2

Ideals, Varieties and Standard Bases

2.1 Ideals and Varieties

We begin with an easy, but important, observation about the algebraic set $V(f_1,\ldots,f_s)$ with $f_i \in R = K[x_1,\ldots,x_n]$:

If $f_1(p) = 0,\ldots,f_s(p) = 0$ for $p \in \mathbb{A}^n(K)$, then also any R-linear combination of the f_i vanishes on p, that is,

$$\left(\sum_{i=1}^{s} r_i \cdot f_i\right)(p) = \sum_{i=1}^{s} r_i(p) f_i(p) = 0$$

for all $r_i \in R$. Hence, $V(f_1,\ldots,f_s)$ depends only on the ideal

$$\langle f_1,\ldots,f_s\rangle = \{\textstyle\sum_{i=1}^{s} r_i f_i \mid r_i \in R\} \subset R,$$

generated by $f_1,\ldots,f_s$. Recall:

Definition 2.1.1 *Let R be a commutative ring with 1. An* ***ideal*** *is a non-empty subset $I \subset R$ with*

$$\begin{aligned} a + b &\in I \\ ra &\in I \end{aligned}$$

for all $a,b \in I$ and $r \in R$.

If $S \subset R$ then

$$\langle S\rangle = \left\{\textstyle\sum_{\mathit{finite}} r_i f_i \mid r_i \in R,\ f_i \in S\right\}$$

is the ideal ***generated*** *by S.*

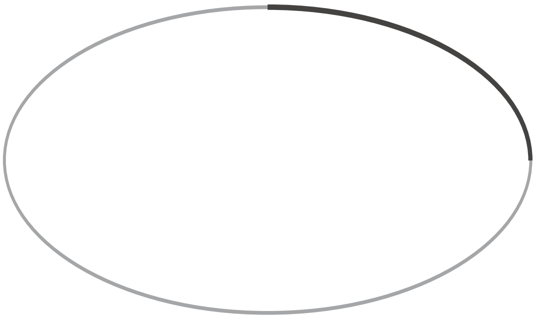

Figure 2.1: Elliptical arc

Recall, that the definition of an ideal is motivated in algebra by the following: For a subgroup $I \subset R$ the additive group R/I becomes a ring with multiplication induced by that of R if and only if I is an ideal (prove this as an easy exercise).

By the above observation it is natural to consider, instead of the vanishing locus of a set of equations, the vanishing locus of an ideal:

Definition 2.1.2 *If $I \subset K[x_1, \dots, x_n]$ then*

$$V(I) = \{p \in K^n \mid f(p) = 0 \; \forall f \in I\}$$

is called the ***vanishing locus*** *of I.*

This is indeed an affine variety, because any ideal $I \subset k[x_1, \dots, x_n]$ is finitely generated, as we will prove in Theorem 2.1.7.

Definition 2.1.3 *Let $S \subset \mathbb{A}^n(K)$ be a subset. Then*

$$I(S) = \{f \in K[x_1, \dots, x_n] \mid f(p) = 0 \; \forall p \in S\}$$

is (as we have seen above) an ideal, the ***vanishing ideal*** *of S.*

Example 2.1.4 *Consider the elliptical arc*

$$S = \left\{(x_1, x_2) \in \mathbb{A}^n(\mathbb{R}) \mid x_1^2 + 2x_2^2 = 1 \text{ and } x_1, x_2 \geq 0\right\}$$

shown in black in Figure 2.1. We have

$$I(S) = \left(x_1^2 + 2x_2^2 - 1\right)$$

hence $V(I(S))$ is the complete ellipse, the smallest algebraic set containing S. This is the closure

$$\overline{S} = V(I(S))$$

of S in the so called Zariski topology:

*The **Zariski topology** on $\mathbb{A}^n(K)$ has as closed sets the $V(I)$ for ideals $I \subset K[x_1, \dots, x_n]$. See also Exercise 2.2, which you need to show that this indeed gives a topology.*

By I and V inclusion reversing maps

$$\{\text{affine algebraic sets } X \subset \mathbb{A}^n(K)\} \underset{V}{\overset{I}{\rightleftarrows}} \{\text{ideals in } K[x_1, \dots, x_n]\}$$

between the set of algebraic subsets of $\mathbb{A}^n(K)$ and the set of ideals of $K[x_1, \dots, x_n]$ are given. It remains to show that any ideal $I \subset K[x_1, \dots, x_n]$ is finitely generated, that is, there are finitely many $f_1, \dots, f_s \in R$ with $I = \langle f_1, \dots, f_s \rangle$. We begin with a characterization of these ideals:

Theorem 2.1.5 *Let R be a commutative ring with 1. The following conditions are equivalent:*

1) *Every ideal $I \subset R$ is **finitely generated** .*

2) *Every ascending chain*

$$I_1 \subset I_2 \subset I_3 \subset \dots \subset I_n \subset \dots$$

of ideals terminates, that is, there is an m, such that

$$I_m = I_{m+1} = I_{m+2} = \dots$$

3) *Every non-empty set of ideals has a maximal element with respect to inclusion.*

*If R satisfies these conditions, then R is called **Noetherian**.*

These rings are called Noetherian after Emmy Noether (1882-1935), who has formulated the general structure theory for this class of rings and used this to give a simpler and more general proof of the theorems of Kronecker and Lasker.

Proof. (1) $\Longrightarrow$ (2): Let $I_1 \subset I_2 \subset \dots$ be a chain of ideals. Then

$$I = \bigcup_{j=1}^{\infty} I_j$$

is also an ideal: If $a, b \in I$, then there are $j_1, j_2 \in \mathbb{N}$ with $a \in I_{j_1}$, $b \in I_{j_2}$, and

$$a + b \in I_{\max(j_1, j_2)} \subset I$$

By (1) the ideal I is finitely generated, hence there are $a_1, \dots, a_s \in I$ with $I = \langle f_1, \dots, f_s \rangle$. For every f_k there is a j_k with $f_k \in I_{j_k}$. For

$$m := \max\{j_k \mid k = 1, \dots, s\}$$

we have $f_1, \dots, f_s \in I_m$, so

$$I = \langle f_1, \dots, f_s \rangle \subset I_m \subset I_{m+1} \subset \dots \subset I$$

and hence

$$I_m = I_{m+1} = \dots$$

(2) $\Longrightarrow$ (3): Assume that (3) does not hold. Then there is a set M of ideals, such that for every $I \in M$ there is an $I' \in M$ with $I \subsetneqq I'$ strictly contained. Hence, by induction, we obtain a sequence

$$I_1 \subsetneqq I_2 \subsetneqq I_3 \subsetneqq \dots$$

of ideals in M, which does not terminate, that is, (2) is not satisfied.

(3) $\Longrightarrow$ (1): Let I be an arbitrary ideal. The set

$$M = \{I' \subset I \mid I' \text{ finitely generated}\}$$

is non-empty, for example, $\langle 0 \rangle \in M$. Let J be a maximal element of M. So there are $f_1, \dots, f_s \in J$ with $J = \langle f_1, \dots, f_s \rangle$. We show that $I = J$: If this is not true, then there is an $f \in I \backslash J$ with

$$J \subsetneqq \langle f_1, \dots, f_s, f \rangle \subset I.$$

This contradicts the maximality of J. ∎

Example 2.1.6 *1) The ring of integers $\mathbb{Z}$ is Noetherian, since all ideals of $\mathbb{Z}$ are of the form*

$$\langle n \rangle = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$$

and, hence, are finitely generated (by a single element). See Exercise 2.1.

2) A field K only has the ideals (0) and $K = (1)$, in particular, K is Noetherian.

3) If R is Noetherian and $I \subset R$ an ideal, then the quotient ring R/I is Noetherian:

Let $\pi : R \to R/I$ be the canonical epimorphism. If $J \subset R/I$ an ideal then by assumption $\pi^{-1}(J) = \langle f_1, \dots, f_s \rangle$, and $J = \langle \pi(f_1), \dots, f(f_s) \rangle$.

4) The polynomial ring $K[x_1, x_2, ...]$ *in infinitely many variables is not Noetherian. Also the ring*

$$R = \{f \in \mathbb{Q}[X] \mid f(0) \in \mathbb{Z}\}$$

of polynomials in $\mathbb{Q}[X]$ *with integer values at* 0 *is not Noetherian. See Exercise 2.4.*

Hilbert has shown in 1890, that the polynomial ring $K[x_1, ...x_n]$ over a field K is Noetherian:

Theorem 2.1.7 (Hilbert's basis theorem) *If* R *is a Noetherian ring, then also* $R[x]$ *is Noetherian.*

Using that a field K and the ring of integers $\mathbb{Z}$ are Noetherian, by induction on the number n of variables

$$R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$$

we obtain:

Corollar 2.1.8 *Let* K *be a field. Then the polynomial rings* $K[x_1, ...x_n]$ *and* $\mathbb{Z}[x_1, ...x_n]$ *in* n *variables are Noetherian.*

The fact that $K[x_1, ...x_n]$is Noetherian, is the basis of all algorithms, we will discuss.

For the proof of Theorem 2.1.7 we consider the lead coefficients in R of polynomials in $R[x]$. If

$$f = a_k x^k + ... + a_1 x + a_0 \in R[x]$$

with $a_k \neq 0$ then the **degree** of f is $\deg(f) = k$, its **lead coefficient** is $\mathrm{LC}(f) = a_k$, its **lead term** $\mathrm{LT}(f) = a_k x^k$, and its **lead monomial** $\mathrm{L}(f) = x^k$.

