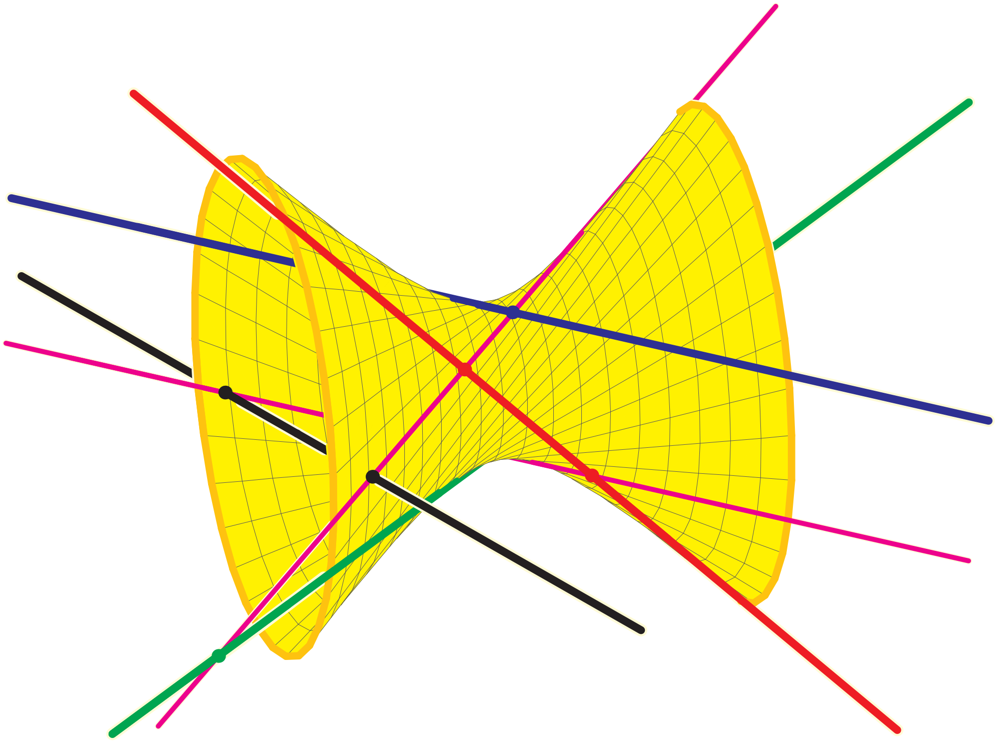
Algebraic Geometry for Applications

Frank Sottile
Department of Mathematics
Texas A&M University
College Station
Texas 77843 USA



January 15, 2026

Contents

Introduction

CHAPTER 1

Varieties

Algebraic geometry uses tools from algebra to study geometric objects called (algebraic) varieties, which arise as the common zeroes of some polynomials. We develop basic notions of algebraic geometry, perhaps the most fundamental being the dictionary between algebraic and geometric concepts. We also introduce basic objects, including affine and projective varieties along with their coordinate rings. We treat maps between varieties, including finite maps, and products of varieties. We provide additional algebraic background in the appendices and pointers to other sources of introductions to algebraic geometry in the references provided at the end of the chapter.

1.1. Affine varieties

Let $\mathbb{K}$ be a field, which for us will almost always be either the complex numbers $\mathbb{C}$, the real numbers $\mathbb{R}$, or the rational numbers $\mathbb{Q}$. These different fields each have their individual strengths and weaknesses. The complex numbers are *algebraically closed* in that every univariate polynomial has a complex root. Algebraic geometry works best over an algebraically closed field, and many introductory texts restrict themselves to the complex numbers. Quite often real number answers are needed in applications. Because of this, we will often consider real varieties and work over $\mathbb{R}$. Symbolic computation provides many useful tools for algebraic geometry, but it requires a field such as $\mathbb{Q}$, which can be represented on a computer. Much of what we do remains true for arbitrary fields, such as the Gaussian rationals $\mathbb{Q}[i]$, or $\mathbb{C}(t)$, the field of rational functions in the variable t, or finite fields. We will at times use this added generality.

Algebraic geometry concerns the interplay of algebra and geometry, with its two most fundamental objects being the ring $\mathbb{K}[x_1,\dots,x_n]$ of polynomials in variables $x_1,\dots,x_n$ with coefficients in $\mathbb{K}$ and the space $\mathbb{K}^n$ of n-tuples $a=(a_1,\dots,a_n)$ of numbers from $\mathbb{K}$, called *affine space*. Evaluating a polynomial $f\in\mathbb{K}[x_1,\dots,x_n]$ at points of $\mathbb{K}^n$ defines a function $f\colon\mathbb{K}^n\to\mathbb{K}$ on affine space. We use these polynomial functions to define our primary object of interest.

Definition 1.1.1. An *affine variety* is the set of common zeroes of some polynomials. Given a set $S\subset\mathbb{K}[x_1,\dots,x_n]$ of polynomials, the affine variety defined by S is the set

$$\mathcal{V}(S) \ :=\ \{a\in\mathbb{K}^n \mid f(a)=0 \quad \text{for } f\in S\}\,.$$

This is a *subvariety* of $\mathbb{K}^n$ or simply a *variety* or (*affine*) *algebraic variety*. ⋄

If X and Y are varieties with $Y\subset X$, then Y is a *subvariety* of X. In Exercise 2, you will be asked to show that if $S\subset T$ are sets of polynomials, then $\mathcal{V}(S)\supset\mathcal{V}(T)$.

