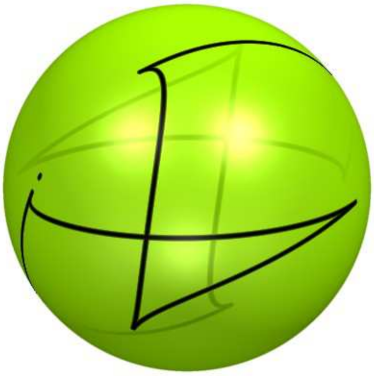
A First Course in Computational Algebraic Geometry

Wolfram Decker and Gerhard Pfister

– With Pictures by Oliver Labs –



Contents

Preface

Most of mathematics is concerned at some level with setting up and solving various types of equations. Algebraic geometry is the mathematical discipline which handles solution sets of systems of polynomial equations. These are called algebraic sets.

Making use of a correspondence which relates algebraic sets to ideals in polynomial rings, problems concerning the geometry of algebraic sets can be translated into algebra. As a consequence, algebraic geometers have developed a multitude of often highly abstract techniques for the qualitative and quantitative study of algebraic sets, without, in the first instance, considering the equations. Modern computer algebra algorithms, on the other hand, allow us to manipulate the equations and, thus, to study explicit examples. In this way, algebraic geometry becomes accessible to experiments. The experimental method, which has proven to be highly successful in number theory, is now also added to the toolbox of the algebraic geometer.

In these notes, we discuss some of the basic operations in geometry and describe their counterparts in algebra. We explain how the operations can be carried through using computer algebra methods, and give a number of explicit examples, worked out with the computer algebra system SINGULAR. In this way, our book may serve as a first introduction to SINGULAR, guiding the reader to performing his own experiments.

In detail, we proceed along the following lines:

Chapter 0 contains remarks on computer algebra systems in general and just a few examples of what can be computed in different application areas.

In Chapter 1, we focus on the geometry–algebra dictionary, illustrating its entries by including a number of Singular examples.

Chapter 2 contains a discussion of the algorithms involved and gives a more thorough introduction to Singular.

For the fun of it, in Chapter 3, we show how to find the solution of a well–posed Sudoku by solving a corresponding system of polynomial equations.

Finally, in Chapter 4, we discuss a particular classification problem in group theory, and explain how a combination of theory and explicit computations has led to a solution of the problem. Here, algorithmic methods from group theory, number theory, and algebraic geometry are involved.

Due to the expository character of these notes, proofs are only included occasionally. For all other proofs, references are given.

For a set of Exercises, see

`http://www.mathematik.uni-kl.de/∼pfister/Exercises.pdf`.

The notes grew out of a course we taught at the African Institute for the Mathematical Sciences (AIMS) in Cape Town, South Africa. Teaching at AIMS was a wonderful experience and we would like to thank all the students for their enthusiasm and the fun we had together. We very much appreciated the facilities at AIMS and we are grateful to its staff for constant support.

We thank Oliver Labs for contributing the illustrations along with hints on improving the text, Christian Eder and Stefan Steidel for reading parts of the manuscript and making helpful suggestions, and Petra Bäsell for typesetting the notes.

Kaiserslautern, *Wolfram Decker*
October 2011 *Gerhard Pfister*

0
General Remarks on Computer Algebra Systems

Computer algebra algorithms allow us to compute in and with a multitude of mathematical structures. Accordingly, there is a large number of computer algebra systems suiting different needs. There are general purpose and special purpose computer algebra systems. Some well–known general purpose systems are commercial, whereas many of the special purpose systems are open–source and can be downloaded from the internet for free. General purpose systems aim at providing basic functionality for a variety of different application areas. In addition to tools for symbolic computation, they usually offer tools for numeric computation and for visualization.

Example 0.1 Maple is a commercial general purpose system. In showing a few of its commands at work, we start with examples from calculus, namely definite and indefinite integration:

```
> int(sin(x), x = 0 .. Pi);
                              2
> int(x/(x^2-1), x);
            1/2 ln(x - 1) + 1/2 ln(x + 1)
```

For linear algebra applications, we first load the corresponding package. Then we demonstrate how to perform Gaussian elimination and how to compute eigenvalues, respectively.

```
with(LinearAlgebra);
A := Matrix([[2, 1, 0], [1, 2, 1], [0, 1, 2]]);
```

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

```
GaussianElimination(A);
```

$$\begin{bmatrix} 2 & 1 & 0 \\ 0 & 3/2 & 1 \\ 0 & 0 & 4/3 \end{bmatrix}$$

```
Eigenvalues(A);
```

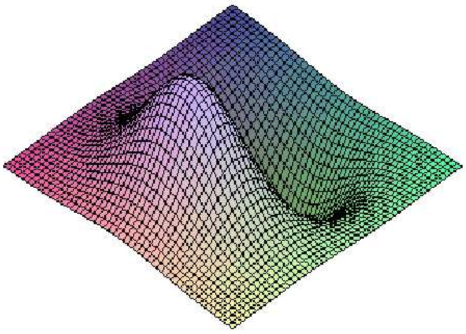
$$\begin{bmatrix} 2 \\ 2-\sqrt{2} \\ 2+\sqrt{2} \end{bmatrix}$$

Next, we give an example of numerical solving†:

```
> fsolve(2*x^5-11*x^4-7*x^3+12*x^2-4*x = 0);
                   -1.334383488, 0., 5.929222024
```

Finally, we show one of the graphic functions at work:

```
> plot3d(x*exp(-x^2-y^2),x = -2 .. 2,y = -2 .. 2,grid = [49, 49]);
```



For applications in research, general purpose systems are often not powerful enough: The implementation of the required basic algorithms may not be optimal with respect to speed and storage handling, and more advanced algorithms may not be implemented

† Note that only the real roots are computed.

at all. Many special purpose systems have been created by people working in a field other than computer algebra and having a desperate need for computing power in the context of some of their research problems. A pioneering and prominent example is Veltman's Schoonship which helped to win a Nobel price in physics in 1999 (awarded to Veltman and t'Hooft 'for having placed particle physics theory on a firmer mathematical foundation').

Example 0.2 GAP is a free open–source system for computational discrete algebra, with particular emphasis on Computational Group Theory. In the following GAP session, we define a subgroup G of the symmetric group S_{11} (the group of permutations of $\{1, \ldots, 11\}$) by giving two generators in cycle[†] notation. We check that G is simple (that is, its only normal subgroups are the trivial subgroup and the whole group itself). Then we compute the order $|G|$ of G, and factorize this number:

```
gap> G := Group([(1,2,3,4,5,6,7,8,9,10,11),(3,7,11,8)(4,10,5,6)]);
Group([(1,2,3,4,5,6,7,8,9,10,11), (3,7,11,8)(4,10,5,6)])
gap> IsSimple(G);
true
gap> size := Size(G);
7920
gap> Factors(size);
[ 2, 2, 2, 2, 3, 3, 5, 11 ]
```

From the factors, we see that G has a Sylow 2–subgroup[‡] of order $2^4 = 16$. We use GAP to find such a group P:

```
gap> P := SylowSubgroup(G, 2);


Group([(2,8)(3,4)(5,6)(10,11), (3,5)(4,6)(7,9)(10,11),
     (2,4,8,3)(5,10,6,11)])
```

Making use of the *Small Groups Library* included in GAP, we check that, up to isomorphism, there are 14 groups of order 16, and that P is the 8th group of order 16 listed in this library:

[†] The cycle (4,10,5,6), for instance, maps 4 to 10, 10 to 5, 5 to 6, 6 to 4, and any other number to itself.

[‡] If G is a finite group, and p is a prime divisor of its order $|G|$, then a subgroup U of G is called a *Sylow p–subgroup* if its order $|U|$ is the highest power of p dividing $|G|$.

```
gap> SmallGroupsInformation(16);
 There are 14 groups of order 16.
 They are sorted by their ranks.
    1 is cyclic.
    2 - 9 have rank 2.
    10 - 13 have rank 3.
    14 is elementary abelian.
gap> IdGroup( P );
[ 16, 8 ]
```

Now, we determine what group P is. First, we check that P is neither Abelian nor the dihedral group of order 16 (the *dihedral group* of order $2n$ is the symmetry group of the regular n–gon):

```
gap> IsAbelian(P);
false
gap> IsDihedralGroup(P);
false
```

Further information on P is obtained by studying the subgroups of P of order 8. In fact, we consider the third such subgroup returned by GAP and name it H:

```
gap> H := SubgroupsOfIndexTwo(P)[3];
Group([(2,3,11,5,8,4,10,6)(7,9), (2,4,11,6,8,3,10,5)(7,9),
     (2,5,10,3,8,6,11,4)(7,9), (2,6,10,4,8,5,11,3)(7,9)])
gap> IdGroup(H);
[ 8, 1 ]
gap> IsCyclic(H);
true
```

Thus, H is the cyclic group C_8 of order 8 (*cyclic groups* are generated by just one element). Further checks show, in fact, that P is a semidirect product of C_8 and the cyclic group C_2. See [Wild (2005)] for the classification of groups of order 16.

Remark 0.3 The group G studied in the previous example is known as the *Mathieu group* M_{11}. We should point out that researchers in group and representation theory have created quite a number of useful electronic libraries such as the *Small Groups Library* considered above.

Example 0.4 Magma is a commercial system focussing on algebra, number theory, geometry and combinatorics. We use it to factorize the 8th Fermat number:

```
> Factorization(2^(2^8)+1);
[<1238926361552897,1>,
<93461639715357977769163558199606896584051237541638188580280321,1>]
```

Next, we meet our first example of an algebraic set: In *Weierstraß normal form*, an *elliptic curve* over a field K is a nonsingular† curve in the xy–plane defined by one polynomial equation of type

$$y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0,$$

with coefficients $a_i \in K$. In the following Magma session, we define an elliptic curve E in Weierstraß normal form over the finite field F with 5^{90} elements by specifying the coefficients a_i. Then we count the number of points on E with coordinates in F.

```
F := FiniteField(5,90);
E := EllipticCurve([Zero(F),Zero(F),One(F),-One(F),Zero(F)]);
E;
Elliptic Curve defined by y^2 + y = x^3 + 4*x over GF(5^90)
#E;
807793566946316088741610050849537214477762546152780718396696352
```

The significance of elliptic curves stems from the fact that they carry an (additive) group law. Having specified a base point (the zero element of the group), the addition of points is defined by a geometric construction involving secant and tangent lines. For elliptic curves in Weierstraß normal form, it is convenient to choose the unique point at infinity of the curve as the base point (see Section 1.2.1 for points at infinity and Example 0.6 below for a demonstration of the group law).

Remark 0.5 Elliptic curves, most notably elliptic curves defined over $\mathbb{Q}$ respectively over a finite field, are of particular importance in number theory. They take center stage in the conjecture of [Birch and Swinnerton–Dyer (1965)] ‡, they are key ingredients

† Informally, a curve is nonsingular if it admits a unique tangent line at each of its points. See, for instance, [Silverman (2009)] for a formal definition and for more information on elliptic curves.

‡ The Birch and Swinnerton–Dyer conjecture asserts, in particular, that an elliptic curve E over $\mathbb{Q}$ has an infinite number of points with rational coordinates iff its associated L–series satisfies $L(E, 1) = 0$.

in the proof of Fermat's last theorem [Wiles (1995)], they are important for integer factorization [Lenstra (1987)], and they find applications in cryptography [Koblitz (1987)]. As with other awesome conjectures in number theory, the Birch and Swinnerton–Dyer conjecture is based on computer experiments.

Example 0.6 Sage is a free open–source mathematics software system which combines the power of many existing open–source packages into a common Python–based interface. To show it at work, we start as in Example 0.1 with computations from calculus. Then, we compute all prime numbers between two given numbers.

```
sage: limit(sin(x)/x, x=0)
1
sage: taylor(sqrt(x+1), x, 0, 5)
7/256*x^5 - 5/128*x^4 + 1/16*x^3 - 1/8*x^2 + 1/2*x + 1
sage: list(primes(10000000000, 10000000100))
[10000000019, 10000000033, 10000000061, 10000000069, 10000000097]
```

Finally, we define an elliptic curve E in Weierstraß normal form over $\mathbb{Q}$ and demonstrate the group law on this curve. The representation of the results takes infinity into account in the sense that the points are given by their homogeneous coordinates in the projective plane (see Section 1.2 for the projective setting). In particular, $(0 : 1 : 0)$ denotes the unique point at infinity of the curve which is chosen to be the zero element of the group.

```
sage: E = EllipticCurve([0,0,1,-1,0])
sage: E
Elliptic Curve defined by y^2 + y = x^3 - x over Rational Field
sage: P = E([0,0])
sage: P
(0 : 0 : 1)
sage: O = P - P
sage: O
(0 : 1 : 0)
sage: Q = E([-1,0])
sage: Q
(-1 : 0 : 1)
sage: Q + O
(-1 : 0 : 1)
sage: P + Q - (P+Q)
(0 : 1 : 0)
Q + (P + R) - ((Q + P) + R)
(0 : 1 : 0)
```

Among the systems combined by Sage are Maxima, a general purpose system which is free and open–source, GAP, the system introduced in Example 0.2, PARI/GP, a system for number theory, and Singular, the system featured in these notes.

Singular is a free open–source system for polynomial computations, with special emphasis on commutative and noncommutative algebra, algebraic geometry, and singularity theory. As most other systems, Singular consists of a precompiled kernel, written in C/C++, and additional packages, called libraries and written in the C–like Singular user language. This language is interpreted on runtime. Singular binaries are available for most common hardware and software platforms. Its release versions can be downloaded through `ftp` from

`ftp://www.mathematik.uni-kl.de/pub/Math/Singular/`

or via your favourite webbrowser from Singular's webpage

`http://www.singular.uni-kl.de/` .

Singular also provides an extensive online manual and help function. See its webpage or enter `help;` in a Singular session.

Most algorithms implemented in Singular rely on the basic task of computing Gröbner bases. Gröbner bases are special sets of generators for ideals in polynomial rings. Their definition and computation is subject to the choice of a monomial ordering such as the *lexicographical ordering* $>_{\mathrm{lp}}$ and the *degree reverse lexicographical ordering* $>_{\mathrm{dp}}$. We will treat Gröbner bases and their computation by Buchberger's algorithm in Chapter 2. Singular examples, however, will already be presented beforehand.

Singular Example 0.7 We enter the polynomials of the system

$$\begin{array}{lcl} x+y+z-1 & = & 0 \\ x^2+y^2+z^2-1 & = & 0 \\ x^3+y^3+z^3-1 & = & 0 \end{array}$$

in a Singular session. For this, we first have to define the corresponding polynomial ring which is named R and endowed with the lexicographical ordering. Note that the 0 in the definition of R refers to the prime field of characteristic zero, that is, to $\mathbb{Q}$.

```
> ring R = 0, (x,y,z), lp;
> poly f1 = x+y+z-1;
> poly f2 = x2+y2+z2-1;
> poly f3 = x3+y3+z3-1;
```

Next, we define the ideal generated by the polynomials and compute a Gröbner basis for this ideal (the system given by the Gröbner basis elements has the same solutions as the original system).

```
> ideal I = f1, f2, f3;
> ideal GI = groebner(I);  GI;
GI[1]=z3-z2
GI[2]=y2+yz-y+z2-z
GI[3]=x+y+z-1
```

In the first equation of the new system, the variables x and y are eliminated. In the second equation, x is eliminated. As a consequence, the solutions can, now, be directly read off:

$$(1,0,0),\ (0,1,0),\ (0,0,1).$$

The example indicates that $>_{\mathrm{lp}}$ is what we will call an *elimination ordering*. If such an ordering is chosen, Buchberger's algorithm generalizes Gaussian elimination. For most applications of the algorithm, however, the elimination property is not needed. It is, then, usually more efficient to choose the ordering $>_{\mathrm{dp}}$.

Multivariate polynomial factorization is another basic task on which some of the more advanced algorithms in Singular rely. Starting with the first computer algebra systems in the 1960's, the design of algorithms for polynomial factorization has always been an active area of research. To keep the size of our notes within reasonable limits, we will not treat this here. We should point out, however, that algorithms for polynomial factorization do not depend on monomial orderings. Nevertheless, choosing such an ordering is always part of a ring definition in SINGULAR.

Singular Example 0.8 We factorize a polynomial in $\mathbb{Q}[x, y, z]$ using the SINGULAR command `factorize`. The resulting output is a list, showing as a first entry the factors, and as a second entry the corresponding multiplicities.

```
> ring R = 0, (x,y,z), dp;
> poly f = -x7y4+x6y5-3x5y6+3x4y7-3x3y8+3x2y9-xy10+y11-x10z
. +x8y2z+9x6y4z+11x4y6z+4x2y8z-3x5y4z2+3x4y5z2-6x3y6z2+6x2y7z2
. -3xy8z2+3y9z2-3x8z3+6x6y2z3+21x4y4z3+12x2y6z3-3x3y4z4+3x2y5z4
. -3xy6z4+3y7z4-3x6z5+9x4y2z5+12x2y4z5-xy4z6+y5z6-x4z7+4x2y2z7;
> factorize(f);
[1]:
   _[1]=-1
   _[2]=xy4-y5+x4z-4x2y2z
   _[3]=x2+y2+z2
[2]:
   1,1,3
```

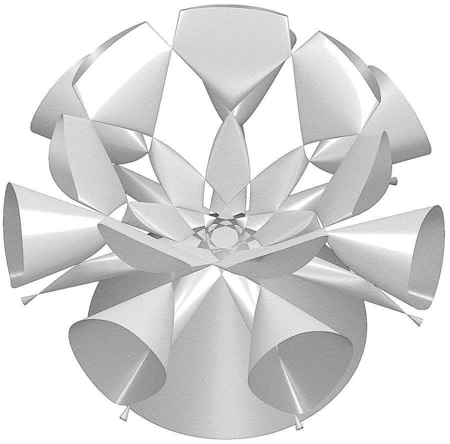
Remark 0.9 In recent years, quite a number of the more abstract concepts in algebraic geometry have been made constructive. They are, thus, not only easier to understand, but also accessible to computer algebra methods. A prominent example is the desingularization theorem of Hironaka (see [Hironaka (1964)]) for which Hironaka received the Fields Medal. In fact, Villamajor's constructive version of Hironaka's proof has led to an algorithm whose SINGULAR implementation allows us to resolve singularities in many cases of interest (see [Bierstone and Milman (1997)], [Frühbis–Krüger and Pfister (2006)], [Bravo et al. (2005)]).

When studying plane curves or surfaces in 3–space, it is often desirable to visualize the geometric objects under consideration. Excellent tools for this are SURF and its descendants SURFEX† and SURFER‡. Comparing SURFEX and SURFER, we should note that SURFEX has more features, whereas SURFER is easier to handle.

† `http://surf.sourceforge.net`

‡ `http://www.oliverlabs.net/welcome.php`

Example 0.10 The following Surfer picture shows a surface in 3–space found by Oliver Labs using Singular:



Singular Example 0.11 We set up the equation of Labs' surface in Singular. The equation is defined over a finite extension field of $\mathbb{Q}$ which we implement by entering its minimal polynomial:

```
> ring R = (0,a), (x,y,w,z), dp;
> minpoly = a^3 + a + 1/7;
> poly a(1) = -12/7*a^2 - 384/49*a - 8/7;
> poly a(2) = -32/7*a^2  + 24/49*a   - 4;
> poly a(3) =    -4*a^2  + 24/49*a   - 4;
> poly a(4) =  -8/7*a^2   + 8/49*a - 8/7;
> poly a(5) =    49*a^2      - 7*a  + 50;
> poly P = x*(x^6-3*7*x^4*y^2+5*7*x^2*y^4-7*y^6)
. +7*z*((x^2+y^2)^3-2^3*z^2*(x^2+y^2)^2
. +2^4*z^4*(x^2+y^2))-2^6*z^7;
> poly C = a(1)*z^3+a(2)*z^2*w+a(3)*z*w^2+a(4)*w^3+(z+w)*(x^2+y^2);
> poly S = P-(z+a(5)*w)*C^2;
> homog(S);  // returns 1 if poly is homogeneous
1
> deg(S);
7
```

We see that `S` is a homogeneous polynomial of degree 7. It defines Labs' surface in *projective* 3–space. This surface is a 'world record' surface in that it has the maximal number of nodes known for a degree–7 surface in projective 3–space (a node constitutes the most simple type of a singularity). We use Singular to confirm that there are precisely 99 nodes (and no other singularities).

First, we compute the dimension of the locus of singularities via the Jacobian criterion (see [Decker and Schreyer (2013)] for the criterion and Sections 1.1.8 and 2.3 for more on dimension):

```
> dim(groebner(jacob(S)))-1;
0
```

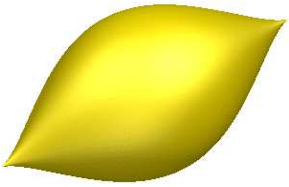
The result means that there are only finitely many singularities. By checking that the nonnodal locus is empty, we verify that all singularities are nodes. Then, we compute the number of nodes:

```
> dim(groebner(minor(jacob(jacob(S)),2))) - 1;
-1
> mult(groebner(jacob(S)));
99
```

Singular Example 0.12 If properly installed, Surf, Surfex, and Surfer can be called from Singular. To give an example, we use Surfer to plot a surface which, as it turns out, resembles a citrus. To begin, we load the Singular library connecting to Surf and Surfer.

```
> LIB "surf.lib";
> ring R = 0, (x,y,z), dp;
> ideal I = 6/5*y^2+6/5*z^2-5*(x+1/2)^3*(1/2-x)^3;
surfer(I);
```

The resulting picture will show in a popup–window:



See http://www.imaginary-exhibition.com for more pictures.

1
The Geometry–Algebra Dictionary

In this chapter, we will explore the correspondence between algebraic sets in affine and projective space and ideals in polynomial rings. More details and all proofs not given here can be found in [Decker and Schreyer (2013)]. We will work over a field K, and write $K[x_1, \dots, x_n]$ for the polynomial ring over K in n variables. All rings considered are commutative with identity element 1.

1.1 Affine Algebraic Geometry

Our discussion of the geometry–algebra dictionary starts with Hilbert's basis theorem which is the fundamental result about ideals in polynomial rings. Then, focusing on the affine case, we present some of the basic ideas of algebraic geometry, with particular emphasis on computational aspects.

1.1.1 Ideals in Polynomial Rings

To begin, let R be any ring.

Definition 1.1 *A subset $I \subset R$ is called an **ideal** of R if the following holds:*

(i) $0 \in I$.
(ii) *If $f, g \in I$, then $f + g \in I$.*
(iii) *If $f \in R$ and $g \in I$, then $f \cdot g \in I$.*

Example 1.2

(i) If $\emptyset \neq T \subset R$ is any subset, then all R–linear combinations $g_1f_1 + \cdots + g_rf_r$, with $g_1, \ldots .g_r \in R$ and $f_1, \ldots, f_r \in T$, form an ideal of R, written $\langle T \rangle_R$ or $\langle T \rangle$, and called the ideal **generated by *T***. We also say that T is a **set of generators** for the ideal. If $T = \{f_1, \ldots, f_r\}$ is finite, we write $\langle T \rangle = \langle f_1, \ldots, f_r \rangle$. We say that an ideal is **finitely generated** if it admits a finite set of generators. A **principal ideal** can be generated by just one element.

(ii) If $\{I_\lambda\}$ is a family of ideals of R, then the intersection $\bigcap_\lambda I_\lambda$ is also an ideal of R.

(iii) The **sum** of a family of ideals $\{I_\lambda\}$ of R, written $\sum_\lambda I_\lambda$, is the ideal generated by the union $\bigcup_\lambda I_\lambda$.

Now, we turn to $R = K[x_1, \ldots, x_n]$.

Theorem 1.3 (Hilbert's Basis Theorem) *Every ideal of the polynomial ring $K[x_1, \ldots, x_n]$ is finitely generated.*

Starting with Hilbert's original proof [Hilbert (1890)], quite a number of proofs for the basis theorem have been given (see, for instance, [Greuel and Pfister (2007)] for a brief proof found in the 1970s). A proof which nicely fits with the spirit of these notes is due to Gordan [Gordan (1899)]. Though the name Gröbner bases was coined much later by Buchberger†, it is Gordan's paper in which these bases make their first appearance. In fact, Gordan already exhibits the key idea behind Gröbner bases which is to reduce problems concerning arbitrary ideals in polynomial rings to problems concerning monomial ideals. The latter problems are usually much easier.

Definition 1.4 *A* ***monomial*** *in $x_1, \ldots, x_n$ is a product $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, where $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. A* ***monomial ideal*** *of $K[x_1, \ldots, x_n]$ is an ideal generated by monomials.*

† Gröbner was Buchberger's thesis advisor. In his thesis, Buchberger developed his algorithm for computing Gröbner bases. See [Buchberger (1965)].

The first step in Gordan's proof of the basis theorem is to show that monomial ideals are finitely generated (somewhat mistakenly, this result is often assigned to Dickson):

Lemma 1.5 (Dickson's Lemma) *Let $\emptyset \neq A \subset \mathbb{N}^n$ be a subset of multi–indices, and let I be the ideal $I = \langle x^\alpha \mid \alpha \in A\rangle$. Then there exist $\alpha^{(1)}, \dots, \alpha^{(r)} \in A$ such that $I = \langle x^{\alpha^{(1)}}, \dots, x^{\alpha^{(r)}}\rangle$.*

Proof We do induction on n, the number of variables. If $n = 1$, let $\alpha^{(1)} := \min\{\alpha \mid \alpha \in A\}$. Then $I = \langle x^{\alpha^{(1)}}\rangle$. Now, let $n > 1$ and assume that the lemma holds for $n-1$. Given $\alpha = (\overline{\alpha}, \alpha_n) \in \mathbb{N}^n$, with $\overline{\alpha} = (\alpha_1, \dots, \alpha_{n-1}) \in \mathbb{N}^{n-1}$, we write $\overline{x}^{\overline{\alpha}} = x_1^{\alpha_1} \cdots x_{n-1}^{\alpha_{n-1}}$.

Let $\overline{A} = \{\overline{\alpha} \in \mathbb{N}^{n-1} \mid (\overline{\alpha}, i) \in A \text{ for some } i\}$, and let $J = \langle\{\overline{x}^{\overline{\alpha}}\}_{\overline{\alpha}\in\overline{A}}\rangle \subset K[x_1, \dots, x_{n-1}]$. By the induction hypothesis, there exist multi–indices $\beta^{(1)} = (\overline{\beta}^{(1)}, \beta_n^{(1)}), \dots, \beta^{(s)} = (\overline{\beta}^{(s)}, \beta_n^{(s)}) \in A$ such that $J = \langle \overline{x}^{\overline{\beta}^{(1)}}, \dots, \overline{x}^{\overline{\beta}^{(s)}}\rangle$. Let $\ell = \max_j\{\beta_n^{(j)}\}$. For $i = 0, \dots, \ell$, let $\overline{A}_i = \{\overline{\alpha} \in \mathbb{N}^{n-1} \mid (\overline{\alpha}, i) \in A\}$ and $J_i = \langle\{\overline{x}^{\overline{\alpha}}\}_{\overline{\alpha}\in\overline{A}_i}\rangle \subset K[x_1, \dots, x_{n-1}]$. Using once more the induction hypothesis, we get $\beta_i^{(1)} = (\overline{\beta}_i^{(1)}, i), \dots, \beta_i^{(s_i)} = (\overline{\beta}_i^{(s_i)}, i) \in A$ such that $J_i = \langle \overline{x}^{\overline{\beta}_i^{(1)}}, \dots, \overline{x}^{\overline{\beta}_i^{(s_i)}}\rangle$. Let

$$B = \bigcup_{i=0}^{\ell} \{\beta_i^{(1)}, \dots, \beta_i^{(s_i)}\}.$$

Then, by construction, every monomial $x^\alpha, \alpha \in A$, is divisible by a monomial $x^\beta, \beta \in B$. Hence, $I = \langle\{x^\beta\}_{\beta\in B}\rangle$. □

In Corollary 2.28, we will follow Gordan and use Gröbner bases to deduce the basis theorem from the special case treated above.

Theorem 1.6 *Let R be a ring. The following are equivalent:*

(i) *Every ideal of R is finitely generated.*

(ii) ***(Ascending Chain Condition)*** *Every chain*

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

of ideals of R is eventually stationary. That is,

$$I_k = I_{k+1} = I_{k+2} = \dots \quad \textit{for some} \quad k \geq 1.$$

Definition 1.7 *A ring satisfying the equivalent conditions above is called a* ***Noetherian ring.***

Finally, we introduce the following terminology for later use:

Definition 1.8 *We say that an ideal I of R is a* **proper ideal** *if $I \neq R$. A proper ideal $\mathfrak{p}$ of R is a* **prime ideal** *if $f, g \in R$ and $fg \in \mathfrak{p}$ implies $f \in \mathfrak{p}$ or $g \in \mathfrak{p}$. A proper ideal $\mathfrak{m}$ of R is a* **maximal ideal** *if there is no ideal I of R such that $\mathfrak{m} \subsetneqq I \subsetneqq R$.*

1.1.2 Affine Algebraic Sets

Following the usual habit of algebraic geometers, we write $\mathbb{A}^n(K)$ instead of K^n: The **affine n–space** over K is the set

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

Each polynomial $f \in K[x_1, \dots, x_n]$ defines a function

$$f : \mathbb{A}^n(K) \to K,\ (a_1, \dots, a_n) \mapsto f(a_1, \dots, a_n),$$

which is called a **polynomial function** on $\mathbb{A}^n(K)$. Viewing f as a function allows us to talk about the zeros of f. More generally, we define:

Definition 1.9 *If $T \subset K[x_1, \dots, x_n]$ is any set of polynomials, its* ***vanishing locus*** *(or* ***locus of zeros****) in $\mathbb{A}^n(K)$ is the set*

$$\mathrm{V}(T) = \{p \in \mathbb{A}^n(K) \mid f(p) = 0 \text{ for all } f \in T\}.$$

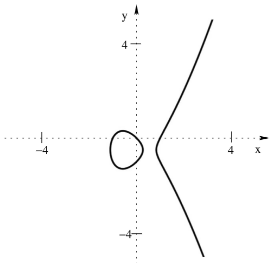
Every such set is called an ***affine algebraic set****.*

It is clear that $\mathrm{V}(T)$ coincides with the vanishing locus of the ideal $\langle T \rangle$ generated by T. Consequently, every algebraic set A in $\mathbb{A}^n(K)$ is of type $\mathrm{V}(I)$ for some ideal I of $K[x_1, \dots, x_n]$. By Hilbert's basis theorem, A is the vanishing locus $\mathrm{V}(f_1, \dots, f_r) = \bigcap_{i=1}^r \mathrm{V}(f_i)$ of a set of finitely many polynomials $f_1, \dots, f_r$. Referring to the vanishing locus of a single nonconstant polynomial as a **hypersurface** in $\mathbb{A}^n(K)$, this means that a subset of $\mathbb{A}^n(K)$ is algebraic iff it can be written as the intersection of finitely many hypersurfaces. Hypersurfaces in $\mathbb{A}^2(K)$ are called **plane curves**.

Example 1.10 We choose $K = \mathbb{R}$ so that we can draw pictures.

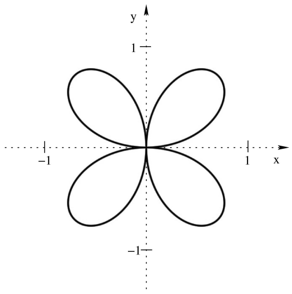
(i) Nondegenerate conics (ellipses, parabolas, hyperbolas) are well–known examples of plane curves. They are defined by degree–2 equations such as $x^2 + y^2 - 1 = 0$.

(ii) As discussed in Example 0.4, elliptic plane curves are defined by degree–3 equations. Here is the real picture of the elliptic curve from Example 0.6:



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

(iii) The four–leaf clover below is given by a degree–6 equation:



$$\left(x^2 + y^2\right)^3 - 4x^2y^2 = 0$$

(iv) The plane curve with degree–5 equation

$$\begin{aligned}&49x^3y^2 - 50x^2y^3 - 168x^3y + 231x^2y^2 - 60xy^3\\&+144x^3 - 240x^2y + 111xy^2 - 18y^3\\&+16x^2 - 40xy + 25y^2 = 0\end{aligned}$$

admits the rational parametrization†

$$x(t) = \frac{g_1(t)}{h(t)}, \quad y(t) = \frac{g_2(t)}{h(t)}$$

† See Definition 1.67 for rational parametrizations. The parametrization here was found using the Singular library `paraplanecurves.lib`.