Proof. Assume $R[x]$ is not Noetherian. Then there is an ideal $I \subset R[x]$ which is not finitely generated. Let $f_1 \in I$ with $\deg(f_1)$ minimal, $f_2 \in I \backslash \langle f_1 \rangle$ mit $\deg(f_2)$ minimal, and inductively

$$f_k \in I \backslash \langle f_1, \ldots, f_{k-1} \rangle$$

with $\deg(f_k)$ minimal. Then

$$\deg(f_1) \leq \deg(f_2) \leq ... \leq \deg(f_k) \leq ...$$

and we obtain an ascending chain of ideals in R

$$\langle \mathrm{LC}(f_1) \rangle \subset \langle \mathrm{LC}(f_1), \mathrm{LC}(f_2) \rangle \subset ... \subset \langle \mathrm{LC}(f_1), \ldots, \mathrm{LC}(f_k) \rangle \subset ...$$

We show that the inclusions are strict (and hence R is not Noetherian): Assume

$$\langle \mathrm{LC}(f_1), \dots, \mathrm{LC}(f_k) \rangle = \langle \mathrm{LC}(f_1), \dots, \mathrm{LC}(f_{k+1}) \rangle$$

Then we can write

$$\mathrm{LC}(f_{k+1}) = \sum_{j=1}^{k} b_j \,\mathrm{LC}(f_j)$$

with $b_j \in R$. Hence

$$\begin{aligned} g &:= \sum_{j=1}^{k} b_j \cdot x^{\deg(f_{k+1}) - \deg(f_j)} \cdot f_j \\ &\in \langle f_1, \dots, f_k \rangle \end{aligned}$$

has the same lead term as f_{k+1}, so

$$\deg(g - f_{k+1}) < \deg(f_{k+1}),$$

a contradiction, since f_{k+1} was chosen to have minimal degree. ■

So any algebraic set can be represented by an ideal, and any ideal gives an algebraic set. However, the V-map is not injective, for example,

$$V(x) = V(x^2) \subset \mathbb{A}^1(K).$$

There are two ways to remedy this situation. One possibility is to generalize our notation of an algebraic set: Given $I \subset R = K[x_1, \dots, x_n]$ we replace $V(I)$ by the **spectrum**

$$\mathrm{Spec}(R/I) = \{P \subset R/I \mid P \text{ prime ideal}\}$$

and consider R/I as the ring of function on $\mathrm{Spec}(R/I)$. Together with the Zariski topology we obtain a generalization of an algebraic set, called a **scheme**. An easier approach is to restrict the class of ideals in consideration. To determine that class of ideals, it is, astonishingly, enough to find out, under which conditions an algebraic set is empty. This is characterized by the following theorem of Hilbert (which we cannot prove here):

Theorem 2.1.9 (Weak Nullstellensatz) *Let K be an algebraically closed field and $I \subset K[x_1, \dots, x_n]$ an ideal. Then*

$$V(I) = \varnothing \Longleftrightarrow I = K[x_1, \dots, x_n]$$

Remark 2.1.10 *The condition, that K is algebraically closed, is necessary. For example, $V(x^2 + y^2 + 1) \subset \mathbb{A}^2(\mathbb{R})$ is empty (it is not empty over $\mathbb{C}$).*

From Theorem 2.1.9 we obtain:

Theorem 2.1.11 (Strong Nullstellensatz) *Let K be an algebraically closed field and $I \subset K[x_1,\dots,x_n]$ an ideal. Then*

$$I(V(I)) = \sqrt{I}.$$

where

$$\sqrt{I} = \{f \in K[x_1,\dots,x_n] \mid \exists a \in \mathbb{N} \text{ with } f^a \in I\}$$

*denotes the **radical** of I.*

Proof. According to the basis theorem, write $I = \langle f_1,\dots,f_s\rangle$. For $f \in I(V(I))$ consider

$$J = \langle I,\ y \cdot f - 1\rangle \subset K[x_1,\dots,x_n,y].$$

Since f vanishes at any common zero of $f_1,\dots,f_s$, and, hence, $y \cdot f - 1$ does not, we have $V(J) = \varnothing$. So by Theorem 2.1.9 $J = K[x_1,\dots,x_n,y]$, that is, there are $c_i, d \in K[x_1,\dots,x_n,y]$ with

$$1 = c_1 \cdot f_1 + \ldots + c_s \cdot f_s + d \cdot (y \cdot f - 1).$$

Substituting $y = \frac{1}{f}$ makes the coefficients to $c_i(x_1,\dots,x_n,\frac{1}{f})$. So multiplying with a sufficiently high power a of f cancels the denominators and yields $f^a \in I$.

The other inclusion is easy. ■

Definition 2.1.12 *An ideal $I \subset K[x_1,\dots,x_n]$ is called a **radical ideal**, if $I = \sqrt{I}$.*

Theorem 2.1.11 shows that, if K is algebraically closed,

$$\{\text{affine algebraic sets } X \subset \mathbb{A}^n(K)\} \underset{V}{\overset{I}{\rightleftarrows}} \{\text{radical ideals in } K[x_1,\dots,x_n]\}$$

is a one-to-one correspondence. In Exercise 2.3 we will prove, that an algebraic set $X = V(I)$ is irreducible, if and only if $I(V(I))$ is prime. This is true over any field K. If K is algebraically closed, then, by the strong Nullstellensatz, $V(I)$ is irreducible iff $I(V(I)) = \sqrt{I}$ is prime. In particular, if I is prime then $V(I)$ is irreducible. Note that this is not true in general if K is not algebraically closed. So for K algebraically closed we obtain a one-to-one correspondence of varieties (irreducible algebraic sets) and prime ideals:

$$\{\text{affine varieties } X \subset \mathbb{A}^n(K)\} \underset{V}{\overset{I}{\rightleftarrows}} \{\text{prime ideals in } K[x_1,\dots,x_n]\}$$

If K is algebraically closed, the points correspond to the maximal ideals, that is, we have a one–to-one correspondence

$$\begin{array}{ccc} \{\text{maximal ideals of } K[x_1,\dots,x_n]\} & \overset{V}{\underset{I}{\rightleftarrows}} & K^n \\ \langle x-a_1,\dots,x-a_n\rangle & & (a_1,\dots,a_n) \end{array}$$

Recall, that an ideal $P \subsetneqq R$ of a commutative ring R with 1 is called **prime ideal**, if $\forall a, b \in R$ it holds

$$a \cdot b \in P \Longrightarrow a \in P \text{ or } b \in P.$$

The ideal P is called **maximal ideal**, if for all ideals $I \subset R$ it holds

$$P \subset I \subsetneqq R \Longrightarrow P = I.$$

Recall also the following, standard and easy to prove, characterization of prime and maximal ideals:

Theorem 2.1.13 *Let R be a commutative ring with 1 and $I \subsetneqq R$ an ideal. Then it holds:*

1) I prime $\Longleftrightarrow$ R/I is an integral domain.

2) I maximal $\Longleftrightarrow$ R/I is a field.

Example 2.1.14 *1) The ideal $\langle x_2\rangle \subset K[x_1,x_2]$ is a prime ideal, because*

$$K[x_1,x_2]/\,(x_2) \cong K[x_1]$$

is an integral domain. On the other hand, $\langle x_1 \cdot x_2\rangle$ is not a prime ideal, since

$$\overline{x_1} \cdot \overline{x_2} = \overline{0} \in K[x_1,x_2]/I$$

and $\overline{x_1}, \overline{x_2} \neq \overline{0}$. Geometrically, the prime ideals $\langle x_1\rangle$ and $\langle x_2\rangle$ correspond to the coordinate axes and $\langle x_1 \cdot x_2\rangle$ to their union

$$V(x_1 \cdot x_2) = V(x_1) \cup V(x_2)$$

2) The ideal $\langle x_2 - x_1^2\rangle \subset K\,[x_1,x_2]$ is a prime ideal, since

$$\begin{array}{rcl} K\,[x_1,x_2]\,/\,\langle x_2 - x_1^2\rangle & \to & K[t] \\ x_1 & \mapsto & t \\ x_2 & \mapsto & t^2 \end{array}$$

is an isomorphism and $K[t]$ is an integral domain.

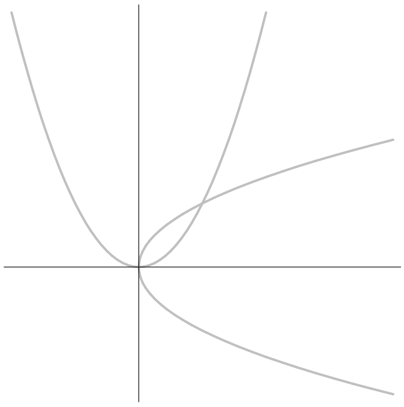

Figure 2.2: Reducible affine algebraic set

The ideal

$$I = \left\langle \left(x_2 - x_1^2\right) \cdot \left(x_1 - x_2^2\right) \right\rangle$$

is not prime, and

$$V(I) = V(x_2 - x_1^2) \cup V(x_1 - x_2^2),$$

see Figure 2.2.

