Computer Algebra

Lecture Notes, Summer Term 2017

Janko Böhm

April 30, 2017

Contents

List of Figures

List of Symbols

1

Introduction

1.1 What is computer algebra and why should we do it?

Computer algebra has two fundamental goals: Provide algorithms for computations with algebraic structures, like fields, vector spaces, rings, ideals, and modules to the computer. And use the algorithms and their implementations to solve mathematical problems in theory and applications. Here, computations usually refer to exact, that is, symbolic ones. However, in some cases, numerical computations can be helpful in obtaining exact results.

So why is it useful to implement algebra in the computer? Of course, there are practical problems, that can be solved by computer algebra, for example, in cryptography, robotics, algebraic statistics, computational biology, and physics. On the other hand, experiments with the computer allow you to get an insight into theoretical problems and test conjectures. In many settings, you can even obtain theoretical results by handling just a single special case by computer. Let us say, we want to prove that the determinant of the matrix

$$A_t = \begin{pmatrix} t-1 & 1 & -1 \\ t & t^2+1 & t+1 \\ t & t^2 & t+2 \end{pmatrix} \in \mathbb{C}[t]^{3\times 3}$$

is non-zero as a polynomial without computing it. For example, the determinant may be too complicated (which is of course not the case in the example). However, it may be possible to compute A_{t_0} for a fixed $t_0 \in \mathbb{C}$. Since substitution is a ring homomorphism,

it is sufficient to find one t_0 such that $\det A_{t_0} \neq 0$, for example,

$$\det A_0 = \det \begin{pmatrix} -1 & 1 & -1 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix} = -2$$

It follows that the determinant, as a continuous function, will be non-zero in an open neighbourhood of t_0. In fact, we then know that it is non-zero for all but finitely many values of t, since $0 \neq \det A_t \in \mathbb{C}[t]$ has only finitely many zeros. This means that the determinant is non-zero on an open set in the so called Zariski topology, that is, on the complement of the zero set of a system of polynomial equations.

In the line of this example, our main focus will be on computations in commutative algebra, specifically on all sorts of algorithms concerned with polynomial rings. Here, the fundamental building block is **Buchberger's algorithm** for computing **Gröbner bases**, which generalizes **Gaussian elimination**. Recall that Gaussian elimination transforms multivariate linear systems of equations into row echelon form

$$\begin{array}{rcrcr} 2x & + & y & = & 1 \\ x & + & 2y & = & -1 \end{array} \quad \mapsto \quad \begin{array}{rcrcr} 2x & + & y & = & 1 \\ -3x & & & = & -3 \end{array}$$

(see Figure 1.1), from which we can read off the solution $(x, y) = (1, -1)$.

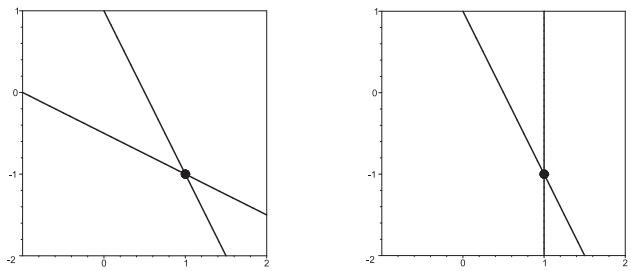

Figure 1.1: Gaussian elimination for the intersection of two lines

Buchberger's algorithm generalizes this idea to higher degree polynomial equations, for example, it transforms

$$\begin{array}{r} 2x^2 - xy + 2y^2 - 2 = 0 \\ 2x^2 - 3xy + 3y^2 - 2 = 0 \end{array} \quad \mapsto \quad \begin{array}{r} 3y + 8x^3 - 8x = 0 \\ 4x^4 - 5x^2 + 1 = 0 \end{array}$$

For most computations we will use the open source computer algebra system Singular [4], which is being developed at TU Kaisers-

lautern. SINGULAR can be either downloaded or conveniently accessed in an online interface.[1]

Example 1.1.1 *We can do the above Gröbner basis calculation in* SINGULAR *by the following code:*

```
ring R=0,(y,x),lp;
ideal I = 2x2-xy+2y2-2, 2x2-3xy+3y2-2;
std(I);
_[1]=4x4-5x2+1
_[2]=3y+8x3-8x
```

The ring definition specifies the characteristic of the prime field (so 0 corresponds to $\mathbb{Q}$), the variables, and an ordering of the variables (lp). To make an analogy to Gaussian elimination, by the ordering you can tell the system, in which order you want to eliminate the variables (for example, if you want a right or left upper triangular matrix as row echelon form). An ideal represents a system of polynomial equations, and `std` refers to the term **standard basis**, which, in the setup considered here, is synonymous to Gröbner basis. From the resulting system we can read off the four solutions $(x, y) = (\pm 1, 0), (\pm\frac{1}{2}, \pm 1)$, see Figure 1.2.

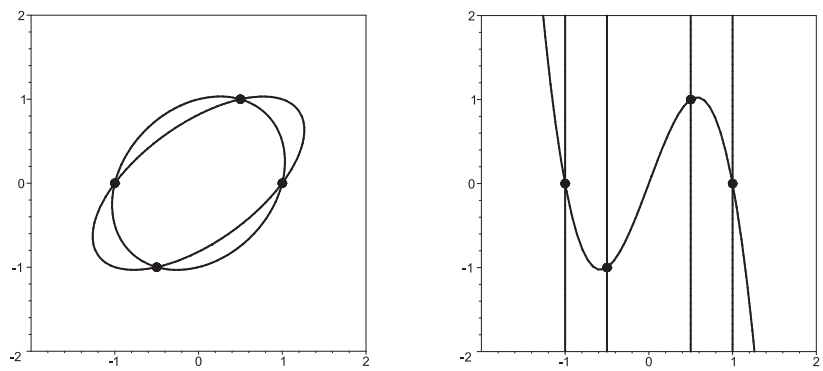

Figure 1.2: Buchberger's algorithm for the intersection of two ellipses

Example 1.1.2 *These plots can be generated in the general purpose (commercial) computer algebra system* MAPLE *[12] by the code*

```
with(plots):
p1:=implicitplot(2*x^2-x*y+2*y^2-2,x=-2..2,y=-2..2):
p2:=implicitplot(2*x^2-3*x*y+3*y^2-2,x=-2..2,y=-2..2):
```

[1] See https://www.singular.uni-kl.de:8003/

```
display(p1,p2,view=[-2..2,-2..2],thickness=2);
p3:=implicitplot(4*x^4-5*x^2+1,x=-2..2,y=-2..2):
p4:=implicitplot(2*x^2-3*x*y+3*y^2-2,x=-2..2,y=-2..2):
display(p3,p4,view=[-2..2,-2..2],thickness=2);
```

As already done in these two plots, we will motivate the algebraic concepts by connecting multivariate systems of polynomial equations to the geometry of their set of solutions, the associated **algebraic variety**. This connection is called **algebraic geometry**, an important branch of mathematics and one of the key applications of commutative algebra. Of course algebraic varieties can get much more interesting than 4 points. First of all, they can have higher dimension, for example, the ellipses considered above have dimension 1 and are called **curves**. One algebraic equation in three variables will give you an example of what is called an algebraic **surface**, that is, a variety of dimension 2. We will learn about an algebraic characterization of the dimension of an algebraic variety using Gröbner bases. Another interesting feature algebraic varieties can have are **singularities**, which are points that do not have a well-defined tangent plane. Considering as an example the hyperboloids $H_t \subset \mathbb{R}^3$ given

$$x^2 + y^2 - z^2 + t = 0$$

varying with the parameter $t \in \mathbb{R}$, the tangent plane at the point (x, y, z) is given by the affine space

$$(x, y, z) + \ker(x, y, -z),$$

since $(x, y, -z)$ is the normal vector of the surface at that point. So every point of H_t has a well-defined tangent plane, provided $t \neq 0$. However, if $t = 0$, then $(0, 0, 0)$ lies on the hyperboloid (which now becomes a double cone) and at this point the dimension of the kernel is not 2 but 3. So H_t is non-singular for $t \neq 0$, but has a singularity at $(0, 0, 0)$ for $t = 0$, see Figure 1.3. These plots were generated by the visualization tool Surfer [8], which provides an easy-to-use graphical interface to the raytracing program Surf [6] for plotting algebraic surfaces in 3-space. It can also be called from Singular.

Using this tool, also Figure 1.4 was generated, which shows the **Kummer quartic surface** in 3-space, which has the maximum number 16 of isolated singularities, a surface given by polynomial of degree 4 in 3 variables can have.

If you look closely, you see that the configuration of singularities of the Kummer quartic is invariant under the symmetry group of the

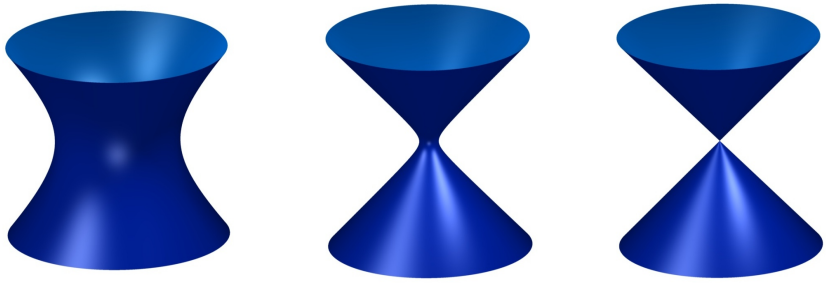

Figure 1.3: Hyperboloids and double cone

Figure 1.4: Kummer quartic

tetrahedron (which is S_4), see Figure 1.5. The **Togliatti quintic** shown in Figure 1.6 has the maximum number of 31 singularities, which a degree 5 surface can have and comes with the symmetry of a 5-gon. Again, the **Barth sextic** has the maximum number of 65 singularities on a degree 6 surface, see Figure 1.7. It comes with the symmetry of an icosahedron, see Figure 1.8.

Before turning to a short summary of the algebraic and geometric foundations necessary for the things to come, we take a quick look of what else is out there in computer algebra. This appetizer to computer algebra in number theory, group theory, calculus and algebraic geometry will hopefully stimulate the appetite at the beginning of the meal.

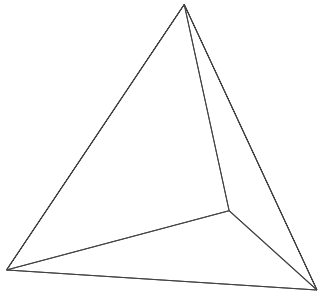

Figure 1.5: Tetrahedron

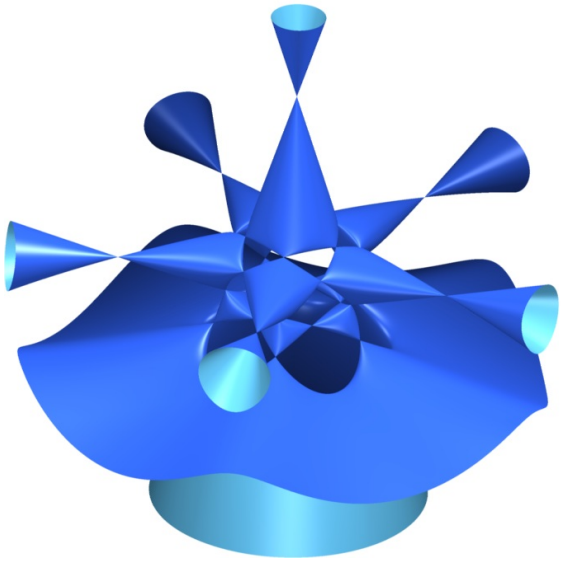

Figure 1.6: Togliatti quintic

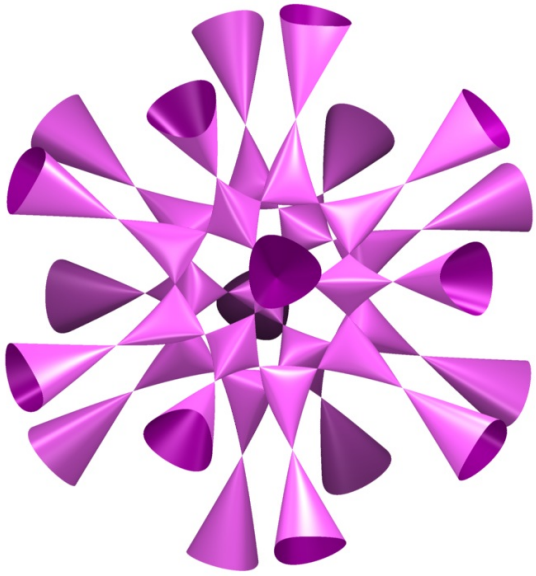

Figure 1.7: Barth sextic

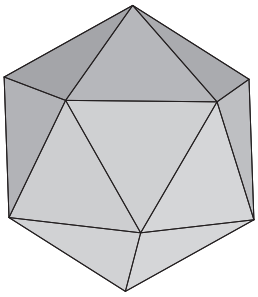

Figure 1.8: Icosahedron

1.2 Numbers

One of the most important algorithms in mathematics is Euclidean algorithm for finding the greatest common divisor. In a generalized form, it will be present explicitly or implicitly in many algorithms we will discuss later on. So let us invest a little bit of time in a reminder on the remainder.

Lemma 1.2.1 (Division with remainder) *For $a, b \in \mathbb{Z}$, $b \neq 0$, there are $q, r \in \mathbb{Z}$ with*

$$a = b \cdot q + r$$

and $0 \leq r < |b|$.

Proof. Without loss of generality $b > 0$. The set

$$\{w \in \mathbb{Z} \mid b \cdot w > a\} \neq \varnothing$$

has a smallest element w. Then set

$$q := w - 1 \qquad r := a - qb$$

■

Theorem 1.2.2 (Euclidean Algorithm) *Suppose* $a_1, a_2 \in \mathbb{Z} \setminus \{0\}$. *Successive division with remainder terminates*

$$\begin{aligned} a_1 &= q_1 a_2 + a_3 \\ &\vdots \\ a_j &= q_j a_{j+1} + a_{j+2} \\ &\vdots \\ a_{n-2} &= q_{n-2} a_{n-1} + a_n \\ a_{n-1} &= q_{n-1} a_n + 0 \end{aligned}$$

and

$$\gcd(a_1, a_2) = a_n.$$

Reading the equations backwards

$$\begin{aligned} a_n &= a_{n-2} - q_{n-2} a_{n-1} \\ &\vdots \\ a_3 &= a_1 - q_1 a_2 \end{aligned}$$

gives a representation

$$\gcd(a_1, a_2) = x \cdot a_1 + y \cdot a_2$$

with $x, y \in \mathbb{Z}$.

Proof. We have $|a_{i+1}| < |a_i|$ for $i \geq 2$ so after finitely many steps $a_i = 0$. Then a_n divides a_{n-1}, hence also $a_{n-2} = q_{n-2} a_{n-1} + a_n$ and inductively $a_{n-2}, \ldots, a_1$. If t is a divisor of a_1 and a_2, then also of $a_3, \ldots, a_n$. ■

Example 1.2.3 *We compute the gcd of* 36 *and* 15*:*

$$\begin{aligned} 36 &= 2 \cdot 15 + 6 \\ 15 &= 2 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0 \end{aligned}$$

hence $\gcd(36, 15) = 3$. *Furthermore, we can express* $\gcd(36, 15)$ *as a* $\mathbb{Z}$ *linear combination of* 36 *and* 15*:*

$$3 = 15 - 2 \cdot 6 = 15 - 2 \cdot (36 - 2 \cdot 15) = 5 \cdot 15 + (-2) \cdot 36$$

Many other number theoretic concepts will show up later in a more general context, for example, factorization in the context of primary decomposition.

Definition 1.2.4 *An element $p \in \mathbb{Z}_{>1}$ is called* ***prime number****, if $p = a \cdot b$, $a, b \in \mathbb{Z}_{\geq 1}$ implies $a = 1$ or $b = 1$.*

Theorem 1.2.5 (Fundamental theorem of arithmetic) *Every number $n \in \mathbb{Z} \setminus \{0, 1, -1\}$ has a unique representation*

$$n = \pm 1 \cdot p_1^{r_1} \cdot \ldots \cdot p_r^{r_r}$$

with ***prime factors*** *$p_1 < \ldots < p_r$ and $r_i \in \mathbb{N}$.*

Algorithm 1.2.6 (Trial division) *Let $n \in \mathbb{Z}$ be composite. The smallest prime factor p of n satisfies*

$$p \leq m := \left\lfloor \sqrt{n} \right\rfloor.$$

If we know all primes $p \leq m$, then we can test $p \mid n$ by division with remainder and, hence, factor n.

Algorithm 1.2.7 (Sieve of Eratosthenes) *We can find all prime numbers smaller than n in the following way: Note all numbers from 2 to n. Starting with $p = 2$, delete all $a \cdot p$ for $a > 1$, and continue with the next largest number p which not has been deleted. Note that p is prime, since it is not a multiple of smaller prime. Stop if $p > \sqrt{n}$.*

We will discuss in Exercise 1.3 an analogue of this in the case of univariate polynomials.

Example 1.2.8 *We compute all primes ≤ 15*

2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	3		5		7		9		11		13		15
2	3		5		7				11		13		

In the first step we delete all multiples of 2, in the second step all multiples of 3. All remaining numbers are prime, since $5 > \sqrt{15}$.

One can even describe the distribution of the primes over all integers:

Theorem 1.2.9 (Prime number theorem) *For $x \in \mathbb{R}_{>0}$ let*

$$\pi(x) = |\{p \leq x \mid p \in \mathbb{N} \text{ prime}\}|$$

Then

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} = 1$$

In Exercise 1.4 we will test the prime number theorem.

Computer algebra in this spirit has many theoretical applications in number theory and algebraic geometry and practical applications, for example, in coding theory or RSA public key cryptography.

In general, number theory explores the properties of numbers, most importantly the interaction of addition and multiplication. This leads to many problems which are easy to formulate, but highly non-trivial to solve. The most famous one is Fermat's last theorem of 1637: There is no (non-trivial) integer solution of the equation

$$x^n + y^n = z^n$$

for $n \geq 3$. With the help of a computer one can test Fermat's last theorem for very large n (using the theoretical result that you only have to test it for so called irregular primes). Fermat's last theorem was finally proven in 1995 (by A. Wiles) after 350 years of work of many people, which led to many new concepts in mathematics. One of the leading systems in number theory is PARI/GP, see [15]. It can calculate, for example, with p-adic numbers, which have played an important role in the proof of Fermat's last theorem. Like we do with power series, we consider two numbers as close to each other, if they differ by a high power of a prime.

Example 1.2.10 *Using the prime $p = 7$ up to powers less than 5 we calculate in* PARI/GP *the square root of 569:*

```
gp > n=569 + O(7^5)
%1 = 2 + 4*7 + 4*7^2 + 7^3 + O(7^5)
gp > sqrt(n)
%2 = 3 + 4*7 + 7^2 + 3*7^3 + 7^4 + O(7^5)
gp > factor((3 + 4*7 + 7^2 + 3*7^3 + 7^4)^2-569)
%2 = [7 5]  [733 1]
```

so we observe, that

$$\left(3 + 4 \cdot 7 + 7^2 + 3 \cdot 7^3 + 7^4\right)^2 - 569 = 12\,319\,531 = 733 \cdot 7^5.$$

Also MAPLE has very efficient implementations of algorithms in number theory:

Example 1.2.11 *Using* MAPLE *you can easily show, that the n-th Fermat number $F_n = 2^{2^n} + 1$ is prime for $0 \leq n \leq 4$ and composite for $5 \leq n \leq 8$, for example:*

```
> ifactor((2^(2^6)+1))
274177 * 67280421310721
```

Using distributed computing one can take this a little bit further. However, it is unknown, whether there are more Fermat primes than the 5 *known ones. See also Exercise 1.4.*

1.3 Groups

The concept of groups has important applications in almost every field of mathematics, including algebraic geometry and commutative algebra. It allows us to describe symmetries in mathematical objects and problems, reducing a more complicated problem to a simpler one. From the practical point of view this can speed up computations.

Consider, for example, the symmetry group G of the octahedron (Figure 1.9), which contains all rotations, reflections, and rotoreflections, which map the octahedron to itself. Numbering the vertices,

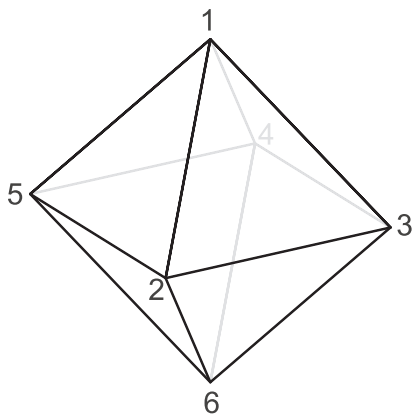

Figure 1.9: Octahedron

we can identify any symmetry with an element of the symmetric group S_6. For example, the rotation by 90 degrees along the axis through 1 and 6 is given by $(2,3,4,5) \in S_6$ using cycle notation.

Let us say, we want to compute the stabilizers of the vertices of the octahedron, that is, the subgroups

$$\mathrm{Stab}(j) = \{\sigma \in G \mid \sigma(j) = j\}\,.$$

By the action of G, it is sufficient to determine $\mathrm{Stab}(1)$, since all stabilizers can be identified by conjugation of groups

$$\mathrm{Stab}(j) = \sigma^{-1}\,\mathrm{Stab}(1)\sigma,$$

where $\sigma \in G$ with $1 = \sigma(j)$. So instead of 6 computations, by taking the symmetry of the problem into account, we only have to do one.

To compute the group order of $\mathrm{Stab}(1)$, we use:

Theorem 1.3.1 (Orbit-counting theorem) *Let G be a group acting on a set X by*

$$G \times X \to X$$

(that is, $ex = x$ and $(g \circ h)x = g(hx)$ for all $x \in X$ and $g, h \in G$). Fix $x \in X$ and write

$$Gx = \{gx \mid g \in G\}$$

*for the **orbit** of x and*

$$\mathrm{Stab}(x) = \{g \in G \mid gx = x\}.$$

*for the **stabilizer** of x. Then*

$$|G| = |Gx| \cdot |\mathrm{Stab}(x)|.$$

Hence

$$|\mathrm{Stab}(1)| = \frac{|G|}{6},$$

and, if p is a point which does not lie on any symmetry plane or axis,

$$|G| = |\mathrm{Stab}(p)| \cdot |Gp| = 1 \cdot (6 \cdot 8) = 48,$$

see Figure 1.10, so

$$|\mathrm{Stab}(1)| = 8.$$

It is easy to guess elements of G and $\mathrm{Stab}(1)$, but how do we know,

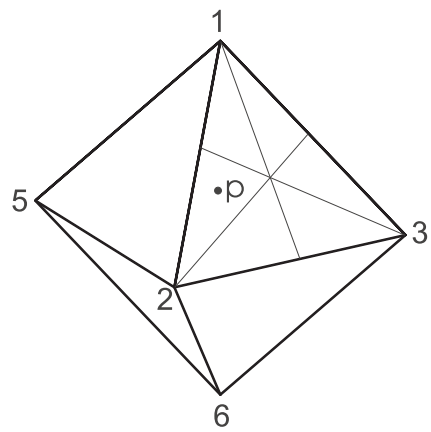

Figure 1.10: Generic point on octahedron.

whether they really generate the respective groups, equivalently, that they generate groups of the correct order? We can leave this tedious calculation to the open source computer algebra system GAP [14], the leading software for group theory:

Example 1.3.2 *We use* GAP *to prove that*

$$\mathrm{Stab}(1) = \langle (2,3,4,5), (2,4) \rangle$$

```
gap> Stab1:=Group((2,3,4,5),(2,4));;
gap> Size(Stab1);
8
gap> Elements(Stab1);
[(),(3,5),(2,3)(4,5),(2,3,4,5),(2,4),(2,4)(3,5),
(2,5,4,3),(2,5)(3,4)]
```

In the same way, we can find generators of the whole symmetry group:

```
gap> G:=Group((2,3,4,5),(1,3)(5,6));;
gap> Size(G);
48
```

Hence

$$G = \langle (2,3,4,5), (1,3)(5,6) \rangle .$$

See Exercise 1.5 for the symmetry group of the icosahedron.

GAP implements algorithms for computing with subgroups of symmetric groups. As we have seen, given a set of generators, it can determine the group order, and the set of all elements. It can also determine, whether two such groups are isomorphic, and specify an isomorphism. Computing inside symmetric groups seems like a restriction, however, this is sufficient for many purposes, because of the following:

Theorem 1.3.3 (Cayley) *Every group G is isomorphic to a subgroup of the group $S(G)$ of bijections $G \to G$.*

Proof. The action of G on itself induced by the group operation

$$\begin{aligned} G \times G &\longrightarrow G \\ (g,h) &\mapsto g \circ h \end{aligned}$$

yields a group homomorphism

$$\begin{array}{rccc} \varphi\colon & G & \to & S(G) \\ & g & \mapsto & \left(\begin{array}{ccc} G & \to & G \\ h & \mapsto & g \circ h \end{array} \right) \end{array}$$

and since

$$\mathrm{Ker}(\varphi) = \{g \in G \mid gh = h \ \forall h \in G\} = \{e\}$$

φ is injective. So by the homomorphism theorem

$$G = G/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi) \subset S(G).$$

■

For finite groups this just amounts to writing down the group table. For $g \in G$ the bijection $\varphi(g)$ maps the e-th row of the group table to the g-th row.

Example 1.3.4 *For* $G = \mathbb{Z}/3 = \left\{\overline{0}, \overline{1}, \overline{2}\right\}$ *with group table*

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

we have

$$\varphi(\overline{1}) = (\overline{0}, \overline{1}, \overline{2}) \in S(G)$$

using cycle notation.

1.4 Symbolic Integration

In addition to the specialized systems like Singular, Gap and Pari/gp, there are general purpose computer algebra systems like the commercial systems Maple [12], and Mathematica [16], and the open source systems Maxima [13], Reduce [10], and Axiom [2]. They are usually less powerful in the specific areas, but provide a larger set of algorithms to manipulate symbolic expressions. Most noteably there is **Risch's algorithm** for symbolic integration of functions which are compositions of rational functions, exponentials, logarithm, radicals, and trigonometric functions. It is based on the theorem of Liouville, which uses the following definitions: A **differential field** is field K with a differentiation map $K \to K$, $f \mapsto f'$, which satisfies the usual rules $(f+g)' = f' + g'$ and $(fg)' = f'g + fg'$. Denote by $\mathrm{Const}(K) = \{f \in K \mid f' = 0\}$ its **subfield of constants**. An **elementary extension** $K \subset E$ is a field extension, which can be obtained by a sequence of extensions, which are either algebraic, **exponential**, that is, transcendental of the form $F \subset F(g)$ with

$$g' = g \cdot f'$$

for some $f \in K$, or **logarithmic**, that is, transcendental of the form $F \subset F(g)$ with

$$g' = \frac{f'}{f}$$

for some $f \in K$.

Theorem 1.4.1 (Liouville) *Let K be a differential field with field of constants $C = \mathrm{Const}(K)$, and $F \in K$. If there is an elementary extension $K \subset E$ and $G \in E$ with*

$$G' = F$$

then there are constants $c_1, ..., c_n \in \overline{C}$ in an algebraic field extension of C, and functions $v \in K$, $u_1, ..., u_n \in K(c_1, ..., c_n)$ such that

$$G = v + \sum_i a_i \ln u_i.$$

This tells us, that if an elementary function has an elementary integral, then this integral can be written in the functions used to write down the integrand and their logarithms. Based on this observation, Risch's algorithm decides the existence of G, and computes G, if it exists. However note, that the only almost complete implementation of Risch's algorithm is that of Axiom.

Example 1.4.2 *We have $\int x^n dx = \frac{1}{n+1} x^{n+1}$ provided $n \neq -1$ and $\int \frac{1}{x} dx = \ln x$. On the other hand, the function e^{-x^2} does not have an elementary integral.*

Example 1.4.3 *We compute the area A inside the ellipse*

$$\left(\frac{x}{a}\right)^2 + \left(\frac{y}{b}\right)^2 = 1$$

using Maple*:*
F:=`int(2*b/a*sqrt(a^2-x^2),x);`
`F:=b/a*sqrt(a^2-x^2)*x+a*b*arctan(x/sqrt(a^2-x^2))`
and hence $A = \pi ab$.

In this spirit, general purpose computer algebra systems are heavily used for solving differential equations and, hence are very popular in physics (most noteably Reduce).

Example 1.4.4 *Consider the damped harmonic oscillator described by the ordinary differential equation (ODE)*

$$x''(t) = -a \cdot x(t) - b \cdot x'(t).$$

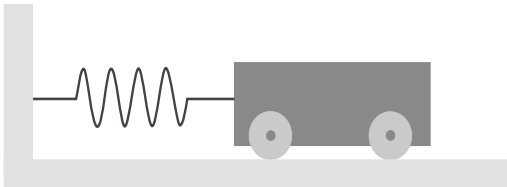

Figure 1.11: Harmonic oscillator

Here t is the time, $x(t)$ the position, $x'(t)$ the speed, and $x''(t)$ the acceleration of the object, see Figure 1.11.

Choosing the parameters $a = 5$ and $b = 1$, and the boundary conditions $x(0) = 1$ (starting position) and $x'(0) = 1$ (starting speed) we solve this differential equation using MAPLE*:*

```
ode := diff(x(t),t$2)+diff(x(t),t)+5*x(t);
```

$\frac{d^2}{dt^2}x(t) + \frac{d}{dt}x(t) + 5 \cdot x(t)$

```
dsolve(ode);
```

$x(t) = C_1 e^{-\frac{1}{2}t} \sin(\frac{\sqrt{19}}{2}t) + C_2 e^{-\frac{1}{2}t} \cos(\frac{\sqrt{19}}{2}t)$

```
f:=subs({_C1=1,_C2=1},subs(%,x(t)));
```

$f := e^{-\frac{1}{2}t} \sin(\frac{\sqrt{19}}{2}t) + e^{-\frac{1}{2}t} \cos(\frac{\sqrt{19}}{2}t)$

```
plot(f,t=0..5);
```

The plot command will generate Figure 1.12 showing the solution $x(t)$.

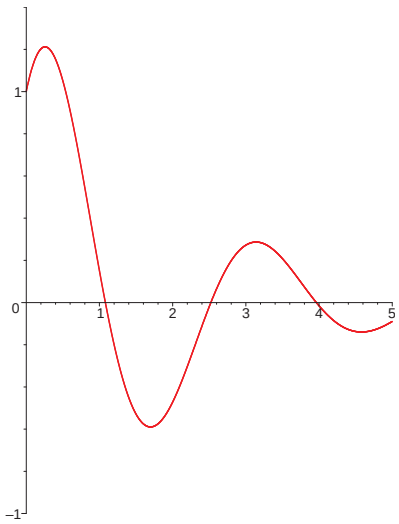

Figure 1.12: Solution to the harmonic oscillator

1.5 Linear Algebra

In addition to the Euclidean algorithm, the second key algorithm generalized by Buchberger's algorithm is Gaussian reduction. We can reformulate Gaussian reduction on a homogeneous linear system of equations over a field K in the following way:

Algorithm 1.5.1 (Gauss) *Consider non-zero homogeneous linear polynomials $f_1, ..., f_n \in K[x_1, ..., x_m]$. Choose an ordering of the variables (without loss of generality $x_1 > x_2 > ... > x_m$). Define $\mathrm{L}(f_i)$ as the largest monomial of f_i and by $\mathrm{LC}(f_i)$ its coefficient.*

As long as there are f_i and f_j with $\mathrm{L}(f_i) = \mathrm{L}(f_j)$ replace f_j by the ***S-pair***

$$\mathrm{spoly}(f_i, f_j) = \mathrm{LC}(f_i) \cdot f_j - \mathrm{LC}(f_j) \cdot f_i.$$

If $f_j = 0$ then delete f_j.

Sort the set of f_j by the size of $\mathrm{L}(f_j)$.

This algorithm terminates with a row echelon form. If we reduce the resulting polynomials by those with smaller lead monomials, and divide all polynomials by their lead coefficients, we obtain the (unique) reduced row echelon form. When discussing Gröbner bases, we will see how the special case of linear equations generalizes to the higher degree setup.

Example 1.5.2 *We solve the system*

$$\begin{array}{lcllllllllll}
f_1 & = & x_1 & + & x_2 & & & & & + & x_5 & = & 0 \\
f_2 & = & x_1 & + & x_2 & + & 2x_3 & + & 2x_4 & + & x_5 & = & 0 \\
f_3 & = & x_1 & + & x_2 & + & x_3 & + & x_4 & + & x_5 & = & 0
\end{array}$$

Gaussian elimination yields

$$\begin{array}{lcllllllllll}
f_1 & = & x_1 & + & x_2 & + & & & & + & x_5 & = & 0 \\
\mathrm{spoly}(f_1, f_2) & = & & & & & 2x_3 & + & 2x_4 & & & = & 0 \\
\mathrm{spoly}(f_1, f_3) & = & & & & & x_3 & + & x_4 & & & = & 0
\end{array}$$

and, since the S-pair of the last two vanishes

$$\begin{array}{lllllllllll}
x_1 & + & x_2 & + & & & & + & x_5 & = & 0 \\
& & & & 2x_3 & + & 2x_4 & & & = & 0
\end{array}$$

Using matrix notation, we can do the Gaussian elimination in Maple *by the following code:*

```
with(LinearAlgebra):
```

```
A := <<1,1,1>|<1,1,1>|<0,2,1>|<0,2,1>|<1,1,1>>:
GaussianElimination(A);
```

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Utilizing the Gröbner basis engine of SINGULAR, *we can do the same computation as follows:*

```
ring R = 0,(x(1..5)),lp;
ideal I = x(1) + x(2) + x(5),
x(1) + x(2) + 2*x(3) + 2*x(4) + x(5),
x(1) + x(2) + x(3) + x(4) + x(5);
option(redSB);
std(I);
_[1] = x(3) + x(4)
_[2] = x(1) + x(2) + x(5)
```

See also Exercise 1.6.

Remark 1.5.3 *Solving an inhomogeneous linear system of equations*

$$f_i = \sum_j a_{ij}x_j - c_i = 0$$

can be reduced to the homogeneous case by homogenizing the system to

$$f_i = \sum_j a_{ij}x_j - c_i y = 0$$

with a homogenization variable y. See also Exercise 1.7. We will come back to this idea later in the context of higher degree polynomial equations.

1.6 Algebraic Geometry

If we pass from linear systems to polynomial equations of higher degree things become much more interesting. Algebraic geometry studies the set of solutions of such systems. It will be the main motivation of the algorithms we encounter in commutative algebra.

Definition 1.6.1 *The **affine space** of dimension n over the field K is defined as*

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

By this notation we express that we (usually) do not care about the structure of K^n as a K-vector space.

Definition 1.6.2 *An* ***affine algebraic set*** *is the common zero set*

$$V(f_1, ..., f_r) = \{p \in \mathbb{A}^n(K) \mid f_1(p) = 0, ..., f_r(p) = 0\}$$

of polynomials $f_1, ..., f_r \in K[x_1, ..., x_n]$.

An affine algebraic set X *is called* ***irreducible****, if it cannot be written as* $X = X_1 \cup X_2$ *with affine algebraic sets* $X_i \subsetneqq X$. *Then we also call* X *an* ***affine algebraic variety****.*

Example 1.6.3 *Affine algebraic varieties commonly known also outside algebraic geometry are* $V(1) = \varnothing$, $V(0) = K^n$, *the set of solutions of a linear system of equations*

$$A \cdot x - b = 0$$

or the graph

$$\Gamma(g) = V(x_2 \cdot b(x_1) - a(x_1)) \subset \mathbb{A}^2(K)$$

of a rational function

$$g = \frac{a}{b} \in K(x_1).$$

For example, the graph of $g(x_1) = \frac{x_1^3 - 1}{x_1}$ *is*

$$V\left(x_2 x_1 - x_1^3 + 1\right) \subset \mathbb{A}^2(K),$$

as depicted in Figure 1.13 for $K = \mathbb{R}$.

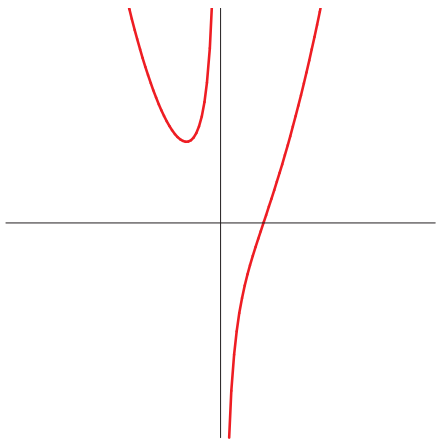

Figure 1.13: Graph of a rational function.

Example 1.6.4 *If $f \in K[x_1, ..., x_n]$ is non-zero and non-constant, then $V(f) \subset \mathbb{A}^n(K)$ is called a* ***hypersurface****. For example, the surfaces shown in the Figures 1.4, 1.6, and 1.7 are hypersurfaces in $\mathbb{A}^3(\mathbb{R})$.*

Note, that $V(f)$ is irreducible, if and only if f is irreducible. In Exercise 1.10 we will discuss, in the case that K is a finite field, a probabilistic test for checking whether f is irreducible.

For the remainder of this section we will take a closer look at elliptic curves. After that, we will discuss the algorithmic foundation for computating with algebraic sets in the next chapter.

Example 1.6.5 *Not every curve in $\mathbb{A}^2(K)$ is a graph, for example, the circle*

$$V(x_1^2 + x_2^2 - 1) \subset \mathbb{A}^2(\mathbb{R})$$

or the elliptic curve

$$V(x_2^2 - x_1^3 - x_1^2 + 2x_1 - 1) \subset \mathbb{A}^2(\mathbb{R})$$

are not, see Figure 1.14.

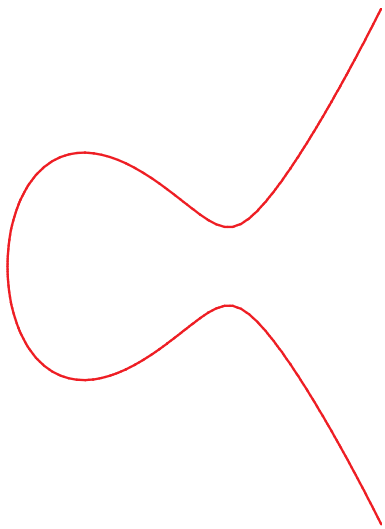

Figure 1.14: Elliptic curve

Example 1.6.6 *In general, an* ***elliptic curve*** *is of the form $E = V(f)$ where $f \in K[x_1, x_2]$ is an irreducible polynomial of degree 3 and $V\left(f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right) = \varnothing$, which guarantees that the curve does not have a singularity. The set of points of an elliptic curve has the*

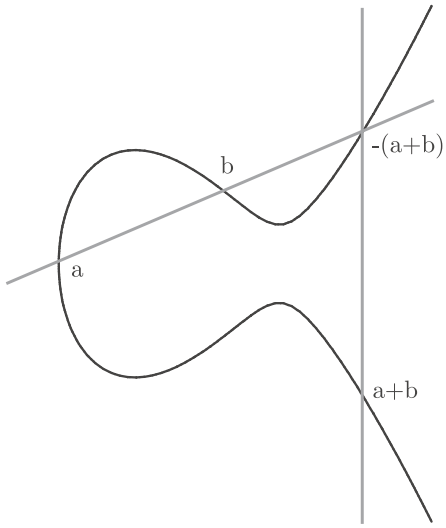

Figure 1.15: Group structure on an elliptic curve.

following remarkable property: It comes with the structure of an abelian group with the operation as specified in Figure 1.15. Can you tell what is the neutral element?

Example 1.6.7 *If we consider elliptic curves over the field* $\mathbb{Q}$

$$E(\mathbb{Q}) = \left\{p \in \mathbb{A}^2(\mathbb{Q}) \mid f(p) = 0\right\}$$

(also called the $\mathbb{Q}$***-rational points*** *of the elliptic curve over* $\mathbb{C}$*), we close the circle back to number theory: The Theorem of Mordell shows, that* $E(\mathbb{Q})$ *as a group is finitely generated. The structure of a finitely generated group is known: It is the product of factors* $\mathbb{Z}$ *and* $\mathbb{Z}/n$ *(that is, of cyclic groups). The question about the number of* $\mathbb{Z}$*-factors of* $E(\mathbb{Q})$ *is the topic of ongoing research (for example, on the conjecture of Birch and Swinnerton-Dyer, which in fact is based on computer experiments, and is one of the one million dollar problems).*

An important application of elliptic curves is public-key cryptography. Given a crypto system based on the discrete logarithm in the prime residue class group $\mathbb{F}_p^\times$ (like Diffie-Hellman key exchange), one can replace $\mathbb{F}_p^\times$ by the group $E(\mathbb{F}_p) \subset \mathbb{A}^2(\mathbb{F}_p)$ of points of an elliptic curve over a finite field $\mathbb{F}_p$. This allows one to achieve the same strength with a much smaller key size.

One can show that (for $p \geq 5$) in a suitable coordinate system every elliptic curve can be written as

$$E(\mathbb{F}_p) = \left\{(x, y) \in \mathbb{A}^2(\mathbb{F}_p) \mid f(x, y) = 0\right\} \cup \{O\}$$

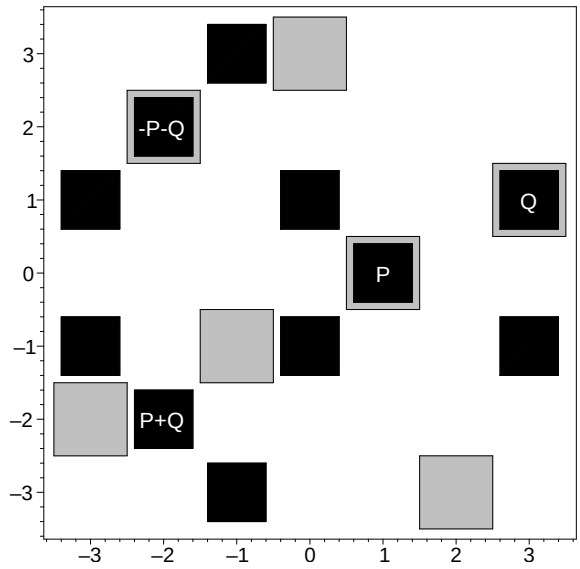

Figure 1.16: Elliptic curve over $\mathbb{F}_7$

with a polynomial

$$f = \left(x^3 + a \cdot x + b\right) - y^2 \in \mathbb{F}_p\left[x, y\right]$$

with $4a^3+27b^2 \neq 0 \bmod p$. Here O denotes the point at infinity, which lies on any line parallel to the y-axis and is the neutral element of the group.

Example 1.6.8 *Figure 1.16 depicts in black the points of the curve*

$$x^3 - 2x + 1 - y^2 = 0$$

over $\mathbb{F}_7$ (where y is the vertical axis). The grey dots are the points of the line

$$x - 2y - 1 = 0$$

through the points $P, Q \in E\left(\mathbb{F}_7\right)$. The sum $P + Q$ is obtained as the reflection of the third point of intersection $-\left(P + Q\right)$ of the line with the curve. Note: If we substitute $x = 2y + 1$ into f, we obtain a polynomial of degree 3 in one variable

$$y^3 + 4y^2 + 2y = 0$$

which has 3 zeros $y = 0, 1, 2$ corresponding to the 3 points of intersection $(1, 0), (3, 1)$ and $(-2, 2)$. This is a special case of ***Bezout's theorem****.*

In the context of cryptography it is of course important to know the group order (that is, the number of points) of $E(\mathbb{F}_p)$. *We answer this question using the computer algebra system* MAGMA, *which is the only closed source system devoted to algebraic geometry, number theory and combinatorics. The curve is specified by the vector* $[0,0,0,a,b]$

```
F := FiniteField(7,1);
E := EllipticCurve([Zero(F),Zero(F),Zero(F),-2,1]);
E;
Elliptic Curve defined by y^2 = x^3 + 5*x +1 over GF(7)
#E;
12
```

Note that this includes O, *not visible in Figure 1.16. Of course we can also do larger examples:*

```
F := FiniteField(NextPrime(10^30),1);
E := EllipticCurve([Zero(F),Zero(F),Zero(F),-2,1]);
#E;
999999999999999242601621761120
```

How does this work? Let p be an odd prime. The **Legendre symbol** is defined for $c \in \mathbb{Z}$ by

$$\left(\frac{c}{p}\right) = \begin{cases} 1 & \text{if} \quad y^2 \equiv c \bmod p \text{ is solveable and } p \nmid c \\ -1 & \text{if} \quad y^2 \equiv c \bmod p \text{ is not solveable} \\ 0 & \text{if} \quad p \mid c \end{cases}$$

With this notation, given $x \in \mathbb{F}_p$ we have

$$\left(\frac{x^3 + a \cdot x + b}{p}\right) = \begin{cases} 1 & \Leftrightarrow \text{ if there are 2 points } (x,-) \in E(\mathbb{F}_p) \\ -1 & \Leftrightarrow \text{ if there is no point } (x,-) \in E(\mathbb{F}_p) \\ 0 & \Leftrightarrow \text{ if there is 1 point } (x,-) \in E(\mathbb{F}_p) \end{cases}$$

that is, there are exactly

$$1 + \left(\frac{x^3 + a \cdot x + b}{p}\right)$$

points of the form $(x,-) \in E(\mathbb{F}_p)$. Hence we obtain (not forgetting the point at infinity O):

Theorem 1.6.9 *On the elliptic curve*

$$E(\mathbb{F}_p) = \left\{(x,y) \in \mathbb{F}_p^2 \mid x^3 + a \cdot x + b = y^2\right\} \cup \{O\}$$

there are exactly

$$|E(\mathbb{F}_p)| = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + a \cdot x + b}{p}\right)$$

points.

See also Exercise 1.8. Theorem 1.6.9 immediately implies:

Corollar 1.6.10 *For the number of points of an elliptic curve $E(\mathbb{F}_p)$ it holds*

$$1 \leq |E(\mathbb{F}_p)| \leq 2p + 1$$

More precisely there is the following theorem (which we cannot prove here):

Theorem 1.6.11 (Hasse) *The number of points of an elliptic curve $E(\mathbb{F}_p)$ satisfies*

$$p + 1 - 2\sqrt{p} \leq |E(\mathbb{F}_p)| \leq p + 1 + 2\sqrt{p}$$

One can show, that all possible values are indeed attained. In Exercise 1.9 we verify this theorem for a finite set of primes.

To compute $|E(\mathbb{F}_p)|$ it remains to evaluate the Legendre symbol, which one can do as follows. To obtain an easier algorithm, we first generalize the Legendre symbol:

Definition 1.6.12 *If $n = p_1 \cdot \ldots \cdot p_r$ with odd primes p_i and $c \in \mathbb{Z}$, then define the **Jacobi symbol** as*

$$\left(\frac{c}{n}\right) := \prod_{i=1}^{r} \left(\frac{c}{p_i}\right).$$

Note, that Singular (like most other computer algebra systems) has a command to compute the Jacobi symbol.

Remark 1.6.13 *If $b \equiv c \bmod n$, then*

$$\left(\frac{b}{n}\right) = \left(\frac{c}{n}\right).$$

For any b and c

$$\left(\frac{b \cdot c}{n}\right) = \left(\frac{b}{n}\right)\left(\frac{c}{n}\right).$$

Theorem 1.6.14 (Law of quadratic reciprocity) *If $b, c > 0$ are odd, then*

$$\left(\frac{b}{c}\right) = (-1)^{\frac{(b-1)(c-1)}{4}} \left(\frac{c}{b}\right)$$

and

$$\left(\frac{2}{c}\right) = (-1)^{\frac{c^2-1}{8}}.$$

A proof can be found in most books on algebra or number theory. The formulas of Remark 1.6.13 and Theorem 1.6.14 yield a recursive algorithm to compute the Jacobi symbol.

Example 1.6.15 *We apply this algorithm:*

$$\begin{aligned}\left(\frac{55}{103}\right) &= -\left(\frac{103}{55}\right) = -\left(\frac{48}{55}\right) = -\left(\frac{2}{55}\right)^4\left(\frac{3}{55}\right)\\ &= \left(\frac{55}{3}\right) = \left(\frac{1}{3}\right) = 1\end{aligned}$$

Hypersurfaces $X = V(f) \subset \mathbb{A}^n(K)$, as considered above, are given by a single non-constant equation $f \in K[x_1, ..., x_n]$. We also speak of an algebraic set of **codimension** 1. The set of 4 points in $\mathbb{A}^2(\mathbb{R})$ we considered in Figure 1.2 was given by two equations

$$\begin{aligned}2x^2 - xy + 2y^2 - 2 &= 0\\ 2x^2 - 3xy + 3y^2 - 2 &= 0\end{aligned}$$

and has codimension 2. Once we give a precise definition of the dimension $\dim X$ of a variety X, we can define the codimension as the difference

$$\operatorname{codim} X = n - \dim X.$$

We will see that, in general, the codimension can differ from the number of equations. As in the case of linear equations and vector spaces, the first step is to write down an independent set of equations, that is, a Gröbner basis. Even then, the codimension can be smaller than the number of equations, however, we will describe an algorithm to compute the dimension (and hence the codimension) from a Gröbner basis.

