Chapter 1

Introduction

In commutative algebra we are studying systems of polynomial equations. We consider a system of algebraic equations

$$\begin{aligned} f_1(x_1,\ldots,x_n) &= 0, \\ &\vdots \\ f_m(x_1,\ldots,x_n) &= 0, \end{aligned} \tag{1.1}$$

over some field K, i.e. $f_i \in K[x_1,\ldots,x_n]$. Let $\overline{K}$ be the algebraic closure of K, and $\mathbb{A}^n(\overline{K}) = \mathbb{A}^n$ the n-dimensional affine space over $\overline{K}$. A root $\alpha = (\alpha_1,\ldots,\alpha_n) \in \mathbb{A}^n$ of (2.2.1) is also a root of any linear combination of the f_i's, i.e. of any element of the ideal $I = \langle f_1,\ldots,f_m\rangle$ generated by the f_i's. So when we are studying solutions of systems of algebraic equations, we are actually studying common solutions for all elements of a polynomial ideal. On the other hand, because of Hilbert's basis theorem, every ideal in $K[x_1,\ldots,x_n]$ is generated by a finite basis. So the common solutions of any polynomial ideal I are actually the solutions of a finite system of algebraic equations.

The collection of points in $\mathbb{A}^n$ satifying (1.1) is a so-called algebraic set (or variety), and we denote it by $V(I)$. If $V(I)$ consists of only finitely many points, i.e. its dimension is 0, then we also say that I is a 0-dimensional ideal. In this section we assume that the ideal I generated by the polynomials in (1.1) is 0-dimensional (although much of this theory applies also to higher dimensional ideals). The problem we are considering is the following:

Problem "Solution of 0-dimensional system of algebraic equations":

given: $I = \langle f_1,\ldots,f_m\rangle \subseteq K[x_1,\ldots,x_n]$, 0-dimensional,

find: all solutions of I in $\mathbb{A}^n$.

What we actually want are the *elimination ideals* of I, i.e.

$$I_k = I \cap K[x_1,\ldots,x_k], \qquad \text{for } 1 \le k \le n,$$

the ideals consisting of all those polynomials in I just depending on the first k variables. Having determined these elimination ideals, we can successively solve for the variables. So the determination of the elimination ideals plays the same rôle for nonlinear algebraic equations as the Gaussian algorithm plays for linear equations.

The method of resultants:

Let R be a commutative ring, $f(x), g(x) \in R[x]$ two univariate polynomials over R. The resultant of f and g, $h = \mathrm{res}(f,g)$, is an element of $\langle f, g\rangle$, and $\mathrm{res}(f,g) = 0$ if and only if f and g have a common factor (ref. [Wae70], [Win96], [CLO98]).

Example 1.1: Consider the following system of equations:

$$\begin{aligned} f_1(x,y) &= 2x^4 - 3x^2y + y^4 - 2y^3 + y^2 &&= 0,\\ f_2(x,y) = \tfrac{\partial}{\partial x} f_1(x,y) &= 8x^3 - 6xy &&= 0. \end{aligned}$$

The solutions of this system are those points on the tacnode curve (see Fig. 1.3), which are either singular or have a vertical tangent. We are looking for the solutions in the plane over an algebraically closed field containing the field of definition $\mathbb{Q}$, i.e. over $\mathbb{C}$ or actually over $\overline{\mathbb{Q}}$, the field of algebraic numbers. The resultant w.r.t. x is

$$r(y) = \mathrm{res}_x(f_1, f_2) = (y^4 - 2y^3 + y^2)(64y^4 - 128y^3 - 8y^2)^2.$$

$r(y)$ has the roots

$$y = 0,\ 1,\ 1 + \frac{3}{4}\sqrt{2},\ 1 - \frac{3}{4}\sqrt{2}.$$

If, for instance, we substitute $1 + \frac{3}{4}\sqrt{2}$ for y in f_1 and f_2, we get

$$x = \frac{1}{4}\sqrt{12 + 9\sqrt{2}}.$$

So

$$(1 + \frac{3}{4}\sqrt{2},\ \frac{1}{4}\sqrt{12 + 9\sqrt{2}})$$

is one of the roots of this system of algebraic equations. □

This works perfectly for equations in 2 variables. For more variables, there can be "extraneous factors" of the resultant, i.e. solutions of the resultant, which cannot be continued to solutions of the given system.