In fact, any radical ideal can be written as an intersection of prime ideals, more generally, any ideal as an intersection of, so called, primary ideals. We will discuss in detail an algorithm which computes this primary decomposition.

Example 2.1.15 *The ideal $\langle x_1, x_2 \rangle \subset K[x_1, x_2]$ is a maximal ideal, since $K[x_1, x_2]/\langle x_1, x_2 \rangle \cong K$ is a field.*

See also the Exercises 2.5 and 2.6.

So the bottom line is: Any geometric problem concerning affine algebraic sets, can be translated into a problem concerning ideals in polynomial rings.

2.2 Introduction to the Ideal Membership Problem and Gröbner Bases

Suppose we want to obtain information about a variety $V(I) \subset \mathbb{A}^n(K)$ specified by an ideal $I = \langle f_1, \ldots, f_s \rangle \subset K[x_1, \ldots, x_n]$ which again is given by generators $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$. For example, we may want to determine, whether $V(I)$ is contained in the hypersurface $V(f)$. Equivalently, we have to determine whether $f \in \langle f_1, \ldots, f_s \rangle$. This question is called the **ideal membership problem** and appears as a fundamental buildung block in many more advanced algorithms.

Example 2.2.1 *Consider the twisted cubic curve $C = V(I)$ defined by $I = \langle y - x^2,\ z - x^3 \rangle$, see Figure 2.3. By definition, C is contained in the hypersurfaces $V(y - x^2)$ and $V(z - x^3)$. However, is it also contained in the hypersurface $V(z - xy)$? Figure 2.4suggests yes, and we easily find a representation*

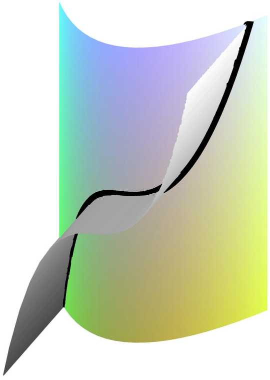

Figure 2.3: Twisted cubic

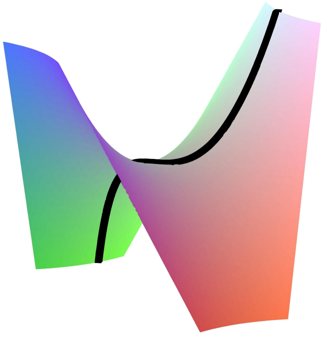

Figure 2.4: Surface containing the twisted cubic

$$z - xy = (-x) \cdot \left(y - x^2\right) + 1 \cdot \left(z - x^3\right).$$

How to find such a representation in a systematic way?

Before solving the ideal membership problem in general, let us first discuss two special settings, the linear and the univariate case.

Example 2.2.2 *Let $f_1, \ldots, f_s, f \in K[x_1, \ldots, x_n]$ be linear. Then testing $f \in I = \langle f_1, \ldots, f_s \rangle$ is easy and can be done in the following two steps:*

1) Apply Algorithm 1.5.1 to obtain linear equations $g_1, \ldots, g_r$ in row echelon form, so $L(g_1) > \ldots > L(g_r)$.

```
2) For $i = 1, \ldots, r$ do
        If $L(f) = L(g_i)$ then
            $f = f - \frac{LC(f)}{LC(g_i)} g_i$
   If $f = 0$ then return true else return false.
```

As a second special case, consider higher degree equations in a single variable. The polynomial ring $K[x]$ in one variable over a field K is an example of a Euclidean domain:

Definition 2.2.3 *A **Euclidean domain** is an integral domain R together with a map (called **Euclidean norm**)*

$$d : R \backslash \{0\} \longrightarrow \mathbb{N}_0$$

such that for any $a, b \in R \backslash \{0\}$ there exist $g, r \in R$ with

1) $a = g \cdot b + r$ and

2) $r = 0$ or $d(r) < d(b)$.

Example 2.2.4 *The ring of integers $\mathbb{Z}$ with $d(n) = |n|$ and the polynomial ring $K[X]$ in one variable X over a field K with $d(f) =$ $\deg(f)$ is Euclidean.*

There are many more Euclidean domains, for example, $\mathbb{Z}[i]$ with

$$d(a_1 + i \cdot a_2) = |a_1 + i \cdot a_2|^2 = a_1^2 + a_2^2.$$

The Euclidean algorithm given in Theorem 1.2.2 and its proof carry over directly to any Euclidean domain by replacing the absolute value by d.

Theorem 2.2.5 *Euclidean domains are principal ideal domains (any ideal is principal, that is, generated by a single element).*

Proof. Let $I \subset R$ be an ideal in a Euclidean domain. The ideal $I = \langle 0 \rangle$ is principal. Otherwise, there is a non-zero $b \in I$ with $d(b)$ minimal. Let $a \in I$ be arbitrary and $a = g \cdot b + r$ with $r = 0$ or $d(r) < d(b)$. By $a, b \in I$ also $r \in I$. As $d(b)$ was chosen minimal, we get $r = 0$ and, hence, $a \in \langle b \rangle$. This proves $I \subset \langle b \rangle \subset I$. ■

Corollar 2.2.6 *If R is a principal ideal domain, and $f_1, \ldots, f_s \in R$, then*

$$\langle f_1, \ldots, f_s \rangle = \langle \gcd(f_1, \ldots, f_s) \rangle$$

Proof. As R is a principal ideal domain,

$$\langle f_1, \ldots, f_s \rangle = \langle d \rangle$$

with $d \in R$, hence $d \mid f_i$ for all i. On the other hand, there are $x_i \in R$ with

$$d = x_1 f_1 + ... + x_s f_s.$$

So every divisor of all f_i divides d. Hence

$$d = \gcd(f_1, \ldots, f_s).$$

Recall that the gcd is only unique up to units in R. ■

Hence, the ideal membership problem translates into the following characterization

$$f \in \langle f_1, \ldots, f_s \rangle \quad \Longleftrightarrow \quad \gcd(f_1, \ldots, f_s) \text{ divides } f.$$

Example 2.2.7 *We test whether*

$$x^3 + x \in I = \left\langle x^4 - 1,\ x^4 - 3x^2 - 4 \right\rangle \subset \mathbb{Q}[x]$$

The Euclidean algorithm yields

$$\begin{array}{lcrcl} x^4 - 3x^2 - 4 & = & 1 \cdot (x^4 - 1) & + & (-3x^2 - 3) \\ x^4 - 1 & = & x^2 \cdot (x^2 + 1) & + & (-x^2 - 1) \\ & = & (x^2 - 1) \cdot (x^2 + 1) & + & 0 \end{array}$$

hence

$$I = \left\langle x^2 + 1 \right\rangle$$

and division with remainder

$$x^3 + x = x \cdot (x^2 + 1) + 0,$$

shows that, $x^3 + x \in I$.

So what about the general case?

Example 2.2.8 *Suppose we want to check whether*

$$x^2 - y^2 \in \left\langle x^2 + y,\ xy + x \right\rangle .$$

In order to do division with remainder, we have to decide which term of a polynomial is the lead term. Ordering by degree is not sufficient, consider $xy^2 + x^2y$. For example, we could order the monomials in a lexicographic way, that is, like the words in a telephone book. Then

$$L(x^2 + y) = x^2 \qquad L(xy + x) = xy$$

and the usual strategy for division with remainder would give

$$\begin{array}{ll} \boldsymbol{x}^2 - y^2 = & 1 \cdot (\boldsymbol{x}^2 + y) + (-y^2 - y) \\ x^2 + y & \\ \hline \boldsymbol{-y}^2 - y & \end{array}$$

The lead terms we write in bold face red. So the remainder is $-y^2 - y \neq 0$, however

$$\boldsymbol{x}^2 - y^2 = -y\left(\boldsymbol{x}^2 + y\right) + x\left(\boldsymbol{xy} + x\right) \in \left\langle x^2 + y, \quad xy + x \right\rangle .$$

The problem is caused by the cancelling of the lead terms in this expression. How to resolve the problem?

Simply add to the set of generators all polynomials, which can be obtained by canceling lead terms. The result is what is called a ***Gröbner basis****. In the example we would add $x^2 - y^2$ and then*

$$-y^2 - y = (x^2 - y^2) + (-1) \cdot (x^2 + y).$$

Finally, we could get rid of $x^2 - y^2$ or $x^2 + y$ as it is sufficient to keep one generator for each possible lead monomial. This results in a ***minimal*** *Gröbner basis*

$$\boldsymbol{x}^2 - y^2,\ \boldsymbol{xy} + x,\ \boldsymbol{y}^2 + y$$

or

$$\boldsymbol{x}^2 + y,\ \boldsymbol{xy} + x,\ \boldsymbol{y}^2 + y.$$

The second one is the unique ***reduced*** *Gröbner basis, which can be obtained by removing terms in $\mathrm{tail}(f) = f - \mathrm{LT}(f)$ which are divisable by some lead monomial. For any of these Gröbner bases, the division of $x^2 - y^2$ will give remainder zero: For the first one this is trivial, since $x^2 - y^2$ is already an element of the Gröbner basis. For the second one, we can continue the above calculation, resulting in the expression*

$$\boldsymbol{x}^2 - y^2 = 1 \cdot \left(\boldsymbol{x}^2 + y\right) + (-1) \cdot \left(\boldsymbol{y}^2 + y\right) + 0$$

with remainder 0.