The empty set $\emptyset = \mathcal{V}(1)$ and affine space itself $\mathbb{K}^n = \mathcal{V}(0)$ are varieties. Any linear or affine subspace L of $\mathbb{K}^n$ is a variety. Indeed, an affine subspace L has an equation of the form $Ax = b$, where A is a matrix and b is a vector, and so $L = \mathcal{V}(Ax - b)$ is defined by the linear (degree 1) polynomials which form the entries of the vector $Ax - b$. An important special case is when $L = \{b\}$ is a point of $\mathbb{K}^n$. Writing $b = (b_1, \ldots, b_n)$, then L is defined by the equations $x_i - b_i = 0$ for $i = 1, \ldots, n$. An affine subspace may also be parameterized. Let $\Lambda_1, \ldots, \Lambda_n \in \mathbb{K}[y_1, \ldots, y_m]$ be linear polynomials. Then $\{(\Lambda_1(y), \ldots, \Lambda_n(y)) \mid y \in \mathbb{K}^m\}$ is an affine space which is the image of the affine linear map $\varphi\colon \mathbb{K}^m \to \mathbb{K}^n$ defined by $\varphi\colon y \mapsto (\Lambda_1(y), \ldots, \Lambda_n(y))$.

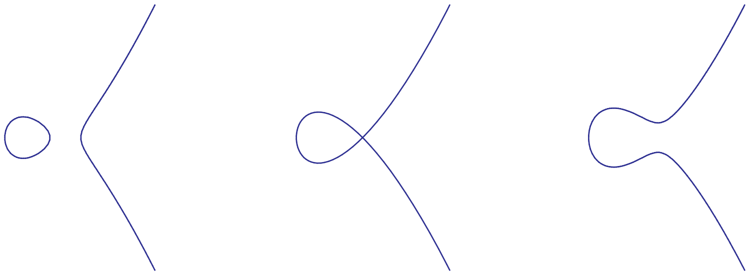
Any finite subset $Z \subset \mathbb{K}^1$ is a variety as $Z = \mathcal{V}(f)$, where

$$f \ := \ \prod_{z \in Z} (x - z)$$

is the monic polynomial with simple zeroes at the points of Z.

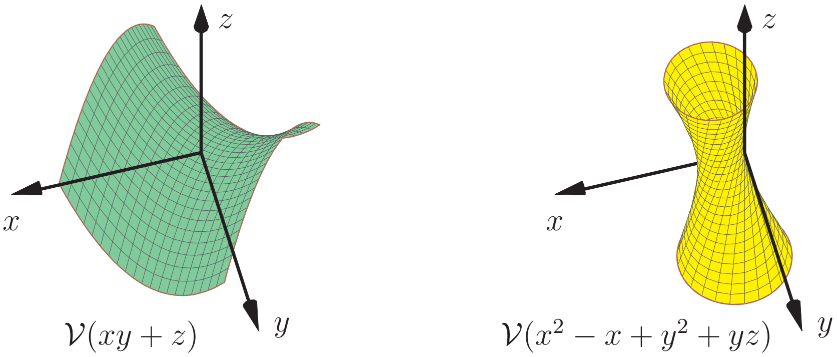
A non-constant polynomial $f(x, y)$ in the variables x and y defines a *plane curve* $\mathcal{V}(f) \subset \mathbb{K}^2$. When $\mathbb{K} = \mathbb{R}$, we show the real plane cubic curves $\mathcal{V}(f + \frac{1}{20})$, $\mathcal{V}(f)$, and $\mathcal{V}(f - \frac{1}{20})$ in $\mathbb{R}^2$, where $f(x, y) := y^2 - x^2 - x^3$.

(1.1.1)



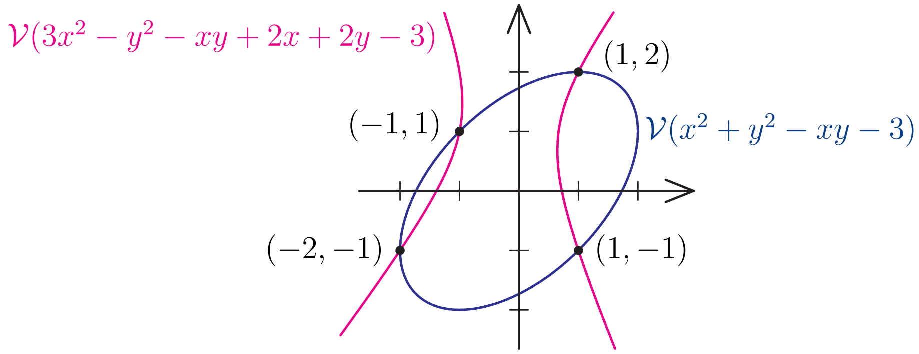
A *quadric* is a variety defined by a single quadratic polynomial. The smooth quadrics in $\mathbb{K}^2$ are the plane conics (circles, ellipses, parabolas, and hyperbolas in $\mathbb{R}^2$) and the smooth quadrics in $\mathbb{R}^3$ are the spheres, ellipsoids, paraboloids, and hyperboloids (a formal definition of smooth variety is given in Section 3.4). We show the hyperbolic paraboloid $\mathcal{V}(xy + z)$ and a hyperboloid of one sheet, $\mathcal{V}(x^2 - x + y^2 + yz)$.