Example 1.2: Consider the system

$$\begin{aligned} f_1(x,y,z) &= 2xy + yz - 3z^2 &&= 0,\\ f_2(x,y,z) &= x^2 - xy + y^2 - 1 &&= 0,\\ f_3(x,y,z) &= yz + x^2 - 2z^2 &&= 0. \end{aligned}$$

We compute

$$
\begin{aligned}
a(x) &= \mathrm{res}_z(\mathrm{res}_y(f_1, f_3), \mathrm{res}_y(f_2, f_3)) \\
&= x^6(x-1)(x+1)(127x^4 - 167x^2 + 4), \\
b(y) &= \mathrm{res}_z(\mathrm{res}_x(f_1, f_3), \mathrm{res}_x(f_2, f_3)) \\
&= (y-1)^3(y+1)^3(3y^2-1)(127y^4 - 216y^2 + 81)(457y^4 - 486y^2 + 81), \\
c(z) &= \mathrm{res}_y(\mathrm{res}_x(f_1, f_3), \mathrm{res}_x(f_2, f_3)) \\
&= z^4(z-1)(z+1)(3z^2-1)(127z^4 - 91z^2 + 16)(457z^4 - 175z^2 + 16).
\end{aligned}
$$

All the solutions of the system, e.g. $(1, 1, 1)$, have coordinates which are roots of a, b, c. But there is no solution of the system having y-coordinate $1/\sqrt{3}$, although $b(1/\sqrt{3}) = 0$. So not every root of these resultants can be extended to a solution of the whole system. □

The method of Gröbner bases:

This method in elimination theory was invented by Buchberger in 1965. For an overview of applications and current research topics we refer to [BuW98]. We don't want to go into details of definition and properties of Gröbner bases here. Let us just make a few crucial remarks:

- a Gröbner basis is a particular basis for a polynomial ideal (over a field or certain other domains), depending on an "admissible" ordering of the terms or monomials,
- every polynomial ideal has a Gröbner basis,
- for every given finite basis for a polynomial ideal I, we can effectively determine, by Buchberger's algorithm or variants thereof, a finite Gröbner basis generating I, i.e. change from an arbitrary basis of I to a Gröbner basis of I,
- Buchberger's algorithm is implemented in the major computer algebra systems such as Maple, Mathematica, and Reduce.

Because of the elimination property of Gröbner bases, we can exactly determine the elimination ideals of a given ideal I by computing a Gröbner basis for I.

Theorem 1.1: (Elimination property) *Let $I = \langle f_1, \ldots, f_m \rangle$ be an ideal in $K[x_1, \ldots, x_n]$. Let G be a Gröbner basis for the ideal I w.r.t. the lexicographic term ordering with $x_1 < \cdots < x_n$. Then*

$$I \cap K[x_1, \ldots, x_k] \;=\; \langle G \cap K[x_1, \ldots, x_k] \rangle,$$

where the ideal on the right-hand side is generated over $K[x_1, \ldots, x_k]$.