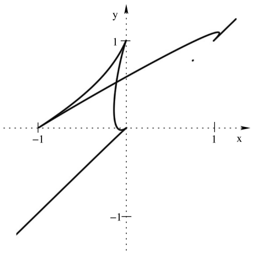
with

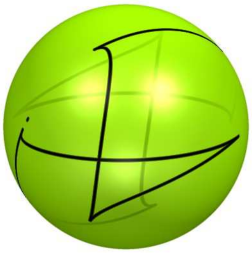
$$\begin{aligned}
g_1(t) &= -1200t^5 - 11480115t^4 - 19912942878t^3 \\
&\quad +272084763096729t^2 + 131354774678451636t \\
&\quad +1562048851670457 7428,
\end{aligned}$$

$$\begin{aligned}
g_2(t) &= 1176t^5 - 11957127t^4 - 18673247712t^3 \\
&\quad +329560549623774t^2 + 158296652767188936t \\
&\quad -1874585949429456255447,
\end{aligned}$$

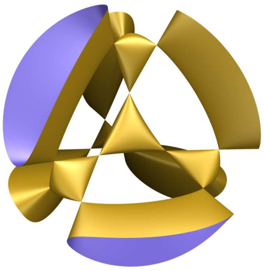
$$\begin{aligned}
h(t) &= -45799075t^4 - 336843036810t^3 \\
&\quad -693864026735607t^2 - 274005776716382844t \\
&\quad -303054680866 65272172.
\end{aligned}$$

In addition to showing the curve in the affine plane, we also present a ‘spherical picture’ of the projective closure of the curve (see Section 1.2.3 for the projective closure):





(v) Labs’ septic from Example 0.10 is a hypersurface in 3–space. Another such hypersurface is the Kummer surface:



Depending on a parameter μ, the equation of the Kummer surface is of type

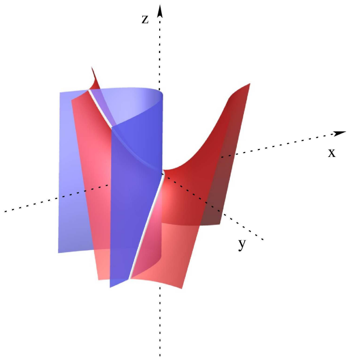
$$\left(x^2+y^2+z^2-\mu^2\right)^2-\lambda\, y_0\, y_1\, y_2\, y_3=0,$$

where the y_i are the tetrahedral coordinates

$$\begin{aligned} y_0 &= 1-z-\sqrt{2}x, & y_1 &= 1-z+\sqrt{2}x,\\ y_2 &= 1+z+\sqrt{2}y, & y_3 &= 1+z-\sqrt{2}y, \end{aligned}$$

and where $\lambda=\frac{3\mu^2-1}{3-\mu^2}$. For the picture, μ was set to be 1.3.

(vi) The **twisted cubic curve** in $\mathbb{A}^3(\mathbb{R})$ is obtained by intersecting the hypersurfaces $\mathrm{V}(y-x^2)$ and $\mathrm{V}(xy-z)$:



Taking vanishing loci defines a map V which sends sets of polynomials to algebraic sets. We summarize the properties of V:

Proposition 1.11

(i) *The map* V *reverses inclusions: If* $I \subset J$ *are subsets of* $K[x_1,\ldots,x_n]$*, then* $\mathrm{V}(I)\supset \mathrm{V}(J)$.

(ii) *Affine space and the empty set are algebraic:*

$$\mathrm{V}(0)=\mathbb{A}^n(K);\quad \mathrm{V}(1)=\emptyset.$$

(iii) *The union of finitely many algebraic sets is algebraic: If* $I_1,\ldots,I_s$ *are ideals of* $K[x_1,\ldots,x_n]$*, then*

$$\bigcup_{k=1}^{s}\mathrm{V}(I_k)=\mathrm{V}(\bigcap_{k=1}^{s} I_k).$$

(iv) *The intersection of any family of algebraic sets is algebraic: If* $\{I_\lambda\}$ *is a family of ideals of* $K[x_1, \ldots, x_n]$, *then*

$$\bigcap_\lambda \mathrm{V}(I_\lambda) = \mathrm{V}\left(\sum_\lambda I_\lambda\right).$$

(v) *A single point is algebraic: If* $a_1, \ldots, a_n \in K$, *then*

$$\mathrm{V}(x_1 - a_1, \ldots, x_n - a_n) = \{(a_1, \ldots, a_n)\}.$$

Proof All properties except (iii) are immediate from the definitions. For (iii), by induction, it suffices to treat the case of two ideals $I, J \subset K[x_1, \ldots, x_n]$. Let $I \cdot J$ be the ideal generated by all products $f \cdot g$, with $f \in I$ and $g \in J$. Then, as is easy to see, $\mathrm{V}(I) \cup \mathrm{V}(J) = \mathrm{V}(I \cdot J)$ and $\mathrm{V}(I) \cup \mathrm{V}(J) \subset \mathrm{V}(I \cap J) \subset \mathrm{V}(I \cdot J)$ (the second inclusion holds since $I \cdot J \subset I \cap J$). The result follows. □

Remark 1.12

(i) Properties (ii)–(iv) above mean that the algebraic subsets of $\mathbb{A}^n(K)$ are the closed sets of a topology on $\mathbb{A}^n(K)$, which is called the **Zariski topology on $\mathbb{A}^n(K)$**.

(ii) If $A \subset \mathbb{A}^n(K)$ is any subset, the intersection of all algebraic sets containing A is the smallest algebraic set containing A. We denote this set by $\overline{A}$. In terms of the Zariski topology, $\overline{A}$ is the closure of A.

(iii) If $A \subset \mathbb{A}^n(K)$ is any subset, the Zariski topology on $\mathbb{A}^n(K)$ induces a topology on A, which is called the **Zariski topology on A**.

(iv) Topological notions such as open, closed, dense, or neighborhood will always refer to the Zariski topology.

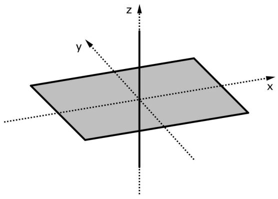
Along with treating the geometry–algebra dictionary, we will state some computational problems for ideals in polynomial rings arising from its entries. These problems are not meant to be attacked by the reader. They rather serve as a motivation for the computational tools developed in Chapter 2, where we will present algorithms to solve the problems. Explicit SINGULAR examples based on the algorithms, however, will already be presented in this chapter.

Problem 1.13 *Give an algorithm to compute ideal intersections.*

Singular Example 1.14

```
> ring R = 0, (x,y,z), dp;
> ideal I = z;  ideal J = x,y;
> ideal K = intersect(I,J);  K;
K[1]=yz
K[2]=xz
```

So $\mathrm{V}(z) \cup \mathrm{V}(x,y) = \mathrm{V}(\langle z\rangle \cap \langle x,y\rangle) = \mathrm{V}(xz,yz)$.



Remark 1.15 The previous example is special in that we consider ideals which are monomial. The intersection of monomial ideals is obtained using a simple recipe: Given $I = \langle m_1,\dots,m_r\rangle$ and $J = \langle m'_1,\dots,m'_s\rangle$ in $K[x_1,\dots,x_n]$, with monomial generators m_i and m'_j, the intersection $I \cap J$ is generated by the least common multiples $\mathrm{lcm}(m_i,m'_j)$. In particular, $I \cap J$ is monomial again. See Section 2.2.4 for the general algorithm.

Our next step in relating algebraic sets to ideals is to define some kind of inverse to the map V:

Definition 1.16 *If $A \subset \mathbb{A}^n(K)$ is any subset, the ideal*

$$\mathrm{I}(A) := \{f \in K[x_1,\dots,x_n] \mid f(p) = 0 \text{ for all } p \in A\}$$

is called the ***vanishing ideal*** *of A.*

We summarize the properties of I and start relating I to V:

Proposition 1.17 *Let $R = K[x_1,\dots,x_n]$.*

(i) $\mathrm{I}(\emptyset) = R$. *If K is infinite, then* $\mathrm{I}(\mathbb{A}^n(K)) = \langle 0\rangle$.

(ii) *If $A \subset B$ are subsets of $\mathbb{A}^n(K)$, then* $\mathrm{I}(A) \supset \mathrm{I}(B)$.

(iii) *If A, B are subsets of $\mathbb{A}^n(K)$, then*

$$\mathrm{I}(A \cup B) = \mathrm{I}(A) \cap \mathrm{I}(B).$$

(iv) *For any subset $A \subset \mathbb{A}^n(K)$, we have*

$$\mathrm{V}(\mathrm{I}(A)) = \overline{A}.$$

(v) *For any subset $I \subset R$, we have*

$$\mathrm{I}(\mathrm{V}(I)) \supset I.$$

Proof Properties (ii), (iii), and (v) are easy consequences of the definitions. The first statement in (i) is also clear. For the second statement in (i), let K be infinite, and let $f \in K[x_1, \dots, x_n]$ be any nonzero polynomial. We have to show that there is a point $p \in \mathbb{A}^n(K)$ such that $f(p) \neq 0$. By our assumption on K, this is clear for $n = 1$ since every nonzero polynomial in one variable has at most finitely many zeros. If $n > 1$, write f in the form $f = c_0(x_1, \dots, x_{n-1}) + c_1(x_1, \dots, x_{n-1})x_n + \dots + c_s(x_1, \dots, x_{n-1})x_n^s$. Then c_i is nonzero for at least one i. For such an i, we may assume by induction that there is a point $p' \in \mathbb{A}^{n-1}(K)$ such that $c_i(p') \neq 0$. Then $f(p', x_n) \in K[x_n]$ is nonzero. Hence, there is an element $a \in K$ such that $f(p', a) \neq 0$. This proves (i). For (iv), note that $\mathrm{V}(\mathrm{I}(A)) \supset A$. Let, now, $\mathrm{V}(T)$ be any algebraic set containing A. Then $f(p) = 0$ for all $f \in T$ and all $p \in A$. Hence, $T \subset \mathrm{I}(A)$ and, thus, $\mathrm{V}(T) \supset \mathrm{V}(\mathrm{I}(A))$, as desired. □

Property (iv) above expresses $\mathrm{V}(\mathrm{I}(A))$ in terms of A. Likewise, we wish to express $\mathrm{I}(\mathrm{V}(I))$ in terms of I. The following example shows that the containment $\mathrm{I}(\mathrm{V}(I)) \supset I$ may be strict.

Example 1.18 We have

$$\mathrm{I}(\mathrm{V}(x^k)) = \langle x \rangle \text{ for all } k \geq 1.$$

Definition 1.19 *Let R be any ring, and let $I \subset R$ be an ideal. Then the set*

$$\sqrt{I} := \{f \in R \mid f^k \in I \text{ for some } k \geq 1\}$$

is an ideal of R containing I. It is called the ***radical*** *of I. If $\sqrt{I} = I$, then I is called a* ***radical ideal****.*

Example 1.20 Consider a principal ideal of $K[x_1, \ldots, x_n]$: If

$$f = f_1^{\mu_1} \cdots f_s^{\mu_s} \in K[x_1, \ldots, x_n]$$

is the decomposition of a polynomial into irreducible factors, then

$$\sqrt{\langle f \rangle} = \langle f_1 \cdots f_s \rangle.$$

The product $f_1 \cdots f_s$, which is uniquely determined by f up to multiplication by a constant, is called the **square–free part** of f. If $f = f_1 \cdots f_s$ up to scalar, we say that f is **square–free**.

Problem 1.21 *Design an algorithm for computing radicals.*

The computation of radicals will be treated in Section 2.4.

Singular Example 1.22

```
> LIB "primdec.lib";   // provides the command radical
> ring  R = 0, (x,y,z), dp;
> poly  p = z2+1;  poly  q = z3+2;
> ideal I = p*q^2,y-z2;
> ideal radI = radical(I);
> I;
I[1]=z8+z6+4z5+4z3+4z2+4
I[2]=-z2+y
> radI;
radI[1]=z2-y
radI[2]=y2z+z3+2z2+2
```

1.1.3 Hilbert's Nullstellensatz

It is clear from the definitions that $\mathrm{I}(\mathrm{V}(I)) \supset \sqrt{I}$. But even this containment may be strict:

Example 1.23 The polynomial $1 + x^2 \in \mathbb{R}[x]$ has no real root. Hence, considering the ideal of the real vanishing locus, we get

$$\mathrm{I}(\mathrm{V}(1 + x^2)) = \mathrm{I}(\emptyset) = \mathbb{R}[x].$$

Here, by the fundamental theorem of algebra, we may remedy the situation by allowing complex roots as well. More generally, given any field K, we may work over the algebraic closure $\overline{K}$ of K. Then, by the very definition of $\overline{K}$, every nonconstant polynomial in one variable has a root. This fact has a multivariate analogue:

Theorem 1.24 (Hilbert's Nullstellensatz, Weak Version) *Let $I \subset K[x_1, \dots, x_n]$ be an ideal, and let $\overline{K}$ be the algebraic closure of K. Formally, regard I as a subset of the larger polynomial ring $\overline{K}[x_1, \dots, x_n]$. Then the following are equivalent:*

(i) *The vanishing locus $\mathrm{V}(I)$ of I in $\mathbb{A}^n(\overline{K})$ is empty.*
(ii) $1 \in I$*, that is,* $I = K[x_1, \dots, x_n]$.

The proof will be given in Section 1.1.8.

Problem 1.25 *Design a test for checking whether 1 is in I.*

Singular Example 1.26

```
> ring  R = 0, (x,y,z), dp;
> ideal  I;
> I[1]=972x2+948xy+974y2+529xz+15yz-933z2+892x-483y-928z-188;
> I[2]=-204x2-408xy-789y2-107xz+543yz-762z2-528x-307y+649z-224;
> I[3]=998x2+7xy-939y2-216xz+617yz+403z2-699x-831y-185z-330;
> I[4]=688x2+585xy-325y2+283xz-856yz+757z2+152x-393y+386z+367;
> I[5]=464x2+957xy+962y2+579xz-647yz-142z2+950x+649y+49z+209;
> I[6]=-966x2+624xy+875y2-141xz+216yz+601z2+386x-671y-75z+935;
> I[7]=936x2-817xy-973y2-648xz-976yz+908z2+499x+773y+234z+35;
> I[8]=-574x2+560xy-199y2+623yz+146z2-821x-99y+166z+711;
> I[9]=124x2-751xy-745y2+678xz-47yz+326z2-447x+462y+225z+579;
> I[10]=902x2+383xy-828y2+865xz-433yz-137z2-265x+913y-928z-400;
> groebner(I);
_[1]=1
```

Problem 1.25 is a special instance of the following problem:

Problem 1.27 (Ideal Membership Problem) *Design a test for checking whether a given $f \in K[x_1, \dots, x_n]$ is in I.*

Remark 1.28 Let $I \subset K[x_1, \dots, x_n]$ be a monomial ideal, given by monomial generators $m_1, \dots, m_r$. Then a monomial is contained in I iff it is divisible by at least one of the m_i. If $f \in K[x_1, \dots, x_n]$ is any nonzero polynomial, we write it as a $K-$linear combination of different monomials, with nonzero scalars. Then $f \in I$ iff the respective monomials are contained in I. See Section 2.2.1 for the general algorithm.

Now, we discuss a second version of the Nullstellensatz which settles our question of how to express $\mathrm{I}(\mathrm{V}(I))$ in terms of I:

Theorem 1.29 (Hilbert's Nullstellensatz, Strong Version) *Let $K = \overline{K}$, and let $I \subset K[x_1, \ldots, x_n]$ be an ideal. Then*

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

Proof As already said earlier, $\sqrt{I} \subset \mathrm{I}(\mathrm{V}(I))$. For the reverse inclusion, let $f \in \mathrm{I}(\mathrm{V}(I))$, and let $f_1, \ldots, f_r$ be generators for I. Then f vanishes on $\mathrm{V}(I)$, and we have to show that $f^k = g_1 f_1 + \cdots + g_r f_r$ for some $k \geq 1$ and some $g_1, \ldots, g_r \in K[x_1, \ldots, x_n] =: R$. We use the *trick of Rabinowitch*: Consider the ideal

$$J := \langle f_1, \ldots, f_r, 1 - tf \rangle \subset R[t],$$

where t is an extra variable. We show that $\mathrm{V}(J) \subset \mathbb{A}^{n+1}(K)$ is empty. Suppose on the contrary that $p = (a_1, \ldots, a_n, a_{n+1}) \in \mathrm{V}(J)$ is a point, and set $p' = (a_1, \ldots, a_n)$. Then $f_1(p') = \cdots = f_r(p') = 0$, so that $p' \in \mathrm{V}(I)$, and $a_{n+1} f(p') = 1$. This contradicts the fact that f vanishes on $\mathrm{V}(I)$.

From the weak Nullstellensatz, we conclude that $1 \in J$. Then we have $1 = \sum_{i=1}^r h_i f_i + h(1 - tf)$ for suitable $h_1, \ldots, h_r, h \in R[t]$. Substituting $1/f$ for t in this expression and multiplying by a sufficiently high power f^k to clear denominators, we get a representation $f^k = \sum_{i=1}^r g_i f_i$ as desired. □

Corollary 1.30 *If $K = \overline{K}$, then* I *and* V *define a one–to–one correspondence*

$$\begin{array}{c} \{\textit{algebraic subsets of } \mathbb{A}^n(K)\} \\ \mathrm{V} \uparrow \downarrow I \\ \{\textit{radical ideals of } K[x_1, \ldots, x_n]\}. \end{array}$$

As we will see more clearly in Section 2.2.3, the trick of Rabinowitch allows us to solve the radical membership problem:

Corollary 1.31 (Radical Membership) *Let K be any field, let $I \subset K[x_1, \ldots, x_n]$ be an ideal, and let $f \in K[x_1, \ldots, x_n]$. Then:*

$$f \in \sqrt{I} \Longleftrightarrow 1 \in J := \langle I, 1 - tf \rangle \subset K[x_1, \ldots, x_n, t],$$

where t is an extra variable.

Based on the Nullstellensatz, we can express geometric properties in terms of ideals. Here is a first example of how this works:

Proposition 1.32 *Let K be any field, and let $I \subset K[x_1, \ldots, x_n]$ be an ideal. The following are equivalent:*

(i) *The vanishing locus $\mathrm{V}(I)$ of I in $\mathbb{A}^n(\overline{K})$ is finite.*
(ii) *For each i, $1 \leq i \leq n$, we have $I \cap K[x_i] \supsetneq \langle 0 \rangle$.*

Problem 1.33 *Design a test for checking whether (ii) holds.*

In Section 1.1.6, we will see that (ii) holds iff the quotient ring $K[x_1, \ldots, x_n]/I$ is finite–dimensional as a K–vector space. How to compute the vector space dimension is a topic of Section 2.3.

Example 1.34 Taking the symmetry of the generators into account, the computation in Example 0.7 shows that the ideal

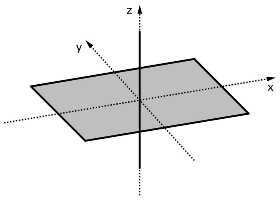
$$\begin{aligned} I = \langle x + y + z - 1,\ x^2 + y^2 + z^2 - 1,\ x^3 + y^3 + z^3 - 1 \rangle \\ \subset \mathbb{Q}[x, y, z] \end{aligned}$$

contains the polynomials

$$z^3 - z^2,\ y^3 - y^2,\ x^3 - x^2.$$

1.1.4 Irreducible Algebraic Sets

As we have seen earlier, the vanishing locus $\mathrm{V}(xz, yz) \subset \mathbb{A}^3(\mathbb{R})$ is the union of the xy–plane and the z–axis:



Definition 1.35 *A nonempty algebraic set $A \subset \mathbb{A}^n(K)$ is called* ***irreducible****, or a* ***subvariety*** *of $\mathbb{A}^n(K)$, if it cannot be expressed as the union $A = A_1 \cup A_2$ of algebraic sets A_1, A_2 properly contained in A. Otherwise, A is called* ***reducible****.*

Proposition 1.36 *Let $A \subset \mathbb{A}^n(K)$ be an algebraic set. Then the following are equivalent:*

(i) *A is irreducible.*
(ii) $\mathrm{I}(A)$ *is a prime ideal.*

Problem 1.37 *Design a test for checking whether a given ideal of $K[x_1, \dots, x_n]$ is prime.*

Corollary 1.38 *If $K = \overline{K}$, then* I *and* V *define a one–to–one correspondence*

$$\begin{array}{c}\{\textit{subvarieties of } \mathbb{A}^n(K)\}\\ \mathrm{V} \uparrow \downarrow I\\ \{\textit{prime ideals of } K[x_1, \dots, x_n]\}.\end{array}$$

Proposition 1.39 *If $K = \overline{K}$, then* I *and* V *define a one–to–one correspondence*

$$\begin{array}{c}\{\textit{points of } \mathbb{A}^n(K)\}\\ \mathrm{V} \uparrow \downarrow I\\ \{\textit{maximal ideals of } K[x_1, \dots, x_n]\}.\end{array}$$

Here is the main result in this section:

Theorem 1.40 *Every nonempty algebraic set $A \subset \mathbb{A}^n(K)$ can be expressed as a finite union*

$$A = V_1 \cup \dots \cup V_s$$

of subvarieties V_i. This decomposition can be chosen to be ***minimal*** *in the sense that $V_i \not\supset V_j$ for $i \neq j$. The V_i are, then, uniquely determined and are called the* ***irreducible components*** *of A.*

Proof The main idea of the proof is to use **Noetherian induction**: Assuming that there is an algebraic set $A \subset \mathbb{A}^n(K)$ which cannot be written as a finite union of irreducible subsets, we get an infinite descending chain of subvarieties V_i of A:

$$A \supset V_1 \supsetneq V_2 \supsetneq \dots$$

This contradicts the ascending chain condition in the polynomial ring since taking vanishing ideals is inclusion reversing. □

Problem 1.41 *Design an algorithm to find the irreducible components of a given algebraic set.*

The algebraic concept of primary decomposition, together with algorithms for computing such decompositions, gives an answer to both Problems 1.41 and 1.37. See Section 2.4.

If K is a subfield of $\mathbb{C}$, and if all irreducible components in $\mathbb{A}^n(\mathbb{C})$ are points (that is, we face a system of polynomial equations with just finitely many complex solutions), we may find the solutions via *triangular decomposition.* This method combines lexicographic Gröbner bases with *univariate numerical solving*. See [Decker and Lossen (2006)].

Singular Example 1.42

```
> ring  S = 0, (x,y,z), lp;
> ideal I = x2+y+z-1, x+y2+z-1, x+y+z2-1;
> LIB "solve.lib";
> def R = solve(I,6); // creates a new ring in which the solutions
.                     // are defined; 6 is the desired precision
> setring R; SOL;
//-> [1]:         [2]:     [3]:           [4]:     [5]:
//->    [1]:         [1]:     [1]:           [1]:     [1]:
//->        0.414214     0        -2.414214      1        0
//->    [2]:         [2]:     [2]:           [2]:     [2]:
//->        0.414214     0        -2.414214      0        1
//->    [3]:         [3]:     [3]:           [3]:     [3]:
//->        0.414214     1        -2.414214      0        0
```

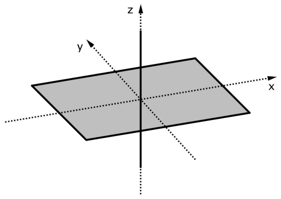
In this simple example, the solutions can also be read off from a lexicographic Gröbner basis as in Example 0.7:

```
> groebner(I);
//-> _[1]=z6-4z4+4z3-z2       _[2]=2yz2+z4-z2
//-> _[3]=y2-y-z2+z           _[4]=x+y+z2-1
```

1.1.5 Removing Algebraic Sets

The set theoretic difference of two algebraic sets need not be an algebraic set:

Example 1.43 Consider again the union of the xy–plane and the z–axis in $\mathbb{A}^3(\mathbb{R})$:



Removing the plane, the residual set is the punctured z–axis, which is not defined by polynomial equations. Indeed, if a polynomial $f \in \mathbb{R}[x, y, z]$ vanishes on the z–axis except possibly at the origin o, then the univariate polynomial $g(t) := f(0, 0, t)$ has infinitely many roots since $\mathbb{R}$ is infinite. Hence, $g = 0$ (see the proof of Proposition 1.17), so that f vanishes at o, too.

In what follows, we explain how to find polynomial equations for the Zariski closure of the difference of two algebraic sets, that is, for the smallest algebraic set containing the difference. We need:

Definition 1.44 *Let I, J be two ideals of a ring R. Then the sets*

$$I : J := \{f \in R \mid fg \in I \textit{ for all } g \in J\}$$

and

$$I : J^{\infty} := \{f \in R \mid fJ^k \subset I \textit{ for some } k \geq 1\} = \bigcup_{k=1}^{\infty} (I : J^k)$$

*are ideals of R containing I. They are called the **ideal quotient** of I by J and the **saturation** of I with respect to J, respectively.*

Problem 1.45 *Design algorithms to compute ideal quotients and saturation.*

Since the polynomial ring $K[x_1, \ldots, x_n]$ is Noetherian by Hilbert's basis theorem, and since $I : J^k = (I : J^{k-1}) : J$ for any two ideals $I, J \subset K[x_1, \ldots, x_n]$, the computation of $I : J^{\infty}$ just means to iterate the computation of ideal quotients: The ascending chain

$$I : J \subset I : J^2 \subset \cdots \subset I : J^k \subset \cdots$$

is eventually stationary. How to compute ideal quotients will be discussed in Section 2.2.5.

Theorem 1.46 *Let I, J be ideals of $K[x_1, \ldots, x_n]$. Then, considering vanishing loci and the Zariski closure in $\mathbb{A}^n(\overline{K})$, we have*

$$\overline{\mathrm{V}(I) \setminus \mathrm{V}(J)} = \mathrm{V}(I : J^\infty) \subset \mathbb{A}^n(\overline{K}).$$

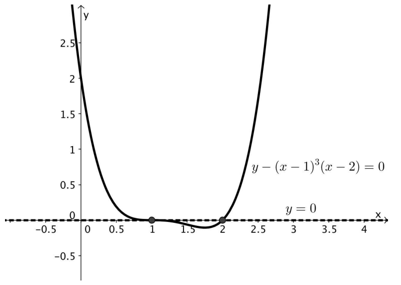
If I is a radical ideal, then

$$\overline{\mathrm{V}(I) \setminus \mathrm{V}(J)} = \mathrm{V}(I : J) \subset \mathbb{A}^n(\overline{K}).$$

The theorem is another consequence of Hilbert's Nullstellensatz. See [Decker and Schreyer (2013)].

Singular Example 1.47 We illustrate the geometry of ideal quotients by starting from an ideal I which defines the intersection of the curve $C = \mathrm{V}(y - (x-1)^3(x-2)) \subset \mathbb{A}^2(\mathbb{R})$ with the x–axis:

```
> ring R = 0, (x,y), dp;
> ideal I = y-(x-1)^3*(x-2), y;
```

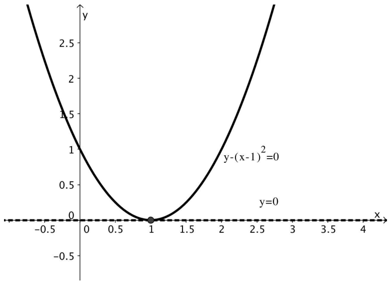


```
> ideal GI = groebner(I);  GI;
GI[1]=y
GI[2]=x4-5x3+9x2-7x+2
> factorize(GI[2]);
[1]:
   _[1]=1
   _[2]=x-1
   _[3]=x-2
[2]:
   1,3,1
```

There are two intersection points, namely $p = (0,1)$ and $q = (0,2)$. The ideal $J = \langle (x-1)(x-2) \rangle$ defines a pair of parallel lines which intersect the x–axis in p and q, respectively. We compute the ideal quotient $I_1 = I : J$:

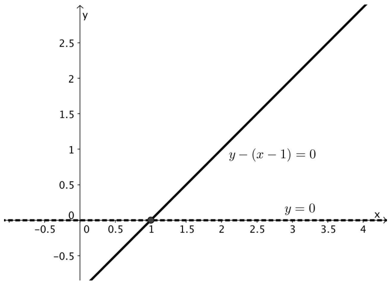
```
> ideal J = (x-1)*(x-2);
> ideal I1 = quotient(I,J);   I1;
I1[1]=y
I1[2]=x2-2x+1
> factorize(I1[2]);
[1]:
   _[1]=1
   _[2]=x-1
[2]:
   1,2
```

The resulting ideal I_1 defines the intersection of the parabola $C_1 = \mathrm{V}(y-(x-1)^2)$ with the x–axis which consists of the point $p = (0, 1)$ only. In fact, the x–axis is the tangent to C_1 at p:



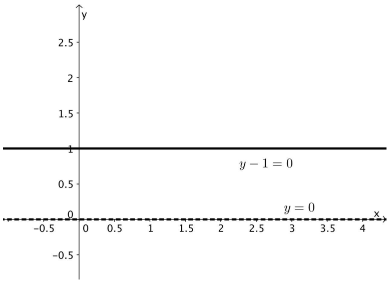
Computing the ideal quotient $I_2 = I_1 : J$, we may think of the result as defining the intersection of a line with the x–axis at p:

```
> ideal I2 = quotient(I1,J);  I2;
I2[1]=y
I2[2]=x-1
```



A final division also removes p:

```
> ideal I3 = quotient(I2,J);  I3;
I3[1]=1
```



Singular Example 1.48 To simplify the output in what follows, we work over the field with 2 elements:

```
> ring R = 2, (x,y,z), dp;
> poly F = x5+y5+(x-y)^2*xyz;
> ideal J = jacob(F);  J;
//->    J[1]=x4+x2yz+y3z     J[2]=y4+x3z+xy2z    J[3]=x3y+xy3
> maxideal(2);
//->  _[1]=z2   _[2]=yz   _[3]=y2   _[4]=xz   _[5]=xy   _[6]=x2
> ideal H = quotient(J,maxideal(2));   H;
//->   H[1]=y4+x3z+xy2z   H[2]=x3y+xy3   H[3]=x4+x2yz+y3z
//->   H[4]=x3z2+x2yz2+xy2z2+y3z2   H[5]=x2y2z+x2yz2+y3z2
//->   H[6]=x2y3
> H = quotient(H,maxideal(2));  H;
H[1]=x3+x2y+xy2+y3
H[2]=y4+x2yz+y3z
H[3]=x2y2+y4
> H = quotient(H,maxideal(2));  H;
H[1]=x3+x2y+xy2+y3
H[2]=y4+x2yz+y3z
H[3]=x2y2+y4

> LIB "elim.lib";   // provides the command sat
> int p = printlevel;
> printlevel = 2;  // print more information while computing
> sat(J,maxideal(2));
// compute quotient 1
// compute quotient 2
// compute quotient 3
// saturation becomes stable after 2 iteration(s)
[1]:
   _[1]=x3+x2y+xy2+y3
   _[2]=y4+x2yz+y3z
   _[3]=x2y2+y4
[2]:
   2
> printlevel = p;  // reset printlevel
```

1.1.6 Polynomial Maps

Since algebraic sets are defined by polynomials, it should not be a surprise that the maps relating algebraic sets to each other are defined by polynomials as well:

Definition 1.49 *Let $A \subset \mathbb{A}^n(K)$ and $B \subset \mathbb{A}^m(K)$ be (nonempty) algebraic sets. A map $\varphi : A \to B$ is called a* ***polynomial map****, or a* ***morphism****, if there are polynomials $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$ such that $\varphi(p) = (f_1(p), \ldots, f_m(p))$ for all $p \in A$.*

In other words, a map $A \to B$ is a polynomial map iff its components are restrictions of polynomial functions on $\mathbb{A}^n(K)$ to A. Every such restriction is called a **polynomial function on *A***.

Given two polynomial functions $p \mapsto f(p)$ and $p \mapsto g(p)$ on A, we may define their sum and product according to the addition and multiplication in K: send p to $f(p) + g(p)$ and to $f(p) \cdot g(p)$, respectively. In this way, the set of all polynomial functions on A becomes a ring, which we denote by $K[A]$. Since this ring is generated by the coordinate functions $p \mapsto x_i(p)$, we define:

Definition 1.50 *Let $A \subset \mathbb{A}^n(K)$ be a (nonempty) algebraic set. The* ***coordinate ring*** *of A is the ring of polynomial functions $K[A]$ defined above.*

Note that K may be considered as the subring of $K[A]$ consisting of the constant functions. Hence, $K[A]$ is naturally a K–algebra. Next, observe that each morphism $\varphi : A \to B$ of algebraic sets gives rise to a homomorphism

$$\varphi^* : K[B] \to K[A],\ g \mapsto g \circ \varphi,$$

of K–algebras. Conversely, given any homomorphism $\phi : K[B] \to K[A]$ of K–algebras, one can show that there is a unique polynomial map $\varphi : A \to B$ such that $\phi = \varphi^*$. Furthermore, defining the notion of an **isomorphism** as usual by requiring that there exists an inverse morphism, it turns out that $\varphi : A \to B$ is an isomorphism of algebraic sets iff φ^* is an isomorphism of K–algebras.

Example 1.51 Let $C = \mathrm{V}(y - x^2, xy - z) \subset \mathbb{A}^3(\mathbb{R})$ be the twisted cubic curve. The map

$$\mathbb{A}^1(\mathbb{R}) \to C,\ t \mapsto (t, t^2, t^3),$$

is an isomorphism with inverse map $(x, y, z) \mapsto x$.