(1.1.2)



These examples, finite subsets of $\mathbb{K}^1$, plane curves, and quadrics, are varieties defined by a single polynomial and are called *hypersurfaces*. Any variety is an intersection of hypersurfaces, one for each polynomial defining the variety. The set of four points

$\{(-2,-1),(-1,1),(1,-1),(1,2)\}$ in $\mathbb{K}^2$ is a variety. It is the intersection of an ellipse $\mathcal{V}(x^2+y^2-xy-3)$ and a hyperbola $\mathcal{V}(3x^2-y^2-xy+2x+2y-3)$.



The quadrics of (1.1.2) meet in the variety $\mathcal{V}(xy+z,\ x^2-x+y^2+yz)$, which is shown on the right in Figure 1.1.1. This intersection is the union of two space curves. One is the line $x=1, y+z=0$, while the other is the cubic space curve which has parametrization $t \mapsto (t^2,t,-t^3)$. Observe that the sum of the degrees of these curves, 1 (for the line) and 3 (for the space cubic) is equal to the product $2\cdot 2$ of the degrees of the quadrics defining the intersection. We will have more to say on this in Section 3.5.

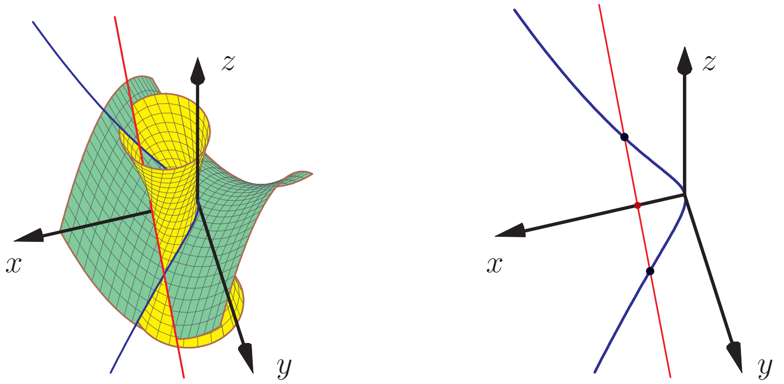


FIGURE 1.1.1. Intersection of two quadrics.

The intersection of the hyperboloid $x^2+(y-\frac{3}{2})^2-z^2=\frac{1}{4}$ with the sphere $x^2+y^2+z^2=4$ centered at the origin with radius 2 is a singular space curve (the ∞ on the left sphere in Figure 1.1.2). If we instead intersect the hyperboloid with the sphere centered at the origin having radius 1.9, then we obtain the smooth quartic space curve drawn on the right sphere in Figure 1.1.2.

More generally, the intersection of any collection of algebraic varieties is again a variety, and the same is true for any finite union. In Exercise 4 you are asked to prove the following.

LEMMA 1.1.2. *Let $\{X_j \mid j\in J\}$ be any collection of varieties in $\mathbb{K}^n$.*

(i) The intersection $\bigcap\{X_j \mid j\in J\}$ is a variety in $\mathbb{K}^n$.

(ii) Suppose that J is finite. Then the union $\bigcup\{X_j \mid j\in J\}$ is a variety in $\mathbb{K}^n$.

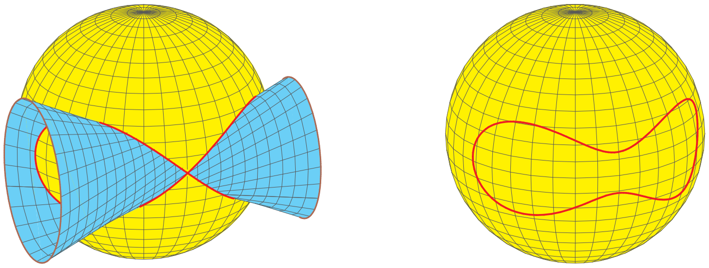


Figure 1.1.2. Quartics on spheres.

Consider $X = \mathcal{V}(xy, xz, yz) \subset \mathbb{K}^3$. Suppose that $(a, b, c) \in X$. As $ab = 0$, either $a = 0$ or $b = 0$. If $a = 0$, then we have the further equation $bc = 0$, and thus one of b or c is zero. Continuing this reasoning, we see that at least two of the three coordinates of a point in X must vanish, so that X is the union of the three coordinate axes in $\mathbb{K}^3$.

The product $X \times Y$ of two varieties X and Y is again a variety. Indeed, suppose that $X \subset \mathbb{K}^n$ is defined by the polynomials $f_1, \dots, f_s \in \mathbb{K}[x_1, \dots, x_n]$ and that $Y \subset \mathbb{K}^m$ is defined by the polynomials $g_1, \dots, g_t \in \mathbb{K}[y_1, \dots, y_m]$. Then $X \times Y \subset \mathbb{K}^n \times \mathbb{K}^m = \mathbb{K}^{n+m}$ is defined by the polynomials $f_1, \dots, f_s, g_1, \dots, g_t \in \mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_m]$. Given a point $x \in X$, the product $\{x\} \times Y$ is a subvariety of $X \times Y$ which may be identified with Y simply by forgetting the coordinate x.