1.7 Exercises

Exercise 1.1 *Install* Singular, Gap, Pari/Gp, *and* Surfer *and try the examples featured in Chapter 1. Check out the online help pages.*

Exercise 1.2 *1) Implement the Euclidian Algorithm for computing the greatest common divisor in $\mathbb{Z}$. Test your implementation at examples.*

2) Use your implementation to cancel

$$\frac{90189116021}{18189250063}.$$

Exercise 1.3 *Let p be a prime and $\mathbb{F}_p = \mathbb{Z}/p$ the field with p elements.*

1) *Use an analogue of the sieve of Eratosthenes to find all irreducible polynomials in $\mathbb{F}_2[x]$ of degree ≤ 3.*

2) *Factor $x^5 + x^2 + x + 1 \in \mathbb{F}_2[x]$ into a product of irreducible polynomials.*

3) *Determine all elements of*

$$K = \mathbb{F}_2[x] / \left(x^2 + x + 1\right),$$

the addition table of K, and the multiplication table of K. Prove that K is a field. What is the characteristic of K?

Exercise 1.4 *Test the prime number theorem:*

1) *Write a procedure to compute*

$$\pi(x) = |\{p \leq x \mid p \in \mathbb{N} \text{ prime}\}|$$

for $x > 0$.

2) *Plot $\frac{\pi(x)}{x}$ and $\frac{1}{\ln(x)}$ and compare for large x.*

3) *Show that, according to the prime number theorem, the total expected number of Fermat primes is finite.*

Recall, that a Fermat prime is a prime number of the form

$$F_n = 2^{2^n} + 1$$

with $n \in \mathbb{N}_0$.

Exercise 1.5 *Let G be the symmetry group of the icosahedron (Figure 1.17).*

1) *Compute the group order of G.*

2) *Find generators of G as a subgroup of S_{12}. Prove your claim using* GAP.

Exercise 1.6 *Let $A \in \mathbb{Q}^{n \times m}$ be a matrix. Using the* SINGULAR *command Gröbner basis command* `std` *for ideals, implement a procedure which computes the reduced row echelon form of A.*

You may also want to use the following commands, see the online help: `ring`, `matrix`, `proc`, `int`, `nrows`, `ncols`, `def`, `basering`, `imap`, `poly`, `ideal`, `for`, `option(redSB)`, `diff`, `maxideal`, `setring`, `return`.

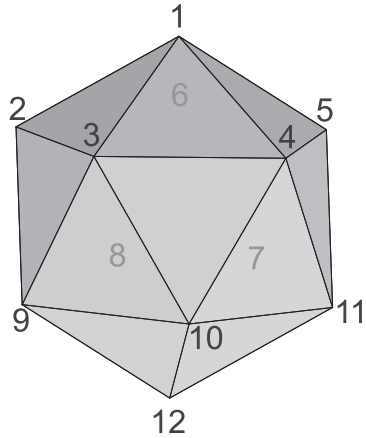

Figure 1.17: Icosahedron with numbering of the vertices.

Exercise 1.7 *Using the idea of homogenization, describe an algorithm for describing the set of solutions of an inhomogeneous system of linear equations, which is based on the algorithm for solving a homogeneous system.*

Exercise 1.8 *Let $p \geq 5$ be a prime, and*

$$E_{a,b}(\mathbb{F}_p) = \left\{(x,y) \in \mathbb{A}^2(\mathbb{F}_p) \mid f_{a,b}(x,y) = 0\right\} \cup \{O\}$$

an elliptic curve given by

$$f_{a,b} = x^3 + a \cdot x + b - y^2 \in \mathbb{F}_p[x,y].$$

with $4a^3 + 27b^2 \neq 0 \bmod p$. Write a procedure, which computes the number of points $|E_{a,b}(\mathbb{F}_p)|$ of the elliptic curve.

Note: You can simply test all points of $\mathbb{A}^2(\mathbb{F}_p)$, or make use of the Singular *command* `Jacobi`.

Exercise 1.9 *Using your procedure from Exercise 1.8, prove Hasse's theorem*

$$p + 1 - 2\sqrt{p} \leq |E_{a,b}(\mathbb{F}_p)| \leq p + 1 + 2\sqrt{p}$$

for all primes p with $5 \leq p \leq 53$. Verify that $|E_{a,b}(\mathbb{F}_p)|$ takes all possible values.

Exercise 1.10 *Let p be a prime and $f \in \mathbb{F}_p[x_1, ..., x_n]$ a non-constant polynomial. For every point $x \in \mathbb{A}^n(\mathbb{F}_p)$ the polynomial f can take p possible values $f(x)$. Assume that an irreducible polynomial f takes these values with equal probability $\frac{1}{p}$ for randomly chosen x.*

1) *What is the probability that* $f(x) = 0$ *for random* x *under the assumption that* f *is the product of two irreducible polynomials.*

2) *Derive from this a probabilistic test for irreducibility.*

3) *Try out examples and compare with the* SINGULAR *command* `factorize` *or the* MAPLE *command* `Factor() mod p`.

2

Ideals, varieties and Gröbner bases

2.1 Ideals and varieties

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

If $f_1(p) = 0, ..., f_s(p) = 0$ 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, $V(f_1, ..., f_s)$ depends only on the ideal

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

generated by $f_1, ..., f_s$. 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

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

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

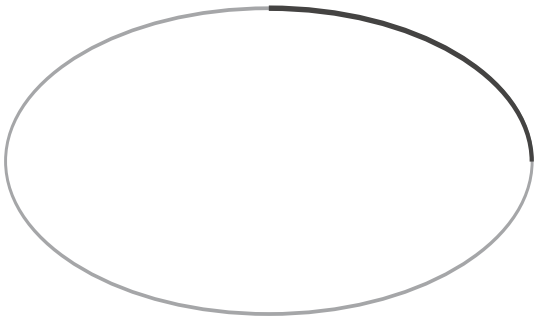

Figure 2.1: Elliptical arc

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 $I \subset K[x_1, ..., x_n]$ 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 $I \subset k[x_1, ..., x_n]$ 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*

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

*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 $I \subset K[x_1, ..., x_n]$. See also Exercise 2.2, which you need to show that this indeed gives a topology.*

By I and V inclusion reversing maps

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

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

$$I_1 \subset I_2 \subset I_3 \subset ... \subset I_n \subset ...$$

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

$$I_m = I_{m+1} = I_{m+2} = ...$$

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 $I_1 \subset I_2 \subset ...$ 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 $a_1, ..., a_s \in I$ with $I = \langle f_1, ..., f_s \rangle$. For every f_k there is a j_k with $f_k \in I_{j_k}$. For

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

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

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

and hence

$$I_m = I_{m+1} = ...$$

(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

$$I_1 \subsetneqq I_2 \subsetneqq I_3 \subsetneqq ...$$

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 $f_1, ..., f_s \in J$ with $J = \langle f_1, ..., f_s \rangle$. We show that $I = J$: If this is not true, then there is an $f \in I \backslash J$ with

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

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 $\pi^{-1}(J) = \langle f_1, ..., f_s \rangle$, and $J = \langle \pi(f_1), ..., f(f_s) \rangle$.

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

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

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, $f_2 \in I \setminus \langle f_1 \rangle$ mit $\deg(f_2)$ minimal, and inductively

$$f_k \in I \setminus \langle f_1, ..., f_{k-1} \rangle$$

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

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

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

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

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

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

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 $I \subset R = K[x_1, ..., x_n]$ 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 $I \subset K[x_1, ..., x_n]$ an ideal. Then*

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

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 $I \subset K[x_1, ..., x_n]$ an ideal. Then*

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

where

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

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

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

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

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

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

Substituting $y = \frac{1}{f}$ makes the coefficients to $c_i(x_1, ..., x_n, \frac{1}{f})$. 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 $I \subset K[x_1, ..., x_n]$ is called a **radical ideal**, if $I = \sqrt{I}$.*

Theorem 2.1.11 shows that, if K is algebraically closed,

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

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:

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

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

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

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.

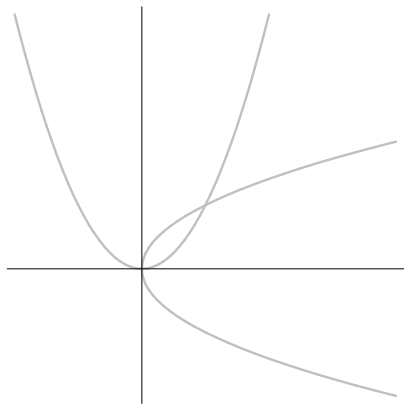

Figure 2.2: Reducible affine algebraic set

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 $I = \langle f_1, ..., f_s \rangle \subset K[x_1, ..., x_n]$ which again is given by generators $f_1, ..., f_s \in K[x_1, ..., x_n]$. For example, we may want to determine, whether $V(I)$ is contained in the

hypersurface $V(f)$. Equivalently, we have to determine whether $f \in \langle f_1, ..., f_s \rangle$. 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*

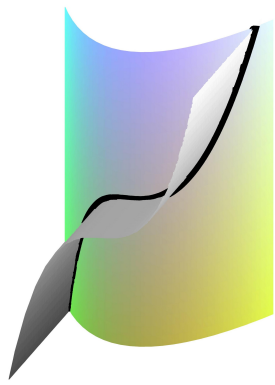

Figure 2.3: Twisted cubic

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,

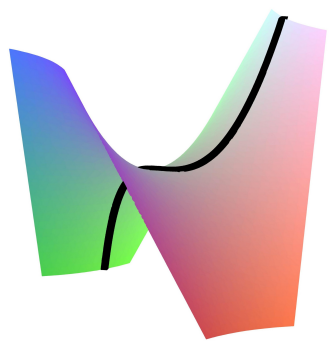

Figure 2.4: Surface containing the twisted cubic

and we easily find a representation

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

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**)*

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

such that for any $a, b \in R \setminus \{0\}$ 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 $f_1, ..., f_s \in R$, then*

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

Proof. As R is a principal ideal domain,

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

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

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

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

Hence, the ideal membership problem translates into the following characterization

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

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 $g_1, ..., g_r$, division will give remainder zero if and only if $f \in \langle g_1, ..., g_r \rangle$. We begin by formalizing this concept:

2.3 Monomial orderings

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

Definition 2.3.1 *A **monomial ordering** (or **semigroup ordering**) on the semigroup of monomials in the variables $x_1, ..., x_n$ 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 $x_1, ..., x_n$ has only finitely many minimal elements with respect to divisibility.*

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

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

Among the $m_1, ..., m_u$ 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 $I \subset K[x_1, ..., x_n]$ 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 $r_j \in K[x_1, ..., x_n]$ 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* $\exists 1 \le i \le n$: $\alpha_n = \beta_n, \ldots, \alpha_{i+1} = \beta_{i+1}, \alpha_i < \beta_i$.

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****.*

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* $f = \sum_\alpha c_\alpha x^\alpha$ *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****.*

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 $x_1, ..., x_n$, there is a weight vector $w \in \mathbb{Z}^n$ with*

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

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 $\lambda_i \in \mathbb{Q}_{>0}$, hence

$$0 \notin \operatorname{convHull}(D_> \cap M) = \left\{\textstyle\sum_{i=1}^r \lambda_i \delta_i \mid \delta_i \in D,\ \lambda_i \in \mathbb{Q}_{\geq 0},\ \sum_{i=1}^r \lambda_i = 1\right\}.$$

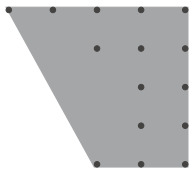

Figure 2.5: A convex hull

For an example in Figure 2.5 the grey area is the convex hull of the black points. By $0 \notin \mathrm{convHull}(D_> \cap M))$, there is a $w \in \mathbb{Z}^n$ such that $\mathrm{convHull}(D_>)$ 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 $1, x_1, ..., x_n \in M$. ■

Example 2.3.15 *For the lexicographical ordering $>$ in the variables x_1, x_2, the set $D_>$ is plotted in Figure 2.6. The figure also shows*

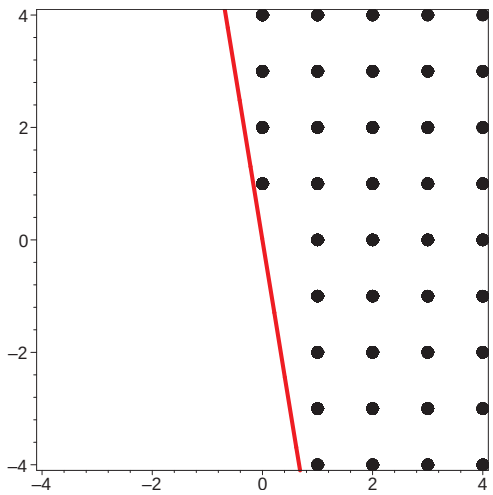

Figure 2.6: $D_>$ for the ordering lp

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.

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 g. This definition can be generalized to ideals with more than one generator.

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.

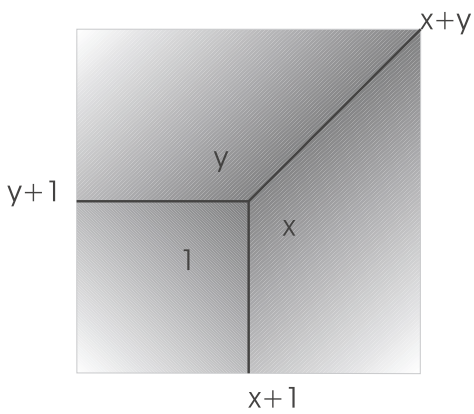

Figure 2.7: Gröbner fan of the line.

2.4 Division with remainder and Gröbner bases

Write $R = K[x_1, ..., x_n]$. Given a global monomial ordering, it is pretty clear, how to do division with remainder. Algorithm 2.4.1 divides $f \in R$ by $g_1, ..., g_s \in R$.

Algorithm 2.4.1 Division with remainder

Input: $f \in R$, $g_1, \ldots, g_s \in R$, $>$ 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 $L(r)$ is not divisible by any $L(g_i)$.

```
q = 0
r = f
while r ≠ 0 and L(g_i) | L(r) for some i do
    Cancel the lead term of r:
    a = LT(r) / LT(g_i)
    q = q + a · g_i
    r = r − a · 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. ■

Remark 2.4.1 *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 2.4.1 will compute*

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

that is, the geometric series expansion of

$$\frac{x}{x - x^2} = \frac{1}{1 - x}.$$

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 $1 - x$).

Example 2.4.2 *Using lp divide $x^2y + x$ by $y - 1$ and $x^2 - 1$.*

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

We will now show that Algorithm 2.4.1 solves the ideal membership problem, provided we divide by a Gröbner basis.

Definition 2.4.3 *Given a monomial ordering $>$ and a subset $G \subset R$, we define the* ***leading ideal*** *of G as*

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

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 2.4.4 (Gröbner basis) *Let I be an ideal and $>$ a global monomial ordering. A finite set $0 \notin G \subset I$ is called a* ***Gröbner basis*** *of I with respect to $>$, if*

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

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

Theorem 2.4.5 *Every ideal $I \subset R$ has a Gröbner basis.*

Proof. Since $L(I)$ is finitely generated, $L(I) = \langle m_1, ..., m_s \rangle$ 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

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

so $g_1, ..., g_s$ form a Gröbner basis of I. ■

From the definition it is not clear whether a Gröbner basis of I is indeed a set of generators of I. Solving the ideal membership problem will answer also this question. To clarify the behaviour of Algorithm 2.4.1, we first formalize its properties:

Definition 2.4.6 *Given a list $G = (g_1, ..., g_s) \subset R$, 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 all $0 \neq f \in R$ 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 $a_i g_i \neq 0$.

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

Lemma 2.4.7 *Algorithm 2.4.1 is a normal form. 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 Gröbner bases, we can now decide the ideal membership problem:

Theorem 2.4.8 (Ideal membership) *Let* $I \subset R$ *be an ideal and* $f \in R$. *If* $G = (g_1, ..., g_s)$ *is a Gröbner basis of* I *and* NF *is a normal form, then*

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

Proof. Write $f = \sum_i a_i g_i + r$ with $r = \mathrm{NF}(f, G)$. If $r = 0$ then $f = \sum_i a_i g_i \in \langle G \rangle \subset I$. On the other hand, if $r \neq 0$ then by Definition 2.4.6 (2.)

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

So, by definition of the lead ideal,

$$r \notin I,$$

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

Lemma 2.4.9 *If* $J \subset I \subset R$ *are ideals with* $L(J) = L(I)$ *then* $I = J$.

Proof. Let $G = (g_1, ..., g_s)$ be a Gröbner basis of J, NF a normal form, $f \in I$ and $f = \sum_i a_i g_i + r$ with $r = \mathrm{NF}(f, G)$. So $r \in I$. If $r \neq 0$, then by Definition 2.4.6 (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 2.4.10 *If* G *is a Gröbner 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 Gröbner basis of $\langle G \rangle \subset I$ and $L(\langle G \rangle) = L(I)$. Equality follows from Lemma 2.4.9. ■

Example 2.4.11 *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*

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

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:

Example 2.4.12 *At every step of Algorithm 2.4.1, 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 2.4.2. 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 2.4.13 *A polynomial* $f \in R$ *is called* ***reduced*** *with respect to a set* $G \subset R$*, if no term of* f *is contained in* $L(G)$*.*

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

Algorithm 2.4.2 yields a reduced normal form, the **reduced Buchberger normal form**.

Algorithm 2.4.2 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 ≠ 0 do
    if L(g_i) | L(h) for some i then
        Cancel the lead term of h:
        a = LT(h) / LT(g_i)
        q = q + a · g_i
        h = h − a · g_i
    else
        Put the lead term into the remainder:
        r = r + LT(h)
        h = h − LT(h)
```

Example 2.4.14 *So, also putting terms into the remainder in the intermediate steps, we can continue in Example 2.4.12:*

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

which leads to the same remainder $x+1$ as in Example 2.4.2. Indeed, the remainder is now unique:

Theorem 2.4.15 *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 $G = (g_1, ..., g_s)$ and suppose that

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

Then

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

(using Corollary 2.4.10). 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 2.4.16 *In* SINGULAR *we can compute the reduced Buchberger normal form in Example 2.4.14 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.*

Remark 2.4.17 *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 2.4.2 and 2.4.14 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 $G = (g_1, \ldots, g_s)$, we can obtain a unique expression

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

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 $G = (y - 1, x^2 - 1)$.

2.5 Computing Gröbner 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. Again write $R = K[x_1, ..., x_n]$ and fix a global monomial ordering $>$.

Definition 2.5.1 *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 2.5 computes a Gröbner basis.

Algorithm 2.5.1 Buchberger

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

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

```
G = {g_1, ..., g_s}
repeat
    H = G
    for all f, g ∈ H do
        r = NF(spoly(f, g), H)
        if r ≠ 0 then
            G = G ∪ {r}
until G = H
```

Proof. If $r \neq 0$ then $L(r) \notin L(H)$ by Definition 2.4.6(2.), hence

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

So, by the Noetherian property of R, the algorithm terminates.

To show that the final result is a Gröbner basis, we prove: ■

Theorem 2.5.2 (Buchberger's criterion) *If* $I \subset R$ *is an ideal,* NF *a normal form and* $G = (g_1, ..., g_s)$ *a list of elements of* I*, then the following conditions are equivalent:*

1) *G is a Gröbner basis of I.*

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

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

Proof. (1) ⇒ (2) ⇒ (3): If G is a Gröbner basis we get $\mathrm{NF}(f, G) = 0$ for all $f \in I$ by Theorem 2.4.8. Furthermore, $\mathrm{spoly}(g_i, g_j) \in I$.

(2) ⇒ (1): If $f \in I$ then by $\mathrm{NF}(f, G) = 0$ and Definition 2.4.6(3.) we have an expression

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

with $L(f) \geq L(a_i g_i)$ 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

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

Clearly $L(f) \leq \max_i L(a_i g_i)$. 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

$$0 = \mathrm{spoly}(g_{i_1}, g_{i_2}) - \sum_{i=1}^{s} c_i g_i.$$

Such a relation is called a **syzygy**. Subtracting a multiple of this equality from $f = \sum_{i=1}^{s} a_i g_i$ 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 Gröbner bases of modules will enable us to give a very elegant proof later.

Example 2.5.3 *Using Buchberger's criterion we can easily check that* $G = (\boldsymbol{x}^2 - 1, \boldsymbol{y} - 1)$ *is a Gröbner basis of* $I = \langle G \rangle$*: For the S-pair*

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

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

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

Example 2.5.4 *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 division with remainder.

	$\Rsh$	$\boldsymbol{-tx} + y$	$\Rsh$	$\boldsymbol{-t^2x} + z$	$\Rsh$	$\boldsymbol{-ty} + z$	$\Rsh$	$\boldsymbol{t^3y} - zx$
$\boldsymbol{t^2} - x$	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 2.5.5 *A Gröbner 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 2.5.6 *From any Gröbner basis we can obtain a minimal one by deleting elements.*

Proof. Given a Gröbner 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 clearly generates the same ideal, and, hence, the corresponding g_i form a Gröbner basis. ■

Theorem 2.5.7 *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

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

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

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

Finally $\mathrm{NF}(s, G) = 0$ by Theorem 2.4.8 and $s \in I$. ■

Remark 2.5.8 *If $G = (g_1, \ldots, g_s)$ is minimal and* NF *is a reduced normal form, then $H = (h_1, \ldots, h_s)$ with*

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

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 2.5.9 *In Example 2.5.4 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 2.5.10 *For Example 2.5.4 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 2.5.11 *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
```

2.6 Exercises

Exercise 2.1 *Show the following:*

1) *Any ideal of* $\mathbb{Z}$ *is of the form*

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

with $n \in \mathbb{Z}$.

2) *Let* $\langle n \rangle \subset \mathbb{Z}$ *be an ideal and* $n > 0$. *Then*

$$(n) \text{ is a prime ideal} \Longleftrightarrow n \text{ is a prime number.}$$

Exercise 2.2 *Let* $I, J \subset K[x_1, ..., x_n]$ *be ideals. Show that*

$$V(I + J) = V(I) \cap V(J)$$

and

$$V(I \cdot J) = V(I \cap J) = V(I) \cup V(J).$$

Recall that $I \cap J$,

$$I + J = \{f + g \mid f \in I \text{ and } g \in J\}$$
$$I \cdot J = \langle f \cdot g \mid f \in I \text{ and } g \in J \rangle$$

are ideals.

Exercise 2.3 1) *Let* K *be a field and* $X \subset \mathbb{A}^n(K)$ *an affine algebraic set. Prove that* X *is irreducible if and only if* $I(X) \subset K[x_1, ..., x_n]$ *is prime.*

2) *Show that, if K is algebraically closed and I is prime, then $V(I)$ is irreducible.*

3) *Give an example of a prime ideal $I \subset K[x_1, ..., x_n]$ over a field K such that $V(I)$ is reducible.*

4) *For K algebraically closed, prove that*

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

is a one-to-one correspondence.

Exercise 2.4 *Prove that the following rings are not Noetherian:*

1) *The polynomial ring $K[x_1, x_2, ...]$ in infinitely many variables.*

2) *The ring*
$$R = \{f \in \mathbb{Q}[X] \mid f(0) \in \mathbb{Z}\}$$
of polynomials with integer values at 0.

Exercise 2.5 *Let K be a field and $(a_1, ..., a_n) \in K^n$. Prove that*

$$\langle x_1 - a_1, ..., x_n - a_n \rangle \subset K[x_1, ..., x_n]$$

is a maximal ideal.

Hint: Develop a multivariate division with remainder.

Exercise 2.6 *Determine all maximal ideals of $\mathbb{R}[x]$.*

Exercise 2.7 *Let $>$ be a semigroup ordering on the monomials in the variables $x_1, ..., x_n$. Prove that the following conditions are equivalent:*

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).

Exercise 2.8 *Sort all monomials of degree ≤ 2 in the variables x, y, z with respect to the monomial orderings lp, dp, and ls.*

Exercise 2.9 *If $>$ is a monomial ordering on x_1, x_2 define*

$$D_> = \left\{\alpha - \beta \mid x^\alpha > x^\beta\right\} \subset \mathbb{Z}^2$$

1) *Plot the set $D_>$ for the monomial orderings lp and dp.*

2) *Assuming that we consider only monomials of degree $\leq d$, find weight vectors $u = (u_1, u_2)$ which represent lp and dp, respectively.*

   What about the weight ordering $>_w$ with weight vector $w \in \mathbb{Z}^2$ and tie break ordering lp?

Exercise 2.10 *Let $I = \langle f_1, f_2, f_3\rangle \subset \mathbb{R}[x, y, z]$ be the ideal generated by*

$$\begin{aligned} f_1 &= x^2 + y^2 - 1 \\ f_2 &= x^2 + z^2 - 1 \\ f_3 &= x + y + z \end{aligned}$$

1) *Compute the reduced Gröbner basis of I with respect to lp.*

2) *Deduce from this, that $V(I)$ consists of 4 points.*

Exercise 2.11 *Use Buchberger's algorithm to compute the reduced 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 $t > z > y > x$.

Exercise 2.12 *Let $I \subset K[x_1, ..., x_n]$ be an ideal and* NF *a reduced normal form. Show that*

$$\begin{array}{ccc} K[x_1, ..., x_n]/I & \to & {}_K\langle x^\alpha \mid x^\alpha \notin L(I)\rangle \\ \overline{f} & \mapsto & \mathrm{NF}(f, I) \end{array}$$

is an isomorphism of K-vectorspaces.

Exercise 2.13 *Let*

$$I = \left\langle y + x^2 + 1, xy + y^2 + y\right\rangle \subset \mathbb{R}[x, y]$$

and fix the monomial ordering lp.

1) *Find the minimal generators of $L(I)$.*

2) *Show that $\overline{1}, \overline{x}, \overline{y}, \overline{y^2}$ form a vectorspace basis of $\mathbb{R}[x, y]/I$.*

3) *Compute the multiplication table of $\mathbb{R}[x, y]/I$ with respect to this basis.*

3

Computing with ideals and algebraic sets

We now discuss how to use Buchberger's algorithm to compute with algebraic sets, or equivalently with ideals. We have already seen, how to decide, whether an algebraic set is contained in a hypersurface by solving the ideal membership problem.

3.1 Sums and intersections of ideals

Given two ideals $I, J \subset R = K[x_1, ..., x_n]$, by

$$V(I) \cap V(J) = V(I + J)$$

the intersection of algebraic sets corresponds to the sum of ideals, see Exercise 2.2. If

$$I = \langle f_1, ..., f_s \rangle \qquad J = \langle g_1, ..., g_r \rangle$$

then

$$I + J = \langle f_1, ..., f_s, g_1, ..., g_r \rangle ,$$

so computing the sum is trivial. Note, however, that even if $(f_1, ..., f_s)$ and $(g_1, ..., g_r)$ are Gröbner bases, $(f_1, ..., f_s, g_1, ..., g_r)$ may not be.

On the other hand, by

$$V(I) \cup V(J) = V(I \cap J)$$

the union of algebraic sets corresponds to the intersection of ideals (see again Exercise 2.2), which can be obtained as follows:

Algorithm 3.1.1 *Let $I, J \subset R$ be ideals and*

$$I = \langle f_1, ..., f_s \rangle \qquad J = \langle g_1, ..., g_r \rangle$$

With

$$L = \langle t \cdot f_1, \ldots, t \cdot f_s, (1-t) \cdot g_1, \ldots, (1-t) \cdot g_r \rangle \subset R[t]$$

it holds

$$I \cap J = L \cap R$$

Proof. If $f \in I \cap J$, then

$$R \ni f = t \cdot f - (1-t) \cdot f \in L.$$

On the other hand if $f \in L \cap R$, then

$$f(x,t) = t\textstyle\sum_{i=1}^{s} a_i(x,t) f_i(x) + (1-t)\sum_{j=1}^{r} b_j(x,t) g_j(x)$$

is independent of t, hence

$$I \ni \textstyle\sum_{i=1}^{s} a_i(x,1) f_i(x) = f(x,1) = f(x,0) = \sum_{j=1}^{r} b_j(x,0) g_j(x) \in J.$$

■

To turn this result into an algorithm, we need a way to compute the intersection of L with the subring $R \subset R[t]$. Before discussing this fundamental problem in the next section, we try out ideal intersection in SINGULAR:

Example 3.1.2 *Consider the points*

$$\begin{array}{ll} P_1 = V(\langle x, y \rangle) & P_2 = V(\langle x-1, y \rangle) \\ P_3 = V(\langle x, y-1 \rangle) & P_4 = V(\langle x-1, y-1 \rangle) \end{array}$$

in $\mathbb{A}^2_K$. *Then the union* $P_1 \cup P_2 \cup P_3 \cup P_4$ *is defined by the ideal*

$$\langle x, y \rangle \cap \langle x-1, y \rangle \cap \langle x, y-1 \rangle \cap \langle x-1, y-1 \rangle .$$

We compute a Gröbner basis of this intersection using SINGULAR*:*

```
ring R=0,(x,y),lp;
ideal I1 = x,y;
ideal I2 = x-1,y;
ideal I3 = x,y-1;
ideal I4 = x-1,y-1;
std(intersect(I1,I2,I3,I4));
_[1]=y2-y
_[2]=x2-x
```

Hence

$$\langle x, y \rangle \cap \langle x-1, y \rangle \cap \langle x, y-1 \rangle \cap \langle x-1, y-1 \rangle = \left\langle x^2 - x, y^2 - y \right\rangle,$$

so the four points are represented as the intersection of two pairs of parallel lines, see Figure 3.1.

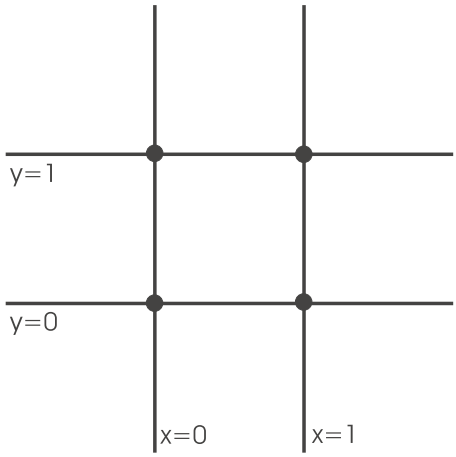

Figure 3.1: Four points as the intersection of two pairs of lines

In the context of primary decomposition, we will discuss, how to do the converse, that is, how to represent a given ideal as an intersection.

In Exercise 6.1 we will develop an algorithm for computing intersections of ideals with the help of syzygyies.

3.2 Elimination of variables

We now discuss how to intersect an ideal with a polynomial subring. Geometrically this corresponds to the projection of algebraic sets.

Definition 3.2.1 *A monomial ordering $>$ on*

$$R = K[x_1, ..., x_m, x_{m+1}, ..., x_n]$$

is called ***elimination ordering*** *for $x_1, ..., x_m$ if for all $f \in R$ it holds*

$$L(f) \in K[x_{m+1}, ..., x_n] \Rightarrow f \in K[x_{m+1}, ..., x_n].$$

Example 3.2.2 *The lexicographic ordering with $x_1 > ... > x_n$ is clearly an elimination ordering (for any $1 < m < n$).*

Algorithm 3.2.3 *Let $I \subset R$ be an ideal, $>$ an elimination ordering for $x_1, ..., x_m$, and G a Gröbner basis of I with respect to $>$. Then*

$$H = \{g \in G \mid L(g) \in K[x_{m+1}, ..., x_n]\}$$

is a Gröbner basis of $J = I \cap K[x_{m+1}, ..., x_n]$.

Proof. If $g \in H \subset G \subset I$, so $L(g) \in K[x_{m+1}, ..., x_n]$, then by Definition 3.2.1 we have $g \in K[x_{m+1}, ..., x_n]$, so $g \in J$. This shows $H \subset J$.

From this we get $L(H) \subset L(J)$. For the other inclusion: If

$$f \in J \subset I$$

then $L(f) \in L(I) = L(G)$, hence there is a $g \in G$ with

$$L(g) \mid L(f).$$

Since $L(f) \in K[x_{m+1}, ..., x_n]$, also $L(g) \in K[x_{m+1}, ..., x_n]$, that is, $g \in H$. This proves that $L(J) \subset L(H)$, and, hence, H is a Gröbner basis of J. ■

Example 3.2.4 *Consider the twisted cubic*

$$C = V(I) \subset \mathbb{A}^3_K$$

defined by

$$I = \langle y - x^2,\ z - x^3 \rangle \subset K[x, y, z].$$

We compute the intersection

$$P = I \cap K[y, z]$$

by computing a Gröbner basis of I with respect to lp with $x > y > z$:

```
ring R=0,(x,y,z),lp;
ideal I = y-x2,z-x3;
std(I);
_[1]=y3-z2
_[2]=xz-y2
_[3]=xy-z
_[4]=x2-y
```

Hence

$$P = \langle y^3 - z^2 \rangle$$

The curve $V(P)$ corresponds to the image of C under the projection map

$$\mathbb{A}^3_K \to \mathbb{A}^2_K,\ (x, y, z) \mapsto (y, z)$$

see Figure 3.2. The elimination ideal can also be computed with the following command (no matter what the monomial order is):

```
eliminate(I,x);
_[1]=y3-z2
```

To eliminate several variables, put their product into the second argument.

In the next section we discuss the relation between the geometric concept of projection and the algebraic concept of elimination.

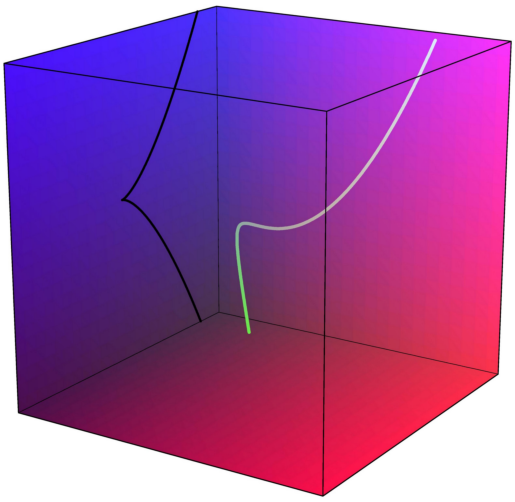

Figure 3.2: Projection of the twisted cubic

3.3 Projection and elimination

For any ideal $I \subset K[x_1, ..., x_n]$, for $0 \leq m < n$ consider the **elimination ideal**

$$I_m = I \cap K[x_{m+1}, ..., x_n]$$

and the **projection**

$$\begin{aligned} \pi_m : \quad & \mathbb{A}_K^n \to \mathbb{A}_K^{n-m} \\ & \pi_m(a_1, ..., a_n) = (a_{m+1}, ..., a_n) \end{aligned}$$

forgetting the first m coordinates.

Example 3.3.1 *For*

$$\begin{aligned} I &= \left\langle x^2 - 1, y^2 - 4 \right\rangle \\ V(I) &= \{(1,2), (-1,2), (1,-2), (-1,-2)\} \end{aligned}$$

then $\pi_1(V(I)) = \{-2, 2\}$ *and* $I_1 = \langle y^2 - 4 \rangle$. *We will see how to use the idea of projection to solve algebraic systems with a finite set of solutions.*

Example 3.3.2 *The projection of an algebraic set may not be an algebraic set: For the hyperbola* $S = V(xy - 1)$ *we have* $\pi_1(S) = \mathbb{A}_K^1 \setminus \{0\}$, *see Figure 3.3.*

Hence, the right question is, how to describe the closure of the projection in the Zariski topology. Recall that the closed sets of

the Zariski topology are the algebraic sets. For any subset $S \subset \mathbb{A}_K^n$ the Zariski closure is

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

In particular, for an algebraic set S, we have $S = V(I(S))$.

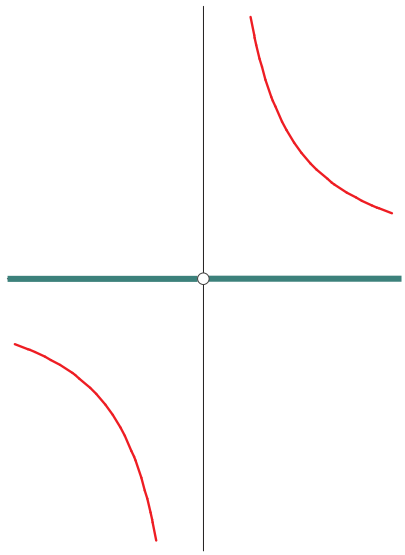

Figure 3.3: Projection of a hyperbola

Theorem 3.3.3 *If $K = \overline{K}$ and $I \subset K[x_1, ..., x_n]$ is an ideal, then*

$$\overline{\pi_m(V(I))} = V(I_m)$$

for all $0 \leq m < n$.

Proof. If $(a_{m+1}, ..., a_n) = \pi_m(a_1, ..., a_n) \in \pi_m(V(I))$ and $f \in I_m$, then, considering f as an element of $I \subset R$, we have

$$f(a_{m+1}, ..., a_n) = f(a_1, ..., a_n) = 0,$$

hence

$$\pi_m(V(I)) \subset V(I_m).$$

Since $V(I_m)$ is closed, this also holds true for the closure.

Any $g \in I(\pi_m(V(I))) \subset K[x_{m+1}, ..., x_n]$ can be considered as an element of $K[x_1, ..., x_n]$ and vanishes on $V(I)$. So by Theorem 2.1.11 (Nullstellensatz) there is an a with $g^a \in I$, so $g^a \in I \cap K[x_{m+1}, ..., x_n] = I_m$. Hence, again by Theorem 2.1.11,

$$I(\pi_m(V(I))) \subset \sqrt{I_m} = I(V(I_m)),$$

so by applying V we get

$$V(I_m) = \overline{V(I_m)} = V\left(I(V(I_m))\right) \subset V\left(I\left(\pi_m(V(I))\right)\right) = \overline{\pi_m(V(I))}.$$

■

Example 3.3.4 *Considering the ideal*

$$I = \left\langle x - st,\ y - t,\ z - s^2 \right\rangle \subset K[s,t,x,y,z]$$

we compute the projection on the variables x, y, z using SINGULAR*:*

```
ring R=0,(s,t,x,y,z),lp;
ideal I = x-st, y-t, z-s2;
std(I);
_[1]=x2-y2z
_[2]=t-y
_[3]=sy-x
_[4]=sx-yz
_[5]=s2-z
```

Hence

$$\overline{\pi_2\left(V\left(I\right)\right)} = V(x^2 - y^2 z).$$

We will now discuss how to interpret this calculation.

3.4 Polynomial maps between algebraic sets

Proposition 3.4.1 *Suppose $K = \overline{K}$ and we are given a polynomial map*

$$\begin{aligned} \varphi: \quad & \mathbb{A}_K^m \to \mathbb{A}_K^n \\ & t = (t_1, .., t_m) \mapsto (f_1(t), ..., f_n(t)) \end{aligned}$$

with $f_i \in k\left[t_1, .., t_m\right]$. Then for the closure of the image of φ it holds

$$\overline{\mathrm{im}(\varphi)} = V\left(J_m\right)$$

where

$$J = \langle x_1 - f_1,\ \ ..., x_n - f_n \rangle \subset k\left[t_1, .., t_m, x_1, ..., x_n\right]$$

Proof. With the graph

$$\Gamma(\varphi) = \{(t,x) \in \mathbb{A}_K^{n+m} \mid x = \varphi(t)\} = V(J).$$

we have

$$\pi_m(V(J)) = \pi_m(\Gamma(\varphi)) = \operatorname{im}(\varphi).$$

Using Theorem 3.3.3 it follows

$$\overline{\operatorname{im}(\varphi)} = V(J_m).$$

■

Example 3.4.2 *The* ***Whitney umbrella*** *is the image of the map*

$$\begin{array}{rccc} \varphi: & \mathbb{A}^2_K & \to & \mathbb{A}^3_K \\ & (s,t) & \mapsto & (st, t, s^2) \end{array}$$

Applying Proposition 3.4.1, we have already determined in Example 3.3.4 that the

$$\overline{\operatorname{im}(\varphi)} = V(x^2 - y^2 z).$$

Figure 3.4 shows the Whitney umbrella over the reals $K = \mathbb{R}$.

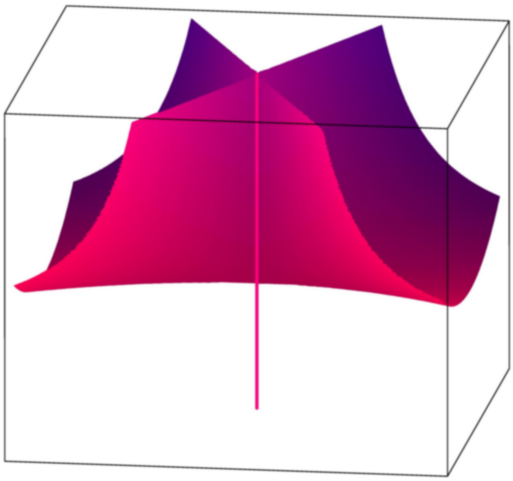

Figure 3.4: Whitney umbrella

In general we define:

Definition 3.4.3 *A* ***polynomial parametrization*** *of the algebraic variety* $X \subset \mathbb{A}^n_K$ *is a morphism* $\varphi: \mathbb{A}^m_K \to \mathbb{A}^n_K$ *with* $\overline{\operatorname{im}(\varphi)} = X$.

Computing the ideal of the image of a polynomial parametrization is also referred to as **implicitation**, since we determine implicit equations for the image of the parametrization.

Example 3.4.4 *Given a homogeneous linear system of equations, using Gaussian elimination we can compute a parametrization of the solution set.*

For example, consider the linear system of equations from Example 1.5.2

$$\begin{array}{ccccccccccccc} f_1 & = & x_1 & + & x_2 & & & & & + & x_5 & = & 0 \\ f_2 & = & x_1 & + & x_2 & + & x_3 & + & x_4 & + & x_5 & = & 0 \end{array}$$

Gaussian elimination yields

$$\begin{array}{ccccccccccc} x_1 & + & x_2 & + & & & & + & x_5 & = & 0 \\ & & & & x_3 & + & x_4 & & & = & 0 \end{array}$$

So we obtain a basis of the vector space of solutions

$$V(\langle f_1, f_2\rangle) = \left\langle \begin{pmatrix} -1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right\rangle$$

and, hence, a parametrization

$$\begin{array}{rccc} \varphi: & \mathbb{A}_K^3 & \to & \mathbb{A}_K^5 \\ & (t_1, t_2, t_3) & \mapsto & (-t_1 - t_3,\ t_3, -t_2,\ t_2,\ t_1) \end{array}$$

with

$$V(\langle f_1, f_2\rangle) = \mathrm{im}(\varphi).$$

Even more general we define:

Definition 3.4.5 *A map $\varphi : X \to Y$ between algebraic sets $X \subset \mathbb{A}_K^m$ and $Y \subset \mathbb{A}_K^n$, which is induced by a polynomial map $\varphi' : \mathbb{A}_K^m \to \mathbb{A}_K^n$ with $\varphi'(X) \subset Y$ is called a* ***morphism****.*

Proposition 3.4.6 *If $X = V(I) \subset \mathbb{A}_K^m$ with an ideal $I \subset K[t_1, ..., t_m]$ and*

$$\begin{array}{rl} \varphi: & X \to \mathbb{A}_K^n \\ & t = (t_1, .., t_m) \mapsto (f_1(t), ..., f_n(t)) \end{array}$$

is a morphism, then

$$\overline{\mathrm{im}(\varphi)} = V(J_m)$$

where

$$J = \langle I\rangle + \langle x_1 - f_1(t),\ ..., x_n - f_n(t)\rangle \subset k[t_1, .., t_m, x_1, ..., x_n].$$

Proof. Again

$$\Gamma(\varphi) = \{(t,x) \in \mathbb{A}_K^{n+m} \mid x = \varphi(t),\ t \in X\} = V(J)$$

is the graph, and we can argue as in the proof of Proposition 3.4.1. ■

Example 3.4.7 *The image of the sphere*

$$S = V(t_1^2 + t_2^2 + t_3^2 - 1) \subset \mathbb{A}_K^3$$

under the morphism

$$\begin{array}{rccc} \varphi: & S & \to & \mathbb{A}_K^3 \\ & (t_1, t_2, t_3) & \mapsto & (t_1t_2,\ t_1t_3,\ t_2t_3) \end{array}$$

is the ***Steiner surface****. Figure 3.5 shows an image for* $K = \mathbb{R}$*. By computing a Gröbner basis of*

$$J = \left\langle t_1^2 + t_2^2 + t_3^2 - 1,\ x - t_1t_2,\ y - t_1t_3,\ z - t_2t_3 \right\rangle$$

with respect to an elimination ordering for t_1, t_2, t_3*, by Proposition 3.4.6 we get*

$$\overline{\mathrm{im}(\varphi)} = V(x^2y^2 + x^2z^2 + y^2z^2 - xyz).$$

See also Exercise 3.3.

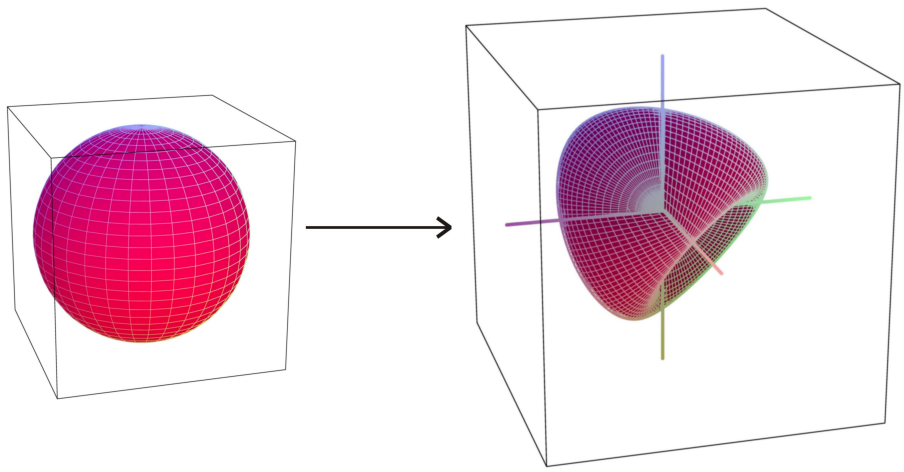

Figure 3.5: Steiner surface over the reals

The elimination ideal can be interpreted as the kernel of a ring homomorphism. Recall that the kernel of a ring homomorphism is an ideal (in fact, the ideal definition is motivated by the key properties of kernels).

Proposition 3.4.8 *Let $I \subset K[t_1, ..., t_m]$ be an ideal. The kernel* $\ker(f)$ *of a ring homomorphism*

$$\begin{array}{rccc} f: & K[x_1, ..., x_n] & \to & K[t_1, ..., t_m]/I \\ & x_i & \mapsto & \bar{f}_i \end{array}$$

is an ideal, and

$$\ker(f) = J_m$$

with

$$J = \langle I \rangle + \langle x_1 - f_1(t), \ ..., x_n - f_n(t) \rangle \subset K\left[t_1, .., t_m, x_1, ..., x_n\right].$$

Note that J is independent of the representatives f_i of the classes $\bar{f}_i$, since we add I.

Proof. Write $I = \langle g_1, ..., g_s \rangle \subset K[t_1, ..., t_m]$. We have

$$\begin{aligned} & h(x) \in \ker(f) \\ \Leftrightarrow\ & h(f_1(t), ..., f_n(t)) \in I \\ \Leftrightarrow\ & \exists a_i(t) \in K[t_1, ..., t_m] : h(f_1(t), ..., f_n(t)) = \textstyle\sum_{i=1}^{s} a_i(t) g_i(t) \\ \Leftrightarrow\ & h(x) \in J \cap K\left[x_1, ..., x_n\right] \end{aligned}$$

For the last equivalence observe that, by Taylor's formula,

$$h(x) = h(f_1(t), ..., f_n(t)) + \textstyle\sum_{i=1}^{n} c_i(x, t) \cdot (x_i - f_i(t))$$

with some $c_i(t, x) \in K\left[t_1, .., t_m, x_1, ..., x_n\right]$. ■

So Proposition 3.4.6 can be written in a more intrinsic way as follows: If $X = V(J)$ and

$$\begin{array}{rl} \varphi: & \mathbb{A}_K^m \to \mathbb{A}_K^n \\ & t = (t_1, .., t_m) \mapsto (f_1(t), ..., f_n(t)) \end{array}$$

then

$$\overline{\varphi(X)} = V(\ker(f)).$$

On the level of schemes, we would simply define the image as the scheme defined by $\ker(f)$.

Example 3.4.9 *By computing a kernel, the ideal of the Steiner surface in Example 3.4.7 can be determined as follows:*