Example 1.2 (continued) We are considering the system of equations

$$\begin{array}{lll} f_1(x,y,z) & = 2xy + yz - 3z^2 & = 0, \\ f_2(x,y,z) & = x^2 - xy + y^2 - 1 & = 0, \\ f_3(x,y,z) & = yz + x^2 - 2z^2 & = 0. \end{array}$$

The set of polynomials $F = \{f_1, f_2, f_3\}$ generates an ideal $I = \langle f_1, f_2, f_3 \rangle$ in $\mathbb{Q}[x_1, x_2, x_3]$. The Gröbner basis for I w.r.t. the lexicographic term ordering with $x > y > z$ (i.e., we consider x as the highest variable) is

$$G = \{g_1, g_2, g_3, g_4\},$$

with

$$\begin{array}{ll} g_1 & = 78x - 2921z^5 + 3744z^3 - 901z, \\ g_2 & = 104y^2 - 2667z^6 + 3562z^4 - 895z^2 - 104, \\ g_3 & = 52yz - 2667z^6 + 3562z^4 - 947z^2, \\ g_4 & = 127z^7 - 218z^5 + 107z^3 - 16z. \end{array}$$

From this Gröbner basis G we can see immediately:

- every solution of $g_4(z) = z(z-1)(z+1)(127z^4 - 91z^2 + 16) = 0$, e.g. -1, can be extended to a solution of the system g_2, g_3, g_4, e.g. $(-1,-1)$, and every such solution can be extended to a solution of the whole system, e.g. $(-1,-1,-1)$,

- the system has 8 solutions (counted with multiplicity). This number corresponds to the 8 terms $1, y, z, z^2, \ldots, z^6$, which are not a multiple of any leading term in G,

- the 2-nd elimination ideal (eliminating x), for instance, is $\langle g_2, g_3, g_4 \rangle$. $\square$

Although the basis G in the previous example might not look simpler than F, it has obvious advantages over F. In particular, G is triangularized, i.e. it contains one polynomial, g_4, which depends only on the least variable, z. In fact, because of the elimination property of Gröbner bases, every polynomial $g(z) \in I \cap \mathbb{Q}[z]$ is a multiple of g_4. Similarly, all the polynomials in I depending only on z and y are linear combinations of g_2, g_3, g_4 (over $\mathbb{Q}[y,z]$).

In order to decide, whether a polynomial $f(x,y,z)$ is in I, we can employ the *division algorithm*, i.e. in f we successively replace any occurrence of x by

$$\frac{1}{78}(2921z^5 - 3744z^3 + 901z),$$

any occurrence of y^2 by

$$\frac{1}{104}(2667z^6 - 3562z^4 + 895z^2 + 104),$$

any occurrence of yz by

$$\frac{1}{52}(2667z^6 - 3562z^4 + 947z^2),$$

and any occurrence of z^7 by

$$\frac{1}{127}(218z^5 - 107z^3 + 16z).$$

Obviously, if we reach 0 by this division process, we have represented f as a linear combination of the basis polynomials, i.e. $f \in I$. Conversely, w.r.t. a Gröbner basis, f must be reducible to 0 by the division algorithm (this fails to be so for an arbitrary basis).

Besides determination of elimination ideals, there are many other algebraic and geometric problems that can be successfully treated by Gröbner bases. Let us list just a few of them:

- ideal membership problem, i.e. "$f \in I$?",
- radical membership problem, i.e. "$f \in \sqrt{I}$?",
- equality of ideals, i.e. "$I = J$?",
- arithmetic of ideals, i.e. computation of $I \cap J, I : J$ ($I + J, I \cdot J$ are easy),
- computation of dimension of ideals, $\dim(I)$,
- computation of syzygies of sequences of polynomials.

Applications of the Gröbner basis method in mathematics, sciences, and engineering are collected in [TrW00].

Geometry of algebraic curves and surfaces

Algebraic curves and surfaces have been studied intensively in algebraic geometry for decades and even centuries. Thus, there exists a huge amount of theoretical knowledge about these geometric objects. Recently, algebraic curves and surfaces play an important and ever increasing rôle in computer aided geometric design, computer vision, and computer aided manufacturing. Consequently, theoretical results need to be adapted to practical needs. We need efficient algorithms for generating, representing, manipulating, analyzing, rendering algebraic curves and surfaces.