The set $\mathrm{Mat}_{m\times n}$ or $\mathrm{Mat}_{m\times n}(\mathbb{K})$ of $m\times n$ matrices with entries in $\mathbb{K}$ is identified with the affine space $\mathbb{K}^{mn}$, which may be written $\mathbb{K}^{m\times n}$. An interesting class of varieties are linear algebraic groups, which are algebraic subvarieties of the space $\mathrm{Mat}_{n\times n}$ square matrices that are closed under multiplication and taking inverses. The *special linear group* is the set of matrices with determinant 1,

$$SL_n \;:=\; \{M \in \mathrm{Mat}_{n\times n} \mid \det M = 1\}\,,$$

which is a linear algebraic group. Since the determinant of a matrix in $\mathrm{Mat}_{n\times n}$ is a polynomial in its entries, SL_n is the variety $\mathcal{V}(\det - 1)$. We will later show that SL_n is smooth, irreducible, and has dimension $n^2 - 1$. (We must first, of course, define these notions.)

The *general linear group* $GL_n := \{M \in \mathrm{Mat}_{n\times n} \mid \det M \neq 0\}$ at first does not appear to be a variety as it is defined by the non-vanishing of a polynomial. You will show in Exercise 9 that it may be identified with the set $\{(t, M) \in \mathbb{K} \times \mathrm{Mat}_{n\times n} \mid t \det M = 1\}$, which is a variety. When $n = 1$, $GL_1 = \{a \in \mathbb{K} \mid a \neq 0\}$ is the group of units (invertible elements) in $\mathbb{K}$, written $\mathbb{K}^\times$. This is your first example of an important class of varieties called *principal affine open sets*.

Many subsets of $\mathbb{K}^n$ are not varieties. The set $\mathbb{Z}$ of integers is not a variety. The same is true for any other infinite proper subset of $\mathbb{K}$ whose complement is also infinite, for example, the infinite sequence $\{1, \frac{1}{2}, \frac{1}{3}, \dots\}$ is not a subvariety of $\mathbb{R}$ or of $\mathbb{C}$.

Other subsets which are not varieties (for the same reasons) include the unit disc in $\mathbb{R}^2$, $\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}$ or the complex numbers with positive real part. We show these in Figure 1.1.3. These last two, which are defined by inequalities, involving real

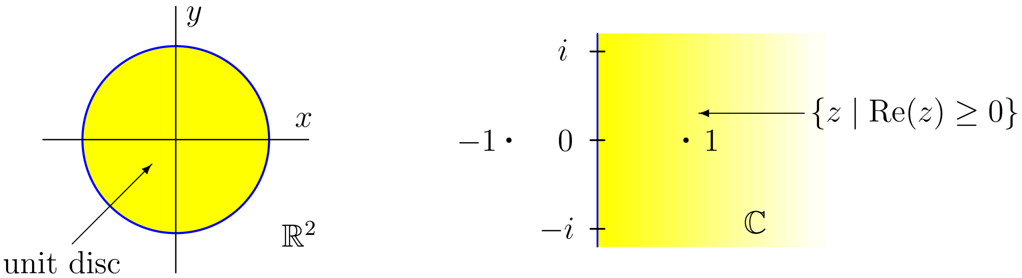


Figure 1.1.3. Unit disc and positive half-plane.

polynomials are examplesa of *semi-algebraic* sets.

Exercises for Section 1.1.

1. Show that no proper nonempty open subset S of $\mathbb{R}^n$ or $\mathbb{C}^n$ is a variety. Here, we mean open in the usual (Euclidean) topology on $\mathbb{R}^n$ and $\mathbb{C}^n$. (Hint: Consider the Taylor expansion of any polynomial that vanishes identically on S.)
2. Let $S \subset T \subset \mathbb{K}[x_1, \ldots, x_n]$ be sets of polynomials. Show that $\mathcal{V}(S) \supset \mathcal{V}(T)$.
3. Describe all subvarieties of $\mathbb{K}$.
4. Suppose that X and Y are varieties in $\mathbb{K}^n$. Prove that $X \cap Y$ and $X \cup Y$ are varieties. Generalize your arguments to prove Lemma 1.1.2.
5. Show that any finite subset Z of $\mathbb{K}^n$ is a variety.
6. Prove that $\mathcal{V}(y - x^2) = \mathcal{V}(y^3 - y^2x^2,\ x^2y - x^4)$ in $\mathbb{K}^2$.
7. Show that the following sets are not algebraic varieties.
   (a) $\mathbb{Z} \subset \mathbb{C}$ and $\mathbb{Z} \subset \mathbb{R}$.
   (b) $\{(x, y) \in \mathbb{R}^2 \mid y = \sin x\}$.
   (c) $\{(\cos t, \sin t, t) \in \mathbb{R}^3 \mid t \in \mathbb{R}\}$.
   (d) $\{(x, e^x) \in \mathbb{R}^2 \mid x \in \mathbb{R}\}$.
8. Express the cubic space curve with parametrization (t, t^2, t^3) for $t \in \mathbb{K}$ as a variety in each of the following ways.
   (a) An intersection of a quadric hypersurface and a cubic hypersurface.
   (b) An intersection of two quadrics.
   (c) An irredundant intersection of three quadrics.
9. Let $\mathbb{K}^{n \times n}$ be the set of $n \times n$ matrices over $\mathbb{K}$.
   (a) Show that the set $SL_n(\mathbb{K}) \subset \mathbb{K}^{n \times n}$ of matrices with determinant 1 is an algebraic variety.
   (b) Show that the set of singular matrices in $\mathbb{K}^{n \times n}$ is an algebraic variety.
   (c) Show that the set $GL_n(\mathbb{K})$ of invertible matrices is not an algebraic variety in $\mathbb{K}^{n \times n}$. Show that $GL_n(\mathbb{K})$ can be identified with an algebraic subset of $\mathbb{K}^{n^2+1} = \mathbb{K}^{n \times n} \times \mathbb{K}^1$ via a map $GL_n(\mathbb{K}) \to \mathbb{K}^{n^2+1}$.
10. Let $\mathbb{K}^{m \times n}$ be the set of $m \times n$ matrices over $\mathbb{K}$. Suppose that $0 \leq r \leq \min\{m, n\}$.
    (a) Show that the set of matrices of rank at most r is an algebraic variety.
    (b) Show that the set of matrices of rank exactly r is not an algebraic variety when $r > 0$ and $\mathbb{K}$ is infinite.