```
ring S = 0,(x,y,z),dp;
ring R = 0,(t1,t2,t3),dp;
ideal I = t1^2+t2^2+t3^2-1;
qring Q = std(I);
map f = S, ideal(t1*t2, t1*t3, t2*t3);
setring S;
kernel(Q,f);
_[1]=x2y2+x2z2+y2z2-xyz
```

Note, that the ring homomorphism f is defined in the target ring Q (and gives a reference to the source ring S). On the other hand the kernel is computed in the source ring S (and you have to give a reference to the target ring Q).

3.5 Rational maps between varieties

More generally, one can consider maps given by rational functions. This is indeed necessary, for example to parametrize a circle, see Exercise 3.2. We discuss how to determine the image of a rational map. This is the algorithmic basis of birational geometry, which studies algebraic varieties up to birational maps, that is, rational maps which admit a rational inverse.

Definition 3.5.1 *A **rational map***

$$\varphi = \left(\frac{f_1}{g_1}, \ldots, \frac{f_n}{g_n}\right) : \mathbb{A}_K^m \dashrightarrow \mathbb{A}_K^n$$

is a tuple of rational functions $\frac{f_i}{g_i} \in K(t_1, .., t_m)$. Hence it defines a map

$$\begin{aligned} \varphi : \quad & \mathbb{A}_K^m \backslash Z \to \mathbb{A}_K^n \\ & t = (t_1, .., t_m) \mapsto \left(\tfrac{f_1(t)}{g_1(t)}, \ldots, \tfrac{f_n(t)}{g_n(t)}\right) \end{aligned}$$

where $\mathbb{A}_K^m \backslash Z$ is the locus on which all component functions are defined, that is, $Z = V(g_1 \cdot \ldots \cdot g_n)$. The image of φ is defined as

$$\operatorname{im}(\varphi) = \varphi(\mathbb{A}_K^m \backslash Z).$$

The dashed arrow indicates that the map is not defined on the whole of $\mathbb{A}_K^m$. Of course any polynomial map is also a rational map.

Proposition 3.5.2 *Suppose $K = \overline{K}$,*

$$\varphi = \left(\frac{f_1}{g_1}, \ldots, \frac{f_n}{g_n}\right) : \mathbb{A}_K^m \dashrightarrow \mathbb{A}_K^n$$

is a rational map, and $g = g_1 \cdot \ldots \cdot g_n$. *Then for the closure of the image of* φ *it holds*

$$\overline{\operatorname{im}(\varphi)} = V(J_{m+1})$$

where

$$J = \langle g_1 x_1 - f_1,\ \ldots,\ g_n x_n - f_n,\ 1 - gs \rangle \subset K[s, t_1, .., t_m, x_1, \ldots, x_n].$$

The idea of the proof is simple: The equation $1 - gs$ removes the solutions (t, x) of the equations $g_i x_i - f_i$ with some $g_i(x) = 0$.

Proof. With the map

$$\begin{aligned} \iota : \mathbb{A}_K^m \backslash Z &\to \mathbb{A}_K^{n+m+1} \\ \iota(t) &\mapsto \left(g(t)^{-1}, t, \varphi(t)\right) \end{aligned}$$

we obtain a commutative diagram

$$\begin{tikzcd} & \mathbb{A}_K^{n+m+1} \arrow[dr, "\pi_{m+1}"] & \\ \mathbb{A}_K^m \backslash Z \arrow[ur, "\iota"] \arrow[rr, "\varphi"] & & \mathbb{A}_K^n \end{tikzcd}$$

It holds

$$\iota(\mathbb{A}_K^m \backslash Z) = V(J)$$

since $(s, t, x) \in V(J)$ if and only if

$$g_i(t) \neq 0 \forall i \text{ and } x_i = \frac{f_i(t)}{g_i(t)} \forall i \text{ and } s = \frac{1}{g(t)}$$

that is $(s, t, x) \in \iota(\mathbb{A}_K^m \backslash Z)$. Applying π_{m+1} we get

$$\varphi(\mathbb{A}_K^m \backslash Z) = \pi_{m+1}(V(J))$$

and hence, by Theorem 3.3.3,

$$\overline{\varphi(\mathbb{A}_K^m \backslash Z)} = \overline{\pi_{m+1}(V(J))} = V(J_{m+1}).$$

■

Remark 3.5.3 *With the notation as in Proposition 3.5.2, the graph of* φ *is*

$$\Gamma(\varphi) = V(J \cap K[t_1, .., t_m, x_1, \ldots, x_n]).$$

Example 3.5.4 *Consider the rational map*

$$\begin{array}{rccc} \varphi: & \mathbb{A}^1_K & \dashrightarrow & \mathbb{A}^2_K \\ & t & \mapsto & \left(\frac{1-t^2}{t^2+1}, \frac{2t}{t^2+1}\right) \end{array}$$

defined on the complement of $Z = V(t^2+1)$. *To determine the image, we calculate a Gröbner basis of*

$$I = \left\langle \left(t^2+1\right)x - \left(1-t^2\right),\ \left(t^2+1\right)y - 2t,\ 1 - \left(t^2+1\right)^2 s \right\rangle$$

for lp with $s > t > x > y$ *using* SINGULAR:

```
ring R=0,(s,t,x,y),lp;
ideal I = (t2+1)*x-(1-t2), (t2+1)*y-2t, 1-(t2+1)^2*s;
option(redSB);
std(I);
_[1]=x2+y2-1
_[2]=ty+x-1
_[3]=tx+t-y
_[4]=4s-2x+y2-2
```

Hence, the closure of the image of φ

$$C = \overline{\operatorname{im}(\varphi)} = V(I_2) = V(x^2+y^2-1)$$

is a circle.

Definition 3.5.5 *A* ***rational parametrization*** *of the algebraic variety* $X \subset \mathbb{A}^n_K$ *is a rational map* $\varphi : \mathbb{A}^m_K \dashrightarrow \mathbb{A}^n_K$ *with* $\overline{\operatorname{im}(\varphi)} = X$.

In general the parametrization problem is much more complicated. Indeed, most varieties do not admit a rational parametrization. For the circle, however, the problem is easy:

Remark 3.5.6 *To find* φ, *we do stereographic projection from a point* P *on the circle* C *to a line, for example, from* $P = (-1, 0)$ *to* $\{x = 0\}$. *So consider the* ***linear system*** *of all lines*

$$L_t = \{y - t(x+1) = 0\} \subset \mathbb{A}^2_K$$

through P, *and* $t \in \mathbb{P}^1_K = \mathbb{A}^1_K \cup \{\infty\}$. *Writing*

$$\begin{array}{lcl} L_t \cap C & = & \{P, P_t\} \\ L_t \cap \{x = 0\} & = & \{Q_t\} = \{(0, t)\} \end{array}$$

we define

$$\varphi(Q_t) = P_t,$$

see Figure 3.6. As an exercise do the calculation. Note that the affine space $\mathbb{A}^1_K$ is not sufficient to parametrize all points of C: In order to obtain P we have to consider the vertical line L_∞ which corresponds to the point at infinity on $\mathbb{A}^1_K$. Hence, we have to pass from affine to the ***projective space*** $\mathbb{P}^1_K$.

This is a hint, that birational geometry should better be done with projective varieties.

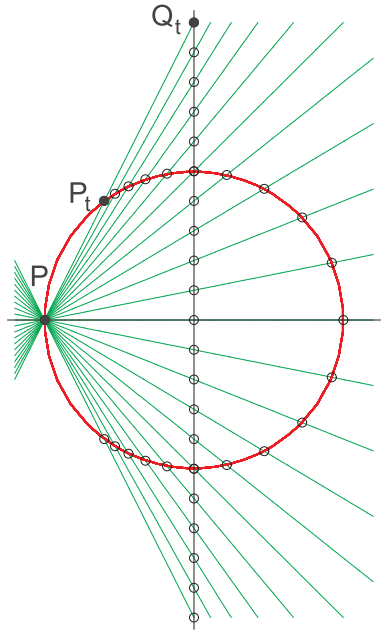

Figure 3.6: Rational parametrization of the circle.

Remark 3.5.7 *The parametrization is indeed birational. The inverse*

$$\varphi^{-1} = \left(\frac{x}{x+1}\right) : \mathbb{A}^1_K \dashrightarrow C$$

is obtained by solving the equation of the line for t.

Like in the case of polynomial maps, we can generalize rational maps between affine spaces to rational maps between algebraic varieties.

Definition 3.5.8 *If $I \subset K[x_1, ..., x_n]$ is a prime ideal and $X = V(I) \subset \mathbb{A}^n_K$ is the corresponding algebraic variety, then the* ***coordinate ring***

$$K[X] = K[x_1, ..., x_n]/I$$

of X is an integral domain. Hence, we can form the quotient field

$$K(X) = \mathrm{quot}(K[X])$$

by calculating with fractions. It describes the rational functions on X and is called the ***rational function field*** *of X.*

The ***domain of definition*** *$D(q)$ of $q \in K(X)$ is*

$$D(q) = \left\{ x \in X \mid \exists \bar{f}, \bar{g} \in K[X] \text{ with } \bar{g}(x) \neq 0 \text{ and } q = \frac{\bar{f}}{\bar{g}} \right\}.$$

So q is a well-defined map $q : D(q) \to \mathbb{A}^1_K$.

Definition 3.5.9 *A* ***rational map***

$$\varphi = (q_1, \ldots, q_n) : X \dashrightarrow \mathbb{A}^n_K$$

is a tuple of rational functions $q_i \in K(X)$. The ***domain of definition*** *$D(\varphi)$ of φ is*

$$D(\varphi) = D(q_1) \cap \ldots \cap D(q_n),$$

and the image of φ is

$$\mathrm{im}(\varphi) = \varphi(D(\varphi)).$$

If $Y \subset \mathbb{A}^n_K$ is a variety, then a rational map

$$\varphi : X \dashrightarrow Y$$

is a rational map $\varphi : X \dashrightarrow \mathbb{A}^n_K$ with $\mathrm{im}(\varphi) \subset Y$.

A straightforward combination of the ideas of Propositions 3.4.6 and 3.5.2 generalizes these result to an algorithm for computing the image of a rational map $X \dashrightarrow \mathbb{A}^n_K$ (we skip the proof):

Algorithm 3.5.10 *Suppose $K = \overline{K}$, $I \subset K[t_1, \ldots, t_m]$ is a prime ideal, $X = V(I) \subset \mathbb{A}^m_K$ is the corresponding algebraic variety*

$$\varphi = \left(\frac{\bar{f}_1}{\bar{g}_1}, \ldots, \frac{\bar{f}_n}{\bar{g}_n} \right) : X \dashrightarrow \mathbb{A}^n_K$$

is a rational map, and $g = g_1 \cdot \ldots \cdot g_n$. Then for the closure of the image of φ it holds

$$\overline{\mathrm{im}\,(\varphi)} = V\left(J_{m+1}\right)$$

where

$$J = \langle I \rangle + \langle g_1 x_1 - f_1, \ \ldots, \ g_n x_n - f_n, \ 1 - gs \rangle \subset k\left[s, t_1, .., t_m, x_1, \ldots, x_n\right].$$

Example 3.5.11 *We compute the image of the node*

$$X = V(t_1^3 + t_1^2 - t_2^2) \subset \mathbb{A}_K^2$$

(see Figure 3.7) under the rational map

$$\frac{\bar{t}_1}{\bar{t}_2} : X \dashrightarrow \mathbb{A}_K^1$$

using SINGULAR*:*

```
ring R=0,(s,t1,t2,x),lp;
ideal I = t1^3+t1^2-t2^2, t2*x-t1,1-t2*s;
std(I);
t2*x^3+x^2-1
t1-t2*x
s*x^2-s+x^3
s*t2-1
```

Hence the closure of the image

$$\overline{\operatorname{im}(\varphi)} = V(0) = \mathbb{A}_K^1$$

is the whole of $\mathbb{A}_K^1$.

The map φ *is indeed birational: From the equations*

$$\begin{aligned} t_2x^3 + x^2 - 1 &= 0 \\ t_1 - t_2x &= 0 \end{aligned}$$

we can read off the inverse

$$\varphi^{-1} = \left(-\frac{x^2-1}{x^2}, \frac{x^2-1}{x^3}\right) : \mathbb{A}_K^1 \dashrightarrow X$$

which yields a rational parametrization of X.

See also Exercise 1.5.2.

Example 3.5.12 *Let* $I = \langle xy - zw \rangle \subset R = K[x,y,z,w]$ *and* $X = V(I) \subset \mathbb{A}_K^3$. *Then* $K[X] = R/I$ *is not a unique factorization domain, for example,*

$$\bar{x}\bar{y} = \bar{z}\bar{w}.$$

Hence we have two representations for the rational function

$$q = \frac{\bar{x}}{\bar{z}} = \frac{\bar{w}}{\bar{y}} \in K(X)$$

So

$$S \backslash V(z) \subset D(q) \quad \text{and} \quad S \backslash V(y) \subset D(q)$$

hence

$$S \backslash V(y,z) \subset D(q).$$

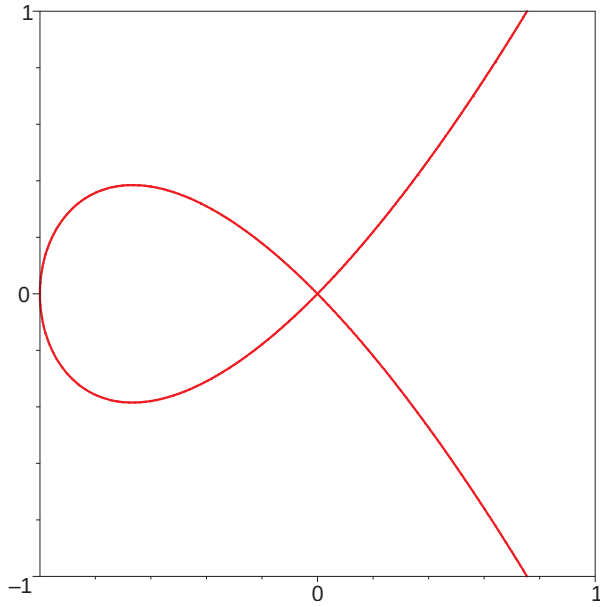

Figure 3.7: Node

Do we have equality? How to compute the domain of a rational function in general? The following lemma describes the domain by an ideal:

Algorithm 3.5.13 *Let $X \subset \mathbb{A}^n_K$ be a variety and $q = \frac{\bar{f}}{\bar{g}} \in K(X)$. Then the domain of definition of q is the complement*

$$D(q) = X \backslash V(N)$$

of the vanishing locus of the ideal

$$N = \{\gamma \in K[x_1, ..., x_n] \mid \gamma \cdot f \in \langle g \rangle + I(X)\}.$$

Proof. The possible denominators of q are the elements of the ideal

$$\overline{N} = \{\bar{\gamma} \in K[X] \mid \bar{\gamma} \cdot q \in K[X]\}$$

It is the image of N under the canonical epimorphism

$$K[x_1, ..., x_n] \to K[x_1, ..., x_n]/I(X) = K[X]$$

since

$$\bar{\gamma} \in K[X] \Leftrightarrow \bar{\gamma} \cdot \frac{\bar{f}}{\bar{g}} \in K[X] \Leftrightarrow \bar{\gamma} \cdot \bar{f} \in \langle \bar{g} \rangle \Leftrightarrow \gamma \cdot f \in \langle g \rangle + I(X) \Leftrightarrow \gamma \in N.$$

■

How can we compute the ideal N using Gröbner bases? It is a special case of an ideal quotient

$$I : J = \{w \in R \mid w \cdot J \subset I\}$$

of two ideals $I, J \subset R$. Indeed,

$$N = (\langle g \rangle + I(X)) : \langle f \rangle .$$

3.6 Ideal quotients

We discuss how to compute ideal quotients using Gröbner bases. Ideal quotients will also play a major role in primary decomposition.

Definition 3.6.1 *Let R be a ring. For ideal $I, J \subset R$ the* ***ideal quotient*** *is*

$$I : J = \{f \in R \mid f \cdot J \subset I\} .$$

Remark 3.6.2 *For all ideals $I, J \subset R$ it holds*

(1) $I : J$ *is an ideal of* R,

(2) $I \subset (I : J)$,

(3) $J \subset I$ *if and only if* $I : J = \langle 1 \rangle$.

For all ideals $I_1, \ldots, I_s, J \subset R$ it holds

(4) $(I_1 \cap \ldots \cap I_s) : J = (I_1 : J) \cap \ldots \cap (I_s : J)$,

(5) $J : (I_1 + \ldots + I_s) = (J : I_1) \cap \ldots \cap (J : I_s)$,

For all ideals $I, J, L \subset R$ it holds

(6) $(I : J) : L = I : (J \cdot L)$.

We do the straightforward proof in Exercise 3.5.

For computational purposes we now focus on ideals in $R = K[x_1, \ldots, x_n]$. By Remark 3.6.2.(5) and the ideal intersection algorithm 3.1.1, it is sufficient to compute ideal quotients by principal ideals: If $J = \langle g_1, \ldots, g_r \rangle$ then

$$I : J = I : (\langle g_1 \rangle + \ldots + \langle g_r \rangle) = (I : \langle g_1 \rangle) \cap \ldots \cap (I : \langle g_r \rangle) .$$

Again using the ideal intersection algorithm, we can compute:

Algorithm 3.6.3 *Let $I \subset R$ be an ideal and $g \in R$. If we write*

$$I \cap \langle g \rangle = \langle g \cdot f_1, \ldots, g \cdot f_s \rangle$$

with $f_i \in R$, then it holds

$$I : \langle g \rangle = \langle f_1, \ldots, f_s \rangle .$$

Proof. Any element of $I \cap \langle g \rangle$ is a multiple of g, so

$$I \cap \langle g \rangle = \langle g \cdot f_1, \ldots, g \cdot f_s \rangle .$$

By

$$\langle f_1, \ldots, f_s \rangle \cdot g \subset I$$

we have

$$\langle f_1, \ldots, f_s \rangle \subset I : \langle g \rangle .$$

On the other hand, if $f \in I : \langle g \rangle$, then $f \cdot g \in I \cap \langle g \rangle$, so

$$f \cdot g = \textstyle\sum_i a_i \cdot g \cdot f_i = g \cdot \sum_i a_i \cdot f_i$$

with $a_i \in R$. Hence

$$f = \textstyle\sum_i a_i f_i \in \langle f_1, \ldots, f_s \rangle .$$

■

Example 3.6.4 *We compute the domain of*

$$q = \frac{\bar{x}}{\bar{z}} \in K(X)$$

where $X = V(xy - zw) \subset \mathbb{A}^4_K$ using Singular*:*

```
ring R=0,(x,y,z,w),dp;
ideal I = xy-zw;
quotient(I+ideal(z),ideal(x));
_[1]=z
_[2]=y
```

So the domain of q is the complement of the plane $V(y, z) \subset X$.

We can interpret ideal quotients geometrically as follows:

Theorem 3.6.5 *Let $I, J \subset R$ be ideals.*

1) *If $I \subset R$ is a prime ideal, and $J \not\subset I$ is an ideal then $I : J = I$.*

2) If $I = \bigcap_{l=1}^{s} I_l$ with I_l prime and J is an ideal, then

$$I : J = \bigcap_{J \notin I_l} I_l$$

Proof. Let $g \in J$ with $g \notin I$. If $f \in I : J$, that is, $f \cdot J \subset I$, then $f \cdot g \in I$. Since I is a prime ideal, it follows that $f \in I$.

Using the first claim and Remark 3.6.2.(5) and (3), the second claim follows:

$$I : J = (\bigcap_{J \notin I_l} \underbrace{(I_l : J)}_{I_l}) \cap (\bigcap_{J \subset I_l} \underbrace{(I_l : J)}_{R})$$

■

For prime ideals I_l by the Nullstellensatz

$$J \subset I_l \Rightarrow V(I_l) \subset V(J) \Rightarrow \sqrt{J} \subset I_l \Rightarrow J \subset I_l$$

that is,

$$J \subset I_l \Leftrightarrow V(I_l) \subset V(J)$$

hence:

Corollar 3.6.6 *If $I = \bigcap_{l=1}^{s} I_l$ with $I_l \subset R$ prime and $J \subset R$ is an ideal, then*

$$V(I : J) = \bigcup_{V(I_l) \notin V(J)} V(I_l)$$

This implies

$$V(I : J) = \overline{V(I) \backslash V(J)}$$

Example 3.6.7 *Consider the ideal*

$$I = \left\langle x^2 - x,\ y^2 - y \right\rangle = \langle x, y \rangle \cap \langle x, y-1 \rangle \cap \langle x-1, y \rangle \cap \langle x-1, y-1 \rangle \subset K[x, y]$$

with

$$V(I) = \{(0,0), (0,1), (1,0), (1,1)\}.$$

For $J = \langle x - y \rangle$ we compute:

```
ring R=0,(x,y),dp;
ideal I = x2-x, y2-y;
ideal J = x-y;
quotient(I, J);
_[1]=x+y-1
_[2]=y2-y
```

So

$$I : J = \left\langle x + y - 1,\ y^2 - y \right\rangle,$$

hence

$$V(I : J) = \{(0,1), (1,0)\},$$

see Figure 3.8.

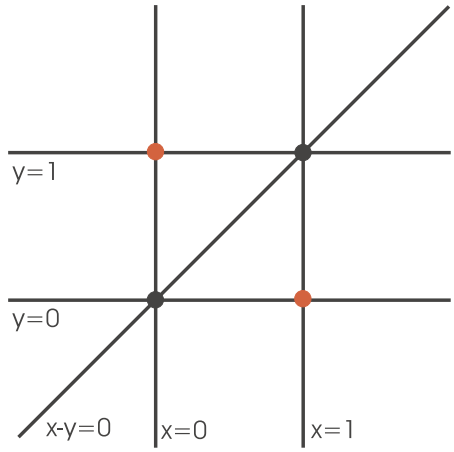

Figure 3.8: Ideal quotient

3.7 Solving algebraic systems with a finite set of solutions

Suppose $K = \overline{K}$. Given an ideal $I \subset K[x_1, ..., x_n]$ with a finite set of solutions, how to compute the points of $V(I)$ explicitly? The naive algorithm would be:

1) Project to each coordinate, that is, compute $I \cap K[x_i] = \langle f_i \rangle$ by elimination (note that $K[x_i]$ is a principal ideal domain).

2) Compute the finite sets $V(f_i)$, for example by numerical techniques.

3) Check, which points of $V(f_1) \times ... \times V(f_n)$ are contained in $V(I)$.

Example 3.7.1 *Consider the ideal*

$$I = \left\langle 2x^2 - xy + 2y^2 - 2,\ 2x^2 - 3xy + 3y^2 - 2 \right\rangle$$

from Section 1.1.

```
ring R=0,(x,y),lp;
ideal I = 2x2-xy+2y2-2, 2x2-3xy+3y2-2;
eliminate(I,x);
_[1] = y3-y
eliminate(I,y);
_[1] = 4x4 - 5x2 + 1
```

Hence, by

$$I \cap K[y] = \left\langle y^3 - y \right\rangle = \langle y(y+1)(y-1) \rangle$$

and

$$I \cap K[x] = \left\langle 4x^4 - 5x^2 + 1 \right\rangle = \langle (x+1)(x-1)(2x+1)(2x-1) \rangle$$

we get

$$V(I) \subset \{0, -1, 1\} \times \{-1, 1, -\frac{1}{2}, \frac{1}{2}\}.$$

Testing these 9 *points with respect to the generators of* I *yields*

$$V(I) = \left\{ (1,0), (-1,0), \left(\frac{1}{2}, 1\right), \left(-\frac{1}{2}, -1\right) \right\}.$$

But we can do better. The cornerstone is the following theorem:

Theorem 3.7.2 *Let* $K = \overline{K}$, $I \subset K[x_1, ..., x_n]$. *Then the following are equivalent:*

1) $|V(I)| < \infty$

2) *If* G *is a Gröbner basis of* I, *then for every* i *there is a* $g \in G$ *with*

$$L(g) = x_i^{\alpha_i}$$

and $\alpha_i \geq 0$.

3) $\dim_K(K[x_1, ..., x_n]/I) < \infty$.

Proof. For (1) $\Rightarrow$ (2) consider the projection

$$\pi : V(I) \to \mathbb{A}^1_K, \ (a_1, ..., a_n) \mapsto a_i$$

Then

$$f = \prod_{t \in \pi(V(I))} (x_i - t) \in I(V(I)) = \sqrt{I},$$

hence $f^w \in I$ for some $w \geq 1$, so $L(f^w) \in L(I)$.

(2) $\Leftrightarrow$ (3) follows, since (by Exercise 2.12)

$$K[x_1, ..., x_n]/I \cong {}_K\langle x^\alpha \mid x^\alpha \notin L(I) \rangle$$

as K-vector spaces.

(3) $\Rightarrow$ (1): Since $\dim_K(K[x_1, ..., x_n]/I) < \infty$ the classes $\bar{x}_i^0, \bar{x}_i^1, \bar{x}_i^2, ...$ are linearly dependent, so there is a $0 \neq f_i \in K[x_i]$ with $f_i \in I$. As above,

$$V(I) \subset V(f_1) \times ... \times V(f_n).$$

■

In Exercise 3.8 we show that $\dim_K(K[x_1, ..., x_n]/I)$ is a bound for the number of solutions, and equality holds if I is radical.

Remark 3.7.3 *By the previous theorem, if $V(I) \neq \emptyset$, the minimal Gröbner basis of I for lp with $x_1 > ... > x_n$ contains equations*

$$\begin{aligned}
&\boldsymbol{x}_1^{\alpha_1} - g_1(x_1, ..., x_n)\\
&\boldsymbol{x}_2^{\alpha_2} - g_2(x_2, ..., x_n)\\
&\vdots\\
&\boldsymbol{x}_{n-1}^{\alpha_{n-1}} - g_{n-1}(x_{n-1,}x_n)\\
&g_n(x_n)
\end{aligned}$$

with $\alpha_i > 0$.

To determine $V(I)$ solve the equations for $x_n, ..., x_1$ and keep those solutions, which satisfy the remaining Gröbner basis elements. This can be done by numerical methods for solving univariate polynomial equations.

Example 3.7.4 *Consider again, the intersection of two ellipses from Section 1.1. As we have already seen there, for $y > x$ we get:*

```
ring R=0,(y,x),lp;
ideal I = 2x2-xy+2y2-2, 2x2-3xy+3y2-2;
std(I);
_[1]=4x4-5x2+1
_[2]=3y+8x3-8x
```

Solving $4x^4 - 5x^2 + 1 = 0$ yields

$$x = 1, -1, \frac{1}{2}, -\frac{1}{2}$$

and from the second equation we get

$$V(I) = \left\{(1,0), (-1,0), (\frac{1}{2}, 1), (-\frac{1}{2}, -1)\right\}.$$

On the other hand, for $x > y$,

```
ring R=0,(x,y),lp;
ideal I = 2x2-xy+2y2-2, 2x2-3xy+3y2-2;
std(I);
_[1]=y3-y
_[2]=2xy-y2
_[3]=2x2-3xy+3y2-2
```

so we get

$$y = 0, 1, -1.$$

Solving the third equality yields

$$V(I) \subset \left\{(1,0), (-1,0), (1,1), (\frac{1}{2}, 1), (-1,-1), (-\frac{1}{2}, -1)\right\}.$$

To obtain $V(I)$, we discart the solutions $(1,1), (-1,-1)$ which do not satisfy $2xy - y^2 = 0$.

See also Exercise 3.9.

3.8 Exercises

Exercise 3.1 *Show that for*

$$C = \left\{\left(t^2 - 1, t^3 - t\right) \mid t \in \mathbb{R}\right\} \subset \mathbb{A}^2_{\mathbb{R}}$$

we have $I(C) = \langle x^3 + x^2 - y^2 \rangle$. *Make a plot of the curve.*

Exercise 3.2 *Show, that for* $\operatorname{char}(K) \neq 2$ *the circle* $C = V(x^2 + y^2 - 1) \subset \mathbb{A}^2_K$ *does not admit a polynomial parametrization.*

Exercise 3.3 *Let*

$$S = V\left(t_1^2 + t_2^2 + t_3^2 - 1\right) \subset \mathbb{A}^3_K$$

be the unit sphere, and consider the morphism

$$\begin{aligned} \alpha : S &\to \mathbb{A}^3_K \\ (t_1, t_2, t_3) &\mapsto (t_1 t_2,\ t_1 t_3,\ t_2 t_3) \end{aligned}$$

Show, that

1) *if* $K = \mathbb{R}, \mathbb{C}$ *then*

$$X = \overline{\operatorname{im}(\alpha)} = V\left(x_1^2 x_2^2 + x_1^2 x_3^2 + x_2^2 x_3^2 - x_1 x_2 x_3\right),$$

2) *if* $K = \mathbb{C}$, *then* $\operatorname{im}(\alpha) = X$,

3) *if* $K = \mathbb{R}$, *then* $\operatorname{im}(\alpha) \subsetneqq X$.

Exercise 3.4 *Compute the closure of the image of the curve (Figure 3.9)*

$$C = V\left(y^3 - 3x^2 y - (x^2 + y^2)^2\right) \subset \mathbb{A}^2_{\mathbb{R}}$$

under the rational map

$$\varphi = \left(\frac{\bar{x}^2}{\bar{y}^2}, \frac{\bar{x}}{\bar{y}}\right) : C \dashrightarrow \mathbb{A}^2_{\mathbb{R}}$$

Exercise 3.5 *Let* $R = K[x_1, \ldots, x_n]$ *be a polynomial ring over a field* K *and for ideals* $I, J \subset R$

$$I : J = \{f \in R \mid f \cdot J \subset I\}$$

the ideal quotient. Prove that:

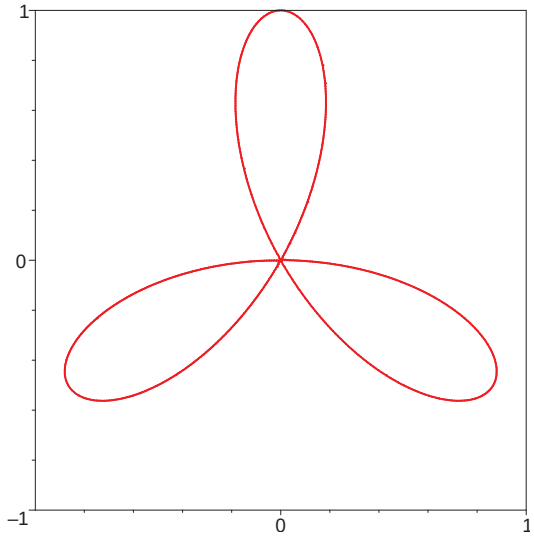

Figure 3.9: Curve with triple point

1) *For all ideals* $I, J \subset R$ *it holds*

   (a) $I : J$ *is an ideal of* R,

   (b) $I \subset (I : J)$,

   (c) $J \subset I$ *if and only if* $I : J = \langle 1 \rangle$.

2) *For all ideal* $I_1, \ldots, I_s, J \subset R$ *it holds*

   (a) $(I_1 \cap \ldots \cap I_s) : J = (I_1 : J) \cap \ldots \cap (I_s : J)$,

   (b) $J : (I_1 + \ldots + I_s) = (J : I_1) \cap \ldots \cap (J : I_s)$.

3) *For all ideals* $I, J, L \subset R$ *it holds*

$$(I : J) : L = I : (J \cdot L).$$

Exercise 3.6 *Let* $R = K[x_1, \ldots, x_n]$.

1) *Using the* SINGULAR *command* `eliminate`, *write a procedure that computes* $I \cap J$ *for ideals* $I, J \subset R$.

2) *Suppose* $J = \langle g \rangle \subset R$ *is principal and* $I \subset R$ *is an ideal. Applying your ideal intersection command from (1), write a* SINGULAR *procedure which computes* $I : J$.

3) *For any two ideals* $I, J \subset R$, *write a procedure that computes* $I : J$. *Try out some examples.*

Exercise 3.7 *Let*

$$I = \left\langle xz - y^2,\ x - yz \right\rangle \subset \mathbb{R}[x, y, z]$$

1) *Use your implementation from Exercise 3.6 to compute*

$$J = I : \langle x \rangle$$

and

$$I : J$$

Compare with the SINGULAR *command* `quotient`.

2) *Write I as an intersection of two prime ideals.*

3) *Make a plot of $V(I) \subset \mathbb{A}^3_{\mathbb{R}}$. Hint: Find a polynomial parametrization of $V(J)$.*

Exercise 3.8 *Let $K = \overline{K}$, and $I \subset K[x_1, ..., x_n]$ with $|V(I)| < \infty$. Show that*

$$|V(I)| \leq \dim_K (K[x_1, ..., x_n]/I)$$

and equality holds if I is radical.

Hint: Use interpolation to find a basis.

Exercise 3.9 *Let $K = \overline{K}$, and $I \subset K[x_1, ..., x_n]$ with $|V(I)| < \infty$. Then the following conditions are equivalent:*

1) *For all $p, q \in V(I)$ with $p \neq q$ we have $p_n \neq q_n$ and I is radical.*

2) *The reduced Gröbner basis of I with respect to the lexicographic ordering with $x_1 > ... > x_n$ has the form*

$$\begin{aligned} & x_1 - g_1(x_n) \\ & x_2 - g_2(x_n) \\ & \vdots \\ & x_{n-1} - g_{n-1}(x_n) \\ & g_n(x_n) \end{aligned}$$

and $g_n(x_n)$ is squarefree.

Hint: Use Exercise 3.8.

4

Modules over principal ideal domains

4.1 Overview

In the same way as for ideals, we first discuss the special case of modules over principal ideal domains R like $\mathbb{Z}$ or the polynomial ring $K[x]$ in one variable over a field. Examples you know are vector spaces over a field K, or abelian groups G, which are exactly the $\mathbb{Z}$-modules with the scalar multiplication

$$\mathbb{Z} \times G \to G,\ (n, g) \mapsto n \cdot g = \underbrace{g + \ldots + g}_{n}$$

Groups as $\mathbb{Z}$-modules play an important role, for example, in the theory of toric varieties (divisor class group).

For modules over principle ideal domains, we will describe an algorithm, which generalizes, like Buchberger's algorithm, both Gaussian reduction and the Euclidean algorithm. An interesting class of R-modules (however not the most general, as we will see) are images $M = \mathrm{im}(A)$ of matrices $A \in R^{n \times m}$. To describe M and to decide, whether a given vector $v \in R^n$ is contained in M, we require a suitable normal form for A.

From linear algebra over a field K we know: If $A \in K^{n \times m}$, then there are changes of bases $T \in \mathrm{GL}(m, K)$ and $S \in \mathrm{GL}(n, K)$, which transform A to the normal form

$$S \cdot A \cdot T = \left(\begin{array}{ccc|c} 1 & & & \\ & \ddots & & 0 \\ & & 1 & \\ \hline & 0 & & 0 \end{array}\right) = D$$

(where the number of ones on the diagonal is the rank of A). Then $v \in \mathrm{im}(A)$ if and only if $S \cdot v \in \mathrm{im}(D)$, which in turn we can decide immediately.

If we replace K by a principal ideal domain R, then we cannot expect the normal form to be that simple any more: By the adjoint matrix formula for the inverse, a matrix $T \in R^{n\times n}$ is invertible if and only if $\det(T)$ is a unit. For example $A = (2) \in \mathbb{Z}^{1\times 1}$ already is in normal form, because $\mathbb{Z}^\times = \{\pm 1\}$. In general we can achieve that

$$S \cdot A \cdot T = D = \left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & 0 \\ & & d_r & \\ \hline & 0 & & 0 \end{array}\right) \in R^{n\times m}$$

where d_i is a divisor of d_{i+1} for all i and the d_i are uniquely determined by A.

The chapter is organized as follows: We first prove this claim in the elementary divisor theorem. The proof also gives an algorithm to obtain S, T and D. Using the normal form D we prove various structure results: Generalizing vector spaces over a field, we first recall some basic facts on modules over a ring, and then describe finitely generated modules over principle ideal domains. In particular, we will discuss finitely generated abelian groups ($\mathbb{Z}$-modules), and the Jordan normal form.

4.2 The elementary divisor algorithm

Remark 4.2.1 *A matrix $A \in R^{n\times n}$ is invertible (that is, $A \in \mathrm{GL}(n, R)$) if and only if its determinant is a unit, that is,*

$$\det(A) \in R^\times$$

Proof. If $A \cdot A^{-1} = E$, then $\det(A) \cdot \det(A^{-1}) = 1$. On the other hand, if $\det(A) \in R^\times$, then

$$A^{-1} = \frac{A^{adj}}{\det(A)} \in R^{n\times n}$$

with the adjoint matrix $A^{adj} = \left((-1)^{i+j} \det(A_{ji})\right)_{i,j} \in R^{n\times n}$, where A_{ji} is obtained by canceling the j-th row and i-th column of A. ■

Theorem 4.2.2 (Elementary divisor theorem) *Let R be a principal ideal domain and $A \in R^{n\times m}$. Then there are $S \in \mathrm{GL}(n, R)$ and*

$T \in \mathrm{GL}(m, R)$ and $r \leq \min(n, m)$ with

$$S \cdot A \cdot T = D = \left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & 0 \\ & & d_r & \\ \hline & 0 & & 0 \end{array}\right) \in R^{n \times m}$$

and

$$d_1 \mid d_2, \quad d_2 \mid d_3 \quad \ldots \quad d_{r-1} \mid d_r \neq 0$$

*The d_i are uniquely determined by A up to multiplication with units, and are called the **elementary divisors** of A, and D is called the **Smith normal form** of A.*

Remark 4.2.3 *In the special case where $R = K$ is a field, we can achieve $d_i = 1$ and we obtain S as a product of row operations and T as a product of column operations, see Section 1.5. Permuting rows and columns, we can assume that $a_{11} \neq 0$ (if $A \neq 0$). Subtracting the $\frac{a_{1,j}}{a_{1,1}}$-multiple of the first column from the j-th column (and in the same way for rows) we transform A to*

$$\left(\begin{array}{c|ccc} a_{1,1} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & * & \\ 0 & & & \end{array}\right)$$

Finally, multiply the first column by $\frac{1}{a_{1,1}}$. The claim follows by induction.

In a ring R it is in general not possible to form $\frac{a_{1,j}}{a_{1,1}}$ as $a_{1,1}$ may not be a unit. We now prove Theorem 4.2.2 in the case that R is a Euclidean domain (see Definition 2.2.3). Here we can replace the division $\frac{a_{1,j}}{a_{1,1}}$ by the division with remainder. The proof yields an algorithm to compute the Smith normal form.

Proof. Let R be a Euclidean domain with norm d. We may assume that $A \neq 0$.

1) By permuting rows and columns we can assume that $a_{1,1} \neq 0$ and
$$d(a_{1,1}) \leq d(a_{i,j}) \text{ or } a_{i,j} = 0$$
for all $(i, j) \neq (1, 1)$.

2) If some entry $a_{1,j}$ in the first row (analogously for the first column) is not divisible by $a_{1,1}$, then write by division with remainder
$$a_{1,j} = q \cdot a_{1,1} + r$$

with $d(r) < d(a_{1,1})$. The case $r = 0$ does not happen, since by assumption $a_{1,1} \nmid a_{1,j}$.

After subtracting q times the 1st column from the j-th column, we obtain

$$d(a_{1,1}) > d(a_{1,j})$$

Now go back to step (1). This process terminates, since $d(a_{1,1})$ becomes smaller in every run.

3) If, now, all entries of the first row and column are divisible by $a_{1,1}$, by adding multiples of the first column, we can transform A into

$$\left(\begin{array}{c|ccc} a_{1,1} & 0 & \cdots & 0 \\ \hline & & & \\ * & & * & \\ & & & \end{array}\right)$$

and, by adding multiples of the first row, further to

$$\left(\begin{array}{c|ccc} a_{1,1} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right)$$

If A' has an entry $a_{i,j}$, which is not divisible by $a_{1,1}$, we add the i-th row to the first row and go back to (2). Again, $d(a_{1,1})$ decreases strictly.

4) If all entries of A are divisible by $a_{1,1}$, then also the entries of A', since they are R-linear combinations of entries of A.

By induction on $\min(n, m)$ the claim follows.

For the induction start ($n = 1$ or $m = 1$) the steps (1) – (3) are the Euclidean algorithm on the entries of the matrix. ■

Before discussing the general case over a principle ideal domain R and the uniqueness, we test the algorithm at an example:

Example 4.2.4 *We compute the Smith normal form of*

$$A = \begin{pmatrix} 6 & 9 & 6 \\ 6 & 6 & 7 \end{pmatrix} \in \mathbb{Z}^{2\times 3}$$

and at the same time $S \in \mathrm{GL}(2, \mathbb{Z})$ *and* $T \in \mathrm{GL}(3, \mathbb{Z})$ *by simultaneously doing the row and column operations on a* 2×2 *respectively* 3×3 *unit matrix. Division by remainder (step* 2*) yields*

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 6 & 3 & 6 \\ 6 & 0 & 7 \end{pmatrix} \quad \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Permuting (step 1)

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 3 & 6 & 6 \\ 0 & 6 & 7 \end{pmatrix} \quad \begin{pmatrix} -1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Reducing the first row and column (step 3)

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 7 \end{pmatrix} \quad \begin{pmatrix} -1 & 3 & 2 \\ 1 & -2 & -2 \\ 0 & 0 & 1 \end{pmatrix}$$

Since 7 is not divisible by 3, we add the second to the first row

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 3 & 6 & 7 \\ 0 & 6 & 7 \end{pmatrix} \quad \begin{pmatrix} -1 & 3 & 2 \\ 1 & -2 & -2 \\ 0 & 0 & 1 \end{pmatrix}$$

Division by remainder (step 2)

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 3 & 6 & 1 \\ 0 & 6 & 7 \end{pmatrix} \quad \begin{pmatrix} -1 & 3 & 4 \\ 1 & -2 & -4 \\ 0 & 0 & 1 \end{pmatrix}$$

Permuting (step 1)

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 6 & 3 \\ 7 & 6 & 0 \end{pmatrix} \quad \begin{pmatrix} 4 & 3 & -1 \\ -4 & -2 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Reducing the first row and column (step 3)

$$\begin{pmatrix} 1 & 1 \\ -7 & -6 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -36 & -21 \end{pmatrix} \quad \begin{pmatrix} 4 & -21 & -13 \\ -4 & 22 & 13 \\ 1 & -6 & -3 \end{pmatrix}$$

Applying the algorithm to the submatrix obtained by deleting (or ignoring) the first row and column, we can proceed, for example, as follows

$$\begin{pmatrix} -36 & -21 \end{pmatrix} \mapsto \begin{pmatrix} -15 & -21 \end{pmatrix} \mapsto \begin{pmatrix} -15 & -6 \end{pmatrix} \mapsto \begin{pmatrix} -3 & -6 \end{pmatrix} \mapsto \begin{pmatrix} -3 & 0 \end{pmatrix}$$

(in this case this is just the Euclidean algorithm computing the gcd). This yields the Smith normal form

$$D = S \cdot A \cdot T$$

with

$$S = \begin{pmatrix} 1 & 1 \\ -7 & -6 \end{pmatrix} \qquad D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \end{pmatrix} \qquad T = \begin{pmatrix} 4 & 2 & -9 \\ -4 & 1 & 2 \\ 1 & -3 & 6 \end{pmatrix}$$

Hence, the elementary divisors of A are

$$d_1 = 1 \qquad d_2 = 3$$

up to multiplication with units $\mathbb{Z}^\times = \{1, -1\}$.

Using the MAPLE *package* LINEARALGEBRA *we can do the calculation as follows:*

```
with(LinearAlgebra):
A := Matrix([[6,9,6],[6,6,7]]):
SmithForm(A);
```

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix}$$