One interesting subproblem is the rational parametrization of curves and surfaces. Consider an affine plane algebraic curve $\mathcal{C}$ in $\mathbb{A}^2(\overline{K})$ defined by the bivariate polynomial $f(x, y) \in K[x, y]$, i.e.

$$\mathcal{C} = \{(a, b) \mid (a, b) \in \mathbb{A}^2(\overline{K}) \text{ and } f(a, b) = 0\}.$$

Of course, we could also view this curve in the projective plane $\mathbb{P}^2(\overline{K})$, defined by $F(x, y, z)$, the homogenization of $f(x, y)$.

A pair of rational functions $(x(t), y(t)) \in \overline{K}(t)$ is a *rational parametrization* of the curve $\mathcal{C}$, if and only if $f(x(t), y(t)) = 0$ and for almost every point $(x_0, y_0) \in \mathcal{C}$ (i.e. up to finitely many exceptions) there is a parameter value $t_0 \in \overline{K}$ such that $(x_0, y_0) = (x(t_0), y(t_0))$. Only irreducible curves, i.e. curves whose defining polynomial is absolutely irreducible, can have a rational parametrization. Almost any rational transformation of a rational parametrization is again a rational parametrization, so such parametrizations are not unique.

Implicit representations (by defining polynomial) and parametric representations (by rational parametrization) both have their particular advantages and disadvantages. Given an implicit representation of a curve and a point in the plane, it is easy to check whether the point is on the curve. But it is hard to generate "good" points on the curve, i.e. for instance points with rational coordinates if the defining field is $\mathbb{Q}$. On the other hand, generating good points is easy for a curve given parametrically, but deciding whether a point is on the curve requires the solution of a system of algebraic equations. So it is highly desirable to have efficient algorithms for changing from implicit to parametric representation, and vice versa.

Example 1.3: Let us consider curves in the plane (affine or projective) over $\mathbb{C}$. The curve defined by $f(x, y) = y^2 - x^3 - x^2$ (see Fig. 1.1.1) is rationally parametrizable, and actually a parametrization is $(t^2 - 1, t(t^2 - 1))$.

On the other hand, the elliptic curve defined by $f(x, y) = y^2 - x^3 + x$ (see Fig 1.1.2) does not have a rational parametrization.

The tacnode curve (see Fig. 1.1.3) defined by $f(x, y) = 2x^4 - 3x^2y + y^4 - 2y^3 + y^2$ has the parametrization

$$x(t) = \frac{t^3 - 6t^2 + 9t - 2}{2t^4 - 16t^3 + 40t^2 - 32t + 9}, \quad y(t) = \frac{t^2 - 4t + 4}{2t^4 - 16t^3 + 40t^2 - 32t + 9}.$$

The criterion for parametrizability of a curve is its genus. Only curves of genus 0, i.e. curves having as many singularities as their degree permits, have a rational parametrization. $\square$

Computing such a parametrization essentially requires the full analysis of singularities (either by successive blow-ups, or by Puiseux expansion) and the determination of a regular point on the curve. We can control the quality of the resulting parametrization by controlling the field over which we choose this regular point. Thus, finding a regular curve point over a minimal field extension on a curve of genus 0 is one of the central problems in rational parametrization, compare [SeW91]. The determination of rational points on algebraic curves can be an extremely complicated problem. But for curves of genus 0 the situation can actually be controlled very well. For a curve over a field K of characteristic 0, we can determine whether the curve has a regular point over K, or otherwise find a quadratic field extension which admits such a regular point.

