \in I \setminus \langle f_1, \ldots, f_k \rangle$ is a polynomial of degree smaller than $d_{k+1}$, a contradiction to the choice of $f_{k+1}$. $\square$

**Definition 1.3.6.** For ideals $I, J \subset A$ we define:

(1) The **ideal quotient** of $I$ by $J$ is defined as

$$I : J := \{a \in A \mid aJ \subset I\}\,.$$

The **saturation of $I$ with respect to $J$** is

$$I : J^\infty = \{a \in A \mid \exists\, n \text{ such that } aJ^n \subset I\}\,.$$

(2) The **radical** of $I$, denoted by $\sqrt{I}$ or $\mathrm{rad}(I)$ is the ideal

$$\sqrt{I} = \{a \in A \mid \exists\, d \in \mathbb{N} \text{ such that } a^d \in I\}\,,$$

$I$ is called **reduced** or a **radical ideal** if $I = \sqrt{I}$.

(3) $a \in A$ is called **nilpotent** if $a^n = 0$ for some $n \in \mathbb{N}$; the minimal $n$ is called **index of nilpotency**. The set of nilpotent elements of $A$ is equal to $\sqrt{\langle 0 \rangle}$ and called the **nilradical** of $A$.

(4) $\langle 0 \rangle : J = \mathrm{Ann}_A(J)$ is the **annihilator** of $J$ and, hence, $\langle 0 \rangle : \langle f \rangle = \langle 0 \rangle$ if and only if $f$ is a non–zerodivisor of $A$.

*Note* 1.3.7. (Generators of) Ideal quotient, saturation, radical can be effectively computed.

SINGULAR commands:

| | |
|---|---|
| **quotient(I,J);** | (command in the SINGULAR kernel) |
| **sat(I,J);** | (procedure in `elmi.lib`) |
| **radical(I);** | (procedure in `primdec.lib`) |

## 1.4 Normal Forms and Gröbner Bases

Let $>$ be a fixed global monomial ordering on $\mathrm{Mon}(x_1, \ldots, x_n)$, $K$ a field and let

$$R = K[x_1, \ldots, x_n]$$

**Definition 1.4.1.** Let $I \subset R$ be an ideal. A finite set $G \subset R$ is called a **Gröbner basis** or **standard basis** of $I$ if

$$G \subset I, \text{ and } L(I) = L(G)\,.$$

Hence $G \subset I$ is a Gröbner basis, if for any $f \in I \smallsetminus \{0\}$ there exists a $g \in G$ satisfying $\mathrm{LM}(g) \mid \mathrm{LM}(f)$. We say $G$ is a Gröbner (standard) basis if it is a Gröbner (standard) basis of $\langle G \rangle_R$.

**Existence** of a Gröbner basis (**non-constructive**):
Choose a finite set of generators $m_1, \ldots, m_s$ of $L(I) \subset K[x]$, which exists, since $K[x]$ is Noetherian. These generators are leading monomials of suitable elements $g_1, \ldots, g_s \in I$. The set $\{g_1, \ldots, g_s\}$ is a standard basis for $I$.

**Definition 1.4.2.** Let $G \subset R$ be any subset.

(1) $G$ is called **interreduced** (or **minimal**) if $0 \notin G$ and if $\mathrm{LM}(g) \nmid \mathrm{LM}(f)$ for any two elements $f \neq g$ in $G$.

(2) $G$ is called **(completely) reduced** if $G$ is interreduced and if, for any $g \in G$, $\mathrm{LC}(g) = 1$ and no monomial of tail $(g)$ is divisible by any $\mathrm{LM}(f)$, $f \in G$.

- Every Gröbner basis $G$ can be transformed into an interreduced one by just deleting elements of $G$.
- We shall see later that reduced Gröbner bases can always be computed and are unique.

**Definition 1.4.3.** Let $G \subset R$ be a finite list. A map

$$\mathrm{NF} : R \to R,\ f \mapsto \mathrm{NF}(f \mid G)\,,$$

is called a **normal form** on $R$ with respect to $G$, if

(0) $\mathrm{NF}(0 \mid G) = 0\,,$

and, for all $f \in R$,

(1) $\mathrm{NF}(f \mid G) \neq 0 \Longrightarrow \mathrm{LM}\big(\mathrm{NF}(f \mid G)\big) \notin L(G)$.

(2) If $G = \{g_1, \ldots, g_s\}$, then $r := f - \mathrm{NF}(f \mid G)$ has a **standard representation**, that is the remainder

$$r = f - \mathrm{NF}(f \mid G) = \sum_{i=1}^{s} a_i g_i\,, \quad a_i \in R\,, \quad s \geq 0\,,$$

satisfies $\mathrm{LM}(r) \geq \mathrm{LM}(a_i g_i)$ for all $i$ such that $a_i g_i \neq 0$.

NF is called a **reduced normal form**, if, moreover, $\mathrm{NF}(f \mid G)$ has leading coefficient 1 and no monomial of its tail is divisible by $\mathrm{LM}(g), g \in G$.

**Lemma 1.4.4.** *Let $I \subset R$ be an ideal, $G \subset I$ a standard basis of $I$ and $\mathrm{NF}(- \mid G)$ a normal form on $R$ with respect to $G$.*

*(1) For any $f \in R$ we have $f \in I$ if and only if $\mathrm{NF}(f \mid G) = 0$.*

*(2) If $J \subset R$ is an ideal with $I \subset J$, then $L(I) = L(J)$ implies $I = J$.*

*(3) $I = \langle G \rangle_R$, that is, the standard basis $G$ generates $I$ as $R$–ideal.*

*(4) If $\mathrm{NF}(- \mid G)$ is a reduced normal form, then it is unique (i.e. depends only on $G$ and on $>$).*

*Proof.* (1) If $\mathrm{NF}(f \mid G) = 0$ then $uf \in I$ and, hence, $f \in I$. If $\mathrm{NF}(f \mid G) \neq 0$, then $\mathrm{LM}\big(\mathrm{NF}(f \mid G)\big) \notin L(G) = L(I)$, hence $\mathrm{NF}(f \mid G) \notin I$, which implies $f \notin I$, since $\langle G \rangle_R \subset I$. To prove (2), let $f \in J$ and assume that $\mathrm{NF}(f \mid G) \neq 0$.
Then $\mathrm{LM}\big(\mathrm{NF}(f \mid G)\big) \notin L(G) = L(I) = L(J)$, contradicting
$\mathrm{NF}(f \mid G) \in J$.
Hence, $f \in I$ by (1).

(3) follows from (2), since $L(I) = L(G) \subset L(\langle G \rangle_R) \subset L(I)$, in particular, $G$ is also a standard basis of $\langle G \rangle_R$. Finally, to prove (4), let $f \in R$ and assume that $h, h'$ are two reduced normal forms of $f$ with respect to $G$. Then no monomial of the power series expansion of $h$ or $h'$ is divisible by any monomial of $L(G)$ and, moreover, $h - h' = (f - h') - (f - h) \in \langle G \rangle_R = I$.

If $h - h' \neq 0$, then $\mathrm{LM}(h - h') \in L(I) = L(G)$, a contradiction, since $\mathrm{LM}(h - h')$ is a monomial of either $h$ or $h'$. $\square$

**Definition 1.4.5.** Let $f, g \in R \smallsetminus \{0\}$ with $\mathrm{LM}(f) = x^\alpha$ and $\mathrm{LM}(g) = x^\beta$. Set

$$\gamma := \mathrm{lcm}(\alpha, \beta) := \big(\max(\alpha_1, \beta_1), \ldots, \max(\alpha_n, \beta_n)\big)$$

and let $\mathrm{lcm}(x^\alpha, x^\beta) := x^\gamma$ be the **least common multiple** of $x^\alpha$ and $x^\beta$. The $s$–**polynomial** (**spoly**, for short) of $f$ and $g$ is

$$\mathrm{spoly}(f, g) := x^{\gamma - \alpha} f - \frac{\mathrm{LC}(f)}{\mathrm{LC}(g)} \cdot x^{\gamma - \beta} g\,.$$

If $\mathrm{LM}(g)$ divides $\mathrm{LM}(f)$, say $\mathrm{LM}(g) = x^\beta$, $\mathrm{LM}(f) = x^\alpha$, then the $s$–polynomial is particularly simple,

$$\mathrm{spoly}(f, g) = f - \frac{\mathrm{LC}(f)}{\mathrm{LC}(g)} \cdot x^{\alpha-\beta} g\,,$$

and $\mathrm{LM}\big(\mathrm{spoly}(f, g)\big) < \mathrm{LM}(f)$. We use in this case the notation

$$f \xrightarrow[g]{} h \;\text{ if }\; h = \mathrm{spoly}(f, g).$$

**Algorithm 1.4.6** (NFBuchberger($f \mid G$))**.** Assume that $>$ is a global monomial ordering.

Input: $f \in K[x]$, $G \in \mathcal{G}$, where $\mathcal{G}$ denotes the class of finite lists.

Output: $h \in K[x]$, a normal form of $f$ with respect to $G$.

- $h := f$;
- while ($h \neq 0$ and $G_h := \{g \in G \mid \mathrm{LM}(g)$ divides $\mathrm{LM}(h)\} \neq \emptyset$)
  choose any $g \in G_h$;
  $h := \mathrm{spoly}(h, g)$;
- return $h$;

Note that each specific choice of "any" can give a different normal form function.

**Algorithm 1.4.7** (redNFBuchberger($f \mid G$))**.** Assume that $>$ is a global monomial ordering.

Input: $f \in K[x]$, $G \in \mathcal{G}$

Output: $h \in K[x]$, a reduced normal form of $f$ with respect to $G$

- $h := 0$, $g := f$;
- while ($g \neq 0$)
  $g :=$ NFBuchberger ($g \mid G$);
  if ($g \neq 0$)
    $h := h + \mathrm{LT}(g)$;
    $g := \mathrm{tail}(g)$;
- return $h/\mathrm{LC}(h)$;

*Example* 1.4.8. Let $>$ be the ordering `dp` on $\mathrm{Mon}(x, y, z)$,

$$f = x^3 + y^2 + 2z^2 + x + y + 1\,, \quad G = \{x^2, y + z\}\,.$$

NFBuchberger proceeds as follows:

$\mathrm{LM}(f) = x^3,\ G_f = \{x^2\}$,

$h_1 = \mathrm{spoly}(f, x^2) = y^2 + 2z^2 + x + y + 1$, ($f \underset{x^2}{\longrightarrow} h_1$);

$\mathrm{LM}(h_1) = y^2,\ G_{h_1} = \{y + z\}$,

$h_2 = \mathrm{spoly}(h_1, y + z) = -yz + 2z^2 + x + y + 1$, ($h_1 \underset{y+z}{\longrightarrow} h_2$);

$\mathrm{LM}(h_2) = yz,\ G_{h_2} = \{y + z\}$,

$h_3 = \mathrm{spoly}(h_2, y + z) = 3z^2 + x + y + 1$, ($h_2 \underset{y+z}{\longrightarrow} h_3$); $G_{h_3} = \emptyset$.

Hence, $\mathrm{NF}\textsc{Buchberger}(f \mid G) = \underline{3z^2} + x + y + 1$.