```
(S, T) := SmithForm(A, output=['U', 'V']):
S, T;
```

$$\begin{pmatrix} 0 & 1 \\ -1 & 3 \end{pmatrix}, \begin{pmatrix} -2 & 1 & -9 \\ 1 & -1 & 2 \\ 1 & 0 & 6 \end{pmatrix}$$

Note that S and T are not uniquely determined.

If, more generally, R is a principal ideal domain, we can prove Theorem 4.2.2 in a similar way, replacing the Euclidean algorithm by the following remark:

Remark 4.2.5 *Let R be a principal ideal domain, and $A = (a_{1,1},\ a_{1,2}) \in R^{1\times 2}$. Then there are $x, y \in R$ with*

$$\gcd(a_{1,1}, a_{1,2}) = d = x \cdot a_{1,1} + y \cdot a_{1,2}$$

(note that if R is not a principal ideal domain then in general $\gcd(a_{1,1}, a_{1,2}) \notin \langle a_{1,1},\ a_{1,2}\rangle$, hence such a representation of the gcd does not exist; note also, that over a Euclidean domain R, we can find x and y by the Euclidean algorithm). Write

$$a_{1,1} = u \cdot d \qquad a_{1,2} = v \cdot d$$

with $u, v \in R$. Then with

$$T = \begin{pmatrix} x & -v \\ y & u \end{pmatrix} \in \mathrm{GL}(2, R)$$

we have

$$A \cdot T = (d,\ 0)\,.$$

This procedure allows us to replace the steps $(1) - (3)$ *of the elementary divisor algorithm: If* $a_{1,1} \neq 0$ *then we can make all other entries in the first row and column zero. This process terminates, since the entries* $a_{1,1}$ *appearing in the process generate an ascending chain of ideals, which terminates, since* R *is Noetherian.*

Note that $\det(T) = 1$*, that is,* $T \in \mathrm{SL}(2, R)$*.*

Remark 4.2.6 *In the elementary divisor algorithm all transformations have determinant* ± 1 *(row/column transformations and permutation matrices). Hence, in Theorem 4.2.2 we can achieve that* $T \in \mathrm{SL}(m, R)$ *and* $S \in \mathrm{SL}(n, R)$ *(how?).*

That r and the elementary divisors d_i are unique up to units, follows from:

Theorem 4.2.7 *For the elementary divisors* $d_1, \ldots, d_r$ *of* $A \in R^{n \times m}$ *it holds*

$$d_1 \cdot \ldots \cdot d_i = \gcd\left(\det\left(A_{I,J}\right) \mid |I| = |J| = i\right) =: D_i$$

for $i \leq r$*. For* $i > r$ *all* $\det\left(A_{I,J}\right) = 0$*.*

Here, if $I \subset \{1, \ldots, n\}$ *and* $J \subset \{1, \ldots, m\}$*, we denote by*

$$A_{I,J} \in R^{|I| \times |J|}$$

the submatrix of A *with the rows* I *and the columns* J*. The* $\det\left(A_{I,J}\right)$ *with* $|I| = |J| = i$ *are also called the* $i \times i$*-**minors** of* A*.*

The D_i *are also called the* i*-th **determinantal divisors** of* A*.*

Note that $d_1 = D_1$ *is the greatest common divisor of all entries of* A*.*

Proof. We sketch the proof using some results from (multi-)linear algebra: The entries of the representing matrix of the i-th exterior power $\bigwedge^i A$ of A (with respect to a suitable basis) are exactly the $i \times i$-minors of A. Moreover, if $S \in R^{n \times n}$, then

$$\left(\bigwedge^i S\right) \cdot \left(\bigwedge^i A\right) = \bigwedge^i (S \cdot A)$$

If $S \in \mathrm{GL}(n, R)$, then for the gcd of the entries it holds

$$\gcd\left(\bigwedge^i (S \cdot A)\right) = \gcd\left(\bigwedge^i A\right)$$

(up to units), as any entry of $\bigwedge^i (S \cdot A)$ is a linear combination of the entries of $\bigwedge^i A$ and hence $\gcd\left(\bigwedge^i (S \cdot A)\right)$ is divisible by $\gcd\left(\bigwedge^i A\right)$. The converse is also true since $A = S^{-1} \cdot (S \cdot A)$.

For the base change T in the source we proceed in a similar fashion.

If we now have

$$S \cdot A \cdot T = D = \left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & 0 \\ & & d_r & \\ \hline & 0 & & 0 \end{array}\right)$$

according to the elementary divisor theorem, then

$$\begin{aligned} \gcd\left(\bigwedge^i A\right) &= \gcd\left(\bigwedge^i D\right) \\ &= \gcd\left(d_{j_1} \cdot \ldots \cdot d_{j_i} \mid 1 \leq j_1 < \ldots < j_i \leq r\right) \\ &= d_1 \cdot \ldots \cdot d_i \end{aligned}$$

since $d_j \mid d_k$ for $j \leq k$. ■

Example 4.2.8 *For*

$$A = \begin{pmatrix} 1 & 1 & 1 \\ -3 & 1 & 1 \\ 1 & -3 & 1 \\ 1 & 1 & -3 \end{pmatrix}$$

we compute the Smith normal form:

$$A \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 4 \\ 0 & -4 & 0 \\ 0 & 0 & -4 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 4 \\ 0 & -4 & 0 \\ 0 & 0 & -4 \end{pmatrix}$$

$$\mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & -4 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix} = D$$

On the other hand,

$$D_1 = 1 = d_1$$

the 2×2*-minors are equal to* 0, ± 4 *or* 8, *hence*

$$D_2 = 4 = d_1 \cdot d_2$$

and the 3×3*-minors are* ± 16, *hence*

$$D_3 = 16 = d_1 \cdot d_2 \cdot d_3.$$

The elementary divisor theorem 4.2.2 describes the structure of finitely generated modules over principal ideal domains:

4.3 Modules and presentations

We recall some basic facts on modules. Here R is any (not necessarily commutative) ring.

Definition 4.3.1 *An R-(left)-**module** $(M,+,\cdot)$ is a set M with maps*

$$\begin{aligned} + &: M \times M \longrightarrow M \\ \cdot &: R \times M \longrightarrow M \end{aligned}$$

such that

1) *$(M,+)$ is an abelian group,*

2) *the scalar multiplication $\cdot$ is distributive over the addition $+$, that is,*

$$\begin{aligned} r \cdot (m_1 + m_2) &= r \cdot m_1 + r \cdot m_2 \\ (r_1 \overset{R}{+} r_2) \cdot m &= r_1 \cdot m + r_2 \cdot m \end{aligned}$$

for all $r, r_1, r_2 \in R$ and $m, m_1, m_2 \in M$, and

3) *for all $r, s \in R$ and $m \in M$ it holds*

$$(r \overset{R}{\cdot} s) \cdot m = r \cdot (s \cdot m)$$

If R has a multiplicative unit 1, then we require, in addition, that $1 \cdot m = m$.

Usually it is clear from the context whether $+$ refers to the addition in R or M. If we want to be more precise, we note R respectively M over $+$ (and in the same way for $\cdot$).

Example 4.3.2 1) *Let $R = K$ be a field. Then a K-module is nothing else than a K-vector space.*

2) *A $\mathbb{Z}$-module G is nothing else than an abelian group $(G,+)$. The scalar multiplication is*

$$\begin{aligned} \mathbb{Z} \times G &\longrightarrow G \\ (n,g) &\longmapsto n \cdot g := \underbrace{g + \ldots + g}_{n\text{-times}} \end{aligned}$$

with $(-1) \cdot g := -g$.

3) *Let $(R,+,\cdot)$ be a commutative ring. Then a subset $I \subset R$ is an ideal if and only if $(I,+,\cdot)$ is an R-module.*

4) *If M_1 and M_2 are modules over R, then also the direct product $M_1 \times M_2$ is an R-module with $r \cdot (m_1, m_2) = (r \cdot m_1, r \cdot m_2)$, in particular:*

5) *If R is a ring, then*

$$R^n = \underbrace{R \times \ldots \times R}_{n}$$

is an R-module.

6) *Let $(M,+,\cdot)$ be an R-module. A* ***submodule*** *$U \subset M$ is a subgroup of $(M,+)$, on which the scalar multiplication can be restricted, that is, with*

$$r \cdot m \in U$$

for all $m \in U$ and $r \in R$. A submodule is again an R-module.

A subset $U \subset M$ is a submodule if and only if $U \neq \varnothing$ and

$$\begin{aligned} m_1 + m_2 &\in U \\ r \cdot m &\in U \end{aligned}$$

for all $m_i, m \in U$ and $r \in R$.

7) *Let M be an R-module and $U \subset M$ a submodule. Then the quotient group M/U is again an R-module (the* ***quotient module****) with the scalar multiplication*

$$r \cdot \bar{m} = r \cdot (m + U) = r \cdot m + U = \overline{r \cdot m}$$

for $r \in R$ and $m \in M$.

8) *Let V be a K-vector space and $A \in \operatorname{End}(V)$ an endomorphism (for example, $V = K^n$ and $A \in K^{n \times n}$). Then by the substitution homomorphism*

$$\begin{array}{ccc} K[x] & \longrightarrow & \operatorname{End}(V) \\ x & \longmapsto & A \end{array}$$

we can make the K-vector space V into a $K[x]$-module by defining the scalar multiplication as

$$\begin{aligned} K[x] \times V &\longrightarrow V \\ (f, v) &\longmapsto f \cdot v := f(A)(v) \end{aligned}$$

9) *An R-Algebra S is a ring $(S,+,\cdot)$ with an injective ring homomorphism $\varphi : R \to S$ and $\varphi(r)\cdot s = s\cdot\varphi(r)$ for all $r \in R$ and $s \in S$. With the scalar multiplication*

$$\begin{array}{rcl} * : R\times S & \longrightarrow & S \\ (r,s) & \longmapsto & r * s := \varphi(r)\cdot s \end{array}$$

S becomes an R-module.

Hence, an R-algebra is nothing else than a set S with operations

$$\begin{array}{ll} + : S\times S \to S & \textit{(addition)} \\ \cdot : S\times S \to S & \textit{(multiplication)} \\ * : R\times S \to S & \textit{(scalar multiplication)} \end{array}$$

such that

(a) *$(S,+,*)$ is an R-module,*

(b) *$(S,+,\cdot)$ is a ring, and*

(c) *for all $r \in R$ and $s_1, s_2 \in S$ it holds*

$$r * (s_1\cdot s_2) = (r * s_1)\cdot s_2 = s_1\cdot(r * s_2)\,.$$

Definition 4.3.3 *An R-**module homomorphism** is an R-linear group homomorphism $f : M \to N$ between R-modules, that is,*

1) *$f(m_1+m_2) = f(m_1)+f(m_2)$ for all $m_1, m_2 \in M$*

2) *$f(r\cdot m) = r\cdot f(m)$ for all $m \in M$ and $r \in R$.*

Kernel $\ker(f)$ *and image* $\operatorname{im}(f)$ *are submodules, and the homomorphism theorem for modules holds*

$$M/\ker(f) \cong \operatorname{im}(f)\,.$$

We define $\operatorname{coker}(f) = N/\operatorname{im}(f)$ *as the **cokernel** of f.*

Definition 4.3.4 *Let M be an R-module.*

1) *M is called **finitely generated**, if there is a surjective R-module homomorphism*

$$\varphi : R^r \to M\,.$$

*The images $m_i = \varphi(e_i) \in M$ of the standard basis vector e_i are called **generators**. The map φ is surjective if and only if,*

every element M can be written as an R-linear combination of $m_1, ..., m_r$, that is,

$$\forall m \in M \ \exists a_1, ..., a_r \in R \text{ with } m = a_1 m_1 + ... + a_r m_r.$$

We then write

$$M = \langle m_1, ..., m_r \rangle .$$

2) *M is called **free** of rank r, if there is an isomorphism $\varphi : R^r \to M$, that is*

$$M \cong R^r .$$

*The above representation $m = a_1 m_1 + ... + a_r m_r$ is then unique, and we call $m_1, ..., m_r$ a **basis** of M.*

3) *An R-module M is called **finitely presented**, if M is finitely generated and $\ker(\varphi)$ is also finitely generated.*

Example 4.3.5 *Considered as a $\mathbb{Z}$-module, the rational numbers $\mathbb{Q}$ are not finitely generated: Assume $\mathbb{Q}$ is generated by $r_1, ..., r_n$. Then there is a $d \in \mathbb{Z}$ coprime to the denominators r_i and $\frac{1}{d}$ does not lie in the $\mathbb{Z}$-module (that is, abelian group) $\langle r_1, ..., r_n \rangle$ generated by $r_1, ..., r_n$.*

A K-vector space of dimension r is, considered as a K-module, free of rank r (as any vector space has a basis).

The ring $R = K[x_1, x_2, ...]$ of polynomials in countably many variables is as an R-module finitely generated (by 1). However its submodule

$$M = \{ f \in R \mid f(0) = 0 \}$$

is not, since it contains all x_i, however any finite set of polynomials involves only finitely many variables.

The following short hand notation is very useful:

Definition 4.3.6 *A sequence of R-module homomorphisms*

$$... \to M_i \xrightarrow{\varphi_i} M_{i+1} \xrightarrow{\varphi_{i+1}} M_{i+2} \to ...$$

*is called **exact**, if*

$$\operatorname{im}(\varphi_i) = \ker(\varphi_{i+1}) \ \ \forall i.$$

Remark 4.3.7 *A homomorphism $\varphi : N \to M$ is surjective, if the sequence*

$$N \xrightarrow{\varphi} M \to 0$$

is exact, and it is injective, if

$$0 \to N \xrightarrow{\varphi} M$$

is exact.

Remark 4.3.8 *Hence, a module M is finitely generated if there is an exact sequence*

$$R^n \xrightarrow{\pi} M \to 0.$$

With the inclusion ι of the kernel, we obtain an exact sequence

$$0 \to \ker(\varphi) \xrightarrow{\iota} R^n \xrightarrow{\pi} M \to 0$$

So a module M is finitely presented if there is an exact sequence

$$R^m \xrightarrow{A} R^n \xrightarrow{\pi} M \to 0$$

with $A \in R^{n\times m}$. This matrix A is called ***presentation matrix*** *of M, and describes M completely, since by the homomorphism theorem*

$$\begin{array}{ccccccc} R^n/\operatorname{im}(A) & = & R^n/\ker(\pi) & \cong & \operatorname{im}(\pi) & = & M \\ & & \overline{e_i} & \mapsto & \pi(e_i) & & \end{array}$$

That is, the image of A contains all relations between the generators $\pi(e_i)$ of M (where e_i denotes the standard basis of R^n). Or to put it in a different way, up to isomorphism we obtain M from the free module R^n by imposing the calculation rules

$$r_1 e_1 + \ldots + r_n e_n = 0$$

for all

$$\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \in \operatorname{im}(A).$$

Every finitely generated module over a Noetherian ring can be represented in this way: In the same way as for ideals we can show the following equivalence (Exercise 4.4):

Definition and Theorem 4.3.9 *Let R be a commutative ring with 1. An R-module M is called* ***Noetherian****, if it satisfies the following equivalent conditions:*

1) *Every ascending chain of submodules terminates.*

2) *Every submodule of M is finitely generated.*

3) *Every set of submodules has a maximal element.*

Using the chain condition it is any easy exercise to show the following (Exercise 4.5):

Lemma 4.3.10 *Let*

$$0 \to U \xrightarrow{\iota} F \xrightarrow{\pi} M \to 0$$

be an exact sequence of R-modules. Then F is Noetherian if and only if U and M are Noetherian.

Lemma 4.3.11 *Let R be a Noetherian ring. Then R^n is a Noetherian module.*

Proof. First note, that R is a Noetherian R-module by Example 4.3.2.(3). Since

$$\begin{array}{ccccccccc} 0 & \to & R & \to & R^n & \to & R^{n-1} & \to & 0 \\ & & a_1 & \mapsto & \begin{pmatrix} a_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} & \mapsto & \begin{pmatrix} a_2 \\ \vdots \\ a_n \end{pmatrix} & & \end{array}$$

is exact, the claim follows by induction and Lemma 4.3.10. ■

Since for any finitely generated R-module M we have an exact sequence

$$0 \to U \to R^n \to M \to 0$$

with a submodule $U \subset R^n$, it follows by Lemma 4.3.10:

Theorem 4.3.12 *Finitely generated modules over Noetherian rings are finitely presented.*

This also proves: Finitely generated modules over Noetherian rings are Noetherian.

In particular, we can apply Theorem 4.3.12 to describe $\mathbb{Z}$-modules (that is, finitely generated abelian group) and finitely generated $K[x]$-modules by a presentation matrix.

Example 4.3.13 *We consider the abelian group G with the presentation as $\mathbb{Z}$-module*

$$0 \to \mathbb{Z}^3 \xrightarrow{A} \mathbb{Z}^4 \xrightarrow{\pi} G \to 0$$

given by the matrix

$$A = \begin{pmatrix} 1 & 1 & 1 \\ -3 & 1 & 1 \\ 1 & -3 & 1 \\ 1 & 1 & -3 \end{pmatrix}$$

First compute the Smith normal form $D = S \cdot A \cdot T$ of A with

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 \\ 2 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \qquad T = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$$

(see Exercise 4.2.8). So we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \to & \mathbb{Z}^3 & \overset{A}{\to} & \mathbb{Z}^4 & \overset{\pi}{\to} & G & \to & 0 \\ & & \uparrow T & & \downarrow S & & \cong & & \\ 0 & \to & \mathbb{Z}^3 & \overset{D}{\to} & \mathbb{Z}^4 & \to & \operatorname{coker}(D) & \to & 0 \end{array}$$

Hence, the columns $c_i = S^{-1}(e_i)$ of

$$S^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 \\ 1 & -1 & 1 & 0 \\ 1 & 0 & -1 & 1 \end{pmatrix}$$

represent generators $\overline{c_1}, \overline{c_2}, \overline{c_3}, \overline{c_4}$ of $\operatorname{coker}(A) = \mathbb{Z}^4/\operatorname{im}(A)$ with the relations

$$1 \cdot \overline{c_1} = 0 \qquad 4 \cdot \overline{c_2} = 0 \qquad 4 \cdot \overline{c_3} = 0$$

In particular, the generator $\overline{c_1}$ can be omitted. We can see this directly:

$$\begin{pmatrix} 1 \\ -3 \\ 1 \\ 1 \end{pmatrix} = A \cdot e_1 \in \operatorname{im}(A)$$

In the same way, since $G \cong \operatorname{coker}(A)$, the elements

$$v_i = \pi(S^{-1}(e_i)) \in G$$

are generators of G with the relations

$$4 \cdot v_2 = 0 \qquad 4 \cdot v_3 = 0$$

Hence we can write G as a product of cyclic groups

$$G \cong \operatorname{coker}(D) \cong \mathbb{Z}/4 \times \mathbb{Z}/4 \times \mathbb{Z}$$

where the factors correspond to the generators

$$v_2 = \pi \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} \qquad v_3 = \pi \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix} \qquad v_4 = \pi \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \in G$$

In the next section we give the general result:

4.4 Finitely generated modules over principal ideal domains

Using the elementary divisor theorem we can describe finitely generated modules over principal ideal domains.

Let R be a principal ideal domain and M a finitely generated R-module. By Theorem 4.3.12, M is finitely presented

$$R^m \overset{A}{\to} R^n \overset{\pi}{\to} M \to 0$$

and $A \in R^{n\times m}$. The elementary divisor theorem 4.2.2 yields $S \in \mathrm{GL}(n,R)$ and $T \in \mathrm{GL}(m,R)$ with

$$\begin{array}{ccccccc} R^m & \overset{A}{\to} & R^n & \overset{\pi}{\to} & M & \to & 0 \\ \uparrow T & & \downarrow S & & \cong & & \\ R^m & \overset{D}{\to} & R^n & \to & M' & \to & 0 \end{array}$$

and

$$D = \left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & 0 \\ & & d_r & \\ \hline & 0 & & 0 \end{array}\right)$$

With the standard basis vectors e_i of R^n

$$v_i = \pi\left(S^{-1}(e_i)\right)$$

are generators of M with the relations

$$d_1 v_1 = 0 \quad \dots \quad d_r v_r = 0$$

If d_i is a unit, then $d_i v_i = 0$ implies $v_i = 0$, hence we can delete the generator v_i (and with it the i-th row of D). The last $m-r$ columns can be deleted, as this does not change $\mathrm{im}(A) = \ker(\pi)$.

To formulate this as a theorem we use the following notation:

Definition 4.4.1 *An R-module M is the* ***direct sum***

$$M = U_1 \oplus \ldots \oplus U_n$$

of submodules $U_1, \ldots, U_n \subset M$, if M is generated by the elements of the U_i and for all $u_i \in U_i$ it holds

$$u_1 + \ldots + u_n = 0 \quad \Longrightarrow \quad u_1 = \ldots = u_n = 0$$

Definition 4.4.2 *A module is called* ***cyclic****, if it is generated by a single element.*

Theorem 4.4.3 *Let R be a principal ideal domain and M a finitely generated R-module. Then it holds:*

1) *There are generators $v_1, ..., v_n$ of M and $d_1, ..., d_r \in R$, $r \leq n$ with $d_i \notin R^\times$ and $d_i \mid d_{i+1}$ for $i = 1, ..., r-1$, such that M is described by the relations*

$$d_1 v_1 = 0 \quad \dots \quad d_r v_r = 0$$

2) *M is the direct sum*

$$M = U_1 \oplus ... \oplus U_n$$

of cyclic submodules and

$$U_i \cong \begin{cases} R/\langle d_i \rangle & \text{for } i \leq r \\ R & \text{for } i > r \end{cases}$$

3) *that is,*

$$M \cong R/\langle d_1 \rangle \times \dots \times R/\langle d_r \rangle \times R^{n-r}$$

*The **rank** $n - r$ of M is uniquely determined by M, also the **elementary divisors** d_i of M (up to units).*

Corollar 4.4.4 *Let R be a principal ideal domain and M a finitely generated R-module. Let*

$$T = \{m \in M \mid \exists r \in R \text{ with } r \cdot m = 0\} \subset M$$

*be the **torsion submodule** of M. There is a free submodule $F \subset M$ with*

$$M = T \oplus F.$$

The torsion submodule T is canonical as a submodule, the free part F, on the other hand, is not (rather the quotient $M/T \cong F$ is canonical).

Definition 4.4.5 *The module M is called **torsion-free**, if $T = \{0\}$, and M is called a **torsion module**, if $M = T$.*

Remark 4.4.6 *Corollary 4.4.4 shows: A finitely generated module over a principal ideal domain is free if and only if it is torsion-free.*

From this it follows:

Remark 4.4.7 *Let R be a principal ideal domain. Then every submodule of a free R-module is again free.*

Example 4.4.8 *The ideal $M = \langle x, y\rangle \subset R = K[x, y]$ is not principal. As an R-submodule of R the module M is torsion-free, however not free (see Exercise 4.6).*

Example 4.4.9 *In Example 4.3.13*

$$G = \underbrace{\langle v_2\rangle \oplus \langle v_3\rangle}_{T} \oplus \underbrace{\langle v_4\rangle}_{F}$$

with the (unique) torsion submodule

$$T = \langle v_2, v_3\rangle \cong \mathbb{Z}/4 \times \mathbb{Z}/4$$

and the (non-unique) free part

$$F = \langle v_4\rangle \cong \mathbb{Z}.$$

In Section 4.6 and in Exercise 4.8 we will also see examples over $K[x]$.

The decomposition in Theorem 4.4.3 can be refined: If $d \in R$ and $d = p_1^{e_1}, ..., p_k^{e_k}$ is a prime factorization (with all $e_i > 0$), then by the Chinese remainder theorem

$$R/(d) \cong R/\langle p_1^{e_1}\rangle \times ... \times R/\left\langle p_k^{e_k}\right\rangle$$

as the ideals $\langle p_i^{e_i}\rangle$ are pairwise coprime. Hence it holds:

Theorem 4.4.10 *Let R be a principal ideal domain and M a finitely generated R-module. Then there is a $t \in \mathbb{N}_0$ and prime elements $p_1, ..., p_s \in R$ and $e_1, ..., e_s \in \mathbb{N}$ with*

$$M \cong R/\langle p_1^{e_1}\rangle \times \ldots \times R/\langle p_s^{e_s}\rangle \times R^t$$

and this product is unique up to reordering of the factors.

4.5 Fundamental theorem of finitely generated abelian groups

As a special case we consider finitely generated $\mathbb{Z}$-modules, that is, finitely generated abelian groups. We summarize for this case the results of the preceding section:

Theorem 4.5.1 *Let G be a finitely generated abelian group. Then it holds:*

1) *G is the direct sum of cyclic subgroups.*

2) *There is $0 \leq r \leq n$ and $d_1, ..., d_r \geq 2$ with $d_i \mid d_{i+1}$ for $i = 1, ..., r-1$, such that*
$$G \cong \mathbb{Z}/(d_1) \times \ldots \times \mathbb{Z}/(d_r) \times \mathbb{Z}^{n-r}$$

3) *There are prime numbers $p_1, ..., p_s$ (not necessarily pairwise different) and $e_1, ..., e_s \in \mathbb{N}$ with*
$$G \cong \mathbb{Z}/(p_1^{e_1}) \times \ldots \times \mathbb{Z}/(p_s^{e_s}) \times \mathbb{Z}^{n-r}$$

Here r and n and the d_i (up to permutation) are uniquely determined by G. The same is true for the $p_i^{e_i}$.

Example 4.5.2 *Let G be given by the presentation matrix*
$$A = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 18 \end{pmatrix} \in \mathbb{Z}^{5\times 5}$$
By the elementary divisor algorithm we obtain the Smith normal form D of A
$$A \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 18 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 12 & 0 \\ 0 & 0 & 0 & 18 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 36 \end{pmatrix} = D$$
Hence, the elementary divisor representation in Theorem 4.5.1 is
$$G \cong \mathbb{Z}/2 \times \mathbb{Z}/6 \times \mathbb{Z}/36$$
and the prime power representation (by $6 = 2 \cdot 3$ and $36 = 2^2 \cdot 3^2$) is
$$G \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/2^2 \times \mathbb{Z}/3^2.$$
From this we can recover the elementary divisor representation
$$\begin{array}{rcccccc} G & \cong & \mathbb{Z}/2 & \times & \mathbb{Z}/2 & \times & \mathbb{Z}/2^2 \\ & & & \times & \mathbb{Z}/3 & \times & \mathbb{Z}/3^2 \\ & \cong & \mathbb{Z}/2 & \times & \mathbb{Z}/6 & \times & \mathbb{Z}/36 \end{array}$$
since by the condition $d_i \mid d_{i+1}$ it holds: If we write the elementary divisors
$$d_i = p_1^{e_{i,1}} \cdot \ldots \cdot p_t^{e_{i,t}}$$
with prime numbers $p_1, ..., p_t$ and $e_{i,j} \geq 0$, then $e_{i,j} \leq e_{i+1,j}$. Moreover we can use any prime power only once. See also Exercise 4.7.

4.6 The Jordan normal form

In linear algebra over a field K the Jordan normal form of an endomorphism $A = (a_{i,j}) \in K^{n\times n}$ is one of the key constructions.

Considering the $K[x]$-module structure on K^n associated to A, we can determine the Jordan normal form of A by applying the elementary divisor algorithm to the presentation matrix of K^n as a $K[x]$-module.

Remark 4.6.1 *In Example 4.3.2.(8) we have seen, that K^n becomes a $K[x]$-module with the scalar multiplication*

$$\begin{aligned} K[x] \times K^n &\longrightarrow K^n \\ (f, v) &\longmapsto f(A) \cdot v \end{aligned}$$

induced by substituting x by A. From the $K[x]$-module structure we can recover the K-linear map

$$\begin{array}{ccc} K^n & \to & K^n \\ v & \mapsto & x \cdot v \end{array}$$

Hence, a $K[x]$-module structure on K^n is the same as an endomorphism $A \in K^{n\times n}$.

Remark 4.6.2 *A subvector space $U \subset K^n$ is a $K[x]$-submodule if and only if $A(U) \subset U$.*

Proof. Let $u \in U$. Then $f \cdot u \in U \ \forall f \in K[x]$ if and only if $x \cdot u \in U$, if and only if $A \cdot u \in U$. ■

Remark 4.6.3 *The standard basis vectors $e_1, ..., e_n$ of K^n are generators of K^n as a $K[x]$-module, that is, there is an exact sequence*

$$K[x]^n \xrightarrow{\pi} K^n \longrightarrow 0$$

Among the e_i we have the obvious relations

$$x \cdot e_j = A \cdot e_j = \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{n,j} \end{pmatrix} = \sum_{i=1}^{n} a_{i,j} \cdot e_i \in K^n$$

By these relations, any element $\sum_{i=1}^{n} f_i \cdot e_i \in K[x]^n$ with $f_i \in K[x]$ can be reduced to a vector of constants (that is, to an element of K^n). So these relations generate $\ker(\pi)$ as a $K[x]$-module.

Hence K^n as a $K[x]$-module has the presentation

$$K[x]^n \xrightarrow{xE-A} K[x]^n \longrightarrow K^n \longrightarrow 0$$

with the presentation matrix

$$xE - A = \begin{pmatrix} x - a_{1,1} & -a_{1,n} & \cdots & -a_{1,n} \\ -a_{2,1} & x - a_{2,2} & & \vdots \\ \vdots & & \ddots & \vdots \\ -a_{n,1} & \cdots & \cdots & x - a_{n,n} \end{pmatrix}$$

In linear algebra this matrix is also called the ***characteristic matrix*** *of A.*

Remark 4.6.4 *The kernel of the substitution homomorphism*

$$\begin{array}{rccc} \varphi_A : & K[x] & \to & K^{n\times n} \\ & x & \mapsto & A \end{array}$$

is a principal ideal in $K[x]$. The ***minimal polynomial*** *p_A of A is defined in linear algebra as the monic generator of the kernel*

$$\ker(\varphi_A) = \langle p_A \rangle .$$

So for every $v \in K^n$ the scalar multiplication $p_A \cdot v = 0$ is zero, that is, K^n is a (finitely generated) torsion module.

According to the theorem of Cayley-Hamilton the ***characteristic polynomial***

$$\chi_A = \det(xE - A) \in \ker(\varphi_A)$$

is in the kernel, so $p_A \mid \chi_A$.

Lemma 4.6.5 *Assume that the characteristic polynomial χ_A factors into linear factors. Then K^n as a $K[x]$-module is the direct sum*

$$K^n = U_1 \oplus \ldots \oplus U_s$$

of cyclic submodules

$$U_i \cong K[x]/\langle (x - \lambda_i)^{e_i} \rangle$$

and

$$\prod_{i=1}^{s} (x - \lambda_i)^{e_i} = \chi_A$$

Proof. Applying the elementary divisor algorithm to $xE - A$ we obtain $S, T \in \mathrm{SL}(n, K[x])$ with

$$S \cdot (xE - A) \cdot T = D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$$

and $d_i \neq 0$ (note, that K^n is a torsion module). Decomposing further by the Chinese remainder theorem (that is, applying Theorem 4.4.10) yields a decomposition

$$K^n = U_1 \oplus \ldots \oplus U_s$$

into a direct sum of submodules U_i and isomorphisms

$$\alpha_i : U_i \xrightarrow{\cong} K[x]/\langle p_i^{e_i} \rangle$$

with irreducible polynomials $p_i \in K[x]$. Then it holds

$$\prod_{i=1}^{s} p_i^{e_i} = d_1 \cdot \ldots \cdot d_n = \det(D) = \det(xE - A) = \chi_A.$$

Since χ_A decomposes into linear factors, the p_i are of the form $p_i = x - \lambda_i$ with $\lambda_i \in K$. ■

We now describe a K-vector space basis of U_i, in which $A|_{U_i}$ becomes a Jordan block: As a K-vector space

$$K[x]/\langle (x - \lambda_i)^{e_i} \rangle$$

has the basis

$$\overline{1},\ \overline{x - \lambda_i},\ \overline{(x - \lambda_i)^2},\ \ldots,\ \overline{(x - \lambda_i)^{e_i - 1}}$$

The preimages

$$v_{i,j} = \alpha_i^{-1}\left(\overline{(x - \lambda_i)^j}\right)$$

under the isomorphism $\alpha_i : U_i \longrightarrow K[x]/\langle p_i^{e_i} \rangle$ give a basis $\mathcal{B}_i = (v_{i,j})_{j=0,\ldots,e_i-1}$ of U_i.

Then it holds

$$(A - \lambda_i E) \cdot v_{i,j} = (x - \lambda_i) \cdot \alpha_i^{-1}\left(\overline{(x - \lambda_i)^j}\right) = \alpha_i^{-1}\left(\overline{(x - \lambda_i)^{j+1}}\right) = v_{i,j+1}$$

for $j = 0, \ldots, e_i - 2$ and

$$(A - \lambda_i E) \cdot v_{i,e_i-1} = (x - \lambda_i) \cdot v_{i,e_i-1} = 0.$$

Hence, with respect to the basis $\mathcal{B}_i$ the matrix A has as representing matrix an $e_i \times e_i$-**Jordan block** with eigenvalue λ_i

$$M_{\mathcal{B}_i}^{\mathcal{B}_i}\left(A\,|_{U_i}\right) = J\left(\lambda_i, e_i\right) := \begin{pmatrix} \lambda_i & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda_i \end{pmatrix} \in K^{e_i \times e_i}$$

This proves:

Theorem 4.6.6 (Jordan normal form) *Let $A \in K^{n\times n}$, and suppose $\chi_A(t)$ factors over K into linear factors (which is true, for example, if $K = \mathbb{C}$). Then there is an $S \in \mathrm{GL}(n, K)$, such that*

$$SAS^{-1} = J = \begin{pmatrix} \boxed{J\left(\lambda_1, e_1\right)} & & & 0 \\ & \boxed{J\left(\lambda_2, e_2\right)} & & \\ & & \ddots & \\ 0 & & & \boxed{J\left(\lambda_s, e_s\right)} \end{pmatrix}$$

has block diagonal form with Jordan blocks $J\left(\lambda_i, r_i\right)$ with (not necessarily pairwise different) eigenvalues $\lambda_1, \ldots, \lambda_s$ on the diagonal. Up to permutation of the blocks, J is uniquely determined by A.

Remark 4.6.7 *The prime power factors of the last elementary divisor d_n correspond to the maximal Jordan blocks, those of the second last to blocks of size one less, and so on. In particular, $d_n = p_A$ is the minimal polynomial of A.*

Example 4.6.8 *We try out the algorithm for*

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

(which, for simplicity is already in Jordan normal form). First we compute the Smith normal form of $xE - A$:

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

$$\mapsto \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & x^3 & 0 & 0 \\ 0 & 0 & 0 & x & 0 \\ 0 & 0 & 0 & 0 & x-1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & x & 0 \\ 0 & 0 & 0 & 0 & x^3(x-1) \end{pmatrix} = D$$

From the elementary divisors we can read off, that the Jordan normal form of A has one Jordan block of the size

$$\begin{array}{l} 1\times 1 \text{ with eigenvalue } 0 \\ 3\times 3 \text{ with eigenvalue } 0 \\ 1\times 1 \text{ with eigenvalue } 1 \end{array}$$

Example 4.6.9 *Suppose A would have two 1×1 blocks and one 3×3 block, all with eigenvalue 0, then the Smith normal form of $xE - A$ would be*

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & x & 0 & 0 \\ 0 & 0 & 0 & x & 0 \\ 0 & 0 & 0 & 0 & x^3 \end{pmatrix}$$

For another example see Exercise 4.8.

4.7 Exercises

Exercise 4.1 *1) Compute the Smith normal form of*

$$A = \begin{pmatrix} 4 & 6 & 2 \\ 2 & 3 & 2 \\ 2 & 3 & 0 \end{pmatrix} \in \mathbb{Z}^{3\times 3}$$

and $S, T \in \mathrm{GL}(3,\mathbb{Z})$ with

$$S\cdot A\cdot T = D$$

2) Determine a basis of $\mathrm{im}(A)$ and describe $\mathbb{Z}^3/\mathrm{im}(A)$.

Exercise 4.2 *Let*

$$g_1 = \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix},\ g_2 = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix},\ g_3 = \begin{pmatrix} -3 \\ -3 \\ -3 \end{pmatrix},\ g_4 = \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix} \in \mathbb{Z}^3$$

Determine a basis of the subgroup of $\mathbb{Z}^3$ generated by $g_1, \ldots, g_4$.

Exercise 4.3 *Let G be a finite abelian group, and*

$$\mathbb{Z}^n \xrightarrow{A} \mathbb{Z}^n \to G \to 0$$

a presentation of G by $A = (a_{i,j}) \in \mathbb{Z}^{n\times n}$. Prove that for the order of the group G it holds

$$|G| = |\det A|\,.$$

Exercise 4.4 *An R-module M is called Noetherian if it satisfies the following equivalent conditions:*

1) *Every ascending chain of submodules terminates.*
2) *Every submodule of M is finitely generated.*
3) *Every non-empty set of submodules contains a maximal element.*

Prove the equivalence.

Exercise 4.5 *Let*

$$0 \to U \xrightarrow{a} F \xrightarrow{\pi} M \to 0$$

be an exact sequence of R-modules. Prove that M is Noetherian if and only if U and M are Noetherian.

Exercise 4.6 *Let K be a field and $R = K[x, y]$. Show that $M = \langle x, y \rangle \subset R$ as an R-module is torsion-free, but not free.*

Exercise 4.7 *Find the elementary divisors d_i of*

$$G = \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3^2 \times \mathbb{Z}/3^2 \times \mathbb{Z}/3^5 \times \mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/7$$

that is, a representation $G \cong \mathbb{Z}/d_1 \times \ldots \times \mathbb{Z}/d_r$ with $d_i \geq 2$ and $d_i \mid d_{i+1}$ for $i = 1, \ldots, r-1$.

Exercise 4.8 *Let*

$$B = \begin{pmatrix} 2 & 0 & -1 \\ -1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} \in \operatorname{End}\left(\mathbb{C}^3\right)$$

1) *Compute the Smith normal form D of*

$$A = xE - B \in \mathbb{C}[x]^{3\times 3}$$

and $S, T \in \mathrm{GL}\left(3, \mathbb{C}[x]\right)$ with $D = S \cdot A \cdot T$.

2) *Determine from this the Jordan normal form of B.*

5

Free resolutions and invariants

5.1 Overview

If M is a finitely generated module over a principal ideal domain R, then by Theorem 4.4.3 there is an exact presentation sequence

$$0 \to R^r \xrightarrow{D} R^s \xrightarrow{\pi} M \to 0$$

where

$$D = \left(\begin{array}{ccc} d_1 & & \\ & \ddots & \\ & & d_r \\ \hline & 0 & \end{array} \right)$$

Note that exactness at the module R^r is achieved by deleting any zero column in the Smith normal form. In this way, one can describe the structure of M completely.

In which way can we generalize this to the setup of modules M over say $R = K[x_1, ..., x_n]$? What we have in mind, is to obtain invariants encoding information about the algebraic variety $X = V(f_1, ..., f_r) \subset \mathbb{A}^n_K$ given by $f_i \in R$ from

$$M = \operatorname{coker}(f_1, ..., f_r) = R^1 / \operatorname{im}(f_1, ..., f_r)$$

which is, as an R-module, isomorphic to the coordinate ring $K[X] = R/I$ of X.

In particular, we are interested in the dimension of X, the degree of X and the genus of X. We already have some idea, what the dimension of an algebraic variety should be, for example, the dimension of a hypersurface should be $n-1$. The degree of a hypersurface should be the degree of the equation, and if X is finite, the

degree should be the number of solutions counted with multiplicity. The genus of X you perhaps know from topology. Nevertheless, we will have to make the definitions precise and see how to compute these invariants. The canonical setting to do this, are ideals generated by homogeneous polynomials. So we will also give a short primer on the corresponding projective varieties in Section 5.3.

5.2 Free resolutions

With the notation as in the introduction, the R-module

$$M = \operatorname{coker}(A) \cong R/I$$

with

$$A = (f_1, \ldots, f_r) \in R^{1\times r}$$

has the presentation

$$R^r \xrightarrow{A} R^1 \to M \to 0.$$

If X is not a hypersurface, then A will have a non-trivial kernel.

Example 5.2.1 *For $I = \langle x, y\rangle \subset R = K[x, y]$, we have*

$$A = (x, y)$$

and $\ker(A) = \operatorname{im}(B)$ *with*

$$B = \begin{pmatrix} y \\ -x \end{pmatrix}$$

Obviously, $\ker(B) = 0$*, hence, we have an exact sequence*

$$0 \to R^1 \xrightarrow{B} R^2 \xrightarrow{A} R^1 \to R/I \to 0$$

In Theorem 5.10.7 we will formulate a general algorithm, which, given A, will determine a matrix B with

$$\ker(A) = \operatorname{im}(B)$$

using a straightforward generalization of Buchberger's algorithm from ideals to modules. Recall, that we encountered the module of relations (syzygies) between the generators f_i in the proof of Buchberger's criterion. In addition to the computation of B, a rigorous theory of Gröbner bases of modules will allow us to give a much nicer proof of Buchberger's criterion.

If we iterate this process of writing $\ker(A) = \operatorname{im}(B)$, we obtain what is called a free resolution:

Definition 5.2.2 *Let M be an R-module. An* ***exact sequence***

$$\ldots \to F_i \xrightarrow{\phi_i} F_{i-1} \xrightarrow{\phi_{i-1}} \ldots \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} F_0 \xrightarrow{\phi_0} M \to 0$$

with free modules F_i is called a ***free resolution*** *of M. It is called* ***finite*** *if $F_i = 0$ for $i > l$ for some integer l, which is called the length of the resolution.*

The ***i-th syzygy module*** *of M is $\mathrm{im}(\phi_i) = \ker(\phi_{i-1})$.*

A priori it is not clear that the length is finite. This is not even true if R is Noetherian and M is finitely generated (and hence finitely presented):

Example 5.2.3 *Let $R = K[x,y]/\langle xy\rangle$. The R-module $\langle \overline{x}\rangle$ is finitely generated, however, it has the infinite free resolution*

$$\ldots \to R^1 \xrightarrow{\overline{y}} R^1 \xrightarrow{\overline{x}} R^1 \xrightarrow{\overline{y}} R^1 \xrightarrow{\overline{x}} \langle \overline{x}\rangle \to 0$$

However, for modules over the polynomial ring, we will prove the following key theorem by Hilbert:

Theorem 5.2.4 (Syzygy theorem) *Let $R = K[x_1, \ldots, x_n]$. Every finitely generated R-module has a finite free resolution. All modules in the resolution are finitely generated, and the length is at most n.*

Example 5.2.5 *We compute the finite free resolution in Example 5.2.1 using* Singular*:*

```
ring R=0,(x,y),lp;
ideal I=x,y;
def L=res(I,0);
   1          2          3
 R     <--  R     <--  R
 0          1          2
matrix(L[1]);
_[1,1] = y
_[1,2] = x
 matrix(L[2]);
_[1,1] = -x
_[2,1] = y
```

If the second argument of `res` *is positive, then* Singular *will stop after computing the given number of steps of the resolution.*
Increasing the number of generators we get similar complexes:

```
ring R=0,(x(1..4)),lp;
```

```
ideal I=x(1..4);
def L=res(I,0);
   1          4          6          4          1
R     <--  R     <--  R     <--  R     <--  R
0          1          2          3          4
```

In general this kind of resolution is called ***Koszul complex****. For n independent variables,*

$$\operatorname{rank}(F_i) = \binom{n}{i}.$$

We will come back to this in Exercise 5.10.

5.3 Projective algebraic sets and graded ideals

Many results in algebraic geometry improve, if we replace the affine space $\mathbb{A}^n_K$ by projective space $\mathbb{P}^n_K$. For example any line in $\mathbb{A}^2_K$ gets added its point at infinity, which leads to the desirable fact that any two distinct lines intersect in a point: Two parallel lines intersect at their common point at infinity. More generally, Bezout's theorem shows: If $K = \overline{K}$, two curves in $\mathbb{P}^2_K$ of degree d_1 and d_2 intersect precisely in $d_1 \cdot d_2$ points counted with multiplicity. Our main motivation to pass to projective varieties is to give algorithms for computing the above mentioned invariants like dimension, degree and genus.

In this section we will discuss the basics of graded rings, homogeneous ideals and the associated projective algebraic sets. We investigate how to associate to a projective algebraic set and affine algebraic set, and vice versa.

Definition 5.3.1 *The n-dimensional* ***projective space*** *over K is*

$$\mathbb{P}^n(K) = \left\{1\text{-}\textit{dimensional vector subspaces of } K^{n+1}\right\}$$

If $\langle (p_0, .., p_n) \rangle \in \mathbb{P}^n(K)$, so in particular $(p_0, .., p_n) \neq 0$, then we write

$$(p_0 : \ldots : p_n) := \langle (p_0, .., p_n) \rangle .$$

The quotient symbol : indicates that the generator of the 1-dimension vector space is only unique up to multiplication with a non-zero constant:

$$(p_0 : \ldots : p_n) = (q_0 : \ldots : q_n) \Longleftrightarrow \exists \lambda \neq 0 : \lambda \cdot (p_0, \ldots, p_n) = (q_0, \ldots, q_n)$$

With the group action

$$K^\times \times K^{n+1} \to K^{n+1},\ (\lambda, (p_0, ..., p_n)) \mapsto \lambda \cdot (p_0, ..., p_n)$$

we have

$$\mathbb{P}^n(K) = \left(K^{n+1} - \{0\}\right)/K^\times.$$

This quotient construction has a generalization in the setting of toric geometry and geometric invariant theory.

For example, we can think of $\mathbb{P}^2(\mathbb{R})$ as a half sphere with opposite boundary points identified (since they generate the 1-dimension vector space), see Figure 5.1.

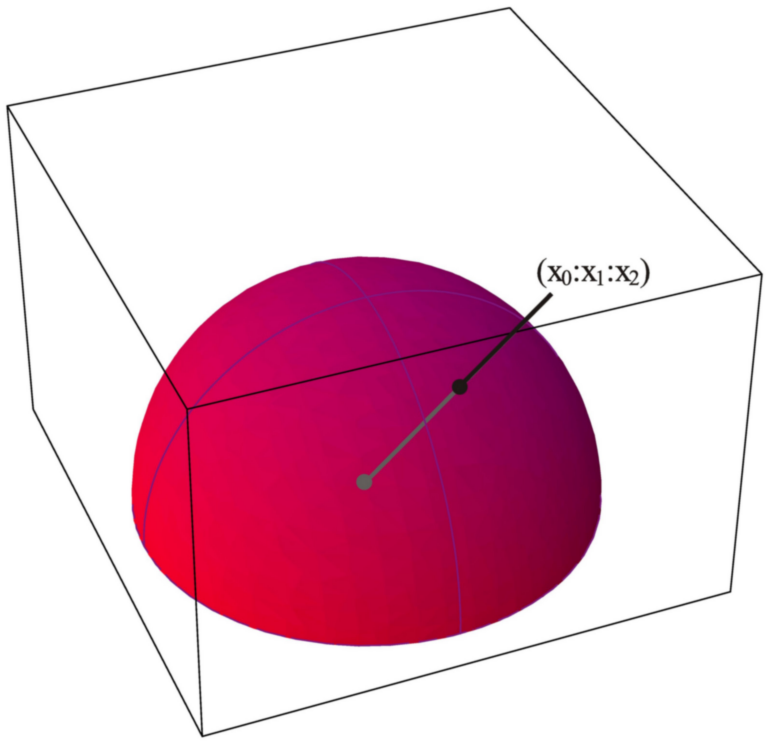

Figure 5.1: Projective space $\mathbb{P}^2(\mathbb{R})$.

To specify algebraic subsets of $\mathbb{P}^n(K)$ we have to consider homogeneous polynomials:

Definition 5.3.2 *A **graded ring** is a ring R together with a fixed decomposition*

$$R = \bigoplus_{\alpha \in G} R_\alpha$$

as a direct sum of abelian groups, where G is a monoid (that is semigroup with unit), such that

$$R_\alpha R_\beta \subset R_{\alpha+\beta}.$$

If $f \in R_\alpha$ then f is called ***homogeneous*** *of degree α.*

If $f \in R$ then $f = \sum_{\alpha \in G,\ finite} f_\alpha$ with the uniquely determined ***homogeneous components*** *$f_\alpha \in R_\alpha$.*

An ideal $I \subset R$ is called homogeneous, if it is generated by homogeneous elements.

Definition 5.3.3 *The* ***standard grading*** *on $K[x_0, ..., x_n]$ by $\mathbb{N}_0$ is given by setting $\deg x_i = 1 \forall i$. Then*

$$K[x_0, ..., x_n] = \bigoplus_{d=0}^{\infty} K[x_0, ..., x_n]_d$$

where

$$K[x_0, ..., x_n]_d = \left\{ \sum_{|\alpha|=d} c_\alpha x^\alpha \in K[x_0, ..., x_n] \right\}$$

Example 5.3.4 *In the standard grading on $K[x, y]$ the polynomials $3x^2y$ and $3x^2y + 5xy^2$ are homogeneous, whereas $3x^2y + 5x$ is not.*

However if you consider the grading of $K[x, y]$ by $\mathbb{N}_0^2$ with $\deg x = e_1$ and $\deg y = e_2$, then the degree of a monomial is its exponent vector. Hence $3x^2y$ is homogeneous of degree $(2, 1)$, however $3x^2y + 5xy^2$ and $3x^2y + 5x$ are not. The homogeneous polynomials are precisely the constant multiples of monomials.

If not mentioned otherwise, in what follows, we will always consider the standard grading on $R = K[x_0, ..., x_n]$.

If $f \in R$ is homogeneous of degree d, then

$$f(\lambda \cdot (p_0, ..., p_n)) = \lambda^d \cdot f(p_0, ..., p_n)$$

hence the condition $f(p_0 : ... : p_n) = 0$ for $(p_0 : ... : p_n) \in \mathbb{P}^n(K)$ is well-defined.

Definition 5.3.5 *If $I \subset R$ is homogeneous, then the* ***projective algebraic set*** *defined by I is*

$$V(I) = \{p \in \mathbb{P}^n(K) \mid f(p) = 0 \ \forall \ \textit{homogeneous } f \in I\}$$

and if $X \subset \mathbb{P}^n(K)$

$$I(X) = \langle f \in R \textit{ homogeneous} \mid f(p) = 0 \ \forall p \in X \rangle$$

is the ***homogeneous zero ideal*** *of X.*

Remark 5.3.6 *Consider the* ***hyperplane at infinity***

$$H = \{p \in \mathbb{P}^n(K) \mid p_0 = 0\}$$

and the corresponding ***affine chart***

$$U = \{p \in \mathbb{P}^n(K) \mid p_0 \neq 0\}$$

so $\mathbb{P}^n(K) = U \cup H$. *The map*

$$\begin{array}{rccc} \varphi: & \mathbb{A}^n(K) & \to & U \\ & (p_1, \ldots, p_n) & \mapsto & (1 : p_1 : \ldots : p_n) \\ & \left(\frac{p_1}{p_0}, \ldots, \frac{p_n}{p_0}\right) & \leftarrow\!\shortmid & (p_0 : p_1 : \ldots : p_n) \end{array}$$

is a well-defined bijection. Figure 5.2 depicts the identification of $\mathbb{A}^2(\mathbb{R})$ *with* $U \subset \mathbb{P}^2(\mathbb{R})$. *The horizontal lines correspond to the points of* H.

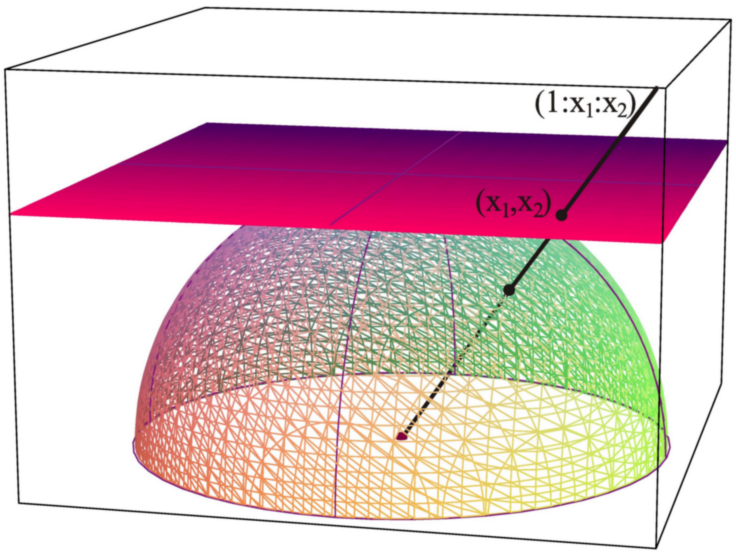

Figure 5.2: Mapping $\mathbb{A}^2(\mathbb{R})$ into $\mathbb{P}^2(\mathbb{R})$ by stereographic projection.

If $F \in K[x_0, \ldots, x_n]$ *is homogeneous, then its* ***dehomogenization*** *is*

$$F^{\mathrm{a}} = F(1, x_1, \ldots, x_n).$$

Given a homogeneous ideal $I \subset K[x_0, \ldots, x_n]$, *the ideal*

$$I^{\mathrm{a}} = \{F^{\mathrm{a}} \mid F \in I\} \subset K[x_1, \ldots, x_n]$$

is called the dehomogenization of I. *In this way we can associate to the projective algebraic set* $X = V(I) \subset \mathbb{P}^n(K)$ *the affine algebraic set*

$$\varphi^{-1}(X \cap U) = V(I^{\mathrm{a}}).$$

Proof. $(1 : x_1 : \ldots : x_n) \in V(I) \Leftrightarrow F(1, x_1, \ldots, x_n) = 0 \ \forall$ homogeneous $F \in I \Leftrightarrow (x_1, \ldots, x_n) \in V(I^{\mathrm{a}})$. ■

Note that, more generally, any choice of a homogeneous linear form l yields an affine chart $U = \{l(p) \neq 0\}$.

Example 5.3.7 *The projective parabola* $X = V(x_1^2 - x_2x_0) \subset \mathbb{P}^2(\mathbb{R})$ *consists of the points* $(1 : x_1 : x_2)$ *corresponding to the point* $(x_1, x_2) \in V(x_1^2 - x_2) \subset \mathbb{A}^2(\mathbb{R})$ *of the affine parabola (Figure 5.3) and one point at infinity* $(0 : 0 : 1)$*, so*

$$\begin{array}{ccc} U = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2(\mathbb{R}) \mid x_0 \neq 0\} & \to & \mathbb{A}^2(\mathbb{R}) \\ \cup & & \cup \\ X = V(x_1^2 - x_2x_0) & \to & V(x_1^2 - x_2) \\ (1 : x_1 : x_2) & \mapsto & (x_1, x_2) \end{array}$$

In Figure 5.3 the projective parabola is depicted by identifying a 1*-dimensional subspaces of* $\mathbb{A}^3(\mathbb{R})$ *with its generator on the upper half sphere. Projecting the upper half sphere into the* (x_1, x_2)*-plane maps the projective parabola into the unit disc, see Figure 5.5.*

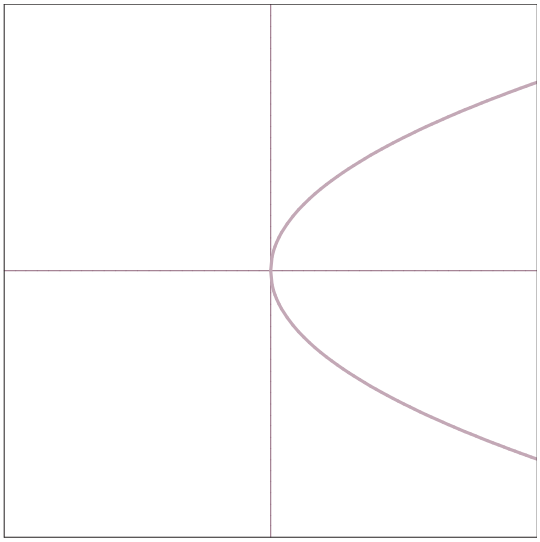

Figure 5.3: Parabola $x - y^2 = 0$ in $\mathbb{A}^2(\mathbb{R})$.

Similar to affine algebraic geometry, the key to the identification of projective algebraic sets with homogeneous ideals is a projective version of the strong Nullstellensatz. To formulate this theorem, we need the following easy but fundamental fact about homogeneous ideals:

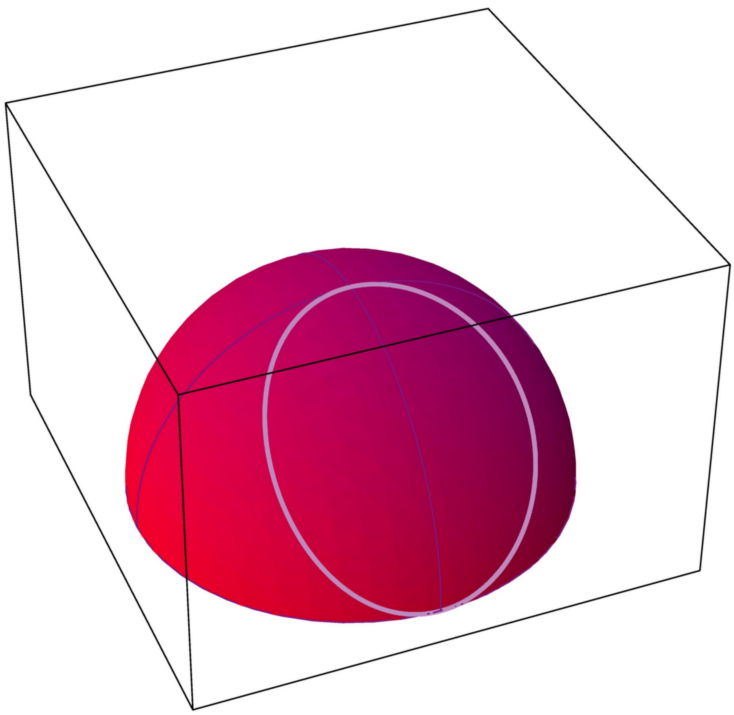

Figure 5.4: Projective parabola

Lemma 5.3.8 *An ideal $I \subset R$ is homogeneous if and only if for every $f \in I$ also the homogeneous summands $f_i \in R_i$ of $f = \sum_i f_i$ are in I.*

Proof. Assume the latter. Then the homogeneous summands of any set of generators are in I, hence I is generated by these summands. On the other hand, assume $I = \langle f_1, ..., f_r \rangle$ with $f_j \in R_{d_j}$ homogeneous, and let $f = \sum_j a_j f_j \in I$. Write $a_j = \sum_i a_{i,j}$ with $a_{i,j} \in R_i$, so

$$f = \sum_j \sum_i a_{i,j} f_j = \sum_d \underbrace{\sum_{i+d_j=d} a_{i,j} f_j}_{g_d}$$

with $g_d \in R_d$. Obviously all $g_d \in I$. Since there is no cancellation between the homogeneous polynomials $g_d \in R_d$, they are the homogeneous summands of f. ■

Note that this generalizes Lemma 2.3.6 if we use the grading by the exponent vector. Using Lemma 5.3.8, it is straightforward to prove (see Exercise 5.1):

Corollar 5.3.9 *The radical of a homogeneous ideal is homogeneous.*

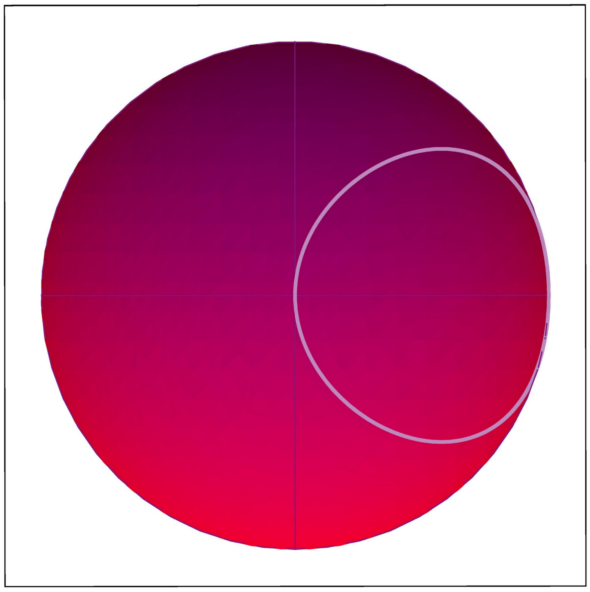

Figure 5.5: Projective parabola as a subset of the unit disc.

Theorem 5.3.10 (Projective strong Nullstellensatz) *Let $K = \overline{K}$ and $I \subset K[x_0, ..., x_n]$ homogeneous with $V(I) \neq \varnothing$. Then*

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

Proof. Let $X = V(I) \subset \mathbb{P}^n(K)$ and consider the affine cone $C(X) = V(I) \subset \mathbb{A}^{n+1}(K)$. Then by the (affine) strong Nullstellensatz 2.1.11 and Exercise 5.2 we have

$$\sqrt{I} = I(C(X)) = I(X).$$

■

From this it follows immediately:

Corollar 5.3.11 *If $K = \overline{K}$ then there is a $1:1$-map*

$$\left\{ \begin{array}{c} \textit{projective algebraic sets} \\ X \subset \mathbb{P}^n(K) \end{array} \right\} \underset{V}{\overset{I}{\rightleftarrows}} \left\{ \begin{array}{c} \textit{homogeneous ideals } J \subset R \\ \textit{with } J = \sqrt{J} \textit{ and } J \neq \langle x_0, ..., x_n \rangle \end{array} \right\}$$

Proof. Note that there are precisely two homogeneous radical ideals I with $V(I) = \varnothing$ namely $I = \langle x_0, ..., x_n \rangle$ and $I = \langle 1 \rangle$. Hence, if we exclude the irrelevant ideal $\langle x_0, ..., x_n \rangle$, by Theorem 5.3.10 we get a $1:1$ map. ■

Finally we show, that to any affine variety we can associate a projective one:

Definition 5.3.12 *Given $f \in K[x_1, ..., x_n]$, the* ***homogenization*** *of f is*

$$f^{\mathrm{h}} = x_0^{\deg f} \cdot f\left(\frac{x_1}{x_0}, ..., \frac{x_n}{x_0}\right) \in K[x_0, ..., x_n]$$

which clearly is a homogeneous polynomial.

If $I \subset K[x_1, ..., x_n]$, then the homogenization of I is defined as

$$I^{\mathrm{h}} = \left\langle f^{\mathrm{h}} \mid f \in I \right\rangle \subset K[x_0, ..., x_n],$$

which, by definition, is a homogeneous ideal.

Example 5.3.13 *For $F = x_0^3 + x_0^2 x_1$ we get $F^{\mathrm{a}} = 1 + x_1$, hence $(F^{\mathrm{a}})^{\mathrm{h}} = x_0 + x_1$. So if we dehomogenize and then homogenize, we remove any common x_0-power of the terms. On the other hand, by definition it is clear that for $f \in K[x_1, ..., x_n]$ it holds $(f^{\mathrm{h}})^{\mathrm{a}} = f$.*

Definition 5.3.14 *Let $X \subset \mathbb{A}^n(K)$ be an affine algebraic set. We define the* ***projective closure*** *of X as*

$$\mathrm{pc}(X) = V(I(X)^{\mathrm{h}}) \subset \mathbb{P}^n(K),$$

the vanishing locus of the homogenization of the zero ideal of X.

Theorem 5.3.15 *The projective closure of an affine algebraic set X is the smallest projective algebraic set containing $\varphi(X)$.*

Proof. We note that $\varphi(X) \subset \mathrm{pc}(X)$: If $f \in I(X)$ then $f^{\mathrm{h}}(1, x_1, ..., x_n) = 0 \ \forall (x_1, ..., x_n) \in X$. Since any (hence any homogeneous) element of $I(X)^{\mathrm{h}}$ is a linear combination of polynomials f^{h} with $f \in I(X)$, the claim follows.

Suppose $\varphi(X) \subset V(F_1, ..., F_r)$ with $F_i \in K[x_0, ..., x_n]$ homogeneous. Then $f_i = F_i(1, x_1, ..., x_n) \in I(X)$, so $f_i^{\mathrm{h}} \in I(X)^{\mathrm{h}}$, hence also $F_i \in I(X)^{\mathrm{h}}$. This shows $\langle F_1, ..., F_r \rangle \subset I(X)^{\mathrm{h}}$, so

$$\mathrm{pc}(X) = V(I(X)^{\mathrm{h}}) \subset V(F_1, ..., F_r).$$

■

Remark 5.3.16 *We define the* ***Zariski topology*** *on $\mathbb{P}^n(K)$ by considering as closed sets the projective algebraic sets. The theorem shows that the projective closure of X is the Zariski closure of $\varphi(X)$, that is,*

$$\mathrm{pc}(X) = \overline{\varphi(X)}.$$

Example 5.3.17 *If we homogenize the defining ideal I of an affine variety $X = V(I)$, then $\mathrm{pc}(X) = V(I^{\mathrm{h}})$, however only if $K = \overline{K}$, see Exercise 5.3. As a counterexample in case $K \neq \overline{K}$, consider $I = \langle x_1^2 + x_2^4 \rangle \in \mathbb{R}[x_1, x_2]$. Then*

$$\{(1:0:0)\} = \mathrm{pc}(V(I)) \subsetneqq V(I^{\mathrm{h}}) = \{(1:0:0), (0:1:0)\}.$$

Algorithm 5.3.18 *Let $I \subset K[x_1, ..., x_n]$ be an ideal. If $G = (g_1, ..., g_r)$ is a Gröbner basis of I with respect to any weighted degree ordering $>$ with weight vector $w = (1, ..., 1)$, then*

$$G^{\mathrm{h}} = (g_1^{\mathrm{h}}, ..., g_r^{\mathrm{h}})$$

is a Gröbner basis of I with respect to the monomial ordering

$$x_0^a x^\alpha >_h x_0^b x^\beta \iff x^\alpha > x^\beta \text{ or } (x^\alpha = x^\beta \text{ and } a > b)$$

Proof. By the choice of $>$, we have for all $f \in K[x_1, ..., x_n]$ that

$$\deg L_>(f) = \deg f,$$

hence

$$L_{>_h}(f^{\mathrm{h}}) = L_>(f).$$

By the Gröbner basis definition, our assumption is

$$L_>(I) = L_>(G)$$

and we have to show

$$L_{>_h}(I^{\mathrm{h}}) = L_{>_h}(G^{\mathrm{h}}).$$

By $L_{>_h}(g_i^{\mathrm{h}}) = L_>(g_i)$ and Lemma 5.3.8, this amounts to proving that if $F \in I^{\mathrm{h}}$ is homogeneous then there is an i with $L_>(g_i) \mid L_{>_h}(F)$. For this write

$$F = \sum_i l_i \cdot f_i^{\mathrm{h}}$$

with $l_i \in K[x_0, ..., x_n]$ and $f_i \in I$. Then

$$F^{\mathrm{a}} = \sum_i l_i^{\mathrm{a}} \cdot f_i \in I$$

so, by assumption, there is an i with

$$L_>(g_i) \mid L_>(F^{\mathrm{a}}).$$

Moreover, for the homogeneous polynomial F there is an $s \geq 0$ with $F = x_0^s \cdot (F^{\mathrm{a}})^{\mathrm{h}}$. Hence, it follows that $L_>(F^{\mathrm{a}}) = L_{>_h}((F^{\mathrm{a}})^{\mathrm{h}})$ divides $L_{>_h}(F)$. ■

Example 5.3.19 *Consider the affine twisted cubic*

$$C = V(I) \subset \mathbb{A}^3(K)$$

defined by

$$I = \left\langle x_1^2 - x_2,\ x_1^3 - x_3 \right\rangle \subset K[x_1, x_2, x_3].$$

Note, that the degree reverse lexicographical ordering refines the grading by the total degree as required in Algorithm 5.3.18. Hence, we can compute the homogenization in SINGULAR *as follows:*

```
ring R = 0,(x(0..3)),dp;
ideal I = x(1)^2-x(2), x(1)^3-x(3);
std(I);
_[1]=x(2)^2-x(1)*x(3)
_[2]=x(1)*x(2)-x(3)
_[3]=x(1)^2-x(2)
```

So

$$I^{\mathrm{h}} = \left\langle x_2^2 - x_1x_3,\ x_1x_2 - x_0x_3,\ x_1^2 - x_2x_0 \right\rangle.$$

Note that homogenizing the given set of generators of I will not yield the correct result:

$$V(x_1^2 - x_2x_0,\ x_1^3 - x_0^2x_3) = \mathrm{pc}(C) \cup V(x_0, x_1),$$

recall Exercise 3.7.

5.4 Graded modules and the Hilbert function

Suppose we are given a projective variety $X \subset \mathbb{P}^n(K)$ and $I(X) = \langle f_1, \ldots, f_r \rangle$ generated by homogeneous polynomials $f_i \in R = K[x_0, \ldots, x_n]$. We will determine the invariants of X mentioned above from a finite free resolution of the R-module

$$M = \operatorname{coker}\begin{pmatrix} f_1 & \ldots & f_r \end{pmatrix} \cong R/I.$$

This module comes with an additional structure, we will have to respect when computing the resolution to obtain well-defined results: M is a graded module. In general, we define:

Definition 5.4.1 *Let $R = \bigoplus_{i \in \mathbb{N}_0} R_i$ be a graded ring. A* ***graded R-module*** *is an R-module M together with a decomposition*

$$M = \bigoplus_{i \in \mathbb{Z}} M_i$$

as abelian groups such that

$$R_i M_j \subset M_{i+j}$$

for all i, j.

Example 5.4.2 *Considering* $I = \langle x_0^3 - x_1^3 - x_2^3 \rangle \subset R = K[x_0, x_1, x_2]$ *choosing lp with* $x_0 > x_1 > x_2$ *we have as a* K*-vector space*

$$R/I =_K \langle \bar{x}^\alpha \mid x^\alpha \notin L(I) \rangle =_K \langle \bar{x}^\alpha \mid 0 \le \alpha_0 \le 2,\ \alpha_1, \alpha_2 \ge 0 \rangle$$

so R/I *is a graded* R*-module with the decomposition into* K*-vector spaces*

$$\begin{aligned} R/I =_K \langle 1 \rangle \oplus_K \langle \bar{x}_0, \bar{x}_1, \bar{x}_2 \rangle \oplus_K \left\langle \bar{x}_0^2, \bar{x}_0\bar{x}_1, \bar{x}_0\bar{x}_2, \bar{x}_1^2, \bar{x}_1\bar{x}_2, \bar{x}_2^2 \right\rangle \\ \oplus_K \left\langle \bar{x}_0^2\bar{x}_1, \bar{x}_0^2\bar{x}_2, \bar{x}_0\bar{x}_1^2, \bar{x}_0\bar{x}_1\bar{x}_2, \bar{x}_0\bar{x}_2^2, \bar{x}_1^3, \bar{x}_1^2\bar{x}_2, \bar{x}_1\bar{x}_2^2, \bar{x}_2^3 \right\rangle \oplus \ldots \end{aligned}$$

In general, if $I \subset R = K[x_0, \ldots, x_n]$ is a homogeneous ideal, and I_j is the K-vector space of homogeneous polynomials of degree j in I, then

$$I = \bigoplus_j I_j,$$

since, by Lemma 5.3.8, all homogeneous summands of an element are again in I. So also

$$R/I = \bigoplus_j R_j/I_j$$

is a graded R-module, and

$$\dim_K(R_j/I_j) = \dim_K(R_j) - \dim_K(I_j).$$

This immediately raises the question, which information we can derive from the K-vector space dimensions of the graded pieces.

Definition and Theorem 5.4.3 *Consider* $R = K[x_0, \ldots, x_n]$ *with the standard grading, and let* M *be a graded* R*-module. If* M *is finitely generated, then* M_i *is a* K*-vector space of finite dimension. The* ***Hilbert function*** *of* M *is defined as*

$$\begin{array}{rccl} H_M : & \mathbb{Z} & \to & \mathbb{N}_0 \\ & i & \mapsto & \dim_K M_i \end{array}$$

Proof. If $\dim_K M_s = \infty$, then the submodule $\bigoplus_{i \ge s} M_i \subset M$ is not finitely generated, since any element in M_s can only be a K-linear combination of R-module generators. ■

Example 5.4.4 *The Hilbert function of R/I in Example 5.4.2 is*

i	0	1	2	3	4
$H_{R/I}(i)$	1	3	6	9	12

so for $i \geq 1$ it seems that

$$H_{R/I}(i) = 3i$$

agrees with a polynomial. This is a general phenomenon:

The following theorem by Hilbert shows that all information encoded in the Hilbert function is determined by only finitely many values:

Definition and Theorem 5.4.5 *Let $R = K[x_0, ..., x_n]$ with the standard grading, and M a finitely generated graded R-module. Then there is an $i_0 \in \mathbb{Z}$ and a polynomial $P_M \in \mathbb{Q}[t]$ of degree $\leq n$ with*

$$H_M(i) = P_M(i)$$

for all integers $i \geq i_0$.

*The polynomial P_M is called the **Hilbert polynomial** of M.*

Definition 5.4.6 *If $X \subset \mathbb{P}^n(K)$ is a projective variety, and $I = I(X) \subset R = K[x_0, ..., x_n]$ is the homogeneous zero ideal, then we define,*

1) *the **dimension** of X as the degree of $P_{R/I}$*

$$\dim(X) = \deg(P_{R/I}),$$

2) *the **degree** of X as $\dim(X)!$ times the lead coefficient of $P_{R/I}$*

$$\deg(X) = \dim(X)! \cdot \mathrm{LC}(P_{R/I}),$$

3) *the **arithmetic genus** of X as*

$$p_a(X) = (-1)^{\dim(X)} \left(P_{R/I}(0) - 1\right).$$

For an affine algebraic set X we define these invariants as the invariants of the projective closure $\mathrm{pc}(X)$.

Example 5.4.7 *Returning to Example 5.4.2, we use* SINGULAR *to compute the Hilbert polynomial $P_{R/I}$ and, hence, determine these invariants for $C = V(I)$:*

```
ring R=0,(x(0..2)),dp;
ideal I = x(0)^3-x(1)^3 - x(2)^3;
LIB "poly.lib";
hilbPoly(I);
0, 3
```

This tells us that

$$P_{R/I} = 3i + 0$$

so $\dim(C) = 1$, $\deg(C) = 3$ *and* $p_a(C) = 1$, *which makes sense for an elliptic curve. See also Exercise 5.3.*

By the proof of Theorem 5.4.5 we obtain an algorithm to compute the Hilbert polynomial. It uses graded free resolutions:

5.5 Graded free resolutions

Definition 5.5.1 *A homomorphism $f : M \to N$ of graded R-modules is called* ***homogeneous*** *if $f(M_i) \subset N_i$ for all i.*

Proposition 5.5.2 *If $f : M \to N$ is a homogeneous homomorphism of R-modules, the R-modules*

$$\begin{aligned} \ker(f) &\subset M \\ \operatorname{im}(f) &\subset N \\ \operatorname{coker}(f) &= N/\operatorname{im}(f) \end{aligned}$$

are graded.

Considering the homomorphisms

$$f_i = f\,|_{M_i} \colon M_i \to N_i$$

the proof is an easy exercise.

Remark 5.5.3 *If*

$$0 \to U \to M \to Q \to 0$$

is an exact sequence of graded modules with homogeneous homomorphisms then by the homomorphism theorem

$$H_U(i) - H_M(i) + H_Q(i) = 0$$

for all i.

Consider the homomorphism of $K[x]$-modules

$$K[x]^1 \to K[x]^1,\ e_1 \mapsto x \cdot e_1$$

where $e_1 = 1$ denotes the unit basis vector. This map clearly should be homogeneous. However, according to our definition it is not, since e_1 of degree $\deg(e_1) = 0$ is mapped to $x{\cdot}e_1$ of degree $\deg(x{\cdot}e_1) = \deg(x) + \deg(e_1) = 1$. This problem can easily be solved by shifting the degrees:

Definition 5.5.4 *If M is a graded R-module and $a \in \mathbb{Z}$, then the graded R-module $M(a)$ is defined by*

$$M(a)_i = M_{a+i}$$

*and is called the **a-th twist** of M.*

The module $K[x]^1(-1)$ has one generator $e_1' = 1$ of degree $\deg(e_1') = 1$, which is mapped by

$$K[x]^1(-1) \to K[x]^1,\ e_1' \mapsto x \cdot e_1$$

to $x \cdot e_1$ of degree $\deg(x \cdot e_1) = 1 + 0 = 1$. Hence, this homomorphism is homogeneous. More generally:

Example 5.5.5 *If $f_i \in R = K[x_0, ..., x_n]$ are homogeneous and $I = \langle f_1, ..., f_r \rangle \subset R$ then*

$$A = (f_1, ..., f_r) : \textstyle\bigoplus_{i=1}^r R(-\deg f_i) \to R$$

is a homogeneous homomorphism. In particular, $\operatorname{coker} A$ *is a graded R-module and* $\operatorname{coker} A \cong R/I$ *by a homogeneous isomorphism.*

Definition 5.5.6 *If M is a graded R-module, then a free resolution*

$$... \to F_i \xrightarrow{\phi_i} F_{i-1} \xrightarrow{\phi_{i-1}} ... \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} F_0 \xrightarrow{\phi_0} M \to 0$$

*is called **graded** if all ϕ_i are homogeneous.*

In particular, R and all F_i are graded.

Theorem 5.5.7 (Graded syzygy theorem) *Let $R = K[x_0, ..., x_n]$. Every finitely generated graded R-module has a finite graded free resolution. The free modules are finitely generated and the length is at most $n + 1$.*

We will prove Theorem 5.5.7 (and 5.2.4) by constructing a resolution using Gröbner basis techniques. Before, we use the graded syzygy theorem to prove Theorem 5.4.5 by giving an explicit construction of the Hilbert polynomial.

5.6 Construction of the Hilbert polynomial

Remark 5.6.1 *Let $R = K[x_0, ..., x_n]$. Since in R there are precisely*

$$\binom{i+n}{n} = \prod_{j=1}^{n} \frac{i+j}{j}$$

monomials of degree $i \geq 0$ and no monomials of negative degree, we have

$$H_R(i) = \binom{i+n}{n}_0 := \begin{cases} \binom{i+n}{n} & \text{for } i \geq -n \\ 0 & \text{otherwise} \end{cases}$$

Note that $\binom{i+n}{n} = 0$ for $i = -n, ..., -1$.

Hence for $i \geq -n$ the Hilbert function agrees with a polynomial of degree n:

$$H_R(i) = \frac{1}{n!}(i+n) \cdot ... \cdot (i+1).$$

So, for the twist $R(a)$ it holds

$$H_{R(a)}(i) = H_R(i+a) = \binom{i+a+n}{n}_0$$

Example 5.6.2 *For the Hilbert function of $R = K[x_0, x_1, x_2]$ as an R-module, we get*

i	0	1	2	3	4
$H_R(i)$	1	3	6	10	15

and for $i \geq -2$

$$H_R(i) = \frac{1}{2}(i+2)(i+1),$$

see Figure 5.6.

Remark 5.6.3 *If $R = K[x_0, ..., x_n]$ and $F = \bigoplus_{j=1}^{s} R(a_j)$, then*

$$H_F(i) = \sum_{j=1}^{s} \binom{i+a_j+n}{n}_0$$

and for $i \geq -\min\{a_j\} - n$

$$H_F(i) = \sum_{j=1}^{s} \binom{i+a_j+n}{n}$$

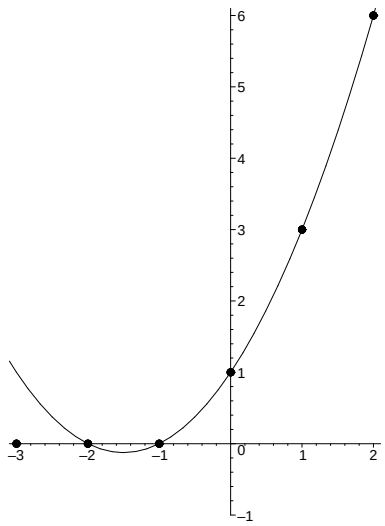

Figure 5.6: Hilbert function of $K[x_0, x_1, x_2]$.

Example 5.6.4 *If* $R = K[x_0, x_1, x_2]$ *and* $M = R(-2) \oplus R(-3)$ *we have*

$$H_R(i) = \frac{1}{2}\left(i(i-1) + (i-1)(i-2)\right) = (i-1)^2$$

for $i \geq 1 = -\min\{-2, -3\} - 2$, *see Figure 5.7. For example, written in terms of the standard basis vectors* e_1 *of degree* 2 *and* e_2 *of degree* 3,

$$M_2 = \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle$$

and

$$M_3 =_K \left\langle \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} x_1 \\ 0 \end{pmatrix}, \begin{pmatrix} x_2 \\ 0 \end{pmatrix}, \begin{pmatrix} x_3 \\ 0 \end{pmatrix} \right\rangle$$

Note that $\deg(x_i e_1) = 1 + 2 = 3$.

Using these elementary observations and the graded syzygy theorem, we now prove Theorem 5.4.5. For a different proof see Exercises 5.8 and 5.6.

Proof. By Theorem 5.5.7, any finitely generated graded R-module has a finite graded free resolution

$$0 \to F_l \xrightarrow{\phi_l} F_{l-1} \xrightarrow{\phi_{l-1}} \ldots \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} F_0 \xrightarrow{\phi_0} M \to 0$$

So by Remark 5.5.3,

$$H_M(t) = \sum_{i=0}^{r} (-1)^i H_{F_i}(t).$$

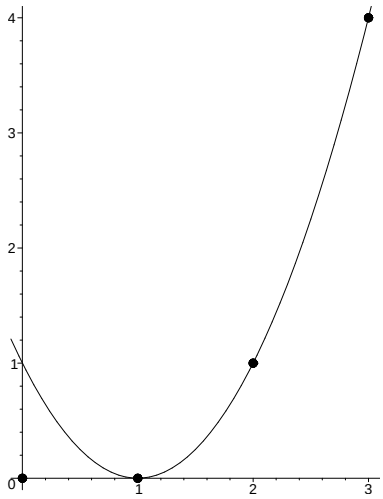

Figure 5.7: Hilbert function of $R(-2) \oplus R(-3)$ for $R = K[x_0, x_1, x_2]$.

Writing

$$F_i = \bigoplus_{j=1}^{s_i} R(a_{i,j})$$

by Remarks 5.6.1 and 5.6.3, we have

$$H_{F_i}(t) = \sum_{j=1}^{s_i} \binom{t + a_{i,j} + n}{n}_0$$

so

$$H_M(t) = \sum_{i=0}^{r} (-1)^i \sum_{j=1}^{s_i} \binom{t + a_{i,j} + n}{n}_0$$

Hence for $i \geq -\min\{a_{i,j}\} - n$ the Hilbert function agrees with the polynomial

$$H_M(t) = \sum_{i=0}^{r} (-1)^i \sum_{j=1}^{s_i} \binom{t + a_{i,j} + n}{n}$$

of degree $\leq n$. ■

Algorithm 5.6.5 *The constructive proof immediately yields an algorithm to compute both the Hilbert function and the Hilbert polynomial from a graded free resolution.*

Example 5.6.6 *For the plane cubic* $I = \langle x_0^3 - x_1^3 - x_2^3 \rangle \subset R = K[x_0, x_1, x_2]$ *from Example 5.4.2 the resolution of* R/I *is*

$$0 \to R(-3)^1 \to R \to R/I \to 0$$

and

$$\begin{aligned} H_M(t) &= \dim_K R_t - \dim_K I_t \\ &= \dim_K R_t - \dim_K R_{t-3} \\ &= \binom{t+2}{2} - \binom{t-1}{2} \\ &= \frac{1}{2}\left((t+2)(t+1) - (t-1)(t-2)\right) \\ &= 3t \end{aligned}$$

Example 5.6.7 *Consider the projective twisted cubic* $C = V(I) \subset \mathbb{P}^3(K)$*, where*

$$I = \left\langle x_2^2 - x_1x_3,\ x_1x_2 - x_0x_3,\ x_1^2 - x_2x_0 \right\rangle.$$

A finite free resolution of R/I *is given by*

$$0 \to R(-3)^2 \to R(-2)^3 \to R \to R/I \to 0$$

as the following SINGULAR *calculation shows:*

```
ring R=0,(x0,x1,x2,x3),dp;
ideal I=x2^2-x1*x3, x1*x2-x0*x3, x1^2-x2*x0;
def L=res(I,0);
   1          3          2
 R     <--  R     <--  R
 0          1          2
print(betti(L),"betti");
          0  1  2
------------------
 0:       1  -  -
 1:       -  3  2
------------------
 total:   1  3  2
```

In general, for a graded free resolution

$$0 \to F_l \to F_{l-1} \to \ldots \to F_1 \to F_0 \to M \to 0$$

the column i *of this so called* ***Betti table*** *corresponds to the free module* F_i*. The rank of* F_i *is given in the last row "total". At row position* j *and column position* i *the number of free generators of* F_i *of degree* $j+i$ *is indicated.*

The shift by i *has the benefit of leading to a more compact table, since, homogeneous maps given by linear polynomials have source and target in the same row (as we will see, we can assume that the maps* ϕ_i *are given by matrices with entries of degree at least* 1*).*

See also Exercise 5.5.

Example 5.6.8 *From the resolution we obtain for* $t \geq 0 = 3 - 3$

$$\begin{aligned} H_{R/I}(t) &= \binom{t+0+3}{3} - 3\binom{t-2+3}{3} + 2\binom{t-3+3}{3} \\ &= \frac{1}{3!}\left((t+3)(t+2)(t+1) - 3(t+1)t(t-1) + 2t(t-1)(t-2)\right) \\ &= 3t+1 \end{aligned}$$

so in the alternating sum the t^3 *and* t^2 *terms cancel, and we obtain a polynomial of degree* 1*. Hence,*

$$\dim(C) = 1 \qquad \deg(C) = 3 \qquad p_a(C) = 0$$

For an example of higher dimension, see Exercise 5.5.

5.7 Monomial orderings for modules

Let $R = K[x_1, ..., x_n]$. For the moment we do not consider any grading on R. To compute free resolution we have to extend the Buchberger algorithm from ideals of R to the setup of submodules of the free module R^t.

First of all, what are the monomials? Write e_i for the i-th standard basis vector of R^t. Then, like in the case of polynomials, any element of R^t can be written as a sum of terms of the form $c_\alpha x^\alpha e_i$. For example, in $K[x, y]^2$

$$\begin{pmatrix} 2x + y^2 \\ x \end{pmatrix} = 2xe_1 + y^2 e_1 + xe_2.$$

Hence we define:

Definition 5.7.1 *An element of the form* $x^\alpha e_i \in R^t$ *we call a* ***monomial****, and a non-zero constant multiple of a monomial we call a* ***term****.*

A ***monomial ordering*** *on* R^t *is an ordering* $>$ *on the set of monomials in* R^t *such that*

1) $>$ *is a total ordering*

2) $>$ *respects multiplication, that is,*

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

for all $\alpha, \beta, \gamma, i, j$.

3) $x^\alpha e_i > x^\beta e_i \Leftrightarrow x^\alpha e_j > x^\beta e_j$ *for all* α, β, i, j.

Remark 5.7.2 *By setting* $x^\alpha > x^\beta \Leftrightarrow x^\alpha e_i > x^\beta e_i$ *the ordering* $>$ *uniquely determines a monomial ordering on* R*, which we again denote by* $>$.

Definition 5.7.3 *A monomial ordering on* R^t *is called* ***global*** *if the induced ordering on* R *is global.*

Remark 5.7.4 *The ordering* $>$ *on* R^t *is a well ordering if and only if the induced ordering* $>$ *on* R *is a well ordering.*

Proof. The implication $\Rightarrow$ is trivial. On the other hand, any set of monomials is a union $M = M_1e_1 \cup ... \cup M_se_s$ where M_i are sets of monomials in R. So if $>$ is a well ordering on R then M_i has a smallest element m_i, and there is a smallest element in the finite set $\{m_1e_1, ..., m_se_s\}$. ■

Example 5.7.5 *Given a monomial ordering* $>$ *on* R *there are two canonical ways of producing a monomial ordering on* R^t*:*

1) Priority to the monomials $(>, c)$*:*

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

2) Priority to the components $(c, >)$*:*

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

Example 5.7.6 *In* SINGULAR *we can give priority to the monomials by*

```
ring R = 0,(x,y),(lp,c);
[1,0]>[0,1];
1
[x,0]>[y,0];
1
[0,x]>[y,0];
1
```

and priority to the components by

```
ring R = 0,(x,y),(c,lp);
[0,x]>[y,0];
0
[y,0]>[0,x];
1
```

If you use `C` *instead of* `c`*, then the ordering of the unit basis vectors is reversed.*

Definition 5.7.7 *With respect to a given monomial ordering* $>$ *on* R^t*, for any element*

$$v = \sum_{\alpha,i} c_\alpha x^\alpha e_i$$

the ***leading monomial*** *is the largest monomial* $x^\alpha e_i$ *with* $c_\alpha \neq 0$ *and is denoted by* $L(v)$*. Furthermore, we denote by* $LC(v) = c_\alpha$ *the* ***leading coefficient****, and by* $LT(v) = c_\alpha x^\alpha e_i$ *the* ***leading term****.*

Example 5.7.8 *Using* (lp, c) *on* $K[x, y]^2$*, for*

$$f = \begin{pmatrix} x \\ 5x^2y + xy^2 \end{pmatrix} = 5x^2y \cdot e_2 + x \cdot e_1 + xy^2 \cdot e_2$$

we get

$$L(f) = x^2y \cdot e_2 \qquad LC(f) = 5 \qquad LT(f) = 5x^2y \cdot e_2$$

In Singular*:*

```
ring R=0,(x,y),(lp,c);
vector f = [x, 5x2y+xy2];
leadmonom(f);
x2y*gen(2)
leadcoef(f);
5
lead(f);
5x2y*gen(2)
```

To do one more example, for

$$f = \begin{pmatrix} y + z \\ x + y \end{pmatrix} \in K[x, y, z]^2$$

with respect to (lp, c) *we have*

$$L(f) = x \cdot e_2$$

and with respect to (c, lp)

$$L(f) = y \cdot e_1$$

In Singular*:*

```
ring R=0,(x,y,z),(lp,c);
vector f = [y+z, x+y];
leadmonom(f);
x*gen(2)
ring R=0,(x,y,z),(c,lp);
vector f = [y+z, x+y];
```

```
leadmonom(f);
[y]
```

Note, that for (lp, c), Singular writes the elements of R^t in terms of unit basis vectors, and for (c, lp) as lists. Note also, that in the list notation, trailing zeros are skipped. You can also use both ways to input vectors.

Definition 5.7.9 *The monomials of R^t come with a natural partial order, which we call* ***divisibility***

$$x^\alpha e_i \mid x^\beta e_j \Longleftrightarrow i = j \text{ and } x^\alpha \mid x^\beta$$

Moreover, given two terms $c_1 x^\alpha e_i$ and $c_2 x^\beta e_j$ with $x^\alpha e_i \mid x^\beta e_j$ we define their quotient as

$$\frac{c_2 x^\beta e_j}{c_1 x^\alpha e_i} = \frac{c_2 x^\beta}{c_1 x^\alpha} \in R.$$

Definition 5.7.10 *A submodule $U \subset R^t$ is called* ***monomial****, if it is generated by monomials.*

Lemma 5.7.11 *Every monomial submodule has a unique set of* ***minimal generators*** *consisting of monomials.*

Proof. Let $U = \langle M \rangle \subset R^t$ be generated by the set of monomials M. By Lemma 4.3.11 the free module R^t is Noetherian, hence U is finitely generated by $f_1, ..., f_r \in U$ (see Definition and Theorem 4.3.9). Like in the case of ideals, write $f_i = \sum_{j=1}^{u} r_{i,j} m_j$ with $m_j \in M$. Then $U \subset \langle m_1, ..., m_u \rangle \subset \langle M \rangle = U$. Among the m_j consider the minimal elements with respect to divisibility.

Note that

$$x^\alpha e_i \leq x^\beta e_j \Longleftrightarrow x^\alpha e_i \mid x^\beta e_j$$

gives a partial order on the set of monomials of R^t. ■

5.8 Division with remainder and Gröbner bases for modules

The basic setup for the theory of Gröbner bases of submodules of R^t works just like in the case of ideals (that is, $t = 1$) as described in Section 2.4. To convince ourselves that this is indeed the case, let us recall the fundamental steps.

Definition 5.8.1 *Given a list $G = (g_1, ..., g_s)$ of elements of R^t, a* ***normal form*** *is a map $\mathrm{NF}(-, G) : R^t \to R^t$ 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 all $0 \neq f \in R$ 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 $a_i g_i \neq 0$.

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

Using Definition 5.7.9, Division with remainder in R (Algorithm 2.4.1) generalizes immediately to Algorithm 5.8.1 in R^t. It gives a normal form in the sense of Definition 5.8.1.

Algorithm 5.8.1 Division with remainder for modules

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

Output: An expression

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

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

```
q = 0
r = f
while r ≠ 0 and L(g_i) | L(r) for some i do
    Cancel the lead term of r:
    a = LT(r)/LT(g_i) ∈ R as given in Definition 5.7.9
    q = q + a · g_i
    r = r − a · g_i
```

Example 5.8.2 *Let $R = K[x_1, ..., x_5]$ and consider the monomial ordering (lp, c) on R^5 obtained from lp by giving priority to the monomials. Let $g_i \in R^5$ be the i-th column of the matrix*

$$A = \left(\begin{array}{c|c|c|c|c} 0 & \boldsymbol{x}_2 & 0 & 0 & -\boldsymbol{x}_1 \\ -x_2 & 0 & \boldsymbol{x}_3 & 0 & 0 \\ 0 & -x_3 & 0 & \boldsymbol{x}_4 & 0 \\ 0 & 0 & -x_4 & 0 & x_5 \\ \boldsymbol{x}_1 & 0 & 0 & -x_5 & 0 \end{array}\right)$$

and $U = \mathrm{im}(A) = \langle g_1, \ldots, g_5 \rangle \subset R^5$. *We try out Algorithm 5.8.1 to divide some vectors* $v \in R^5$ *by* $G = (g_1, \ldots, g_5)$*:*

$$v = \begin{pmatrix} 0 \\ 0 \\ 0 \\ -x_2x_4 \\ \boldsymbol{x_1x_3} \end{pmatrix} = x_3 \begin{pmatrix} 0 \\ -x_2 \\ 0 \\ 0 \\ \boldsymbol{x_1} \end{pmatrix} + \begin{pmatrix} 0 \\ \boldsymbol{x_2x_3} \\ 0 \\ -x_2x_4 \\ 0 \end{pmatrix}$$
$$= x_3 \begin{pmatrix} 0 \\ -x_2 \\ 0 \\ 0 \\ \boldsymbol{x_1} \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ \boldsymbol{x_3} \\ 0 \\ -x_4 \\ 0 \end{pmatrix} + 0$$

which shows that $v \in U$.

In the following example the division terminates early:

$$v = \begin{pmatrix} 0 \\ 0 \\ 0 \\ x_1 - x_2x_4 \\ \boldsymbol{x_1x_3} \end{pmatrix} = x_3 \begin{pmatrix} 0 \\ -x_2 \\ 0 \\ 0 \\ \boldsymbol{x_1} \end{pmatrix} + \begin{pmatrix} 0 \\ x_2x_3 \\ 0 \\ x_1 - x_2x_4 \\ 0 \end{pmatrix}$$

This can be fixed by considering reduced division, just like in Algorithm 2.4.2, which will put x_1e_4 *into the remainder. Recall, that for testing whether a normal form is zero, this is not a problem: If we would put terms into the remainder in intermediate steps, they would never go away again (since in every step the lead term decreases). So once Algorithm 5.8.1 stops with a non-zero remainder, we know that also reduced division will not give zero (and vice versa).*

Finally, for

$$v = \begin{pmatrix} 0 \\ 0 \\ \boldsymbol{-x_1x_3} \\ x_2x_5 \\ 0 \end{pmatrix} = x_1g_2 + x_2g_5$$

Algorithm 5.8.1 will not do anything, and return v *as the remainder, although* $v \in U$. *The reason is that* G *is not a Gröbner basis. We will return to this in the next section.*

In Singular *these calculation can be done as follows:*

```
ring R = 0,(x(1..5)),(lp,c);
module M = [0,-x(2),0,0,x(1)],
           [x(2),0,-x(3),0,0],
```

```
            [0,x(3),0,-x(4),0],
            [0,0,x(4),0,-x(5)],
            [-x(1),0,0,x(5),0];
reduce([0,0,0,-x(2)*x(4),x(1)*x(3)],M,1);
0
reduce([0,0,0,x(1)-x(2)*x(4),x(1)*x(3)],M,1);
x(1)*gen(4)+x(2)*x(3)*gen(2)-x(2)*x(4)*gen(4)
reduce([0,0,-x(1)*x(3),x(2)*x(5),0],M,1);
-x(1)*x(3)*gen(3)+x(2)*x(5)*gen(4)
```

Provided we divide by a Gröbner basis, division with remainder solves the submodule membership problem:

Definition 5.8.3 *Given a monomial ordering $>$ and a subset $G \subset R^t$, we define the* ***leading module*** *of G as*

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

the monomial submodule generated by the leading monomials.

Definition 5.8.4 *Let $U \subset R^t$ be a submodule and $>$ a global monomal ordering on R^t. A finite set $0 \notin G \subset U$ is called* ***Gröbner basis*** *of U with respect to $>$, if*

$$L(G) = L(U).$$

Theorem 2.4.8, Lemma 2.4.9 and Corollary 2.4.10 generalize immediately to the module setup:

Theorem 5.8.5 (Submodule membership) *Let $U \subset R^t$ be a submodule and $f \in R^t$. If $G = (g_1, ..., g_s)$ is a Gröbner basis of U and* NF *is a normal form, then*

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

Proof. Write $f = \sum_i a_i g_i + r$ with $r = \mathrm{NF}(f, G)$. If $r = 0$ then $f \in \langle G \rangle \subset U$. On the other hand, if $r \neq 0$ then by Definition 5.8.1 (2.)

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

So, $r \notin U$, hence $f = \sum_i a_i g_i + r \notin U$. ■

Lemma 5.8.6 *If $V \subset U \subset R^t$ are submodules with $L(V) = L(U)$ then $U = V$.*

Proof. Let $G = (g_1, ..., g_s)$ be a Gröbner basis of V, NF a normal form, $f \in U$ and $f = \sum_i a_i g_i + r$ with $r = \mathrm{NF}(f, G)$. So $r \in U$. If $r \neq 0$, then by Definition 5.8.1 (2.)

$$L(r) \notin L(G) = L(V) = L(U).$$

Hence $r \notin U$, a contradiction. ■

Corollar 5.8.7 *If G is a Gröbner basis of the submodule $U \subset R^t$, then*

$$U = \langle G \rangle .$$

Proof. We have $L(U) = L(G) \subset L(\langle G \rangle) \subset L(U)$, so G is a Gröbner basis of $\langle G \rangle \subset U$ and $L(\langle G \rangle) = L(U)$. Equality follows from Lemma 5.8.6. ■

Remark 5.8.8 *To have a uniquely determined remainder, we proceed as follows: A vector $f \in R^t$ is called **reduced** with respect to a set $G \subset R^t$, if no term of f is contained in $L(G)$. A normal form is called **reduced normal form**, if $\mathrm{NF}(f, G)$ is reduced with respect to G for all f and G.*

Arguing in the same way as in proof of Theorem 2.4.15 shows that, for a reduced normal form, the remainder is unique.

Also Algorithm 2.4.2 immediately generalizes to the module case, yielding a reduced normal form. Recall that for reduced division with remainder we do not stop if the lead monomial is not divisible by some lead monomial of G, but instead put the lead term into the remainder and continue.

Example 5.8.9 *Using reduced division with remainder, we can continue the second calculation in Example 5.8.2:*

$$v = \begin{pmatrix} 0 \\ 0 \\ 0 \\ x_1 - x_2x_4 \\ \boldsymbol{x_1x_3} \end{pmatrix} = x_3 \begin{pmatrix} 0 \\ -x_2 \\ 0 \\ 0 \\ \boldsymbol{x_1} \end{pmatrix} + \begin{pmatrix} 0 \\ x_2x_3 \\ 0 \\ \boldsymbol{x_1} - x_2x_4 \\ 0 \end{pmatrix}$$

$$= x_3 \begin{pmatrix} 0 \\ -x_2 \\ 0 \\ 0 \\ \boldsymbol{x_1} \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ x_1 \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ \boldsymbol{x_3} \\ 0 \\ -x_4 \\ 0 \end{pmatrix}$$

In SINGULAR*:*

```
ring R = 0,(x(1..5)),(lp,c);
module M = [0,-x(2),0,0,x(1)],
           [x(2),0,-x(3),0,0],
           [0,x(3),0,-x(4),0],
           [0,0,x(4),0,-x(5)],
           [-x(1),0,0,x(5),0];
reduce([0,0,0,x(1)-x(2)*x(4),x(1)*x(3)],M);
x(1)*gen(4)
```

5.9 Computing Gröbner bases of submodules

Fix a global monomial ordering $>$ on R^t. We follow the same strategy as in Section 2.5 by cancelling lead terms via S-polynomials. Clearly, lead terms can only cancel if they occur in the same component of the vectors. Hence, we define:

Definition 5.9.1 *The* ***least common multiple*** *of two monomials $x^\alpha e_i$ and $x^\beta e_j$ in R^t is*

$$\operatorname{lcm}(x^\alpha e_i, x^\beta e_j) = \begin{cases} \operatorname{lcm}(x^\alpha, x^\beta) & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

Definition 5.9.2 *The syzygy polynomial or* ***S-polynomial*** *of $f, g \in R^t$ is defined as the vector*

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

In particular, writing $L(f) = x^\alpha e_i$ and $L(g) = x^\beta e_j$, if $i \neq j$ then $\operatorname{spoly}(f,g) = 0$. On the other hand, if $i = j$ then, according to Definition 5.7.9, we have a well defined quotient

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

Using this notation, Buchberger's algorithm for ideals carries over directly to Algorithm 5.9.1. Clearly we have to consider in the algorithm only pairs of elements $f \neq g$ which have the lead term in the same component.

Algorithm 5.9.1 Buchberger

Input: $U = \langle g_1, \ldots, g_s \rangle \subset R^t$ a submodule, $>$ a global monomial ordering, and NF a normal form.

Output: A Gröbner basis of U with respect to $>$.