By relating algebraic sets to rings, we start a new section in the geometry–algebraic dictionary. To connect this section to the previous sections, where we related algebraic sets to ideals, we recall the definition of a quotient ring:

Definition 1.52 *Let R be a ring, and let I be an ideal of R. Two elements $f, g \in R$ are said to be* ***congruent modulo I*** *if $f - g \in I$. In this way, we get an equivalence relation on R. We write $\overline{f} = f + I$ for the equivalence class of $f \in R$, and call it the* ***residue class*** *of f modulo I. The set R/I of all residue classes becomes a ring, with algebraic operations*

$$\overline{f} + \overline{g} = \overline{f + g} \ \text{ and } \ \overline{f} \cdot \overline{g} = \overline{f \cdot g}.$$

We call R/I the ***quotient ring*** *of R modulo I.*

Now, returning to the coordinate ring of an affine algebraic set A, we note that two polynomials $f, g \in K[x_1, \ldots, x_n]$ define the same polynomial function on A iff their difference is contained in the vanishing ideal $\mathrm{I}(A)$. We may, thus, identify $K[A]$ with the quotient ring $K[x_1, \ldots, x_n]/\mathrm{I}(A)$, and translate geometric properties expressed in terms of $\mathrm{I}(A)$ into properties expressed in terms of $K[A]$. For example:

- A is irreducible $\Longleftrightarrow$ $\mathrm{I}(A)$ is prime $\Longleftrightarrow$ $K[x_1, \ldots, x_n]/\mathrm{I}(A)$ is an integral domain.

For another example, let $I \subset K[x_1, \ldots, x_n]$ be *any* ideal. Then, as one can show, Proposition 1.32 can be rewritten as follows:

- The vanishing locus $\mathrm{V}(I)$ of I in $\mathbb{A}^n(\overline{K})$ is finite $\Longleftrightarrow$ the K–vector space $K[x_1, \ldots, x_n]/I$ is finite–dimensional.

Definition 1.53 *A ring of type $K[x_1, \ldots, x_n]/I$, where I is an ideal of $K[x_1, \ldots, x_n]$, is called an* ***affine* K*–algebra***, *or simply an* ***affine ring***.

With regard to computational aspects, we should point out that it were calculations in affine rings which led Buchberger to design his Gröbner basis algorithm. In fact, to implement the arithmetic operations in $K[x_1, \ldots, x_n]/I$, we may fix a monomial ordering $>$ on $K[x_1, \ldots, x_n]$, represent each residue class by a normal form with respect to $>$ and I, and add and multiply residue classes by adding and multiplying normal forms. Computing normal forms, in turn, amounts to compute remainders on multivariate polynomial division by the elements of a Gröbner basis for I with respect to $>$. See Algorithm 1 and Proposition 2.27 in Chapter 2.

Singular Example 1.54

```
> ring R = 0, (z,y,x), lp;
> ideal I = y-x2, z-xy;
> qring S = groebner(I);   // defining a quotient ring
> basering;                // shows current ring
//   characteristic : 0
//   number of vars : 3
//        block   1 : ordering lp
//                  : names    z y x
//        block   2 : ordering C
// quotient ring from ideal
_[1]=y-x2
_[2]=z-yx
> poly f = x3z2-4y4z+x4;
> reduce(f,groebner(0));  // division with remainder
-4x11+x9+x4
```

Closely related to normal forms is a result of Macaulay which was a major motivation for Buchberger and his thesis advisor Gröbner. Together with Buchberger's algorithm, this result allows one to find explicit K–vector space bases for affine rings $K[x_1, \ldots, x_n]/I$ (and, thus, to determine the vector space dimension). In fact, as in Gordan's proof of the basis theorem, one can use Gröbner bases to reduce the case of an arbitrary ideal I to that of a monomial ideal (see Theorem 2.55 for a precise statement).

Singular Example 1.55 In Example 0.7, we computed a lexicographic Gröbner basis `GI` for the ideal

$$\begin{aligned} I = \langle x+y+z-1,\ x^2+y^2+z^2-1,\ x^3+y^3+z^3-1\rangle \\ \subset \mathbb{Q}[x,y,z]. \end{aligned}$$

By inspecting the elements of GI, we saw that the system defined by the three generators of I has precisely the three solutions

$$(1,0,0),\ (0,1,0),\ (0,0,1)$$

in $\mathbb{A}^3(\overline{\mathbb{Q}})$. In particular, there are only finitely many solutions. As said earlier in this section, this means that the $\mathbb{Q}$–vector space $\mathbb{Q}[x,y,z]/I$ has finite dimension. We check this using Singular:

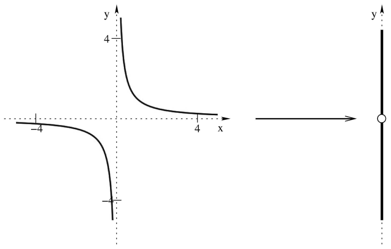
```
> vdim(GI); // requires Groebner basis
6
```

In general, if finite, the dimension $d = \dim_K(K[x_1,\dots,x_n]/I)$ is an upper bound for the number of points in the vanishing locus of I in $\mathbb{A}^n(\overline{K})$. In fact, given a point $p \in \mathrm{V}(I) \subset \mathbb{A}^n(\overline{K})$, there is a natural way of assigning a multiplicity to the pair (p, I). Counted with multiplicity, there are exactly d solutions. See Section 1.1.9.

1.1.7 The Geometry of Elimination

The image of an affine algebraic set under a morphism need not be an algebraic set†‡:

Example 1.56 The projection map $(x,y) \mapsto y$ sends the hyperbola $\mathrm{V}(xy-1)$ onto the punctured y–axis:



In what follows, we show how to obtain polynomial equations for the Zariski closure of the image of a morphism. We begin by considering the special case of a projection map as in the example above. For this, we use the following notation:

† We may, however, represent the image as a *constructible set.* See [Kemper (2007)] for an algorithmic approach.

‡ In projective algebraic geometry, morphisms are better behaved.

Definition 1.57 *Given an ideal $I \subset K[x_1, \ldots, x_n]$ and an integer $0 \leq k \leq n$, the **kth elimination ideal** of I is the ideal*

$$I_k = I \cap K[x_{k+1}, \ldots, x_n].$$

Note that $I_0 = I$ and that I_n is an ideal of K.

Remark 1.58 As indicated earlier, one way of finding I_k is to compute a Gröbner basis of I with respect to an elimination ordering for $x_1, \ldots, x_k$. Note that $>_{\mathrm{lp}}$ has the elimination property for *each* set of initial variables: If G is a Gröbner basis of I with respect to $>_{\mathrm{lp}}$ on $K[x_1, \ldots, x_n]$, then $G \cap K[x_{k+1}, \ldots, x_n]$ is a Gröbner basis of I_k with respect to $>_{\mathrm{lp}}$ on $K[x_{k+1}, \ldots, x_n]$, for $k = 0, \ldots, n-1$. See Section 2.2.2 for details.

Theorem 1.59 *Let $I \subset K[x_1, \ldots, x_n]$ be an ideal, let $A = \mathrm{V}(I)$ be its vanishing locus in $\mathbb{A}^n(\overline{K})$, let $0 \leq k \leq n-1$, and let*

$$\pi_k : \mathbb{A}^n(\overline{K}) \to \mathbb{A}^{n-k}(\overline{K}),\ (x_1, \ldots, x_n) \mapsto (x_{k+1}, \ldots, x_n),$$

be projection onto the last $n-k$ components. Then

$$\overline{\pi_k(A)} = \mathrm{V}(I_k) \subset \mathbb{A}^{n-k}(\overline{K}).$$

Proof As we will explain in Section 2.5 on Buchberger's algorithm and field extensions, the ideal generated by I_k in the polynomial ring $\overline{K}[x_{k+1}, \ldots, , x_n]$ is the first elimination ideal of the ideal generated by I in $\overline{K}[x_1, \ldots, , x_n]$. We may, hence, suppose that $K = \overline{K}$. The theorem is, then, an easy consequence of the Nullstellensatz. We leave the details to the reader. □

In what follows, we write $x = \{x_1, \ldots, x_n\}$ and $y = \{y_1, \ldots, y_m\}$, and consider the x_i and y_j as the coordinate functions on $\mathbb{A}^n(\overline{K})$ and $\mathbb{A}^m(\overline{K})$, respectively. Moreover, if $I \subset K[x]$ is an ideal, we write $IK[x, y]$ for the ideal generated by I in $K[x, y]$.

Corollary 1.60 *With notation as above, let $I \subset K[x]$ be an ideal, let $A = \mathrm{V}(I)$ be its vanishing locus in $\mathbb{A}^n(\overline{K})$, and let*

$$\varphi : A \to \mathbb{A}^m(\overline{K}),\ p \mapsto (f_1(p), \ldots, f_m(p)),$$

be a morphism, given by polynomials $f_1, \ldots, f_m \in K[x]$. *Let* J *be the ideal*

$$J = IK[x,y] + \langle f_1 - y_1, \ldots, f_m - y_m \rangle \subset K[x,y].$$

Then

$$\overline{\varphi(A)} = \mathrm{V}(J \cap K[y]) \subset \mathbb{A}^m(\overline{K}).$$

That is, the vanishing locus of the elimination ideal $J \cap K[y]$ *in* $\mathbb{A}^m(\overline{K})$ *is the Zariski closure of* $\varphi(A)$.

Proof The result follows from Theorem 1.59 since the ideal J describes the graph of φ in $\mathbb{A}^{n+m}(\overline{K})$. □

Remark 1.61 Algebraically, as we will see in Section 2.2.6, the ideal $J \cap K[y]$ is the kernel of the ring homomorphism

$$\phi : K[y_1, \ldots, y_m] \to S = K[x_1, \ldots, x_n]/I, \ y_i \mapsto \overline{f}_i = f_i + I.$$

Recall that the elements $\overline{f}_1, \ldots, \overline{f}_m$ are called **algebraically independent** over K if this kernel is zero.

Under an additional assumption, the statement of Corollary 1.60 holds in the geometric setting over the original field K:

Corollary 1.62 *Let* I, $f_1, \ldots, f_m$, *and* J *be as in Corollary 1.60, let* $A = \mathrm{V}(I) \subset \mathbb{A}^n(K)$, *and let*

$$\varphi : A \to \mathbb{A}^m(K), \ p \mapsto (f_1(p), \ldots, f_m(p)),$$

be the morphism defined by $f_1, \ldots, f_m$ *over* K. *Suppose that the vanishing locus of* I *in* $\mathbb{A}^n(\overline{K})$ *is the Zariski closure of* A *in* $\mathbb{A}^n(\overline{K})$. *Then*

$$\overline{\varphi(A)} = \mathrm{V}(J \cap K[y]) \subset \mathbb{A}^m(K).$$

If K is infinite, then the condition on A in Corollary 1.62 is fulfilled for $A = \mathbb{A}^n(K)$. It, hence, applies in the following Example:

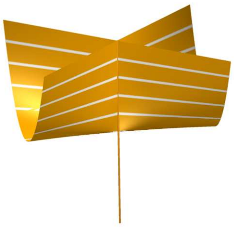
Singular Example 1.63 We compute the Zariski closure B of the image of the map

$$\varphi : \mathbb{A}^2(\mathbb{R}) \to \mathbb{A}^3(\mathbb{R}), \ (s,t) \mapsto (st, t, s^2).$$

According to the discussion above, this means to create the relevant ideal J and to compute a Gröbner basis of J with respect to a monomial ordering such as $>_{\mathrm{lp}}$. Here is how to do it in SINGULAR:

```
> ring RR = 0, (s,t,x,y,z), lp;
> ideal J = x-st, y-t, z-s2;
> groebner(J);

_[1]=x2-y2z
_[2]=t-y
_[3]=sy-x
_[4]=sx-yz
_[5]=s2-z
```

The first polynomial is the only polynomial in which both variables s and t are eliminated. Hence, the desired algebraic set is $B = \mathrm{V}(x^2 - y^2z)$. This surface is known as the Whitney umbrella:



$\mathrm{V}(x^2 - y^2z)$

Alternatively, we may use the built–in SINGULAR command `eliminate` to compute the equation of the Whitney umbrella:

```
> ideal H = eliminate(J,st);
> H;
H[1]=y2z-x2
```

For further SINGULAR computations involving an ideal obtained by eliminating variables, it is usually convenient to work in a ring which only depends on the variables still regarded. One way of accomplishing this is to make use of the `imap` command:

```
> ring R = 0, (x,y,z), dp;
> ideal H = imap(RR,H);  // maps the ideal H from RR to R
> H;
H[1]=y2z-x2
```

The map φ above is an example of a polynomial parametrization:

Definition 1.64 *Let $B \subset \mathbb{A}^m(K)$ be algebraic. A* ***polynomial parametrization*** *of B is a morphism $\varphi : \mathbb{A}^n(K) \to \mathbb{A}^m(K)$ such that B is the Zariski closure of the image of φ.*

Instead of just considering polynomial maps, we are more generally interested in rational maps, that is, in maps of type

$$t = (t_1, \ldots, t_n) \mapsto \left(\frac{g_1(t)}{h_1(t)}, \ldots, \frac{g_m(t)}{h_m(t)} \right),$$

with polynomials $g_i, h_i \in K[x_1, \ldots, x_n]$ (see Example 1.10, (iv)). Note that such a map may not be defined on all of $\mathbb{A}^n(K)$ because of the denominators. We have, however, a well–defined map

$$\varphi : \mathbb{A}^n(K) \setminus \mathrm{V}(h_1 \cdots h_m) \to \mathbb{A}^m(K),\ t \mapsto \left(\frac{g_1(t)}{h_1(t)}, \ldots, \frac{g_m(t)}{h_m(t)} \right).$$

Our next result will allow us to compute the Zariski closure of the image of such a map:

Proposition 1.65 *Let K be infinite. Given $g_i, h_i \in K[x] = K[x_1, \ldots, x_n]$, $i = 1, \ldots, m$, consider the map*

$$\varphi : U \to \mathbb{A}^m(K),\ t \mapsto \left(\frac{g_1(t)}{h_1(t)}, \ldots, \frac{g_m(t)}{h_m(t)} \right),$$

where $U = \mathbb{A}^n(K) \setminus \mathrm{V}(h_1 \cdots h_m)$. Let J be the ideal

$$J = \langle h_1 y_1 - g_1, \ldots, h_m y_m - g_m, 1 - h_1 \cdots h_m \cdot w \rangle \subset K[w, x, y],$$

where y stands for the coordinate functions $y_1, \ldots, y_m$ on $\mathbb{A}^m(K)$, and where w is an extra variable. Then

$$\overline{\varphi(U)} = \mathrm{V}(J \cap K[y]) \subset \mathbb{A}^m(K).$$

Singular Example 1.66 We demonstrate the use of Proposition 1.65 in an example:

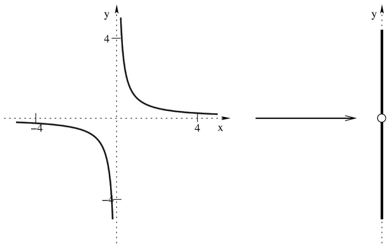
```
> ring RR = 0, (w,t,x,y), dp;
> poly g1 = 2t;  poly h1 = t2+1;
> poly g2 = t2-1;  poly h2 = t2+1;
> ideal J = h1*x-g1, h2*y-g2, 1-h1*h2*w;
> ideal H = eliminate(J,wt);
> H;
H[1]=x2+y2-1
```

The resulting equation defines the unit circle. Note that the circle does not admit a polynomial parametrization.

Definition 1.67 *Let $B \subset \mathbb{A}^m(K)$ be algebraic. A* ***rational parametrization*** *of B is a map φ as in Proposition 1.65 such that B is the Zariski closure of the image of φ.*

1.1.8 Noether Normalization and Dimension

We know from the previous section that the image of an algebraic set under a projection map need not be an algebraic set:



Under an additional assumption, projections are better behaved:

Theorem 1.68 (Projection Theorem) *Let I be a nonzero ideal of $K[x_1, \dots, x_n]$, $n \geq 2$, and let $I_1 = I \cap K[x_2, \dots, x_n]$ be its first elimination ideal. Suppose that I contains a polynomial f_1 which is monic in x_1 of some degree $d \geq 1$:*

$$f_1 = x_1^d + c_1(x_2, \dots, x_n)x_1^{d-1} + \cdots + c_d(x_2, \dots, x_n),$$

with coefficients $c_i \in K[x_2, \dots, x_n]$. Let

$$\pi_1 : \mathbb{A}^n(\overline{K}) \to \mathbb{A}^{n-1}(\overline{K}),\ (x_1, \dots, x_n) \mapsto (x_2, \dots, x_n),$$

be projection onto the last $n-1$ components, and let $A = \mathrm{V}(I) \subset \mathbb{A}^n(\overline{K})$. Then

$$\pi_1(A) = \mathrm{V}(I_1) \subset \mathbb{A}^{n-1}(\overline{K}).$$

In particular, $\pi_1(A)$ is an algebraic set.

Proof Clearly $\pi_1(A) \subset \mathrm{V}(I_1)$. For the reverse inclusion, taking Section 2.5 on Buchberger's algorithm and field extensions into account as in the proof of Theorem 1.59, we may assume that $K = \overline{K}$. Let, then, $p' \in \mathbb{A}^{n-1}(\overline{K}) \setminus \pi_1(A)$ be any point. To conclude that $p' \in \mathbb{A}^{n-1}(\overline{K}) \setminus \mathrm{V}(I_1)$, we have to find a polynomial $g \in I_1$ such that $g(p') \neq 0$.

We claim that every polynomial $f \in K[x_1, \dots, x_n]$ has a representation $f = \sum\limits_{j=0}^{d-1} g_j x_1^j + h$, with polynomials $g_0, \dots, g_{d-1} \in K[x_2, \dots, x_n]$ and $h \in I$, and such that $g_j(p') = 0$, $j = 0, \dots, d-1$.

Once this is established, we apply it to $1, x_1, \dots, x_1^{d-1}$ to get representations

$$\begin{array}{ccccccccc} 1 & = & g_{0,0} & + & \cdots & + & g_{0,d-1}x_1^{d-1} & + & h_0, \\ \vdots & & & & & & & & \vdots \\ x_1^{d-1} & = & g_{d-1,0} & + & \cdots & + & g_{d-1,d-1}x_1^{d-1} & + & h_{d-1}, \end{array}$$

with polynomials $g_{ij} \in K[x_2, \dots, x_n]$ and $h_i \in I$, and such that $g_{ij}(p') = 0$, for all i, j. Writing E_d for the $d \times d$ identity matrix, this reads

$$(E_d - (g_{ij})) \begin{pmatrix} 1 \\ \vdots \\ x_1^{d-1} \end{pmatrix} = \begin{pmatrix} h_0 \\ \vdots \\ h_{d-1} \end{pmatrix}.$$

Setting $g := \det(E_d - (g_{ij})) \in K[x_2, \dots, x_n]$, Cramer's rule gives

$$g \begin{pmatrix} 1 \\ \vdots \\ x_1^{d-1} \end{pmatrix} = B \begin{pmatrix} h_0 \\ \vdots \\ h_{d-1} \end{pmatrix},$$

where B is the adjoint matrix of $(E_d - (g_{ij}))$. In particular, from the first row, we get $g \in I$ and, thus, $g \in I_1$. Furthermore, $g(p') = 1$ since $g_{ij}(p') = 0$ for all i, j. We conclude that $p' \in \mathbb{A}^{n-1}(\overline{K}) \setminus \mathrm{V}(I_1)$, as desired.

To prove the claim, consider the map

$$\phi : K[x_1, \dots, x_n] \to K[x_1],\ f \mapsto f(x_1, p').$$

Since any element $a \in \mathrm{V}(\phi(I))$ would give us a point $(a, p') \in A$, a contradiction to $p' \notin \pi_1(A)$, we must have $\mathrm{V}(\phi(I)) = \emptyset$. This implies that $\phi(I) = K[x_1]$ (otherwise, being a principal ideal, $\phi(I)$ would have a nonconstant generator which necessarily would have a root in $K = \overline{K}$). Hence, given $f \in K[x_1, \ldots, x_n]$, there exists a polynomial $\widetilde{f} \in I$ such that $\phi(\widetilde{f}) = \phi(f)$. Set $\widehat{f} := f - \widetilde{f}$. Then $\widehat{f}(x_1, p') = 0$. Since the polynomial f_1 is monic in x_1 of degree d, division with remainder in $K[x_2, \ldots, x_n][x_1]$ yields an expression

$$\widehat{f} = qf_1 + \sum_{i=0}^{d-1} g_j x_1^j,$$

with polynomials $g_j \in K[x_2, \ldots, x_n]$. Since $\widehat{f}(x_1, p') = 0$, we have $q(x_1, p')f_1(x_1, p') + \sum_{j=0}^{d-1} g_j(p')x_1^j = 0$. Now, since $f_1(x_1, p') \in K[x_1]$ has degree d, the uniqueness of division with remainder in $K[x_1]$ implies that $g_j(p') = 0$, $j = 0, \ldots, d-1$. Setting $h := \widetilde{f} + qf_1$, we have $h \in I$ and $f = \sum_{j=0}^{d-1} g_j x_1^j + h$. This proves the claim. □

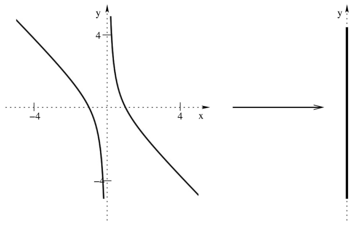
A crucial step towards proving the Nullstellensatz is the following lemma which states that the additional assumption of the projection theorem can be achieved by a coordinate change $\phi : K[x] \to K[x]$ of type $x_1 \mapsto x_1$ and $x_i \mapsto x_i + g_i(x_1)$, $i \geq 2$, which can be taken linear if K is infinite:

Lemma 1.69 *Let $f \in K[x_1, \ldots, x_n]$ be nonconstant. If K is infinite, let $a_2, \ldots, a_n \in K$ be sufficiently general. Substituting $x_i + a_i x_1$ for x_i in f, $i = 2, \ldots, n$, we get a polynomial of type*

$$ax_1^d + c_1(x_2, \ldots, x_n)x_1^{d-1} + \ldots + c_d(x_2, \ldots, x_n),$$

where $a \in K$ is nonzero, $d \geq 1$, and each $c_i \in K[x_2, \ldots, x_n]$. If K is arbitrary, we get a polynomial of the same type by substituting $x_i + x_1^{r^{i-1}}$ for x_i, $i = 2, \ldots, n$, where $r \in \mathbb{N}$ is sufficiently large.

Example 1.70 Substituting $y + x$ for y in $xy - 1$, we get the polynomial $x^2 + xy - 1$, which is monic in x. The hyperbola $\mathrm{V}(x^2 + xy - 1)$ projects *onto* $\mathbb{A}^1(\overline{K})$ via $(x, y) \mapsto y$:



Inverting the coordinate change, we see that the original hyperbola $\mathrm{V}(xy-1)$ projects *onto* $\mathbb{A}^1(\overline{K})$ via $(x,y) \mapsto y-x$.

Now, we use the projection theorem to prove the Nullstellensatz:

Proof of the Nullstellensatz, Weak Version. Let I be an ideal of $K[x_1,\dots,x_n]$. If $1 \in I$, then $\mathrm{V}(I) \subset \mathbb{A}^n(\overline{K})$ is clearly empty. Conversely, suppose that $1 \notin I$. We have to show that $\mathrm{V}(I) \subset \mathbb{A}^n(\overline{K})$ is nonempty. This is clear if $n = 1$ or $I = \langle 0 \rangle$. Otherwise, apply a coordinate change ϕ as in Lemma 1.69 to a nonconstant polynomial $f \in I$. Then $\phi(f)$ is monic in x_1 as required by the projection theorem (adjust the nonconstant leading coefficient in x_1 to 1, if needed). Since $1 \notin I$, also $1 \notin \phi(I) \cap K[x_2,\dots,x_n]$. Inductively, we may assume that $\mathrm{V}(\phi(I) \cap K[x_2,\dots,x_n]) \subset \mathbb{A}^{n-1}(\overline{K})$ contains a point. By the projection theorem, this point is the image of a point in $\mathrm{V}(\phi(I))$ via $(x_1,x_2,\dots,x_n) \mapsto (x_2,\dots,x_n)$. In particular, $\mathrm{V}(\phi(I))$ and, thus, $\mathrm{V}(I)$ are nonempty. □

Remark 1.71 Let $\langle 0 \rangle \neq I \subsetneq K[x_1,\dots,x_n]$ be an ideal. Successively carrying out the induction step in the proof above, applying Lemma 1.69 at each stage, we may suppose after a lower triangular coordinate change

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ * & & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

that the coordinates are chosen such that *each* nonzero elimination ideal $I_{k-1} = I \cap K[x_k,\dots,x_n]$, $k = 1,\dots,n$, contains a monic polynomial of type

$$\begin{aligned} f_k &= x_k^{d_k} + c_1^{(k)}(x_{k+1},\dots,x_n)x_k^{d_k-1} + \ldots + c_{d_k}^{(k)}(x_{k+1},\dots,x_n) \\ &\in K[x_{k+1},\dots,x_n][x_k]. \end{aligned}$$

Then, considering vanishing loci over $\overline{K}$, *each* projection map

$$\pi_k : \mathrm{V}(I_{k-1}) \to \mathrm{V}(I_k),\ (x_k, x_{k+1},\dots,x_n) \mapsto (x_{k+1},\dots,x_n),$$

$k = 1,\dots,n-1$, is surjective.

Let $1 \leq c \leq n$ be minimal with $I_c = \langle 0 \rangle$.

If $c = n$, consider the composite map

$$\pi = \pi_{n-1} \circ \cdots \circ \pi_1 : \mathrm{V}(I) \to \mathrm{V}(I_{n-1}) \subsetneq \mathbb{A}^1(\overline{K}).$$

If $c < n$, consider the composite map

$$\pi = \pi_c \circ \cdots \circ \pi_1 : \mathrm{V}(I) \to \mathbb{A}^{n-c}(\overline{K}).$$

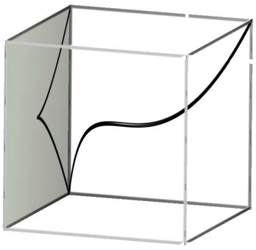
In either case, π is surjective since the π_k are surjective. Furthermore, these maps have finite fibers: if a point $(a_{k+1},\dots,a_n) \in \mathrm{V}(I_k)$ can be extended to a point $(a_k, a_{k+1},\dots,a_n) \in \mathrm{V}(I_{k-1})$, then a_k must be among the finitely many roots of the polynomial $f_k(x_k, a_{k+1},\dots,a_n) \in \overline{K}[x_k]$.

Remark 1.72 Given an ideal I as above and *any* set of coordinates $x_1,\dots,x_n$, let G be a Gröbner basis of I with respect to the lexicographic ordering $>_{\mathrm{lp}}$. Then, as will be clear from the definition of $>_{\mathrm{lp}}$ in Section 2.1, there are monic polynomials $f_k \in K[x_{k+1},\dots,x_n][x_k]$ as above iff such polynomials are among the elements of G (up to nonzero scalar factors). Furthermore, as already said in Remark 1.58, the ideal I_{k-1} is zero iff no element of G involves only $x_k,\dots,x_n$.

Singular Example 1.73 Consider the twisted cubic curve $C = \mathrm{V}(y - x^2, xy - z) \subset \mathbb{A}^3(\mathbb{C})$. Computing a lexicographic Gröbner basis for the ideal $\langle y - x^2, xy - z \rangle$, we get:

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

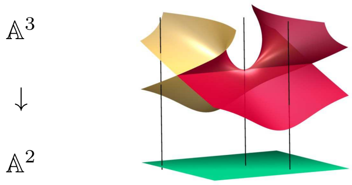
Here, no coordinate change is needed: The last Gröbner basis element $x^2 - y$ is monic in x, the first one $y^3 - z^2$ monic in y. Moreover, the other Gröbner basis elements depend on all variables x, y, z, so that $I_2 = \langle 0 \rangle$. Hence, C is projected *onto* the curve $C_1 = \mathrm{V}(y^3 - z^2)$ in the yz–plane, and C_1 is projected *onto* the z–axis which is a copy of $\mathbb{A}^1(\mathbb{C})$. The following picture shows the real points:



Intuitively, having a composition of projection maps

$$\pi = \pi_c \circ \cdots \circ \pi_1 : A = \mathrm{V}(I) \to \mathbb{A}^{n-c}(\overline{K})$$

which is surjective with finite fibers, the number $d = n - c$ should be the dimension of A:



(if $c = n$ in Remark 1.71, the dimension d of A should be zero). To make this a formal definition, one needs to show that the number d does not depend on the choice of the projection maps. This is more conveniently done on the algebraic side, using the ring theoretic analogue of Remark 1.71.

We need some terminology: If R is a subring of a ring S, we say that $R \subset S$ is a **ring extension**. More generally, if $R \to S$

is any injective ring homomorphism, we identify R with its image in S and consider, thus, $R \subset S$ as a ring extension.

With this terminology, the algebraic counterpart of the projection map $\pi_1 : \mathrm{V}(I) \to \mathrm{V}(I_1)$ is the ring extension

$$R = K[x_2, \dots, x_n]/I_1 \subset S = K[x_1, \dots, x_n]/I$$

which is induced by the inclusion $K[x_2, , \dots, x_n] \subset K[x_1, \dots, x_n]$. We may, then, rephrase the additional assumption of the projection theorem by saying that the element $\overline{x}_1 = x_1 + I \in S$ is integral over R in the following sense:

Definition 1.74 *Let $R \subset S$ be a ring extension. An element $s \in S$ is* ***integral over R*** *if it satisfies a monic polynomial equation*

$$s^d + r_1 s^{d-1} + \dots + r_d = 0, \text{ with all } r_i \in R.$$

The equation is, then, called an ***integral equation*** *for s over R. If every element $s \in S$ is integral over R, we say that S is* ***integral over R****, or that $R \subset S$ is an* ***integral extension****.*

Remark 1.75 Let $R \subset S$ be a ring extension.

(i) If $s_1, \dots, s_m \in S$ are integral over R, then $R[s_1, \dots, s_m]$ is integral over R.

(ii) Let $S \subset T$ be another ring extension. If T is integral over S, and S is integral over R, then T is integral over R.

In the situation of the projection theorem, the extension

$$R = K[x_2, \dots, x_n]/I_1 \subset S = K[x_1, \dots, x_n]/I$$

is integral since $S = R[\overline{x}_1]$ and $\overline{x}_1$ is integral over R.

Example 1.76 The extension

$$K[y] \to K[x, y]/\langle x^2 + xy - 1 \rangle$$

is integral while

$$K[y] \to K[x, y]/\langle xy - 1 \rangle$$

is not. Can the reader see why?

Problem 1.77 *Design an algorithm for checking whether a given extension of affine rings is integral.*

See Section 2.2.7 for an answer to this problem.

Returning to Remark 1.71, we now compose the algebraic counterparts of the projection maps π_k. Taking the second part of Remark 1.75 into account, we obtain the ring theoretic analogue of Remark 1.71:

Theorem 1.78 *Given an affine ring $S = K[x_1, \dots, x_n]/I \neq 0$, there are elements $y_1, \dots, y_d \in S$ such that:*

(i) *$y_1, \dots, y_d$ are algebraically independent over K.*
(ii) *$K[y_1, \dots, y_d] \subset S$ is an integral ring extension.*

If $y_1, \dots, y_d$ satisfy conditions (i) and (ii), the inclusion

$$K[y_1, \dots, y_d] \subset S$$

is called a ***Noether normalization*** *for S.*

This includes the case $d = 0$ in which the assertion means that S is a finite–dimensional K–vector space.

Problem 1.79 *Design an algorithm to find a Noether normalization for a given affine ring.*

In principle, a solution to this problem has already been given in Remark 1.72: Combine randomly chosen lower triangular coordinate changes with lexicographic Gröbner basis computations. The resulting algorithm will be presented in Section 2.2.8.

Singular Example 1.80 For the coordinate ring of the hyperbola $\mathrm{V}(xy - 1)$, Singular finds a coordinate change similar to the one we found in Example 1.70:

```
> ring R = 0, (x,y), dp;
> ideal I = xy-1;
> LIB "algebra.lib";
> noetherNormal(I);  // will implicitly use lp
[1]:
   _[1]=x
   _[2]=4x+y
[2]:
   _[1]=y
```

The result means that the map

$$K[y] \longrightarrow K[x,y]/\langle 4x^2 + xy - 1\rangle$$

constitutes a Noether normalization. Hence,

$$K[y-4x] \subset K[x,y]/\langle xy-1\rangle$$

is a Noether normalization. See also Example 2.48.

We can, now, give the definition of dimension:

Definition 1.81 *Let $I \subsetneq K[x_1,\dots,x_n]$ be a proper ideal, and let $A = \mathrm{V}(I)$ be its vanishing locus in $\mathbb{A}^n(\overline{K})$. If*

$$K[y_1,\dots,y_d] \subset K[x_1,\dots,x_n]/I$$

is a Noether normalization, we define d to be the ***dimension*** *of A, written*

$$\dim(A) = d.$$

Theorem 1.82 *The definition is independent of the choices made.*

In principle, we can compute the dimension by computing a Noether normalization.