To have shorthand notation we underline the leading terms and then the reduced normal form acts as

$$f \longrightarrow \mathrm{NF}(f \mid G) = \underline{3z^2}+x+y+1 \underset{y+z}{\longrightarrow} \underline{3z^2}+x-z+1 \longrightarrow \underbrace{\underline{z^2}+\frac{1}{3}x-\frac{1}{3}z+\frac{1}{3}}_{=\mathrm{RedNF}(f|G)}.$$

## 1.5 Gröbner Basis Algorithm

Let $>$ be a fixed global monomial ordering and let $R = K[x_1, \ldots, x_n]$. Let $\mathcal{G}$ be the class of finite lists (a list is a sequence).

**Algorithm 1.5.1** (Gröbner(G,NF))**.**

Input: $G \in \mathcal{G}$, NF an algorithm returning a normal form.

Output: $S \in \mathcal{G}$ such that $S$ is a Gröbner basis of $I = \langle G \rangle_R \subset R$

- $S := G$;
- $P := \{(f, g) \mid f, g \in S, f \neq g\}$, the pair–set;
- while ($P \neq \emptyset$)
  choose $(f, g) \in P$;
  $P := P \setminus \{(f, g)\}$;
  $h := \mathrm{NF}\big(\mathrm{spoly}(f, g) \mid S\big)$;
  if ($h \neq 0$)
    $P := P \cup \{(h, f) \mid f \in S\}$;
    $S := S \cup \{h\}$;
- return $S$;

Termination of Gröbner: if $h \neq 0$ then $\mathrm{LM}(h) \notin L(S)$ by property (i) of NF. Hence, we obtain a strictly increasing sequence of monomial ideals $L(S)$ of $K[x]$, which becomes stationary as $K[x]$ is Noetherian. That is, after finitely many steps, we always have $\mathrm{NF}\big(\mathrm{spoly}(f, g) \mid S\big) = 0$ for $(f, g) \in P$, and, again after finitely many steps, the pair-set $P$ will become empty. Correctness follows from applying Buchberger's fundamental standard basis criterion below.

**Theorem 1.5.2** (Buchberger's criterion). *Let $I \subset R$ be an ideal and $G = \{g_1, \ldots, g_s\} \subset I$. Let $\mathrm{NF}(- \mid G)$ be a normal form on $R$ with respect to $G$. Then the following are equivalent:*[1]

*(1) $G$ is a standard basis of $I$.*

*(2) $\mathrm{NF}(f \mid G) = 0$ for all $f \in I$.*

*(3) Each $f \in I$ has a standard representation with respect to $\mathrm{NF}(- \mid G)$.*

*(4) $G$ generates $I$ and $\mathrm{NF}\big(\mathrm{spoly}(g_i, g_j) \mid G\big) = 0$ for $i, j = 1, \ldots, s$.*

*Example* 1.5.3. Let $>$ be the ordering `dp` on $\mathrm{Mon}(x, y)$, $f_1 = \underline{x^3} + y^2$, $f_2 = \underline{xyz} - y^2$ (underline leading terms), $G = \{f_1, f_2\}$, NF=NFBUCHBERGER.
GRÖBNER($G$,NF) works as follows:

$S = \{f_1, f_2\}$, $P = \{(f_1, f_2)\}$

The while–loop gives, in the first run:

$(f_1, f_2)$:

$P = \emptyset$

$\mathrm{spoly}(f_1, f_2) = yzf_1 - x^2 f_2 = y^3 z + \underline{x^2 y^2} =: f_3 = \mathrm{NF}(f_3, S)$

$P = \{(f_1, f_3), (f_2, f_3)\}$

$S = \{f_1, f_2, f_3\}$

In the second run:

$(f_1, f_3)$:

$P = \{(f_2, f_3)\}$

$\mathrm{spoly}(f_1, f_3) = y^2 f_1 - x f_3 = y^4 - \underline{xy^3 z} \underset{f_2}{\longrightarrow} 0$

In the third run:

$(f_2, f_3)$:

$P = \emptyset$

$\mathrm{spoly}(f_2, f_3) = xyf_2 - zf_3 = -xy^3 - \underline{y^3 z^2} =: f_4 = \mathrm{NF}(f_4, S)$

$P = \{\cancel{(f_1, f_4)}, (f_2, f_4), (f_3, f_4)\}$

(<u>Note</u>: $\mathrm{spoly}(f_1, f_4) \underset{\{f_1, f_4\}}{\longrightarrow} 0$ by the **product criterion**, since

$\mathrm{LM}(f_1) = x^3$ and $\mathrm{LM}(f_4) = y^3 z^2$ have no common divisor.)

$S = \{f_1, f_2, f_3, f_4\}$

In the fourth run:

$(f_2, f_4)$:

$P = \{(f_3, f_4)\}$

$\mathrm{spoly}(f_2, f_4) = -y^4 z - \underline{x^2 y^3} \underset{f_3}{\longrightarrow} 0$

In the fifth run:

$(f_3, f_4)$:

$P = \emptyset$

$\mathrm{spoly}(f_3, f_4) = \underline{y^4 z^3} - x^3 y^3 \underset{f_4}{\longrightarrow} -\underline{x^3 y^3} - xy^4 z \underset{f_1}{\longrightarrow} -\underline{xy^4 z} + y^5 \underset{f_2}{\longrightarrow} 0$

return$\{f_1, f_2, f_3, f_4\}$, a Gröbner basis of $\langle f_1, f_2 \rangle_R$.

[1] Usually, the implication (4) $\Rightarrow$ (1) is called Buchberger's criterion.

# 2 Constructive Ideal and Module Theory

## 2.1 Operations on Ideals and their Computation

### 2.1.1 Ideal Membership

**Problem:** Given $f, f_1, \dots, f_k \in K[x]$, and let $I = \langle f_1, \dots, f_k \rangle$. Decide whether $f \in I$, or not.

**Solution:** Choose any global monomial ordering $>$ and compute a standard basis $G = \{g_1, \dots, g_s\}$ of $I$. Then $f \in I$ if and only if $\mathrm{NF}(f \mid G) = 0$.

### 2.1.2 Intersection with Subrings (Elimination of variables)

This is one of the most important applications of Gröbner bases.

**Problem:** Given $f_1, \dots, f_k \in K[x] = K[x_1, \dots, x_n]$, $I = \langle f_1, \dots, f_k \rangle_{K[x]}$, find generators of the ideal

$$I' = I \cap K[x_{s+1}, \dots, x_n], \quad s < n\,.$$

Elements of $I'$ are said to be obtained from $I$ by **eliminating** $x_1, \dots, x_s$.
$>$ is called an **elimination ordering** for $x_1, \dots x_s$ if for all $f \in K[x_1, \dots, x_n]$

$$\mathrm{LM}(f) \in K[x_{s+1}, \dots, x_n] \Rightarrow f \in K[x_{s+1}, \dots, x_n]$$

(e.g.: lex or product orderings).

**Solution:** Choose an elimination ordering for $x_1, \dots, x_s$ on $\mathrm{Mon}(x_1, \dots, x_n)$, and compute a standard basis $S = \{g_1, \dots, g_k\}$ of $I$. Those $g_i$, for which $\mathrm{LM}(g_i)$ does not involve $x_1, \dots, x_s$, generate $I'$.
Even more, they are a standard basis of $I'$. This follows from the following Lemma.

**Lemma 2.1.1.** *Let $>$ be an elimination ordering for $x_1, \dots, x_s$ on $\mathrm{Mon}(x_1, \dots, x_n)$, and let $I \subset K[x_1, \dots, x_n]_>$ be an ideal. If $S = \{g_1, \dots, g_k\}$ is a standard basis of $I$, then*

$$S' := \{g \in S \mid \mathrm{LM}(g) \in K[x_{s+1}, \dots, x_n]\}$$

*is a standard basis of $I' := I \cap K[x_{s+1}, \dots, x_n]_{>'}$. In particular, $S'$ generates the ideal $I'$.*

*Proof.* Given $f \in I' \subset I$ there exists $g_i \in S$ such that $\mathrm{LM}(g_i)$ divides $\mathrm{LM}(f)$, since $S$ is a standard basis of $I$. Since $f \in K[x_{s+1}, \dots, x_n]$, we have $\mathrm{LM}(f) \in K[x_{s+1}, \dots, x_n]$ and, hence, $g_i \in S'$. Since $>$ is an elimination ordering $S' \subset I'$. Hence $S'$ is a standard basis of $I'$. □

## 2.2 Gröbner Bases for Modules

**Definition 2.2.1.** Let $A$ be a ring. A set $M$ with two maps, an addition, $+ : M \times M \longrightarrow M$ and a scalar multiplication, $\cdot : A \times M \longrightarrow M$ is called an **$A$-module** if $(M, +)$ is an abelian group and $+$ and $\cdot$ satisfy

- $(a+b)\cdot m = a\cdot m + b\cdot m$
- $a\cdot(m+n) = a\cdot m + a\cdot n$
- $(a\cdot b)\cdot m = a\cdot(b\cdot m)$
- $1\cdot m = m$

for all $a, b \in A$, $m, n \in M$.
For $r > 0$, $A^r$ with componentwise $+$ and $\cdot$ is an $A$-module which is Noetherian if $A$ is Noetherian.

More generally, we have

**Lemma 2.2.2.** *Let $M$ be an $A$-module and $N \subset M$ a submodule.*

*(1) $M$ is Noetherian $\Longleftrightarrow$ $N$ and the factor module $M/N$ are Noetherian*

*(2) If $A$ is Noetherian, then $M$ is Noetherian iff $M$ is finitely generated.*

*Proof.* For the proof see e.g. [GP]. $\square$

We have to extend the notion of monomial orderings to the free module $K[x]^r = \bigoplus_{i=1}^r K[x]e_i$, $e_i = (0,\ldots,1,\ldots,0) \in K[x]^r$, where $K$ is a field.
We call

$$x^\alpha e_i = (0,\ldots,x^\alpha,\ldots,0) \in K[x]^r$$

a **monomial (involving component $i$)**.

**Definition 2.2.3.** Let $>$ be a monomial ordering on $K[x]$. A **(module) monomial ordering** or a **module ordering** on $K[x]^r$ is a total ordering $>_m$ on the set of **monomials** $\{x^\alpha e_i \mid \alpha \in \mathbb{N}^n, i = 1,\ldots,r\}$, which is compatible with the $K[x]$–module structure including the ordering $>$, that is, satisfying

(1) $x^\alpha e_i >_m x^\beta e_j \Longrightarrow x^{\alpha+\gamma} e_i >_m x^{\beta+\gamma} e_j$,

(2) $x^\alpha > x^\beta \Longrightarrow x^\alpha e_i >_m x^\beta e_i$

for all $\alpha, \beta, \gamma \in \mathbb{N}^n$, $i, j = 1,\ldots,r$.

Two module orderings are of particular interest:

$$x^\alpha e_i > x^\beta e_j :\Longleftrightarrow i < j \text{ or } (i = j \text{ and } x^\alpha > x^\beta)\,,$$

giving **priority to the components**, denoted by **(c,$>$)**, and

$$x^\alpha e_i > x^\beta e_j :\Longleftrightarrow x^\alpha > x^\beta \text{ or } (x^\alpha = x^\beta \text{ and } i < j)\,,$$

which gives **priority to the monomials** in $K[x]$, denoted by **($>$,c)**.