```
G = {g_1, ..., g_s}
repeat
    H = G
    for all f, g ∈ H do
        r = NF(spoly(f, g), H)
        if r ≠ 0 then
            G = G ∪ {r}
until G = H
```

Proof. If $r \neq 0$ then $L(r) \notin L(H)$ by Definition 5.8.1(2.), hence

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

Since R^t is Noetherian (Lemma 4.3.11), the algorithm terminates by the chain condition (Definition and Theorem 4.3.9). To show that the final result is a Gröbner basis, we will prove Buchberger's criterion in the next Section 5.10. ■

Example 5.9.3 *Continuing Example 5.8.2, we use Buchberger's algorithm to compute a Gröbner basis of $U \subset R^5$ with respect to (lp, c). In each step the first column denotes the coefficients in the syzygy polynomial and the second the division with remainder.*

	↱ $-\boldsymbol{x}_1\boldsymbol{x}_3\boldsymbol{e}_3 + x_2x_5e_4$	↱ $-\boldsymbol{x}_1\boldsymbol{x}_3\boldsymbol{x}_5\boldsymbol{e}_5 + x_2x_4x_5e_4$
$g_1 = \boldsymbol{x}_1\boldsymbol{e}_5 - x_2e_2$		x_3x_5
$g_2 = \boldsymbol{x}_2\boldsymbol{e}_1 - x_3e_3$	x_1	
$g_3 = \boldsymbol{x}_3\boldsymbol{e}_2 - x_4e_4$		x_2x_5
$g_4 = \boldsymbol{x}_4\boldsymbol{e}_3 - x_5e_5$		x_1x_3
$g_5 = -\boldsymbol{x}_1\boldsymbol{e}_1 + x_5e_4$	x_2	
$g_6 = \boldsymbol{x}_1\boldsymbol{x}_3\boldsymbol{e}_3 - x_2x_5e_4$	1	$-x_4$

For the first calculation, recall that already in Example 5.8.2 we observed that $\mathrm{NF}(g_6, (g_1, \ldots, g_5)) = g_6 \neq 0$. *The second calculation step by step:*

$$\begin{aligned}
\mathrm{spoly}(g_4, g_6) &= -\boldsymbol{x}_1\boldsymbol{x}_3\boldsymbol{x}_5\boldsymbol{e}_5 + x_2x_4x_5e_4 \\
&= x_3x_5 \cdot g_1 + (-\boldsymbol{x}_2\boldsymbol{x}_3\boldsymbol{x}_5\boldsymbol{e}_2 + x_2x_4x_5e_4) \\
&= x_3x_5 \cdot g_1 + x_2x_5 \cdot g_3 + 0
\end{aligned}$$

Since there are no further non-zero S-polynomials, this proves that $(g_1, \ldots, g_6)$ is a Gröbner basis.

Dividing by $(g_1, ..., g_6)$*, the submodule membership test for* g_6 *now obviously works as expected:* $\mathrm{NF}(g_6, (g_1, ..., g_6)) = 0$.

The Gröbner basis calculation in SINGULAR*:*

```
ring R = 0,(x(1..5)),(lp,c);
module M = [0,-x(2),0,0,x(1)],
           [x(2),0,-x(3),0,0],
           [0,x(3),0,-x(4),0],
           [0,0,x(4),0,-x(5)],
           [-x(1),0,0,x(5),0];
std(M);
_[1]=x(4)*gen(3)-x(5)*gen(5)
_[2]=x(3)*gen(2)-x(4)*gen(4)
_[3]=x(2)*gen(1)-x(3)*gen(3)
_[4]=x(1)*gen(5)-x(2)*gen(2)
_[5]=x(1)*gen(1)-x(5)*gen(4)
_[6]=x(1)*x(3)*gen(3)-x(2)*x(5)*gen(4)
print(std(M));
 0,      0,      x(2),   0,      x(1),   0,
 0,      x(3),   0,      -x(2),  0,      0,
 x(4),   0,      -x(3),  0,      0,      x(1)*x(3),
 0,      -x(4),  0,      0,      -x(5),  -x(2)*x(5),
 -x(5),  0,      0,      x(1),   0,      0
```

Remark 5.9.4 *Using the notion of divisibility as introduced in Definition 5.7.9, the definitions of minimal and reduced Gröbner bases carry over from the ideal case immediately.*

Given a Gröbner basis $G = (g_1, ..., g_s)$*, by Lemma 5.7.11, the* g_i *corresponding to the (with respect to divisibility) minimal elements of* $\{L(g_i) \mid i\}$ *form a minimal Gröbner basis.*

Just like in the ideal case (Theorem 2.5.7 and Remark 2.5.8) we can obtain the unique reduced Gröbner basis.

5.10 Buchberger's criterion and computation of syzygy modules

We now prove Buchberger's criterion for Gröbner bases of submodules $U \subset R^t$.

As we have already observed in the ideal case (Theorem 2.5.2), the strategy for the proof is closely related to syzygies. Indeed, the Buchberger test produces a Gröbner basis of the module of syzygies with respect to an appropriately chosen ordering. By iterating this, we will obtain an algorithm to compute free resolutions. This

algorithm is, by far, the fastest way of computing free resolutions. It is implemented in SINGULAR in the command `sres`.

Definition 5.10.1 *For a matrix $G \in R^{t\times s}$ we define the* ***syzygy module*** *of G as the kernel*

$$\mathrm{Syz}(G) = \ker(G) \subset R^s,$$

and the elements are called ***syzygies*** *of G.*

Any matrix $S_G \in R^{s\times g}$ with

$$\mathrm{im}(S_G) = \mathrm{Syz}(G),$$

that is, with generators of $\mathrm{Syz}(G)$ in its columns, we call a ***syzygy matrix*** *of G.*

We use the notation also for a list $G = (g_1, ..., g_s)$ of elements of R^t, then defining the syzygy module of G as $\mathrm{Syz}(G) = \mathrm{Syz}(M_G)$ for the matrix

$$M_G = (g_1 \mid ... \mid g_s) : \begin{array}{ccc} R^s & \to & R^t \\ e_i & \mapsto & g_i \end{array}$$

To summarize, the image of M_G

$$\mathrm{im}(M_G) = \langle g_1, ..., g_s\rangle \subset R^t$$

is the submodule of R^t generated by the g_i, and

$$\mathrm{im}(S_G) = \ker(g_1 \mid ... \mid g_s) \subset R^s$$

is the module of relations between the g_i.

Note also that, by iteratively computing syzygy matrices, we can compute free resolutions. We will do this in more detail in the next section.

See also Exercise 6.1 for an application of the syzygy matrix for computing intersections of ideals.

Remark 5.10.2 *Any syzygy $v = \sum_{i=1}^s v_i e_i \in \mathrm{Syz}(G) \subset R^s$ corresponds to a relation*

$$\sum_{i=1}^s v_i g_i = 0.$$

Given a global monomial ordering $>$, every successful Buchberger test

$$\mathrm{NF}(\mathrm{spoly}(g_i, g_j), G) = 0$$

gives an expression

$$\underbrace{\frac{\mathrm{lcm}(L(g_i),L(g_j))}{LT(g_i)}}_{m} \cdot g_i \quad - \quad \underbrace{\frac{\mathrm{lcm}(L(g_i),L(g_j))}{LT(g_j)}}_{w} \cdot g_j \quad - \quad \sum_{k=1}^{s} a_k g_k \quad = \quad 0$$

and, hence, a syzygy

$$\begin{aligned} \mathrm{s}(g_i, g_j) \quad &:= \quad m \cdot e_i - w \cdot e_j - \textstyle\sum_{k=1}^{s} a_k e_k \\ &\in \quad \mathrm{Syz}(G) \subset R^s \end{aligned}$$

For a Gröbner basis $G = (g_1, ..., g_s)$ we will even prove: With respect to the following ordering, the $\mathrm{s}(g_i, g_j)$ form a Gröbner basis of $\mathrm{Syz}(G)$.

Definition 5.10.3 *Let $G = (g_1, ..., g_s)$ be a list of elements $g_i \in R^t$ and $>$ a monomial ordering on R^t. A monomial ordering $>_G$ on R^s is defined by*

$$x^\alpha e_i >_G x^\beta e_j :\Longleftrightarrow L(x^\alpha g_i) > L(x^\beta g_j) \text{ or } \big(L(x^\alpha g_i) = L(x^\beta g_j) \text{ and } i < j\big)$$

*It is called the **Schreyer ordering** induced by $>$ and G.*

The key property is, that we have control over the lead monomials of the syzygies:

Lemma 5.10.4 *If $i < j$ then*

$$L(\mathrm{s}(g_i, g_j)) = \frac{\mathrm{lcm}(L(g_i), L(g_j))}{L(g_i)} e_i$$

where the left hand side is with respect to $>_G$ and the right hand side with respect to $>$.

Proof. We can assume $\mathrm{s}(g_i, g_j) \neq 0$; otherwise the claim is trivial. Since in an S-polynomial the lead terms cancel we have (using the notation of Remark 5.10.2)

$$L(m \cdot g_i) = L(w \cdot g_j)$$

so by $i < j$ it holds

$$m \cdot e_i >_G w \cdot e_j.$$

Moreover, since NF is a normal form, for all k

$$L(a_k g_k) \leq L(\mathrm{spoly}(g_i, g_j)) < L(m \cdot g_i),$$

that is, also

$$m \cdot e_i >_G L(a_k e_k)$$

for all k. Using both observations,

$$L(\mathrm{s}(g_i, g_j)) = m \cdot e_i.$$

■

Remark 5.10.5 *If $>$ is global, then also $>_G$ is global (Exercise).*

Example 5.10.6 *We return to the resolution of the projective twisted cubic as discussed in Example 5.6.7. So let $C = V(I) \subset \mathbb{P}^3(K)$, where I is generated by the Gröbner basis*

$$G = (\boldsymbol{x}_2^2 - x_1x_3,\ \boldsymbol{x}_1\boldsymbol{x}_2 - x_0x_3,\ \boldsymbol{x}_1^2 - x_0x_2)$$

with respect to dp. For

$$A = \left(\begin{array}{c|c} x_1 & -x_0 \\ -x_2 & x_1 \\ x_3 & -x_2 \end{array}\right)$$

we have $M_G \cdot A = 0$ hence $\mathrm{im}(A) \subset \mathrm{syz}(G)$. We verify that the columns of A form a Gröbner basis of $\mathrm{im}(A)$ with respect to $>_G$. Observe that with respect to dp

$$\begin{aligned} x_1 \cdot x_2^2 &= x_2 \cdot x_1x_2 > x_3 \cdot x_1^2 \\ x_0 \cdot x_2^2 &< x_1 \cdot x_1x_2 = x_2 \cdot x_1^2, \end{aligned}$$

hence the lead terms of the columns of A with respect to $>_G$ are

$$A = \left(\begin{array}{c|c} \boldsymbol{x}_1 & -x_0 \\ -x_2 & \boldsymbol{x}_1 \\ x_3 & -x_2 \end{array}\right)$$

This tells us that there is no non-zero syzygy between the columns, so, assuming that Algorithm 5.9.1 is correct, they form a Gröbner basis of $\mathrm{im}(A)$.

For the moment we do not know whether the columns of A generate $\mathrm{syz}(G)$. This question will be solved as a by-product of the proof of Buchberger's test:

Theorem 5.10.7 (Buchberger test) *Let $>$ be a global monomial ordering on R^t and NF a normal form algorithm. Let $U = \langle g_1, \ldots, g_s \rangle \subset R^t$ be a submodule. If*

$$\mathrm{NF}(\mathrm{spoly}(g_i, g_j), G) = 0$$

for all $i < j$, then

1) *$G = (g_1, \ldots, g_s)$ is a Gröbner basis of U with respect to $>$, and*

2) *the non-zero syzygies $\mathrm{s}(g_i, g_j)$ for $i < j$ form a Gröbner basis G' of $\mathrm{Syz}(G)$ with respect to $>_G$, in particular, by Corollary 5.8.7,*

$$\mathrm{Syz}(G) = \langle G' \rangle .$$

Note that this finishes the proof of correctness of Algorithm 5.9.1. Before proving the theorem, we apply it to Example 5.10.6:

Example 5.10.8 *We do the Buchberger test for*

$$G = (\boldsymbol{x}_2^2 - x_1x_3,\ \boldsymbol{x}_1\boldsymbol{x}_2 - x_0x_3,\ \boldsymbol{x}_1^2 - x_0x_2)$$

and the monomial ordering dp:

	↱	$-\boldsymbol{x}_1^2\boldsymbol{x}_3 + x_0x_2x_3$	↱	$\boldsymbol{x}_0\boldsymbol{x}_2^2 - x_0x_1x_3$	↱	$\boldsymbol{x}_0\boldsymbol{x}_2^3 - x_1^3x_3$
$\boldsymbol{x}_2^2 - x_1x_3$	x_1			$-x_0$	x_1^2	$-x_0x_2$
$\boldsymbol{x}_1\boldsymbol{x}_2 - x_0x_3$	$-x_2$		x_1			
$\boldsymbol{x}_1^2 - x_0x_2$		x_3	$-x_2$		$-x_2^2$	x_1x_3

By Theorem 5.10.7, this shows that G is a Gröbner basis of $I = \langle G \rangle$ with respect to dp. Moreover, it proves that

$$G' = \left(\begin{pmatrix} \boldsymbol{x}_1 \\ -x_2 \\ x_3 \end{pmatrix}, \begin{pmatrix} -x_0 \\ \boldsymbol{x}_1 \\ -x_2 \end{pmatrix}, \begin{pmatrix} \boldsymbol{x}_1^2 - x_0x_2 \\ 0 \\ -x_2^2 + x_1x_3 \end{pmatrix} \right)$$

is a Gröbner basis of the syzygy module $\mathrm{Syz}(G)$ *with respect to* $>_G$. *The last vector can be deleted since its lead monomial $x_1^2e_1$ is divisible by the lead monomial x_1e_1 of the first vector, hence*

$$G' = \left(\begin{pmatrix} \boldsymbol{x}_1 \\ -x_2 \\ x_3 \end{pmatrix}, \begin{pmatrix} -x_0 \\ \boldsymbol{x}_1 \\ -x_2 \end{pmatrix} \right)$$

is a minimal Gröbner basis of $\mathrm{Syz}(G)$. *Indeed, it is the reduced Gröbner basis.*

In particular,

$$\ker(M_G) = \mathrm{im}(M_{G'})$$

with

$$M_{G'} = \left(\begin{array}{c|c} \boldsymbol{x}_1 & -x_0 \\ -x_2 & \boldsymbol{x}_1 \\ x_3 & -x_2 \end{array} \right).$$

We can continue now one step further by considering syzygies of syzygies, that is, we do the Buchberger test for G'. As already observed in Example 5.10.6, there is no non-trivial syzygy between the vectors in G', that is, $\ker(M_{G'}) = 0$. *Hence,*

$$0 \to R^2 \overset{M_{G'}}{\to} R^3 \overset{M_G}{\to} R^1 \to R/I \to 0$$

is a free resolution.

In fact, since we begin with a graded matrix of generators M_G, also the syzygy matrix $M_{G'}$, as produced by the theorem, is a graded homomorphism. So, taking the grading into account, we have proven that the projective twisted cubic has the graded free resolution

$$0 \to R^2(-3) \overset{M_{G'}}{\to} R^3(-2) \overset{M_G}{\to} R^1 \to R/I \to 0$$

with Betti table

	0	1	2
0 :	1	–	–
1 :	–	3	2
total :	1	3	2

Proof. Fix an arbitrary element

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

Then

$$g = \textstyle\sum_{i=1}^{s} a_i e_i \in R^s$$

is a preimage of f under M_G, that is,

$$M_G(g) = f.$$

Using $>_G$ and a reduced normal form NF' on R^s we get an expression

$$g = \textstyle\sum_{i,j} g_{i,j} \cdot \mathrm{s}(g_i, g_j) + \underbrace{\mathrm{NF}'(g, G')}_{\sum_{k=1}^{s} r_k e_k}$$

with $g_{i,j} \in R$. Then for all k with $r_k \neq 0$, it holds

$$L(r_k e_k) \notin \langle L(\mathrm{s}(g_i, g_j)) \mid i, j \text{ with } \mathrm{s}(g_i, g_j) \neq 0 \rangle .$$

By Lemma 5.10.4, for $k < j$

$$L(\mathrm{s}(g_k, g_j)) = \frac{\mathrm{lcm}(L(g_k), L(g_j))}{L(g_k)} e_k =: m_{j,k} e_k,$$

so

$$\frac{\mathrm{lcm}(L(g_k), L(g_j))}{L(g_k)} \text{ does not divide } L(r_k) \tag{5.1}$$

for all $k < j$ with $\mathrm{s}(g_k, g_j) \neq 0$.

By

$$g - \mathrm{NF}'(g, G') \in \langle G' \rangle \subset \mathrm{Syz}(G) = \ker(M_G)$$

we get

$$f = M_G(\mathrm{NF}'(g, G')) = \textstyle\sum_{k=1}^{s} r_k g_k.$$

We show that in the sum there cannot be any cancellation of lead terms: If for $k < j$ with $r_k, r_j \neq 0$ it holds

$$L(r_k g_k) = L(r_j g_j),$$

then $L(r_k g_k) = L(r_k)L(g_k) \in R^t$ is divisible by $L(g_k)$ and $L(g_j)$, hence also by $\operatorname{lcm}(L(g_k), L(g_j))$. So

$$\frac{\operatorname{lcm}(L(g_k), L(g_j))}{L(g_k)} \text{ divides } L(r_k),$$

a contradiction to Equation 5.1 (since $\mathrm{s}(g_k, g_j) \neq 0$ by assumption $L(r_k g_k) = L(r_j g_j)$).

- In the case $f \neq 0$ this proves that $L(f) = L(r_k g_k)$ for some k, and hence $L(f) \in L(G)$. So $L(U) = L(G)$, which is the first claim.
- If we take $f = 0$ then g is an arbitrary syzygy. In the case $f = 0$ the argument shows that $r_k = 0$ for all k. Hence $\mathrm{NF}'(g, G') = 0$ for all $g \in \mathrm{Syz}(G)$. This implies the second claim by the following standard Lemma 5.10.9 applied to G'.

■

Lemma 5.10.9 *Let $>$ be a global monomial ordering on R^t, NF a normal form, $U \subset R^t$ a submodule, and $G = (g_1, \ldots, g_s)$ a list of elements of U. Then it is equivalent:*

1) G is a Gröbner basis of U.

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

Proof. The implication (1) $\Rightarrow$ (2) follows from Theorem 5.8.5, since for a Gröbner basis G we get $\mathrm{NF}(f, G) = 0$ for all $f \in U$.

On the other hand let $f \in U$. By $\mathrm{NF}(f, G) = 0$ and Definition 5.8.1(3.) we obtain an expression

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

with $L(f) \geq L(a_i g_i)$ for all i. Hence, there has to be an i with $L(f) = L(a_i g_i)$, which implies $L(g_i) \mid L(f)$.

This proves that $L(U) = L(G)$. ■

Remark 5.10.10 *By Theorem 5.10.7 the conditions in the lemma are equivalent to*

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

See Theorem 2.5.2 in the ideal case.

Remark 5.10.11 (Chain condition) *Clearly it is sufficient to consider in Theorem 5.10.7 a subset of* G' *which has the same lead ideal.*

Suppose $L(g_i), L(g_j)$ *and* $L(g_l)$ *are in the same component and* $i < j < l$. *Then* $\mathrm{s}(g_i, g_j), \mathrm{s}(g_i, g_l), \mathrm{s}(g_j, g_l) \in G'$. *If*

$$L(g_j) \mid \mathrm{lcm}(L(g_i), L(g_l))$$

then $\mathrm{lcm}(L(g_i), L(g_j)) \mid \mathrm{lcm}(L(g_i), L(g_l))$. *Hence*

$$L(\mathrm{s}(g_i, g_j)) \mid L(\mathrm{s}(g_i, g_l)),$$

that is, $\mathrm{s}(g_i, g_l)$ *can be deleted from* G'.

Example 5.10.12 *In Example 5.10.8 for*

$$G = (\boldsymbol{x}_2^2 - x_1x_3,\ \boldsymbol{x}_1\boldsymbol{x}_2 - x_0x_3,\ \boldsymbol{x}_1^2 - x_0x_2)$$

we have

$$x_1x_2 \mid x_1^2x_2^2,$$

so only $\mathrm{s}(g_1, g_2)$ *and* $\mathrm{s}(g_2, g_3)$ *are needed in* G' *(as already observed above).*

5.11 Computing free resolutions

By iterating Theorem 5.10.7 we can compute free resolutions. However, we have to show that the process of computing syzygies of syzygies terminates. For this we show the Syzygy Theorem 5.2.4 by proving:

Theorem 5.11.1 *Let* $R = K[x_1, \ldots, x_n]$. *Every finitely generated* R*-module* M *has a finite free resolution*

$$0 \to R^{t_l} \xrightarrow{\phi_l} R^{t_{l-1}} \xrightarrow{\phi_{l-1}} \ldots \xrightarrow{\phi_1} R^{t_0} \to M \to 0$$

such that, if we denote the j*-th column of* ϕ_i *by* $g_{i,j}$, *it holds*

$$L(g_{i,j}) \in K[x_i, \ldots, x_n]^{t_{i-1}}$$

for all j. *The length of the resolution* $l \leq n$.

To prove the theorem, we develop an algorithm computing the desired resolution. First note that by Theorem 4.3.12, any finitely generated R-module is finitely presented.

Algorithm 5.11.1 Free resolution

Input: An R-module M with a finite presentation

$$R^{t'_1} \xrightarrow{\phi'_1} R^{t_0} \to M \to 0$$

and a monomial ordering $>$ on R^{t_0}.

Output: A finite free resolution of M as in Theorem 5.11.1.

1: Put a Gröbner basis of $\mathrm{im}(\phi'_1)$ with respect to $>$ into the columns of the matrix ϕ_1 (apply Algorithm 5.9.1).
2: $a = 1$
3: **while** $\phi_a \neq 0$ **do**
4: Applying Remark 5.9.4, replace ϕ_a by a matrix

$$\phi_a : R^{t_a} \to R^{t_{a-1}}$$

with a **minimal** Gröbner basis in its columns.
5: **Sort** the columns of $\phi_a = (g_{a,1} \mid \ldots \mid g_{a,t_a})$ such that the $L(g_{a,i})$ involving the same unit vector are in descending order with respect to lp.
6: Compute a **syzygy matrix** $\phi_{a+1} : R^{t_{a+1}} \to R^{t_a}$ with $\mathrm{im}(\phi_{a+1}) = \ker(\phi_a)$ such that the columns of ϕ_{a+1} form a Gröbner basis of $\mathrm{im}(\phi_{a+1})$ with respect to $>_{\phi_a}$ (apply Theorem 5.10.7).
7: $a = a + 1$

Proof. First observe: If the $L(g_{a,i})$ involve only $x_v, \ldots, x_n$ then the $L(\mathrm{s}(g_{a,i}, g_{a,j}))$ with respect to $>_{\phi_a}$ involve only $x_{v+1}, \ldots, x_n$.

Proof: Suppose $i < j$, and

$$L(g_{a,i}) = x_v^{\alpha_v} \cdot \ldots \cdot x_n^{\alpha_n} \cdot e_q$$
$$L(g_{a,j}) = x_v^{\beta_v} \cdot \ldots \cdot x_n^{\beta_n} \cdot e_q.$$

By Lemma 5.10.4

$$L(\mathrm{s}(g_{a,i}, g_{a,j})) = \left(\prod_{l=v}^{n} x_l^{\max\{\alpha_l, \beta_l\} - \alpha_l}\right) \cdot e_i.$$

If the leftmost nonzero entry of $\alpha - \beta$ is positive (lexicographic ordering), then $\alpha_v \geq \beta_v$, hence

$$\max\{\alpha_v, \beta_v\} - \alpha_v = 0,$$

which proves the claim.

Applying this observation inductively, there is some $a \leq n$ such that $L(\mathrm{s}(g_{a,i}, g_{a,j}))$ does not involve $x_1, \ldots, x_n$ for all $\mathrm{s}(g_{a,i}, g_{a,j}) \neq 0$.

Suppose that there is some $\mathrm{s}(g_{a,i}, g_{a,j}) \neq 0$. Then, in the above notation,

$$\alpha_i \geq \beta_i \text{ for all } i,$$

which implies that

$$L(g_{a,j}) \mid L(g_{a,i}).$$

This contradicts the assumption that the Gröbner basis $(g_{a,1}, \ldots, g_{a,t_a})$ was chosen minimal, hence ϕ_{a+1} must be zero. ■

Remark 5.11.2 *Let $U \subset R^t$ be a graded R-module and $g_1, \ldots, g_s \in U$ homogeneous of degree $\deg(g_a) = d_a$. Since monomials can only cancel if they have the same degree, also any $\mathrm{spoly}(g_i, g_j) \neq 0$ is homogeneous of some degree $d_{i,j}$. By the same argument, the equation*

$$\frac{\mathrm{lcm}(L(g_i), L(g_j))}{LT(g_i)} \cdot g_i \quad - \quad \frac{\mathrm{lcm}(L(g_i), L(g_j))}{LT(g_j)} \cdot g_j \quad - \quad \sum_{k=1}^{s} a_k g_k \quad = \quad 0$$

involves only monomials of degree $d_{i,j}$. If we now define a grading on R^s by

$$\deg(e_a) = d_a$$

also $\mathrm{s}(g_i, g_j)$ is homogeneous of degree $d_{i,j}$. If we put the $\mathrm{s}(g_i, g_j)$ into the columns of ϕ, we obtain a graded homomorphism

$$\phi : \bigoplus_{i,j} R(-d_{i,j}) \to \bigoplus_a R(-d_a).$$

Together with Theorem 5.11.1, this proves the graded Syzygy Theorem 5.5.7.

Example 5.11.3 *Let $R = K[x_0, \ldots, x_6]$. We compute a graded free resolution of R/I for the ideal I generated by the entries of*

$$\phi_1 = (x_1x_2x_5,\ x_1x_2x_6,\ x_3x_4x_6,\ x_3x_4x_7,\ x_5x_7)\,.$$

This is a graded map

$$\phi_1 : R(-3)^4 \oplus R(-2)^1 \to R^1.$$

The generators are already sorted by lexicographically. Using dp, the Buchberger test gives:

		↱ 0	↱ 0	↱ 0	↱ 0	↱ 0	↱ 0
3	$x_1x_2x_5$	$\boldsymbol{-x_6}$			$\boldsymbol{-x_7}$		
3	$x_1x_2x_6$	x_5				$\boldsymbol{-x_3x_4}$	$\boldsymbol{-x_5x_7}$
3	$x_3x_4x_6$		$\boldsymbol{-x_7}$			x_1x_2	
3	$x_3x_4x_7$		x_6	$\boldsymbol{-x_5}$			
2	x_5x_7			x_3x_4	x_1x_2		$x_1x_2x_6$
deg		4	4	4	4	5	5

In the table, we also indicate (in blue) the degrees of the generators and the syzygies, according to Remark 5.11.2.

Note, that the remaining syzygies

	↱ 0	↱ 0	↱ 0	↱ 0
$x_1x_2x_5$	$\boldsymbol{-x_3x_4x_6}$	$\boldsymbol{-x_3x_4x_7}$		
$x_1x_2x_6$			$\boldsymbol{-x_3x_4x_7}$	
$x_3x_4x_6$	$x_1x_2x_5$			$\boldsymbol{-x_7}$
$x_3x_4x_7$		$x_1x_2x_5$	$x_1x_2x_6$	
x_5x_7				x_3x_4

can be skipped, since they do not give any new lead terms. Hence

$$\phi_2 = \left(\begin{array}{c|c|c|c|c|c} \boldsymbol{-x_6} & 0 & 0 & \boldsymbol{-x_7} & 0 & 0 \\ x_5 & 0 & 0 & 0 & \boldsymbol{-x_3x_4} & \boldsymbol{-x_5x_7} \\ 0 & \boldsymbol{-x_7} & 0 & 0 & x_1x_2 & 0 \\ 0 & x_6 & \boldsymbol{-x_5} & 0 & 0 & 0 \\ 0 & 0 & x_3x_4 & x_1x_2 & 0 & x_1x_2x_6 \end{array}\right)$$

Observer that the lead terms of the syzygies do not involve x_1.

As a graded map

$$\phi_2 : R(-4)^4 \oplus R(-5)^2 \to R(-3)^4 \oplus R(-2)^1.$$

We now proceed with the next step: The syzygies $g_{2,i}$ are already sorted lexicographically by the lead monomials.

		↱ $-g_{2,6}$	↱ $-x_1x_2x_5x_7e_3 + x_1x_2x_3x_4x_6e_5$
4	$g_{2,1} = \boldsymbol{-x_6e_1} + x_5e_2$	$\boldsymbol{x_7}$	
4	$g_{2,2} = \boldsymbol{-x_7e_3} + x_5e_4$		$-x_1x_2x_5$
4	$g_{2,3} = \boldsymbol{-x_5e_4} + x_3x_4e_5$		$-x_1x_2x_6$
4	$g_{2,4} = \boldsymbol{-x_7e_1} + x_1x_2e_5$	$-x_6$	
5	$g_{2,5} = \boldsymbol{-x_3x_4e_2} + x_1x_2e_3$		$\boldsymbol{-x_5x_7}$
5	$g_{2,6} = \boldsymbol{-x_5x_7e_2} + x_1x_2x_6e_5$	1	x_3x_4
deg		5	7

The division with remainder for the second syzygy in detail:

$$\begin{aligned} &\boldsymbol{-x_1\,x_2x_5x_7e_3} + x_1x_2x_3x_4x_6e_5 \\ &= x_1x_2x_5(\boldsymbol{-x_7e_3} + x_6e_4) - \boldsymbol{x_1x_2x_5x_6e_4} + x_1x_2x_3x_4x_6e_5 \\ &= x_1x_2x_5(\boldsymbol{-x_7e_3} + x_6e_4) + x_1x_2x_6(\boldsymbol{-x_5e_4} + x_3x_4e_5) \end{aligned}$$

Hence

$$\phi_3 = \left(\begin{array}{c|c} \boldsymbol{x_7} & 0 \\ 0 & -x_1x_2x_5 \\ 0 & -x_1x_2x_6 \\ -x_6 & 0 \\ 0 & \boldsymbol{-x_5x_7} \\ 1 & x_3x_4 \end{array}\right)$$

As a graded homomorphism,

$$\phi_3 : R(-7)^1 \oplus R(-5)^1 \to R(-4)^4 \oplus R(-5)^2.$$

Since there are no syzygies between the columns of ϕ_3, we have found a free resolution

$$0 \to R^2 \xrightarrow{\phi_3} R^6 \xrightarrow{\phi_2} R^5 \xrightarrow{\phi_1} R^1 \to R/I \to 0.$$

which is graded as

$$0 \to R(-7)^1 \oplus R(-5)^1 \xrightarrow{\phi_3} R(-4)^4 \oplus R(-5)^2 \xrightarrow{\phi_2} R(-3)^4 \oplus R(-2)^1 \xrightarrow{\phi_1} R^1 \to R/I \to 0.$$

Written as a Betti diagram

	0	1	2	3
0 :	1			
1 :		1		
2 :		4	4	1
3 :			2	
4 :				1
total :	1	5	6	2

In SINGULAR *we can compute the resolution as follows:*

```
ring R = 0,(x(1..7)),dp;
ideal I = x(5)*x(7), x(3)*x(4)*x(7),
          x(3)*x(4)*x(6), x(1)*x(2)*x(6), x(1)*x(2)*x(5);
resolution r = sres(I,0);
   1          5          6          2
 R    <--   R    <--   R    <--   R
 0          1          2          3
resolution not minimized yet
```

The last output refers to the fact that we can simplify the resolution at the expense of loosing the Gröbner basis property for the columns of the ϕ_i. Essentially, the constant entry of ϕ_3 allows us to remove the last column of ϕ_2.

```
r = minres(list(r));
   1          5          5          1
 R    <--   R    <--   R    <--   R
 0          1          2          3
print(betti(r),"betti");
          0  1  2  2
 0:       1  -  -  -
 1:       -  1  -  -
 2:       -  4  4  -
 3:       -  -  1  -
 1:       -  -  -  1
 total:   1  5  5  1
```

In Exercise 5.5 we have already derived the numerical invariants of $X = V(I) \subset \mathbb{P}^6$ from this resolution. Note that the Hilbert polynomial, by Theorem 5.4.5, is an invariant of R/I, hence does not depend on the choice of the graded free resolution.

In general we proceed as follows:

Definition 5.11.4 *Let $R = K[x_0, ..., x_n]$. A free resolution*

$$0 \to F_l \xrightarrow{\phi_l} F_{l-1} \xrightarrow{\phi_{l-1}} ... \xrightarrow{\phi_1} F_0 \to M \to 0$$

*of a graded R-module M is called **minimal** if*

$$\mathrm{im}(\phi_i) \subset \langle x_0, ..., x_n \rangle \cdot F_{i-1}$$

for all i.

This means that all entries of the maps ϕ_i are contained in the ideal $\langle x_0, ..., x_n \rangle$, that is, they do not have any constant non-zero entry.

Remark 5.11.5 *One can show that the minimal free resolution is unique up to isomorphism. See Exercise 5.12.*

We can make a resolution minimal as follows:

Remark 5.11.6 *Consider a graded exact sequence*

$$... \longrightarrow R^{t_{i+1}} \xrightarrow{\phi_{i+1}} R^{t_i} \xrightarrow{\phi_i} R^{t_{i-1}} \longrightarrow ...$$

Note that a change of basis

$$\begin{tikzcd}
R^{t_{i+1}} \arrow[r, "\phi_{i+1}"] \arrow[dr] & R^{t_i} \arrow[r, "\phi_i"] \arrow[d, "T"'] & R^{t_{i-1}} \arrow[dl] \\
& R^{t_i} &
\end{tikzcd}$$

with graded $T \in \mathrm{GL}(t_i, R)$, results in a graded exact sequence

$$... \longrightarrow R^{t_{i+1}} \xrightarrow{T \circ \phi_{i+1}} R^{t_i} \xrightarrow{\phi_i \circ T^{-1}} R^{t_{i-1}} \longrightarrow ...$$

Suppose ϕ_{i+1} has a non-zero constant entry at position (a, b). We can make all other entries of column b and row a zero by graded row and column operations.

Deleting row a and column b in ϕ_{i+1}, and column a in ϕ_i, we obtain an exact sequence

$$\ldots \longrightarrow R^{t_{i+1}-1} \xrightarrow{\phi'_{i+1}} R^{t_i-1} \xrightarrow{\phi'_i} R^{t_{i-1}} \longrightarrow \ldots$$

For more than one non-zero constant entry, first do row and column reductions to ϕ_{i+1} such that $\phi_{i+1} \bmod \langle x_0, \ldots, x_n \rangle$ is of the form

$$\left(\begin{array}{ccc|c} & 0 & & 0 \\ \hline 1 & & 0 & \\ & \ddots & & 0 \\ 0 & & 1 & \end{array}\right)$$

Note that $R/\langle x_0, \ldots, x_n \rangle \cong K$ is a field. Then proceed as above. Note that, by graded operations, constant entries stay constant.

In Exercise 5.13 we turn these observations into an explicit algorithm.

Example 5.11.7 *By row operations we get*

$$T \circ \phi_3 = \left(\begin{array}{c|c} 0 & -x_3x_4x_7 \\ 0 & -x_1x_2x_5 \\ 0 & -x_1x_2x_6 \\ 0 & x_3x_4x_6 \\ 0 & -x_5x_7 \\ \hline 1 & x_3x_4 \end{array}\right)$$

with

$$T = \begin{pmatrix} 1 & & & & & -x_7 \\ & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & x_6 \\ & & & & 1 & \\ & & & & & 1 \end{pmatrix} \qquad T^{-1} = \begin{pmatrix} 1 & & & & & x_7 \\ & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & -x_6 \\ & & & & 1 & \\ & & & & & 1 \end{pmatrix}$$

Then, necessarily, in

$$\phi_2 \circ T^{-1} = \left(\begin{array}{ccccc|c} -x_6 & 0 & 0 & -x_7 & 0 & 0 \\ x_5 & 0 & 0 & 0 & -x_3x_4 & 0 \\ 0 & -x_7 & 0 & 0 & x_1x_2 & 0 \\ 0 & x_6 & -x_5 & 0 & 0 & 0 \\ 0 & 0 & x_3x_4 & x_1x_2 & 0 & 0 \end{array}\right)$$

the last column vanishes. Denoting by ϕ'_2 and ϕ'_3 the submatrices as marked above we obtain the minimal graded free resolution

$$0 \to R(-7)^1 \xrightarrow{\phi'_3} R(-4)^4 \oplus R(-5)^1 \xrightarrow{\phi'_2} R(-3)^4 \oplus R(-2)^1 \xrightarrow{\phi_1} R^1 \to R/I \to 0.$$

The Betti diagram is obtained from that of the non-minimial resolution by a diagonal cancellation between a position (i,j) and $(i-1,j+1)$:

	0	1	2	3
0 :	1			
1 :		1		
2 :		4	4	1
3 :			2	
4 :				1
total :	1	5	6	2

$\longmapsto$

	0	1	2	3
0 :	1			
1 :		1		
2 :		4	4	
3 :			1	
4 :				1
total :	1	5	5	1

Note that any diagonal cancellation does not change the Hilbert polynomial.

5.12 Exercises

Exercise 5.1 *Prove that the radical of a homogeneous ideal is homogeneous.*
Hint: Use Lemma 5.3.8 considering the homogeneous summand of maximal degree.

Exercise 5.2 *Let $R = K[x_1,\dots,x_n]$ and $I \subset R$ a homogeneous ideal. Consider $X = V(I) \subset \mathbb{P}^n(K)$ and let*

$$C(X) = V(I) \subset \mathbb{A}^{n+1}(K)$$

be the affine cone of X. Show that if $X \neq \varnothing$, then

$$I(C(X)) = I(X).$$

Hints: Recall that

$$I(C(X)) = \{f \in R \mid f(p) = 0 \ \forall p \in C(X)\}$$

and

$$I(X) = \langle f \in R \text{ homogeneous} \mid f(p) = 0 \ \forall p \in X \rangle .$$

Use Lemma 5.3.8 considering the summand of degree zero.

Exercise 5.3 *Let $K = \overline{K}$, $I \subset K[x_1,\dots,x_n]$ an ideal and $X = V(I) \subset \mathbb{A}^n(K)$. Show that the projective closure of X is the vanishing locus of the homogenization of I, that is,*

$$\mathrm{pc}(X) = V(I^{\mathrm{h}}).$$

Hint: Recall that

$$\mathrm{pc}(X) = V(I(X)^{\mathrm{h}}).$$

Prove that

$$f \in \sqrt{I} \Longrightarrow f^h \in \sqrt{I^h}$$

and use the strong Nullstellensatz.

Exercise 5.4 *Consider the affine twisted cubic curve* $C = V(I)$ *with*

$$I = \left\langle x_1^2 - x_2,\ x_1^3 - x_3 \right\rangle \subset K[x_1, x_2, x_3].$$

1) *Compute the reduced Gröbner basis of* $I^{\mathrm{h}} \subset R = K[x_0, x_1, x_2, x_3]$ *with respect to dp.*

2) *Compute a free resolution of* R/I^{h} *as an* R*-module.*

3) *Determine the dimension, degree and arithmetic genus of the projective twisted cubic* $\mathrm{pc}(C) = V(I^{\mathrm{h}}) \subset \mathbb{P}^3(K)$.

Exercise 5.5 *Compute for the projective variety* $X \subset \mathbb{P}^6$, $I = I(X) \subset R = \mathbb{C}[x_0, ..., x_6]$ *with graded free resolution*

$$0 \leftarrow R/I \leftarrow R^1 \leftarrow R(-2) \oplus R(-3)^4 \leftarrow R(-5)^1 \oplus R(-4)^4 \leftarrow R(-7)^1 \leftarrow 0.$$

1) *the Hilbert polynomial* $P_{R/I}$,

2) *dimension* $\dim(X)$, *degree* $\deg(X)$, *and arithmetic genus* $p_a(X)$, *and*

3) *the Betti table of the resolution.*

Exercise 5.6 *Let* $R = K[x_0, ..., x_n]$, *let* $p_1, ..., p_d \in \mathbb{P}^n(K)$ *be distinct points and* $I_j = I(p_j) \subset R$.

1) *Determine the Hilbert polynomial* P_{R/I_j} *of one point.*

2) *Show that the sequence*

$$\begin{array}{ccccccccc} 0 & \to & I_i \cap I_j & \to & I_i \oplus I_j & \to & I_i + I_j & \to & 0 \\ & & & & (f, g) & \mapsto & f - g & & \end{array}$$

is exact.

3) *Considering* $I = I(p_1) \cap ... \cap I(p_d)$, *prove by induction that the Hilbert polynomial of* d *distinct points satisfies*

$$P_{R/I} = d.$$

Hint: $I_i + I_j = ?$

Exercise 5.7 *Let $h_i \in \mathbb{Z}$ be a sequence of integers with $i \in \mathbb{N}$, and let*

$$h'_i = h_i - h_{i-1}$$

be its first difference. Assume that h'_i agrees for all $i \geq i_0$ with a polynomial of degree $\leq n-1$ with rational coefficients.

Show that h_i agrees with a polynomial of degree $\leq n$ with rational coefficients for all $i \geq i_0$.

Exercise 5.8 *Let M be a finitely generated graded $R = K[x_0, ..., x_n]$-module.*

1) *Consider the multiplication by x_n*

$$\begin{array}{rccc} f: & M(-1) & \to & M \\ & m & \mapsto & x_n \cdot m \end{array}$$

Show that $\operatorname{coker}(f)$ *and* $\ker(f)$ *are* finitely generated *graded $K[x_0, ..., x_{n-1}]$-modules.*

2) *Using induction on n and Exercise 5.7, deduce that the Hilbert function $H_M(i)$ agrees for large i with a polynomial of degree $\leq n$ with rational coefficients (reproving Theorem 5.4.5 by different means).*

Hints: What do you get if you multiply $\operatorname{coker}(f)$ *and* $\ker(f)$ *by x_n? Derive from f an exact sequence of graded K-vector spaces.*

Exercise 5.9 *Let $R = K[x, y]$ and*

$$f = \begin{pmatrix} xy + y^2 \\ xy^2 - 1 \\ x^2y + x^2 + xy^2 + xy \end{pmatrix}, \quad g_1 = \begin{pmatrix} y \\ 0 \\ xy + x \end{pmatrix}, \quad g_2 = \begin{pmatrix} x + 1 \\ y^2 \\ 0 \end{pmatrix} \in R^3$$

Divide f by (g_1, g_2) using the monomial ordering extending lp to R^3 by giving

1) *priority to the monomials in R,*

2) *priority to the components.*

Exercise 5.10 *Let $R = K[x_0, x_1, x_2, x_3]$ and let $>$ be the ordering dp. Consider the ideal*

$$I = \langle x_0, x_1, x_2, x_3 \rangle \subset R,$$

with Gröbner basis $G = (x_0, x_1, x_2, x_3)$.

1) *By verifying Buchberger's criterion for G, determine for the syzygy module* $\mathrm{Syz}(G)$ *a Gröbner basis with respect to* $>_G$.

2) *Iterate this to compute a graded free resolution of R/I.*

3) *Determine $P_{R/I}$.*

Exercise 5.11 *In $R = K[x_1, ..., x_5]$, consider the ideal*

$$I = \langle x_1x_3,\ x_2x_4,\ x_3x_5,\ x_4x_1,\ x_5x_2 \rangle\,,$$

and let $>$ be the ordering dp.

1) *Using the* SINGULAR *commands*

```
resolution A = res(I,0);
resolution B = sres(I,0);
```

compute graded free resolutions of R/I.

2) *From the matrices* `A[i]` *and* `B[i]` *determine the respective Betti tables.*

3) *From each of the Betti tables derive the Hilbert polynomial $P_{R/I}$. What do you observe?*

4) *For the projective variety $X = V(I) \subset \mathbb{P}^4$, compute* $\dim(X)$, $\deg(X)$, *and* $p_a(X)$.

Exercise 5.12 *Let $R = K[x_1, ..., x_n]$, and*

$$\ldots \xrightarrow{f_2} F_1 \xrightarrow{f_1} F_0 \xrightarrow{f_0} M \to 0$$
$$\ldots \xrightarrow{g_2} G_1 \xrightarrow{g_1} G_0 \xrightarrow{g_0} N \to 0$$

be exact complexes of R-modules with all F_i and G_i free.

1) *Show that every homomorphism $\alpha : M \to N$ extends to a commutative diagram*

$$\begin{tikzcd}
\ldots \arrow[r, "f_2"] & F_1 \arrow[r, "f_1"] \arrow[d, "\alpha_1"'] & F_0 \arrow[r, "f_0"] \arrow[d, "\alpha_0"'] & M \arrow[r] \arrow[d, "\alpha"'] & 0 \\
\ldots \arrow[r, "g_2"] & G_1 \arrow[r, "g_1"] & G_0 \arrow[r, "g_0"] & N \arrow[r] & 0
\end{tikzcd}$$

with homomorphisms $\alpha_i : F_i \to G_i$.

2) *The homomorphisms α_i are unique up to homotopy, that is, if $\alpha_i' : F_i \to G_i$ also extend α then there are $h_i : F_i \to G_{i+1}$ with*

$$\alpha_i - \alpha_i' = h_{i-1} \circ f_i + g_{i+1} \circ h_i$$

for all i.

3) *Considering two minimal free resolutions*

$$\begin{aligned} \ldots &\xrightarrow{f_2} F_1 \xrightarrow{f_1} F_0 \xrightarrow{f_0} M \to 0 \\ \ldots &\xrightarrow{g_2} G_1 \xrightarrow{g_1} G_0 \xrightarrow{g_0} M \to 0 \end{aligned}$$

of a graded module M and $f = \mathrm{id}_M$, show that all α_i are isomorphisms.

Exercise 5.13 *Describe an algorithm to transform a graded free resolution into a minimal one.*

Exercise 5.14 *Let $R = K[x_0, \ldots, x_6]$ and*

$$I = \langle x_0x_1x_4,\ x_0x_3x_4,\ x_1x_2x_5,\ x_1x_4x_5,\ x_0x_3x_6,\ x_2x_3x_6,\ x_2x_5x_6 \rangle$$

1) *Using Algorithm 5.11.1, compute a graded free resolution of R/I.*

2) *Determine from this a minimal free resolution.*

3) *For both resolutions, write down the Betti tables and mark the diagonal cancellations.*

4) *Compute dimension, degree and genus of $V(I) \subset \mathbb{P}^6$.*

6

Computing with modules

6.1 Overview

Based on Theorem 5.10.7 to compute the syzygy module of a Gröbner basis, we can derive algorithms to compute with finitely presented modules over the polynomial ring $R = K[x_1, ..., x_n]$. We start out with an algorithm computing generators of the kernel of an arbitrary matrix over R. We can apply this, for example, to derive an ideal intersection algorithm, see Exercise 6.1. The second basic task is to find a presentation of the subquotient of two submodules of R^t, which are given by generators. Based on these basic tasks, we will derive an algorithm for computing the module $\mathrm{Hom}_R(M, N)$ of homomorphisms $M \to N$ between two R-modules M and N. This is a fundamental algorithm for many tasks in algebraic geometry and commutative algebra. One application, we will have a quick look at, are deformations of algebraic varieties. Here, given a variety $X = V(I)$ by an ideal $I \subset R$, one can obtain from $\mathrm{Hom}_R(I, R/I)$ information about deforming X in a way which keeps key invariants like the Hilbert polynomial constant. Figure 6.1 shows the deformation of the union of three lines $V(x_0x_1x_2) \subset \mathbb{P}^2$ into an elliptic curve, that is, a smooth plane cubic.

6.2 Computing kernels

Theorem 5.10.7 only provides an algorithm to compute the kernel of a matrix $(g_1 \mid ... \mid g_a) \in R^{t\times a}$ whose columns $g_i \in R^t$ form a Gröbner basis with respect to some ordering. However, we can easily derive an algorithm for the more general task of computing the kernel (syzygy module) of an arbitrary matrix (that is, homomorphism of free R-modules of finite rank).

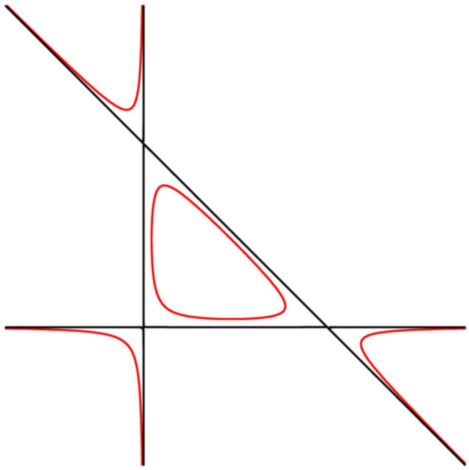

Figure 6.1: Deformation of three lines into an elliptic curve (real picture).

Algorithm 6.2.1 Kernel

Input: Matrix $M = (g_1 \mid \ldots \mid g_a) \in R^{t \times a}$.
Output: A matrix S with $\mathrm{im}(S) = \ker(M)$.

1: Compute a Gröbner basis $g_1, \ldots, g_a, g_{a+1}, \ldots, g_{a+b}$.
2: From the syzygies $\mathrm{s}(g_i, g_j)$ build a matrix

$$T = \left(\begin{array}{ccc|c} & * & & * \\ \hline 1 & & * & \\ & \ddots & & * \\ 0 & & 1 & \end{array}\right) \in R^{(a+b)\times s}$$

that is, put the Buchberger tests leading to a new Gröbner basis element first.
3: Apply column operations to T to obtain

$$T' = \left(\begin{array}{ccc|c} & * & & S \\ \hline 1 & & * & \\ & \ddots & & 0 \\ 0 & & 1 & \end{array}\right) \in R^{(a+b)\times s}$$

4: Return S.

Proof. By Theorem 5.10.7, $\ker(g_1, \ldots, g_{a+b}) = \mathrm{im}(T)$. Since the first a columns of T' are linearly independent, any syzygy which involves only $g_1, \ldots, g_a$ is a linear combination of the last b columns.

■

Example 6.2.1 *In Example 5.11.3, by column operations*

$$\left(\begin{array}{c|c} x_7 & 0 \\ 0 & -x_1x_2x_5 \\ 0 & -x_1x_2x_6 \\ -x_6 & 0 \\ 0 & -x_5x_7 \\ \hline 1 & x_3x_4 \end{array}\right) \mapsto \left(\begin{array}{c|c} x_7 & -x_3x_4x_7 \\ 0 & -x_1x_2x_5 \\ 0 & -x_1x_2x_6 \\ -x_6 & x_3x_4x_6 \\ 0 & -x_5x_7 \\ \hline 1 & 0 \end{array}\right)$$

hence

$$\mathrm{Syz}\begin{pmatrix} -x_6 & 0 & 0 & -x_7 & 0 \\ x_5 & 0 & 0 & 0 & -x_3x_4 \\ 0 & -x_7 & 0 & 0 & x_1x_2 \\ 0 & x_6 & -x_5 & 0 & 0 \\ 0 & 0 & x_3x_4 & x_1x_2 & 0 \end{pmatrix} = \left\langle \begin{pmatrix} -x_3x_4x_7 \\ -x_1x_2x_5 \\ -x_1x_2x_6 \\ x_3x_4x_6 \\ -x_5x_7 \end{pmatrix} \right\rangle$$

In Singular *we can compute a syzygy matrix using the command* `syz`*:*