Singular Example 1.83 As expected, the dimension of the twisted cubic curve is 1 (see Example 1.73), while that of the Whitney umbrella is 2:

```
> ring R = 0, (x,y,z), dp;
> ideal I = x2-y2z;
> LIB "algebra.lib";
> noetherNormal(I);
[1]:
   _[1]=x
   _[2]=3x+y
   _[3]=9x+3y+z
[2]:
   _[1]=y
   _[2]=z
```

Combining randomly chosen coordinate changes with lexicographic Gröbner basis computations to compute the dimension via a Noether normalization can be very slow.

Problem 1.84 *Design a fast algorithm for computing dimension.*

Being based on a Noether normalization

$$K[y_1, \ldots, y_d] \subset K[x_1, \ldots, x_n]/I,$$

our definition of the dimension of an algebraic set $A = \mathrm{V}(I) \subset \mathbb{A}^n(\overline{K})$ is algebraic in nature. In fact, we may as well say that d is the **dimension** of the affine ring $K[x_1, \ldots, x_n]/I$. The notion of Krull dimension allows us to assign a dimension to any ring:

Definition 1.85 *Let $R \neq 0$ be a ring. A sequence*

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m$$

*of prime ideals of R with strict inclusions is called a **chain of prime ideals** of R of **length** m. The **Krull dimension of R**, written $\dim(R)$, is the supremum of the lengths of such chains. If $I \subsetneq R$ is an ideal, the **Krull dimension of I**, written $\dim(I)$, is defined to be the dimension of R/I.*

For affine rings, we have, now, two notions of dimension. Using a refined version of the Noether normalization theorem, one can show that these notions agree.

Remark 1.86 According to what we said above, a proper ideal $I \subsetneq K[x_1, \ldots, x_n]$ is zero–dimensional iff $K[x_1, \ldots, x_n]/I$ is a finite–dimensional K–vector space. Recall from Section 1.1.6 that this means that the vanishing locus of I in $\mathbb{A}^n(\overline{K})$ is finite.

We will treat the computation of dimension in Section 2.3.

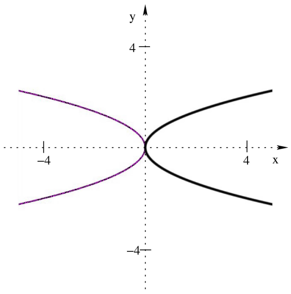
1.1.9 Local Studies

In the previous sections, we focused on the geometry of an algebraic set considered in its entirety. Rather than taking this global point of view, however, one is often interested in examining the behaviour of an algebraic set "near“ one of its points.

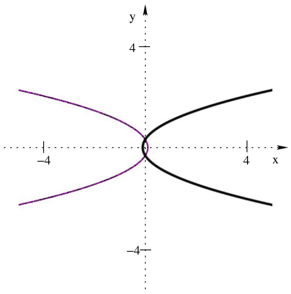
This local point of view will, for example, be taken when defining multiplicities of solutions in the sense discussed at the end of Section 1.1.6. A particular example where multiplicities occur is the classical theorem of Bézout. Given two plane curves C, D

defined by squarefree polynomials of degrees d, e without a common factor, the theorem states that C and D meet in $d \cdot e$ points, provided we work in the right setting, and provided we count the intersection points with multiplicities.

Working in the right setting means that we consider the curves in the projective plane over an algebraically closed field (we will treat projective spaces in Section 1.2.1). The intersection multiplicities, on the other hand, account for tangency:



The degree of tangency can be measured from a dynamical point of view: Slightly perturb the equations defining the curves and count the intersection points occuring near the point under examination:



A less intuitive but much more practical approach to local studies in general and intersection multiplicites in particular comes from algebra. We briefly explore this in what follows. To simplify our notation, we suppose that the point under consideration is the origin $o = (0, \ldots, 0)$ of $\mathbb{A}^n(K)$. The case of an arbitrary point $p = (a_1, \ldots, a_n) \in \mathbb{A}^n(K)$ can be dealt with by translating p to o (send x_i to $x_i - a_i$ for all i). When dealing with solutions over

$\overline{K}$, this requires that we extend K by adjoining each coordinate a_i not contained in K.

Polynomial functions are defined on all of $\mathbb{A}^n(K)$. Locally near o, in addition to the polynomial functions, we may consider functions obtained by inverting polynomial functions: If $f \in K[x_1, \dots, x_n]$ is not vanishing at o, the function $q \mapsto 1/f(q)$ is defined on the Zariski open neighborhood $\mathbb{A}^n(K) \setminus \mathrm{V}(f)$ of o in $\mathbb{A}^n(K)$. Algebraically, this leads us to enlarge $K[x_1, \dots, x_n]$ by considering the ring extension $K[x_1, \dots, x_n] \subset \mathcal{O}_o$, where $\mathcal{O}_o$ is the ring of fractions

$$\mathcal{O}_o := \left\{ \frac{g}{h} \;\middle|\; g, h \in K[x_1, \dots, x_n], h(o) \neq 0 \right\} \subset K(x_1, \dots, x_n).$$

Here, as usual, $K(x_1, \dots, x_n)$ denotes the field of rational functions in $x_1, \dots, x_n$ with coefficients in K. In particular, we think of g/h as an equivalence class under the equivalence relation given by $(g, h) \sim (g', h') \Longleftrightarrow gh' = hg'$.

Definition 1.87 *Let $I \subsetneq K[x_1, \dots, x_n]$ be a proper ideal, and let A be the vanishing locus of I in $\mathbb{A}^n(\overline{K})$. Suppose that $p \in A$ is an* ***isolated point of A****. That is, there is a Zariski open neighborhood of p in $\mathbb{A}^n(\overline{K})$ containing no other points of A. The* ***multiplicity of p as a solution of I****, written* $\operatorname{mult}(p \mid I)$*, is defined as follows: If $p = o$ is the origin, set*

$$\operatorname{mult}(o \mid I) = \dim_K(\mathcal{O}_o / I\mathcal{O}_o)$$

(here, $I\mathcal{O}_o$ denotes the ideal generated by I in $\mathcal{O}_o$). If p is different from o, translate p to o, extending K if needed, and apply the recipe above over the extended field.

Our final remark in Section 1.1.6 on counting solutions with multiplicities can now be made precise (see [Cox et al. (2005), Theorem 4.2.2] for a proof):

Proposition 1.88 *With notation as in Definition 1.87, suppose that A is finite (then each point of A is an isolated point of A).*

The following holds:

$$\dim_K(K[x_1,\ldots,x_n]/I) = \sum_{p\in A} \operatorname{mult}(p \mid I).$$

Example 1.89 If I is the ideal

$$I = \langle x+y+z-1,\ x^2+y^2+z^2-1,\ x^3+y^3+z^3-1\rangle \\ \subset \mathbb{Q}[x,y,z],$$

then $\mathbb{Q}[x,y,z]/I$ is a $\mathbb{Q}$–vector space of dimension 6 (see Example 1.55). On the other hand, the vanishing locus of I over $\overline{\mathbb{Q}}$ consists precisely of the three points

$$(1,0,0),\ (0,1,0),\ (0,0,1)$$

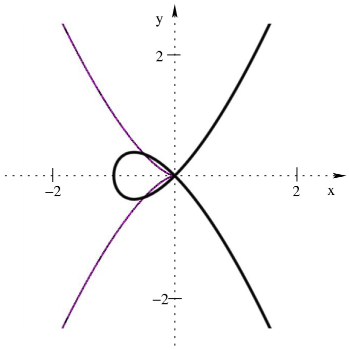
(see Example 0.7). Since it is clear from the symmetry of the generators of I that each point has the same multiplicity as a solution of I, we find that each point has multiplicity 2. How to compute this using Singular will be shown in Example 2.59.

With respect to the intersection multiplicities in Bézout's theorem, let two square–free polynomials $f,g \in K[x,y]$ without a common factor be given. Let $C,D \subset \mathbb{A}^2(\overline{K})$ be the curves defined by f,g, and let $p \in \mathbb{A}^2(\overline{K})$ be a point. Then the **i**ntersection multiplicity of C and D at p is defined to be

$$i_p(C,D) = \operatorname{mult}(p \mid \langle f,g\rangle).$$

Example 1.90 Consider the affine plane curves with equations

$$y^2 - x^2(x+1) = 0 \ \text{ and } \ y^2 + x^3 = 0\ :$$



Computing a lexicographic Gröbner basis, we see that the curves intersect in the three points

$$p = (0,0),\ q_1 = (-\tfrac{1}{2}, \tfrac{1}{4}\sqrt{2}),\ q_2 = (-\tfrac{1}{2}, -\tfrac{1}{4}\sqrt{2}):$$

```
> ring R = 0, (x,y), lp;
> ideal I = y2-x3-x2, y2+x3;
> groebner(I);
_[1]=8y4-y2
_[2]=2xy2+y2
_[3]=x2-2y2
```

In Example 2.58, we will use Singular to check that the intersection multiplicities are as follows:

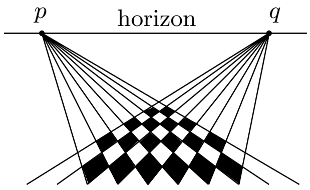
$$i_p(C,D) = 4,\ i_{q_1}(C,D) = i_{q_2}(C,D) = 1.$$

1.2 Projective Algebraic Geometry

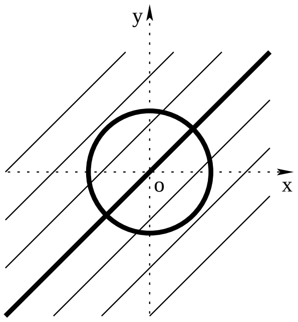
Example 1.90 at the end of the previous section shows that Bézout's theorem does not hold in the *affine* plane: Counted with multiplicity, the number of intersection points in $\mathbb{A}^2(\overline{\mathbb{Q}})$ is $4 + 1 + 1 = 6$, which is smaller than the product $3 \cdot 3 = 9$ of the degrees of the defining equations. To come up for the "missing" intersection points, we have to take the behaviour of the curves at infinity into account. Formally, this means that we will work in the projective space instead of the affine space. In this way, many statements in algebraic geometry become simpler in that cumbersome case by case considerations are avoided.

1.2.1 The Projective Space

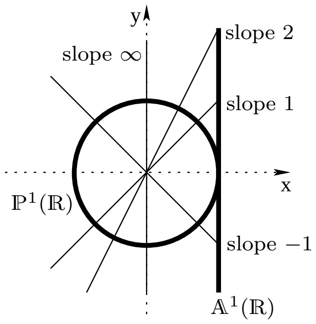
The idea of the projective plane goes back to Renaissance painters who considered "vanishing points" on the horizon to allow for perspective drawing:



The picture indicates that the missing intersection point of a class of parallel lines† in $\mathbb{A}^2(\mathbb{R})$ can be realized by asking that all lines in a given class meet in the same point at infinity, with different classes corresponding to different points. Note that each class contains precisely one line through, say, the origin o:



This line is determined by its slope, where the slope is either a real number or, in the case of the y–axis, ∞:



We may, thus, identify the set of all classes of parallel lines with the extended set

$$\mathbb{P}^1(\mathbb{R}) := \mathbb{A}^1(\mathbb{R}) \cup \{\infty\}.$$

This set is called the **real projective line**. Intuitively, we should think of the projective line as the horizon H (in the first picture of this section, the horizon is missing the point $\{\infty\}$, which in that picture corresponds to the class of lines parallel to the horizon).

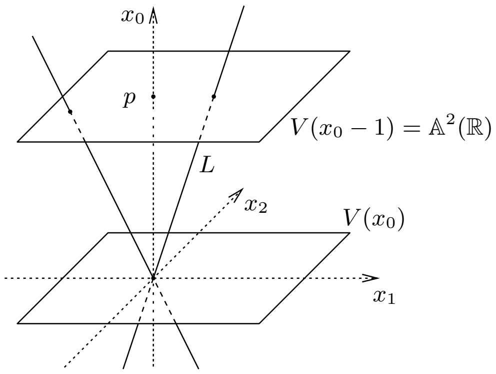
† A class of parallel lines consists of all lines parallel to a given line.

We may, then, define the **real projective plane** by adding all points on H to $\mathbb{A}^2(\mathbb{R})$:

$$\mathbb{P}^2(\mathbb{R}) := \mathbb{A}^2(\mathbb{R}) \cup H = \mathbb{A}^2(\mathbb{R}) \cup \mathbb{P}^1(\mathbb{R}).$$

A (projective) line in $\mathbb{P}^2(\mathbb{R})$ is, then, a line $L \subset \mathbb{A}^2(\mathbb{R})$ together with the common point at infinity of all lines parallel to L. Moreover, we regard H as a line in $\mathbb{P}^2(\mathbb{R})$, and call it the **line at infinity**. This makes sense since, now, any pair of distinct lines determines a unique point, and any pair of distinct points determines a unique line.

Using the above definition, it is cumbersome to work with $\mathbb{P}^2(\mathbb{R})$ since we do not represent its points on equal footing: A point in $\mathbb{A}^2(\mathbb{R})$ is represented by its coordinates, a point in H by a class of parallel lines. To motivate the formal definition given below, we note that – similar to $\mathbb{P}^1(\mathbb{R})$ – we may think of $\mathbb{P}^2(\mathbb{R})$ as the set of lines through the origin, this time through the origin o in $\mathbb{A}^3(\mathbb{R})$:



Here, we write x_0, x_1, x_2 for the coordinates on $\mathbb{A}^3(\mathbb{R})$ and choose $\mathrm{V}(x_0 - 1) \subset \mathbb{A}^3(\mathbb{R})$ as a reference plane for $\mathbb{A}^2(\mathbb{R})$. Then each point of $\mathbb{A}^2(\mathbb{R})$ determines a line in $\mathbb{A}^3(\mathbb{R})$ through o. In this way, we get all lines through o, except those lying in the plane $\mathrm{V}(x_0)$ which, in turn, form a copy of H.

We make the following general definition:

Definition 1.91 *The* ***projective n–space*** *over the field K is the set*

$$\begin{aligned}\mathbb{P}^n(K) &= \{\textit{lines through the origin in } \mathbb{A}^{n+1}(K)\}\\ &= \{\textit{one–dimensional linear subspaces of } K^{n+1}\}.\end{aligned}$$

We call $\mathbb{P}^1(K)$ and $\mathbb{P}^2(K)$ the ***projective line*** *and the* ***projective plane*** *over K, respectively.*

Considering a line L through the origin $o \in \mathbb{A}^{n+1}(K)$ as an element of the new space $\mathbb{P}^n(K)$, we call it a **point** of $\mathbb{P}^n(K)$. This point p is, then, determined (or represented) by any point $(a_0, \dots, a_n) \in L \setminus \{o\}$. Accordingly, we write $p = (a_0 : \dots : a_n)$, and call the tuple $(a_0, \dots, a_n)$ a set of **homogeneous coordinates** for p. Here, the colons indicate that the homogeneous coordinates are determined up to a nonzero scalar multiple (if $a_i \neq 0$, the ratios $a_j : a_i$ depend on p only).

Representing the points of $\mathbb{P}^n(K)$ in this way means that we regard $\mathbb{P}^n(K)$ as the quotient of $\mathbb{A}^{n+1}(K) \setminus \{o\}$ under the equivalence relation defined by $(a_0, \dots, a_n) \sim (b_0, \dots, b_n)$ iff $(a_0, \dots, a_n) = \lambda(b_0, \dots, b_n)$ for some $0 \neq \lambda \in K$:

$$\mathbb{P}^n(K) \cong \left(\mathbb{A}^{n+1}(K) \setminus \{o\}\right) / \sim,$$

and we have the **canonical projection**

$$\pi : \mathbb{A}^{n+1}(K) \setminus \{o\} \to \mathbb{P}^n(K),\ (a_0, \dots, a_n) \mapsto (a_0 : \dots : a_n).$$

1.2.2 Projective Algebraic Sets

Since homogeneous coordinates are determined up to scalar multiples only, the definition of vanishing loci in the projective setting has to be done with some care. To illustrate what may happen, consider the polynomial $f = y - x^2 \in \mathbb{Q}[x, y]$ and the point $p = (1 : 1) = (2 : 2) \in \mathbb{P}^1(\mathbb{Q})$: Clearly, $f(1, 1) = 0$, but $f(2, 2) \neq 0$. However, if a *homogeneous* polynomial $f \in K[x_0, \dots, x_n]$ is given, then $f(\lambda x_0, \dots, \lambda x_n) = \lambda^{\deg(f)} f(x_0, \dots, x_n)$ for all $\lambda \in K \setminus \{0\}$. This implies, then, that

$$f(a_0, \dots, a_n) = 0 \iff f(\lambda a_0, \dots, \lambda a_n) = 0 \ \text{ for all } \ \lambda \in K \setminus \{0\}.$$

Hence, if f is homogeneous, and $p = (a_0 : \cdots : a_n) \in \mathbb{P}^n(K)$, it makes sense to say whether $f(p) = 0$ or $f(p) \neq 0$.

Definition 1.92 *If $T \subset K[x_0, \ldots, x_n]$ is any set of homogeneous polynomials, its **vanishing locus** in $\mathbb{P}^n(K)$ is the set*

$$\mathrm{V}(T) = \{p \in \mathbb{P}^n(K) \mid f(p) = 0 \textit{ for all } f \in T\}.$$

*Every such set is called a **projective algebraic set**. If $T = \{f_1, \ldots, f_r\}$ is finite, we write $\mathrm{V}(f_1, \ldots, f_r) = \mathrm{V}(T)$.*

Example 1.93 The algebraic subsets of $\mathbb{P}^n(K)$ defined by homogeneous polynomials of degree 1 are precisely the subsets $\mathbb{P}(W) = \big\{\text{one–dimensional linear subspaces of } W\big\} \subset \mathbb{P}^n(K)$, where $W \subset K^{n+1}$ is a linear subspace. Every such subset is called a **linear subspace** of $\mathbb{P}^n(K)$ of dimension $\dim_K(W) - 1$.

To extend the correspondence between algebraic sets and ideals to the projective setting, we define:

Definition 1.94 *A **homogeneous ideal** of $K[x_0, \ldots, x_n]$ is an ideal generated by homogeneous polynomials.*

Note that any polynomial $f \in K[x_0, \ldots, x_n]$ can be uniquely written as a sum $f = f_0 + f_1 + f_2 + \ldots$, where the f_i are homogeneous of degree i. The f_i are called the **homogeneous components** of f. It is easy to see that an ideal I of $K[x_0, \ldots, x_n]$ is homogeneous iff for each $f \in I$, the homogeneous components of f are in I as well. Hence, by Hilbert's basis theorem, I is generated by finitely many *homogeneous* polynomials $f_1, \ldots, f_r$. We, then, define the **v**anishing locus $\mathrm{V}(I)$ of I in $\mathbb{P}^n(K)$ to be $\mathrm{V}(I) = \mathrm{V}(f_1, \ldots, f_r)$ (note that this definition is independent of the choice of homogeneous generators). In the same way, we define the vanishing locus $\mathrm{V}(I)$ of I in $\mathbb{P}^n(\overline{K})$.

Definition 1.95 *If $A \subset \mathbb{P}^n(K)$ is any subset, its **vanishing ideal** in $S = K[x_0, \ldots, x_n]$ is the homogeneous ideal*

$$\mathrm{I}(A) := \langle f \in S \mid f \textit{ is homogeneous and } f(p) = 0 \textit{ for all } p \in A\rangle.$$

The correspondences V and I behave as in the affine case, and notions such as **hypersurface**, **Zariski topology**, **irreducible** (or **subvariety** of $\mathbb{P}^n(K)$), and **irreducible component** are defined as earlier. The Nullstellensatz now reads as follows:

Theorem 1.96 (Hilbert's Nullstellensatz, Projective Version) *Let $I \subset K[x_0, \dots, x_n]$ be a homogeneous ideal. Then:*

(i) *The vanishing locus $\mathrm{V}(I)$ of I in $\mathbb{P}^n(\overline{K})$ is empty iff*

$$I \supset \langle x_0, \dots, x_n \rangle^k \ \text{ for some } \ k \geq 1.$$

(ii) *If $K = \overline{K}$ and $\mathrm{V}(I)$ is nonempty, then*

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

This version of the Nullensatz can be easily deduced from its affine versions (consider the vanishing locus of I in $\mathbb{A}^{n+1}(\overline{K})$). Note that the radical of a homogeneous ideal is homogeneous, too.

Corollary 1.97 *If $K = \overline{K}$, then there is an inclusion–reversing one–to–one correspondence*

$$\begin{gathered}\{\text{algebraic subsets of } \mathbb{P}^n(K)\} \\ \mathrm{V} \uparrow \downarrow I \\ \{\text{homogeneous radical ideals of } K[x_0, \dots, x_n] \\ \text{not equal to } \langle x_0, \dots, x_n \rangle\}.\end{gathered}$$

Here, subvarieties of $\mathbb{P}^n(K)$ correspond to homogeneous prime ideals of $K[x_0, \dots, x_n]$ other than $\langle x_0, \dots, x_n \rangle$.

1.2.3 Affine Charts and the Projective Closure

Our idea of taking infinity into account when considering affine algebraic sets fits nicely with our formal definitions in the projective setting. In fact, just as in our provisional definition of the real projective plane, we can write $\mathbb{P}^n(K)$ as the union of $\mathbb{A}^n(K)$ and a **hyperplane at infinity**:

$$\mathbb{P}^n(K) = U_0 \cup H_0 \cong \mathbb{A}^n(K) \cup \mathbb{P}^{n-1}(K),$$

where

$$U_0 := \{(a_0 : \dots : a_n) \in \mathbb{P}^n(K) \mid a_0 \neq 0\},$$

and H_0 is the complement $H_0 = \mathbb{P}^n(K) \setminus U_0 = \mathrm{V}(x_0)$. We identify H_0 with $\mathbb{P}^{n-1}(K)$ by disregarding the first coordinate, and U_0 with $\mathbb{A}^n(K)$ via

$$\begin{aligned} \varphi_0 : U_0 \to \mathbb{A}^n(K), \quad (a_0 : \cdots : a_n) &= (1 : \tfrac{a_1}{a_0} : \cdots : \tfrac{a_n}{a_0}) \\ &\mapsto (\tfrac{a_1}{a_0}, \ldots, \tfrac{a_n}{a_0}). \end{aligned}$$

This map is bijective, with inverse

$$\mathbb{A}^n(K) \to U_0,\ (b_1, \ldots, b_n) \mapsto (1 : b_1 : \cdots : b_n).$$

The algebraic concepts behind φ_0 and its inverse are dehomogenization and homogenization, respectively. We recall the definitions. Given a homogeneous polynomial $F \in K[x_0, x_1, \ldots, x_n]$, the polynomial $F(1, x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ is called the **dehomogenization** of F with respect to x_0. Conversely, given a polynomial $f \in K[x_1, \ldots, x_n]$, the polynomial

$$f^h := x_0^{\deg(f)} f(x_1/x_0, \ldots, x_n/x_0) \in K[x_0, x_1, \ldots, x_n]$$

is homogeneous of degree $\deg(f)$, and is called the **homogenization** of f with respect to x_0. We have

$$f^h(1, x_1, \ldots, x_n) = f \ \text{ and } F = x_0^s \cdot F(1, x_1, \ldots, x_n)^h,$$

where s is the highest power of x_0 dividing F.

It is immediate from the definitions that if $A = \mathrm{V}(T) \subset \mathbb{P}^n(K)$ is a projective algebraic set, given by a set of homogeneous polynomials $T \subset K[x_0, x_1, \ldots, x_n]$, and T_a is obtained from T by dehomogenizing each polynomial of T with respect to x_0, then $\varphi_0(A \cap U_0)$ is the affine algebraic set $\mathrm{V}(T_a) \subset \mathbb{A}^n(K)$. In what follows, we will identify $A \cap U_0$ with $\varphi_0(A \cap U_0)$. Vice versa, if $A = \mathrm{V}(T) \subset \mathbb{A}^n(K)$ is any affine algebraic set, where now T is a subset of $K[x_1, \ldots, x_n]$, then it is easy to check that $\varphi_0^{-1}(A)$ is the closed subset $\mathrm{V}(T^h) \cap U_0$ of U_0, where $T^h \subset K[x_0, \ldots, x_n]$ is obtained from T by homogenizing each element of T with respect to x_0. Regarding A as the subset $\varphi_0^{-1}(A) \subset \mathbb{P}^n(K)$, the following definition makes sense:

Definition 1.98 *If $A \subset \mathbb{A}^n(K) \cong U_0$ is an affine algebraic set, the smallest projective algebraic set $\overline{A}$ in $\mathbb{P}^n(K)$ containing A is called the **projective closure** of A.*

Proposition 1.99 *Let $A \subset \mathbb{A}^n(K) \cong U_0$ be an affine algebraic set, and let $\overline{A}$ be its projective closure in $\mathbb{P}^n(K)$. Then:*

(i) $\overline{A} \cap U_0 = A$.

(ii) *A is irreducible iff $\overline{A}$ is irreducible.*

(iii) *If $A = V_1 \cup \cdots \cup V_s$ is the decomposition into irreducible components, then $\overline{A} = \overline{V}_1 \cup \cdots \cup \overline{V}_s$ is the decomposition into irreducible components.*

In particular, no irreducible component of $\overline{A}$ is contained in the hyperplane at infinity.

Definition 1.100 *Let $I \subset K[x_1, \ldots, x_n]$ be an ideal. The **homogenization** of I with respect to an extra variable x_0 is the ideal*

$$I^h = \langle f^h \mid f \in I \rangle \subset K[x_0, \ldots, x_n].$$

Proposition 1.101 *Let $I \subset K[x_1, \ldots, x_n]$ be an ideal, and let I^h be its homogenization with respect to x_0. Considering vanishing loci over the algebraic closure $\overline{K}$ of K, we get: The projective algebraic set $\mathrm{V}(I^h) \subset \mathbb{P}^n(\overline{K})$ is the projective closure of the affine algebraic set $\mathrm{V}(I) \subset \mathbb{A}^n(\overline{K})$.*

We should point out that if finitely many generators for I are given, then the homogenized generators may fail to generate I^h. For an example and the solution to the computational problem below, see Section 2.2.10 in the next Chapter.

Problem 1.102 *Give an algorithm to find homogenized ideals.*

In the discussion above, there is nothing special with x_0: For $0 \le i \le n$, we define U_i, H_i and φ_i by using x_i instead of x_0. The U_i are known as the **(affine) coordinate charts** of $\mathbb{P}^n(K)$. They cover $\mathbb{P}^n(K)$:

$$\mathbb{P}^n(K) = \bigcup_{i=0}^{n} U_i.$$

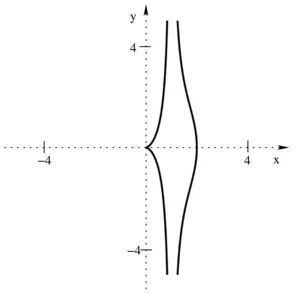
Hence, $\mathbb{P}^n(K)$ looks locally like $\mathbb{A}^n(K)$, and we may study a projective algebraic set $A \subset \mathbb{P}^n(K)$ by examining the different intersections $A \cap U_i$.

Example 1.103 The affine plane curve

$$\mathrm{V}((x^2+y^2)(x-1)^2-x^2)\subset\mathbb{A}^2(\mathbb{R})$$

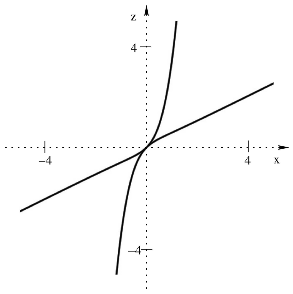
is known as the **conchoide of Nicomedes**. Its projective closure C is defined by the equation $(x^2+y^2)(x-z)^2-z^2x^2=0$. We show C in all three coordinate charts:

$z=1$



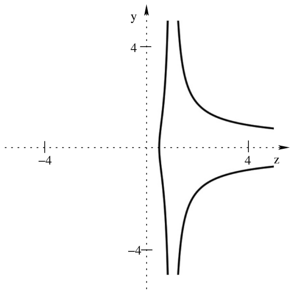
$(x^2+y^2)(x-1)^2-x^2=0$

$y=1$



$(x^2+1)(x-z)^2-z^2x^2=0$

$x=1$



$(1+y^2)(1-z)^2-z^2=0$

To see all affine charts simultaneously, consider their preimage under the restriction of the projection $\mathbb{A}^3(\mathbb{R})\setminus\{0\}\to\mathbb{P}^2(\mathbb{R})$ to the unit sphere $\mathrm{V}(x^2+y^2+z^2-1)\subset\mathbb{A}^3(\mathbb{R})$:

In the picture, the great circles shown in black correspond to the respective lines $\mathrm{V}(z)$, $\mathrm{V}(y)$, and $\mathrm{V}(x)$ at infinity. The curve C is shown in white.

Using coordinate charts, the notion of dimension carries over from the affine to the projective setting:

Definition 1.104 *The* ***dimension*** *of a projective algebraic subset* $A = \mathrm{V}(T) \subset \mathbb{P}^n(\overline{K})$*, written* $\dim(A)$*, is the number*

$$\dim(A) = \max\{\dim(A \cap U_i) \mid i = 0, \ldots, n\}.$$

One can show that this number is one less than the dimension of the affine algebraic set defined by T in $\mathbb{A}^{n+1}(\overline{K})$.

1.2.4 The Hilbert Polynomial

Let $S = K[x_0, \ldots, x_n]$. Recall that each polynomial $f \in S$ can be uniquely written as the sum of its homogeneous components. Ring theoretically, this means that S can be written as the direct sum $S = \bigoplus_{d \geq 0} S_d$, where S_d consists of the homogeneous polynomials of degree d. This decomposition is compatible with multiplication in the sense that $S_d \cdot S_e \subset S_{d+e}$. We refer to this fact by saying that S is a **graded ring**. In the same spirit, an ideal $I \subset S$ is homogeneous iff it can be written as a direct sum

$$I = \bigoplus_{d \geq 0} (I \cap S_d).$$

In turn, this means that the quotient ring S/I inherits a grading

$$S/I = \bigoplus_{d \geq 0} (S/I)_d = \bigoplus_{d \geq 0} S_d/(I \cap S_d).$$

To simplify our notation in what follows, we will write $M = S/I$ and, accordingly, $M_d = (S/I)_d$.

Definition 1.105 *The function*

$$\mathrm{H}_M : \mathbb{N} \to \mathbb{N},\; d \mapsto \dim_K(M_d),$$

is called the ***Hilbert function*** *of* M. *The formal power series*

$$\mathrm{HP}_M(t) := \sum_{d \geq 0} \mathrm{H}_M(d) \cdot t^d \in \mathbb{Z}[[t]]$$

is called the ***Hilbert–Poincaré series*** *of* M.

Hilbert showed that the infinitely many values of the Hilbert function can be expressed in finite terms:

Theorem 1.106 (Polynomial Nature of the Hilbert Function) *There exists a unique polynomial* $\mathrm{P}_M(t) \in \mathbb{Q}\,[t]$ *such that*

$$\mathrm{H}_M(d) = \mathrm{P}_M(d) \;\; \textit{for all} \;\; d \gg 0.$$

This polynomial is called the ***Hilbert polynomial*** *of* $M = S/I$.

Remark 1.107 An important fact is that the degree of $\mathrm{P}_M(t)$ is equal to $\dim(I) - 1$. In algebraic geometry, the Hilbert polynomial is used to rediscover or define numerical invariants of projective algebraic sets and their embedding. For this purpose, if $A \subset \mathbb{P}^n(\overline{K})$ is a projective algebraic set with **homogeneous coordinate ring** $\overline{K}[A] = \overline{K}[x_0, \dots, x_n]/\mathrm{I}(A)$, we define the **Hilbert polynomial** of A to be the polynomial $\mathrm{P}_A(t) = \mathrm{P}_{\overline{K}[A]}(t)$. Then the degree d of P_A is the dimension of A. The **degree** of A, written $\deg(A)$, is defined to be $d!$ times the leading coefficient of $\mathrm{P}_A(t)$. Geometrically, this is the number of points in which A meets a sufficiently general linear subspace of $\mathbb{P}^n(\overline{K})$ of complementary dimension $n - d$. Furthermore, the **arithmetic genus** of A is defined to be $p_a(A) = (-1)^d\big(\mathrm{P}_A(0) - 1\big)$. It is, then, clear that the Hilbert polynomial of a projectice algebraic curve C is of type $\mathrm{P}_C(t) = \deg(C) \cdot t - p_a + 1$. Note that invariants of algebraic sets are often useful in that they allow us to partition a given classification problem into more handy pieces. See [Decker and Schreyer (2013)] for more details.