Fix a module ordering $>_m$ and denote it also with $>$. Any vector $f \in K[x]^r \smallsetminus \{0\}$ can be written uniquely as

$$f = cx^\alpha e_i + f^*$$

with $c \in K \smallsetminus \{0\}$ and $x^\alpha e_i > x^{\alpha^*} e_j$ for any non–zero term $c^* x^{\alpha^*} e_j$ of $f^*$: We define as before

$$
\begin{aligned}
\mathrm{LM}(f) &:= x^\alpha e_i\,, && \textbf{leading monomial}\\
\mathrm{LC}(f) &:= c\,, && \textbf{leading coefficient}\\
\mathrm{LT}(f) &:= cx^\alpha e_i, && \textbf{leading term}\\
\mathrm{tail}(f) &:= f^* && \textbf{tail}
\end{aligned}
$$

For $I \subset K[x]^r$ a submodule we call

$$L_>(I) := L(I) := \langle\, \mathrm{LT}(g) \mid g \in I \smallsetminus \{0\}\,\rangle_{K[x]} \subset K[x]^r$$

the **leading module** of $\langle I\rangle_K$ (which coincides with $LM(I) = \langle \mathrm{LM}(g) \mid g \in I \setminus \{0\}\rangle_{K[x]}$ since $K$ is a field).

The set of monomials of $K[x]^r$ may be identified with $\mathbb{N}^n \times E^r \subset \mathbb{N}^n \times \mathbb{N}^r = \mathbb{N}^{n+r}$, $E^r = \{e_1, \ldots, e_r\}$.

We say that $x^\beta e_j$ is **divisible by** $x^\alpha e_i$ if $i = j$ and $x^\alpha \mid x^\beta$.
Let $>$ be a fixed global monomial ordering. Again we write

$$R := K[x] = K[x_1, \ldots, x_n].$$

**Definition 2.2.4.** Let $I \subset R^r$ be a submodule. A finite set $G \subset I$ is called a **Gröbner** or **standard basis** of $I$ if and only if $L(G) = L(I)$, that is, for any $f \in I \smallsetminus \{0\}$ there exists a $g \in G$ satisfying $\mathrm{LM}(g) \mid \mathrm{LM}(f)$.

The notion of **minimal** and **reduced Gröbner basis** is the same as for ideals. Also the definitions of **normal form** and of **s–polynomial**.

The normal form algorithm and **Buchberger's Gröbner basis algorithm** extend easily to submodules $I \subset R^r$.

## 2.3 Exact Sequences and free Resolutions

**Definition 2.3.1.** A sequence of $A$–modules and homomorphisms

$$\cdots \to M_{k+1} \xrightarrow{\varphi_{k+1}} M_k \xrightarrow{\varphi_k} M_{k-1} \to \cdots$$

is called a **complex** if $\mathrm{Ker}(\varphi_k) \subset \mathrm{Im}(\varphi_{k+1})$. It is called **exact at** $M_k$ if

$$\mathrm{Ker}(\varphi_k) = \mathrm{Im}(\varphi_{k+1})\,.$$

It is called **exact** if it is exact at all $M_k$. An exact sequence

$$0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$$

is called a **short exact sequence**.

**Definition 2.3.2.** Let $A$ be a ring and $M$ a finitely generated $A$–module. A **free resolution** of $M$ is an exact sequence

$$\ldots \longrightarrow F_{k+1} \xrightarrow{\varphi_{k+1}} F_k \longrightarrow \ldots \longrightarrow F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \to 0$$

with finitely generated free $A$–modules $F_i$ for $i \geq 0$.

Frequently the complex of free $A$-modules (without $M$)

$$F_\bullet : \ \ldots \longrightarrow F_{k+1} \xrightarrow{\varphi_{k+1}} F_k \longrightarrow \ldots \longrightarrow F_1 \xrightarrow{\varphi_1} F_0 \longrightarrow 0$$

is called a free resolution of $M$.
A free resolution has **(finite) length** $n$ if $F_k = 0$ for all $k > n$ and $n$ is minimal with this property.

## 2.4 Computing Resolutions and the Syzygy Theorem

In the following definition $R$ can be an arbitrary ring.

**Definition 2.4.1.** A **syzygy** or **relation** between $k$ elements $f_1, \dots, f_k$ of an $R$–module $M$ is a $k$–tuple $(g_1, \dots, g_k) \in R^k$ satisfying

$$\sum_{i=1}^{k} g_i f_i = 0\,.$$

The set of all syzygies between $f_1, \dots, f_k$ is a submodule of $R^k$, it is the kernel of the ring homomorphism

$$\varphi : F_1 := \bigoplus_{i=1}^{k} R\varepsilon_i \longrightarrow M\,, \quad \varepsilon_i \longmapsto f_i\,,$$

where $\{\varepsilon_1, \dots, \varepsilon_k\}$ denotes the canonical basis of $R^k$. $\varphi$ surjects onto the $R$–module $I := \langle f_1, \dots, f_k\rangle_R$ and

$$\mathrm{syz}(I) := \mathrm{syz}(f_1, \dots, f_k) := \mathrm{Ker}(\varphi)$$

is called the **module of syzygies** of $I$ with respect to the generators $f_1, \dots, f_k$.

**Theorem 2.4.2** (Hilbert's Syzygy Theorem). *Let $R = K[x_1, \dots, x_n]$. Then any finitely generated $R$–module $M$ has a free resolution*

$$0 \to F_m \to F_{m-1} \to \cdots \to F_0 \to M \to 0$$

*of length $m \leq n$, where the $F_i$ are free $R$–modules.*

*Proof.* For the proof we refer to [GP]. □

**Algorithm 2.4.3** ($\textsc{syz}(f_1, \dots, f_k)$)**.** Let $>$ be any monomial ordering on $\mathrm{Mon}(x_1, \dots, x_n)$ and $R = K[x]$.

Input: $f_1, \dots, f_k \in K[x]^r$.

Output: $S = \{s_1, \dots, s_\ell\} \subset K[x]^k$ such that $\langle S\rangle = \mathrm{syz}(f_1, \dots, f_k) \subset R^k$.

- $F := \{f_1 + e_{r+1}, \dots, f_k + e_{r+k}\}$, where $e_1, \dots, e_{r+k}$ denote the canonical generators of $R^{r+k} = R^r \oplus R^k$ such that $f_1, \dots, f_k \in R^r = \bigoplus_{i=1}^{r} Re_i$;
- compute a standard basis $G$ of $\langle F\rangle \subset R^{r+k}$ with respect to $(c, >)$;
- $G_0 := G \cap \bigoplus_{i=r+1}^{r+k} Re_i = \{g_1, \dots, g_\ell\}$, with $g_i = \sum_{j=1}^{k} a_{ij} e_{r+j}$, $i = 1, \dots, \ell$;
- $s_i := (a_{i1}, \dots a_{ik})$, $i = 1, \dots, \ell$;
- return $S = \{s_1, \dots, s_\ell\}$.

**Algorithm 2.4.4** ($\textsc{Resolution}(I, m)$)**.** Let $>$ be a global monomial ordering on $\mathrm{Mon}(x_1, \dots, x_n)$ and $R = K[x]$.

Input: $f_1, \ldots, f_k \in K[x]^r$, $I = \langle f_1, \ldots, f_k \rangle \subset R^r$, and $m$ a positive integer.

Output: A list of matrices $A_1, \ldots, A_m$ with $A_i \in \mathrm{Mat}(r_{i-1} \times r_i, K[x])$, $i = 1, \ldots, m$, such that

$$\ldots \longrightarrow R^{r_m} \xrightarrow{A_m} R^{r_{m-1}} \longrightarrow \ldots \longrightarrow R^{r_1} \xrightarrow{A_1} R^r \longrightarrow R^r/I \longrightarrow 0$$

is the beginning of a free resolution of $R^r/I$.

- $i := 1$;
- $A_1 := \mathrm{matrix}(f_1, \ldots, f_k) \in \mathrm{Mat}(r \times k, K[x])$;
- while $(i < m)$
  $i := i + 1$;
  $A_i := \mathrm{syz}(A_{i-1})$;
- return $A_1, \ldots, A_m$.

## 2.5 Operations on Modules and their Computation

Let $K$ be a field, $>$ a global monomial ordering on $K[x]$, $x = (x_1, \ldots, x_n)$, and $R = K[x]$.

The **module membership problem** can be formulated as follows:
**Problem:** Given polynomial vectors $f, f_1, \ldots, f_k \in K[x]^r$, decide whether

$$f \in I := \langle f_1, \ldots, f_k \rangle \subset R^r$$

or not.

**Solution:** Compute a standard basis $G = \{g_1, \ldots, g_s\}$ of $I$ with respect to $>_m$ and choose a normal form NF on $R^r$. Then

$$f \in I \iff \mathrm{NF}(f \mid G) = 0\,.$$

**Additional Problem:** If $f \in I = \langle f_1, \ldots, f_r \rangle \subset R^r$ then express $f$ as a linear combination $f = \sum_{i=1}^k g_i f_i$ with $g_i \in K[x]$.

**Solution:** Compute a standard basis $G$ of $\mathrm{syz}(f, f_1, \ldots, f_k) \subset R^{k+1}$ w.r.t. the ordering $(c, >)$. Now choose any vector $h = (1, -g_1, \ldots, -g_k) \in G$. Then $f = \sum_{i=1}^k g_i f_i$.

**Intersection with Free Submodules (Elimination of Module Components)** Let $R^r = \bigoplus_{i=1}^r Re_i$, where $\{e_1, \ldots, e_r\}$ denotes the canonical basis of $R^r$, $R = K[x]$.
**Problem:** Given $f_1, \ldots, f_k \in R^r$, $I = \langle f_1, \ldots, f_k \rangle \subset R^r$, find a (polynomial) system of generators for the submodule

$$I' := I \cap \bigoplus_{i=s+1}^{r} Re_i\,.$$

Elements of the submodule $I'$ are said to be obtained from $f_1, \dots, f_k$ **by eliminating** $e_1, \dots, e_s$.

**Solution:** Compute a standard basis $G = \{g_1, \dots, g_s\}$
of $I$ w.r.t. $(c, >)$. Then

$$G' := \left\{ g \in G \;\middle|\; \mathrm{LM}(g) \in \bigoplus_{i=s+1}^{r} K[x]e_i \right\}$$

is a standard basis for $I'$.

# 3 Constructive Normalization of Affine Rings

## 3.1 Integral Closure of Rings and Ideals

Let $K$ be a perfect field (e.g. $\mathrm{char}(K) = 0$ or $K$ finite) and $A = K[x_1, \dots, x_n]/\langle f_1, \dots, f_k\rangle$ reduced (i.e. if $a \in A$ and $a^p = 0$ for some $p > 0$ then $a = 0$).