1.2. Varieties and Ideals

The strength and richness of algebraic geometry as a subject and source of tools for applications comes from its dual, simultaneously algebraic and geometric, nature. Intuitive geometric concepts are tamed via the precision of algebra while basic algebraic notions are enlivened by their geometric counterparts. The source of this dual nature is a correspondence—in fact an equivalence—between algebraic concepts and geometric concepts that we call the algebra-geometry dictionary.

We defined varieties $\mathcal{V}(S)$ associated to sets $S \subset \mathbb{K}[x_1, \ldots, x_n]$ of polynomials,

$$\mathcal{V}(S) \ := \ \{x \in \mathbb{K}^n \mid f(x) = 0 \text{ for all } f \in S\}\,.$$

We would like to invert this association. Given a subset Z of $\mathbb{K}^n$, consider the collection of polynomials that vanish on Z,

$$\mathcal{I}(Z) \ := \ \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid f(z) = 0 \text{ for all } z \in Z\}\,.$$

The map $\mathcal{I}$ reverses inclusions so that $Z \subset Y$ implies $\mathcal{I}(Z) \supset \mathcal{I}(Y)$.

These two inclusion-reversing maps

$$\{\text{Subsets } S \text{ of } \mathbb{K}[x_1, \ldots, x_n]\} \quad \underset{\mathcal{I}}{\overset{\mathcal{V}}{\rightleftarrows}} \quad \{\text{Subsets } Z \text{ of } \mathbb{K}^n\} \tag{1.2.1}$$

form the basis of the algebra-geometry dictionary of affine algebraic geometry. We will refine this correspondence to make it more precise.

An *ideal* is a subset $I \subset \mathbb{K}[x_1, \ldots, x_n]$ that is closed under addition and under multiplication by polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. If $f, g \in I$ then $f + g \in I$ and if we also have $h \in \mathbb{K}[x_1, \ldots, x_n]$, then $hf \in I$. The *ideal* $\langle S \rangle$ generated by a subset S of $\mathbb{K}[x_1, \ldots, x_n]$ is the intersection of all ideals contaiing S, the smallest ideal containing S. It is the set of all expressions of the form

$$h_1 f_1 + \cdots + h_m f_m$$

where $f_1, \ldots, f_m \in S$ and $h_1, \ldots, h_m \in \mathbb{K}[x_1, \ldots, x_n]$. We work with ideals because if f, g, and h are polynomials and $x \in \mathbb{K}^n$ with $f(x) = g(x) = 0$, then $(f + g)(x) = 0$ and $(hf)(x) = 0$. Thus $\mathcal{V}(S) = \mathcal{V}(\langle S \rangle)$, and so we may restrict the map $\mathcal{V}$ of the correspondence (1.2.1) to the ideals of $\mathbb{K}[x_1, \ldots, x_n]$. In fact, we lose nothing if we restrict the left-hand-side of the correspondence (1.2.1) to the ideals of $\mathbb{K}[x_1, \ldots, x_n]$.

LEMMA 1.2.1. *For any subset Z of $\mathbb{K}^n$, $\mathcal{I}(Z)$ is an ideal of $\mathbb{K}[x_1, \ldots, x_n]$.*

PROOF. Let $f, g \in \mathcal{I}(Z)$ be polynomials which vanish at all points of Z. Then $f + g$ vanishes on Z, as does hf, where h is any polynomial in $\mathbb{K}[x_1, \ldots, x_n]$. This shows that $\mathcal{I}(Z)$ is an ideal of $\mathbb{K}[x_1, \ldots, x_n]$. □

When $S \subset \mathbb{K}[x_1, \ldots, x_n]$ is infinite, the variety $\mathcal{V}(S)$ is defined by infinitely many polynomials. Hilbert's Basis Theorem tells us that only finitely many of these polynomials are needed.

Hilbert's Basis Theorem. *Every ideal I of $\mathbb{K}[x_1, \ldots, x_n]$ is finitely generated.*

We will prove a stronger form of this (Theorem 2.2.10) in Chapter 2, but use it here. Hilbert's Basis Theorem implies important finiteness properties of algebraic varieties.