Another way of expressing the infinitely many values of the Hilbert function in finite terms is to represent the Hilbert–Poincaré series as a rational function. There are two ways of doing this:

Theorem 1.108 (Representation of the Hilbert–Poincaré Series I) *There exists a unique polynomial $Q_M(t) \in \mathbb{Z}[t]$ such that*

$$\mathrm{HP}_M(t) = \frac{Q_M(t)}{(1-t)^n}\,.$$

Theorem 1.109 (Representation of the Hilbert–Poincaré Series II) *Let $d = \deg(\mathrm{P}_M(t)) = \dim(I) - 1$. There exists a unique polynomial $\widehat{Q}_M(t) \in \mathbb{Z}[t]$ with $\widehat{Q}_M(1) \neq 0$ and such that*

$$\mathrm{HP}_M(t) = \frac{\widehat{Q}_M(t)}{(1-t)^{d+1}}\,.$$

Problem 1.110 *Give algorithms for finding the Hilbert–Poincaré series and the Hilbert polynomial, respectively.*

Remark 1.111 The computation of the Hilbert polynomial can be reduced to that of the Hilbert–Poincaré series represented as in Theorem 1.109. Indeed, if $\widehat{Q}_M^{(i)}$ denotes the ith formal derivative of $\widehat{Q}_M$ (defined by mimicking the usual rules of differentiation), and if we set

$$a_i = \frac{\widehat{Q}_M^{(i)}(1)}{i!}\,, \quad i = 0, \ldots, d\,,$$

then

$$\mathrm{P}_M(t) = \sum_{i=0}^{d} (-1)^{d-i} a_{d-i} \binom{t+i}{i}\,.$$

We will come back to this in Section 2.3, where we will show how to compute the Hilbert–Poincaré series and give Singular examples.

2
Computing

In this chapter, we will present solutions to the computational problems stated in the previous chapter. We will give the most important definitions and theorems, some proofs, and a number of examples. All proofs can be found in [Greuel and Pfister (2007)]. Most of the SINGULAR examples can be found on the CD in [Greuel and Pfister (2007)]. We will, again, work over a field K.

2.1 Standard Bases and SINGULAR

We begin by introducing a general and flexible notion of monomial ordering. Relying on this, we will treat the concept of standard bases, which is more general than that of Gröbner bases. In fact, standard bases will allow us to compute not only in

- polynomial rings and
- quotient rings of polynomial rings,

but also in

- localizations of the above.

In geometrical applications, the latter is needed for local studies as in Section 1.1.9.

To simplify our notation, we write $K[x] = K[x_1, \ldots, x_n]$ for the polynomial ring over K in the set of variables $x = \{x_1, \ldots, x_n\}$. As in the previous chapter, a monomial in $x = \{x_1, \ldots, x_n\}$ is written using multi–indices: If $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, set $x^\alpha =$

$x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ and $\deg(x^\alpha) = \alpha_1 + \cdots + \alpha_n$. We write

$$\mathrm{Mon}_n := \mathrm{Mon}(x_1, \ldots, x_n) := \{x^\alpha \mid \alpha \in \mathbb{N}^n\}.$$

Each nonzero polynomial $f \in K[x]$ is a K–linear combination of different monomials, with nonzero scalars. Our starting point is that this representation of f is only determined up to the order of its summands. We can make this order unique by choosing a total ordering on the set of monomials. For our purposes, it is necessary that the orderings considered are compatible with the semigroup structure on the set of monomials.

Definition 2.1 *A **monomial ordering** (or **semigroup ordering) on $\mathbf{Mon}_n$** is a total ordering*† $>$ *on* Mon_n *satisfying*

$$x^\alpha > x^\beta \Longrightarrow x^\gamma x^\alpha > x^\gamma x^\beta, \quad \textit{for all} \;\; \alpha, \beta, \gamma \in \mathbb{N}^n.$$

If R is any ring, and $>$ is a monomial ordering on Mon_n*, then we also say that $>$ is a **monomial ordering on $R[x]$**.*

Definition 2.2 *Let $>$ be a fixed monomial ordering on* Mon_n*. Given a polynomial $0 \neq f \in K[x]$, we write it in a unique way as a sum of nonzero terms:*

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

with $a_\alpha, a_\beta, \ldots, a_\gamma \in K$. Then we define:

$$\begin{aligned}
\mathrm{LM}(f) &:= \texttt{leadmonom(f)} := x^\alpha, \\
\mathrm{LE}(f) &:= \texttt{leadexp(f)} := \alpha, \\
\mathrm{LT}(f) &:= \texttt{lead(f)} := a_\alpha x^\alpha, \\
\mathrm{LC}(f) &:= \texttt{leadcoef(f)} := a_\alpha, \\
\mathrm{tail}(f) &:= f - \mathrm{LT}(f) = a_\beta x^\beta + \cdots + a_\gamma x^\gamma, \\
\mathrm{ecart}(f) &:= \deg(f) - \deg(\mathrm{LM}(f)).
\end{aligned}$$

† Given a relation $\geq$ on a set M and $a, b \in M$, we write $a > b$ if $a \geq b$ and $a \neq b$. We then call $>$ a *total ordering* on M if $\geq$ is a total ordering on M. That is, the following hold for all $a, b, c \in M$: (1) If $a \geq b$ and $b \geq a$, then $a = b$ (*Antisymmetry*). (2) If $a \geq b$ and $b \geq c$, then $a \geq c$ (*Transitivity*). (3) $a \geq b$ or $b \geq a$ (*Totality*).

We refer to these data as the ***leading monomial****, the* ***leading exponent****, the* ***leading term****, the* ***leading coefficient****, the* ***tail****, and the* ***ecart*** *of f, respectively.*

Singular Example 2.3 With respect to the lexicographical ordering $>_{\mathrm{lp}}$ (formally defined in Example 2.7 below), we get:

```
> ring R = 0, (x,y,z), lp;
> poly f = y4z3+2x2y2z2+3x5+4z4+5y2;
> f;                          // display f in a lex-ordered way
3x5+2x2y2z2+y4z3+5y2+4z4
> leadmonom(f);               // leading monomial
x5
> leadexp(f);                 // leading exponent
5,0,0
> lead(f);                    // leading term
3x5
> leadcoef(f);                // leading coefficient
3
> f - lead(f);                // tail
2x2y2z2+y4z3+5y2+4z4
```

Definition 2.4 *A monomial ordering $>$ on* Mon_n *is called*

(i) ***global*** *if $x^\alpha > 1$ for all $\alpha \neq (0,\dots,0)$,*
(ii) ***local*** *if $x^\alpha < 1$ for all $\alpha \neq (0,\dots,0)$, and*
(iii) ***mixed*** *if it is neither global nor local.*

Remark 2.5

(i) Since a monomial ordering is compatible with the semigroup structure on Mon_n, it suffices to check the defining conditions above for the variables x_i, $i = 1,\dots,n$.
(ii) Mixed orderings are needed, for instance, to eliminate variables with respect to a local monomial ordering (see Example 2.34). They will not play a role in this book.

Lemma 2.6 *Let $>$ be a monomial ordering on* Mon_n. *Then the following are equivalent:*

(i) *$>$ is a well–ordering*†.
(ii) *$>$ is global.*

† A *well–ordering* is a total ordering on a set such that each nonempty subset has a least element.

Proof To show (i) $\Rightarrow$ (ii), suppose that $>$ is not global, so that $x_i < 1$ for some i. Then $\{(x_i)^n\}_{n\geq 0}$ is a set of monomials with no least element, so that $>$ is not a well–ordering. Conversely, to show (ii) $\Rightarrow$ (i), suppose that $>$ is global, and let $\mathfrak{M} \subset \mathrm{Mon}_n$ be a nonempty set of monomials. Then, by Dickson's Lemma 1.5, the ideal generated by $\mathfrak{M}$ in $K[x]$ is, in fact, generated by a finite subset $\mathfrak{L} \subset \mathfrak{M}$. This means that every element $x^\beta \in \mathfrak{M}$ is divisible by an element $x^\alpha \in \mathfrak{L}$. But then $x^\alpha < x^\beta$ since $x_i > 1$ for all i. We conclude that the least element of $\mathfrak{L}$ (which exists since $\mathfrak{L}$ is finite) is a least element of $\mathfrak{M}$. □

Example 2.7 The following are examples of monomial orderings:

(i) The **lexicographical ordering** $>_{\mathrm{lp}}$:

$$\begin{aligned} x^\alpha >_{\mathrm{lp}} x^\beta \quad :\Leftrightarrow \quad & \exists\, 1 \leq i \leq n :\ \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \\ & \alpha_i > \beta_i \,. \end{aligned}$$

(ii) The **degree reverse lexicographical ordering** $>_{\mathrm{dp}}$:

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

(iii) The **local lexicographical ordering** $>_{\mathrm{ls}}$:

$$\begin{aligned} x^\alpha >_{\mathrm{ls}} x^\beta \quad :\Leftrightarrow \quad & \exists\, 1 \leq i \leq n :\ \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \\ & \alpha_i < \beta_i \,. \end{aligned}$$

(iv) The **local degree reverse lexicographical ordering** $>_{\mathrm{ds}}$:

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

(v) **Product orderings**: Let $>_1$ and $>_2$ be monomial orderings on $\mathrm{Mon}(x_1, \ldots, x_s)$ and $\mathrm{Mon}(x_{s+1}, \ldots, x_n)$, respectively. The **product ordering** $> \;=\; (>_1, >_2)$ is defined by

$$\begin{aligned} x^\alpha > x^\beta \quad :\Leftrightarrow \quad & x_1^{\alpha_1}\cdots x_s^{\alpha_s} >_1 x_1^{\beta_1}\cdots x_s^{\beta_s} \text{ or} \\ & \big(x_1^{\alpha_1}\cdots x_s^{\alpha_s} = x_1^{\beta_1}\cdots x_s^{\beta_s} \text{ and} \\ & \quad x_{s+1}^{\alpha_{s+1}}\cdots x_n^{\alpha_n} >_2 x_{s+1}^{\beta_{s+1}}\cdots x_n^{\beta_n}\big)\,. \end{aligned}$$

(vi) **Matrix orderings**†: Let $M \in \mathrm{GL}(n,\mathbb{R})$‡, and denote the rows of M by $m_1,\dots,m_n$. Then set:

$$\begin{aligned} x^\alpha >_M x^\beta \quad :\Leftrightarrow \quad & \exists\, 1 \le i \le n :\; m_1\alpha = m_1\beta,\dots, \\ & m_{i-1}\alpha \;= m_{i-1}\beta,\; m_i\alpha > m_i\beta\,. \end{aligned}$$

Note that $>_{\mathrm{lp}}$ and $>_{\mathrm{dp}}$ are global. A product ordering $(>_1,>_2)$ is global iff $>_1$ and $>_2$ are global. The characterization of global matrix orderings is left as an exercise for the reader.

Singular Example 2.8

```
> ring R1 = 0, (x,y,z,t), lp;
> poly p = 3x+y2+7z3+8t; p;
3x+y2+7z3+8t
> ring R2 = 0, (x,y,z,t), dp;
> poly p = imap(R1,p);  // maps p from R1 to R2
> p;
7z3+y2+3x+8t
> ring R3 = 0, (x,y,z,t), ls;
> poly p = imap(R1,p); p;
8t+7z3+y2+3x
> ring R4 = 0, (x,y,z,t), (dp(2),ds(2));  // product ordering
> poly p = imap(R1,p); p;
y2+3x+8t+7z3
> ring R5 = 0,(x,y,z,t), M(-1,-1,1,1,1,0,0,0,0,1,0,0,0,0,1,0);
> poly p = imap(R1,p); p;
7z3+8t+3x+y2
```

Lemma 2.9 *Let $>$ be a monomial ordering on* Mon_n. *Then*

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

is a ***multiplicatively closed set****. That is,* $1 \in S_>$ *and the product of any two elements of* $S_>$ *is in* $S_>$.

† Every monomial ordering can be defined by a matrix (see [Greuel and Pfister (2007)]).

‡ If K is any field, $\mathrm{GL}(n,K)$ denotes the *general linear group* consisting of all invertible $n \times n$ matrix with entries in K.

Proof For $f, g \in K[x] \smallsetminus \{0\}$, we have $\mathrm{LM}(fg) = \mathrm{LM}(f)\mathrm{LM}(g)$. □

The technique of localizing rings at multiplicatively closed sets is central to commutative algebra. It has important applications in the local study of algebraic sets (this is where the name localization comes from). By localizing at the multiplicative closed subset $K[x] \setminus \langle x \rangle$, for instance, we get the ring of fractions $\mathcal{O}_0$ considered in Section 1.1.9. In the algebraic setting, this ring is usually denoted by $K[x]_{\langle x \rangle}$. In the context of standard bases, the general definition of localization boils down to the following: If $>$ is any monomial ordering on Mon_n, then set

$$K[x]_> := S_>^{-1}K[x] = \left\{ \frac{f}{u} \;\middle|\; f, u \in K[x],\ u \neq 0,\ \mathrm{LM}(u) = 1 \right\} .$$

Here, f/u denotes the equivalence class of $(f, u) \in K[x] \times S_>$ under the equivalence relation defined by

$$(f, u) \sim (f', u') \Longleftrightarrow fu' = uf'.$$

The set $K[x]_>$ becomes a ring, with algebraic operations

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}, \quad \frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}.$$

Definition 2.10 *If $>$ is a monomial ordering on* Mon_n*, then the* ***localization of $K[x]$ with respect to $S_>$*** *(or the* ***ring associated to $K[x]$ and $>$****) is the ring $K[x]_>$ defined above.*

In what follows, $>$ will denote a fixed monomial ordering on Mon_n.

Remark 2.11 The following properties are easy to prove:

(i) There are canonical inclusions

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

(ii) $K[x]_> = K[x]$ iff $S_> = K \setminus \{0\}$ iff $>$ is global.

(iii) $K[x]_> = K[x]_{\langle x \rangle}$ iff $S_> = K[x] \setminus \langle x \rangle$ iff $>$ is local.

Definition 2.12 *Given $0 \neq f \in K[x]_>$, we choose $u \in K[x] \setminus \{0\}$ such that $\mathrm{LT}(u) = 1$ and $uf \in K[x]$. Then, generalizing the* *notions introduced in Definition 2.2 for polynomials, we define:*†

$$\begin{aligned} \mathrm{LM}(f) &:= \mathrm{LM}(uf), & \mathrm{LE}(f) &:= \mathrm{LE}(uf),\\ \mathrm{LT}(f) &:= \mathrm{LT}(uf), & \mathrm{LC}(f) &:= \mathrm{LC}(uf),\\ \mathrm{tail}(f) &:= f - \mathrm{LT}(f). \end{aligned}$$

Definition 2.13 *For any subset $G \subset K[x]_>$, the* ***leading ideal*** *of G is the ideal of $K[x]$ defined by*

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

Definition 2.14 *Let $I \subset K[x]_>$ be an ideal.*

(i) *A finite set $G \subset K[x]_>$ is called a* ***standard basis***‡ *of I if*

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

That is, the leading monomials of the elements of G generate the leading ideal of I or, in turn, for any $f \in I \setminus \{0\}$ there exists an element $g \in G$ such that $\mathrm{LM}(g)|\mathrm{LM}(f)$.

(ii) *If we just say that G is a standard basis, we mean that G is a standard basis of the ideal $\langle G\rangle_{K[x]_>}$ generated by G.*

(iii) *If $>$ is global, a standard basis is also called a* ***Gröbner basis****.*

Proposition 2.15 *Each nonzero ideal $I \subset K[x]_>$ has a standard basis G, consisting of elements in $K[x]$. Moreover, if $g, h \in G$ and $\mathrm{LM}(g)|\mathrm{LM}(h)$, then $G \setminus \{h\}$ is also a standard basis of I.*

Proof By Dickson's Lemma 1.5, $\mathrm{L}(I)$ is generated by a finite set of leading monomials $\mathrm{LM}(f)$, $f \in I$. That is, there are $f_1, \dots, f_r \in I$ such that $\mathrm{L}(I) = \langle \mathrm{LM}(f_1), \dots, \mathrm{LM}(f_r)\rangle$. Clearing denominators, we may assume that the f_i are in $K[x]$, proving the first statement. The second statement holds since $\mathrm{L}(G) = \mathrm{L}(G \setminus \{h\})$. □

† It is easy to see that the definition does not depend on the choice of u.

‡ As already said in the previous chapter, the idea of standard bases goes back to Gordan [Gordan (1899)]. Later, monomial orderings were used by Macaulay [Macaulay (1939)] and Gröbner [Gröbner (1939)] to study Hilbert functions of graded ideals and, more generally, to find K–bases of zero–dimensional quotient rings. Formally, the notion of a standard basis was introduced independently by Hironaka [Hironaka (1964)] and Grauert [Grauert (1972)] (for special local orderings). The name Gröbner basis in the case of global orderings was coined by Buchberger [Buchberger (1965)].

Definition 2.16 *A standard basis $G = \{f_1, \dots, f_r\}$ is called a* ***reduced standard basis*** *if the following hold for all i:*

(i) $\mathrm{LC}(f_i) = 1$.
(ii) $\mathrm{LM}(f_i)$ *is not divisible by* $\mathrm{LM}(f_j)$*, for $j \neq i$.*
(iii) *No monomial of* $\mathrm{tail}(f_i)$ *is divisible by* $\mathrm{LM}(f_j)$*, for all j.*

Remark 2.17 If $>$ is global and, hence, a well–ordering, each nonzero ideal of $K[x]$ has a unique reduced Gröbner basis.

Singular Example 2.18

```
> ring R = 0, (x,y), dp;  // a global ordering
> ideal I = x3+2y2+5,  x3+3y2+x+5;
> ideal GI = std(I);  // compute a standard (Groebner) basis
> GI;
GI[1]=y2+x
GI[2]=x3+3y2+x+5
> option(redSB);       // to obtain a reduced standard basis
> GI = std(GI);   GI;
J[1]=y2+x
J[2]=x3-2x+5
```

The computation of standard bases as in the example above is based on a practical standard basis criterion. For this, we need:

Definition 2.19 *Let $f, g \in K[x] \setminus \{0\}$ with $\mathrm{LM}(f) = x^\alpha$ and $\mathrm{LM}(g) = x^\beta$. Let $x^\gamma := \mathrm{lcm}(x^\alpha, x^\beta)$ be the least common multiple of x^α and x^β.*† *We define the* s–***polynomial*** *of f and g by*

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

If $\mathrm{LM}(g)$ *divides* $\mathrm{LM}(f)$*, the s–polynomial is particularly simple:*

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

and $\mathrm{LM}\big(\mathrm{spoly}(f,g)\big) < \mathrm{LM}(f)$.

Before we show how to implement the s–polynomial in Singular, we note that we can use Singular's C–like user language, in particular, to define procedures which combine several commands to form a new one. A procedure definition begins with the keyword

† Note that $\gamma = \big(\max(\alpha_1, \beta_1), \dots, \max(\alpha_n, \beta_n)\big)$.

`proc` followed by a name and an optional parameter list with specified SINGULAR types. Return values of a procedure can be specified by using the `return` command.

Singular Example 2.20 We implement s–polynomials:

```
> ring R = 0, (x,y,z,t), lp;
> proc spoly(poly f, poly g)
. {
.    poly m = lcm(leadmonom(f),leadmonom(g));
.    poly h = m/leadmonom(f)*f
.           -leadcoef(f)/leadcoef(g)*m/leadmonom(g)*g;
.    return(h);
. }
> poly f = 7x3y+zt;   poly g = 8xyzt+y2;
> spoly(f,g);
-7/8x2y2+z2t2
```

In view of the desired standard bases criterion, but also with regard to actually computing standard bases, the notions of normal form (for global monomial orderings) and weak normal form (for nonglobal monomial orderings) are crucial. The global case is technically simpler and therefore treated first. The idea behind normal forms is to extend Euclidean division with remainder to polynomials in several variables, allowing at the same time more than one divisor. We will later present an axiomatic approach which will specify the properties of normal forms. For now, we introduce **normal forms** by giving an algorithm to compute them:

Algorithm 1 NF($f \mid G$)

```
Input: $>$ a global monomial ordering, $f \in K[x]$, $G$ a finite list of
    elements in $K[x]$
Output: $h \in K[x]$, a normal form of $f$ with respect to $G$
    if $f = 0$ then
      return 0;
    $h := f$;
    while $h \neq 0$ and $T_h := \{g \in G \mid \mathrm{LM}(g)|\mathrm{LM}(h)\} \neq \emptyset$ do
      choose the first $g \in T_h$;
      $h := \mathrm{spoly}(h, g)$;
    return $h$;
```

Remark 2.21 The algorithm terminates since $>$ is global and, thus, a well–ordering, and since always $\mathrm{LM}(h) > \mathrm{LM}(\mathrm{spoly}(h, g))$. If $h = \mathrm{NF}(f \mid G) \neq 0$, then $\mathrm{LM}(h)$ is not divisible by any $\mathrm{LM}(g)$, $g \in G$. If we replace the last line of the algorithm by the line

$$\textbf{return}\ \ \mathrm{LT}(h) + \mathrm{NF}(\mathrm{tail}(h) \mid G);$$

then none of the monomials of the normal form is divisible by any $\mathrm{LM}(g)$, $g \in G$. We will, then, speak of a **reduced normal form**.

Singular Example 2.22

```
> ring R = 0, (x,y,z), dp;
> poly f = x2yz+xy2z+y2z+z3+xy;
> poly f1 = xy+y2-1;   poly f2 = xy;   ideal I = f1, f2;
> reduce(f,I);
// ** I is no standard basis
y2z+z3                // reduced NF w.r.t. a non-standard basis
> I = f2,f1;
> reduce(f,I);
// ** I is no standard basis
y2z+z3-y2+xz+1        // reduced NF for a different numbering in I
> ideal GI = std(I);  // a standard (Groebner) basis of I
> GI;
GI[1]=x
GI[2]=y2-1
> reduce(f,GI,1);     // 3rd parameter 1 avoids tail reduction
z3+xy+z
> reduce(f,GI);       // reduced NF
z3+z
```

Still focusing on the global case, we now formulate the desired standard basis criterion:

Theorem 2.23 (Buchberger's Criterion) *Let $I \subset K[x]$ be an ideal, let $G = \{g_1, \dots, g_s\} \subset I$, and let $>$ be a global monomial ordering on* Mon_n*. Then the following are equivalent:*

(i) *G is a standard basis of I.*
(ii) *For all $f \in K[x]$, we have* $\mathrm{NF}(f \mid G) = 0$ *iff $f \in I$.*
(iii) $\mathrm{NF}(\mathrm{spoly}(g_i, g_j) \mid G) = 0$ *for all $i < j$.*

Proof (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) are consequences of Proposition 2.27 below: note that $\mathrm{spoly}(g_i, g_j) \in I$ for all $i < j$. (iii) $\Rightarrow$ (i) is the difficult part. See [Greuel and Pfister (2007)] for details. □

The criterion yields the following standard basis algorithm:

Algorithm 2 std($f \mid F$)

```
Input: $>$ a global monomial ordering, $F \subset K[x]$ a finite set of
    polynomials
Output: $G$, a standard basis of $\langle F \rangle$
  $G := F$;
  $P := \{(f,g) \mid f,g \in G\}$;
  while $P \neq \emptyset$ do
    choose $(f,g) \in P$;
    $P := P \smallsetminus \{(f,g)\}$;
    $h := \mathrm{NF}(\mathrm{spoly}(f,g) \mid G)$;
    if $h \neq 0$ then
      $P := P \cup \{(f,h) \mid f \in G\}$;
      $G := G \cup \{h\}$;
  return $G$;
```

Now, we address the nonglobal case:

Remark 2.24 Theorem 2.23 is also true for a nonglobal monomial ordering $>$ if we replace $K[x]$ by $K[x]_>$ and if we choose a weak normal form NF as in Definition 2.25 below. Whereas normal forms may not exist in the nonglobal case, weak normal forms can be computed by Algorithm 3 below. Based on this, Algorithm 2 will compute a polynomial standard basis of $\langle F \rangle_{K[x]_>}$.†

Definition 2.25 *Let $>$ be any monomial ordering on $K[x]$, and let $\mathcal{G}$ denote the set of all finite lists $G \subset K[x]_>$. Then a map*

$$\mathrm{NF} : K[x]_> \times \mathcal{G} \to K[x]_>,\ (f,G) \mapsto \mathrm{NF}(f \mid G)\,,$$

*is called a **weak normal form** on $K[x]_>$ if, for all $G \in \mathcal{G}$,*

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

† For global orderings, Algorithm 2.1 is Buchberger's algorithm, which generalizes both Gaussian elimination and Euclid's gcd algorithm. For local orderings, it is *Mora's tangent cone algorithm*, which itself is a variant of Buchberger's algorithm. The general case is a variation of Mora's algorithm, which is due to Greuel and Pfister and has been implemented in SINGULAR since 1990 (see [Greuel and Pfister (2007)]).

and, for all $f \in K[x]_>$ *and* $G \in \mathcal{G}$*, we have:*

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

(iii) *There is a* ***standard representation*** *for* f *with respect to* $\mathrm{NF}(- \mid G)$*. That is, if* $G = \{g_1, \dots, g_s\}$*, there exists a unit* $u \in K[x]_>$ *together with an expression of type*

$$uf - \mathrm{NF}(f \mid G) = \sum_{i=1}^{s} a_i g_i, \quad a_i \in K[x]_> \,, \quad s \geq 0 \,,$$

where $\mathrm{LM}(\sum_{i=1}^{s} a_i g_i) \geq \mathrm{LM}(a_j g_j)$ *for all* j *with* $a_j g_j \neq 0$.

If $>$ *is global, and* $u = 1$ *in* (iii)*, then* NF *is called a* ***normal form*** *on* $K[x]$*. A normal form is* ***reduced*** *if no monomial of* $\mathrm{NF}(f \mid G)$ *is divisible by a leading monomial of an element of* G*.*

In (iii) above, if $f \in K[x]$ and $G \subset K[x]$, then $u, a_1, \dots, a_s$ can be chosen to be in $K[x]$ as well.

Proposition 2.26 *Let* $>$ *be a monomial ordering on* $K[x]$*. Then there exists a weak normal form on* $K[x]_>$*. If* $>$ *is global, then there exists a normal form on* $K[x]$*.*

Proof The second statement is clear from Algorithm 1, the first one from Algorithm 3 below. For a proof that Algorithm 3 terminates, see [Greuel and Pfister (2007)] (this is more difficult than showing that Algorithm 1 terminates). □

Algorithm 3 weakNF($f \mid G$)

Input: $>$ a monomial ordering, $f \in K[x]$, G a finite list in $K[x]$
Output: $h \in K[x]$, a weak normal form of f with respect to G

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

Proposition 2.27 *Let $>$ be a monomial ordering on $K[x]$, let $I \subset K[x]_>$ be an ideal, and let* NF *be a weak normal form on $K[x]_>$. Let G be a standard basis of I. Then the following hold:*

(i) *For any $f \in K[x]_>$, we have $f \in I$ iff* $\mathrm{NF}(f \mid G) = 0$.

(ii) *G generates I.*†

(iii) *If $>$ is global, if* NF *is a reduced normal form, and if $f \in K[x]$, then* $\mathrm{NF}(f \mid G)$ *only depends on $>$ and I.*

Proof (i) Assume $f \in K[x]$ and $G = \{g_1, \ldots, g_s\} \subset K[x]$. Let

$$uf = \sum_{i=1}^{s} a_i g_i + \mathrm{NF}(f \mid G) \qquad (2.1)$$

be a standard representation, with $u \in S_>, a_1, \ldots, a_s \in K[x]$. Note that u is a unit in $K[x]_>$. If $\mathrm{NF}(f \mid G) = 0$, then $uf \in I$, hence $f \in I$. If $\mathrm{NF}(f \mid G) \neq 0$, then $\mathrm{LM}(\mathrm{NF}(f \mid G)) \notin \mathrm{L}(G) = \mathrm{L}(I)$, hence $\mathrm{NF}(f \mid G) \notin I$. This implies $f \notin I$.

(ii) follows from (i) and (2.1).

To prove (iii), let $\overline{\mathrm{NF}}$ be another reduced normal form. Given $f \in K[x]$, we have standard representations $f = \sum_{i=1}^{s} a_i g_i + \mathrm{NF}(f \mid G)$ and $f = \sum_{i=1}^{s} \overline{a}_i g_i + \overline{\mathrm{NF}}(f \mid G)$, with $a_i, \overline{a}_i \in K[x]$. This implies that $\mathrm{NF}(f \mid G) - \overline{\mathrm{NF}}(f \mid G) \in I$. Hence, if we would have $\overline{\mathrm{NF}}(f \mid G) \neq \mathrm{NF}(f \mid G)$ for some f, then one of the monomials of $\mathrm{NF}(f \mid G)$ or $\overline{\mathrm{NF}}(f \mid G)$ would be in $\mathrm{L}(I) = \mathrm{L}(G)$, a contradiction to the properties of reduced normal forms. □

We are, now, ready to finish Gordan's proof of Hilbert's basis theorem (see Section 1.1.1). More generally, we show:

Corollary 2.28 *Each ring of type $K[x]_>$ is Noetherian.*

Proof Proposition 2.15 shows that every ideal in $K[x]_>$ has a (finite) standard basis. By part (ii) of Proposition 2.27, this standard basis generates the ideal. □

† If $f_1, \ldots, f_r \in K[x]$ are generators for $I \subset K[x]_>$, and $G \subset K[x]$, then G does not necessarily generate the ideal $\widetilde{I} = \langle f_1, \ldots, f_r \rangle_{K[x]}$. Consider the following example: Let x be a single variable, let $>$ be the unique local ordering on $K[x]$, and let $I \subset K[x]_>$ be the ideal generated by x. Then $x^2 + x = (x+1) \cdot x \in \widetilde{I}$, but $\langle x^2 + x \rangle_{K[x]} \subsetneq \widetilde{I}$ since $x \notin \langle x^2 + x \rangle_{K[x]}$. Nevertheless, $G = \{x + x^2\}$ is a standard basis of I generating I.

The standard basis algorithm requires the choice of a monomial ordering. The performance of the algorithm and the resulting basis depend in a crucial way on this choice.

Singular Example 2.29

```
> ring R1 = 32003, x(1..5), lp;
> int d = 8;
> ideal MId = maxideal(d);
> LIB "random.lib";
> ideal I = randomid(maxideal(d),10,32002);
> int t = timer;          // computing time in seconds
> ideal GI = std(I);
> timer - t;
67
> size(GI);
2243

> ring R2 = 32003, x(1..5), dp;
> ideal I = imap(R1,I);    // maps the ideal I from R1 to R2
> t = timer;
> ideal GI = std(I);
> timer - t;
25
> size(GI);
1351
```

This example is somewhat typical since usually the ordering $>_{\mathrm{dp}}$ performs better than others. Therefore, if no special properties of the resulting Gröbner basis are needed, it is recommended to use $>_{\mathrm{dp}}$. On the other hand, computing the image of a polynomial map requires orderings such as $>_{\mathrm{lp}}$ (see Section 2.2). This can cause problems in that there are examples in which the direct computation of a Gröbner basis with respect to $>_{\mathrm{lp}}$ is not feasible, whereas a Gröbner basis with respect to $>_{\mathrm{dp}}$ can be computed in almost no time.

Singular Example 2.30

```
> ring R1 = 0, (x,y,z), lp;
> ideal I = 3x3y+x3+xy3+y2z2, 2x3z-xy-xz3-y4-z2, 2x2yz-2xy2+xz2-y4;
> ideal GI = std(I);
error: no more memory
```

```
> ring R2 = 0, (x,y,z), dp;
> ideal I = imap(R1,I);
> option(redSB);           // forces computation of reduced GB
> int t = timer;
> ideal GI = std(I);
> timer - t;               // time in seconds
0
```

Gröbner basis conversion algorithms take their cue from what we just observed: In principle, they compute a Gröbner basis with respect to an appropriately chosen fast ordering, and convert the result to a Gröbner basis with respect to the desired slow ordering.

If $I \subset K[x]$ is a zero–dimensional ideal, then $K[x]/I$ is a finite dimensional K–vector space (see Remark 1.86). In this case, the so called *FGLM conversion algorithm* (see [Faugère et al. (1993)]) converts Gröbner bases by means of linear algebra (Gaussian elimination). We reconsider the example above using FGLM:

```
> dim(GI);
0
setring R1;
> t = timer;
> ideal J = fglm(R2,GI);    // GI must be a reduced Groebner basis
> timer - t;
0
```

Here is some numerical information on the computed Gröbner basis:

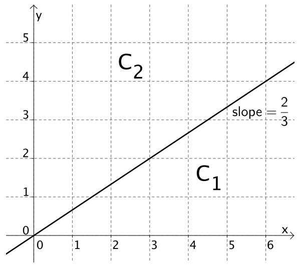
```
> size(J);                  // number of generators
8

> size(string(J))/68;       // number of lines with 68 characters
                            // needed to display J:
631

> deg(J[1..size(J)]);       // degrees of the generators
35 34 34 34 34 34 34 34

> leadmonom(J[1..size(J)]); // generators for L(I) w.r.t. lp
z35 yz6 y2z4 y3z2 y5 xz2 xy x3

> leadcoef(J[8]);           // leading coeff. of 8th generator
64400936316237739859695098418592766025128073489865909063485822
67651806942677443883093109641441627364249598438582596862938314
965556548533870597328962260825040847335705757819599104
```

A conversion algorithm which works even if $K[x]/I$ is not finite dimensional is the Gröbner walk algorithm which approaches the target Gröbner basis for I in several steps, "walking" along a path through the so called *Gröbner fan* of I. In each step, a Gröbner basis with respect to an "intermediate" monomial ordering is computed. There are several strategies to choose the path through the Gröbner fan, leading to different variants of the algorithm. In our example, we use the so called *fractal walk* and get:

```
> LIB "grwalk.lib";
> t = timer;
> ideal JJ = fwalk(I);
> timer - t;
0
```

One can show that each ideal $I \subset K[x]$ has only finitely many distinct leading ideals as we vary over all global monomial orderings on $K[x]$. Equivalently, there are only finitely many distinct reduced Gröbner bases. Roughly speaking, the *Gröbner fan* of I is a fan of polyhedral cones such that the topdimensional cones correspond to the different reduced Gröbner bases. Rather than giving a formal definition, we illustrate the Gröbner fan by examples.