We describe algorithms to compute

- the **normalisation** $\overline{A}$ of $A$, that is, the integral closure of $A$ in the total ring of fractions $Q(A)$,
- an ideal $I_N \subset A$ describing the **non-normal locus**, that is,

$$V(I_N) = N(A) := \{P \in \operatorname{Spec} A \mid A_P \text{ is not normal}\},$$

We can also compute for any ideal $I \subset A$, the integral closure $\overline{I}$ of $I$ in $A$ (cf. [GP]).

**Definition 3.1.1.** For any ring $A$ we define the **total ring of fractions** $Q(A)$ as the **localization of** $A$ w.r.t. the **multiplicatively closed** set $S = \{s \in A \mid sa = 0 \Rightarrow a = 0 \,\forall\, a \in A\}$ of **non-zero divisors** of $A$. That is

$$Q(A) = \{\frac{a}{s} \mid s \in S,\, a \in A\}$$

with usual $+$ and $\cdot$ of fractions. where $\frac{a}{s}$ is the equivalence class of pairs $(a, s)$ with $(a, s) \sim (a', s')$ iff $as' = a's$. $(Q(A), +, \cdot)$ is a ring; if $A$ is a **domain** (i.e. $S = A \setminus \{0\}$), then $Q(A)$ is a field, the **field of fractions** of $A$.

## 3.2 Key-Lemma

**Definition 3.2.1.** $b \in Q(A)$ is **integral** over $A$ if it satisfies a relation

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0\,, \quad a_i \in A\,.$$

We define the **normalisation** of $A$ as $\overline{A} := \{b \in Q(A) \mid b \text{ is integral over } A\}$, that is, $\overline{A}$ is the **integral closure** of $A$ in $Q(A)$.

**Lemma 3.2.2** (Key-lemma)**.** *Let $J \subset A$ be an ideal, containing a non-zerodivisor $f$ of $A$. Then*

$$A \subset \operatorname{Hom}_A(J, J) \subset \operatorname{Hom}_A(J, A) \cap \overline{A} \subset \operatorname{Hom}_A(J, \sqrt{J})$$

*with*

$$\operatorname{Hom}_A(J, A) \xrightarrow{\cong} \{h \in Q(A) \mid hJ \subset A\} \subset Q(A)\,, \quad \varphi \longmapsto \tfrac{\varphi(f)}{f}\,.$$

*Remark* 3.2.3.

(1) By the Cayley-Hamilton theorem, the characteristic polynomial of $\varphi$ defines an integral relation of $\varphi \in \operatorname{Hom}_A(J, J)$.

(2) $\operatorname{Hom}_A(J, J) \cong \frac{1}{f}(fJ : J) \subset \bar{A}$.

*Proof.* For the proof we refer to [GP], Lemma 3.6.1. and Lemma 3.6.4. ∎

## 3.3 A Criterion for Normality

The following criterion is basically due to Grauert and Remmert (1971).

**Proposition 3.3.1** (Criterion for normality)**.** *Let $A$ be a reduced Noetherian ring and $J \subset A$ an ideal satisfying*

*(1) $J$ contains a non-zerodivisor of $A$,*

*(2) $J = \sqrt{J}$,*

*(3) $V(J) \supset N(A) = V(C), \quad C = \mathrm{Ann}_A(\overline{A}/A)$.*

*Then*

$$A = \overline{A} \iff A = \mathrm{Hom}_A(J, J).$$

*An ideal $J$ with (1), (2), (3) is called* test ideal *for the normalization.*

*Proof.* "$\Longleftarrow$" (3) $\Rightarrow$ $\exists\, d \geq 0$ minimal s.th. $\overline{A}J^d \subset A$.

$$\begin{aligned} &\text{Assume } d > 0 \\ &\Rightarrow\ \exists\, h \in \overline{A},\ a \in J^{d-1} : ha \notin A,\ \ haJ \subset hJ^d \subset \overline{A}J^d \subset A \\ &\qquad\Rightarrow\ ha \in \overline{A} \cap \mathrm{Hom}_A(J, A) = \underbrace{\mathrm{Hom}_A(J, J)}_{= A} \quad \text{(key-lemma)} \end{aligned}$$

That is a contradiction and we conclude that $d = 0$ and thus $A = \overline{A}$. $\square$

## 3.4 Test Ideals

Let $R = K[x_1, \ldots, x_n]$, $A = R/I$ reduced, $I = \langle f_1, \ldots, f_k \rangle$, $K$ a perfect field. Let

$$\mathrm{Sing}(A) = \{P \in \mathrm{Spec}\, A \mid A_P \text{ is not regular}\}$$

be the **singular locus** of $A$. We have $N(A) \subset \mathrm{Sing}(A)$.

If $A$ is equidimensional of codimension $c$, then the **Jacobian ideal**

$$J = \left\langle f_1, \ldots, f_k,\ c\text{-minors of } \left(\frac{\partial f_i}{\partial x_j}\right) \right\rangle$$

defines $\mathrm{Sing}(A)$.

In general, we can use an **equidimensional** or **primary decomposition** to compute an ideal $J$ s.th. $V(J) = \mathrm{Sing}(A)$. Since $A$ is reduced, $J$ contains a non-zerodivisor of $A$.

Hence we can compute test ideals as follows (all steps are effective):

- compute $J$ such that $V(J) = \mathrm{Sing}(A)$
- compute $\sqrt{J}$

Then $\sqrt{J}$ is a test ideal for the normalization. Note that we can as well compute any ideal $J' \subset J$ containing a non-zero divisor, then $\sqrt{J'}$ is also a test ideal.

## 3.5 Algorithm to Compute the Normalization

The idea of the algorithm is to compute the endomorphism ring $A^{(1)} = \mathrm{Hom}_A(J,J)$ for some test ideal $J \subset A$. If $A = A^{(1)}$ then $A$ is already normal by Proposition 3.3.1. If not, we compute $A^{(2)} = \mathrm{Hom}_{A^{(1)}}(J^{(1)}, J^{(1)})$ for a test ideal $J^{(1)} \subset A^{(1)}$. If $A^{(1)} = A^{(2)}$ then $\overline{A} = A^{(1)}$, otherwise we continue in the same way to obtain a sequence of rings

$$A \subset A^{(1)} \subset \ldots \subset A^{(i)} \subset \ldots \subset \overline{A}.$$

The process must stop since $A$ is affine, by a theorem of M. Noether. In order to do the computations effectively, we must present $A^{(i)}$ as affine ring. This is described in the following lemma.

**Lemma 3.5.1.** *Let $A$ be a reduced Noetherian ring, let $J \subset A$ be an ideal and $x \in J$ a non–zerodivisor. Then*

*(1) $A = \mathrm{Hom}_A(J,J)$ if and only if $xJ : J = \langle x \rangle$.*

*Moreover, let $\{u_0 = x,\, u_1, \ldots, u_s\}$ be a system of generators for the $A$–module $xJ : J$. Then we can write*

*(2) $u_i \cdot u_j = \sum_{k=0}^{s} x\xi_k^{ij} u_k$ with suitable $\xi_k^{ij} \in A$, $1 \le i \le j \le s$.*

*Let $(\eta_0^{(k)}, \ldots, \eta_s^{(k)}) \in A^{s+1}$, $k = 1, \ldots, m$, generate the syzygy module $\mathrm{syz}(u_0, \ldots, u_s)$, and let $I \subset A[t_1, \ldots, t_s]$ be the ideal*

$$I := \left\langle \left\{ t_i t_j - \sum_{k=0}^{s} \xi_k^{ij} t_k \;\middle|\; 1 \le i \le j \le s \right\},\ \left\{ \sum_{\nu=0}^{s} \eta_\nu^{(k)} t_\nu \;\middle|\; 1 \le k \le m \right\} \right\rangle,$$

*where $t_0 := 1$. Then*

*(3) $t_i \mapsto u_i/x$, $i = 1, \ldots, s$, defines an isomorphism*

$$A[t_1, \ldots, t_s]/I \xrightarrow{\cong} \mathrm{Hom}_A(J,J) \cong \frac{1}{x} \cdot (xJ : J)\,.$$

*Proof.* (1) follows immediately from Remark 3.2.3(2).

To prove (2), note that $\mathrm{Hom}_A(J,J) = (1/x) \cdot (xJ : J)$ is a ring, which is generated as $A$–module by $u_0/x, \ldots, u_s/x$. Therefore, there exist $\xi_k^{ij} \in A$ such that $(u_i/x) \cdot (u_j/x) = \sum_{k=0}^{s} \xi_k^{ij} \cdot (u_k/x)$.

(3) Obviously, $I \subset \mathrm{Ker}(\phi)$, where $\phi : A[t_1, \ldots, t_s] \to (1/x) \cdot (xJ : J)$ is the ring map defined by $t_i \mapsto u_i/x$, $i = 1, \ldots, s$. On the other hand, let $h \in \mathrm{Ker}(\phi)$. Then, using the relations $t_i t_j - \sum_{k=0}^{s} \xi_k^{ij} t_k$, $1 \le i \le j \le s$, we can write $h \equiv h_0 + \sum_{i=1}^{s} h_i t_i \mod I$, for some $h_0, h_1, \ldots, h_s \in A$.

Now $\phi(h) = 0$ implies $h_0 + \sum_{i=1}^{s} h_i \cdot (u_i/x) = 0$, hence, $(h_0, \ldots, h_s)$ is a syzygy of $u_0 = x, u_1, \ldots, u_s$ and, therefore, $h \in I$. □

*Example* 3.5.2. Let $A := K[x,y]/\langle x^2 - y^3 \rangle$ and $J := \langle x, y \rangle \subset A$. Then $x \in J$ is a non–zerodivisor in $A$ with $xJ : J = x\langle x, y \rangle : \langle x, y \rangle = \langle x, y^2 \rangle$, therefore,

$\mathrm{Hom}_A(J,J) = \langle 1,\, y^2/x\rangle$ (using Remark 3.2.3(2)). Setting $u_0 := x$, $u_1 := y^2$, we obtain $u_1^2 = y^4 = x^2y$, that is, $\xi_0^{11} = y$. Hence, we obtain an isomorphism

$$A[t]/\langle t^2 - y,\, xt - y^2,\, yt - x\rangle \xrightarrow{\cong} \mathrm{Hom}_A(J,J)\,.$$

of $A$–algebras. Note that $A[t]/\langle t^2 - y,\, xt - y^2,\, yt - x\rangle \simeq K[t]$.

Now, using Proposition 3.3.1 and Lemma 3.5.1 we obtain an algorithm to compute the integral closure. We describe the algorithm for the case that $A = K[x_1,\dots,x_n]/I$ is an integral domain over a field $K$ of characteristic 0, that is, especially $I$ is prime.

**Algorithm 3.5.3** (NORMALIZATION($I$)).

Input: $I := \langle f_1,\dots,f_k\rangle \subset K[x]$ a prime ideal, $x = (x_1,\dots,x_n)$.

Output: A polynomial ring $K[t]$, $t = (t_1,\dots,t_N)$, a prime ideal $P \subset K[t]$ and $\pi : K[x] \to K[t]$ such that the induced map $\pi : K[x]/I \to K[t]/P$ is the normalization of $K[x]/I$.