Indeed, we will show in general, that when dividing f by a Gröbner basis $g_1, \dots, g_r$, division will give remainder zero if and only if $f \in \langle g_1, \dots, g_r \rangle$. We begin by formalizing this concept:

2.3 Monomial Orderings

For monomials we use multi-index notation $x^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$ with the exponent vector $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}_0^n$.

Definition 2.3.1 *A* ***monomial ordering*** *(or* ***semigroup ordering****) on the semigroup of monomials in the variables $x_1, \dots, x_n$ is an ordering $>$ with*

1) $>$ is a total ordering

2) $>$ respects multiplication, that is,

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

for all α, β, γ.

Definition and Theorem 2.3.2 *A* ***global ordering*** *is a monomial ordering $>$ with the following equivalent properties*

1) $>$ is a well ordering

(that is, any non-empty set of monomials has a smallest element)

2) $x_i > 1$ $\forall i$.

3) $x^\alpha > 1$ for all $0 \neq \alpha \in \mathbb{N}_0^n$.

4) If $x^\beta \mid x^\alpha$ and $x^\alpha \neq x^\beta$ then $x^\alpha > x^\beta$

(that is, $>$ refines divisibility).

If $x_i < 1$ $\forall i$, then $>$ is called a ***local ordering****.*

Proof. The implications (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) are easy, see Exercise 2.7. With respect to (4) $\Rightarrow$ (1), we have to prove that any non-empty set of monomials has only finitely many minimal elements with respect to divisibility. Then, by assumption (4) we only have to consider those minimal elements, and, since $>$ is a total ordering, among them there is a smallest. ■

Lemma 2.3.3 (Dickson, Gordan) *Any non-empty set of monomials in the variables $x_1, \ldots, x_n$ has only finitely many minimal elements with respect to divisibility.*

Proof. Let $M \neq \varnothing$ be a set of monomials in the variables $x_1, \ldots, x_n$, and $\langle M \rangle \subset K[x_1, \ldots, x_n]$ the ideal generated by the elements of M. By the Hilbert basis theorem 2.1.7 we have $\langle M \rangle = \langle f_1, \ldots, f_s \rangle$ with polynomials $f_i = \sum_{j=1}^{u} r_{i,j} m_j$ where $r_{i,j} \in K[x_1, \ldots, x_n]$ and $m_1, \ldots, m_u \in M$. Hence

$$\langle M \rangle \subset \langle m_1, \ldots, m_u \rangle \subset \langle M \rangle .$$

Among the $m_1, \ldots, m_u$ consider the minimal elements with respect to divisibility. ■

The ideal we have encountered in the proof is an example of a monomial ideal:

Definition 2.3.4 *An ideal $I \subset K[x_1, \ldots, x_n]$ is called a **monomial ideal**, if it is generated by monomials.*

Corollar 2.3.5 *Every monomial ideal has a unique set of **minimal generators** consisting of monomials.*

Proof. See the proof of Lemma 2.3.3 (or apply the lemma to the set of monomials in the ideal). ■

In the proof we have also encountered the following trivial, but important, observation:

Lemma 2.3.6 *Let $I = \langle M \rangle$ be a monomial ideal generated by the monomials in M. If $f \in I$, then every term of f is in I.*

In particular, if $f \in I$ is a monomial, then there is an $m \in M$ with $m \mid f$.

Proof. If $f = \sum_{j=1}^{u} r_j m_j \in I$ with $r_j \in K[x_1, \ldots, x_n]$ and $m_j \in M$, any term of f is a term of some (perhaps several) $r_j m_j$ and hence a multiple of some m_j. ■

We discuss some specific monomial orderings, there are many more. First note:

Example 2.3.7 *In one variable all global orderings are equivalent to the ordering defined by $x > 1$, all local orderings to that defined by $x < 1$.*

Definition 2.3.8 *The following definitions yield global monomial orderings:*

1) ***Lexicographical*** *ordering:*

$x^\alpha > x^\beta \iff$ *the leftmost nonzero entry of* $\alpha - \beta$ *is positive.*

In SINGULAR *this ordering is abbreviated as* ***lp****.*

2) ***Degree reverse lexicographical*** *ordering:*

$x^\alpha > x^\beta \Leftrightarrow \deg x^\alpha > \deg x^\beta$ *or* $\deg x^\alpha = \deg x^\beta$ *and* $\exists 1 \leq i \leq n:$ $\alpha_n = \beta_n, \ldots, \alpha_{i+1} = \beta_{i+1}, \alpha_i < \beta_i$.

In SINGULAR *this ordering is abbreviated as* ***dp****.*

An example of a local ordering is the ***negative lexicographical ordering****:*
$x^\alpha > x^\beta \iff$ *the leftmost nonzero entry of* $\alpha - \beta$ *is negative.*
In SINGULAR *this ordering is abbreviated as* ***ls****.*

The degree reverse lexicographical ordering usually gives a better performance than the lexicographical one. This is especially apparent if we are computing a Gröbner basis of an ideal which is homogeneous, that is, which can be genereated by homogeneous polynomials. Recall that a polynomial is called **homogeneous** if all its monomials have the same degree. Note, that a homogeneous ideal has a lot of non-homogeneous elements.

The lexicographical ordering is nevertheless very important, since it has the so called elimination property, that is, it allows one to bring polynomial systems into a triangular form. We will come back to this property later.

Example 2.3.9 *For lp on the monomials in* x, y, z *we have (identifying monomials and exponent vectors)*

$$\begin{aligned} x = (1,0,0) > y &= (0,1,0) > z = (0,0,1) \\ xy^2 = (1,2,0) &> (0,3,4) = y^3z^4 \\ x^3y^2z^4 = (3,2,4) &> (3,1,5) = x^3y^1z^5 \end{aligned}$$

on the other hand, for dp we get

$$\begin{aligned} x = (1,0,0) > y &= (0,1,0) > z = (0,0,1) \\ xy^2 = (1,2,0) &< (0,3,4) = y^3z^4 \\ x^3y^2z^4 = (3,2,4) &> (3,1,5) = x^3yz^5 \end{aligned}$$

and for ls

$$\begin{aligned} x = (1,0,0) < y &= (0,1,0) < z = (0,0,1) \\ xy^2 = (1,2,0) &< (0,3,4) = y^3z^4 \\ x^3y^2z^4 = (3,2,4) &< (3,1,5) = x^3yz^5 \end{aligned}$$

In Singular *we can compare monomials as follows:*

```
ring R=0,(x,y,z),lp;
x>y;
1
y>z;
1
xy2>y3z4;
1
x3y2z4>x3yz5
1
ring R=0,(x,y,z),dp;
x>y;
1
y>z;
1
xy2>y3z4;
0
x3y2z4>x3yz5
1
ring R=0,(x,y,z),ls;
1>z;
1
z>y;
1
y>x;
1
xy2>y3z4;
0
x3y2z4>x3yz5
0
```

Our definitions in the linear and univariate case generalize directly:

Definition 2.3.10 *With respect to a given monomial ordering $>$, for any polynomial $0 \neq f = \sum_\alpha c_\alpha x^\alpha$ the* ***leading monomial*** *is the largest monomial x^α with $c_\alpha \neq 0$ and is denoted by $L(f)$. Furthermore, we denote by $LC(f) = c_\alpha$ the* ***leading coefficient****, and by $LT(f) = c_\alpha x^\alpha$ the* ***leading term****. For $f = 0$ we set $L(0) = LT(0) = LC(0) = 0$.*

Example 2.3.11 *Using lp we have*

$$L(5x^2y + yx^2) = x^2y.$$

In Singular *we compute the lead term, monomial and coefficient as follows:*

```
ring R=0,(x,y,z),lp;
poly f = 5x2y+xy2;
lead(f);
5x2y
leadcoef(f);
5
leadmonom(f);
x2y
```

Definition 2.3.12 *A monomial ordering $>$ is called a* ***weighted degree ordering*** *if there is some $w \in \mathbb{R}^n$ with non-zero entries such that*

$$w\alpha > w\beta \Rightarrow x^\alpha > x^\beta .$$

Example 2.3.13 *If $>$ is any monomial ordering and $w \in \mathbb{R}^n$, then $>_w$ given by*

$$x^\alpha >_w x^\beta \Leftrightarrow w\alpha > w\beta \text{ or } \left(w\alpha = w\beta \text{ and } x^\alpha > x^\beta \right)$$

is a monomial ordering.

The ordering $>$, which takes over if the w-weights of x^α and x^β are equal, is called ***tie-break*** *ordering.*

By construction, $>_w$ is a weighted degree ordering, it is global if $w_i > 0$ $\forall i$ and it is local if $w_i < 0$ $\forall i$.

For the purpose of explicit computations, which will only involve a finite number of monomials, we can represent any monomial ordering by a weight vector:

Proposition 2.3.14 *Given a monomial ordering $>$ and a finite set M of monomials in the variables $x_1, \dots, x_n$, there is a weight vector $w \in \mathbb{Z}^n$ with*

$$x^\alpha > x^\beta \Longleftrightarrow w \cdot \alpha > w \cdot \beta$$

for all $x^\alpha, x^\beta \in M$.

We can choose w such that $w_i > 0$ if $x_i > 1$ and $w_i < 0$ if $x_i < 1$.