Example 2.31 Let $I = \langle x^2+y^3, y^4\rangle \subset \mathbb{Q}[x,y]$. Then the Gröbner fan of I consists of the following two cones:

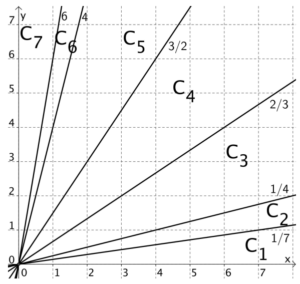


Any point in one of the C_i defines a line through this point and the origin with a certain slope m. Consider the matrix ordering $>_{M_m}$ defined by

$$M_m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}.$$

Then $\{y^3+x^2, x^2y, x^4\}$ is a Gröbner basis of I with respect to $>_{M_m}$ for all points in C_2 (that is, for all $\infty > m > \frac{2}{3}$). Furthermore, $\{x^2+y^3, y^4\}$ is a Gröbner basis with respect to $>_{M_m}$ for all points in C_1 (that is, for all $\frac{2}{3} > m \geq 0$). Note that C_1 contains the point $(1,0)$ for which $>_{M_m}$ is just $>_{\mathrm{lp}}$, and C_2 contains the point $(1,1)$ for which $>_{M_m}$ is what is called the the degree lexicographical ordering, written $>_{\mathrm{Dp}}$.

The Gröbner fan of the ideal $I = \langle x^2 - y^3, x^3 - y^2 + x\rangle \subset \mathbb{Q}[x,y]$ is more complicated:



Note that C_1, again, contains the point $(1,0)$ corresponding to $>_{\mathrm{lp}}$ (as usual, with $x > y$). Here, the Gröbner basis is $\{y^3 - x^2, x^3 - y^2 + x\}$. The cone C_4 contains the point $(1,1)$ corresponding to $>_{\mathrm{Dp}}$. Here, the Gröbner basis is $\{y^3 - x^2, x^3 - y^2 + x\}$. With respect to orderings corresponding to points in C_7, the Gröbner basis is $\{x^8 - 3x^6 + 3x^4 - x^3 - x^2, xy - x^7 + 2x^5 - x^3 + x^2, y^2 - x^3 - x\}$. In particular, this is a Gröbner basis with respect to the lexicographical ordering (now, with $y > x$).

2.2 Applications

Within this section, we explain how to solve a number of computational problems in commutative algebra using standard bases.

2.2.1 Ideal Membership

Problem: Given $f, f_1, \ldots, f_r \in K[x]$ and a monomial ordering $>$ on $K[x]$, let $I = \langle f_1, \ldots, f_r\rangle_{K[x]_>}$. We wish to decide whether $f \in I$, or not.

Solution: Compute a standard basis G of I with respect to $>$ and a (weak) normal form $\mathrm{NF}(f \mid G)$. Then $f \in I$ iff $\mathrm{NF}(f \mid G) = 0$. Correctness follows from Proposition 2.27.

Singular Example 2.32

```
> ring R  = 0, (x,y), dp;
> ideal I = x10+x9y2,y8-x2y7;
> ideal J = std(I);
> poly f  = x2y7+y14;
> reduce(f,J,1);        // 3rd parameter 1 avoids tail reduction
-xy12+x2y7              // f is not in I
> f  = xy13+y12;
> reduce(f,J,1);
0                       // f is in I
```

2.2.2 Elimination

Problem: Given $f_1, \ldots, f_r \in K[x]$, let $I = \langle f_1, \ldots, f_r \rangle_{K[x]}$. We wish to find generators of the kth elimination ideal

$$I_k = I \cap K[x_{k+1}, \ldots, x_n] \,.$$

Elements of the ideal I_k are said to be obtained from $f_1, \ldots, f_r$ *by eliminating* $x_1, \ldots, x_k$.

Definition 2.33 *A monomial ordering $>$ on $K[x_1, \ldots, x_n]$ is called an* ***elimination ordering*** *for $x_1, \ldots, x_k$ if*

$$\mathrm{LM}(f) \in K[x_{k+1}, \ldots, x_n] \implies f \in K[x_{k+1}, \ldots, x_n]$$

for all nonzero $f \in K[x_1, \ldots, x_n]$.

Example 2.34 The lexicographical ordering $>_{\mathrm{lp}}$ is an elimination ordering for *any* initial set of initial variables $x_1, \ldots, x_k$. If k is fixed, $>_1$ is any *global* monomial ordering on $K[x_1, \ldots, x_k]$, and $>_2$ is arbitrary, consider the product ordering $> = (>_1, >_2)$ (which is a mixed ordering if $>_2$ is local). Then

$$K[x_1, \ldots, x_n]_> = K[x_{k+1}, \ldots, x_n]_{>_2}[x_1, \ldots, x_k],$$

and $>$ is an elimination ordering for $x_1, \ldots, x_k$. Note, however, that *no local monomial ordering has this property*: If $1 > x_i$ for some $i \leq k$ and $>$ is local, then $\mathrm{LM}(1+x_i) = 1 \in K[x_{k+1}, \ldots, x_n]$, but $1 + x_i \notin K[x_{k+1}, \ldots, x_n]$.

The following lemma allows us to solve the elimination problem:

Lemma 2.35 *Let $>$ be an elimination ordering for $x_1, \ldots, x_k$ on $\mathrm{Mon}(x_1, \ldots, x_n)$, and let $I \subset K[x_1, \ldots, x_n]_>$ be an ideal. If $G \subset K[x]$ is a standard basis of I, then*

$$G' := \{g \in G \mid \mathrm{LM}(g) \in K[x_{k+1}, \ldots, x_n]\}$$

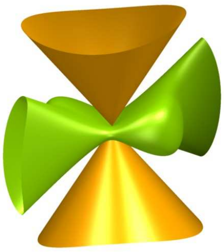
is a standard basis of $I' := I \cap K[x_{k+1}, \ldots, x_n]_{>'}$, where $>'$ on $\mathrm{Mon}(x_{k+1}, \ldots, x_n)$ is induced by $>$. In particular, $I' = \langle G' \rangle$.

Proof Writing $R' = K[x_{k+1}, \ldots, x_n]$, we first have $G' \subset R'$: If $\mathrm{LM}(g) \in R'$, then $g \in R'$ since $>$ is an elimination ordering for $x_1, \ldots, x_k$. Second, if $f \in I \cap R'$, then there is a $g \in G$ such that $\mathrm{LM}(g) | \mathrm{LM}(f)$. This implies that $\mathrm{LM}(g) \in R'$, so that $g \in G'$. □

Singular Example 2.36

```
> ring R1 = 0, (t,x,y,z), dp;
> ideal I = t2+x2+y2+z2,t2+2x2-xy-z2,t+y3-z3;
> ideal J = eliminate(I,t);  // the built-in Singular command
> J;
J[1]=x2-xy-y2-2z2    J[2]=y6-2y3z3+z6+2x2-xy-z2

> ring R2 = 0, (t,x,y,z), (dp(1),dp(3)); // using a product order
> ideal I = imap(R1,I);
> ideal J = std(I);   J;
J[1]=x2-xy-y2-2z2    J[2]=y6-2y3z3+z6+2x2-xy-z2    J[3]=t+y3-z3
```

The hypersurfaces defined by J[1] and J[2] meet in the origin:



2.2.3 Radical Membership

Problem: Let $f_1, \ldots, f_r \in K[x]_>$, let $>$ be a monomial ordering on Mon_n, and let $I = \langle f_1, \ldots, f_r \rangle_{K[x]_>}$. Given an element $f \in K[x]_>$, we want to decide whether $f \in \sqrt{I}$.

As already stated in Corollary 1.31, a solution to this problem is based on the *trick of Rabinowitsch*:†

Lemma 2.37 *Let R be a ring, let $I \subset R$ be an ideal, and let $f \in R$. If t is an extra variable, then*

$$f \in \sqrt{I} \iff 1 \in J := \langle I, 1 - tf \rangle_{R[t]}.$$

Proof If $f \in \sqrt{I}$, then $f^k \in I$ for a suitable k. In particular, $t^k f^k \in J$ and, thus,

$$\begin{aligned} 1 &= t^k f^k + (1 - t^k f^k) \\ &= t^k f^k + (1 - tf)(1 + tf + \ldots + t^{k-1} f^{k-1}) \in J. \end{aligned}$$

The other direction is similar to the corresponding part of the proof of Theorem 1.29. □

Singular Example 2.38

```
> ring R1 = 0, (x,y,z), dp;
> ideal I = x5,xy3,y7,z3+xyz;
> poly f = x+y+z;

> ring R2 = 0, (t,x,y,z), dp; // need t for radical test
> ideal I = imap(R1,I);
> poly f = imap(R1,f);
> ideal J = I,1-t*f;
> std(J);
_[1]=1                // f is in the radical

> LIB "primdec.lib";  // to double check, we compute the radical
> setring R1;
> radical(I);
_[1]=z   _[2]=y     _[3]=x
```

† Note that we can even compute the full radical $\sqrt{I}$, but this is a much harder computation (see Proposition 2.73 and Remark 2.75).

2.2.4 Ideal Intersections

Problem: Given $f_1, \dots, f_r, h_1, \dots, h_s \in K[x]$ and a monomial ordering $>$, let $I_1 = \langle f_1, \dots, f_r \rangle_{K[x]_>}$ and $I_2 = \langle h_1, \dots, h_s \rangle_{K[x]_>}$. We wish to find generators for $I_1 \cap I_2$.

Lemma 2.39 *Consider the ideal*

$$J := \langle tf_1, \dots, tf_r, (1-t)h_1, \dots, (1-t)h_s \rangle_{K[x]_>[t]},$$

where t is an extra variable. Then $I_1 \cap I_2 = J \cap K[x]_>$.

Proof If $f = \sum_{i=1}^r \xi_i f_i = \sum_{j=1}^s \eta_j h_j \in I_1 \cap I_2$, then

$$f = tf + (1-t)f = \sum_{i=1}^r \xi_i t f_i + \sum_{j=1}^s \eta_j (1-t) h_j \in J \cap K[x]_>.$$

If $f = \sum_{i=1}^r \xi_i t f_i + \sum_{j=1}^s \eta_j (1-t) h_j \in J \cap K[x]_>$, then

$$f = \sum_{i=1}^r \xi_i|_{(t=1)} f_i \quad \text{and} \quad f = \sum_{j=1}^s \eta_j|_{(t=0)} h_j.$$

That is, $f \in I_1 \cap I_2$. □

Singular Example 2.40

```
> ring R1 = 0, (x,y,z), dp;
> ideal I1 = x,y;  ideal I2 = y2,z;
> intersect(I1,I2);              // the built-in Singular command
_[1]=y2    _[2]=yz    _[3]=xz

> ring R2 = 0, (t,x,y,z), dp;   // the method described above
> ideal I1 = imap(R1,I1);  ideal I2 = imap(R1,I2);
> ideal J = t*I1+(1-t)*I2;
> eliminate(J,t);
_[1]=yz  _[2]=xz   _[3]=y2
```

2.2.5 Ideal Quotients

Problem: Given $f_1, \dots, f_r, h_1, \dots, h_s \in K[x]$ and a monomial ordering $>$, let $I_1 = \langle f_1, \dots, f_r \rangle_{K[x]_>}$ and $I_2 = \langle h_1, \dots, h_s \rangle_{K[x]_>}$. We want to compute

$$I_1 : I_2 = \{ g \in K[x]_> \mid gI_2 \subset I_1 \}.$$

Since, obviously, $I_1 : \langle h_1, \ldots, h_s\rangle_{K[x]_>} = \bigcap_{i=1}^s (I_1 : \langle h_i\rangle_{K[x]_>})$, we are reduced to computing $I_1 : \langle h_i\rangle_{K[x]_>}$ for each i.

Lemma 2.41 *If $I \subset K[x]_>$ is an ideal and $0 \neq h \in K[x]_>$, we may write $I \cap \langle h\rangle_{K[x]_>} = \langle g_1 \cdot h, \ldots, g_t \cdot h\rangle_{K[x]_>}$ with convenient $g_i \in K[x]$. Then $I : \langle h\rangle_{K[x]_>} = \langle g_1, \ldots, g_t\rangle_{K[x]_>}$.*

Singular Example 2.42

```
> ring R = 0, (x,y,z), dp;
> ideal I1 = x,y;
> ideal I2 = y2,z;
> quotient(I1,I2);        // the built-in Singular command
_[1]=y    _[2]=x
```

2.2.6 Kernel of a Ring Map

Let $>_1$ on $K[y] = K[y_1, \ldots, y_m]$ and $>_2$ on $K[x]$ be monomial orderings. Let $J \subset K[y]_{>_1}$ and $I \subset K[x]_{>_2}$ be ideals, and let $\overline{f}_1 = f_1 + I, \ldots, \overline{f}_m = f_m + I \in K[x]/I$. Consider the ring homomorphism

$$\phi : R_1 := (K[y]_{>_1})/J \longrightarrow (K[x]_{>_2})/I =: R_2,\ y_i \mapsto \overline{f}_i.$$

Set $J_0 := J \cap K[y]$, $I_0 := I \cap K[x]$. Then ϕ is induced by the map

$$\widetilde{\phi} : K[y]/J_0 \longrightarrow K[x]/I_0\,,\ y_i \mapsto \overline{f}_i\,,$$

and we have a commutative diagram

$$\begin{tikzcd}
K[y]/J_0 \arrow[r, "\widetilde{\phi}"] \arrow[d, hook] & K[x]/I_0 \arrow[d, hook] \\
R_1 \arrow[r, "\phi"] & R_2\,.
\end{tikzcd}$$

Problem: Given I, J, and ϕ as above, find generators for $\ker(\phi)$.

Solution: If $I_0 = \langle g_1, \ldots, g_s\rangle_{K[x]}$ and $J_0 = \langle h_1, \ldots, h_t\rangle_{K[y]}$, set

$$H := \langle h_1, \ldots, h_t, g_1, \ldots, g_s, y_1 - f_1, \ldots, y_m - f_m\rangle \subset K[x, y],$$

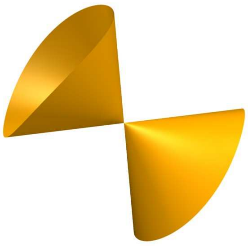
and compute $H' := H \cap K[y]$ by eliminating $x_1, \ldots, x_n$ from H. Then, by the following lemma, H' generates $\ker(\phi)$.

Lemma 2.43 *With notation as above,* $\ker(\phi) = \ker(\widetilde{\phi})R_1$ *and* $\ker(\widetilde{\phi}) = \big(H \cap K[y]\big) \bmod J_0$. *In particular, if* $>_1$ *is global, then* $\ker(\phi) = \ker(\widetilde{\phi})$.

Proof We treat the case where $>_1$ is global (for the general case, see [Greuel and Pfister (2007)]). If $h \in K[y]$, we have $h \bmod J \in \ker(\phi)$ iff $h(f_1, \dots, f_m) \in I$. Applying Taylor's formula, $h = h(f_1, \dots, f_m) + \sum_{i=1}^{m} \xi_i(y_i - f_i)$ for suitable $\xi_i \in K[x, y]$. □

Singular Example 2.44

```
> ring R1 = 0, (x,y,z), dp;
> ring R2 = 0, (a,b), dp;
> map phi = R1,a2,ab,b2;
> ideal I0;                    // the zero ideal
> setring R1;
> preimage(R2,phi,I0);         // the built-in Singular command
_[1]=y2-xz
```



```
> ring R3 = 0, (x,y,z,a,b), dp;   // the method described above
> ideal H = x-a2, y-ab, z-b2;
> eliminate(H,ab);
_[1]=y2-xz
```

2.2.7 Integrality Criterion

Let $I = \langle g_1, \dots, g_s \rangle \subset K[x]$ be an ideal, and let $\overline{f}_1 = f_1 + I, \dots, \overline{f}_m = f_m + I \in K[x]/I$. Consider the polynomial ring $K[y] = K[y_1, \dots, y_m]$ together with the ring homomorphism

$$\phi : K[y] \to S = K[x]/I, \; y_i \mapsto \overline{f}_i,$$

and let H be the ideal

$$H := \langle g_1, \ldots, g_s, y_1 - f_1, \ldots, y_m - f_m \rangle \subset K[x, y].$$

Let $>_{\mathrm{lp}}$ be the lexicographical ordering on $K[x, y]$, with $x_1 > \cdots > x_n$ and $x_i > y_j$ for all i, j, and let G be a Gröbner basis of H with respect to $>_{\mathrm{lp}}$. Then, by Sections 2.2.7 and 2.2.2, the elements of $G \cap K[y]$ generate $\ker \phi$. View $R := K[y]/\ker \phi$ as a subring of S by means of ϕ.

Problem: Given $R \subset S$ as above, decide whether $R \subset S$ is integral.

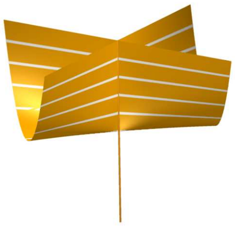
Lemma 2.45 *With notation as above, $R \subset S$ is integral iff for each i, $1 \leq i \leq n$, there is an element of G whose leading monomial is of type $x_i^{\alpha_i}$, for some $\alpha_i \geq 1$.*

Proof Inductively, starting with $i = n$, an element of G with leading monomial $x_i^{\alpha_i}$ defines an integral equation for $\overline{x}_i$ over $R[\overline{x}_{i+1}, \ldots, \overline{x}_n]$. Hence, the result follows from Remark 1.75. See [Greuel and Pfister (2007)] for details. □

Singular Example 2.46 Consider the parametrization

$$\varphi : \mathbb{A}^2(\mathbb{R}) \to \mathbb{A}^3(\mathbb{R}),\ (s, t) \mapsto (st, t, s^2),$$

of the Whitney umbrella $\mathrm{V}(x^2 - y^2 z)$ as in Example 1.63.



On the algebraic side, we get the ring monomorphism

$$\begin{aligned} \varphi^* : R = \mathbb{R}[x, y, z]/\langle x^2 - y^2 z \rangle &\longrightarrow S = \mathbb{R}[s, t], \\ \overline{x} \mapsto st,\ \ \overline{y} \mapsto t,\ \ &\overline{z} \mapsto s^2. \end{aligned}$$

Considering $R \subset S$ as a ring extension by means of φ^*, we see that it is integral since we have the integral equations $t - \overline{y} = 0$ and $s^2 - \overline{z} = 0$. Let us check this with Singular:

Singular Example 2.47

```
> ring R = 0, (s,t,x,y,z), lp;   // the method described above
> ideal H = x-st, y-t, z-s2;
> ideal GH = std(H);  GH;
GH[1]=x2-y2z
GH[2]=t-y
GH[3]=sy-x
GH[4]=sx-yz
GH[5]=s2-z

> ring R = 0, (s,t,x,y,z), dp;
> ideal H = x-st, y-t, z-s2;
> LIB "algebra.lib";
> finitenessTest(std(H),1..2);   // the built-in Singular command
[1]:
   1
[2]:
   _[1]=s
   _[2]=t
[3]:
   _[1]=x
   _[2]=y
   _[3]=z
[4]:
   _[1]=t-y
   _[2]=s2-z
```

The first entry `1` in the list indicates that the ring extension is integral. The second entry gives the variables whose powers occur as a leading monomial of one of the Gröbner basis elements. The third entry contains the variables which do not have this property. The last entry contains the integral relations.

2.2.8 Noether Normalization

Problem: Given an ideal $I \subsetneq K[x]$, find $y_1, \ldots, y_d \in K[x]/I$ such that:

(i) $y_1, \ldots, y_d$ are algebraically independent over K.
(ii) $K[y_1, \ldots, y_d] \subset K[x]/I$ is an integral ring extension.

Solution (see Remarks 1.71, 1.72): Assume that K is infinite. Let

$$\phi : \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ * & & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

be a random lower triangular linear coordinate change, and let $G = \{f_1, \dots, f_r\}$ be the reduced Gröbner basis of $\phi(I)$ with respect to the lexicographical ordering, with $x_1 > \cdots > x_n$. Suppose that G is sorted such that $\mathrm{LM}(f_r) > \cdots > \mathrm{LM}(f_1)$. Let c be minimal with $G \cap K[x_{c+1}, \dots, x_n] = \emptyset$. Then the residue classes $\overline{x}_{c+1}, \dots, \overline{x}_n \in K[x]/\phi(I)$ are algebraically independent over K.

For $i = 1, \dots, c$, test whether G contains a polynomial with leading monomial $x_i^{\alpha_i}$ for some $\alpha_i \geq 1$. If the test returns true for all i, then $K[x_{c+1}, \dots, x_n] \subset K[x]/\phi(I)$ is a Noether normalization. This implies that $K[\phi^{-1}(x_{c+1}), \dots, \phi^{-1}(x_n)] \subset K[x]/I$ is a Noether normalization. If the test returns false for some i, then try again with a new choice of ϕ.

Singular Example 2.48

```
> ring R = 0, (x,y,z), lp;
> ideal I = x2+y2+z2,x3+y3+z3;
> map phi = R,x,x+y,2x+3y+z;
> ideal J = phi(I);
> J = std(J);  J;
J[1]=1156y6+2448y5z+2292y4z2+1224y3z3+393y2z4+72yz5+6z6
J[2]=68xz4-5780y5-5882y4z-2042y3z2-59y2z3+230yz4+50z5
J[3]=40xyz2+44xz3+1734y4+2244y3z+1253y2z2+390yz3+50z4
J[4]=68xy2+56xyz+14xz2+34y3+44y2z+19yz2+2z3
J[5]=6x2+14xy+4xz+10y2+6yz+z2

//    k=2
//    Q[z] ---> Q[x,y,z]/phi(I)  is finite
//    Q[x-3y+z] ---> Q[x,y,z]/I  is finite
```

2.2.9 Subalgebra Membership

Problem: If $f, f_1, \dots, f_r \in K[x]$, test whether $f \in K[f_1, \dots, f_r]$.

Solution: Define $\phi : K[y_0, \dots, y_r] \longrightarrow K[x]$, $y_0 \longmapsto f$, $y_i \longmapsto f_i$, and compute $\ker(\phi)$. If $\ker(\phi)$ contains an element of the form $y_0 - g(y_1, \dots, y_r)$, then $f \in K[f_1, \dots, f_r]$.

Singular Example 2.49

```
> ring R1 = 0, (x,y), dp;
> poly f,f1,f2 = x4-y4,x2+y2,x2-y2;
> ring R2 = 0, (x,y,u,v,w), (dp(2),dp(1),dp(2));
> ideal H = u-imap(R1,f), v-imap(R1,f1), w-imap(R1,f2);
> std(H);
_[1]=u-vw _[2]=2y2-v+w _[3]=x2-y2-w
```

Since u is one of the leading monomials, we get $f \in K[f_1, f_2]$.

2.2.10 Homogenization

Problem: Given an ideal $I \subset K[x_1, \ldots, x_n]$, compute the homogenization $I^h = \langle f^h \mid f \in I \rangle \subset K[x_0, \ldots, x_n]$ (see Definition 1.100).

Solution: If $G = \{g_1, \ldots, g_s\}$ is a Gröbner basis of I with respect to some global degree ordering† $>$, then $I^h = \langle g_1^h, \ldots, g_s^h \rangle$:

Lemma 2.50 *With notation as above,* $I^h = \langle g_1^h, \ldots, g_s^h \rangle$.

Proof Let $f \in I$. Then, since G is a Gröbner basis, f has a standard representation of type $f = \sum\limits_{i=1}^{s} h_i g_i$ (see Definition 2.25 and Proposition 2.27). That is, $\mathrm{LM}(f) \geq \mathrm{LM}(h_i g_i)$ for all i with $h_i g_i \neq 0$. Since $>$ is a degree ordering, we get $d := \deg(f) \geq \deg(h_i g_i)$ for any such i. Then $x_0^d f = \sum\limits_{i=1}^{s} x_0^{d-\deg(h_i)-\deg(g_i)} x_0^{\deg(h_i)} h_i x_0^{\deg(g_i)} g_i$ implies that $f^h = \sum\limits_{i=1}^{s} x_0^{d-\deg(h_i)-\deg(g_i)} h_i^h g_i^h \in \langle g_1^h, \ldots, g_s^h \rangle$. □

Our next example shows that it is not enough to homogenize an arbitrary set of generators of an ideal to find its homogenization.

Singular Example 2.51

```
> ring R = 0, (x,y,z,w), dp;
> ideal I = y-x2, xy-z;          // the ideal of the twisted cubic
> ideal J = homog(I,w);          // only generators are homogenized
> ideal HI = homog(std(I),w);    // the projective twisted cubic
> HI;
```

† A monomial ordering $>$ is called a **degree ordering** if $x^\alpha > x^\beta$ implies $\deg(x^\alpha) \geq \deg(x^\beta)$. Note that $>_{\mathrm{dp}}$ is a degree ordering.

```
HI[1]=y2-xz
HI[2]=xy-zw
HI[3]=x2-yw
> reduce(HI,std(J));
_[1]=y2-xz
_[2]=0
_[3]=0
> reduce(J,std(HI));
_[1]=0
_[2]=0
```

2.3 Dimension and the Hilbert Function

The computation of dimension, of the Hilbert function, and of the Hilbert polynomial will be discussed and explained.

Problem: Let $I \subsetneq K[x]$ be an ideal. Compute the Krull dimension $\dim(K[x]/I) = \dim(I)$ and the K–vector space dimension $\dim_K(K[x]/I)$.

Proposition 2.52 *Let $I \subsetneq K[x]$ be an ideal. Then*

$$\dim(I) = d,$$

where d is the maximal cardinality of a subset of variables $u \subset \{x_1, \dots, x_n\}$ with

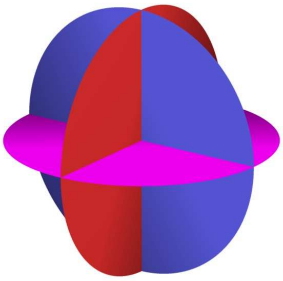
$$I \cap K[u] = \langle 0 \rangle.$$

Proof For a proof, see [Decker and Schreyer (2013)]. □

Note that this includes the case $d = 0$ in which $I \cap K[x_i] \supsetneq \langle 0 \rangle$ for all i (see Remark 1.86 and Proposition 1.32).

Definition 2.53 *A* ***maximal independent set*** *of variables for I is a subset u of variables of maximal cardinality as above.*

Example 2.54 If $I = \langle xy, xz \rangle \subset K[x, y, z]$, then $I \cap K[y, z] = \langle 0 \rangle$ and $I \cap K[x] = \langle 0 \rangle$. The sets $\{y, z\}$ and $\{x\}$ are maximal in the sense that they cannot be extended. But only $u = \{y, z\}$ is a maximal independent set for I.



Proposition 2.52 does not give a practical method for finding the Krull dimension since it requires the computation of quite a number of different elimination ideals. On the other hand, by Lemma 2.57 below, the case of a monomial ideal can be handled in a purely combinatorial way. Hence, the following result is the key to computing dimension in general:

Proposition 2.55 *Let $>$ be any monomial ordering on $K[x]$, and let $I \subset K[x]$ be an ideal. Then*

$$\dim(K[x]_>/IK[x]_>) = \dim(K[x]/\mathrm{L}(I))$$

and

$$\dim_K(K[x]_>/IK[x]_>) = \dim_K(K[x]/\mathrm{L}(I)).$$

Moreover, if $\dim_K(K[x]_>/IK[x]_>) < \infty$ or $>$ is a global ordering, then the monomials in $K[x] \smallsetminus \mathrm{L}(I)$ represent a basis of the K–vector space $K[x]_>/IK[x]_>$.

Proof For a proof, see [Greuel and Pfister (2007)]. □

Singular Example 2.56 With respect to $>_{\mathrm{dp}}$, considering the reduced Gröbner basis

$$f_1 = x^2 - y, \quad f_2 = xy - z, \quad f_3 = y^2 - xz$$

of the ideal of the twisted cubic curve C (see Example 2.51), we see that $\mathrm{L}(I) = \langle x^2, xy, y^2\rangle$. Since $u = \{z\}$ is a set of variables of maximal cardinality with

$$\langle x^2, xy, y^2\rangle \cap K[u] = \langle 0\rangle,$$

this shows once more that the dimension of C is 1 (see Example 1.83). In SINGULAR, this can be checked using the `dim` command:

```
> ring R = 0, (x,y,z), dp;
> ideal I = y-x2, z-x3;
> dim(std(I));
1
```

The `dim` command is based on Proposition 2.55 and the purely combinatorial lemma below:

Lemma 2.57 *Let $I = \langle m_1, \dots, m_k\rangle \subset K[x]$ be an ideal with monomial generators m_i. Define $d(I, K[x])$ recursively by*

- $d(0, K[x]) = n$,
- $d(I, K[x]) = \max\left\{d(I|_{(x_i=0)}, K[x \smallsetminus x_i]) \mid x_i|m_1\right\}$.

Then $d(I, K[x]) = \dim(K[x]/I)$.

Proof Let $u \subset x$ be a maximal independent set for I. Then $\#u = \dim(K[x]/I)$. If x_i is a variable such that $x_i|m_1$ and $x_i \notin u$, then u is a maximal independent set for $I|_{(x_i=0)} \subset K[x \smallsetminus x_i]$. □

For the vector space dimension $\dim_K(K[x]/I)$, Proposition 2.55 tells us to count the monomials not contained in $\mathrm{L}(I)$, provided this number is finite. Note, however, that it takes some effort to make this combinatorial approach an efficient one.

Singular Example 2.58 *(Intersection Multiplicities)* Reconsidering Example 1.90 from Chapter 1, we show how to compute the intersection multiplicities of the curves $C = \mathrm{V}(f)$ and $D = \mathrm{V}(g)$, where $f = y^2 - x^2(x+1)$ and $g = y^2 + x^3$. The curves intersect in the points $(0,0), (-\frac{1}{2}, \frac{1}{4}\sqrt{2}), (-\frac{1}{2}, -\frac{1}{4}\sqrt{2})$. First, we compute the intersection multiplicity at $o = (0,0)$, that is,

$$i_o(C, D) = \dim_{\mathbb{Q}}\left(\mathbb{Q}[x,y]_{\langle x,y\rangle}/\langle f, g\rangle\right).$$

```
> ring R1 = 0, (x,y), ds;
> ideal I = y2-x3-x2,y2+x3;
> vdim(std(I));  // the vector space dimension of R1/I
4
```

Now we compute the sum of the intersection multiplicities in the three intersection points of the curves, that is, $\dim_{\mathbb{Q}}(\mathbb{Q}[x,y]/\langle f,g\rangle)$ (see Proposition 1.88).

```
> ring R2 = 0, (x,y), dp;
> ideal I = imap(R1,I);
> vdim(std(I));
6
```

This suggests that the intersection multiplicity at $(-\frac{1}{2},\pm\frac{1}{4}\sqrt{2})$ is 1. To test this, we consider the ring $\mathbb{Q}(\sqrt{a})[x,y]$, where $a = \sqrt{1/8}$. We create a map $\phi : \mathbb{Q}(\sqrt{a})[x,y] \to \mathbb{Q}(\sqrt{a})[x,y]$ corresponding to the morphism $\mathbb{A}^2(\mathbb{Q}(\sqrt{a})) \to \mathbb{A}^2(\mathbb{Q}(\sqrt{a}))$ which translates $(-\frac{1}{2},\frac{1}{4}\sqrt{2})$ to $o = (0,0)$. The intersection multiplicity at $(-\frac{1}{2},\frac{1}{4}\sqrt{2})$ is, then:

$$\begin{aligned}&\dim_{\mathbb{Q}(\sqrt{a})}\Big(\big(\mathbb{Q}(\sqrt{a})[x,y]\big)_{\langle x,y\rangle}\Big/\langle\phi(f),\phi(g)\rangle\Big)\\ &\quad = \dim_{\mathbb{Q}(\sqrt{a})}\Big(\big(\mathbb{Q}(\sqrt{a})[x,y]\big)_{\langle x+\frac{1}{2},y-\frac{1}{4}\sqrt{2}\rangle}\Big/\langle f,g\rangle\Big).\end{aligned}$$

```
> ring R3 = (0,a), (x,y), ds;
> minpoly = a2-1/8;
> ideal I = imap(R1,I);
> map phi = R3,x-1/2,y+a;
> I = phi(I);  I;
I[1]=1/4*x+(2a)*y+1/2*x2+y2-x3
I[2]=3/4*x+(2a)*y-3/2*x2+y2+x3
> vdim(std(I));
1
```

Singular Example 2.59 *(Multiplicity of Zeros)* Consider the ideal $I = \langle x+y+z-1, x^2+y^2+z^2-1, x^3+y^3+z^3-1\rangle$ from Examples 0.7, 1.55, and 1.89, and its vanishing locus $\mathrm{V}(I) = \{(1,0,0),(0,1,0),(0,0,1)\}$. We compute the multiplicity of I at $(1,0,0)$, that is,

$$\mathrm{mult}\,((1,0,0)\mid I) = \dim_{\mathbb{Q}}\big(\mathbb{Q}[x,y,z]_{\langle x-1,y,z\rangle}/I\big).$$

Consider the map $\phi : \mathbb{Q}[x,y,z] \to \mathbb{Q}[x,y,z]$ defined by $\phi(x) = x+1, \phi(y) = y, \phi(z) = z$. This corresponds to the morphism $\mathbb{A}^3(\mathbb{Q}) \to \mathbb{A}^3(\mathbb{Q})$ translating $(1,0,0)$ to $o = (0,0,0)$. We compute

$$\mathrm{mult}\,(o\mid\phi(I)) = \dim_{\mathbb{Q}}\big(\mathbb{Q}[x,y,z]_{\langle x,y,z\rangle}/\phi(I)\big):$$

```
> ring R = 0, (x,y,z), ds;
> ideal I = x+y+z-1,x2+y2+z2-1,x3+y3+z3-1;
> map phi = R,x+1,y,z;
> I = phi(I);  I;
I[1]=x+y+z
I[2]=2x+x2+y2+z2
I[3]=3x+3x2+x3+y3+z3
> vdim(std(I));
2
```

Now, we turn to the Hilbert function and the Hilbert polynomial.