- if $I = \langle 0\rangle$ then return $(K[x], \langle 0\rangle, \mathrm{id}_{K[x]})$;
- compute $r := \dim(I)$;
- if we know that the singular locus of $I$ is $V(x_1,\dots,x_n)$[2]
  $J := \langle x_1,\dots,x_n\rangle$;
  else
  compute $J :=$ the ideal of the $(n-r)$–minors of the Jacobian matrix $I$;
- $J :=$ RADICAL$(I + J)$;
- choose $a \in J \setminus \{0\}$;
- if $aJ : J = \langle a\rangle$ return $(K[x], I, \mathrm{id}_{K[x]})$;
- compute a generating system $u_0 = a,\, u_1,\dots,u_s$ for $aJ : J$;
- compute a generating system $\big\{(\eta_0^{(1)},\dots,\eta_s^{(1)}),\dots,(\eta_0^{(m)},\dots,\eta_s^{(m)})\big\}$ for the module of syzygies $\mathrm{syz}(u_0,\dots,u_s) \subset (K[x]/I)^{s+1}$;
- compute $\xi_k^{ij}$ such that $u_i \cdot u_j = \sum_{k=0}^s a \cdot \xi_k^{ij} u_k$, $i,j = 1,\dots s$;
- change ring to $K[x_1,\dots,x_n,t_1,\dots,t_s]$, and set (with $t_0 := 1$)
  $I_1 := \big\langle \{t_it_j - \sum_{k=0}^s \xi_k^{ij} t_k\}_{1\le i\le j\le s}\,,\, \{\sum_{\nu=0}^s \eta_\nu^{(k)} t_\nu\}_{1\le k\le m}\big\rangle + IK[x,t]$;
- return NORMALIZATION$(I_1)$.

Note that $I_1$ is again a prime ideal, since

$$K[x_1,\dots,x_n,t_1,\dots,t_s]/I_1 \cong \mathrm{Hom}_A(J,J) \subset Q(A)$$

is an integral domain.

*Example* 3.5.4 (normalization). Let us illustrate the normalization with Whitney's umbrella

[2] This is useful information because, in this case, we can avoid computing the minors of the Jacobian matrix and the radical (which can be expensive). The property of being an isolated singularity is kept during the normalization loops.

```
ring A = 0,(x,y,z),dp;
ideal I = y2-zx2;
LIB "surf.lib";
plot(I,"rot_x=1.45;rot_y=1.36;rot_z=4.5;");

list nor = normal (I);
def R = nor[1]; setring R;
norid;
//-> norid[1]=0
normap;
//-> normap[1]=T(1)  normap[2]=T(1)*T(2)  normap[3]=T(2)^2
```

Hence, the normalization of $A/I$ is $K[T_1, T_2]$ with normalization map $x \mapsto T_1$, $y \mapsto -T_2^2$, $z \mapsto -T_1T_2$.

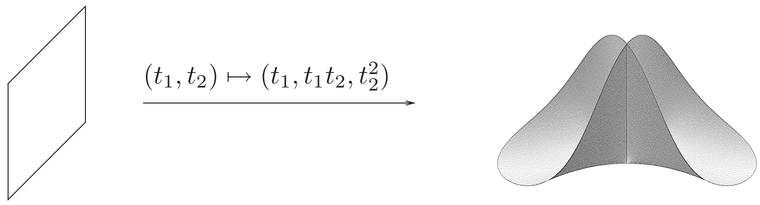



Figure 1: The normalization of Whitney's umbrella.

### 3.6 Algorithm to Compute the Non-Normal Locus

As a corollary of the Grauert-Remmert criterion, we obtain:

**Corollary 3.6.1.** *Let $A$ be a reduced Noetherian ring, $J \subset A$ a test ideal, $f \in J$ a non-zerodivisor of $A$, and set*

$$I_N := \mathrm{Ann}_A\big(\mathrm{Hom}_A(J,J)/A\big) \;\cong\; (fJ : J) : f\,.$$

*Then $V(I_N)$ is the non-normal locus of $A$.*

**Algorithm 3.6.2** (NON–NORMAL LOCUS)**.**

Input: $f_1, \ldots, f_k \in S = K[x_1, \ldots, x_n]$, $I := \langle f_1, \ldots, f_k \rangle$.

Assume: $\sqrt{I} = I$, $K$ perfect.

Output: Generators for $I_N$ s.th. $V(I_N) = N(S/I)$.

- Compute an ideal $\widetilde{J}$ s.th. $V(\widetilde{J}) = \mathrm{Sing}(S/I)$.
- Compute a non-zerodivisor $f \in \widetilde{J}$: choose a linear combination $f$ of the generators of $\widetilde{J}$ and test

$$f \text{ non-zerodivisor} \Longleftrightarrow (I : f) := \big\{ g \in S \;\big|\; gf \in I \big\} \;=\; \{0\}.$$

- Compute the radical $\sqrt{\langle f, I \rangle} =: J$.

- Compute generators $g_1, \ldots, g_\ell$ for $(fJ : J) : f$ as $S$-module.
- Return $\{g_1, \ldots, g_\ell\}$.

*Example* 3.6.3. We compute the non–normal locus of $A := K[x,y,z]/\langle zy^2 - zx^3 - x^6\rangle$.

```
LIB"primdec.lib";
ring A = 0,(x,y,z),dp;
ideal I = zy2-zx3-x6;
ideal sing = I+jacob(I);
ideal J = radical(sing);
qring R = std(I);
ideal J = fetch(A,J);
ideal a = J[1];
ideal re = quotient(a,quotient(a*J,J));
re;
//-> re[1]=y
//-> re[2]=x
```

From the output, we read that the non–normal locus is the $z$–axis (the zero–set of $\langle x, y\rangle$).

# 4 Computation in Local Rings

## 4.1 What is meant by "local" computations ?

There are several **concepts of "local"** in algebraic geometry:

- sometimes it means just an **affine** neighbourhood of a point, the algebraic counterpart being affine rings, that is, rings of the form $\mathbb{C}[\boldsymbol{x}]/I$, where $I \subset \mathbb{C}[\boldsymbol{x}] = \mathbb{C}[x_1, \ldots, x_n]$ is an ideal;
- sometimes it means the study of the **localization at a prime ideal** $\mathfrak{p} \subset \mathbb{C}[\boldsymbol{x}]$, $\mathbb{C}[\boldsymbol{x}]_{\mathfrak{p}}/I$, with $I \subset \mathbb{C}[\boldsymbol{x}]_{\mathfrak{p}}$ some ideal;
- sometimes it means **convergent power series rings** $\mathbb{C}\{\boldsymbol{x}\}/I$, or even **formal power series rings** $\mathbb{C}[[\boldsymbol{x}]]/I$.

Actually, we have for the maximal ideal $\langle \boldsymbol{x} \rangle = \langle x_1, \ldots, x_n \rangle$

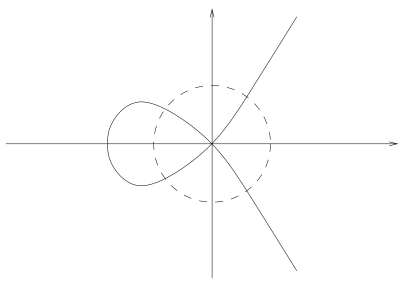
$$\mathbb{C}[\boldsymbol{x}] \subset \mathbb{C}[\boldsymbol{x}]_{\langle \boldsymbol{x} \rangle} \subset \mathbb{C}\{\boldsymbol{x}\} \subset \mathbb{C}[[\boldsymbol{x}]]$$

where the first ring is the "least local" and the last one the "most local".[3]

Hence, when considering "local" properties of a variety $V$, that is, properties of the **germ** $(V, P)$ (= the equivalence class of all open neighbourhoods of $P$ in $V$) of the variety at a given point $P$, one has to specify what "local" should mean, in particular, what is meant by "neighbourhood".

## 4.2 An Example

We want to study the germ at $0 = (0, 0)$ of the plane curve with affine equation $y^2 - x^2(1 + x) = 0$:



The picture indicates:

- **in a small Euclidean neighbourhood** of 0 the curve has **two irreducible components**, meeting transversally, but
- **in the affine plane**, and, hence, in each Zariski neighbourhood[4] of 0 **the curve is irreducible**.

[3] Note that $\mathbb{C}[\boldsymbol{x}]/I$ is not a local ring (except when the variety defined by $I$ consists of only one point) while the other three rings are local.

[4] Such a neighbourhood consists of the curve minus finitely many points different from 0. But a connected open subset of $\mathbb{C}$ minus finitely many points is irreducible (here, the above real picture is misleading).

Let's prove this: consider $f = y^2 - x^2(1+x)$ as element of $\mathbb{C}\{x,y\}$. We have a non-trivial decomposition[5]

$$f = \big(y - x\sqrt{1+x}\big)\big(y + x\sqrt{1+x})\big)$$

with $y \pm x\sqrt{1+x} \in \mathbb{C}\{x,y\}$. The zero-sets of the factors correspond to the two components of $\{f=0\}$ in a small neighbourhood of 0.

However, $f$ is irreducible in $\mathbb{C}[x,y]$, even in $\mathbb{C}[x,y]_{\langle x,y\rangle}$. Otherwise, there would exist $g,h \in \mathbb{C}[x,y]_{\langle x,y\rangle}$ satisfying $f = \big(y+xg\big)\big(y+xh\big)$, hence $g=-h$ and $g^2 = 1+x$. But, since $1+x$ is everywhere defined, $g^2$ and, hence, $g$ must be a polynomial which is impossible, since $g^2$ has degree 1. □

## 4.3 Computational Aspects

We shall show in the following, that (and how) the concept of Gröbner basis computations can be generalized to the local rings $\mathbb{C}[\boldsymbol{x}]_{\langle \boldsymbol{x}\rangle}$, $\mathbb{C}\{\boldsymbol{x}\}$ and $\mathbb{C}[[\boldsymbol{x}]]$, respectively.

In practice, however, **we can basically treat only $\mathbb{C}[\boldsymbol{x}]$ and $\mathbb{C}[\boldsymbol{x}]_{\langle \boldsymbol{x}\rangle}$** (or factor rings of those) in a computer algebra system[6]. In particular, we can neither put a polynomial into Weierstraß normal form (cf. below), nor factorize it in $\mathbb{C}[[\boldsymbol{x}]]$ effectively (except for power series in two variables where the Newton algorithm for computing Puiseux series provides a method) and we do not know any algorithm which would be able to do this even if the input is a polynomial.

Nevertheless, many invariants of (analytic) germs can be computed in $\mathbb{C}[\boldsymbol{x}]_{\langle \boldsymbol{x}\rangle}$, since we have the following

**Facts:** Let $K$ be any field and $I \subset K[\boldsymbol{x}]_{\langle \boldsymbol{x}\rangle}$ an ideal.

- If $\dim_K(K[\boldsymbol{x}]_{\langle x\rangle}/I) < \infty$, then, as local $k$–algebras,

  $$K[\boldsymbol{x}]_{\langle \boldsymbol{x}\rangle}/I \cong K[[\boldsymbol{x}]]/IK[[\boldsymbol{x}]]\,.$$

  In particular, both vector spaces have the same dimension and a common basis represented by monomials.