COROLLARY 1.2.2. *Any variety $X \subset \mathbb{K}^n$ is the intersection of finitely many hypersurfaces.*

PROOF. Let $X = \mathcal{V}(I)$ be defined by the ideal I. By Hilbert's Basis Theorem, I is finitely generated, say by $f_1, \ldots, f_s$, and so $X = \mathcal{V}(f_1, \ldots, f_s) = \mathcal{V}(f_1) \cap \cdots \cap \mathcal{V}(f_s)$. □

EXAMPLE 1.2.3. The ideal of the cubic space curve C of Figure 1.1.1 with parametrization $(t^2, t, -t^3)$ not only contains the polynomials $xy+z$ and x^2-x+y^2+yz, but also y^2-x, x^2+yz, and y^3+z. Not all of these polynomials are needed to define C as $x^2-x+y^2+yz = (y^2-x)+(x^2+yz)$ and $y^3+z = y(y^2-x)+(xy+z)$. In fact three of the quadrics suffice,

$$\mathcal{I}(C) \;=\; \langle xy+z,\ y^2-x,\ x^2+yz\rangle\,. \qquad \diamond$$

LEMMA 1.2.4. *For any subset Z of $\mathbb{K}^n$, if $X = \mathcal{V}(\mathcal{I}(Z))$ is the variety defined by the ideal $\mathcal{I}(Z)$, then $\mathcal{I}(X) = \mathcal{I}(Z)$ and X is the smallest subvariety of $\mathbb{K}^n$ containing Z.*

PROOF. Set $X := \mathcal{V}(\mathcal{I}(Z))$. Then $\mathcal{I}(Z) \subset \mathcal{I}(X)$, since if f vanishes on Z, it will vanish on X. However, $Z \subset X$, and so $\mathcal{I}(Z) \supset \mathcal{I}(X)$, and thus $\mathcal{I}(Z) = \mathcal{I}(X)$.

If Y was a variety with $Z \subset Y \subset X$, then $\mathcal{I}(X) \subset \mathcal{I}(Y) \subset \mathcal{I}(Z) = \mathcal{I}(X)$, and so $\mathcal{I}(Y) = \mathcal{I}(X)$. But then we must have $Y = X$ for otherwise $\mathcal{I}(X) \subsetneq \mathcal{I}(Y)$, as you will show in Exercise 3. □

Thus we also lose nothing if we restrict the right-hand-side of the correspondence (1.2.1) to the subvarieties of $\mathbb{K}^n$. Our correspondence now becomes

$$(1.2.2) \qquad \{\text{Ideals } I \text{ of } \mathbb{K}[x_1, \ldots, x_n]\} \quad \underset{\mathcal{I}}{\overset{\mathcal{V}}{\rightleftarrows}} \quad \{\text{Subvarieties } X \text{ of } \mathbb{K}^n\}\ .$$

This is not a bijection. In particular, the map $\mathcal{V}$ is not one-to-one and the map $\mathcal{I}$ is not onto. There are several reasons for this.

For example, when $\mathbb{K} = \mathbb{Q}$ and $n = 1$, we have $\emptyset = \mathcal{V}(1) = \mathcal{V}(x^2-2)$. The problem here is that the rational numbers are not algebraically closed and we need to work with a larger field (for example $\mathbb{Q}(\sqrt{2})$) to study $\mathcal{V}(x^2-2)$. When $\mathbb{K} = \mathbb{R}$ and $n = 1$, $\emptyset \neq \mathcal{V}(x^2-2)$, but we have $\emptyset = \mathcal{V}(1) = \mathcal{V}(1+x^2) = \mathcal{V}(1+x^4)$. While the problem here is again that the real numbers are not algebraically closed, we view this as a manifestation of positivity. The two polynomials $1+x^2$ and $1+x^4$ only take positive values. When working over $\mathbb{R}$ (as our interest in applications leads us to do so) positivity of polynomials plays an important role.

The problem with the map $\mathcal{V}$ is more fundamental than these examples reveal and occurs even when $\mathbb{K} = \mathbb{C}$. When $n = 1$ we have $\{0\} = \mathcal{V}(x) = \mathcal{V}(x^2)$, and when $n = 2$, we invite the reader to check that $\mathcal{V}(y-x^2) = \mathcal{V}(y^2-yx^2, xy-x^3)$. Note that while $x \notin \langle x^2\rangle$, we have $x^2 \in \langle x^2\rangle$. Similarly, $y - x^2 \notin \mathcal{V}(y^2-yx^2, xy-x^3)$, but

$$(1.2.3) \qquad (y-x^2)^2 \;=\; y^2 - yx^2 \;-\; x(xy-x^3) \;\in\; \langle y^2-yx^2, xy-x^3\rangle\,.$$

These two cases reveal a source for lack of injectivity of the map $\mathcal{V}$—the polynomials f and f^N have the same set of zeroes, for any positive integer N. For example, if $f_1, \ldots, f_s$ are polynomials, then the two ideals

$$\langle f_1,\, f_2,\, \ldots,\, f_s\rangle \qquad \text{and} \qquad \langle f_1,\, f_2^2,\, f_3^3,\, \ldots,\, f_s^s\rangle$$

both define the same variety, and for any $Z \subset \mathbb{K}^n$, if $f^N \in \mathcal{I}(Z)$, then $f \in \mathcal{I}(Z)$.