Problem: If $I \subset K[x]$ is a homogeneous ideal, compute $Q(t) \in \mathbb{Z}[t]$ such that $\mathrm{HP}_{K[x]/I}(t) = \frac{Q(t)}{(1-t)^n}$, where $\mathrm{HP}_{K[x]/I}$ is the Hilbert–Poincaré series of $K[x]/I$ (see Theorem 1.108 in Section 1.2.4) and n is the number of variables in $K[x]$.

Theorem 2.60 *Let $>$ be any monomial ordering on $K[x]$, and let $I \subset K[x]$ be a homogeneous ideal. Then*

$$\mathrm{HP}_{K[x]/I}(t) = \mathrm{HP}_{K[x]/\mathrm{L}(I)}(t).$$

Proof Let $K[x]_d$ be the K–vector space generated by all monomials of degree d, and let $I_d = I \cap K[x]_d, \mathrm{L}(I)_d = \mathrm{L}(I) \cap K[x]_d$. We have to prove that

$$\dim_K \left(K[x]_d/I_d\right) = \dim_K \left(K[x]_d/\mathrm{L}(I)_d\right)$$

for all d. Let $B := \{m \mid m \text{ monomial}, m \notin \mathrm{L}(I), \deg(m) = d\}$. We show that B represents a basis of both $K[x]_d/I_d$ and $K[x]_d/\mathrm{L}(I)_d$. Let G be a standard basis of I, and let $h \in K[x]_d$. Then weakNF$(h \mid G)$ and weakNF$(h \mid \mathrm{L}(G))$ are elements of $K[x]_d$ since weakNF preserves homogeneity. Iterating this process by computing the weakNF of the tail of weakNF$(h \mid G)$ respectively weakNF$(h \mid \mathrm{L}(G))$, we may assume weakNF$(h \mid G) \in \sum_{m\in B} K\cdot m$ and weakNF$(h \mid \mathrm{L}(G)) \in \sum_{m\in B} K \cdot m$. But weakNF$(h \mid G) = 0$ (respectively weakNF$(h \mid \mathrm{L}(G)) = 0$) iff $h \in I$ (respectively $h \in \mathrm{L}(I)$). Hence, B represents a K–basis of both $K[x]_d/I_d$ and $K[x]_d/\mathrm{L}(I)_d$. □

Singular Example 2.61

```
> ring R = 0, (t,x,y,z), dp;
> ideal I = x5y2,x3,y3,xy4,xy7;
> intvec v = hilb(std(I),1);
> v;
1,0,0,-2,0,0,1,0
```

We obtain $Q(t) = t^6 - 2t^3 + 1$ since the output has to be interpreted as follows: If `v` $= (v_0, \ldots, v_d, 0)$, then $Q(t) = \sum_{i=0}^{d} v_i t^i$. This implies that the Hilbert–Poincaré series of $K[t,x,y,z]/I$ is $\mathrm{HP}_{K[t,x,y,z]/I}(t) = \frac{Q(t)}{(1-t)^4}$.

Next, we write a procedure to compute the nominator $Q(t)$ of the Hilbert–Poincaré series for *monomial* ideals using the following property: If $I \subset K[x]$ is a homogeneous ideal and $f \in K[x]$ is homogeneous of degree d, then

$$\mathrm{HP}_{K[x]/I}(t) = \mathrm{HP}_{K[x]/\langle I,f\rangle}(t) + t^d \mathrm{HP}_{K[x]/\langle I:f\rangle}(t).$$

Singular Example 2.62

```
proc MonomialHilbertPoincare(ideal I)
{
   I=interred(I);          // computes a minimal set of generators
   int s=size(I);          // of the monomial ideal I
   if(I[1]==0){return(1);} // I = <0>
   if(I[1]==1){return(0);} // I = <1>
   if(deg(I[s])==1){return((1-var(1))^s);}  // I is generated by
                                            // s of the {var(j)}
   int j=1;
   while(leadexp(I[s])[j]==0){j++;}         // I[s]=var(j)*m
   return(MonomialHilbertPoincare(I+var(j))
         +var(1)*MonomialHilbertPoincare(quotient(I,var(j))));
}

> ring R = 0, (t,x,y,z), dp;
> ideal I = x5y2,x3,y3,xy4,xy7;
> MonomialHilbertPoincare(I);
t6-2t3+1
```

For the Hilbert polynomial, see Remark 1.111.

Singular Example 2.63 We compute the Hilbert polynomial of the projective twisted cubic curve C (see Example 2.51). This will be of type $\mathrm{P}_C = dt - p_a + 1 = 3t + 1$. Hence, the degree $d = \deg(C) = 3$ (this explains the name cubic curve) and the arithmetic genus $p_a(C) = 0$ (see Remark 1.107).

```
> LIB "poly.lib";
> ring R = 0, (x,y,z,w), dp;
> ideal I = y2-xz, xy-zw, x2-yw;
> hilbPoly(I);   // the built-in command
1,3
```

2.4 Primary Decomposition and Radicals

In this section, we address the geometric problem of finding the irreducible components of an algebraic set by treating the more general algebraic concept of primary decomposition.

Definition 2.64 *An ideal $Q \subsetneq R$ of a ring R is a* ***primary ideal*** *if, for any $a, b \in R$, $ab \in Q$ and $a \notin Q$ imply $b \in \sqrt{Q}$.*

It follows easily from the definition that the radical $P = \sqrt{Q}$ of a primary ideal Q is a prime ideal. We also say that Q is ***P*–primary**.

Definition 2.65 *Let $I \subsetneq R$ be an ideal of a ring R. A* ***primary decomposition*** *of I is a decomposition $I = Q_1 \cap \cdots \cap Q_s$ into primary ideals Q_i. A primary decomposition is called* ***irredundant*** *if $P_i = \sqrt{Q_i} \neq P_j = \sqrt{Q_j}$ for all $i \neq j$ and no Q_i can be omitted.*

Using the ascending chain condition, one can show that that every proper ideal I of a Noetherian ring has an irredundant primary decomposition $I = Q_1 \cap \ldots \cap Q_s$. Moreover, the prime ideals $P_i = \sqrt{Q}_i$ are uniquely determined by I. They are called the **associated primes** of I. We say that P_i is a **minimal associated prime** of I if $P_i \not\supset P_j$ for all $j \neq i$. If A is an algebraic set with vanishing ideal $\mathrm{I}(A)$, then the minimal associated primes of $\mathrm{I}(A)$ define precisely the irreducible components of A.

Problem: If $I \subsetneq K[x]$ is a proper ideal, find an irredundant primary decomposition $I = Q_1 \cap \cdots \cap Q_s$.

Solution: There are several algorithms to solve this problem (see [Decker et al. (1998)]). Here we will explain the algorithm of Gianni, Trager, and Zacharias. This algorithm may require general coordinate changes which are guaranteed to exist in characteristic zero (see Proposition 2.68 below). The basic idea of the algorithm is to reduce the general case to the zero–dimensional case, and the zero–dimensional case to polynomial factorization. Note that if I is a zero–dimensional ideal, then the associated primes of I are maximal ideals.

Definition 2.66

(i) *A maximal ideal $M \subset K[x_1, \dots, x_n]$ is called in **general position** with respect to the lexicographical ordering $>_{\mathrm{lp}}$ with $x_1 > \cdots > x_n$ if there exist $g_1, \dots, g_n \in K[x_n]$ with $M = \langle x_1 + g_1(x_n), \dots, x_{n-1} + g_{n-1}(x_n),\ g_n(x_n)\rangle$.*

(ii) *A zero–dimensional ideal $I \subset K[x_1, \dots, x_n]$ is called in **general position** with respect to $>_{\mathrm{lp}}$ with $x_1 > \cdots > x_n$ if all its associated primes $P_1, \dots, P_s$ are in general position and $P_i \cap K[x_n] \neq P_j \cap K[x_n]$ for $i \neq j$.*

Example 2.67

(i) $M = \langle x_1 + x_2^2, x_2^3 + 2\rangle \subset \mathbb{Q}[x_1, x_2]$ is a maximal ideal in general position with respect to $>_{\mathrm{lp}}$ with $x_1 > x_2$.

(ii) $M = \langle x_1^2 + 2, x_2^2 + 7\rangle \subset \mathbb{Q}[x_1, x_2]$ is a maximal ideal that is not in general position.

Proposition 2.68 *Let K be a field of characteristic zero, and let $I \subset K[x]$ be a zero–dimensional ideal. Then there is a nonempty Zariski open subset $U \subset K^{n-1}$ such that for all $\underline{a} = (a_1, \dots, a_{n-1}) \in U$, the coordinate change $\phi_{\underline{a}} : K[x] \to K[x]$ defined by $\phi_{\underline{a}}(x_i) = x_i$ if $i < n$ and*

$$\phi_{\underline{a}}(x_n) = x_n + \sum_{i=1}^{n-1} a_i x_i$$

has the property that $\phi_{\underline{a}}(I)$ is in general position with respect to $>_{\mathrm{lp}}$ with $x_1 > \cdots > x_n$.

For a proof, see [Greuel and Pfister (2007)]. The idea is the following: If $M \subset K[x]$ is a maximal ideal, then $K[x]/M$ is a finite field extension of K generated by $\overline{x}_1 = x_1 + M, \dots, \overline{x}_n = x_n + M$. Using the theorem of the primitive element, it follows that almost all linear combinations of $\overline{x}_1, \dots, \overline{x}_n$ lead to a primitive element of the field extension. The corresponding coordinate change yields the required shape of M.

Proposition 2.69 *Let $I \subset K[x_1, \dots, x_n]$ be a zero–dimensional ideal. Let $\langle g \rangle = I \cap K[x_n]$, $g = g_1^{\nu_1} \dots g_s^{\nu_s}$, g_i monic and prime with $g_i \neq g_j$ for $i \neq j$. Then*

(i) $I = \bigcap_{i=1}^{s} \langle I, g_i^{\nu_i} \rangle$.

If I is in general position with respect to $>_{\mathrm{lp}}$, $x_1 > \dots > x_n$, then

(ii) *$\langle I, g_i^{\nu_i} \rangle$ is a primary ideal for each i.*

Proof The univariate polynomials

$$g^{(i)} := \frac{g}{g_i^{\nu_i}}, \quad i = 1, \dots, s,$$

have greatest common divisor 1, so that $\sum_{i=1}^{s} a_i g^{(i)} = 1$ for suitable $a_i \in K[x_n]$. Let $f \in \bigcap_{i=1}^{s} \langle I, g_i^{\nu_i} \rangle$. Choose $f_i \in I$, $b_i \in K[x]$ such that $f = f_i + b_i g_i^{\nu_i}$ for all i. Then $f = \sum_{i=1}^{s} a_i g^{(i)} \cdot f = \sum_{i=1}^{s} a_i g^{(i)} (f_i + b_i g_i^{\nu_i}) \in I$. This proves (i).

To prove (ii), fix i. First note that $\langle I, g_i^{\nu_i} \rangle \neq K[x]$. Indeed, otherwise, $f + c \cdot g_i^{\nu_i} = 1$ for some $f \in I$, $c \in K[x]$, so $f \cdot g^{(i)} + c \cdot g = g^{(i)} \in I$, impossible. Thus, each $\langle I, g_i^{\nu_i} \rangle$ is a proper zero–dimensional ideal. Let $P \supset \langle I, g_i^{\nu_i} \rangle$ be a maximal ideal. Then P is an associated prime of I containing the irreducible polynomial g_i. Since I is in general position with respect to $>_{\mathrm{lp}}$, P is the only associated prime of I containing $\langle I, g_i^{\nu_i} \rangle$. Hence, $P = \sqrt{\langle I, g_i^{\nu_i} \rangle}$, and $\langle I, g_i^{\nu_i} \rangle$ is primary since it is zero–dimensional. □

Singular Example 2.70 *(Zero–dimensional Decomposition)*

```
> option(redSB);
> ring R = 0, (x,y), lp;
> ideal I = (y2-1)^2,x2-(y+1)^3;
```

The ideal I is not in general position with respect to $>_{\mathrm{lp}}$ since the minimal associated prime $\langle x^2 - 8, y - 1 \rangle$ is not.

```
> map phi = R,x,x+y;     // we choose a generic coordinate change
> map psi = R,x,-x+y;    // and the inverse map
> I = std(phi(I));
> I;
I[1]=y7-y6-19y5-13y4+99y3+221y2+175y+49
I[2]=112xy+112x-27y6+64y5+431y4-264y3-2277y2-2520y-847
I[3]=56x2+65y6-159y5-1014y4+662y3+5505y2+6153y+2100
>factorize(I[1]);
[1]:
   _[1]=1
   _[2]=y2-2y-7
   _[3]=y+1
[2]:
   1,2,3

> ideal Q1 = std(I,(y2-2y-7)^2);  // the candidates for the
                                  // primary ideals
> ideal Q2 = std(I,(y+1)^3);      // in general position
> Q1; Q2;
Q1[1]=y4-4y3-10y2+28y+49   Q2[1]=y3+3y2+3y+1
Q1[2]=56x+y3-9y2+63y-7     Q2[2]=2xy+2x+y2+2y+1
                           Q2[3]=x2

> factorize(Q1[1]);   // primary and general position test
                      // for Q1
[1]:
   _[1]=1
   _[2]=y2-2y-7
[2]:
   1,2

> factorize(Q2[1]);   // primary and general position test
                      // for Q2
[1]:
   _[1]=1
   _[2]=y+1
[2]:
   1,3
```

Hence, both ideals are primary and in general position.

```
> Q1 = std(psi(Q1));       // the inverse coordinate change
> Q2 = std(psi(Q2));       // the result
> Q1; Q2;
Q1[1]=y2-2y+1    Q2[1]=y2+2y+1
Q1[2]=x2-12y+4   Q2[2]=x2
```

We obtain that I is the intersection of the primary ideals Q_1 and Q_2, with associated prime ideals $\langle y-1, x^2-8\rangle$ and $\langle y+1, x\rangle$.

Now, we reduce the general case to the zero–dimensional case:

Proposition 2.71 *Let $I \subsetneq K[x]$ be an ideal, and let $u \subset x$ be a maximal independent set of variables for I. Then:*

(i) *The ideal $IK(u)[x \smallsetminus u]$ generated by I in $K(u)[x \smallsetminus u]$ is zero–dimensional.*

(ii) *If $\{g_1, \ldots, g_s\} \subset I \subset K[x]$ is a Gröbner basis of $IK(u)[x \smallsetminus u]$, and $h := \mathrm{lcm}\big(\mathrm{LC}(g_1), \ldots, \mathrm{LC}(g_s)\big) \in K[u]$, then*

$$IK(u)[x \smallsetminus u] \cap K[x] = I : \langle h^\infty \rangle,$$

and this ideal is equidimensional† *of dimension* $\dim(I)$*.*

(iii) *If $I : h^d = I : h^{d+1}$, then $I = (I : h^d) \cap \langle I, h^d \rangle$.*

(iv) *If $IK(u)[x \smallsetminus u] = Q_1 \cap \cdots \cap Q_s$ is an irredundant primary decomposition, then also*

$$IK(u)[x \smallsetminus u] \cap K[x] = (Q_1 \cap K[x]) \cap \cdots \cap (Q_s \cap K[x])$$

is an irredundant primary decomposition.

Proof For a proof, see [Greuel and Pfister (2007)]. □

Example 2.72 Let $I = \langle xy, xz \rangle \subset \mathbb{Q}[x, y, z]$. Then:

- $u = \{y, z\}$ is a maximal independent set and $I\mathbb{Q}(y, z)[x] = \langle x \rangle_{\mathbb{Q}(y,z)[x]}$.
- $\{xy\} \subset I$ is a Gröbner basis of $I\mathbb{Q}(y, z)[x]$ and $h = y$.
- $I : h = I : h^2 = \langle x \rangle_{\mathbb{Q}[x,y,z]}$ and $I = (I : h) \cap \langle I, h \rangle = \langle x \rangle \cap \langle xz, y \rangle$.
- We have to continue with $\langle xz, y \rangle =: J$.
- $u = \{x\}$ is a maximal independent set and $J\mathbb{Q}(x)[y, z] = \langle y, z \rangle_{\mathbb{Q}(x)[y,z]}$.
- $\{xz, y\} \subset J$ is a Gröbner basis of $J\mathbb{Q}(x)[y, z]$ and $h = x$.
- $J : h = J : h^2 = \langle y, z \rangle_{\mathbb{Q}[x,y,z]}$ and $J = (J : h) \cap \langle J, h \rangle = \langle y, z \rangle \cap \langle x, y \rangle$.
- This implies $I = \langle x \rangle \cap \langle y, z \rangle \cap \langle x, y \rangle$. Since $\langle x \rangle \subset \langle x, y \rangle$, we obtain $I = \langle x \rangle \cap \langle y, z \rangle$.

Finally, we briefly address the computation of the radical.

† That is, all associated primes of I have the same dimension $\dim(I)$.

Proposition 2.73 *Let $I \subset K[x_1, \ldots, x_n]$ be a zero–dimensional ideal. For $i = 1, \ldots, n$, let $I \cap K[x_i] = \langle f_i \rangle$, and let g_i be the square–free part of f_i. Then $\sqrt{I} = I + \langle g_1, \ldots, g_n \rangle$.*

Proof For a proof, see [Greuel and Pfister (2007)]. □

Singular Example 2.74

```
> ring R = 0, (x,y), dp;
> ideal I = xy4-2xy2+x,x2-x,y4-2y2+1;
> I = std(I);  I;
I[1]=x2-x
I[2]=y4-2y2+1
> dim(I);                       // the dimension is zero
0
> ideal u = finduni(I);         // finds univariate polynomials
                                // in each variable in I
> u;
u[1]=x2-x
u[2]=y4-2y2+1
> ideal radI = I,x2-1,y2-1;     // the squarefree parts of
                                // u[1],u[2] are added to I
> std(radI);                    // the radical
_[1]=x-1
_[2]=y2-1
```

Remark 2.75 As for primary decomposition, computing radicals in general can be reduced to the zero–dimensional case.

2.5 Buchberger's Algorithm and Field Extensions

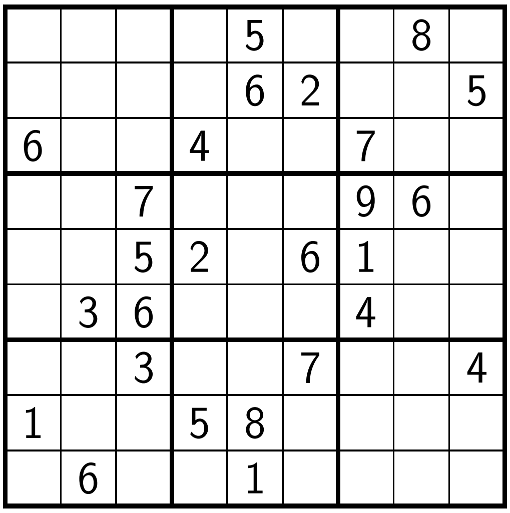
Let $L \supset K$ be a field extension such as $\overline{K} \supset K$. If I is an ideal of $K[x_1, \ldots, x_n]$, then any Gröbner basis for I is also a Gröbner basis for the ideal generated by I in $L[x_1, \ldots, x_n]$ since all computations in Buchberger's algorithm are carried through over K.

This shows, in particular, that if a property of ideals can be checked using Gröbner bases, then I has this property iff the ideal generated by I in $L[x_1, \ldots, x_n]$ has this property. To give an example, we know that elimination ideals can be computed using Gröbner bases. It follows that if I_k is the kth elimination ideal of I, then the ideal generated by I_k in $L[x_{k+1}, \ldots, , x_n]$ is the kth elimination ideal of the ideal generated by I in $L[x_1, \ldots, x_n]$.

See [Decker and Schreyer (2013)] for more on this.

3
Sudoku

In this chapter, we will explain how to solve a Sudoku using ideas from algebraic geometry and computer algebra. In fact, we will represent the solutions of a Sudoku as the points in the vanishing locus of a polynomial ideal I in 81 variables, and we will show that the unique solution of a well–posed Sudoku can be read off from the reduced Gröbner basis of I. We should point out, however, that attacking a Sudoku can be regarded as a graph colouring



				5			8	
				6	2			5
6			4			7		
		7				9	6	
		5	2		6	1		
	3	6				4		
		3			7			4
1			5	8				
	6			1				

Fig. 3.1. Sudoku

problem†, with one colour for each of the numbers $1, \ldots, 9$, and that graph theoretical methods for solving the Suduko are much more efficient than Gröbner basis methods.

A completed Sudoku is a particular example of what is called a Latin square. A *Latin square* of order n is an $n \times n$ square grid whose entries are taken from a set of n different symbols, with each symbol appearing exactly once in each row and each column. For a Sudoku, usually $n = 9$, and the symbols are the numbers from 1 to 9. In addition to being a Latin square, a completed Sudoku is subject to the condition that each number from 1 to 9 appears exactly once in each of the nine distinguished 3×3 blocks.

Latin squares can be at least traced back to the medieval islamic world. They appear in the work of Leonhard Euler who created examples using Latin characters. The invention of the modern Sudoku is credited to the US-American architect Howard Garns. Examples where first published by Dell Magazines in 1979 under the name *Number Place*. The name *Sudoku* was coined in Japan where the puzzles became popular in the mid 1980s.

To model a Sudoku by polynomial equations, we represent its 81 cells by 81 variables, say $x_1, \ldots, x_{81}$. Then the entry a_i in the ith cell of a completed Sudoku satisfies $a_i \in \{1, \ldots, 9\}$ iff a_i is a root of the univariate polynomial $F_i \in \mathbb{Q}[x_i]$ defined by $F_i(x_i) = \prod_{k=1}^{9}(x_i - k)$. The polynomial $F_i(x_i) - F_j(x_j)$ vanishes on $\mathrm{V}(x_i - x_j)$, so that $x_i - x_j$ is a factor of $F_i(x_i) - F_j(x_j)$, for $i \neq j$. In other words, we have well–defined polynomials

$$G_{ij}(x_i, x_j) = \frac{F_i - F_j}{x_i - x_j} \in \mathbb{Q}[x_i, x_j],\ i \neq j.$$

The condition that neither a row, nor a column, nor a distinguished 3×3 block in a completed Sudoku has repeated entries is modelled as follows. Set

$$E = \{(i,j) \mid 1 \leq i < j \leq 81, \text{ and the } i\text{th and } j\text{th cell are in the} \\ \text{same row, column, or distinguished } 3 \times 3 - \text{block}\}.$$

Let $I \subset \mathbb{Q}[x_1, \ldots, x_{81}]$ be the ideal which is generated by the 891 polynomials F_i, $i = 1, \ldots, 81$, and G_{ij}, $(i,j) \in E$.

† A famous example of a graph colouring problem is the four–colour problem which was solved by Appel and Hagen in 1976 with a computer–assisted proof. See [Appel and Haken (1977)].

Proposition 3.1 *With notation as above, let* $\mathrm{V}(I)$ *be the vanishing locus of* I *in* $\mathbb{A}^{81}(\overline{\mathbb{Q}})$*, and let* $a = (a_1, \ldots, a_{81}) \in \mathbb{A}^{81}(\overline{\mathbb{Q}})$ *be a point. Then* $a \in \mathrm{V}(I)$ *iff* $a_i \in \{1, \ldots, 9\}$*, for* $i = 1, \ldots, 81$*, and* $a_i \neq a_j$*, for* $(i, j) \in E$*.*

Proof If the conditions on the right hand side are fulfilled, then the F_i and G_{ij} vanish at a, so that $a \in \mathrm{V}(I)$. Conversely, let $a \in \mathrm{V}(I)$. Then $F_i(a) = 0$ and, thus, $a_i \in \{1, \ldots, 9\}$ for all i. To show that $a_i \neq a_j$ for $(i, j) \in E$, suppose to the contrary that $a_i = a_j =: b$ for some (i, j). Since substituting b for x_j in $F_i(x_i) = (x_i - x_j)G_{ij}(x_i, x_j) + F_j(x_j)$ gives $F_i(x_i) = (x_i - b)G_{ij}(x_i, b)$, and since $G_{ij}(b, b) = 0$ by assumption, this would imply that b is a zero of F_i of order at least two, which is impossible. □

We say that a Sudoku is **well–posed** if it has a unique solution.

Proposition 3.2 *Let* S *be an explicitly given, well–posed Sudoku with preassigned numbers* $\{a_i\}_{i \in L}$*, for some subset* $L \subset \{1, \ldots, 81\}$*. We associate to* S *the ideal* $I_S = I + \langle \{x_i - a_i\}_{i \in L} \rangle$*. Then, with respect to any global monomial ordering, the reduced Gröbner basis of* I_S *has the shape* $x_1 - a_1, \ldots, x_{81} - a_{81}$*, and* $(a_1, \ldots, a_{81})$ *is the solution of the Sudoku.*

Proof Taking Proposition 3.1 and the Nullstellensatz into account, the assumption that S has a unique solution $(a_1, \ldots, a_{81})$ implies that $\sqrt{I_S}$ is the maximal ideal $\langle x_1 - a_1, \ldots, x_{81} - a_{81} \rangle$. In particular, I_S contains a suitable power of $x_i - a_i$, for each i. Since I_S also contains the square–free polynomials $F_i(x_i) = \prod_{k=1}^{9}(x_i - k)$, we conclude that the elimination ideals $I_S \cap K[x_i]$ are generated by the $x_i - a_i$. Thus, $I_S = \langle x_1 - a_1, \ldots, x_{81} - a_{81} \rangle$, and the shape of the reduced Gröbner basis is as claimed. □

Based on the discussion above, we present Singular procedures to solve a Sudoku. The first step is to create the set E, the polynomials F_i, and the ideal generated by the polynomials F_i and G_{ij}, respectively. This is done by the following three procedures:

```
proc createE()
{
   int i,j,k,l,a,b;
   list E;
   for(j = 1; j <= 9; j++)
   {
      for(k = 1; k <= 9; k++)
      {
         i = (j-1)*9+k;
         a = j mod 3; if(a == 0) { a = 3; }
         b = k mod 3; if(b == 0) { b = 3; }
         for(l = k+1; l <= 9; l++)
         {
             E[size(E)+1] = list(i,i+l-k);
         }
         for(l = j+4-a; l <= 9; l++)
         {
             E[size(E)+1] = list(i,(l-1)*9+k);
         }
         if(a != 3)
         {
             E[size(E)+1] = list(i,j*9+k-b+1);
             E[size(E)+1] = list(i,j*9+k-b+2);
             E[size(E)+1] = list(i,j*9+k-b+3);
         }
         if(a == 1)
         {
             E[size(E)+1] = list(i,(j+1)*9+k-b+1);
             E[size(E)+1] = list(i,(j+1)*9+k-b+2);
             E[size(E)+1] = list(i,(j+1)*9+k-b+3);
         }
      }
   }
   return(E);
}


proc createF()
{
   int i;
   ideal F;
   poly p = (var(1)-1);
   for(i = 2; i <= 9; i++)
   {
      p = p*(var(1)-i);
   }
   F[1] = p;
   for(i = 2; i <= nvars(basering); i++)
   {
      F[i] = subst(p,var(1),var(i));
   }
   return(F);
}

proc createG(ideal F, list E)
{
   int i;
   ideal G = F;
   for(i = 1; i <= size(E); i++)
   {
      G[size(G)+1] = (F[E[i][1]] - F[E[i][2]])/
                     (var(E[i][1]) - var(E[i][2]));
   }
   return(G);
}
```

Starting from the ideal created so far, the next step is to implement the ideal I_S from Proposition 3.2. That is, we have to include the polynomials which encode the preassigned values of the Sudoku. We suppose that these values are given in form of a 9×9 integer matrix, where cells with no preassigned value are represented by a zero.

```
proc addPreass(ideal G, intmat M)
{
   int i,j,k;
   for(i = 1; i <= 9; i++)
   {
      for(j = 1; j <= 9; j++)
      {
         if(M[i,j] != 0)
         {
            k = (i-1)*9+j;
            G[size(G)+1] = var(k)-M[i,j];
         }
      }
   }
   return(G);
}
```

The procedure below reads the solution of the Sudoku from the reduced Gröbner basis for the ideal I_S, which is required as input:

```
proc prepareRes(ideal G)    // G a Groebner basis
{
   intmat M[9][9];
   int i,j,k;
   for(i = 1; i <= size(G); i++)
   {
      j = ((i-1) div 9) +1;
      k = i mod 9;
      if(k == 0) { k = 9; }
      M[j,k] = int(leadcoef(-G[size(G)-i+1][2]));
   }
   return(M);
}
```

Finally, we present the main procedure which calls all procedures defined above:

```
proc Sudoku(intmat M)
{
   list E = createE();
   ring R = 32003, x(1..81), dp;
   ideal F = createF();
   ideal G = createG(F,E);
   G = addPreass(G,M);
   option(redSB);
   G = std(G);
   intmat N = prepareRes(G);
   return(N);
}
```

Singular Example 3.3 Having entered our procedures in a Singular session, the Sudoku in Figure 3.1 is solved as follows:

```
> intmat M1[9][9] =  0,0,0,0,5,0,0,8,0,
.                    0,0,0,0,6,2,0,0,5,
.                    6,0,0,4,0,0,7,0,0,
.                    0,0,7,0,0,0,9,6,0,
.                    0,0,5,2,0,6,1,0,0,
.                    0,3,6,0,0,0,4,0,0,
.                    0,0,3,0,0,7,0,0,4,
.                    1,0,0,5,8,0,0,0,0,
.                    0,6,0,0,1,0,0,0,0;
> print(Sudoku(M1));
```

The completed Sudoku is:

```
3  4  1  7  5  9  2  8  6
8  7  9  1  6  2  3  4  5
6  5  2  4  3  8  7  9  1
2  1  7  3  4  5  9  6  8
4  8  5  2  9  6  1  3  7
9  3  6  8  7  1  4  5  2
5  9  3  6  2  7  8  1  4
1  2  4  5  8  3  6  7  9
7  6  8  9  1  4  5  2  3
```

Solving this Sudoku is not so easy – on an iMac with a 2,8 GHz processor, about 5 hours of computing time are needed. The following Sudoku is much easier and solved in about a second:

```
> intmat M2[9][9] =  0,6,0,1,0,4,0,5,0,
.                    0,0,8,3,0,5,6,0,0,
.                    2,0,0,0,0,0,0,0,1,
.                    8,0,0,4,0,7,0,0,6,
.                    0,0,6,0,0,0,3,0,0,
.                    7,0,0,9,0,1,0,0,4,
.                    5,0,0,0,0,0,0,0,2,
.                    0,0,7,2,0,6,9,0,0,
.                    0,4,0,5,0,8,0,7,0;
print(Sudoku(M2));
```

The solution is:

```
9  6  3  1  7  4  2  5  8
1  7  8  3  2  5  6  4  9
2  5  4  6  8  9  7  3  1
8  2  1  4  3  7  5  9  6
4  9  6  8  5  2  3  1  7
7  3  5  9  6  1  8  2  4
5  8  9  7  1  3  4  6  2
3  1  7  2  4  6  9  8  5
6  4  2  5  9  8  1  7  3
```

4

A Problem in Group Theory Solved by Computer Algebra

We shall briefly report on the paper [Bandman et al. (2006)] in which a problem in finite group theory could be translated to algebraic geometry and solved using computer algebra. We begin by collecting some facts about nilpotent and solvable groups.