- The inclusion $K[\boldsymbol{x}]_{\langle \boldsymbol{x}\rangle}/I \subset K[[\boldsymbol{x}]]/IK[[\boldsymbol{x}]]$ **is faithfully flat**, that is, a sequence of $K[\boldsymbol{x}]_{\langle \boldsymbol{x}\rangle}/I$–modules

  $$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

  is exact if and only if the induced[7] sequence of $K[[\boldsymbol{x}]]/IK[[\boldsymbol{x}]]$–modules is exact.

## 4.4 Rings Associated to Monomial Orderings

To implement local rings in a computer algebra system one has to abort the restriction that monomial orderings are well-orderings. Hence, we define:

[5] This is, up to units, also the factorization in $\mathbb{C}[[x,y]]$, since the factorization is unique.

[6] Singular is apparently the only existing computer algebra system which systematically has incorporated standard basis algorithms in local rings.

[7] by applying $\_ \otimes_{K[\boldsymbol{x}]_{\langle \boldsymbol{x}\rangle}/I} K[[\boldsymbol{x}]]/IK[[\boldsymbol{x}]]$

**Definition 4.4.1.** A **monomial ordering** is a *total* ordering $>$ on the set of monomials $\boldsymbol{x}^\alpha := x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$ which is compatible with the semigroup structure, that is, satisfies

$$\boldsymbol{x}^\alpha > \boldsymbol{x}^\beta \implies \boldsymbol{x}^\gamma \boldsymbol{x}^\alpha > \boldsymbol{x}^\gamma \boldsymbol{x}^\beta \text{ for all } \alpha, \beta, \gamma \in \mathbb{Z}^n_{\geq 0}.$$

To any such monomial ordering $>$ we associate the multiplicatively closed set

$$S_> := \{u \in K[\boldsymbol{x}] \setminus \{0\} \mid \mathrm{LM}(u) = 1\}$$

and the ring

$$K[\boldsymbol{x}]_> := S_>^{-1} K[\boldsymbol{x}] = \left\{ \frac{f}{u} \,\middle|\, f, u \in K[\boldsymbol{x}],\, \mathrm{LM}(u) = 1 \right\}.$$

The following lemma follows easily from Lemma 1.2.5.

**Lemma 4.4.2.**

*(1) The following are equivalent:*

*(a)* $K[\boldsymbol{x}]_> = K[\boldsymbol{x}]$.

*(b)* $\boldsymbol{x}^\alpha > 1$ *for all* $\alpha \neq (0, \ldots, 0)$, *i.e.* $>$ *is global.*

*(2) In genaral we have*

$$K[\boldsymbol{x}] \subset K[\boldsymbol{x}]_> \subset K[[\boldsymbol{x}]].$$

Recall that in SINGULAR the global orderings are indicated by `p` as 2nd letter (referring to "`p`olynomial ring"): `lp`, `dp`, etc.

## 4.5 Local Monomial Orderings

The following Lemma follows again from Lemma 1.2.5.

**Lemma 4.5.1.** *The following are equivalent:*

*(a)* $K[\boldsymbol{x}]_> = K[\boldsymbol{x}]_{\langle x \rangle}$.

*(b)* $\boldsymbol{x}^\alpha < 1$ *for all* $\alpha \neq (0, \ldots, 0)$, *i.e.* $>$ *is local.*

*(c) the* ***inverse ordering*** $\left(\boldsymbol{x}^\alpha >' \boldsymbol{x}^\beta :\Leftrightarrow \boldsymbol{x}^\alpha < \boldsymbol{x}^\beta\right)$ ***is global***.

*Example* 4.5.2. The following are (the probably most important) **local monomial orderings**:

- *Negative degree reverse lexicographical ordering* $>_{\mathtt{ds}}$:

$$\begin{aligned}\boldsymbol{x}^\alpha >_{\mathtt{ds}} \boldsymbol{x}^\beta \quad :\Longleftrightarrow \quad & \deg \boldsymbol{x}^\alpha < \deg \boldsymbol{x}^\beta, \\ & \text{or } \big(\deg \boldsymbol{x}^\alpha = \deg \boldsymbol{x}^\beta \text{ and } \exists\, 1 \leq i \leq n : \\ & \qquad \alpha_n = \beta_n, \ldots, \alpha_{i+1} = \beta_{i+1},\, \alpha_i < \beta_i\big).\end{aligned}$$

- *Weighted negative degree reverse lexicographical orderings* $>_{\mathtt{ws}(\boldsymbol{w})}$, defined as $>_{\mathtt{ds}}$, but replacing the degree of $\boldsymbol{x}^\alpha$ by the weighted degree

$$\mathrm{wdeg}(\boldsymbol{x}^\alpha) = w_1\alpha_1 + \ldots + w_n\alpha_n,$$

  where $w_1 > 0$, $w_2, \ldots, w_n \geq 0$

- *Negative lexicographical ordering* $>_{\mathtt{ls}}$, which is defined to be the inverse of the lexicographical ordering.

- *Product orderings* of the latter.

## 4.6 Rings Associated to Mixed Orderings

If the monomial ordering is neither local nor global then we call it a **mixed** ordering. In this case:

$$K[\boldsymbol{x}] \subsetneq K[\boldsymbol{x}]_{>} \subsetneq K[\boldsymbol{x}]_{\langle x\rangle}\,,$$

and $(K[\boldsymbol{x}]_>)^* \cap K[\boldsymbol{x}] = S_> = \{u \in K[\boldsymbol{x}] \setminus \{0\} \mid \mathrm{LM}(u) = 1\}$, where $R^*$ denotes the group of units in the ring $R$.

*Example* 4.6.1. Consider $K[\boldsymbol{x}, \boldsymbol{y}] = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$, equipped with a **product ordering** $(>_1, >_2)$. Then we have

(1) $>_1$ *global* , $>_2$ *local* :

$$K[\boldsymbol{x}, \boldsymbol{y}]_> = (K[\boldsymbol{y}]_{\langle \boldsymbol{y}\rangle})[\boldsymbol{x}] = K[\boldsymbol{y}]_{\langle \boldsymbol{y}\rangle} \otimes_K K[\boldsymbol{x}]\,.$$

(2) $>_1$ *local* , $>_2$ *global* :

$$(K[\boldsymbol{x}]_{\langle \boldsymbol{x}\rangle})[\boldsymbol{y}] \subsetneq K[\boldsymbol{x}, \boldsymbol{y}]_> \subsetneq K[\boldsymbol{x}, \boldsymbol{y}]_{\langle \boldsymbol{x}\rangle}\,,$$

(3) $>_1$ *global* , $>_2$ *arbitrary* :

$$K[\boldsymbol{x}, \boldsymbol{y}]_> = (K[\boldsymbol{y}]_{>_2})[\boldsymbol{x}]\,.$$

**Definition 4.6.2** (Ring maps)**.** Let $>_1$, $>_2$ be monomial orderings on $K[\boldsymbol{x}]$, respectively $K[\boldsymbol{y}]$. Then $f_1, \ldots, f_n \in K[\boldsymbol{y}]_{>_2}$ define a unique ring map

$$\varphi : K[\boldsymbol{x}]_{>_1} \to K[\boldsymbol{y}]_{>_2}\,, \quad x_i \mapsto f_i\,,$$

provided that $h(f_1, \ldots, f_n) \in S_{>_2}$ **for all** $h \in S_{>_1}$.

## 4.7 Leading Data

Let $>$ be any monomial ordering and $f \in K[\boldsymbol{x}]_>$. Then we can (and do) choose a $u \in K[\boldsymbol{x}]$ such that $\mathrm{LM}(u) = 1$ and $uf \in K[\boldsymbol{x}]$ and define

$$\begin{aligned} \mathrm{LM}(f) &:= \mathrm{LM}(uf)\,, && \text{the leading monomial of } f,\\ \mathrm{LC}(f) &:= \mathrm{LC}(uf)\,, && \text{the leading coefficient of } f,\\ \mathrm{LT}(f) &:= \mathrm{LT}(uf)\,, && \text{the leading term of } f, \end{aligned}$$

and $\mathrm{tail}(f) := f - \mathrm{LT}(f)$.

Moreover, we define for any $G \subset K[x]_>$ the **leading ideal**

$$L_>(G) := L(G) := \langle \mathrm{LM}(g) \mid g \in G \setminus \{0\}\rangle_{K[x]}\,.$$

Note that these definitions are independent of the choice of $u$.

It is useful to consider $K[\boldsymbol{x}]_>$ as a subring of $K[[\boldsymbol{x}]]$, the formal power series ring. Then $\mathrm{LT}(f)$ **corresponds to the largest (w.r.t. $>$) term in the power series expansion** of $f$ and $\mathrm{tail}(f)$ is the power series of $f$ with the leading term deleted. In particular, these notions are compatible with the obvious extension of leading data to formal power series rings (w.r.t. a local monomial ordering).

*Example* 4.7.1. Let $f = \frac{2x}{1-x} + x = 3x + \sum_{k=2}^{\infty} 2x^k$, then

$$\mathrm{LT}(f) = \mathrm{LT}((1+x)f) = 3x\,.$$

As in the polynomial ring, the leading ideal $L(I)$ encodes much information about the ideal $I$, for instance:

**Theorem 4.7.2.** *Let $>$ be any monomial ordering on $K[\boldsymbol{x}]$, and let $I \subset K[\boldsymbol{x}]$ be an ideal. Then*

*(a)* $\dim(K[\boldsymbol{x}]_>/IK[\boldsymbol{x}]_>) = \dim(K[\boldsymbol{x}]/L(I))\,,$

*(b)* $\dim_K(K[\boldsymbol{x}]_>/IK[\boldsymbol{x}]_>) = \dim(K[\boldsymbol{x}]/L(I))\,.$

*Moreover, if* $\dim(K[\boldsymbol{x}]_>/IK[\boldsymbol{x}]_>) < \infty$*, then the monomials in $K[\boldsymbol{x}] \setminus L(I)$ represent a $K$-basis of $K[\boldsymbol{x}]_>/IK[\boldsymbol{x}]_>$.*

Since the leading ideal of an ideal is finitely generated, we can transfer the concept of Gröbner bases to $R = K[\boldsymbol{x}]_>$, respectively to $R = K[[\boldsymbol{x}]]$, and obtain the notion of a standard basis (as introduced independently by Hironaka (1964) and Grauert (1972)): a finite set $G \subset R$ is called a **standard basis** (SB) of $I$ if

$$G \subset I, \text{ and } L(I) = L(G)\,.$$

Moreover, we can extend the latter notions without further modifications to free $R$-modules with finite basis $e_1, \dots, e_r$.

## 4.8 Division with Remainder

The Division Theorems by Weierstraß and Grauert generalize division with remainder to free modules over formal power series rings:

**Theorem 4.8.1** (Division Theorem (Grauert))**.** *Let $F$ be a free $K[[\boldsymbol{x}]]$-module with a finite basis $e_1, \dots, e_r$, let $>$ be a local monomial ordering on $F$, and let $f, f_1, \dots, f_m \in F \setminus \{0\}$. Then there exist $g_1, \dots, g_r \in K[[\boldsymbol{x}]]$ and a* ***remainder*** *$h \in F$ such that*

$$f = \sum_{j=1}^{m} g_j f_j + h$$

*and, for all $j = 1, \dots, m$,*

*(a)* $\mathrm{LM}(f) \geq \mathrm{LM}(g_j f_j)$ *;*

*(b) if $h \neq 0$ then no monomial of $h$ is divisible by* $\mathrm{LM}(f_j)$.