```
ring R = 0, (x(1..7)),dp;
matrix M[5][5] = -x(6), 0, 0, -x(7), 0,
x(5), 0, 0, 0, -x(3)*x(4), 0,
0, -x(7), 0, 0, x(1)*x(2),
0, x(6), -x(5), 0, 0,
0, 0, x(3)*x(4), x(1)*x(2), 0;
print(syz(M));
x(3)*x(4)*x(7),
x(1)*x(2)*x(5),
x(1)*x(2)*x(6),
-x(3)*x(4)*x(6),
x(5)*x(7)
```

For another example, see Exercise 6.2.

6.3 Computing subquotients

Definition 6.3.1 *Given two matrices $A \in R^{t\times a}$ and $B \in R^{t\times b}$ the* ***subquotient*** *with* ***generators*** *A and* ***relations*** *B is the R-module*

$$\mathrm{subquot}(A,B) = \frac{\mathrm{im}(A)+\mathrm{im}(B)}{\mathrm{im}(B)}.$$

Here we add $\mathrm{im}(B)$, before dividing it out again, to make the quotient well-defined.

Remark 6.3.2 *In particular,*

$$\begin{aligned}\mathrm{im}(A) &= \mathrm{subquot}(A, 0)\\ \mathrm{coker}(B) &= \mathrm{subquot}(E_t, B)\end{aligned}$$

where E_t denotes the $t \times t$ unit matrix.

The following algorithm determines a presentation

$$R^c \xrightarrow{C} R^a \to \mathrm{subquot}(A, B) \to 0$$

of the subquotient.

Algorithm 6.3.1 Subquotient

Input: $A \in R^{t\times a}$ and $B \in R^{t\times b}$.
Output: $C \in R^{a\times c}$ with

$$\mathrm{subquot}(A, B) \cong \mathrm{coker}(C)$$

1: By computing a syzygy matrix of $\left(\begin{array}{c|c} A & B \end{array}\right) \in R^{t\times(a+b)}$ determine $C \in R^{a\times c}$ and $D \in R^{b\times c}$ with

$$\ker\left(\begin{array}{c|c} A & B \end{array}\right) = \mathrm{im}\left(\frac{C}{D}\right)$$

2: Return C.

Proof. We have a presentation

$$R^c \xrightarrow{\left(\begin{array}{c} C \\ \hline D \end{array}\right)} R^{a+b} \xrightarrow{\left(\begin{array}{c|c} A & B \end{array}\right)} \mathrm{im}(A) + \mathrm{im}(B) \to 0$$

Dividing by $\mathrm{im}(B)$, yields an exact sequence

$$R^c \xrightarrow{C} R^a \xrightarrow{\bar{A}} \frac{\mathrm{im}(A) + \mathrm{im}(B)}{\mathrm{im}(B)} \to 0$$

where $\bar{A}$ denotes the map

$$\begin{array}{rccc} \bar{A}: & R^a & \to & R^t/\mathrm{im}(B) \\ & e_i & \mapsto & Ae_i + \mathrm{im}(B) \end{array}$$

induced by A. ■

See also Exercise 6.3.

Example 6.3.3 *For*

$$A = (x, y) \qquad B = (x^2, y^2)$$

we have

$$\ker(x, y, x^2, y^2) = \operatorname{im}\begin{pmatrix} -y & x & 0 \\ x & 0 & y \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

hence

$$\operatorname{subquot}(A, B) \cong \operatorname{coker}(C)$$

with

$$C = \begin{pmatrix} -y & x & 0 \\ x & 0 & y \end{pmatrix}$$

The presentation sequence of $\operatorname{subquot}(A, B)$ *is*

$$\begin{array}{ccccccc} R^3 & \xrightarrow{C} & R^2 & \longrightarrow & \langle x, y\rangle / \langle x^2, y^2\rangle & \longrightarrow & 0 \\ & & e_1 & \longmapsto & \bar{x} & & \\ & & e_2 & \longmapsto & \bar{y} & & \end{array}$$

In Singular *we can obtain* C *by applying the* `modulo` *command to the images of* A *and* B*:*

```
ring R=0,(x,y),dp;
module A = x,y;
module B = x2,y2;
print(modulo(A,B));
0,x,-y,
y,0,x
```

Note that the sorting of the columns of C *is irrelevant.*

Remark 6.3.4 *Suppose* M *is a finitely presented module*

$$R^c \xrightarrow{C} R^a \xrightarrow{\pi} M \to 0$$

and $\pi(e_i) = \overline{A \cdot e_i}$*. Then*

$$M = \operatorname{subquot}(A, B) \cong \operatorname{coker}(C).$$

Writing M *as the subquotient of* A *and* B*, keeps track of the generators of* M*, that is, of the map* π*. Writing* M *as the cokernel of* C *looses the information about* π*.*

6.4 Hom and the Hilbert scheme

Definition 6.4.1 *For R-modules M and N let*

$$\mathrm{Hom}_R(M,N) = \{f : M \to N \mid f \text{ is an } R\text{-module homomorphism}\}$$

be the ***module of homomorphisms****. It has the structure of an R-module by*

$$(f+g)(m) = f(m) + g(m)$$
$$(r \cdot f)(m) = r \cdot f(m)$$

for $m \in M$ and $r \in R$.

Before discussing how to compute Hom by Gröbner basis techniques (specifically, Algorithms 6.2.1 and 6.3.1) we give a sketch of an important application in algebraic geometry:

It is based on the key fact that algebraic subsets of $\mathbb{P}^n_K$ are again parametrized by an algebraic set. More precisely, we have to consider schemes $\mathrm{Proj}(R/I)$, which corresponds to homogeneous ideals I, which are not necessarily radical. In general, the remainder of this subsection is intended to give you some impression. To be completely precise, we would need much more technical background.

Example 6.4.2 *Consider the set $\mathcal{H}_{n,d}$ of hypersurfaces in $\mathbb{P}^n_K$ of degree d. Every element $X \in \mathcal{H}_{n,d}$ is of the form*

$$X = V(I)$$

where $I = \langle f \rangle$ and

$$f = \sum_{|\alpha|=d} c_\alpha x^\alpha \in K[x_0, \ldots, x_n]$$

is homogeneous of degree $\deg(f) = d$. So X corresponds to an element

$$(c_\alpha)_\alpha \in \mathbb{P}^{m-1}_K$$

where m is the dimension of the vector space $K[x_0, \ldots, x_n]_d$ of polynomials of degree d. Hence

$$\mathcal{H}_{n,d} \cong \mathbb{P}^{m-1}_K.$$

All elements $X \in \mathcal{H}_{n,d}$ have the same Hilbert polynomial

$$P_X(t) := P_{R/I}(t) = \binom{t+n}{n} - \binom{t-d+n}{n}.$$

It turns out that this idea is the right strategy in general:

Definition 6.4.3 *The* ***Hilbert scheme*** $\mathcal{H}_n$ *is the set all subschemes of* $\mathbb{P}^n_K$.

Theorem 6.4.4 *The Hilbert scheme*

$$\mathcal{H}_n = \bigcup_{P \in K[t]} \mathcal{H}_{n,P}$$

is the disjoint union of projective schemes $\mathcal{H}_{n,P}$ *such that* $P_X = P$ *for all* $X \in \mathcal{H}_{n,P}$. *For fixed degree of* X, *there are only finitely many* P *with* $\mathcal{H}_{n,P} \neq \emptyset$.

We cannot prove this here. In general, the Hilbert scheme is also difficult to construct. However, the following theorem (which we also cannot prove here) allows us to describe $\mathcal{H}_{n,P}$ locally at a point X by computing a module of homomorphisms. As we will see in the next section, this is a task which can easily be handled algorithmically.

Theorem 6.4.5 *Let* $X \in \mathcal{H}_{n,P}$ *given by the homogeneous ideal* $I \subset K[x_0, ..., x_n]$. *The tangent space of* $\mathcal{H}_{n,P}$ *at* X *is*

$$\mathrm{Hom}(I, R/I)_0$$

the K*-vector space of graded homomorphisms* $I \to R/I$.

The elements of $\mathrm{Hom}(I, R/I)_0$ *are called the homogeneous* ***first order deformations*** *of* I.

Recall that the tangent space gives a linear approximation of a variety at a given point. See Figure 6.2 for a tangent space of a conic. Keep in mind, that in Theorem 6.4.5 we are not talking

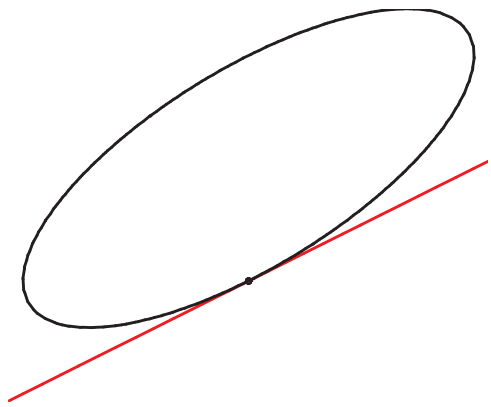

Figure 6.2: A tangent to a conic

about a tangent space of X, but rather about the tangent space of the space of all possible X at a specific X.

Remark 6.4.6 *Suppose X is defined by $I = \mathrm{im}(g_1, ..., g_s)$ and*

$$\mathrm{Hom}(I, R/I)_0 = \langle \phi_1, ..., \phi_m \rangle .$$

Then for parameters t, the ideal

$$\left\langle g_i + \sum_{j=1}^m t_j \cdot \phi_j(g_i) \mid i = 1, ..., s \right\rangle$$

determines a deformation X_t of X. However $P_{X_t} = P_X$ is only true modulo appropriate higher order terms in $\langle t_0, ..., t_m \rangle^2$ (in analogy to a Taylor series). Moreover, there can be algebraic relations between the t_j.

Example 6.4.7 *In the setup of Example 6.4.2, consider the hypersurface $I = \langle x_0 \cdot ... \cdot x_n \rangle$. Then a basis of $\mathrm{Hom}(I, R/I)_0$ is given by the homomorphisms*

$$\begin{array}{rccc} \phi_\alpha : & I & \to & R/I \\ & x_0 \cdot ... \cdot x_n & \mapsto & x^\alpha \end{array}$$

where $|\alpha| = d$ and $\alpha \neq (1, ..., 1)$.

To do some examples, we first develop an algorithm to compute Hom in general.

6.5 Computing Hom

First note that

$$\mathrm{Hom}_R(R^s, R^t) \cong R^{t \cdot s}$$

is a free module. We choose the identification of matrices and vectors

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,s} \\ \vdots & & \vdots \\ a_{t,1} & \cdots & a_{t,s} \end{pmatrix} \mapsto \begin{pmatrix} a_{1,1} \\ \vdots \\ a_{t,1} \\ \hline \vdots \\ a_{t,s} \end{pmatrix}$$

For those who know about the tensor product: Denote by a star the dual vector respectively module. We have $\mathrm{Hom}_R(R^s, R^t) \cong R^t \otimes (R^s)^*$, where $A = (a_{i,j})$ is identified with $\sum_{i=1}^t \sum_{j=1}^s a_{i,j} \cdot e_i \otimes e_j^*$. Hence, the above identification amounts to an ordering of the basis vectors $e_i \otimes e_j^*$ of the tensor product.

Algorithm 6.5.1 Hom

Input: R-modules M and N given by presentations

$$R^{s_1} \xrightarrow{f_1} R^{s_0} \to M \to 0$$
$$R^{t_1} \xrightarrow{g_1} R^{t_0} \to N \to 0$$

Output: $\mathrm{Hom}_R(M, N)$ as a subquotient.

1: By Algorithm 6.2.1, compute g_2 such that

$$R^{t_2} \xrightarrow{g_2} R^{t_1} \xrightarrow{g_1} R^{t_0} \to N \to 0$$

is exact.

2: Construct the $(s_1 t_0) \times (s_0 t_0 + s_1 t_1)$ matrix

$$\begin{array}{ccc} \mathrm{Hom}\,(R^{s_0}, R^{t_0}) \oplus \mathrm{Hom}\,(R^{s_1}, R^{t_1}) & \xrightarrow{\delta} & \mathrm{Hom}\,(R^{s_1}, R^{t_0}) \\ (A,\ B) & \mapsto & A \cdot f_1 - g_1 \cdot B \end{array}$$

3: By Algorithm 6.2.1 compute a matrix γ with $\ker(\delta) = \mathrm{im}(\gamma)$.

4: Construct the $(s_0 t_0 + s_1 t_1) \times (s_0 t_1 + s_1 t_2)$ matrix

$$\begin{array}{ccc} \mathrm{Hom}\,(R^{s_0}, R^{t_1}) \oplus \mathrm{Hom}\,(R^{s_1}, R^{t_2}) & \xrightarrow{\rho} & \mathrm{Hom}\,(R^{s_0}, R^{t_0}) \oplus \mathrm{Hom}\,(R^{s_1}, R^{t_1}) \\ (C,\ D) & \mapsto & (g_1 \cdot C,\ C \cdot f_1 - g_2 \cdot D) \end{array}$$

5: Return $\mathrm{subquot}(\gamma, \rho)$.

For the proof of correctness we make the following observations:

Remark 6.5.1 *First note that $\delta \cdot \rho = 0$, so*

$$\mathrm{subquot}(\gamma, \rho) = \ker(\delta)/\mathrm{im}(\rho).$$

Lemma 6.5.2 *The map*

$$\begin{array}{ccc} \pi : \ker(\delta) & \to & \mathrm{Hom}_R(M, N) \\ (A,\ B) & \mapsto & \overline{A} = \left(\overline{e_i} \mapsto \overline{A \cdot e_i}\right) \end{array}$$

is well-defined and surjective.

Proof. Let $(A, B) \in \ker(\delta)$. Then we have a commutative diagram

$$\begin{tikzcd} R^{s_1} \arrow[r, "f_1"] \arrow[d, "B"'] & R^{s_0} \arrow[r] \arrow[d, "A"'] & M \arrow[r] \arrow[d, "\bar{A}"'] & 0 \\ R^{t_1} \arrow[r, "g_1"] & R^{t_0} \arrow[r] & N \arrow[r] & 0 \end{tikzcd}$$

where $\overline{A}$ is well defined: Suppose $v \in \operatorname{im}(f_1)$. So $v = f_1 w$ with $w \in R^{s_1}$, hence $A \cdot v = g_1 B w \in \operatorname{im}(g_1)$.

Moreover, any $f : M \to N$, $\overline{e_j} \mapsto \sum_i a_{ij}\overline{e_i}$ is induced by $A : R^{s_0} \to R^{t_0}$, $e_j \mapsto \sum_i a_{ij} e_i$, and

$$\operatorname{im}(A \cdot f_1) \subset \operatorname{im}(g_1).$$

Hence there are b_{ij} with

$$A \cdot f_1 \cdot e_j = \sum_i b_{ij} e_i$$

and we set $B = (b_{ij})$. ■

For correctness of the algorithm it remains to prove:

Lemma 6.5.3 $\ker(\pi) = \operatorname{im}(\rho)$.

Proof. We can collect all maps in the diagram

$$\begin{tikzcd}
 & R^{s_1} \arrow[r, "f_1"] \arrow[dl, "D"'] \arrow[d, "B"] & R^{s_0} \arrow[r] \arrow[dl, "C"'] \arrow[d, "A"] & M \arrow[r] \arrow[d, "\bar{A}"] & 0 \\
R^{t_2} \arrow[r, "g_2"] & R^{t_1} \arrow[r, "g_1"] & R^{t_0} \arrow[r] & N \arrow[r] & 0
\end{tikzcd}$$

First note that $(A, B) \in \ker(\pi)$ if and only if $\operatorname{im}(A) \subset \operatorname{im}(g_1)$ and $A \cdot f_1 = g_1 \cdot B$.

- If $(A, B) = (g_1 \cdot C,\ C \cdot f_1 - g_2 \cdot D) \in \operatorname{im}(\rho)$, then

  $$A \cdot f_1 = g_1 \cdot C \cdot f_1 = g_1 \cdot (C \cdot f_1 - g_2 \cdot D) = g_1 \cdot B$$

  and $\operatorname{im}(A) = \operatorname{im}(g_1 \cdot C) \subset \operatorname{im}(g_1)$.

- On the other hand, let $(A, B) \in \ker(\pi)$. Since $\operatorname{im}(A) \subset \operatorname{im}(g_1)$ there is $C \in \operatorname{Hom}_R(R^{s_0}, R^{t_1})$ with $A = g_1 \cdot C$. Moreover, by $A \cdot f_1 = g_1 \cdot B$, we have

  $$g_1 \cdot (C \cdot f_1 - B) = A \cdot f_1 - g_1 \cdot B = 0,$$

  that is,

  $$\operatorname{im}(C \cdot f_1 - B) \subset \ker(g_1) = \operatorname{im}(g_2).$$

  Hence there is $D \in \operatorname{Hom}_R(R^{s_1}, R^{t_2})$ with

  $$g_2 \cdot D = C \cdot f_1 - B.$$

■

Example 6.5.4 *For $X = V(I) \subset \mathbb{P}^5$ defined by*

$$I = \mathrm{im}(g_1) \subset R^1$$
$$g_1 = (x_0x_1, x_2x_3, x_4x_5)$$

we have a minimal graded free resolution

$$0 \to R(-6)^1 \to R(-4)^3 \xrightarrow{g_2} R(-2)^3 \xrightarrow{g_1} R^1 \to R/I \to 0$$

with

$$g_2 = \begin{pmatrix} -x_2x_3 & -x_4x_5 & 0 \\ x_0x_1 & 0 & -x_4x_5 \\ 0 & x_0x_1 & -x_2x_3 \end{pmatrix}$$

Hence

$$P_X(t) = 4t^2 + 2,$$

so X is a genus 1 surface of degree 8. It is an example of a so called ***K3-surface****, which is the two-dimensional analogue of an elliptic curve.*

Our goal is to compute the tangent space $\mathrm{Hom}(I, R/I)_0$ of $\mathcal{H}_{5,4t^2+2}$ at X.

We use the opportunity to demonstrate one more computer algebra system: MACAULAY2 *has a similar functionality as* SINGULAR. *It is very well suited for the type of calculations required in Algorithm 6.5.* MACAULAY2 *(like* SINGULAR *and* GAP*) has a built-in function for computing Hom:*

```
i1:  R = QQ[x_0..x_5];
i2:  I = ideal(x_0*x_1,x_2*x_3,x_4*x_5)
o2:  ideal ( x_0x_1 x_2x_3 x_4x_5 )
o2:  Ideal of R
```

A matrix with the generators of I:

```
i3:  g1 = gens I
o3:  | x_0x_1 x_2x_3 x_4x_5 |
o3:  Matrix R^1 <--- R^3
```

To consider I as a submodule of R^1 do:

```
i4:  M = image g1
o4:  image | x_0x_1 x_2x_3 x_4x_5 |
o4:  R-module, submodule of R^1
```

To consider R/I as a submodule of R^1 do:

```
i5:  N= coker g1
o5:  cokernel | x_0x_1 x_2x_3 x_4x_5 |
o5:  R-module, quotient of R^1
```

Construct $\mathrm{Hom}_R(I, R/I)$*:*

```
i6:  H = Hom(M, N)
o6:  cokernel |  x_0x_1 x_2x_3 x_4x_5  0      0      0      0      0      0      |
              |  0      0      0      x_0x_1 x_2x_3 x_4x_5 0      0      0      |
              |  0      0      0      0      0      0      x_0x_1 x_2x_3 x_4x_5 |
```

A matrix with a K*-vectorspace basis in degree* 0 *in its columns:*

```
i7:  T = basis(0,H);
```

The K*-vector space dimension of* $\mathrm{Hom}_R(I, R/I)_0$*:*

```
i8:  rank source T
o8:  54
```

For example the 11*th basis vector (indexing starts at* 0*):*

```
i9:  T_{10}
o9:  |  x_2^2  |
     |  0      |
     |  0      |
o9:  Matrix
```

We can interpret a given basis vector as a homomorphism, for example:

```
i10:  homomorphism T_{10}
o10:  | x_2^2 0 0 |
o10:  Matrix
```

This homomorphism maps the generators of I *to* R/I *as follows:*

$$x_0x_1 \mapsto \bar{x}_2^2, \quad x_2x_3 \mapsto 0, \quad x_4x_5 \mapsto 0$$

From `o6` *it is clear that a basis of* $\mathrm{Hom}_R(I, R/I)_0$ *is given by the* $54 = 18 + 18 + 18$ *homomorphisms*

$$\begin{aligned} &x_0x_1 \mapsto \bar{x}^\alpha, \quad x_2x_3 \mapsto 0, \quad x_4x_5 \mapsto 0, \\ &x_0x_1 \mapsto 0, \quad x_2x_3 \mapsto \bar{x}^\alpha, \quad x_4x_5 \mapsto 0 \\ &x_0x_1 \mapsto 0, \quad x_2x_3 \mapsto 0, \quad x_4x_5 \mapsto \bar{x}^\alpha \end{aligned}$$

where $\deg(x^\alpha) = 2$ *and* $x^\alpha \neq x_0x_1, x_2x_3, x_4x_5$.

Example 6.5.5 *For* $X = V(I) \subset \mathbb{P}^2$ *defined by*

$$\begin{aligned} I &= \mathrm{im}(g_1) \\ g_1 &= (x_0x_1,\ x_0x_2,\ x_1x_2) \end{aligned}$$

we have a minimal graded free resolution

$$0 \to R(-3)^2 \xrightarrow{g_2} R(-2)^3 \xrightarrow{g_1} R^1 \to R/I \to 0$$

with

$$g_2 = \begin{pmatrix} -x_2 & 0 \\ x_1 & -x_1 \\ 0 & x_0 \end{pmatrix}$$

Hence

$$P_X(t) = 3,$$

so X is the union of 3 points, indeed,

$$I = \langle x_0, x_1 \rangle \cap \langle x_0, x_2 \rangle \cap \langle x_1, x_2 \rangle .$$

We follow Algorithm 6.5, step-by-step, to obtain $\mathrm{Hom}_R(I, R/I)$. *The usual diagram reads*

$$\begin{tikzcd}
 & R(-3)^2 \arrow[r, "g_2"] \arrow[dl, "D"'] \arrow[d, "B"] & R(-2)^3 \arrow[r, "g_1"] \arrow[dl, "C"'] \arrow[d, "A"] & I \arrow[r] \arrow[d, "\bar{A}"] & 0 \\
R(-3)^2 \arrow[r, "g_2"] & R(-2)^3 \arrow[r, "g_1"] & R^1 \arrow[r] & R/I \arrow[r] & 0
\end{tikzcd}$$

Hence

$$\begin{aligned}
A &\in \mathrm{Hom}_R\left(R(-2)^3, R^1\right) && \cong R(2)^3 \\
B &\in \mathrm{Hom}_R\left(R(-3)^2, R(-2)^3\right) && \cong R(1)^6 \\
\delta(A,B) = A \cdot g_2 - g_1 \cdot B &\in \mathrm{Hom}_R\left(R(-3)^2, R^1\right) && \cong R(3)^2
\end{aligned}$$

and

$$\delta : R(2)^3 \oplus R(1)^6 \to R(3)^2$$

is represented by

$$\delta = \begin{array}{c}
\begin{array}{ccc|ccccccc} a_{11} & a_{12} & a_{13} & b_{11} & b_{21} & b_{31} & b_{12} & b_{22} & b_{32} \end{array} \\
\left(\begin{array}{ccc||ccccccc}
-x_2 & x_1 & 0 & -x_0x_1 & -x_0x_2 & -x_1x_2 & 0 & 0 & 0 \\
0 & -x_1 & x_0 & 0 & 0 & 0 & -x_0x_1 & -x_0x_2 & -x_1x_2
\end{array}\right)
\end{array}$$

To obtain the first block, compute

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \end{pmatrix} \cdot g_2 = \begin{pmatrix} -a_{11}x_2 + a_{12}x_1 & -a_{12}x_1 + a_{13}x_0 \end{pmatrix}$$

set one $a_{i,j} = 1$ and all others zero and use again the above identification of matrices with vectors. For the second block, compute

$$g_1 \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \\ b_{31} & b_{32} \end{pmatrix} = \begin{pmatrix} x_0x_1b_{11} + x_0x_2b_{21} + x_1x_2b_{31} & x_0x_1b_{12} + x_0x_2b_{22} + x_1x_2b_{32} \end{pmatrix}$$

and proceed in the same way. If you know about the tensor product, the blocks are tensor products of matrices.

Turning to ρ,

$$C \in \mathrm{Hom}_R\left(R(-2)^3, R(-2)^3\right) \cong R^9$$
$$D \in \mathrm{Hom}_R\left(R(-3)^2, R(-2)^3\right) \cong R^4$$

and

$$\rho(C, D) = (g_1 \cdot C, C \cdot g_2 - g_2 \cdot D)$$

is in the direct sum of

$$\mathrm{Hom}_R\left(R(-2)^3, R^1\right) \cong R(2)^3$$

and

$$\mathrm{Hom}_R\left(R(-3)^2, R(-2)^3\right) \cong R(1)^6.$$

Hence

$$\rho : R^9 \oplus R^4 \to R(2)^3 \oplus R(1)^6$$

and, in the same way as above, one observes that

$$\rho = \begin{array}{c} \\ A \\ \\ B \\ \end{array} \begin{array}{c} \begin{array}{ccccc} & C & & & D \end{array} \\ \left(\begin{array}{c|c|c||c|c} g_1 & 0 & 0 & 0 & 0 \\ \hline 0 & g_1 & 0 & 0 & 0 \\ \hline 0 & 0 & g_1 & 0 & 0 \\ \hline\hline -x_2E_3 & x_1E_3 & 0 & -g_2 & 0 \\ \hline 0 & -x_1E_3 & x_0E_3 & 0 & -g_2 \end{array}\right) \end{array}$$

where E_3 *denotes the* 3×3 *unit matrix.*
To compute $\ker(\delta)/\mathrm{im}(\rho)$ *by Algorithms 6.2.1 and 6.3.1, we continue in* MACAULAY2*:*

```
i1:  R = QQ[x_0..x_2];
i2:  I = ideal(x_0*x_1,x_0*x_2,x_1*x_2)
o2:  ideal ( x_0x_1 x_0x_2 x_1x_2 )
o2:  Ideal of R
```

Compute a graded minimal free resolution:

```
i3:  cc = res I;
i4:  betti cc
            0  1  2
o4: total:  1  3  2
         0: 1  .  .
         1: .  3  2
i5:  g1 = cc.dd_1
o5:  | x_0x_1 x_0x_2 x_1x_2 |
o5:  Matrix R^1 <--- R^3
i6:  g2 = cc.dd_2
```

```
o6:  {2} |  -x_2  0     |
     {2} |   x_1  -x_1  |
     {2} |  0     x_0   |
o6:  Matrix R^3<--- R^2
```

We form the matrices δ and ρ:

```
i7:  T0 = target g1; T1 = source g1; T2 = source g2;
i8:  S0 = source g1; S1 = source g2;
i9:  M0 = Hom(S1,T0);
i10:  M1 = Hom(S0, T0) ++ Hom(S1, T1);
i11:  M2 = Hom(S0, T1) ++ Hom(S1, T2);
i12:  degrees M0
o12:  {{-3},{-3}}
i13:  degrees M1
o13:  {{-2},{-2},{-2},{-1},{-1},{-1},{-1},{-1},{-1}}
i14:  degrees M2
o14:  {{0},{0},{0},{0},{0},{0},{0},{0},{0},{0},{0},{0},{0}}
i15:  delta11 = transpose g2;
i16:  delta12 = -id_(R^2)**g1;
i17:  delta = map(M0,M1,matrix {{delta11, delta12}});
o17:  {-3} |  x_2   x_1   0     -x_0x_1  -x_0x_2  -x_1x_2  0        0        0        |
      {-3} |  0     -x_1  x_0   0        0        0        -x_0x_1  -x_0x_2  -x_1x_2  |

i18:  rho11 = id_(R^3)**g1;
i19:  rho21 = (transpose g2)**id_(R^3);
i20:  rho12 = map(R^3,R^4,0);
i21:  rho22 = -(id_(R^2))**g2;
i22:  rho = map(M1,M2,matrix{{rho11,rho12},{rho21,rho22}});
o22:  {-2} |  x_0x_1  x_0x_2  x_1x_2  0       0       0       0       0       0       0       0       0       0     |
      {-2} |  0       0       0       x_0x_1  x_0x_2  x_1x_2  0       0       0       0       0       0       0     |
      {-2} |  0       0       0       0       0       0       x_0x_1  x_0x_2  x_1x_2  0       0       0       0     |
      {-1} |  -x_2    0       0       x_1     0       0       0       0       0       x_2     0       0       0     |
      {-1} |  0       -x_2    0       0       x_1     0       0       0       0       -x_1    x_1     0       0     |
      {-1} |  0       0       -x_2    0       0       x_1     0       0       0       0       -x_0    0       0     |
      {-1} |  0       0       0       -x_1    0       0       x_0     0       0       0       0       x_2     0     |
      {-1} |  0       0       0       0       -x_1    0       0       x_0     0       0       0       -x_1    x_1   |
      {-1} |  0       0       0       0       0       -x_1    0       0       x_0     0       0       0       -x_0  |
```

Now compute the Hom-module as a subquotient:

```
i23:  H =(ker delta)/(image rho);
```

Basis in degree 0*:*

```
i24:  B = basis(0,H)
o24:  {-1} |  x_0  0    0    0    0    0    |
      {-1} |  0    x_1  0    0    0    0    |
      {-1} |  0    0    x_0  0    0    0    |
      {-1} |  0    0    0    x_1  0    0    |
      {-1} |  0    0    0    0    x_2  0    |
      {-1} |  0    0    0    0    0    x_2  |
       {0} |  0    0    0    0    0    0    |
```

To obtain the homomorphisms, we consider for each column, the corresponding linear combination of the generators of H:

```
i25:  (gens H) * (matrix entries B)
o25:  {-2} |  x_0^2   x_1^2   0       0       0       0       |
      {-2} |  0       0       x_0^2   0       0       x_2^2   |
      {-2} |  0       0       0       x_1^2   x_2^2   0       |
      {-1} |  0       0       x_0     0       0       0       |
      {-1} |  -x_0    0       0       0       x_1     0       |
      {-1} |  0       -x_1    0       0       0       x_1     |
      {-1} |  0       0       -x_0    -x_1    0       0       |
      {-1} |  0       0       0       0       -x_1    0       |
      {-1} |  0       0       0       0       0       -x_1    |
```

Every column corresponds to a tuple (A, B), the first three entries to A and the last six to B. Hence the possible A are

$$\begin{aligned}&(x_0^2, 0, 0),\ (x_1^2, 0, 0),\\ &(0, x_0^2, 0),\ (0, x_2^2, 0),\\ &(0, 0, x_1^2),\ (0, 0, x_2^2).\end{aligned}$$

6.6 Exercises

Exercise 6.1 *Let $R = K[x_1, \dots, x_n]$. Given ideals $I = \langle f_1, \dots, f_a \rangle \subset R$ and $J = \langle g_1, \dots, g_b \rangle \subset R$, consider the matrix*

$$G = \begin{pmatrix} f_1 & \dots & f_a & 0 & \dots & 0 & 1 \\ 0 & \dots & 0 & g_1 & \dots & g_b & 1 \end{pmatrix} \in R^{2\times(a+b+1)},$$

and let $S = \operatorname{syz}(G) \in R^{(a+b+1)\times g}$ be a syzygy matrix of G.

1) *Show that the entries of the last row of S generate $I \cap J$.*

2) *Applying this algorithm, compute the intersection*

$$\langle x_1, x_2 \rangle \cap \langle x_1 - x_3, x_2 - x_3 \rangle \subset K[x_1, x_2, x_3].$$

Hint: You can use the SINGULAR *command* ***syz****.*

Exercise 6.2 *Let $R = K[x_0, \dots, x_6]$, and*

$$A = \begin{pmatrix} 0 & x_1 & 0 & 0 & 0 & 0 & -x_6 \\ -x_1 & 0 & x_3 & 0 & 0 & 0 & 0 \\ 0 & -x_3 & 0 & x_5 & 0 & 0 & 0 \\ 0 & 0 & -x_5 & 0 & x_0 & 0 & 0 \\ 0 & 0 & 0 & -x_0 & 0 & x_2 & 0 \\ 0 & 0 & 0 & 0 & -x_2 & 0 & x_4 \\ x_6 & 0 & 0 & 0 & 0 & -x_4 & 0 \end{pmatrix} \in R^{7\times 7}$$

1) *Compute a Gröbner basis of A with respect to (dp, c).*

2) *From the Buchberger test, determine generators of* $\ker(A)$.

Exercise 6.3 *Let $R = K[x_0, x_1, x_2]$. For*

$$A = \begin{pmatrix} x_1 & x_0 & 0 \\ 0 & x_2 & x_1 \end{pmatrix}$$
$$B = \begin{pmatrix} x_1x_2 & x_0x_1 & 0 & 0 \\ 0 & 0 & x_1x_2 & x_0x_1 \end{pmatrix}$$

compute a presentation of

$$\operatorname{subquot}(A, B) = \frac{\operatorname{im}(A) + \operatorname{im}(B)}{\operatorname{im}(B)}.$$

Exercise 6.4 *Let $R = K[x_0, \ldots, x_4]$ and*

$$I = \langle x_0x_1,\ x_1x_2,\ x_2x_3,\ x_3x_4,\ x_4x_0 \rangle \subset R$$

With the help of a computer algebra system, determine:

1) $\operatorname{Hom}_R(I, R/I)$ *as a subquotient,*

2) *a basis of* $\operatorname{Hom}_R(I, R/I)_0$, *and*

3) *interpret your basis vectors as homomorphisms $I \to R/I$.*

Exercise 6.5 *Let $R = K[x_0, \ldots, x_3]$ and*

$$I = \langle x_0x_1,\ x_2x_3 \rangle \subset R$$

In a step-by-step calculation,

1) *determine δ and ρ as needed in Algorithm 6.5 to present* $\operatorname{Hom}_R(I, R/I)$,

2) *compute γ with* $\operatorname{im}(\gamma) = \ker(\delta)$,

3) *compute a presentation of* $\operatorname{Hom}_R(I, R/I) = \operatorname{subquot}(\gamma, \rho)$,

4) *determine a basis of* $\operatorname{Hom}_R(I, R/I)_0$, *and*

5) *interpret your basis vectors as homomorphisms $I \to R/I$.*

7

Primary decomposition

7.1 Overview

As we have already seen in Section 3.1, the union of algebraic sets $X_1 = V(I_1)$ and $X_2 = V(I_2)$ corresponds to the intersection of the defining ideals

$$X_1 \cup X_2 = V(I_1 \cap I_2)$$

To decompose the problem of analyzing $X_1 \cup X_2$ into the problem of analyzing the simpler pieces X_i, we encounter the following task: Write a given ideal I as an intersection of ideals in analogy to prime factorization of integers. The main question is, what the appropriate building blocks should be. If I is radical, then the decomposition of X into a union of (irreducible) varieties correponds to the decomposition of I into an intersection of prime ideals. For example,

$$I = \langle x_0x_1,\ x_0x_2,\ x_1x_2 \rangle = \langle x_0, x_1 \rangle \cap \langle x_0, x_2 \rangle \cap \langle x_1, x_2 \rangle$$

is the intersection of three prime ideals, and $V(I) \subset \mathbb{P}^2$ is the union of the corresponding 3 points. However we have seen (for example in Section 6.4) that in many settings one also has to consider ideals which are not radical. In this case, it turns out that right the building blocks are primary ideals: An ideal $I \neq R$ of a ring R is called primary if every zerodivisor in R/I is nilpotent.

Let us first focus on decomposing monomial ideals:

7.2 Irreducible decomposition of monomial ideals

Let $R = K[x_0, ..., x_n]$. First of all, we should avoid unnecessary factors:

Definition 7.2.1 *A decomposition*

$$I = \bigcap_{i=1}^{s} Q_i$$

of an ideal $I \subset R$ into an intersection of ideals is called ***irredundant*** *if omitting some Q_j in the intersection does not result in I any more.*

Lemma 7.2.2 *Let $m_1, ..., m_r$ be the unique minimal generators of the monomial ideal I according to Corollary 2.3.5. If*

$$m_1 = u_1 \cdot u_2$$

with $\deg(u_i) > 0$ *and* $\gcd(u_1, u_2) = 1$*, then*

$$I = I_1 \cap I_2$$

with

$$I_j = \langle u_j, m_2, ..., m_r \rangle .$$

Proof. The inclusion $I \subset I_j$ is obvious. On the other hand, let $m \in I_1 \cap I_2$. If $m_i \mid m$ for some $i \geq 2$, then $m \in I$. Otherwise $u_1 \mid m$ and $u_2 \mid m$. Then, by $\gcd(u_1, u_2) = 1$ we have $m_1 \mid m$, hence $m \in I$. ■

Theorem 7.2.3 *Any monomial ideal $I \subset R$ has a unique irredundant decomposition*

$$I = \bigcap_{i=1}^{s} Q_i$$

into ideals

$$Q_i = \left\langle x_{i_1}^{\alpha_1}, ..., x_{i_r}^{\alpha_r} \right\rangle$$

generated by powers of variables.

Proof. For the existence of a decomposition apply Lemma 7.2.2 inductively.

Suppose $I = \bigcap_{i=1}^{s} Q_i$ and

$$\bigcap_{i \neq j} Q_i \subset Q_j$$

then Q_j can be omitted. Proceeding inductively, we obtain an irredundant decomposition.

For the uniqueness, suppose

$$\bigcap_{i=1}^{s} Q_i = \bigcap_{j=1}^{s'} Q'_j$$

are irredundant decompositions into ideals generated by powers of variables. Fix i and let

$$Q_i = \left\langle x_{i_1}^{\alpha_1}, \ldots, x_{i_r}^{\alpha_r} \right\rangle$$

with $\alpha_l > 0$ for all l. Assume that $Q'_j \notin Q_i$ for all j. Then for every j there is an $x_{v_j}^{\beta_j} \in Q'_j$ with $x_{v_j}^{\beta_j} \notin Q_i$, that is,

$$v_j = i_l \Longrightarrow \alpha_l > \beta_j.$$

Clearly

$$m = \operatorname{lcm}(x_{v_1}^{\beta_1}, \ldots, x_{v_{s'}}^{\beta_{s'}}) \in \bigcap_{j=1}^{s'} Q'_j \subset Q_i$$

So there is some l with $x_{i_l}^{\alpha_l} \mid m$, which contradicts $i_l = v_j \Longrightarrow \alpha_l > \beta_j$.

Hence for every i there is j with $Q'_j \subset Q_i$, which proves the claim. ■

Definition 7.2.4 *An ideal I is called **irreducible** if it cannot be written as*

$$I = I_1 \cap I_2$$

with ideals $I_i \supsetneqq I$.

Corollar 7.2.5 *A monomial ideal $Q \subset R$ is irreducible if and only if it is of the form*

$$Q = \left\langle x_{i_1}^{\alpha_1}, \ldots, x_{i_r}^{\alpha_r} \right\rangle.$$

Proof. If Q is not of this form, then by Lemma 7.2.2 it is not irreducible.

On the other hand, suppose is of the given form and

$$Q = I_1 \cap I_2$$

and let

$$I_j = \bigcap_i Q_{j,i}$$

be decompositions as in Theorem 7.2.3 with $Q_{j,i}$ generated by powers of variables. From this we obtain an irredundant decomposition

$$Q = \bigcap_{\text{some } i} Q_{1,i} \cap \bigcap_{\text{some } i} Q_{2,i}$$

which by Theorem 7.2.3 is unique. Since also Q is generated by powers of variables, for some i, j

$$Q = Q_{j,i} \supset I_j$$

hence $Q = I_j$. ■

By Theorem 7.2.3 and Corollary 7.2.5 we have:

Corollar 7.2.6 *Any monomial ideal $I \subset R$ has a unique irredundant decomposition into irreducible ideals.*

Example 7.2.7 *For*

$$I = \left\langle x_0x_1x_2,\ x_0^2x_2,\ x_1^3x_2 \right\rangle$$

we follow the constructive proof of Theorem 7.2.3:

$$\begin{aligned} I &= \left\langle x_0,\ x_1^3x_2 \right\rangle \cap \left\langle x_1x_2,\ x_0^2x_2 \right\rangle \\ &= \left\langle x_0,\ x_1^3x_2 \right\rangle \cap \left\langle x_1,\ x_0^2x_2 \right\rangle \cap \langle x_2 \rangle \\ &= \left\langle x_0,\ x_1^3 \right\rangle \cap \langle x_0,\ x_2 \rangle \cap \left\langle x_1,\ x_0^2 \right\rangle \cap \langle x_1,\ x_2 \rangle \cap \langle x_2 \rangle \\ &= \left\langle x_0,\ x_1^3 \right\rangle \cap \left\langle x_1,\ x_0^2 \right\rangle \cap \langle x_2 \rangle \end{aligned}$$

In SINGULAR *we can compute this decomposition by:*

```
LIB "monomialideal.lib";
ring R = 0,(x(0..2)),dp;
ideal I = x(0)*x(1)*x(2), x(0)^2*x(2), x(1)^3*x(2);
irreddecMon(I);
[1]:
      _[1]=x(0)^2
      _[2]=x(1)
[2]:
      _[1]=x(0)
      _[2]=x(1)^3
[3]:
      _[1]=x(2)
```

We summarize our strategy for computing this decomposition in Algorithm 7.2.1.

Algorithm 7.2.1 Irreducible decomposition of monomial ideals

Input: Monomial ideal I.

Output: The irredundant irreducible decomposition of I.

1: Applying Lemma 7.2.2 inductively to minimal generators compute an irreducible decomposition

$$I = \bigcap_{i=1}^{s} Q_i$$

2: Inductively delete any Q_j with

$$\bigcap_{i \neq j} Q_i \subset Q_j$$

What about non-monomial ideals?

Theorem 7.2.8 *Any ideal $I \subset R$ has a decomposition*

$$I = \bigcap_{i=1}^{s} Q_i$$

into irreducible ideals Q_i.

Proof. Let X be the set of ideals for which the claim is false. By Theorem 2.1.5, X has a maximal element I. Since I cannot be irreducible, we can write $I = I_1 \cap I_2$ with $I \subsetneqq I_j$. Since I was chosen maximal, both I_1 and I_2 have a decomposition into irreducibles, hence also I has. This contradicts the assumption. ■

Example 7.2.9 *If we leave the class of monomial ideals, an irredundant irreducible decomposition is by no means unique. For example*

$$I = \left\langle x^2, xy, y^2 \right\rangle = \left\langle x^2, y \right\rangle \cap \left\langle x, y^2 \right\rangle = \left\langle x^2, x+y \right\rangle \cap \left\langle x, y^2 \right\rangle.$$

This problem can be fixed (partly) by combining irreducible summands in a suitable way. The basic philosophy is that the ideal in Example 7.2.9 should be not decomposed at all.

7.3 Existence of primary decomposition

Definition 7.3.1 *An ideal $I \neq R$ of a ring R is called **primary** if every zerodivisor in R/I is nilpotent.*

Remark 7.3.2 *I is primary if and only if for $f, g \in R$ it holds*

$$fg \in I \Rightarrow f \in I \text{ or } g \in \sqrt{I}.$$

Definition and Theorem 7.3.3 *If I is primary then $P := \sqrt{I}$ is prime. It is called the **associated prime** of I, and I is called **P-primary**.*

Proof. If $f \cdot g \in \sqrt{I}$, there is an m with $(f \cdot g)^m \in I$. Since I is primary, $f^m \in I$ or $g^{m \cdot m'} \in I$, hence $f \in \sqrt{I}$ or $g \in \sqrt{I}$. ■

Lemma 7.3.4 *If $I_1, I_2 \subset R$ are ideals then*

$$\sqrt{I_1 \cap I_2} = \sqrt{I_1} \cap \sqrt{I_2}.$$

Proof. Let $f \in \sqrt{I_1 \cap I_2}$, so $f^m \in I_1 \cap I_2$ for some m. This implies $f \in \sqrt{I_1}$ and $f \in \sqrt{I_2}$.

On the other hand, if $f \in \sqrt{I_1} \cap \sqrt{I_2}$ then $f^m \in I_1$ and $f^{m'} \in I_2$ for some m and m'. Hence $f^{\max\{m,m'\}} \in I_1 \cap I_2$. ■

Lemma 7.3.5 *Any intersection of P-primary ideals is P-primary.*

Proof. Suppose $Q_1, Q_2 \subset R$ are primary and $\sqrt{Q_i} = P$. Let $fg \in Q_1 \cap Q_2$. Hence

$$(f \in Q_1 \text{ or } g \in P) \text{ and } (f \in Q_2 \text{ or } g \in P),$$

that is, $f \in Q_1 \cap Q_2$ or $g \in P$. By Lemma 7.3.4

$$\sqrt{Q_1 \cap Q_2} = P$$

and hence the claim follows. ■

Lemma 7.3.6 *Let R be a ring, $I \subset R$ an ideal. If*

$$I : \langle f \rangle = I : \left\langle f^2 \right\rangle$$

for some $f \in R$, then

$$I = (I : \langle f \rangle) \cap \langle I, f \rangle .$$

Proof. If $g \in (I : \langle f \rangle) \cap \langle I, f \rangle$ then there are $h \in I$, $r \in R$ with

$$g = h + rf.$$

Since $g \in (I : \langle f \rangle)$,

$$fh + rf^2 = fg \in I,$$

hence $rf^2 \in I$, that is, $r \in I : \langle f^2 \rangle = I : \langle f \rangle$. So $rf \in I$, which implies that $g = h + rf \in I$.

The other inclusion is obvious. ■

Proposition 7.3.7 *For any ideal $I \subsetneqq R$ it holds*

$$\textit{prime} \;\Rightarrow\; \textit{irreducible} \;\Rightarrow\; \textit{primary}$$

Proof. For the first implication, suppose $I = I_1 \cap I_2$ with $I \subsetneqq I_1$. Then there is an $f \in I_1 - I$. For any $g \in I_2$

$$fg \in I_1 I_2 \subset I_1 \cap I_2 = I.$$

If I is prime then $g \in I$, which proves that $I_2 = I$.

For the second implication, let $f, g \in R$ with $fg \in I$ and $f \notin I$. By Theorem 2.1.5 the ascending chain

$$I : \langle g \rangle \subset I : \left\langle g^2 \right\rangle \subset \ldots$$

terminates, so there is an m with $I : \langle g^m \rangle = I : \langle g^{m+1} \rangle$. By Lemma 7.3.6 this implies that

$$I = (I : \langle g^m \rangle) \cap \langle I, g^m \rangle .$$

By $fg^m \in I$ we have $f \in I : \langle g^m \rangle$. As $f \notin I$ it holds

$$I \subsetneqq I : \langle g^m \rangle ,$$

hence, since I is irreducible,

$$I = \langle I, g^m \rangle ,$$

This implies $g^m \in I$, that is, $g \in \sqrt{I}$. ■

Definition 7.3.8 *A **primary decomposition** of an ideal I is an expression*

$$I = \bigcap_{i=1}^{s} Q_i$$

*with Q_i primary. A primary decomposition is called **minimal** if it is irredundant and all $\sqrt{Q_i}$ are distinct.*

Theorem 7.3.9 *Any ideal has a minimal primary decomposition.*

Proof. Determine an irredundant irreducible decomposition by Proposition 7.3.7. By Theorem 7.2.8 this is a primary decomposition. By Lemma 7.3.5, we can combine factors which have the same radical. ■

7.4 Algorithm for primary decomposition of monomial ideals

Proposition 7.4.1 *Any irreducible monomial ideal $I = \left\langle x_{i_1}^{\alpha_1}, \ldots, x_{i_r}^{\alpha_r} \right\rangle$ is $\langle x_{i_1}, \ldots, x_{i_r} \rangle$-primary.*

Proof. By Proposition 7.3.7 I is primary. Since $\langle x_{i_1}, \ldots, x_{i_r} \rangle \supset I$ is a prime ideal, the claim follows. ■

Using this observation, we obtain Algorithm 7.4.1 for computing a minimal primary decomposition of a monomial.

Algorithm 7.4.1 Monomial primary decomposition

Input: Monomial ideal I.

Output: Minimal primary decomposition of I.

1: Compute the irredundant irreducible decomposition.

2: Combine factors which have the same radical.

Example 7.4.2 *In Example 7.2.7 we have computed the irredundant irreducible decomposition*

$$I = \left\langle x_0x_1x_2,\ x_0^2x_2,\ x_1^3x_2 \right\rangle = \left\langle x_0,\ x_1^3 \right\rangle \cap \left\langle x_1,\ x_0^2 \right\rangle \cap \langle x_2 \rangle$$

By Proposition 7.4.1

$$\sqrt{\langle x_0,\ x_1^3 \rangle} = \langle x_0,\ x_1 \rangle = \sqrt{\langle x_1,\ x_0^2 \rangle}$$

hence, by

$$\left\langle x_0,\ x_1^3 \right\rangle \cap \left\langle x_1,\ x_0^2 \right\rangle = \left\langle x_0^2, x_0x_1, x_1^3 \right\rangle$$

a minimal primary decomposition of I is

$$I = \left\langle x_0^2, x_0x_1, x_1^3 \right\rangle \cap \langle x_2 \rangle$$

In Singular *we can compute a minimal primary decomposition of any (not necessarily monomial) ideal by:*