4.1 Finite Groups and Thompson's Theorem

As usual, if G is any group (in multiplicative notation, with identity element 1), we write $[x, y] = xyx^{-1}y^{-1}$ for the **commutator** of two elements $x, y \in G$, and

$$[G, G] = \langle [x, y] \mid x, y \in G \rangle$$

for the **commutator subgroup** of G.

Definition 4.1 *Let G be a group. Inductively, define subgroups of G by $G^1 := [G, G]$ and $G^{i+1} := [G^i, G]$. Then G is called **nilpotent** if $G^m = \{1\}$ for some natural number $m \geq 1$.*

Example 4.2

(i) Abelian groups are nilpotent.

(ii) A finite group G is nilpotent iff it is the direct product of its Sylow subgroups. A proof of this theorem can be found, for instance, in [Doerk and Hawkes (1992)].

(iii) The symmetric group S_3 is not nilpotent since $[S_3, S_3]$ is the alternating group A_3, and $[A_3, S_3] = A_3$.

Let us illustrate (iii) and (ii) with a SAGE session:

```
sage: G = SymmetricGroup(3)
sage: G
Symmetric group of order 3! as a permutation group
sage: H = G.commutator(G)
sage: H
Permutation Group with generators [(1,2,3)]
sage: H == AlternatingGroup(3)
True
sage: L=H.commutator(G)
Permutation Group with generators [(1,2,3)]
```

Thus, $[S_3, S_3] = A_3$ and $[A_3, S_3] = A_3$ as claimed in (iii). To give an example for (ii), consider the dihedral Group D_4:

```
sage: D4 = DihedralGroup(4)
sage: D4.cardinality()
8
sage: G = D4.commutator(D4)
sage: G
Permutation Group with generators [(1,3)(2,4)]
sage: G.commutator(D4)
Permutation Group with generators [()]
```

This shows that $[[D_4, D_4], D_4] = \{1\}$, so that D_4 is nilpotent. Since D_4 has order 8, it is itself a 2–Sylow group.

Definition 4.3 *Let G be a group. Inductively, define subgroups of G by $G^{(1)} := [G, G]$ and $G^{(i+1)} := [G^{(i)}, G^{(i)}]$. Then G is called* ***solvable*** *if $G^{(m)} = \{1\}$ for some natural number $m \geq 1$.*

Example 4.4

(i) Any nilpotent group G is solvable since $G^{(i)} \subset G^i$ for all i.
(ii) S_3, S_4 are solvable since $[S_3, S_3] = A_3$, $[S_4, S_4] = A_4$.
(iii) Groups of odd order are solvable.†
(iv) S_5, A_5 are not solvable since $[A_5, A_5] = A_5$, $[S_5, S_5] = A_5$.

We show how to check (iv) and (ii) using Sage:

```
sage: S5 = SymmetricGroup(5)
sage: S5.commutator(S5)
```

† This is the theorem of Feit and Thompson which is a very important result for the classification of finite groups. The proof has more than 300 pages. See [Feit and Thompson (1963)].

```
Permutation Group with generators [(1,2,3), (1,3,4), (1,5,4)]
sage: S5.commutator(S5) == AlternatingGroup(5)
True
sage: A5 = AlternatingGroup(5)
sage: A5.commutator(A5)
Permutation Group with generators [(1,3,4), (2,4,5)]
sage: A5.commutator(A5).order()
60
```

This shows that $[S_5, S_5] = A_5$ and $[A_5, A_5] = A_5$.

```
sage: S4 = SymmetricGroup(4)
sage: G = S4.commutator(S4)
sage: G
Permutation Group with generators [(1,2,3), (1,3,4)]
sage: H = G.commutator(G)
sage: H
Permutation Group with generators [(1,2)(3,4), (1,4)(2,3)]
sage: H.commutator(H)
Permutation Group with generators [()]
```

This shows that S_4 is solvable.

Definition 4.5 *Let K be a field. We write*

$$\mathrm{SL}(n,K) := \{M \in \mathrm{GL}(n,K) \mid \det(M) = 1\}$$

*for the **special linear group** and*

$$\mathrm{PSL}(n,K) := \mathrm{SL}(n,K) \big/ \{a \cdot E_n \mid a^n = 1\}$$

*for the **projective special linear group**. If $K = \mathbb{F}_q$, we also write* $\mathrm{PSL}(n,q) = \mathrm{PSL}(n,\mathbb{F}_q)$.

Example 4.6 We use Sage to check that

$$\mathrm{PSL}(2,5) \cong \mathrm{PSL}(2,4) \cong A_5 :$$

```
sage: G = PSL(2,5)
sage: G
Permutation Group with generators [(3,5)(4,6), (1,2,5)(3,4,6)]
sage: H = PSL(2,4)
sage: H
Permutation Group with generators [(3,4,5), (1,2,3)]
sage: G.is_isomorphic(H)
True
sage: G.is_isomorphic(A5)
```

```
True
```

We need a classification result proved in [Thompson (1968)]:

Theorem 4.7 *The finite nonsolvable simple groups all whose proper subgroups are solvable are contained*† *in the following list:*

(i) $\mathrm{PSL}(2, q)$*,* $q = p^n \geq 4$*,* p *a prime.*
(ii) $\mathrm{PSL}(3, 3)$.
(iii) $\mathrm{Sz}(2^n)$*,* $n \geq 3$ *and odd, the* Suzuki groups.

Remark 4.8 The Suzuki groups can be represented as follows. Let $n = 2m + 1$, and let $q = 2^n$. Consider the automorphism $\theta : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, $\theta(a) = a^{2^{m+1}}$. We have $\theta^2(a) = a^2$, that is, π is the square root of the Frobenius map. Let

$$U(a,b) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ a\theta(a)+b & \theta(a) & 1 & 0 \\ a^2\theta(a)+ab+\theta(b) & b & a & 1 \end{pmatrix},$$

$$M(c) = \begin{pmatrix} c^{1+2^m} & 0 & 0 & 0 \\ 0 & c^{2^m} & 0 & 0 \\ 0 & 0 & c^{-2^m} & 0 \\ 0 & 0 & 0 & c^{-1-2^m} \end{pmatrix}, \qquad T = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Then $\mathrm{Sz}(q) = \langle U(a,b), M(c), T \mid a, b, c \in \mathbb{F}_q,\ c \neq 0 \rangle \subset \mathrm{SL}(4, \mathbb{F}_q)$.

4.2 Characterization of Finite Solvable Groups

Now, we consider the following problem: Use 2–variable identities to characterize the finite groups that are solvable. As a motivation, we recall other characterizations by 2–variable identities:

Example 4.9

(i) A group G is *abelian* iff $xy = yx$ for all $x, y \in G$.
(ii) If G is a group and $x, y \in G$, inductively set $v_1(x, y) := [x, y]$ and $v_{n+1}(x, y) := [v_n, y]$. Then a finite group G is *nilpotent* iff there is an integer $n \geq 1$ such that $v_n(x, y) = 1$ for all $x, y \in G$ (*Engel Identities*). See [Zorn (1936)].

† The list contains more groups than Thompson's list, but is easier to describe.

To characterize finite solvable groups, we introduce Engel–like identities which, as shown by Theorem 4.12 below, are just right:

Notation 4.10 *If G is a group and $x, y \in G$, inductively define*

$$\begin{aligned} e_1(x,y) &:= x^{-2} \cdot y^{-1} \cdot x \quad \textit{and} \\ e_{n+1}(x,y) &:= [x \cdot e_n(x,y) \cdot x^{-1}, y \cdot e_n(x,y) \cdot y^{-1}]. \end{aligned}$$

Remark 4.11 We may think of e_1 as a word in x, x^{-1}, y, and y^{-1}. Given any such word w, set $e_1^w(x,y) := w$ and inductively $e_{n+1}^w(x,y) := [x \cdot e_n^w(x,y) \cdot x^{-1}, y \cdot e_n^w(x,y) \cdot y^{-1}]$. The choice of $w = x^{-2}y^{-1}x$ was motivated by a computer search among the 10000 shortest words w, asking whether the condition from Proposition 4.13 below holds for all $q < 1000$, with $e_n^w(x,y)$ in place of $e_n(x,y)$. The words found were $x^{-2}y^{-1}x$, $x^{-1}yxy^{-1}x$, $y^{-2}x^{-1}$, and $xy^{-2}x^{-1}yx^{-1}$.

Theorem 4.12 *A finite group G is solvable iff there is an integer $n \geq 1$ such that $e_n(x,y) = 1$ for all x, $y \in G$.*

Referring to [Bandman et al. (2006)] for the complete proof, we illustrate the main idea here. First, if G is solvable, then the identities $e_n(x,y) = 1$ are satisfied from a certain n onward.

Second, assume that the converse implication of the theorem is not true, and let G be a counterexample of minimal order. That is, G is a finite nonsolvable group of the smallest order such that $e_n(x,y) = 1$ for some n and all $x, y \in G$. Then G must be simple. Indeed, otherwise, there is a nontrivial proper normal subgroup H of G, and both H and G/H would be solvable (because the identity $e_n = 1$ remains true in the subgroups and the quotients). This would imply that G is solvable.

The idea now is to show that for each group G in Thompson's list, there are $x, y \in G$ with $e_1(x,y) = e_2(x,y)$ and $y \neq x^{-1}$. This implies $1 \neq e_1(x,y) = e_n(x,y)$ for all n.

For PSL$(3,3)$, it turned out that there are 44928 suitable pairs in x, y having this property. One of them is

$$x = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad y = \begin{pmatrix} 2 & 0 & 2 \\ 0 & 1 & 1 \\ 2 & 1 & 1 \end{pmatrix}.$$

In what follows, we shall give an idea on how to deal with the groups $\mathrm{PSL}(2,q)$ (the case of the Suzuki groups is much more difficult and can therefore not be treated here).

Here is what we wish to show:

Proposition 4.13 *If $q = p^n$ for a prime p and $q \neq 2,3$, then there are x, y in $\mathrm{PSL}(2,q)$ with $y \neq x^{-1}$ and $e_1(x,y) = e_2(x,y)$.*

The proof of the proposition is based on explicit computations with the following matrices: If R is any ring, and if $t, b, c \in R$, set

$$x(t) := \begin{pmatrix} t & -1 \\ 1 & 0 \end{pmatrix}, \quad y(b,c) := \begin{pmatrix} 1 & b \\ c & 1+bc \end{pmatrix} \in \mathrm{SL}(2,R).$$

We study the case $R = \mathbb{Z}$ for simultaneous verification in the cases $R = \mathbb{F}_p$, for all primes p. This is even sufficient for the cases $q = p^n$ since the ideals introduced below are defined over $\mathbb{F}_p \subseteq \mathbb{F}_q \subseteq \overline{\mathbb{F}}_q = \overline{\mathbb{F}}_p$.

Let $I \subset \mathbb{Z}[b,c,t]$ be the ideal generated by the four entries of the matrix $e_1(x(t), y(b,c)) - e_2(x(t), y(b,c)) \in \mathrm{SL}(2,\mathbb{Z})$. We use Singular to obtain generators for I:

```
> LIB "linalg.lib";
> ring R = 0, (b,c,t), dp;
> matrix X[2][2] = t, -1,
.                  1,  0;
> matrix Y[2][2] = 1, b,
.                 c, 1+bc;
> matrix iX = inverse(X);   matrix iY = inverse(Y);
> matrix M = iX*Y*iX*iY*X*X-Y*iX*iX*iY*X*iY;
> ideal I = flatten(M); I;
I[1]=b3c2t2+b2c2t3-b2c2t2-bc2t3-b3ct+b2c2t+b2ct2+2bc2t2+bct3
     +b2c2+b2ct+bc2t-bct2-c2t2-ct3-b2t+bct+c2t+ct2+2bc+c2+bt
     +2ct+c+1
I[2]=-b3ct2-b2ct3+b2c2t+bc2t2+b3t-b2ct-2bct2-b2c+bct+c2t+ct2
     -bt-ct-b-c-1
I[3]=b3c3t2+b2c3t3-b2c2t3-bc2t4-b3c2t+b2c3t+2b2c2t2+2bc3t2
     +2bc2t3+b2c2t+2b2ct2+bc2t2-c2t3-ct4-2b2ct+bc2t+c3t+bct2
     +2c2t2+ct3-b2c-b2t+bct+c2t +bt2+3ct2+bc-bt-b-c+1;
I[4]=-b3c2t2-b2c2t3+b2c2t2+bc2t3+b3ct-b2c2t-b2ct2-2bc2t2-bct3
     -2b2ct+c2t2+ct3+b2t-bct-c2t-ct2+b2-bt-2ct-b-t+1
```

Having, in fact, implemented an ideal in $\mathbb{Q}[x,y,z]$, we compute a Gröbner basis of this ideal using `option(contentSB)`:

```
> option(contentSB);       // see the explanation below
> ideal J = std(I); J;
J[1]=bct-t2+2t+1
J[2]=bt3-ct3+t4-b2t+bct-c2t-2bt2+2ct2-3t3+bc+t2+t+1
J[3]=b2c2-b2ct+bc2t-bct2+b2+2bc+c2-b+c-t+2
J[4]=c2t3-ct4+c3t-2c2t2+3ct3-t4-bc2+bt2-2ct2+4t3-2bt+ct-3t2-b-2t
> dim(J);
1
```

Note that `option(contentSB)` forces SINGULAR to perform the usual Buchberger algorithm over $\mathbb{Q}$ without any division. Technically, this amounts to replacing $\mathrm{spoly}(f,g)$ by $\mathrm{LC}(g)\cdot\mathrm{spoly}(f,g)$ (see Definition 2.19). Starting from generators defined over $\mathbb{Z}$, the reductions of the resulting Gröbner basis elements modulo p form a Gröbner basis over $\mathbb{F}_p$, for all primes p not dividing any of the leading coefficients. In our case, where all leading coefficients are 1, we get a Gröbner basis for the ideal $I\,\mathbb{F}_q[b,c,t]$, for all $q=p^n$ (here, $I\,\mathbb{F}_q[b,c,t]$ is the ideal induced by I in $\mathbb{F}_q[b,c,t]$ via reducing the generators modulo p and extending from $\mathbb{F}_p$ to $\mathbb{F}_q$). In particular, the dimension is 1 in all cases, so that $I\,\mathbb{F}_q[b,c,t]$ defines a curve $C^{(q)}$ in $\mathbb{A}^3(\overline{\mathbb{F}_q})$, for all q. We are interested in the $\mathbb{F}_q$–**rational points** of $C^{(q)}$, that is, in the points with coordinates in $\mathbb{F}_q$. In fact, to show Proposition 4.13, it is sufficient to prove:

Proposition 4.14 *With notation as above, let q be as in Proposition 4.13. Then $C^{(q)}$ contains at least one $\mathbb{F}_q$–rational point.*

To establish this result, we apply the *Hasse–Weil theorem* as generalized in [Aubry and Perret (1996)] to possibly singular curves:

Theorem 4.15 *Let $C\subset\mathbb{A}^n(\overline{\mathbb{F}_q})$ be an irreducible affine curve defined by polynomial equations with coefficients in $\mathbb{F}_q$, and let $\overline{C}\subset\mathbb{P}^n(\overline{\mathbb{F}_q})$ be its projective closure. Then the number of $\mathbb{F}_q$–rational points of C is at least $q+1-2p_a\sqrt{q}-d$, where d and p_a are the degree and the arithmetic genus of $\overline{C}$, respectively.*

Remark 4.16

(i) By their very definition, d and p_a can be read off from the Hilbert polynomial $\mathrm{P}_{\overline{C}}(t)=dt-p_a+1$ of $\overline{C}$. Hence, these numbers can be computed directly from the vanishing ideal of $\overline{C}$ – no information on the singularities of $\overline{C}$ is needed. See Remark 1.107 and Section 2.3.

(ii) Theorem 4.15 is an affine version of the Hasse–Weil theorem which can be derived from the projective version stated in [Aubry and Perret (1996)] by taking into account that the number of points of $\overline{C}$ contained in a hyperplane is at most d. See again Remark 1.107.

(iii) The fact that C is irreducible in the affine space over the algebraic closure of its field of definition is sometimes emphasized by saying that C is **absolutely irreducible**.

The next result will allow us to apply Theorem 4.15 in our situation. To state the result, we fix a prime power $q = p^n$ as in Proposition 4.13, and denote by L the algebraic closure $L = \overline{\mathbb{F}_q}$.

Proposition 4.17 *With notation as above, $IL[b, c, t]$ is a prime ideal. Geometrically, the curve $\overline{C^{(q)}}$ is absolutely irreducible.*

To prove this result, we first verify:

Lemma 4.18 *We have $IL(t)[b, c] = \langle f_1, f_2\rangle$, with*

$$\begin{aligned}
f_1 = {} & t^2b^4 - t^3(t-2)b^3 + (-t^5 + 3t^4 - 2t^3 + 2t + 1)b^2 \\
& + t^2(t^2 - 2t - 1)(t-2)b + (t^2 - 2t - 1)^2, \\
f_2 = {} & t(t^2 - 2t - 1)c + t^2b^3 + (-t^4 + 2t^3)b^2 \\
& + (-t^5 + 3t^4 - 2t^3 + 2t + 1)b + (t^5 - 4t^4 + 3t^3 + 2t^2).
\end{aligned}$$

Moreover, $IL[b, c, t] = \langle f_1, f_2\rangle : h^2$, with $h = t(t^2 - 2t - 1)$.

Proof We continue our Singular session to check this:

```
> ring S = (0,t), (c,b), lp;
> ideal I = imap(R,I);   I = std(I);   I;
I[1]=(t7+t6-t5-2t4-t3)*b4+ ...
I[2]=(t8-2t7-4t6+6t5+7t4-6t3-8t2-2t)*c+(t6+t5-t4-2t3-t2)*b4+ ...
```

Since we did not allow any division during the Gröbner basis computation, we now simplify the Gröbner basis "by hand":

```
> I[1]=I[1]/(t5+t4-t3-2t2-t);   I[2]=I[2]-(t4+t3-t2-2t-1)*I[1];
> I[2]=I[2]/(t5-3t3+4t+2);   I;
```

```
I[1]=(t2)*b4+(-t4+2t3)*b3+(-t5+3t4-2t3+2t+1)*b2
      +(t5-4t4+3t3+2t2)*b+(t4-4t3+2t2+4t+1)
I[2]=(t3-2t2-t)*c+(t2)*b3+(-t4+2t3)*b2+(-t5+3t4-2t3+2t+1)*b
      +(t5-4t4+3t3+2t2)
> setring R;   ideal I1 = imap(S,I);
> poly h = t*(t^2-2t-1);   I1 = quotient(I1,h^2);
> reduce(I,std(I1));
_[1]=0
_[2]=0
_[3]=0
_[4]=0
```

□

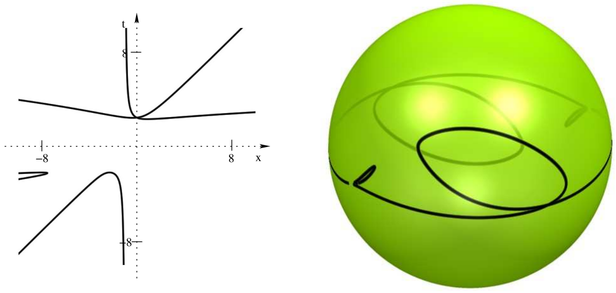
Proof of Proposition 4.17 We have to show that $IL[b,c,t]$ is a prime ideal. For this, relying on a SINGULAR computation as above, one first checks that $I : h = I$. Taking Lemma 2.71, (ii) into account, this implies that

$$IL(t)[b,c] \cap L[b,c,t] = \langle f_1, f_2 \rangle : h^2 = IL[b,c,t].$$

Therefore, it is enough to prove that $IL(t)[b,c]$ is a prime ideal or, equivalently, that f_1 is irreducible in $L(t)[b]$†. This, in turn, is equivalent to proving that f_1 is irreducible in $L[t,b]$. Let $P(t,x) := t^2 f_1(t, x/t)$. Then

$$\begin{aligned} P(t,x) = x^4 - t^2(t-2)x^3 + (-t^5 + 3t^4 - 2t^3 + 2t + 1)x^2 \\ + t^3(t-2)(t^2 - 2t - 1)x + t^2(t^2 - 2t - 1)^2. \end{aligned}$$

We visualize the real curve defined by the polynomial P:



† In $L(t)[b,c]$, the polynomial f_2 is linear in c, whereas f_1 does not depend on c. Hence, $L(t)[b,c]/I \cong L(t)[b]\langle f_1 \rangle$.

The irreducibility of f_1 in $L[t, b]$ follows from that of P in $L[x, t]$. For the latter, we first show that P is not divisible by any factor of x–degree 2. We make the following ansatz:

$$P = (x^2 + ax + b) \cdot (x^2 + gx + d), \tag{4.1}$$

where a, b, g, d are polynomials in t with indeterminates `a(i)`, `b(i)`, `g(i)`, `d(i)` as coefficients. It is easy to see that we can assume

$$\deg(b) \leq 5,\ \deg(a) \leq 3,\ \deg(d) \leq 3,\ \deg(g) \leq 2,$$

so that only finitely many coefficients need to be considered. Then a decomposition (4.1) with coefficients in L does not exist iff the ideal J of the coefficients in x, t of $P-(x^2+ax+b)(x^2+gx+d)$ has no solution in L, that is, if a Gröbner basis of J contains $1 \in \mathbb{F}_p$. In checking this using Singular, we skip the computation to create J over $\mathbb{Z}$ and give just the result (we print [...] to indicate that part of the output is omitted).

```
>J;
J[1]=-b(5)*d(3)
J[2]=-b(5)*g(2)
         [...]
J[11]=-a(0)^2*b(4)+b(0)*b(4)-b(1)*d(3)-b(2)*d(2)-b(3)*d(1)
       -b(4)+2
         [...]
J[14]=-a(0)^2*b(3)+b(0)*b(3)-b(0)*d(3)-b(1)*d(2)-b(2)*d(1)
       -b(3)+4
J[15]=-a(2)-g(2)-2
         [...]
J[24]=-a(0)^2*b(0)+b(0)^2-b(0)
```

Now, we use the `lift` command to verify that $4 \in J$:

```
> matrix M = lift(J,4);
> M;
M[1,1]=-a(0)+8*b(0)*b(3)-8*b(0)*b(4)-16*b(0)*g(1)*g(2)-...
M[2,1]=-a(0)^2+6*a(0)*b(3)-30*a(0)*b(5)*d(1)+...
         [...]
M[11,1]=-1
         [...]
M[14,1]=0
M[15,1]=-a(0)^2*g(2)+12*a(0)*b(3)*g(2)-...
         [...]
M[24,1]=0
```

This shows, in fact, that over $\mathbb{Z}$ and, thus, over each $\mathbb{F}_q$, we have

$$4 = \sum_{i=1}^{24} M[i,1] \cdot J[i].$$

We conclude that if $p \neq 2$, then the polynomial P has no quadratic factor over $L = \overline{\mathbb{F}}_p$. Similarly, one can show that it has no linear factor. This implies that P is absolutely irreducible in $\mathbb{F}_p[t,x]$ for all $p \neq 2$. The case $p = 2$ can be treated similarly. □

Now, having proved Theorem 4.17, we apply it show Theorem 4.14 and, thus, Theorem 4.13. For this, continuing our SINGULAR session, we compute the Hilbert polynomial $\mathrm{P}_{\overline{C^{(q)}}}(t)$.

```
> ring T = 0, (b,c,t,w), dp;
> ideal I = imap(R,I);
> ideal SI = std(I);   SI;
SI[1]=bct-t2+2t+1
SI[2]=bt3-ct3+t4-b2t+bct-c2t-2bt2+2ct2-3t3+bc+t2+t+1
SI[3]=b2c2-b2ct+bc2t-bct2+b2+2bc+c2-b+c-t+2
SI[4]=c2t3-ct4+c3t-2c2t2+3ct3-t4-bc2+bt2-2ct2+4t3-2bt+ct-3t2-b-2t
```

Arguing as earlier, we see that `SI` induces a Gröbner basis of $I\mathbb{F}_q[b,c,t,w]$, for all q. Homogenizing the Gröbner basis elements with respect to w, we get generators for the homogenized ideal $I^h\mathbb{F}_q[b,c,t,w] = (I\mathbb{F}_q[b,c,t,w])^h$ (see Lemma 2.50). In fact, as it easy to see, in the case of $>_{\mathrm{dp}}$, the homogenized Gröbner basis elements form a Gröbner basis for the homogenized ideal. Therefore, the Hilbert polynomial is the same for all q:

```
> SI = homog(SI,w);
> hilbPoly(SI);       // the Hilbert polynomial is 10t - 11
-11,10
```

Proof of Proposition 4.14 From the Hilbert polynomial, we get the degree $d = 10$ and the arithmetic genus $p_a = 12$. Using Theorem 4.15, we obtain:

$$\#(C^{(q)} \cap \mathbb{A}^3(\mathbb{F}_q)) \geq q + 1 - 24\sqrt{q} - 10.$$

This implies that $C^{(q)}$ has at least one $\mathbb{F}_q$–rational point if $q > 593$. For the finitely many remaining cases, the existence of such a point can be checked by a brute force computer search. □

Bibliography

[Appel and Haken (1977)] Appel, K.; Haken, W.: The Solution of the Four-Color Map Problem. Sci. Amer. **237**, 108–121 (1977).

[Aubry and Perret (1996)] Aubry, Y.; Perret, M.: A Weil theorem for singular curves. Arithmetic, Geometry and Coding Theory. Eds.: R. Pellikaan, M. Perret and S.G. Vladut, Walter de Gruyter, Berlin-New York, 1–7 (1996).

[Bandman et al. (2006)] Bandman, T.; Greuel, G.-M.; Grunewald, F.; Kunyavskii, B.; Pfister, G.; Plotkin, E.: Identities for Finite Solvable Groups and Equations in Finite Simple Groups. Compositio Math. **142**, 734–764 (2006).

[Bierstone and Milman (1997)] Bierstone, E.; Milman, P.: Canonical Desingularization in Characteristic Zero by Blowing up the Maximum Strata of a Local Invariant. Invent.Math. **128**, 207–302 (1997).

[Birch and Swinnerton–Dyer (1965)] Birch, H.; Swinnerton–Dyer, H.: Notes on elliptic curves II. Journ. reine u. angewandte Math. **218**, 79–108 (1965).

[Bravo et al. (2005)] Bravo,A.; Encinas,S.; Villamayor,O.: A Simplified Proof of Desingularisation and Applications. Rev. Math. Iberoamericana **21**, 349–458 (2005).

[Buchberger (1965)] Buchberger, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. PhD Thesis, University of Innsbruck, Austria (1965).

[Cox et al. (2007)] Cox, D.; Little, J.; O'Shea, D.: Ideals, Varieties and Algorithms, 3rd ed. Springer (2007).

[Cox et al. (2005)] Cox, D.; Little, J.; O'Shea, D.: Using Algebraic Geometry, 2nd ed. Springer (2005).

[Decker and Lossen (2006)] Decker, W.; Lossen, Chr.: Computing in Algebraic Geometry: A quick start using Singular. Springer (2006).

[Decker et al. (1998)] Decker, W.; Greuel, G.-M.; Pfister, P.: Primary Decomposition: Algorithms and Comparisons. In: Algorithmic Algebra and Number Theory, Springer, 187–220 (1998).

[Decker et al. (1999)] Decker, W.; Greuel, G.-M.; de Jong, T.; Pfister, G.: The Normalization: a new Algorithm, Implementation and Comparisons. In: Proceedings EUROCONFERENCE Computational Methods for Representations of Groups and Algebras (1.4. – 5.4.1997), Birkhäuser, 177–185 (1999).

[Decker and Schreyer (2013)] Decker, W.; Schreyer, F.O.: Varieties, Gröbnerbases, and Algebraic Curves. To appear.

[Dickenstein and Emiris (2005)] Dickenstein, A.; Emiris, I.Z.: Solving Polynomial Equations: Foundations, Algorithms, and Applications. Algorithms and Computations in Mathematics **41**, Springer (2005).

[Doerk and Hawkes (1992)] Doerk, K.; Hawkes, T.: Finite Soluble Groups. De Gruyter Expositions in Mathematics **4**, Berlin (1992)

[Eisenbud et al. (2001)] Eisenbud, D.; Grayson, D.; Stillman, M., Sturmfels, B.: Computations in Algebraic Geometry with Macaulay2. Springer (2001).

[Faugère et al. (1993)] Faugère, J. C.; Gianni, P.; Lazard, D.; Mora, T.: Efficient Computation of Zero–dimensional Gröbner Bases by Change of Ordering. Journal of Symbolic Computation **16**, 329–344 (1993).

[Feit and Thompson (1963)] Feit, Walter; Thompson, John G.: Solvability of groups of odd order. Pacific Journal of Mathematics **13**, 775–1029 (1963).

[Frühbis–Krüger and Pfister (2006)] Frühbis–Krüger, A.; Pfister, G.: Algorithmic Resolution of Singularities. In: C. Lossen, G. Pfister: Singularities and Computer Algebra. LMS Lecture Notes **324**, Cambridge University Press, 157–184 (2006).

[Gianni et al. (1988)] Gianni, P.; Trager, B.; Zacharias, G.: Gröbner Bases and Primary Decomposition of Polynomial Ideals. Journal of Symbolic Computation **6**, 149–167 (1988).

[Gordan (1899)] Gordan, P.: Neuer Beweis des Hilbertschen Satzes über homogene Funktionen. *Nachrichten König. Ges. der Wiss. zu Gött.*, 240–242 (1899).

[Grauert (1972)] Grauert, H.: Über die Deformation isolierter Singularitäten analytischer Mengen. Invent.Math. 15, 171-198, (1972).

[Greuel et al. (2011)] Greuel, G.-M.; Pfister, G.; Schönemann, H.: SINGULAR 3-1-3. A Computer Algebra System for Polynomial Computations. Centre for Computer Algebra, University of Kaiserslautern, `http://www.singular.uni-kl.de` (2011).

[Greuel and Pfister (1998)] Greuel, G.-M.; Pfister, G.: Gröbner Bases and Algebraic Geometry. In: B. Buchberger and F. Winkler (ed.): Gröbner Bases and Applications. LNS **251**, CUP, 109–143 (1998).

[Greuel and Pfister (2002)] Greuel, G.-M.; Pfister, G.: Computer Algebra and Finite Groups. In: Proc. of the ICMS Beijing, 4–14 (2002).

[Greuel and Pfister (2006)] Greuel, G.-M.; Pfister, G.: SINGULAR and Applications. Jahresbericht der DMV **108 (4)**, 167–196 (2006).

[Greuel and Pfister (2007)] Greuel, G.-M.; Pfister G.: A SINGULAR Introduction to Commutative Algebra. Second Edition. Springer (2007).

[Gröbner (1939)] Gröbner, W.: Über die algebraischen Eigenschaften der Integrale von linearen Differentialgleichungen mit konstanten Koeffizienten. Mohatsh. der Mathematik 47, 247-284, (1939).

[Hilbert (1890)] Hilbert, D.: Über die Theorie der algebraischen Formen. Math. Ann. **36**, 473–534 (1890).

[Hironaka (1964)] Hironaka,H.: Resolution of Singularities of an Algebraic Variety over a Field of Characteristic Zero, Ann.Math. **79**, 109–326 (1964).

[Kemper (2007)] Kemper, G.: Morphisms and constructible sets: Making two theorems of Chevalley constructive. Preprint (2007).

[Kreuzer and Robbiano (2000)] Kreuzer, M.; Robbiano, L.: Computational Commutative Algebra 1. Springer (2000).

[Koblitz (1987)] Koblitz, N.: Elliptic Curve Cryptosystems. Mathematics of Computation **48**, 203–209 (1987).

[Labs (2006)] Labs, O.: A Septic with 99 real Nodes. Rend. Sem. Mat. Univ. Pad. **116**, 299–313 (2006).

[Lenstra (1987)] Lenstra Jr., H. W.: Factoring integers with elliptic curves. Annals of Mathematics **2 (126)**, 649–673 (1987).

[Macaulay (1939)] Macaulay, F.S.: Some Properties of Enumeration in the Theory of Modular Systems. Proc. London Math. Soc. 26, 531–555, (1939).

[Miller (1985)] Miller, V.: Use of elliptic curves in cryptography. In: Advances in cryptology—CRYPTO 85, Springer Lecture Notes in Computer Science, **218**, 417–426 (1985).

[Silverman (2009)] Silvermann, Joseph H.: The Arithmetic of Elliptic Curves. Springer (2009).

[Thompson (1968)] Thompson, J.: Non–solvable finite groups all of whose local subgroups are solvable. Bull. Amer. Math. Soc. **74**, 383–437 (1968).

[Vasconcelos (1998)] Vasconcelos, W.V.: Computational Methods in Commutative Algebra and Algebraic Geometry. Springer (1998).

[Wild (2005)] Wild, Marcel: The Groups of Order Sixteen Made Easy. American Mathematical Monthly (2005).

[Wiles (1995)] Wiles, A.: Modular elliptic curves and Fermat's last theorem. Annals of Mathematics **141**, 443–551 (1995).

[Zorn (1936)] Zorn, M.: Nilpotency of finite groups. Bull. Amer. Math.Soc. **42**, 485–486 (1936).

Index