Proof. Consider

$$D_> := \left\{ \alpha - \beta \in \mathbb{Z}^n \mid x^\alpha > x^\beta \right\}.$$

If $\alpha_1 - \beta_1, \alpha_2 - \beta_2 \in D_>$ then

$$x^{\alpha_1 + \alpha_2} = x^{\alpha_1} x^{\alpha_2} > x^{\beta_1} x^{\alpha_2} > x^{\beta_1} x^{\beta_2} = x^{\beta_1 + \beta_2},$$

hence

$$\delta_1, \delta_2 \in D_> \Rightarrow \delta_1 + \delta_2 \in D_>.$$

So for all $\lambda_i \in \mathbb{N}$ and $\delta_i \in D_>$

$$\textstyle\sum_i \lambda_i \delta_i \in D_>.$$

As $0 \notin D_>$, we get $\sum_i \lambda_i \delta_i \neq 0$ for all $\delta_i \in D_>$ and $\lambda_i \in \mathbb{Q}_{>0}$, hence

$$0 \notin \operatorname{convHull}(D_>).$$

Here for a set of vectors $V \subset \mathbb{Z}^n$, we write

$$\operatorname{convHull}(V) = \{\textstyle\sum_{i=1}^r \lambda_i \delta_i \mid \delta_i \in V,\ \lambda_i \in \mathbb{Q}_{\geq 0},\ \sum_{i=1}^r \lambda_i = 1\}$$

For an example in Figure 2.5 the grey area is the convex hull of the black points. So also for

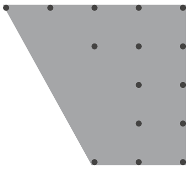

Figure 2.5: A convex hull

$$D_>^M := \left\{\alpha - \beta \in \mathbb{Z}^n \mid x^\alpha, x^\beta \in M,\ x^\alpha > x^\beta\right\}$$

we have

$$0 \notin \operatorname{convHull}(D_>^M).$$

Thus there is a $w \in \mathbb{Z}^n$ such that $\operatorname{convHull}(D_>^M)$ is contained in the half space where the linear form $\delta \mapsto w\delta$ takes positive values. Hence,

$$w\delta > 0 \text{ for all } \delta \in D_>.$$

For the second statement observe: This w satisfies $w_i > 0$ if $x_i > 1$ and $w_i < 0$ if $x_i < 1$, provided that $1, x_1, \ldots, x_n \in M$. ∎

Note that this representation of $>$ via scalar weights obtained from the linear form $w\cdot$ is in general not valid for comparing arbitrary monomials (in one variable it is). However one can represent any monomial ordering in n variables by using a vector valued lexicographic comparison

Example 2.3.15 *For the lexicographical ordering $>$ in the variables x_1, x_2 and the set of all monomials M of degree ≤ 4, the set $D_>^M$ is plotted in Figure 2.6.The figure also shows the line $w\delta = 0$, where w is a weight vector representing lp on all monomials of degree ≤ 4. For more examples see Exercise 2.9.*

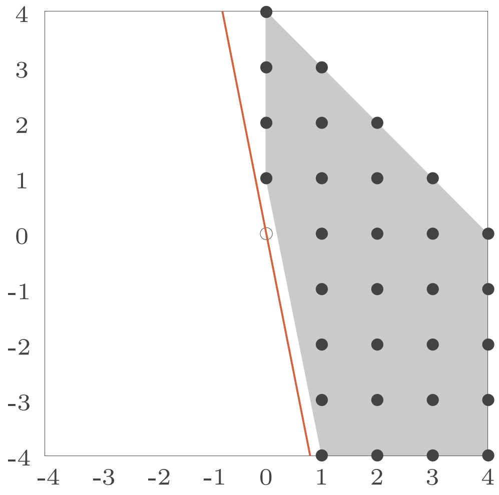

Figure 2.6: $D^M_>$ for the ordering lp and the set M of monomial of degree ≤ 4

You can imagine that a Gröbner basis computation for a fixed ideal will only involve finitely many monomials due to the Noetherian property of the polynomial ring. The equivalent weight vectors w form a cone and these cones fit nicely together in what is called the **Gröbner fan** (that is, the intersection of two such cones is again one of the cones). Figure 2.7 shows the Gröbner fan classifying the non-equivalent weight vectors for $f = x + y + 1$ and the initial term of each cone. Given a weight-vector w, the **initial term** $\mathrm{in}_w(f)$ is the sum of all terms of f with maximal w-weight. Then the Gröbner fan of $\langle f\rangle$ consists of the closures of cones

$$\{w \mid \mathrm{in}_w(f) = g\}$$

for any possible initial form g. These cones are given by linear inequalities. As an exercise determine these inequalities. The definition of the Grönber fan can be generalized to ideals with more than one generator, however to do this, one requires Gröbner basis techniques.

If you have heard about tropical geometry, the tropical variety of an ideal can be considered as a subfan of the Gröbner fan. In the example, it consists of those faces such that $\mathrm{in}_w(f)$ is not a monomial. So the three black half-lines in the figure form the tropical variety of a line.

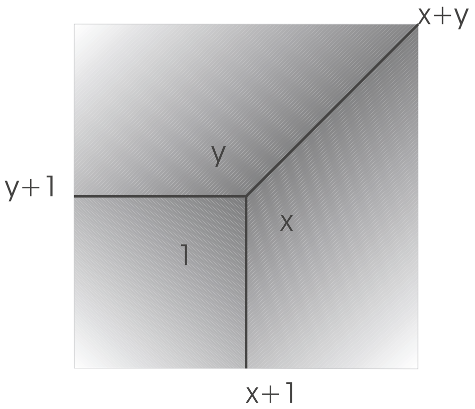

Figure 2.7: Gröbner fan of the line.

2.4 Monomial Orderings and Localizations

Monomial orderings are closely related to the concept of localizations, which again have and important geometric interpretation.

Definition 2.4.1 *A* ***local ring*** *is a ring which has exactly one maximal ideal.*

Definition 2.4.2 *Let R be a ring. Given a* ***multiplicatively closed set*** *$S \subset R$, that is, a set with $1 \in S$ and*

$$s_1, s_2 \in S \Rightarrow s_1 \cdot s_2 \in S$$

the ***localization*** *of R with respect to S is the ring*

$$S^{-1}R := \left\{ \frac{r}{s} \mid r \in R, \;\; s \in S \right\}$$

where $\frac{r}{s}$ is the equivalence class of all (r', s') with respect to the equivalence relation

$$(r, s) \sim (r', s') \Longleftrightarrow \exists q \in S \text{ with } q(rs' - r's) = 0,$$

and addition and multiplication are defined by the usual formulas for calculating with fractions.

Example 2.4.3 *1) With $S = \mathbb{Z}/\{0\}$,*

$$\mathbb{Q} = S^{-1}\mathbb{Z}.$$

2) *More generally we can construct in this way the quotient field $Q(R)$ of an integral domain R, for example the function field*

$$K(x_1, \dots, x_n) = Q(K[x_1, \dots, x_n])$$

over a field K.

3) *If $P \subset R$ is a prime ideal in a ring R, then $S = R \backslash P$ is multiplicatively closed and we write*

$$R_P = S^{-1} R$$

*for the **localization** of R **at the prime ideal** P. The ring $S^{-1}R$ is a local ring with maximal ideal*

$$P \cdot R_P = \left\{ \frac{r}{s} \mid r \in P, \ s \notin P \right\}.$$

Remark 2.4.4 *If R is Noetherian then $S^{-1}R$ is also Noetherian.*

We leave the details as an easy exercise. Geometrically,localization at a prime ideal corresponds to investigating an algebraic set at locally at P:

Example 2.4.5 *Consider the curve $C = V(I) \subset \mathbb{A}^2(K)$ defined by $I = \langle (x-1) \cdot y \rangle \subset R = K[x,y]$. In the localization at the maximal ideal $P = \langle x, y \rangle \subset R$ we have that*

$$I \cdot R_P = \langle y \rangle$$

since $x - 1 \notin P$ is a unit in R_P. So locally at the point $(0,0)$ the curve C looks like a line, whereas at the point $(1,0)$ it looks like the intersection of two line, see Figure 2.8.

Example 2.4.6 *If K is a field and $>$ is a monomial ordering on the semigroup of monomials in $x_1, \dots, x_n$, then*

$$S_> = \{ u \in K[x_1, \dots, x_n] \mid \mathrm{LM}(u) = 1 \}$$

is multiplicatively closed. We write

$$K[x_1, \dots, x_n]_> = S^{-1} K[x_1, \dots, x_n]$$

for the corresponding localization of the polynomial ring with respect to $>$.