We clarify this point with a definition. An ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is *radical* if whenever $f^N \in I$ for some positive integer N, then $f \in I$. The radical $\sqrt{I}$ of an ideal I of $\mathbb{K}[x_1, \ldots, x_n]$ is

$$\sqrt{I} \ := \ \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid f^N \in I\,, \text{ for some } N \geq 1\}\,.$$

You will show in Exercise 4 that $\sqrt{I}$ is the smallest radical ideal containing I. For example (1.2.3) shows that

$$\sqrt{\langle y^2 - yx^2, xy - x^3\rangle} \ = \ \langle y - x^2\rangle\,.$$

The reason for this definition is twofold: first, $\mathcal{I}(Z)$ is radical, and second, an ideal I and its radical $\sqrt{I}$ both define the same variety. We record these facts.

Lemma 1.2.5. *For $Z \subset \mathbb{K}^n$, $\mathcal{I}(Z)$ is a radical ideal. If $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is an ideal, then $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$.*

When $\mathbb{K}$ is algebraically closed, the precise nature of the correspondence (1.2.2) follows from Hilbert's Nullstellensatz (a wonderful German Kompositum: null=zeroes, stelle=places, satz=theorem), another of Hilbert's foundational results in the 1890's that helped to lay the foundations of algebraic geometry and usher in twentieth century mathematics. We first state an apparently weak form of the Nullstellensatz, which describes the ideals defining the empty set.

Theorem 1.2.6 (Weak Nullstellensatz). *Suppose that $\mathbb{K}$ is algebraically closed. If I is an ideal of $\mathbb{K}[x_1, \ldots, x_n]$ with $\mathcal{V}(I) = \emptyset$, then $I = \mathbb{K}[x_1, \ldots, x_n]$.*

The proof of the Weak Nullstellensatz requires some algebraic preliminaries, the most important of which is the following. Recall that if we have rings $A \subset B$, then an element $b \in B$ is *algebraic* over A if there is a nonzero polynomial $f(x) \in A[x]$ such that $f(b) = 0$. An element $b \in B$ that is not algebraic over A, it is *transcendental* over A. Also, B is an *algebraic extension* of A if every element of B is algebraic over A. These notions are reviewed in Section A.1.5.

Lemma 1.2.7. *Let $\mathbb{K}$ be a field and $\mathbb{F} \supset \mathbb{K}$ a field extension that is finitely generated as a $\mathbb{K}$-algebra. Then $\mathbb{F}$ is an algebraic extension of $\mathbb{K}$.*

Proof. We will prove this by contradiction, assuming that $\mathbb{F}$ is a transcendental extension of $\mathbb{K}$ that is finitely generated as a $\mathbb{K}$-algebra, and deduce the contradiction that $\mathbb{F}$ is infinitely generated over $\mathbb{K}$.

Suppose first that $\mathbb{F}$ has transcendence degree one over $\mathbb{K}$, which means that $\mathbb{F}$ contains an element x such that the subfield $\mathbb{K}(x)$ of $\mathbb{F}$ is isomorphic to the field of rational functions in x over $\mathbb{K}$, and that $\mathbb{F}$ is an algebraic extension of $\mathbb{K}(x)$. Then $\mathbb{F}$ is a finitely generated algebraic extension of $\mathbb{K}(x)$ ad therefore it is a finite-dimensional $\mathbb{K}(x)$-vector space. Choose a $\mathbb{K}(x)$-basis $e_1, \ldots, e_n \in \mathbb{F}$ with $e_1 = 1$ and write down the multiplication table of $\mathbb{F}$ in this basis,

$$e_ie_j \ = \ \sum_{k=1}^{n} \frac{a_{ijk}(x)}{b_{ijk}(x)}\, e_k\ , \tag{1.2.4}$$

where $a_{ijk}(x), b_{ijk}(x) \in \mathbb{K}[x]$ are univariate polynomials.

We will show that no finite set $f_1, \ldots, f_m$ of elements of $\mathbb{F}$ generates it as a $\mathbb{K}$-algebra. It is no loss of generality and very convenient to assume that $f_1 = 1$. We may write each f_i in terms of the basis e_j,

$$f_i \ = \ \sum_{j=1}^{n} \frac{c_{ij}(x)}{d_{ij}(x)} e_j \ ,$$

where $c_{ij}(x), d_{ij}(x) \in \mathbb{K}[x]$.

Let $R = \mathbb{K}[f_1, \ldots, f_m]$ be the $\mathbb{K}$-algebra generated by $f_1, \ldots, f_m$. Any element $g \in R$ is a $\mathbb{K}$-linear combination of $f_1 = 1$ and products of the f_i. We may expand this expression in terms of our basis $e_1, \ldots, e_n$ to obtain that g is a $\mathbb{K}(x)$-linear combination of products of the e_j, where the denominators of the coefficients are products of the polynomials $d_{ij}(x)$. Using the formula (1.2.4) to expand the products of the e_j, gives an expression of g as a $\mathbb{K}(x)$-linear combination of $e_1, \ldots, e_n$, where the denominators of the coefficients only involve products of the $b_{ijk}(x)$ and $d_{ij}(x)$.

In particular, if the coefficients in this unique expression of g as a $\mathbb{K}(x)$-linear combination of the e_j are expressed as quotients of coprime polynomials, their denominators are products of irreducible factors found among the $b_{ijk}(x)$ and $d_{ij}(x)$. But this is a finite set of possible irreducible factors for denominators. We conclude that if $h(x) \in \mathbb{K}[x]$ is irreducible and coprime to the $b_{ijk}(x)$ and $d_{ij}(x)$, then $1/h(x) = e_1/h(x) \notin R$. In particular $R \neq \mathbb{F}$, which is a contradiction.