Again, we call any such expression a **standard expression** for $f$ in terms of the $f_i$ and $h$ the **reduced normal form** of $f$ with respect to $I$. As before, for a "normal form" we weaken the condition (b) to $\mathrm{LM}(h)$ is not divisible by any $\mathrm{LM}(f_j)$.

## 4.9 Normal Forms and Standard Bases

The existence of a reduced normal form is the basis to obtain, in the formal power series ring $K[[\boldsymbol{x}]]$, the properties of standard bases already proved for GB in $K[\boldsymbol{x}]$:

- If $S, S'$ are two standard bases of the ideal $I$, then the reduced normal forms with respect to $S$ and $S'$ coincide.
- Buchberger's criterion holds.
- Reduced standard bases are uniquely determined.

The following theorem is one further reason, why for many computations in local analytic geometry it is sufficient to compute in $K[\boldsymbol{x}]_{\langle \boldsymbol{x} \rangle}$.

**Theorem 4.9.1.** *Let $>$ be a* ***local degree ordering*** *on $K[[\boldsymbol{x}]]$ and let $I$ be an ideal in $K[\boldsymbol{x}]$. Then*

$$S \text{ is a standard basis of } I \text{ (w.r.t. } >) \implies S \text{ is a standard basis of } IK[[x]].$$

So far everything was a straight forward transition from polynomial rings to power series rings. But it was theoretical. From the computational point of view there are several problems:

*Example* 4.9.2. Consider in $R = K[x,y]_{\langle x,y \rangle}$ with $> = >_{\mathtt{ls}}$.

$$f = y\,, \quad g = (y-x)(1-y)\,, \quad G = \{g\}\,.$$

Assume $h \in K[x,y]$ is a normal form of $f$ w.r.t. $G$. We have:

$$\begin{aligned} f \notin \langle G \rangle_R = \langle y - x \rangle_R \quad &\implies \quad h \neq 0 \\ &\implies \quad \mathrm{LM}(h) \notin L(G) = \langle y \rangle\,. \end{aligned}$$

Moreover, $h - y = h - f \in \langle G \rangle_R = \langle y - x \rangle_R \implies \mathrm{LM}(h) < 1$.
Therefore, $h = xh'$ for some $h'$ (because of the chosen ordering $>_{\mathtt{ls}}$). However, $y - xh' \notin \langle (y-x)(1-y) \rangle_{K[x,y]}$ (substitute $(0,1)$ for $(x,y)$) and, therefore **no polynomial normal form of $f$ w.r.t. $G$ exists**.

## 4.10 Weak Normal Forms

The fact that for polynomial input data there does not necessarily exist a polynomial normal form leads to the following

**Definition 4.10.1.** Let $R = K[\boldsymbol{x}]_>$ for some monomial ordering $>$. Let $G = \{g_1, \ldots, g_s\}$ be a finite subset of the free $R$–module $F$. A **polynomial** vector $h \in F$ is called a (polynomial) **weak normal form** for $f$ with respect to $G$ if there exists a polynomial unit $u \in R^*$ such that $h$ is a normal form for $uf$ w.r.t. $G$, that is $uf$ satisfies a relation (with $a_i$ polynomials)

$$uf = \sum_{i=1}^{s} a_i g_i + h, \;\; \mathrm{LM}(u) = 1,$$

with $\mathrm{LM}(\sum_{i=1}^{s} a_i g_i) \geq \mathrm{LM}(a_k g_k)$ for all $k$ such that $a_k g_k \neq 0$ and, if $h \neq 0$ then $\mathrm{LM}(h)$ is not divisible by any $\mathrm{LM}(g_i)$.

*Example* 4.10.2 (Example 4.9.2 continued). Setting $u := (1-y)$ and $h := x(1-y)$, we obtain $uy = (y-x)(1-y) + h$, hence, $h$ is a (polynomial) weak normal form.

The same difficulty arises when trying to generalize Buchberger's algorithm. Look at the following

*Example* 4.10.3. Consider in $K[x]_{\langle x \rangle}$ the polynomial $f := x$ and the standard basis $G := \{g = x - x^2\}$. The analogue to the Buchberger algorithm in $K[[x]]$ "computes" the normal form 0 as

$$x - \left(\sum_{i=0}^{\infty} x^i\right)(x - x^2) = 0\,,$$

hence it will produce infinitely many terms (and not the finite expression $1/(1-x)$). Again, this problem would be solved when computing

$$(1-x) \cdot x - g = 0\,.$$

In the following we present the general (weak) normal form algorithm (due to Greuel and Pfister) as implemented in Singular. The basic idea for this algorithm for local rings is due to Mora, but our algorithm is slightly different and more general (works for any monomial ordering).

## 4.11 The Weak Normal Form Algorithm

**Definition 4.11.1.** Let $f \in K[\boldsymbol{x}] \setminus \{0\}$. Then we set

$$\mathbf{ecart}(f) := \deg f - \deg \mathrm{LM}(f).$$

**Algorithm 4.11.2** (weakNF)**.** Let $>$ be any monomial ordering.

Input: $f \in K[\boldsymbol{x}]$, $G = \{f_1, \ldots, f_r\} \subset K[\boldsymbol{x}]$.

Output: $h \in K[\boldsymbol{x}]$, a weak normal form of $f$.

- $h := f$;
- $T := G$;
- while($h \neq 0$ and $T_h := \{g \in T \mid \mathrm{LM}(g)$ divides $\mathrm{LM}(h)\} \neq \emptyset$)
  {
    choose $g \in T_h$ with ecart$(g)$ minimal;
    if (ecart$(g) >$ ecart$(h)$) $\{T := T \cup \{h\}\}$;
    $h :=$ spoly$(h, g)$;
  }
- return $h$;

*Note* 4.11.3. The latter algorithm also applies to free $K[\boldsymbol{x}]_>$-modules with a finite base. Moreover:

- If the **input is homogeneous**, then the ecart is always 0, hence, we obtain Buchberger's Algorithm.
- If $>$ **is global**, then $\mathrm{LM}(g) \mid \mathrm{LM}(h)$ implies $\mathrm{LM}(g) \leq \mathrm{LM}(h)$. Hence, even if added to $T$ during the algorithm, $h$ cannot be used in further reductions.
- The `reduce` command in Singular returns $h$ while the `division` command also returns the factors $u$, $g_1, \ldots, g_r$.

## 4.12 Standard Basis Algorithm

Having the above (weak) normal form algorithm, we can proceed as in $K[\boldsymbol{x}]$ to compute a standard basis of a given ideal:

**Algorithm 4.12.1** (STD)**.** Let $>$ be any monomial ordering, and $R := K[\boldsymbol{x}]_>$.

Input: $G = \{f_1, \ldots, f_r\} \subset K[\boldsymbol{x}]$.

Output: $S \subset K[\boldsymbol{x}]$, such that $S$ is a standard basis for $\langle G \rangle_R$.

- $S := G$;
- $P := \{(f, g) \mid f, g \in S, f \neq g\}$, the pair–set;
- while $(P \neq \emptyset)$
  {
  choose $(f, g) \in P$;
  $P := P \setminus \{(f, g)\}$;
  $h :=$ `weakNF`$\big($**spoly**$(f, g), S\big)$;
  if $(h \neq 0)$
  {
  $P := P \cup \{(h, f) \mid f \in S\}$;
  $S := S \cup \{h\}$;
  }
  }
- return $S$;

The algorithm terminates, since otherwise we would obtain a strictly increasing sequence of monomial ideals $L(S)$ in $K[\boldsymbol{x}]$. Correctness follows from Buchberger's criterion.

The generalization to submodules of a finitely generated free module over R is immediate.

# 5 Singularities

## 5.1 Factorization, Primary Decomposition

*Note* 5.1.1. In Singular the factorization of polynomials, and, more generally, the primary decomposition of ideals, are **implemented only for the polynomial ring** $K[x_1, \ldots, x_n]$ and not for the localization $K[x_1, \ldots, x_n]_{\langle \mathbf{x} \rangle}$.

However, this is not a restriction, since after the factorization in $K[x_1, \ldots, x_n]$ we can pass to the local ring, where all factors not vanishing at 0 become units (see also Application 2).

```
ring r0=0,(x,y),ls;
poly f=(1-y)*(x^2-y^3)*(x^3-y^2)*(y^2-x^2-x^3);
f;
factorize(f);
//-> [1]:
//->    _[1]=1
//->    _[2]=-y2+x2+x3
//->    _[3]=-y2+x3
//->    _[4]=-y3+x2
//->    _[5]=-1+y
//-> [2]:
//->    1,1,1,1,1
```

**Warning**: Factorization in the power series ring $K[[x_1, \ldots, x_n]]$ is not possible except for $K[[x, y]]$ (using Hamburger–Noether expansion, implemented in Singular in `hnoether.lib`).

## 5.2 Singularities

An **(affine) algebraic variety** in $K^n$ is the set

$$X = V(I) = \{x \in K^n \mid f(x) = 0 \, \forall f \in I\}$$

where $I \subset K[x_1, \ldots, x_n]$ is any ideal ($I$ is part of the structure). $K[x_1, \ldots, x_n]/I =: \mathcal{O}_X(X)$ is called the coordinate ring of $X$ and $\mathcal{O}_X$ the ideal sheaf of $X$.

From now on we assume that $K$ is an algebraically closed field.

**Definition 5.2.1.** Let $X \subset K^n$ be an affine algebraic variety and $p \in X$.

The **analytic local ring** of $X$ at $p$ is the factor ring of the ring of formal power series, centered at $p = (p_1, \ldots, p_n)$,

$$\mathcal{O}^{an}_{X,p} := K[[x_1 - p_1, \ldots, x_n - p_n]]/I(X) \cdot K[[x_1 - p_1, \ldots, x_n - p_n]] \, .$$

The ring

$$\mathcal{O}_{X,p} = K[x_1, \ldots, x_n]_{\langle x_1 - p_1, \ldots, x_n - p_n \rangle}$$

is called the **algebraic local ring** of $X$ at the point $p = (p_1, \ldots, p_n)$.

**Lemma 5.2.2.** *Let $\mathcal{O}_{X,p}$ be the algebraic local ring and let $I \subset \mathcal{O}_{X,p}$ be an ideal such that $\dim_K(\mathcal{O}_{X,p}/I) < \infty$. Then*

$$\mathcal{O}_{X,p}/I \cong \mathcal{O}_{X,p}^{an}/I\mathcal{O}_{X,p}^{an}.$$

*In particular, both vector spaces have the same dimension and a common basis represented by monomials.*

*Note* 5.2.3. In general,

$$\begin{aligned}\dim_K \mathcal{O}_{X,0}/I &= \dim_K K[[x_1,\dots,x_n]]/\langle f_1,\dots,f_n\rangle \\ &\neq \dim_K K[x_1,\dots,x_n]/\langle f_1,\dots,f_k\rangle.\end{aligned}$$

## 5.3 Milnor and Tjurina Number

**Definition 5.3.1.**

(1) $f \in K[x]$, $x = (x_1,\dots,x_n)$, has an **isolated critical point** at $p$ if $p$ is an isolated point of $V(\partial f/\partial x_1,\dots,\partial f/\partial x_n)$. Similarly, we say that $p$ is an **isolated singularity** of $f$, or of the hypersurface $V(f) \subset \mathbb{A}_K^n$, if $p$ is an isolated point of $V(f, \partial f/\partial x_1,\dots,\partial f/\partial x_n)$.