```
LIB "primdec.lib";
ring R = 0,(x(0..2)),dp;
ideal I = x(0)*x(1)*x(2), x(0)^2*x(2), x(1)^3*x(2);
primdecGTZ(I);
[1]:
      [1]:
            _[1]=x(2)
      [2]:
            _[1]=x(2)
[2]:
      [1]:
            _[1]=x(1)^3
            _[2]=x(0)*x(1)
            _[3]=x(0)^2
      [2]:
            _[1]=x(1)
            _[2]=x(0)
```

This command returns a list of tuples of a primary ideal Q_i the prime $\sqrt{Q_i}$.

Example 7.4.3 *In general, a minimal primary decomposition is not unique. For example*

$$\left\langle x^2, xy \right\rangle = \langle x \rangle \cap \left\langle x^2, y \right\rangle = \langle x \rangle \cap \left\langle x^2, xy, y^n \right\rangle$$

for all $n \geq 1$.

However, we have uniqueness in the following sense:

7.5 Uniqueness of primary decomposition

Theorem 7.5.1 *If*

$$I = \bigcap_{i=1}^{s} Q_i$$

is a minimal primary decomposition, then the pairwise different prime ideals $\sqrt{Q_i}$ *are uniquely determined.*

They are precisely the primes $P \subset R$ *with* $P = \sqrt{I : \langle b \rangle}$ *for some* $b \in R$.

Remark 7.5.2 *If* Q *is primary and* $b \in R$ *then*

$$b \in Q \Longrightarrow Q : b = R$$
$$b \notin Q \Longrightarrow \sqrt{Q : b} = \sqrt{Q}$$

Proof. The first claim of the remark and the inclusion $\supset$ in the second claim are trivial. Let $x^m \in Q : b$ for some m, that is, $x^m b \in Q$. Since $b \notin Q$ and Q is primary, we have $x^{m \cdot m'} \in Q$ for some m'. ■

We now prove the theorem:

Proof. By the remark

$$I : \langle b \rangle = \bigcap_{i=1}^{s} (Q_i : \langle b \rangle)$$

hence

$$\sqrt{I : \langle b \rangle} = \bigcap_{i=1}^{s} \sqrt{Q_i : \langle b \rangle} = \bigcap_{b \notin Q_i} \sqrt{Q_i}.$$

If $\sqrt{I : \langle b \rangle}$ is prime then by Proposition 7.3.7

$$\sqrt{I : \langle b \rangle} = \sqrt{Q_i}$$

for some i.

Conversely, by minimality of the decomposition, for every j there is

$$b_j \in \bigcap_{i \neq j} Q_i$$

with $b_j \notin Q_j$. Then

$$\sqrt{Q_j} = \sqrt{I : \langle b_j \rangle}.$$

■

Example 7.5.3 *Consider*

$$I = \left\langle x_0 x_1 x_2,\ x_0^2 x_2,\ x_1^3 x_2^2 \right\rangle$$

We compute an irreducible decomposition

$$\begin{aligned} I &= \left\langle x_0,\ x_1^3x_2^2\right\rangle \cap \left\langle x_1,\ x_0^2x_2\right\rangle \cap \langle x_2\rangle \\ &= \left\langle x_0,\ x_1^3\right\rangle \cap \left\langle x_0,\ x_2^2\right\rangle \cap \left\langle x_1,\ x_0^2\right\rangle \cap \langle x_1,\ x_2\rangle \cap \langle x_2\rangle \end{aligned}$$

Since $\langle x_2\rangle \subset \langle x_1,\ x_2\rangle$ *we can delete* $\langle x_1,\ x_2\rangle$. *Note that* $\langle x_0,\ x_2^2\rangle$ *cannot be deleted. So the irredundant irreducible decomposition is*

$$I = \left\langle x_0,\ x_1^3\right\rangle \cap \left\langle x_0,\ x_2^2\right\rangle \cap \left\langle x_1,\ x_0^2\right\rangle \cap \langle x_2\rangle\,.$$

Hence, like in Example 7.4.2, a minimal primary decomposition is

$$I = \left\langle x_0^2, x_0x_1, x_1^3\right\rangle \cap \langle x_2\rangle \cap \left\langle x_0, x_2^2\right\rangle.$$

We verify this also using Singular*:*

```
LIB "primdec.lib";
ring R = 0,(x(0..2)),dp;
ideal I = x(0)*x(1)*x(2), x(0)^2*x(2), x(1)^3*x(2)^2;
primdecGTZ(I);
[1]:
      [1]:
            _[1]=x(2)
      [2]:
            _[1]=x(2)
[2]:
      [1]:
            _[1]=x(1)^3
            _[2]=x(0)*x(1)
            _[3]=x(0)^2
      [2]:
            _[1]=x(1)
            _[2]=x(0)
[3]:
      [1]:
            _[1]=x(2)^2
            _[2]=x(0)
      [2]:
            _[1]=x(2)
            _[2]=x(0)
```

By computing appropriate ideal quotients

```
radical(quotient(I,x(0)^2));
_[1]=x(2)
radical(quotient(I,x(2)^2));
_[1]=x(1)
```

```
_[2]=x(0)
radical(quotient(I,x(1)^3*x(2)));
_[1]=x(2)
_[2]=x(0)
```

we can obtain all possible primes

$$\sqrt{I : \langle x_0^2 \rangle} = \langle x_2 \rangle$$
$$\sqrt{I : \langle x_2^2 \rangle} = \langle x_0, x_1 \rangle$$
$$\sqrt{I : \langle x_1^3 x_2 \rangle} = \langle x_0, x_2 \rangle .$$

In fact, in the case of monomial ideals, the elements b in Theorem 7.5.1 can always be chosen monomial.

Definition 7.5.4 *The $\sqrt{Q_i}$ in the theorem are called the* ***associated primes*** *of I. Write*

$$\mathrm{Ass}(I) = \left\{ \sqrt{Q_i} \mid i \right\} .$$

The minimal elements of $\mathrm{Ass}(I)$ with respect to inclusion are called the ***minimal associated primes*** *of I. Write $\mathrm{Min}(I)$ for the set of minimal associated primes.*

Primary ideals Q_i with $\sqrt{Q_i}$ minimal are called ***isolated*** *primary components, the others are called* ***embedded*** *primary components.*

Example 7.5.5 *In the above example*

$$\mathrm{Ass}(I) = \{ \langle x_2 \rangle , \langle x_0, x_1 \rangle , \langle x_0, x_2 \rangle \}$$

and

$$\mathrm{Min}(I) = \{ \langle x_2 \rangle , \langle x_0, x_1 \rangle \}$$

The primary component $\langle x_0, x_2^2 \rangle$ is embedded in the isolated component $\langle x_2 \rangle$.

In geometric terms, $V(x_0, x_2^2)$ is a point in $\mathbb{P}^2$ which lies on the line $V(x_2)$.

A point specified (as a scheme) by a primary ideal that is not prime is usually referred to as a ***fat point****.*

Remark 7.5.6 *If $I \subset R$ is an ideal then*

$$\sqrt{I} = \bigcap_{P \in \mathrm{Min}(I)} P,$$

in particular,

$$\sqrt{I} = \bigcap_{P \supset I \text{ prime}} P .$$

Proof. Clear by Theorem 7.5.1 and Lemma 7.3.4. ■

Without proof we mention:

Theorem 7.5.7 *The isolated components of a minimal primary decomposition are uniquely determined.*

7.6 Computing primary decomosition in general

7.7 Exercises

Exercise 7.1 *Let S be the set of squarefree monomials in the variables $x_0, ..., x_n$. A* ***simplicial complex*** *Δ on the vertices $x_0, ..., x_n$ is a subset $\Delta \subset S$, such that $x_0, ..., x_n \in \Delta$, and if $m \in \Delta$ and $w \mid m$ then also $w \in \Delta$. The elements of Δ are called* ***faces****, the maximal ones* ***facets****.*

The ***Stanley-Reisner ideal*** *of Δ is the ideal*

$$I_\Delta = \langle m \mid m \in S,\ m \notin \Delta \rangle \subset K[x_0, ..., x_n]$$

generated by the non-faces of Δ.

An element $m \in S$ is called ***coface*** *if $\frac{x_1 \cdot ... \cdot x_n}{m} \in \Delta$, that is, if its complement is a face.*

1) *Show that*
$$I_\Delta = \bigcap_{\substack{x_{i_1} \cdot ... \cdot x_{i_a} \text{ minimal} \\ \text{coface of } \Delta}} \langle x_{i_1}, ..., x_{i_a} \rangle$$

2) *For the simplicial complex*

$$S = \{1,\ x_0,\ x_1,\ x_2,\ x_3,\ x_1x_2,\ x_1x_3,\ x_0x_2,\ x_0x_3,\ x_2x_3,\ x_1x_2x_3\}$$

(see Figure 7.1), determine I_Δ, and its decomposition according to 1). Verify your result by computing the ideal intersection.

Exercise 7.2 *Let $R = K[x_0, x_1, x_2]$ and*

$$I = \left\langle x_0^2x_1,\ x_0^2x_2^2,\ x_1^2,\ x_1x_2^2 \right\rangle \subset R$$

Find the irredundant decomposition of I into irreducible ideals.

Exercise 7.3 *Let $R = K[x_0, x_1, x_2]$ and*

$$I = \left\langle x_0^3,\ x_1^3,\ x_0^2x_2^2,\ x_0x_1x_2^2,\ x_1^2x_2^2 \right\rangle \subset R$$

1) *Find the irredundant decomposition of I into irreducible ideals.*

2) *Find a minimal primary decomposition of I.*

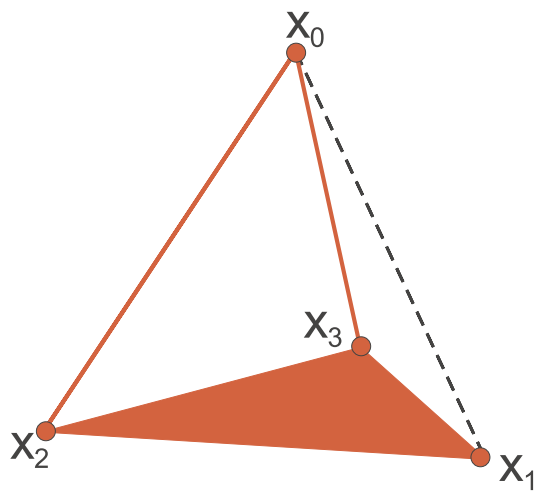

Figure 7.1: Simplicial complex with three maximal faces.

8

Normalization

8.1 Overview

Definition 8.1.1 *Let A be a Noetherian domain. The* ***normalization*** *of A, written $\overline{A}$, is the integral closure of A in its quotient field* $\mathrm{quot}(A)$*. We call A* ***normal*** *if $A = \overline{A}$.*

Recall that the integral closure is unique up to isomorphism. The key setup we have in mind is the normalization of an **affine algebra**

$$A = K[x_1, ..., x_n]/I$$

where I is a prime ideal, and this is the setup we will consider in the following. We will describe an algorithm which computes the normalization as an affine algebra $\overline{A} = A[t_1, ..., t_s]/J$ with a prime ideal $J \subset A$. For simplicity we assume that K has characteristic zero (the algorithm will also work fine if K, more generally, is perfect, for example, if $K = \mathbb{F}_p$).

On the geometric side, A is the coordinate ring of an algebraic variety $X = V(I) \subset \mathbb{A}^n_K$ and $\overline{A}$ is the coordinate ring of an algebraic variety $\overline{X} \subset \mathbb{A}^{n+s}_K$ called the **normalization** of X. The integral ring extension $A \subset \overline{A}$ corresponds on the geometric side to a polynomial map $\overline{X} \to X$.

Example 8.1.2 *In Figure 3.3, we can view the twisted cubic $V(x^2 - y, x^3 - z)$ as the normalization $\overline{X}$ of the cusp $X = V(y^3 - z^2)$. The normalization is only determined up to isomorphism. In fact, the twisted cubic is in bijection to the line $\mathbb{A}^1$ via the paramatrization*

$$\begin{aligned} \mathbb{A}^1 &\to V(x^2 - y, x^3 - z) \\ t &\mapsto (t, t^2, t^3) \end{aligned}$$

In terms of algebra, we can see the normalization map from the line to the cusp immediately: If $I = \langle y^3 - z^2 \rangle \subset K[x, y]$ is the ideal of the cusp, then

$$\begin{array}{rcccc} A = K[y,z]/I & \cong & K[t^2, t^3] & \subset & K[t] = \overline{A} \\ \bar{y} & \mapsto & t^2 & & \\ \bar{z} & \mapsto & t^3 & & \end{array}$$

Since t is a zero of the monic polynomial $T^2 - t^2 \in K[t^2, t^3][T]$, it is integral. Moreover, $K[t]$ is normal since it is factorial:

Example 8.1.3 *Any unique factorization domain is normal.*

Proof. Let R be a unique factorization domain and $\frac{r}{s} \in \operatorname{quot}(R)$ be integral over R and $\gcd(r, s) \in R^\times$. Then there are $a_i \in R$ with

$$\left(\frac{r}{s}\right)^n = \sum_{i=0}^{n-1} a_i \left(\frac{r}{s}\right)^i,$$

and, cancelling the denominator,

$$r^n = s\left(\sum_{i=0}^{n-1} a_i r^i s^{n-1-i}\right).$$

So if p is a prime divisor of s, then also of r, which implies that $\frac{r}{s} \in R$. ■

In terms of geometry, normalization is a technique that improves the singularities of X, by removing singularities of dimension $d-1$ in a d-dimensional variety. In particular, for a curve X, normalization gives a desingularization.

The basic philosophy is that $\overline{X}$ is easier to study than X, but nevertheless yields equivalent information. For example, many results for curves assume, in their natural formulation, that the curve is non-singular, like the Riemann-Roch theorem classifying rational maps between curves.

We remark that also a desingularization of varieties of higher dimension can be achieved, for example, in the case of the singular surfaces in Figures 1.4, 1.6, and 1.7. However, this is more complicated since desingularization does not correspond to a simple algebraic process in terms of A (like normalization of X corresponds to normalization of A).

8.2 Basics on normalization

As in the introduction, let

$$A = K[x_1, ..., x_n]/I$$

with a prime ideal $I \subset K[x_1, ..., x_n]$. We first observe that normality is a local property, that is, it can be tested by testing it at every element of

$$X = \mathrm{Spec}(A) = \{P \subset A \mid P \text{ prime ideal}\}$$

for the spectrum of A. An element $P \in X$ is also called a point of the scheme X.

Recall that, If $S \subset A$ is a **multiplicatively closed set**, then

$$S^{-1}A = \left\{\frac{a}{s} \mid s \in S,\ a \in A\right\} \subset \mathrm{quot}(A)$$

is a ring called the **localization** of A at S. If $P \in X$, then define $A_P = S^{-1}A$ with $S = A - P$.

Theorem 8.2.1 *Normalization commutes with localization, that is,*

$$\overline{A_P} = \overline{A}_P$$

for all $P \in X$.

Proof. Let $\frac{a}{u} \in \overline{A}_P$ so $a \in \overline{A}$. Hence there are a_i with

$$a^n + \sum_{i=1}^n a_i a^{n-i} = 0$$

so

$$\left(\frac{a}{u}\right)^n + \sum_{i=1}^n a_i u^i \left(\frac{a}{u}\right)^{n-i} = 0.$$

This implies $\frac{a}{u} \in \overline{A_P}$.

If $\frac{a}{u} \in \overline{A_P}$, then there are $\frac{a_i}{u_i} \in A_P$ with

$$\left(\frac{a}{u}\right)^n + \sum_{i=1}^n \frac{a_i}{u_i} \left(\frac{a}{u}\right)^{n-i} = 0$$

Hence

$$(a \cdot u_1 \cdot ... \cdot u_n)^n + \sum_{i=1}^n a_i \left(u^i \cdot \prod_{j \neq i} a_j\right) (a \cdot u_1 \cdot ... \cdot u_n)^{n-i} = 0$$

so $a' = a \cdot u_1 \cdot ... \cdot u_n \in \overline{A}$. This implies $a \in \overline{A}_P$. ■

Corollar 8.2.2 *A is normal if and only if A_P is normal for all P.*

Proof. If $A = \overline{A}$ then by Theorem 8.2.1 we have $\overline{A_P} = \overline{A}_P = A_P$ for all P. On the other hand, if $A_P = \overline{A_P}$ for all P then, again using the Theorem 8.2.1, $A_P = \overline{A}_P$ for all $P \in X$. Using [5, Corollary 2.9] this implies $A = \overline{A}$. ■

Definition 8.2.3 *We call*

$$N(A) = \{P \in X \mid A_P \text{ is not normal}\}$$

the ***non-normal locus*** *of A.*

Remark 8.2.4 *By Corollary 8.2.2 the ring A is normal if and only if $N(A)$ is empty.*

Our next goal is to show that the non-normal locus can be described by an ideal. It will be convenient to use the following definitions (inspired by the theory of schemes): For an ideal $J \subset A$ we define by

$$\mathbb{V}(J) = \{P \in X \mid P \supset J\} \subset X$$

its **vanishing locus**. Subsets of the form $\mathbb{V}(J)$ are the closed sets of a topology on X, the Zariski topology. On the other hand, for any subset $Y \subset X$ we write

$$\mathbb{I}(Y) = \bigcap_{P \in Y} P$$

for its **zero ideal**. Then, using Remark 7.5.6, it follows immediately:

Theorem 8.2.5 *If $J \subset A$ is an ideal then*

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

Definition 8.2.6 *The* ***conductor*** *of A in $\overline{A}$ is*

$$\mathcal{C}_A = \{a \in A \mid a\overline{A} \subset A\}.$$

It is an ideal of both A and $\overline{A}$.

Lemma 8.2.7 $N(A) = \mathbb{V}(\mathcal{C}_A)$.

Proof. $N(A) \subset \mathbb{V}(\mathcal{C}_A)$: If $P \in N(A)$, that is, $A_P \subsetneqq \overline{A}_P$ then

$$(\mathcal{C}_A)_P = \mathcal{C}_{A_P} = \{a \in A_P \mid a\overline{A}_P \subset A_P\} \subsetneqq A_P$$

However if $P \notin \mathbb{V}(\mathcal{C}_A)$ then $(\mathcal{C}_A)_P = A_P$.
$\mathbb{V}(\mathcal{C}_A) \subset N(A)$: By

$$\mathbb{V}(\mathcal{C}_A) = \bigcup_{h \in \overline{A}} \mathbb{V}(\{a \in A \mid ah \in A\}),$$

we have to show that for all $h = \frac{p}{q} \in \overline{A} \subset \operatorname{quot}(A)$ it holds

$$\mathbb{V}(\{a \in A \mid ah \in A\}) \subset N(A).$$

So for every prime P we have to prove

$$\{a \in A \mid ah \in A\} \subset P \Longrightarrow A_P \subsetneqq \overline{A}_P.$$

If $A_P = \overline{A}_P$ then the image of h in $\overline{A}_P$ is $\frac{p/q}{1} = \frac{p}{q}$, that is, $q \notin P$. Moreover, $qh = p \in A$, which proves the claim. ■

In order to compute the normalization we require some knowledge about the non-normal locus $N(A)$. In general, $\mathcal{C}_A$ can only be computed a-posteriori from $\overline{A}$. Fortunately, the singular locus of A can be obtained explicitly, and contains the non-normal locus:

Definition 8.2.8 *For an ideal $I = \langle f_1, ..., f_s \rangle \subset K[x_1, ..., x_n]$, the* ***Jacobian ideal*** $\mathrm{Jac}(I)$ *is generated by the $c \times c$ minors of the Jacobian matrix*

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial f_s}{\partial x_1} & \cdots & \frac{\partial f_s}{\partial x_n} \end{pmatrix}$$

where $c = n - \dim(X)$ is the ***codimension*** *of $X = V(I)$. Then the* ***singular locus*** *of A is*

$$\mathrm{Sing}(A) = \mathbb{V}(\mathrm{Jac}(I) + I).$$

Note that we can consider $\mathrm{Jac}(I) + I$ both as an ideal in $A = K[x_1, ..., x_n]/I$ and in $K[x_1, ..., x_n]$, in fact it is easy to prove:

Remark 8.2.9 *There is a bijection between the ideals of A and the ideals of $K[x_1, ..., x_n]$ which contain I.*

Example 8.2.10 *Consider the coordinate ring*

$$A = K[\bar{x}, \bar{y}] = K[x, y]/I$$

of the plane curve $X = \mathbb{V}(I)$ defined by

$$I = \langle x^4 + y^2(y-1)^3 \rangle.$$

Then

$$\mathrm{Jac}(I) = \left\langle x^3,\ 2y(y-1)^3 + 3y^2(y-1)^2 \right\rangle$$

In Singular *we can compute the ideal $\mathrm{Jac}(I) + I \subset K[x, y]$ by the command* `slocus`*:*

```
ring R = 0,(x,y),dp;
ideal I = x^4 + y^2*(y-1)^3;
ideal singI = std(slocus(I));
singI;
```

```
_[1]=y3-2y2+y
_[2]=x3
```

We compute a minimal primary decomposition of the singular locus:

```
primdecGTZ(singI);
[1]:
      [1]:
            _[1]=y2-2y+1
            _[2]=x3
      [2]:
            _[1]=y-1
            _[2]=x
[2]:
      [1]:
            _[1]=y
            _[2]=x3
      [2]:
            _[1]=y
            _[2]=x
```

So

$$\sqrt{\mathrm{Jac}(I) + I} = \langle x, y\rangle \cap \langle x, y-1\rangle\,,$$

and the singular locus of the curve $X = V(I)$ *consists of two points* $(0,0), (0,1)$.

For the non-normal and the singular locus it holds (without proof):

Theorem 8.2.11 $N(A) \subset \mathrm{Sing}(A)$.

8.3 Finiteness of normalization

The following result will allow us to design an algorithm computing $\overline{A}$ in a finite number of steps:

Theorem 8.3.1 *$\overline{A}$ is a finitely generated A-module.*

Hence $\overline{A}$ is a Noetherian A-module by Theorem 4.3.12, since A is a Noetherian ring by Example 2.4(3).

Proof. Noether normalization gives algebraically independent $y_1, ..., y_s \in A$ such that A is a finitely generated $K[y_1, ..., y_s]$-module. Then

$$K[y_1, ..., y_s] \subset A \subset \overline{A} \subset K(y_1, ..., y_s) \subset L := \mathrm{quot}(A)$$

Note that $\overline{K[y_1, ..., y_s]} = \overline{A}$, since $K[y_1, ..., y_s] \subset A$ is finite.

Note that in characteristic zero any finite extension is separable. Hence we may assume that the finite extension $K(y_1, ..., y_s) \subset L$ is Galois. Otherwise we pass to the normal closure $K(y_1, ..., y_s) \subset L \subset L'$. Then the same arguments as below prove that the integral closure of A in L' is finite over A, which implies that $\overline{A}$ is finite over A.

So, with the Galois group G of $K(y_1, ..., y_s) \subset L$, consider the trace

$$\begin{array}{rccc} \mathrm{Tr}: & L & \to & K(y_1, ..., y_s) \\ & x & \mapsto & \sum_{g \in G} g(x) \end{array}$$

The trace yields a nondegenerate bilinear form

$$\begin{array}{l} L \times L \to K(y_1, ..., y_s) \\ (x, y) \mapsto \mathrm{Tr}(xy) \end{array}$$

Hence, for a basis $x_1, ..., x_r \in \overline{A}$ with

$$L = K(y_1, ..., y_s)(x_1, ..., x_r),$$

there is a dual basis $x_1^*, ..., x_r^* \in L$ with

$$\mathrm{Tr}(x_i x_j^*) = \delta_{i,j}$$

and

$$L = K(y_1, ..., y_s)(x_1^*, ..., x_r^*).$$

We show that

$$\overline{A} \subset A x_1^* + ... + A x_r^*$$

and, hence, $\overline{A}$ is a finitely generated A-module: Given $b \in \overline{A}$, there are $a_i \in K(y_1, ..., y_s)$ with

$$b = a_1 x_1^* + ... + a_r x_r^*.$$

By $bx_i \in \overline{A}$ we have

$$a_i = \mathrm{Tr}(bx_i) \in A$$

using that

$$\mathrm{Tr}(\overline{A}) \subset A.$$

Indeed, if $x \in \overline{A}$ then $\mathrm{Tr}(x)$ is a coefficient of the polynomial

$$P = \prod_{g \in G} (T - g(x)).$$

Since P is invariant under G, we have $P \in K(y_1, ..., y_s)[T]$. Since all $g(x)$ for $g \in G$ are integral over A all coefficients are integral, hence $P \in A[T]$. ■

8.4 Grauert-Remmert criterion

The first key observation is that, for any ideal $J \subset A$, the module $\mathrm{Hom}_A(J, J)$ lies between A and $\overline{A}$. Moreover it can be computed as an ideal quotient. We denote by

$$(I_1 :_A I_2) = \{b \in A \mid bI_2 \subset I_1\}$$

the quotient of ideals $I_1, I_2 \subset A$. Note that if $I_i = J_i \bmod I$ with ideals $J_i \subset K[x_1, ..., x_n]$, then by Remark 8.2.9 this ideal quotient can be computed by Algorithm 3.6.3 as

$$(I_1 :_A I_2) = ((J_1 + I) : (J_2 + I)) \bmod I.$$

Lemma 8.4.1 *If $J \subset A$ is an ideal and $0 \neq g \in J$, then:*

1) *Any $\varphi \in \mathrm{Hom}_A(J, J)$ is given by multiplication*

$$\begin{array}{cccc} \varphi & : & J & \to & J \\ & & b & \mapsto & \frac{\varphi(g)}{g} b \end{array}$$

2) *There is a natural inclusion of rings*

$$\begin{array}{ccc} A & \hookrightarrow & \mathrm{Hom}_A(J, J) \\ a & \mapsto & \varphi_a : J \to J \\ & & b \mapsto ab \end{array}$$

3) *There is a natural isomorphism of rings*

$$\begin{array}{ccc} \mathrm{Hom}_A(J, J) & \cong & \frac{1}{g}(gJ :_A J) \\ \varphi & \mapsto & \frac{\varphi(g)}{g} \end{array}$$

4) *Any element of $\frac{1}{g}(gJ :_A J)$ is integral, that is,*

$$\frac{1}{g}(gJ :_A J) \subset \overline{A} \subset \mathrm{quot}(A).$$

Proof.

1) If $\varphi : J \to J$ is a homomorphism and $b \in J$ is any other element, then by A-linearity

$$g \cdot \varphi(b) = \varphi(gb) = b \cdot \varphi(g),$$

hence for $b \neq 0$

$$\frac{\varphi(g)}{g} = \frac{\varphi(b)}{b} \in \mathrm{quot}(A).$$

This implies that $\frac{\varphi(g)}{g} b = \frac{\varphi(b)}{b} b = \varphi(b)$ for $b \neq 0$. For $b = 0$ the claim is trivial.

2) If $\varphi_a = 0$, that is, $ab = 0$ for all $b \in J$. Since $0 \neq g \in J$ is a non-zerodivisor, it follows that $a = 0$.

3) If $\varphi \in \mathrm{Hom}_A(J, J)$ then by (1) we have $\frac{\varphi(g)}{g} J \subset J$, that is, $\varphi(g)J \subset gJ$. This proves that $\varphi(g) \in (gJ :_A J)$ since $\varphi(g) \in J \subset A$, so the specified map is well-defined. Moreover, by (1) it is injective, as $\varphi = 0$ if $\varphi(g) = 0$. It is surjective since for any $g' \in (gJ :_A J)$ a well-defined homomorphism $J \to J$ is given by $b \mapsto \frac{g'}{g} b$.

4) Finally, we have to prove that for

$$b \in (gJ :_A J)$$

the element $\frac{b}{g} \in \mathrm{quot}(A)$ is integral over A: Consider the A-linear multiplication map $L_b : J \to J$, $a \mapsto ab$. Fix A-module generators $g_1, ..., g_s$ of J. By $bJ \subset gJ$, there are

$$b_{ij} \in \langle g \rangle$$

with

$$bg_j = \textstyle\sum_i b_{ij} g_i$$

which yields an $s \times s$-matrix (b_{ij}) representing L_b. By the theorem of Cayley-Hamilton, L_b is a zero of the characteristic polynomial

$$\chi(t) = \det(t \cdot E - (b_{ij})).$$

Hence, there are $a_i \in A$ with

$$b^s + a_1 b^{m-1} + ... + a_{m-1} b^1 + a_m = 0.$$

Since a_i is a linear combination of $i \times i$-minors of (b_{ij}) we have

$$a_i \in \langle g \rangle^i .$$

Hence

$$\left(\frac{b}{g}\right)^s + \frac{a_1}{g}\left(\frac{b}{g}\right)^{s-1} + ... + \frac{a_{s-1}}{g^{s-1}}\left(\frac{b}{g}\right)^1 + \frac{a_s}{g^s} = 0$$

is a monic equation for $\frac{b}{g}$ over A.

■

Remark 8.4.2 *If $J \subset A$ is an ideal and $0 \neq g \in J$, then*

$$(gJ :_A J) = (gJ :_{\mathrm{quot}(A)} J).$$

Proof. The inclusion $\subset$ is clear. If $g' \in \operatorname{quot}(A)$ with $g'J \subset gJ$ then a well-defined homomorphism $\varphi : J \to J$ is given by $b \mapsto \frac{g'}{g}b$. By Lemma 8.4.1(3.) it follows that

$$\frac{\varphi(g)}{g} \in \frac{1}{g}(gJ :_A J),$$

that is,

$$g' = \varphi(g) \in (gJ :_A J).$$

■

The following criterion for normality is due to Grauert and Remmert. It is the basis for an algorithmic approach on computing the normalization. It tells us that, if forming $\operatorname{Hom}_A(J, J)$ does not enlarge A any more, then we have reached $\overline{A}$. However this only works if J sees all of the non-normal locus, that is $N(A) \subset \mathbb{V}(J)$.

Theorem 8.4.3 (Grauert-Remmert criterion) *Let $0 \neq J \subset A$ be a radical ideal with*

$$N(A) \subset \mathbb{V}(J).$$

Then A is normal if and only if the inclusion

$$\begin{array}{ccc} A & \hookrightarrow & \operatorname{Hom}_A(J, J) \\ a & \mapsto & \varphi_a \end{array}$$

is an isomorphism.

Proof. If $A = \overline{A}$ then, by Lemma 8.4.1, we have injective maps $A \to \operatorname{Hom}_A(J, J) \to A$, which proves the claim.

For the converse: By Lemma 8.2.7

$$\mathbb{V}(\mathcal{C}_A) = N(A) \subset \mathbb{V}(J).$$

Hence, by Theorem 8.2.5,

$$J = \sqrt{J} = \mathbb{I}(\mathbb{V}(J)) \subset \mathbb{I}(\mathbb{V}(\mathcal{C}_A)) = \sqrt{\mathcal{C}_A},$$

which implies that there is a smallest $m \geq 0$ with $J^m \subset \mathcal{C}_A$, that is,

$$J^m \overline{A} \subset A.$$

Assume that $m > 0$. Then there is $a \in J^{m-1}$ and $b \in \overline{A}$ with $ab \in \overline{A} - A$. Moreover, $abJ \subset A$, so multiplication by ab defines an A-homomorphism

$$\varphi_{ab} : \begin{array}{ccc} J & \to & A \\ c & \mapsto & abc \end{array}$$

Since $ab \in \overline{A}$ there is a monic equation

$$(ab)^n + a_1(ab)^{n-1} + \ldots + a_n = 0$$

with $a_i \in A$. If $0 \neq c \in J$, then

$$(abc)^n = -a_1c(abc)^{n-1} - \ldots - a_nc^n \in J$$

hence $abc \in \sqrt{J} = J$, that is,

$$\varphi_{ab} \in \mathrm{Hom}_A(J, J).$$

If we assume that $A \to \mathrm{Hom}_A(J, J)$, $a \mapsto \varphi_a$ is an isomorphism, then $ab \in A$, a contradiction. Hence $m = 0$, that is, $\overline{A} = A$. ■

Definition 8.4.4 *A pair (J, g) with J as in Theorem 8.4.3 and $0 \neq g \in J$ is called a **test pair** for A, and J is called a **test ideal** for A.*

By Lemma 1.6.13 we can choose the Jacobian ideal together with any non-zero element as a test pair.

8.5 Normalization algorithm

By Lemma 8.4.1 and Theorem 8.4.3, if A is not normal, computing Hom as an ideal quotient yields a ring

$$A \subsetneqq \mathrm{Hom}_A(J, J) \cong \frac{1}{g}(gJ :_A J) \subset \overline{A} \subset \mathrm{quot}(A),$$

that is strictly larger than A and is contained in $\overline{A}$.

Example 8.5.1 *For A as in Example 8.2.10, the radical of the Jacobian ideal is*

$$J := \langle \bar{x}, \bar{y}(\bar{y} - 1) \rangle_A,$$

and we can take $g := \bar{x} \in J$ as a non–zerodivisor of A. Using Singular *we can determine $\mathrm{Hom}_A(J, J)$ as an ideal quotient:*

```
LIB "normal.lib";
ring R = 0,(x,y),dp;
ideal I = x^4+y^2*(y-1)^3;
qring A = std(I);
ideal J = x, y*(y-1);
quotient(x*J, J);
_[1]=x
_[2]=y3-2y2+y
```

Hence

$$A \subsetneqq A_1 \subset \overline{A} \subset \operatorname{quot}(A)$$

with

$$\begin{aligned} A_1 &= \frac{1}{\bar{x}}\,(\bar{x}J \ :_A \ J) = \frac{1}{\bar{x}}\,\left\langle \bar{x}, \bar{y}(\bar{y}-1)^2 \right\rangle \\ &=_A \left\langle 1, \frac{\bar{y}(\bar{y}-1)^2}{\bar{x}} \right\rangle. \end{aligned}$$

By iterating this calculation, we obtain Algorithm 8.5.1.

Algorithm 8.5.1 Normalization

Input: Prime ideal $I \subset K[x_1, ..., x_n]$.
Output: Normalization $\overline{A}$ of $A = K[x_1, ..., x_n]/I$.

1: Initial test pair: $J_0 := \sqrt{\operatorname{Jac}(I) + I} \subset A$ and select $0 \neq g \in J_0$.
2: $i = 0$
3: **repeat**
4: $\quad i = i + 1$
5: $\quad A_i = \frac{1}{g}(gJ_{i-1} :_{A_{i-1}} J_{i-1})$
6: $\quad J_i = \sqrt{JA_{i-1}}$
7: **until** $A_i = A_{i-1}$

We prove correctness of the algorithm:

Proof. Starting from $A_0 = A$, we get a chain of extensions of reduced Noetherian rings

$$A = A_0 \subset \cdots \subset A_{i-1} \subset A_i \subset \cdots \subset A_m = \overline{A}.$$

Since A is Noetherian, by Theorem 8.3.1 the sequence terminates, that is, for some m we have $A_m = A_{m+1}$. By Theorem 8.4.3 it then holds $A_m = \overline{A}$.

Moreover, (J_i, g) is a test pair for A_i by the following lemma: ■

Lemma 8.5.2 *Let $A \subset A' \subset \overline{A}$ be extensions of rings and (J, g) a test pair for A. Then $(\sqrt{JA'}, g)$ is a test pair for A'.*

Proof. Clearly, every non–zerodivisor $g \in A$ of A is a non–zerodivisor of $\operatorname{quot}(A) \supset A'$. For $J' = \sqrt{JA'}$ we have to show that $N(A') = \mathbb{V}(\mathcal{C}_{A'}) \subset \mathbb{V}(J')$, that is, if $\mathcal{C}_{A'} \subset Q$ for a prime Q then $J' \subset Q$.

Let $P = Q \cap A$. Then P is prime: If $f \cdot g \in P \subset Q$ with $f, g \in A$ then $f \in Q$ or $g \in Q$. Hence $f \in P$ or $g \in P$.

By $\overline{A'} = \overline{A}$ we have

$$Q \supset \mathcal{C}_{A'} = \{a \in A' \mid a\overline{A} \subset A'\} \supset \{a \in A \mid a\overline{A} \subset A\} = \mathcal{C}_A.$$

Hence $Q \cap A \supset \mathcal{C}_A$, that is, $Q \cap A \in \mathbb{V}(\mathcal{C}_A) = N(A) \subset \mathbb{V}(J)$. So $J \subset Q \cap A$, which implies that $JA' \subset Q$. Using Remark 7.5.6 it follows that

$$\sqrt{JA'} = \bigcap_{Q' \supset JA' \text{ prime}} Q' \subset Q.$$

■

Practical computations rely on explicit representations of the A_i as A–algebras. These will be obtained as an application of Lemma 8.5.3 below. To formulate the lemma, we use the following notation. Let $J \subset A$ be an ideal containing a non–zerodivisor g of A, and let A–module generators $u_0 = g, u_1, \ldots, u_s$ for $(gJ :_A J)$ be given. Choose variables $T_1, \ldots, T_s$, and consider the epimorphism

$$\Phi : A[T_1, \ldots, T_s] \to \frac{1}{g}(gJ :_A J),\ T_i \mapsto \frac{u_i}{g},$$

hence

$$\frac{1}{g}(gJ :_A J) \cong A[T_1, \ldots, T_s]/\ker(\Phi).$$

The kernel of Φ describes the A–algebra relations on the u_i/g. These can be computed by Algorithm 3.5.10. In fact, in this setup, they can be described explicitly:

- Each A–module syzygy

  $$\alpha_0 u_0 + \alpha_1 u_1 + \ldots + \alpha_s u_s = 0, \quad \alpha_i \in A,$$

  gives an element $\alpha_0 + \alpha_1 T_1 + \ldots + \alpha_s T_s \in \ker(\Phi)$, which we call a **linear relation**.

- Developing each product $\frac{u_i}{g}\frac{u_j}{g}$, $1 \le i \le j \le s$, as a sum $\frac{u_i}{g}\frac{u_j}{g} = \sum_k \beta_{ijk}\frac{u_k}{g}$, we get elements $T_iT_j - \sum_k \beta_{ijk}T_k$ in $\ker\Phi$, which we call **quadratic relations**.

Lemma 8.5.3 *The linear and quadratic relations generate* $\ker(\Phi)$.

For a proof see [9, Lemma 3.6.7].

Example 8.5.4 *For A_1 as in Example 8.5.1, we find*

$$A[t_1]/I_1 \cong A_1$$
$$\bar{t}_1 \mapsto \frac{\bar{y}(\bar{y}-1)^2}{\bar{x}}$$

with

$$I_1 = \left\langle -t_1\bar{x} + \bar{y}(\bar{y}-1)^2, t_1\bar{y}(\bar{y}-1) + \bar{x}^3, t_1^2 + \bar{x}^2(\bar{y}-1) \right\rangle.$$

In this representation of A_1 we can compute

$$J_1 = \sqrt{{}_{A_1}\langle \bar{x}, \bar{y}(\bar{y}-1)\rangle} = {}_{A_1}\langle \bar{x}, \bar{y}(\bar{y}-1), t_1\rangle.$$

Finally, the following result will allow us to find the normalization in a way such that in all steps of the algorithm the computation of Hom can be carried through in the original ring A:

Theorem 8.5.5 *Let $0 \neq J \subset A$ be an ideal and $A \subset A' \subset \overline{A}$ an intermediate ring, and let $J' = \sqrt{JA'}$. Let U and H be ideals of A and $d \in A$ such that $A' = \frac{1}{d}U$ and $J' = \frac{1}{d}H$, respectively. Then*

$$(gJ' :_{A'} J') = \frac{1}{d}(dgH :_A H) \subset \operatorname{quot}(A).$$

Proof. By Remark 8.4.2, $g \in J \subset J'$ and $\operatorname{quot}(A) = \operatorname{quot}(A')$ we get

$$(gJ' :_{A'} J') = \left(gJ' :_{\operatorname{quot}(A)} J'\right)$$

and, in the same way, by $dg \in H$

$$(dgH :_A H) = \left(dgH :_{\operatorname{quot}(A)} H\right).$$

Moreover

$$\begin{aligned}\left(gJ' :_{\operatorname{quot}(A)} J'\right) &= \left\{a \in \operatorname{quot}(A) \mid a\frac{1}{d}H \subset g\frac{1}{d}H\right\}\\ &= \{a \in \operatorname{quot}(A) \mid aH \subset gH\}\\ &= \left(gH :_{\operatorname{quot}(A)} H\right)\end{aligned}$$

and

$$\begin{aligned}\left(dgH :_{\operatorname{quot}(A)} H\right) &= \{b \in \operatorname{quot}(A) \mid bH \subset dgH\}\\ &= \left\{b \in \operatorname{quot}(A) \mid \frac{b}{d}H \subset gH\right\}\\ &= d\,\{a \in \operatorname{quot}(A) \mid aH \subset gH\}\\ &= d\left(gH :_{\operatorname{quot}(A)} H\right),\end{aligned}$$

which proves the claim. ■

Note that, in the setup of the algorithm, in every step, d can be chosen to be a power of g.

Example 8.5.6 *Continuing Example 8.5.4 we write J_1 as an A-module*

$$J_1 = \frac{1}{\bar{x}}\left\langle \bar{x}^2, \bar{x}\bar{y}(\bar{y}-1), \bar{y}(\bar{y}-1)^2\right\rangle = \frac{1}{d}H_1$$

with $d = \bar{x}$ and $H_1 = \langle \bar{x}^2, \bar{x}\bar{y}(\bar{y}-1), \bar{y}(\bar{y}-1)^2\rangle \subset A$.

Using the test pair $(J_1, \bar{x})$ *and applying Theorem 8.5.5 and Lemma 8.5.3, we get*

$$\frac{1}{\bar{x}}(\bar{x}J_1 :_{A_1} J_1) = \frac{1}{\bar{x}^2}(\bar{x}^2 H_1 :_A H_1) = \frac{1}{\bar{x}^2}\left\langle \bar{x}^2, \bar{x}\bar{y}(\bar{y}-1), \bar{y}(\bar{y}-1)^2 \right\rangle$$
$$=_A \left\langle 1, \frac{\bar{y}(\bar{y}-1)}{\bar{x}}, \frac{\bar{y}(\bar{y}-1)^2}{\bar{x}^2} \right\rangle$$

and

$$\begin{array}{rcl} A_2 := A[t_1,t_2]/I_2 & \cong & {}_A\left\langle 1, \frac{\bar{y}(\bar{y}-1)}{\bar{x}}, \frac{\bar{y}(\bar{y}-1)^2}{\bar{x}^2} \right\rangle \\ \bar{t}_1 & \mapsto & \frac{\bar{y}(\bar{y}-1)^2}{\bar{x}^2} \\ \bar{t}_2 & \mapsto & \frac{\bar{y}(\bar{y}-1)}{\bar{x}} \end{array}$$

with

$$I_2 = \langle t_1\bar{x} - t_2(\bar{y}-1),\ -t_2\bar{x} + \bar{y}(\bar{y}-1),\ t_1\bar{y}(\bar{y}-1) + \bar{x}^2,\ t_1\bar{y}^2(\bar{y}-1)^2 + t_2\bar{x}^3,$$
$$t_1^2 + (\bar{y}-1),\ t_1t_2 + \bar{x}, t_2^2 - t_2\bar{y}\rangle$$

In the final step, we find that A_2 *is normal, so that* $\overline{A} = A_2$.

Example 8.5.7 *The normalization algorithm described above, is available in* SINGULAR. *In fact, this is the first implementation of a normalization algorithm which is practically useable. We apply it to the coordinate ring of the curve from Example 8.5.6:*

```
LIB "normal.lib";
ring R = 0,(x,y),dp;
ideal I = x^4+y^2*(y-1)^3;
list nor = normal(I);
def R1 = nor[1][1];
setring R1;
norid;
norid[1]=T(1)*x-T(2)*y+T(2)
norid[2]=-T(2)*x+y^2-y
norid[3]=T(1)*y^2-T(1)*y+x^2
norid[4]=T(1)*y^4-2*T(1)*y^3+T(1)*y^2+T(2)*x^3
norid[5]=T(1)^2+y-1
norid[6]=T(1)*T(2)+x
norid[7]=T(2)^2-T(1)*y
norid[8]=y^5+x^4-3*y^4+3*y^3-y^2
normap;
normap[1]=x
normap[2]=y
```

We verify that the normalization of the given curve is indeed smooth:

```
std(slocus(norid));
_[1]=1
```

8.6 Exercises

Exercise 8.1 *Determine the normalization of the singularity of type A_k defined by the ideal*

$$\left\langle y^2 - x^{k+1} \right\rangle \subset K[x, y]$$

for $k \geq 2$ even.

Exercise 8.2 *Let $R = K[x, y]$ and let*

$$I = \left\langle y^k - x^k + x^{k+1} \right\rangle \subset R$$

be the ideal of an ordinary k-fold point, where $k \geq 2$. For $A = R/I$ determine A-module generators of $\overline{A}$.

Exercise 8.3 *Determine the normalization of the Whitney umbrella $X = V(I) \subset \mathbb{A}^3$*

$$I = \left\langle x^2 - y^2 z \right\rangle \subset K[x, y, z]$$

(see Figure 3.4).

Exercise 8.4 *For the Steiner surface $X = V(I) \subset \mathbb{A}^3$*

$$I = \left\langle x^2 y^2 + x^2 z^2 + y^2 z^2 - xyz \right\rangle \subset K[x, y, z]$$

(see Figure 3.5) determine A-module generators of $\overline{A}$ where $A = K[x, y, z]/I$.

Index

Bibliography

[1] Atiyah, M. F.; MacDonald, I. G.: *Introduction to commutative algebra* (1969).

[2] The Axiom Group: *Axiom*, http://www.axiom-developer.org/ (2012).

[3] Bosma, W.; Cannon J.; Playoust C.: *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), 235–265.

[4] Decker, W.; Greuel, G.-M.; Pfister, G.; Schönemann, H.: SINGULAR *3-1-5 — A computer algebra system for polynomial computations*, available at http://www.singular.uni-kl.de (2012).

[5] Eisenbud, D.: *Commutative Algebra with a View Toward Algebraic Geometry*. Springer (1995).

[6] Endrass, S.: *Surf*, http://surf.sourceforge.net

[7] Grayson, D. R.; Stillman, M. E.: *Macaulay2, a software system for research in algebraic geometry*, available at http://www.math.uiuc.edu/Macaulay2/ (2009).

[8] Greuel, G.-M.; Meyer, H.; Stussak, Ch.: *Surfer*, http://www.imaginary-exhibition.com/surfer.php (2008).

[9] Greuel, G.-M.; Pfister, G: A Singular introduction to commutative algebra, Springer (2002).

[10] Hearn, A. C.: *REDUCE 3.8*, available at http://reduce-algebra.com/ (2009).

[11] Herzog, J.; Hibi, T.: *Monomial ideals*, Springer (2011).

[12] Maple (Waterloo Maple Inc.): *Maple 16*, http://www.maplesoft.com/ (2012).

[13] Maxima: *Maxima, a Computer Algebra System*. Version 5.25.1, available at http://maxima.sourceforge.net/ (2011).

[14] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.5.6*, available at http://www.gap-system.org (2012).

[15] The PARI-Group, *PARI/GP, version 2.5.3*, available at http://pari.math.u-bordeaux.fr/ (2012).

[16] Wolfram Research, Inc.: *Mathematica Edition: Version 7.0* (2008).