By Definition and Theorem 2.3.2, $>$ is global if and only if $S_> = K^*$, that is

$$K[x_1, \dots, x_n]_> = K[x_1, \dots, x_n].$$

On the other hand if $>$ is local then

$$K[x_1, \dots, x_n]_> = K[x_1, \dots, x_n]_{\langle x_1, \dots, x_n \rangle}.$$

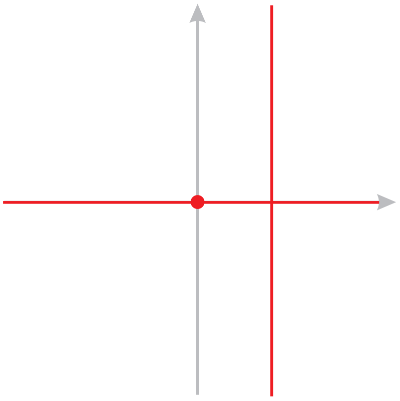

Figure 2.8: Local properties of union of two lines

We can use this construction to describe localizations at arbitrary coordinate planes:

Example 2.4.7 *If $>$ is a local ordering on the monomials in $x_1, \ldots, x_n$, then*

$$K[x_1, \ldots, x_n, y_1, \ldots, y_m]_{\langle x_1, \ldots, x_n \rangle} = K(y_1, \ldots, y_m)[x_1, \ldots, x_n]_>.$$

The proof is Exercise 2.10.

We can extend the notion of a lead monomial to $K[x_1, \ldots, x_n]_>$ in the following way. This will lead to a Gröbner bases theory in $K[x_1, \ldots, x_n]_>$, the so called theory of standard bases.

Definition 2.4.8 *If $f \in K[x_1, \ldots, x_n]_>$ there is a polynomial $u \in K[x_1, \ldots, x_n]$ with*

$$\mathrm{LT}(u) = 1 \text{ and } u \cdot f \in K[x_1, \ldots, x_n].$$

We define

$$L(f) := L(u \cdot f).$$

In the same way, we define

$$\begin{aligned} \mathrm{LC}(f) &:= \mathrm{LC}(u \cdot f) \\ \mathrm{LT}(f) &:= \mathrm{LT}(u \cdot f) \\ \mathrm{tail}(f) &:= \mathrm{tail}(u \cdot f). \end{aligned}$$

In Exercise 2.13 we show that these definitions are independent of the choice of u.

2.5 Division with Remainder and Standard Bases

Fix a monomial ordering on $K[x_1, \dots, x_n]$ and write $R = K[x_1, \dots, x_n]_>$. If we consider a global monomial ordering, that is, $R = K[x_1, \dots, x_n]$, then it is pretty clear, how to do division with remainder. Algorithm 2.5.1 divides $f \in R$ by $g_1, \dots, g_s \in R$.

Algorithm 2.5.1 Division with remainder

Input: $f \in R$, $g_1, ..., g_s \in R$, $>$ be a global ordering on the monomials of R.

Output: An expression

$$f = q + r = \textstyle\sum_{i=1}^{s} a_i g_i + r$$

such that $L(r)$ is not divisible by any $L(g_i)$.

```
$q = 0$
$r = f$
while $r \neq 0$ and $L(g_i) \mid L(r)$ for some $i$ do
    Cancel the lead term of $r$:
    $a = \frac{LT(r)}{LT(g_i)}$
    $q = q + a \cdot g_i$
    $r = r - a \cdot g_i$
```

Proof. In every step the lead term of r becomes smaller with respect to $>$, so the algorithm terminates, since $>$ is a well-ordering. ■

Example 2.5.1 *Using lp divide $x^2y + x$ by $y - 1$ and $x^2 - 1$.*

$$\begin{array}{l l}
\boldsymbol{x^2 y} + x = & x^2\,(\boldsymbol{y} - 1) + 1 \cdot (\boldsymbol{x^2} - 1) + x + 1 \\
x^2y - x^2 & \\
\hline
\boldsymbol{x^2} + x & \\
x^2 - 1 & \\
\hline
\boldsymbol{x} + 1 &
\end{array}$$

Remark 2.5.2 *The assumption that $>$ is global is necessary for the termination: If we divide x by $\boldsymbol{x} - x^2$ using the local ordering $x < 1$, then Algorithm 2.5.1 will compute*

$$\begin{aligned}
x &= 1 \cdot (\boldsymbol{x} - x^2) + \boldsymbol{x^2} \\
&= (1 + x) \cdot (\boldsymbol{x} - x^2) + \boldsymbol{x^3} \\
&\;\vdots \\
&= \left(\textstyle\sum_{i=0}^{\infty} x^i\right) \cdot (\boldsymbol{x} - x^2) + 0
\end{aligned}$$

that is, the geometric series expansion of

$$\frac{x}{x-x^2} = \frac{1}{1-x} = \textstyle\sum_{i=0}^{\infty} x^i.$$

So the algorithm works as expected, but does not give an answer after finitely many steps. We will come back to this (however, the solution is pretty obvious, clear the denominator $1-x$).

We will now show that Algorithm 2.5.1 solves the ideal membership problem, provided we divide by a Gröbner basis, and we will develop a modified version of the algorithm that will also do the job for non-global orderings.

Definition 2.5.3 *Given a monomial ordering $>$ and a subset $G \subset R$, we define the* ***leading ideal*** *of G as*

$$L(G) = L_>(G) = \langle L(f) \mid f \in G \backslash \{0\} \rangle \subset R,$$

the monomial ideal generated by the lead monomials. If the choice of $>$ is clear, we also write $L(G)$.

Given an ideal I the ideal $L(I)$ will contain all possible lead monomials obtainable by cancelling lead term, hence we define:

Definition 2.5.4 (Standard and Gröbner bases) *Let I be an ideal and $>$ a monomial ordering. A finite set*

$$G \subset I$$

with $0 \notin G$ is called a ***standard basis*** *of I with respect to $>$, if*

$$L(G) = L(I).$$

If $>$ is global, then we call a standard basis also a ***Gröbner basis****.*

Note that the inclusion $\subset$ is true for any subset. The existence of a standard basis is easy:

Theorem 2.5.5 *Every ideal $I \subset R$ has a standard basis.*

Proof. Since $L(I)$ is finitely generated, $L(I) = \langle m_1, \dots, m_s \rangle$ with monomials m_i. Furthermore, m_i is divisible by some $L(g_i)$ for some $g_i \in I$, see Lemma 2.3.6. Hence

$$L(I) = \langle L(g_1), \dots, L(g_s) \rangle,$$

so $g_1, \dots, g_s$ form a standard basis of I. ■

From the definition it is not clear whether a standard basis of I is indeed a set of generators of I. Solving the ideal membership problem will answer also this question.

Our goal will be to handle the global and non-global setting in an uniform way. We first formlize the abstract properties of Algorithm 2.5.1 in the notion of a normal form.

Definition 2.5.6 *Given a list $G = (g_1, \dots, g_s) \subset R$, a* ***normal form*** *is a map $\mathrm{NF}(-,G) : R \to R$ with*

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

2) If $\mathrm{NF}(f,G) \neq 0$ then $L(\mathrm{NF}(f,G)) \notin L(G)$.

3) For every $0 \neq f \in R$ there are $a_i \in R$ with

$$f - \mathrm{NF}(f,G) = \textstyle\sum_{i=1}^{s} a_i g_i$$

and $L(f) \geq L(a_i g_i)$ for all i with $a_i g_i \neq 0$. Such an expression we call a ***standard represenation*** *of f.*

We also say that NF *is a normal form, if $\mathrm{NF}(-,G)$ is a normal form for all G.*

As discussed above, in the non-global setting we will have to relax property (3) allowing for clearing denominators:

Definition 2.5.7 *A* ***weak normal form*** *is a map $\mathrm{NF}(-,G) : R \to R$ with condition (1) and (2) of the previous definition and*

3') For every $0 \neq f \in R$ there is a unit $u \in R^*$ such that $u \cdot f$ has a standard representation.

A weak normal form is called ***polynomial weak normal form*** *if for every $f \in K[x_1, \dots, x_n]$ and list $G \subset K[x_1, \dots, x_n]$ there exists a unit $u \in R^* \cap K[x_1, \dots, x_n]$ such that there is a standard expression*

$$u \cdot f - \mathrm{NF}(f,G) = \textstyle\sum_{i=1}^{s} a_i g_i$$

with $a_i \in K[x_1, \dots, x_n]$.

Remark 2.5.8 *1) Any normal form is a weak normal form.*

2) Note that any weak normal form induces a normal form by division with u. However only if $>$ is global, i.e., $R^* = K^*$, this normal form will be polynomial.

Since in the applications we can usually work with polynomial data, we will use polynomial weak normal forms for local orderings, and normal forms for global orderings.