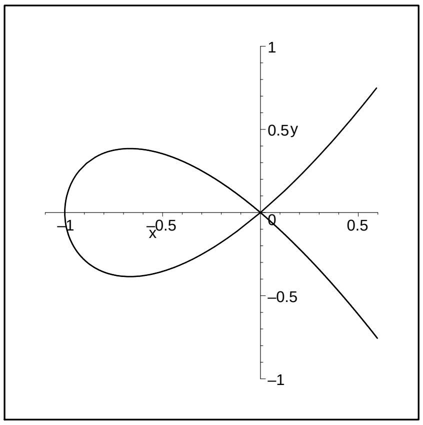

Fig. 1.1.1

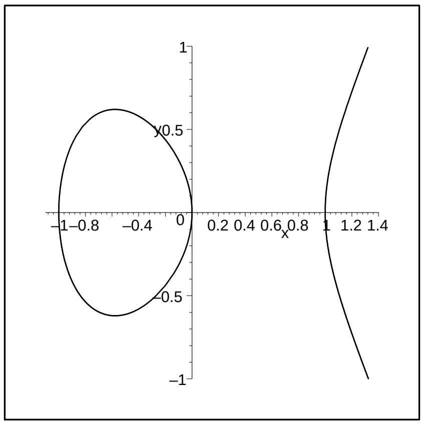

Fig. 1.1.2

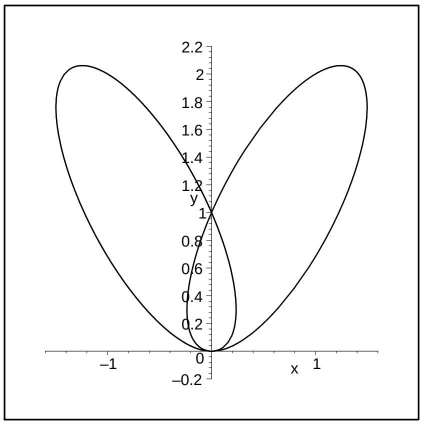

Fig. 1.1.3

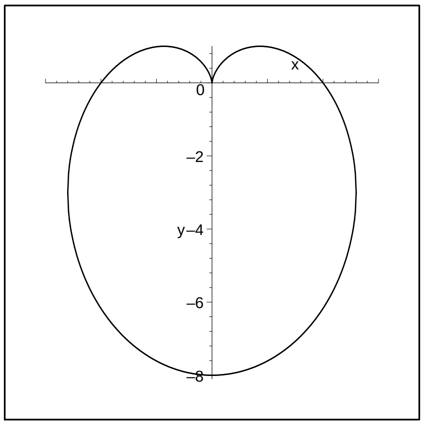

Fig. 1.2.4

Many of these ideas which work for curves can actually be generalized to higher dimensional geometric objects. For instance, one subproblem in computer aided geometric design is the manipulation of offset curves, offset surfaces, pipe and canal surfaces. These are geometric objects keeping certain distances from a generating object. Let us just consider the case of a pipe surface in an example.

An example of such a canal surface is

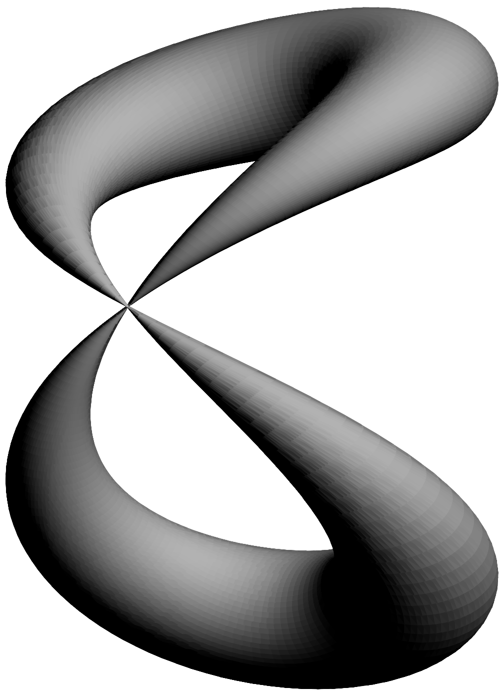

Figure 1.1: canal surface around Viviani's temple