(2) We call the number

$$\mu(f,p) := \dim_K \left( K\langle x_1 - p_1,\dots,x_n - p_n\rangle \Big/ \left\langle \frac{\partial f}{\partial x_1},\dots,\frac{\partial f}{\partial x_n}\right\rangle\right)$$

the **Milnor number**, and

$$\tau(f,p) := \dim_K \left( K\langle x_1 - p_1,\dots,x_n - p_n\rangle \Big/ \left\langle f, \frac{\partial f}{\partial x_1},\dots,\frac{\partial f}{\partial x_n}\right\rangle\right)$$

the **Tjurina number** of $f$ at $p$. We write $\mu(f)$ and $\tau(f)$ if $p = 0$.

*Note* 5.3.2. The Milnor number $\mu(f,p)$ is finite iff $p$ is an isolated critical point of $f$. Similarly, $p$ is an isolated singularity of $V(f)$ iff the Tjurina number $\tau(f,p)$ is finite.

By Lemma 5.2.2 we can compute the Milnor number $\mu(f)$, resp. the Tjurina number $\tau(f)$, by computing a standard basis of $\langle \partial f/\partial x_1,\dots,\partial f/\partial x_n\rangle$, respectively $\langle f, \partial f/\partial x_1,\dots,\partial f/\partial x_n\rangle$ with respect to a local monomial ordering and then apply the Singular command `vdim`.

## 5.4 Local Versus Global Ordering

We can use the interplay between local and global orderings to check the existence of critical points and of singularities outside 0. For this we use the (easy) facts for a polynomial $f \in K[x_1,\dots,x_n]$:

- $\mu(f,p) = 0$ if and only if $p$ is a **non–critical point of** $f$, that is,

$$p \notin V\left(\frac{\partial f}{\partial x_1},\dots,\frac{\partial f}{\partial x_n}\right) =: \mathbf{Crit(f)}\,,$$

- $\tau(f,p)=0$ if and only if $p$ is a non–**singular point point of** $V(f)$, that is,
$$p \notin V\left(f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right) =: \mathbf{Sing(f)}\,.$$

*Note* 5.4.1. We have the following equalities for the **total Milnor number**, respectively the **total Tjurina number**, of $f$:

$$\dim_K \left( K[x_1,\ldots,x_n] \Big/ \left\langle \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n} \right\rangle \right) = \sum_{p \in \operatorname{Crit}(f)} \mu(f,p)\,,$$

$$\dim_K \left( K[x_1,\ldots,x_n] \Big/ \left\langle f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n} \right\rangle \right) = \sum_{p \in \operatorname{Sing}(f)} \tau(f,p)\,,$$

## 5.5 Using Milnor and Tjurina Numbers

We compute the local and the total Milnor, respectively Tjurina, number and check in this way, whether there are further critical, respectively singular, points outside 0. We use first the commands `milnor` and `tjurina` from `sing.lib`:

We first compute the local Milnor and Tjurina number at 0:

```
LIB "sing.lib";
ring r = 0,(x,y,z),ds;          //local ring
poly f = x7+y7+(x-y)^2*x2y2+z2;
milnor(f);
//-> 28                         //Milnor number at 0
tjurina(f);
//-> 24                         //Tjurina number at 0
```

Without using `milnor` and `tjurina`, we have to compute

```
vdim (std(jacob (f)));          //the same as milnor
vdim (std(ideal(f)+jacob(f)));  //the same as tjurina
```

Now we compute the total Milnor and Tjurina number by choosing a global ordering.

```
ring R = 0,(x,y,z),dp;          //affine ring
poly f = x7+y7+(x-y)^2*x2y2+z2;
milnor(f);
//-> 36                         //total Milnor number
tjurina(f);
//-> 24                         //total Tjurina number
```

We see that the difference between the total and the local Milnor number is 8; hence, $f$ has eight critical points (counted with their respective Milnor numbers) outside 0. On the other hand, since the total Tjurina number coincides with the local Tjurina number, $V(f) \subset \mathbb{A}^3$ has no other singular points except 0, i.e. $f(p) \neq 0$ for all critical points $p \neq 0$. In other words, the extra critical points of $f$ do not ly on the zero-set $V(f)$ of $f$.

## 5.6 Application to Projective Singular Plane Curves

**Problem:** Let

$$f(x,y) := y^2 - 2x^{28}y - 4x^{21}y^{17} + 4x^{14}y^{33} - 8x^7y^{49} + x^{56} + 20y^{65} + 4x^{49}y^{16}.$$

Determine the local Tjurina number

$$\tau_{loc}(f) := \dim_{\mathbb{C}} \mathbb{C}\{x,y\}/\langle f, \tfrac{\partial f}{\partial x}, \tfrac{\partial f}{\partial y}\rangle$$

of the singularity at the origin and check whether this is the only singularity of the corresponding complex plane *projective* curve $C$.

*Note* 5.6.1. The projective curve $C \subset \mathbb{P}^2$ is the curve defined by $F = 0$, where $F$ is the homogenization of $f$ w.r.t. a new variable.

```
ring s = 0,(x,y),ds;       // the local ring
poly f = y2-2x28y-4x21y17+4x14y33-8x7y49+x56+20y65+4x49y16;
ideal I = f,jacob(f);
vdim(std(I));
//-> 2260                  // the local Tjurina number of f at 0
```

From 5.4.1 we know that the global Milnor number

$$\tau(f) := \dim_{\mathbb{C}} \mathbb{C}[x,y]/\langle f, \tfrac{\partial f}{\partial x}, \tfrac{\partial f}{\partial y}\rangle$$

equals the sum of the local Tjurina number of all affine singular points of $C$. We compute

```
ring r = 0,(x,y),dp;     // the affine ring
ideal I = fetch(s,I);
vdim(std(I));
//-> 2260
```

We see that the global (affine) and local Tjurina number of $f$ coincide. Hence, the affine singular locus consists only of the origin $(0,0)$, at all other points $V(f)$ is smooth.

Now, we check singularities at infinity:

```
ring sh = 0,(x,y,z),dp;
poly f = fetch(s,f);
poly F = homog(f,z);     // homogeneous polynomial
                         // defining C
ring r1 = 0,(y,z),dp;
map phi = sh,1,y,z;
poly g = phi(F);         // F in affine chart (x=1)
ideal J = g,jacob(g);
vdim(std(J));
//-> 120                 // the global Tjurina number in the
                         // chart x=1

ring r2 = 0,(y,z),ds;    // local ring at (1:0:0)
ideal J = fetch(r1,J);
vdim(std(J));
//-> 120                 // the local Tjurina number at (1:0:0)
```

We have considered all points at infinity except (0:1:0) which is obviously not on C. Hence, we can conclude that there is (precisely) 1 singularity of C at infinity (at $(1:0:0)$) with Tjurina number 120. A closer analysis shows that it is of topological type $x^9 - y^{16} = 0$.

## 5.7 Computing the Genus of a Projective Curve

**Recall:** Let $C$ be a projective curve, then the Hilbert polynomial is of the form

$$H_C(t) = \deg(C) \cdot t - p_a(C) + 1\,,$$

where $\deg(C)$ is called the **degree** of the curve and $p_a(C)$ the **arithmetic genus**. The procedure `hilbPoly` from `poly.lib` computes the Hilbert polynomial.

**Definition 5.7.1.** The **geometric genus** $g(C)$ is the arithmetic genus of the normalization $\widetilde{C}$ of $C$:

$$g(C) := p_a(\widetilde{C}).$$

If we are able to compute the normalization, we can compute the geometric genus. But this is often very time consuming.

**Facts.** Let $\delta(C) := \sum_{p\in C} \dim_K \left(\mathcal{O}_{\widetilde{C},p}/\mathcal{O}_{C,p}\right) = \sum_{p\in C} \delta(C,p)$.

- $p_a(C) = g(C) + \delta(C)$, where $\delta(C)$ is the sum over the local delta invariants in the singular points.
- For a generic projection $C \longrightarrow D$ to a plane curve $D$ which has the same degree $d$ and normalization as $C$, we have

$$g(C) = p_a(D) - \delta(D) = \frac{(d-1)(d-2)}{2} - \delta(D)$$

.

Let $D \subset \mathbb{P}^2$ be a (reduced) plane projective curve given by the homogeneous polynomial $F(x,y,z)$. To compute $\delta(D)$ we have to compute the singularities of $D$ and then compute $\delta(D,p)$ for each singular point $p \in D$ (by using the library `hnoether.lib` in Singular) or to use the normalization.

The procedure `genus` in `normal.lib` offers both possibilities (`genus(_);` and `genus(_,1);`):

```
ring R = 0,(x,y,z),dp;
poly f = (y3-x2)*(y-1);  // a cuspidal cubic with a transversal
                         // line
poly F = homog(f,z);     // defining the projective closure D
LIB "all.lib";           // loads all libraries
hilbPoly(F);
//-> -2,4                // p_a(D)=3, deg(D)=4
genus(F);                // computes delta at the singular points
//-> -1                  // hence D is reducible,
                         // delta(D)=p_a(D)-g(D)=4
genus(F,1);              // uses the normalization
//-> -1
```

*Remark* 5.7.2. The computation shows that $\delta(D) = 4$. We can compute in this example $\delta(D)$ by applying some theory without using SINGULAR:

By construction $f$ has a cusp singularity ($\delta = 1$) at $(0, 0)$ and two nodes at $(\pm 1, 1)$, the two intersection points of $y^3 - x^2 = 0$ and $y - 1 = 0$ (both having $\delta = 1$). By Bézout's theorem the line $y = 1$ intersects the cubic $y^3 = x^2$ at $\infty$ with multiplicity 1. Hence, $D$ must have a node at $\infty = (0 : 0 : 1)$, counting with $\delta = 1$. Hence, the sum of the deltas is $\delta(D) = 4$.

## References

[GP] G.-M. Greuel, G. Pfister, *A* SINGULAR *Introduction to Commutative Algebra*, 2nd edition, Springer-Verlag, Berlin, 2007.

[GPS1] G.-M. Greuel, G. Pfister and H. Schönemann, SINGULAR *online manual*.

[GPS2] G.-M. Greuel, G. Pfister and H. Schönemann, SINGULAR 3-0-4 (2007), `http://www.singular.uni-kl.de`.

[DL] W. Decker, C. Lossen, *Computing in Algebraic Geometry*, Springer-Verlag, Berlin, 2006.

FACHBEREICH MATHEMATIK, UNIVERSITÄT KAISERSLAUTERN, ERWIN-SCHRÖDINGER-STRASSE, D – 67663 KAISERSLAUTERN
*E–mail address:* greuel@mathematik.uni-kl.de
singular@mathematik.uni-kl.de to reach the SINGULAR team