Lemma 2.5.9 *Given a list $G = (g_1, \dots, g_s)$ and any order of preference of the g_i in the division, Algorithm 2.5.1 yields a normal form $\mathrm{NF}(-, G)$. It is called the* ***Buchberger normal form****.*

Proof. We map f to $\mathrm{NF}(f, G) := r$. If the algorithm returns remainder $r \neq 0$ then $L(r)$ is not divisible by any $L(g_i)$, so $L(r) \notin L(G)$ by Lemma 2.3.6. Condition (3) is clear, since in every iteration of the algorithm $L(a \cdot g_i) \leq L(f)$. ■

Using standard bases and a weak normal form, we can now decide the ideal membership problem:

Theorem 2.5.10 (Ideal membership) *Let $I \subset R$ be an ideal and $f \in R$. If $G = \{g_1, \dots, g_s\}$ is a standard basis of I and* NF *is a weak normal form, then*

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

Proof. Consider a standard expression $uf = \sum_i a_i g_i + r$ with $r = \mathrm{NF}(f, G)$, $a_i \in R$ and $u \in R^*$. If $r = 0$ then $uf = \sum_i a_i g_i \in \langle G \rangle \subset I$, hence $f \in I$. On the other hand, if $r \neq 0$ then by Definition 2.5.6 (2.)

$$L(r) \notin L(G) = L(I).$$

So, by definition of the lead ideal,

$$r \notin I,$$

hence $uf = \sum_i a_i g_i + r \notin I$, so $f \notin I$. ■

Lemma 2.5.11 *If $J \subset I \subset R$ are ideals with $L(J) = L(I)$ then $I = J$.*

Proof. Let $G = \{g_1, \dots, g_s\}$ be a standard basis of J, NF a weak normal form, $f \in I$ and $uf = \sum_i a_i g_i + r$ a standard expression with $r = \mathrm{NF}(f, G)$. So $r \in I$. If $r \neq 0$, then by Definition 2.5.6 (2.)

$$L(r) \notin L(G) = L(J) = L(I).$$

By the definition of the lead ideal, we have $r \notin I$, a contradiction. ■

Corollar 2.5.12 *If G is a standard basis of I, then*

$$I = \langle G \rangle \,.$$

Proof. We have $L(I) = L(G) \subset L(\langle G \rangle) \subset L(I)$, so G is a standard basis of $\langle G \rangle \subset I$ and $L(\langle G \rangle) = L(I)$. Equality follows from Lemma 2.5.11. ■

Example 2.5.13 *The generators of the ideal $I = \langle x^2 - 1, y - 1 \rangle$ already form a Gröbner basis with respect to lp: Since $x \notin L(I)$ (Exercise) we have*

$$L(I) = \left\langle x^2, y \right\rangle .$$

Corollar 2.5.14 *For any monomial ordering $>$, the ring*

$$R = K[x_1, \dots, x_n]_>$$

is Noetherian.

Proof. By Theorem 2.5.5 any ideal in R has a standard basis, which consists out of finitely many elements, and by Corollary 2.5.12 this standard basis generates the ideal. ■

In particular, this proves again that $K[x_1, \dots, x_n]$ is Noetherian, see Corollary 2.1.8.

Of course, the result of division with remainder depends on the monomial ordering. But, even if we fix a monomial ordering and divide by a Gröbner basis, the result may not be uniquely determined in the sense that the remainder depends on the order of preference of the divisors g_i in the division algorithm:

Example 2.5.15 *At every step of Algorithm 2.5.1, there can be several choices of g_i such that $L(g_i) \mid L(f)$. We divide $x^2y + x$ by the Gröbner basis $G = \{y - 1, x^2 - 1\}$, using lp as in Example 2.5.1. However we now prefer $x^2 - 1$ over $y - 1$ when possible:*

$$\begin{array}{ll}
\boldsymbol{x^2y} + x = & y \cdot (\boldsymbol{x^2} - 1) + x + y \\
x^2y - y & \\
\hline
\boldsymbol{x} + y &
\end{array}$$

So depending on the choice made, the remainder will be $x + 1$ or $x + y$.

To have a uniquely determined remainder, we proceed as follows:

Definition 2.5.16 *An element $f \in R$ is called **reduced** with respect to a set $G \subset R$, if no term of the power series expansion of f is contained in $L(G)$.*

A normal form NF *is called **reduced normal form**, if* $\mathrm{NF}(f, G)$ *is reduced with respect to G for all f and G.*

Algorithm 2.5.2 yields a reduced normal form, the **reduced Buchberger normal form**.

Algorithm 2.5.2 Reduced division with remainder

Input: $f \in R$, $g_1, ..., g_s \in R$, $>$ be a global ordering on the monomials of R.

Output: An expression

$$f = q + r = \sum_{i=1}^{s} a_i g_i + r$$

such that not term of r is divisible by any $L(g_i)$.

```
$q = 0$
$r = 0$
$h = f$
while $h \neq 0$ do
  if $L(g_i) \mid L(h)$ for some $i$ then
    Cancel the lead term of $h$:
    $a = \frac{LT(h)}{LT(g_i)}$
    $q = q + a \cdot g_i$
    $h = h - a \cdot g_i$
  else
    Put the lead term into the remainder:
    $r = r + LT(h)$
    $h = h - LT(h)$
```

Example 2.5.17 *So, also putting terms into the remainder in the intermediate steps, we can continue in Example 2.5.15:*

$$\begin{array}{l l}
\boldsymbol{x^2y} + x = & y \cdot (\boldsymbol{x}^2 - 1) + \boldsymbol{x} + 1 \cdot (\boldsymbol{y} - 1) + 1 \\
x^2y - y & \\
\cline{1-1}
\boldsymbol{x} + y & \\
\cline{1-1}
\boldsymbol{y} & \\
y - 1 & \\
\cline{1-1}
1 &
\end{array}$$

which leads to the same remainder $x+1$ as in Example 2.5.1. Indeed, the remainder is now unique provided we divide by a Gröbner basis:

Theorem 2.5.18 *Let $>$ be a global ordering, $I \subset R$ an ideal, $f \in R$ and G a Gröbner basis of I. If* NF *is a reduced normal form, then* $\mathrm{NF}(f,G)$ *is uniquely determined by $>$, f and I. We then also write* $\mathrm{NF}(f,I)$.

Proof. Write $G = \{g_1, \dots, g_s\}$ and suppose that

$$\begin{aligned} f &= \textstyle\sum_{i=1}^{s} a_i g_i + r \\ &= \textstyle\sum_{i=1}^{s} a_i' g_i + r' \end{aligned}$$

Then

$$r - r' = \textstyle\sum_{i=1}^{s} (a_i - a_i') g_i \in \langle G \rangle = I$$

(using Corollary 2.5.12). So, if $r - r' \neq 0$, then $L(r - r') \in L(I) = L(G)$. Since $L(r - r')$ is a monomial of r or r', this would mean that r or r' is not reduced with respect to G. ■

Example 2.5.19 *In* Singular *we can compute the reduced Buchberger normal form in Example 2.5.17 by:*

```
ring R=0,(x,y),lp;
ideal I = x2-1,y-1;
```

We first check that the generators of I form a Gröbner basis:

```
I=std(I);
I;
I[1]=x-1
I[2]=x2-1
reduce(x2y+x,I);
x+1
```

The non-reduced version is called by `reduce(-,-,1)`.

Singular *makes the choices in the algorithms for you in a clever way, however, you cannot influence this.*

The standard expression of f respectively uf including the remainder and the unit u is returned by the command **`division`** *(in the stated order):*

```
division(x2y+x,I);
[1]:
_[1,1]=x2
_[2,1]=1
[2]:
_[1]=x+1
[3]:
_[1,1]=1
```

Since we are working with a global ordering, Singular *chooses the unit to be* 1.

Remark 2.5.20 *Even when using a reduced normal form and a Gröbner basis, although the remainder is unique, the generated expression in the generators may not be. In the Examples 2.5.1 and 2.5.17 we obtain*

$$\boldsymbol{x}^2\boldsymbol{y} + x = y \cdot \left(\boldsymbol{x}^2 - 1\right) + 1 \cdot (\boldsymbol{y} - 1) + x + 1$$

and

$$\boldsymbol{x}^2\boldsymbol{y} + x = x^2\,(\boldsymbol{y} - 1) + 1 \cdot \left(\boldsymbol{x}^2 - 1\right) + x + 1$$

respectively.

When dividing f by $G = (g_1, \dots, g_s)$, we can obtain a unique expression

$$f = \textstyle\sum_{i=1}^{s} a_i g_i + r$$

by requiring that no term of $a_i L(g_i)$ is divisible by any $L(g_j)$ for $j < i$.

In the example, the first expression would be returned for $G = (x^2 - 1, y - 1)$, and the second for $G = (y - 1, x^2 - 1)$.

2.6 Computing Standard Bases

In Section 2.2 we have already seen the basic idea for computing a Gröbner basis of an ideal. We will now turn this idea into an algorithm. The formulation will also be applicable in the case of standard bases. So again write $R = K[x_1, \dots, x_n]_>$ for a fixed monomial ordering $>$.

Definition 2.6.1 *The* ***syzygy polynomial*** *or* ***S-polynomial*** *of $f, g \in R$ is defined as*

$$\operatorname{spoly}(f,g) = \frac{\operatorname{lcm}(L(f), L(g))}{LT(f)} f - \frac{\operatorname{lcm}(L(f), L(g))}{LT(g)} g \in R.$$

Doing all possible cancelations of lead terms, Algorithm 2.6 computes a standard basis.

Algorithm 2.6.1 Buchberger

Input: $I = \langle g_1, \dots, g_s\rangle \subset R$ an ideal, $>$ a monomial ordering, and NF a weak normal form.

Output: A standard basis of I with respect to $>$.

```
$G = \{g_1, \dots, g_s\}$
repeat
  $H = G$
  for all $f, g \in H$ do
    $r = \mathrm{NF}(\mathrm{spoly}(f, g), H)$
    if $r \neq 0$ then
      $G = G \cup \{r\}$
until $G = H$
```

Proof. If $r \neq 0$ then $L(r) \notin L(H)$ by Definition 2.5.6(2.), hence

$$L(H) \subsetneqq L(H \cup \{r\}).$$

So, by the Noetherian property of R, the algorithm terminates with $\mathrm{NF}(\mathrm{spoly}(f,g),H) = 0$ for all $f, g \in H$.

To show that the final result is a standard basis, we prove: ∎

Theorem 2.6.2 (Buchberger's criterion) *If $I \subset R$ is an ideal,* NF *a weak normal form and*

$$G = \{g_1, \dots, g_s\} \subset I$$

a set of elements of I with $0 \notin G$, then the following conditions are equivalent:

1) G is a standard basis of I.

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

3) $I = \langle G\rangle$ and $\mathrm{NF}(\mathrm{spoly}(g_i, g_j), G) = 0$ for all $i \neq j$.

Proof. (1) ⇒ (2) ⇒ (3): If G is a standard basis we get $\mathrm{NF}(f,G) = 0$ for all $f \in I$ by Theorem 2.5.10. For the second implication, note that $\mathrm{spoly}(g_i, g_j) \in I$ and by $\mathrm{NF}(f,G) = 0$ and Definition 2.5.6(3') any element of I can be written in terms of the generating system G.

(2) ⇒ (1): If $f \in I$ then again by $\mathrm{NF}(f,G) = 0$ and Definition 2.5.6(3') we have an expression

$$uf = \textstyle\sum_{i=1}^{s} a_i g_i$$

with a unit u and $L(f) = L(uf) \geq L(a_i g_i)$ for all i. So there has to be an i with $L(f) = L(a_i g_i)$, which implies that $L(g_i) \mid L(f)$. Hence $L(f) \in L(G)$.

(3) ⇒ (1): We have to show that if $f \in I$ then $L(f) \in L(G)$. By assumption there are $a_i \in R$ with

$$f = \textstyle\sum_{i=1}^{s} a_i g_i.$$

Clearly $L(f) \le \max_i L(a_i g_i)$. If $L(f) < \max_i L(a_i g_i)$, then some lead terms of summands in $\sum_{i=1}^{s} a_i g_i$ cancel, say $L(a_{i_1} g_{i_1})$ and $L(a_{i_2} g_{i_2})$. By assumption we have a division expression

$$0 = \tilde{u} \cdot \operatorname{spoly}(g_{i_1}, g_{i_2}) - \textstyle\sum_{i=1}^{s} c_i g_i$$

with a unit $\tilde{u}$. Such a relation is called a **syzygy**. Subtracting a multiple of this equality from the equality $f = \sum_{i=1}^{s} a_i g_i$ we obtain a new expression for f with smaller $\max_i L(a_i g_i)$. After finitely many steps $L(f) = \max_i L(a_i g_i)$, hence $L(g_i) \mid L(f)$ for some i, that is, $L(f) \in L(G)$. ∎

For the step (3) ⇒ (1) we have given more like a sketch of a proof. The theory of standard bases for modules will enable us to write down a very elegant proof later.

Example 2.6.3 *Using Buchberger's criterion we can easily check that $G = \{\boldsymbol{x}^2 - 1, \boldsymbol{y} - 1\}$ is a Gröbner basis of $I = \langle G \rangle$ with respect to lp: For the S-pair*

$$s = y(\boldsymbol{x}^2 - 1) - x^2(\boldsymbol{y} - 1) = x^2 - y$$

division with remainder gives $\operatorname{NF}(s, G) = 0$*:*

$$\begin{array}{l l}
\boldsymbol{x}^2 - y = & 1 \cdot (\boldsymbol{x}^2 - 1) - 1 \cdot (\boldsymbol{y} - 1) + 0 \\
x^2 - 1 & \\
\hline
-\boldsymbol{y} + 1 & \\
-y + 1 & \\
\hline
0 &
\end{array}$$

Example 2.6.4 *We apply Buchberger's algorithm to compute a Gröbner basis of*

$$I = \left\langle \boldsymbol{t}^2 - x, \boldsymbol{t}^3 - y, \boldsymbol{t}^4 - z \right\rangle \subset k[t, z, y, x]$$

for the lexicographical ordering $t > z > y > x$. In each step the first column denotes the coefficients in the syzygy polynomial and the second the (reduced) division with remainder.

	↱	$-\boldsymbol{tx} + y$	↱	$-\boldsymbol{t}^2\boldsymbol{x} + z$	↱	$-\boldsymbol{ty} + z$	↱	$\boldsymbol{t}^3\boldsymbol{y} - zx$
$\boldsymbol{t}^2 - x$	t		t^2	x				$-ty$
$\boldsymbol{t}^3 - y$	-1				t			
$\boldsymbol{t}^4 - z$			-1		-1		x	
$\boldsymbol{tx} - y$		1					$-t^3$	$-y$
$\boldsymbol{z} - x^2$				-1		-1		x
$\boldsymbol{ty} - x^2$						1		
$\boldsymbol{y}^2 - x^3$								-1

Writing this in terms of syzygies

$$\begin{pmatrix} \boldsymbol{t}^2 - x \\ \boldsymbol{t}^3 - y \\ \boldsymbol{t}^4 - z \\ \boldsymbol{tx} - y \\ \boldsymbol{z} - x^2 \\ \boldsymbol{ty} - x^2 \\ \boldsymbol{y}^2 - x^3 \end{pmatrix}^t \cdot \begin{pmatrix} t & t^2 + x & 0 & -ty \\ -1 & 0 & t & 0 \\ 0 & -1 & -1 & x \\ 1 & 0 & 0 & -t^3 - y \\ 0 & -1 & -1 & x \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & y^2 - x^3 \end{pmatrix} = 0.$$

As an exercise, do the divisions with remainder and show that all remaining syzygy polynomials reduce to 0*. So a Gröbner basis of* I *is given by*

$$G = (\boldsymbol{t}^2 - x, \boldsymbol{t}^3 - y, \boldsymbol{t}^4 - z, \boldsymbol{tx} - y, \boldsymbol{z} - x^2, \boldsymbol{ty} - x^2, \boldsymbol{y}^2 - x^3).$$

However, do we need all these polynomials?

Definition 2.6.5 *A standard basis* $G = \{g_1, \ldots, g_s\}$ *is called* ***minimal****, if* $L(g_i) \nmid L(g_j)$ *for all* $i \neq j$*.*

If, in addition, $LC(g_i) = 1$ *and* $\operatorname{tail}(g_i)$ *is reduced with respect to* G *for all* i*, then,* G *is called* ***reduced****.*

Remark 2.6.6 *From any standard basis we can obtain a minimal one by deleting elements.*

Proof. Given a standard basis $G = \{g_1, \ldots, g_s\}$, by Lemma 2.3.3, the set $\{L(g_i) \mid i\}$ has a unique subset of minimal elements with respect to divisibility. This subset also generates $L(G)$, and, hence, the corresponding g_i form a standard basis. ■

Remark 2.6.7 *A minimal standard basis is minimal in the sense that we cannot delete any element without loosing the standard basis property.*

Theorem 2.6.8 *Let* $>$ *be a global ordering. Every ideal has a unique reduced Gröbner basis (up to permutation of the elements).*

Proof. Suppose G and H are reduced Gröbner bases of the ideal I. By

$$L(G) = L(I) = L(H)$$

and since G and H are minimal, for any $g \in G$ there is an $h \in H$ with $L(g) = L(h)$. Then

$$s = g - h = \operatorname{tail}(g) - \operatorname{tail}(h)$$

and, as no term of the tails is divisible by any lead term, we have

$$s = \mathrm{NF}(s, G).$$

Finally $s = \mathrm{NF}(s, G) = 0$ by the Ideal Membership Theorem 2.5.10 and $s \in I$. ■

Remark 2.6.9 *Fix a global ordering $>$. If $G = \{g_1, \dots, g_s\}$ is minimal and* NF *is a reduced normal form, then $H = \{h_1, \dots, h_s\}$ with*

$$h_i = \mathrm{NF}(g_i, (g_1, \dots, g_{i-1}, g_{i+1}, \dots, g_s))$$

is the reduced Gröbner basis of I.

Proof. If G is minimal, then $L(g_i)$ is not divisible by any $L(g_j)$ for $i \neq j$, so $L(g_i) = L(h_i)$. By construction, $\mathrm{tail}(h_i)$ is reduced with respect to h_j for $j \neq i$. Moreover, no term of $\mathrm{tail}(h_i)$ is divisible by $L(h_i)$, since by Definition and Theorem 2.3.2 the global ordering refines divisibility. ■

Example 2.6.10 *In Example 2.6.4 a minimal Gröbner basis is*

$$G = \{\boldsymbol{t}^2 - x, \boldsymbol{tx} - y, \boldsymbol{z} - x^2, \boldsymbol{ty} - x^2, \boldsymbol{y}^2 - x^3\}.$$

Example 2.6.11 *For Example 2.6.4 we can compute a minimal Gröbner basis using* Singular *as follows:*

```
ring R=0,(t,z,y,x),lp;
ideal I = t2-x,t3-y,t4-z;
std(I);
_[1]=y2-x3
_[2]=z-x2
_[3]=tx-y
_[4]=ty-x2
_[5]=t2-x
```

In this example, the result is already reduced.

Example 2.6.12 *In general, the Gröbner basis returned* `std` *may not be reduced. To force* Singular *to compute the reduced Gröbner basis, we set the option* `redSB`*:*

```
ring R=0,(x,y),lp;
ideal I = x+y,y;
std(I);
_[1]=y
```

```
_[2]=x+y
option(redSB);
std(I);
_[1]=y
_[2]=x
```