For this argument to be valid, we need that $\mathbb{K}[x]$ has infinitely many irreducible polynomials. If $\mathbb{K}$ is infinite, then the linear polynomials $\{x - a \mid a \in \mathbb{K}\}$ will suffice. More generally, Euclid's proof that there are infinitely many primes in $\mathbb{Z}$ is also valid for $\mathbb{K}[x]$ and it shows that $\mathbb{K}[x]$ has infinitely many irreducible polynomials.

Suppose now that $\mathbb{F}$ has transcendence degree greater than one over $\mathbb{K}$. As it is finitely generated, it has finite transcendence degree, and therefore there is a subextension $\mathbb{E}$ of $\mathbb{K}$ over which $\mathbb{F}$ has transcendence degree one. The previous argument shows that $\mathbb{F}$ cannot be finitely generated as an $\mathbb{E}$-algebra, and thus $\mathbb{F}$ is not finitely generated as a $\mathbb{K}$-algebra. □

Let $b = (b_1, \ldots, b_n) \in \mathbb{K}^n$. In Section 1.1 we observed that the point $\{b\}$ is defined by the linear polynomials $x_i - b_i$ for $i = 1, \ldots, n$. In Exercise 7, you are asked to show that for any polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$, $f(x) - f(b)$ lies in the ideal $\mathfrak{m}_b := \langle x_1 - b_1, \ldots, x_n - b_n \rangle$ defining the point $\{b\}$. Consequently, the quotient ring $\mathbb{K}[x_1, \ldots, x_n]/\mathfrak{m}_b$ is isomorphic to the field $\mathbb{K}$ and so $\mathfrak{m}_b$ is a maximal ideal. When $\mathbb{K}$ is algebraically closed, these are the only maximal ideals of $\mathbb{K}[x_1, \ldots, x_n]$.

Corollary 1.2.8. *Suppose that $\mathbb{K}$ is algebraically closed. Then every maximal ideal $\mathfrak{m}$ of $\mathbb{K}[x_1, \ldots, x_n]$ has the form $\mathfrak{m}_b$ for some $b \in \mathbb{K}^n$.*

Proof. Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{K}[x_1, \ldots, x_n]$. Then $\mathbb{F} = \mathbb{K}[x_1, \ldots, x_n]/\mathfrak{m}$ is a field extension of $\mathbb{K}$ that is finitely generated over $\mathbb{K}$, and hence by Lemma 1.2.7 it is algebraic over $\mathbb{K}$. As $\mathbb{K}$ is algebraically closed, we see that $\mathbb{K} = \mathbb{F}$.

If $b_i \in \mathbb{K}$ is the image of the variable x_i, then we see that $\mathfrak{m} \supset \mathfrak{m}_b$. As both ideals are maximal, they are equal. □

Proof of the weak Nullstellensatz. We prove the contrapositive. Suppose that $I \subsetneq \mathbb{K}[x_1,\dots,x_n]$ is a proper ideal. Then I is contained in a maximal ideal $\mathfrak{m}$. By Corollary 1.2.8, $\mathfrak{m} = \mathfrak{m}_b$ for some $b \in \mathbb{K}^n$ of $\mathbb{K}[x_1,\dots,x_n]$. But then

$$\{b\} \;=\; \mathcal{V}(\mathfrak{m}_b) \;\subset\; \mathcal{V}(I)\,,$$

and so $\mathcal{V}(I) \neq \emptyset$. Thus if $\mathcal{V}(I) = \emptyset$, we must have $I = \mathbb{K}[x_1,\dots,x_n]$, which proves the weak Nullstellensatz. □

A consequence of this proof is that when $\mathbb{K}$ is algebraically closed, there is a 1-1 correspondence

$$\{\text{Points } b \in \mathcal{V}(I)\} \;\longleftrightarrow\; \{\text{Maximal ideals } \mathfrak{m}_b \supset I\}\,.$$

The Fundamental Theorem of Algebra states that any non-constant univariate polynomial $f \in \mathbb{C}[x_1,\dots,x_n]$ has a root (a solution to $f(x) = 0$). We recast the weak Nullstellensatz as a multivariate version of the fundamental theorem of algebra.

Theorem 1.2.9 (Multivariate Fundamental Theorem of Algebra). *Let $\mathbb{K}$ be an algebraically closed field. If the polynomials $f_1,\dots,f_m \in \mathbb{K}[x_1,\dots,x_n]$ generate a proper ideal, then the system of polynomial equations*

$$f_1(x) \;=\; f_2(x) \;=\; \cdots \;=\; f_m(x) \;=\; 0$$

has a solution in $\mathbb{K}^n$.

We now deduce the strong Nullstellensatz, which we will use to complete the characterization (1.2.2). For this, we assume that $\mathbb{K}$ is algebraically closed.

Theorem 1.2.10 (Hilbert's Nullstellensatz). *Let $\mathbb{K}$ be an algebraically closed field. If $I \subset \mathbb{K}[x_1,\dots,x_n]$ is an ideal, then $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$.*

Proof. Since $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$, we have $\sqrt{I} \subset \mathcal{I}(\mathcal{V}(I))$. We show the other inclusion using the 'trick of Rabinowitsch'. Let $f \in \mathcal{I}(\mathcal{V}(I))$ be a polynomial that vanishes on $\mathcal{V}(I)$. Let us introduce a new variable t. Then the variety $\mathcal{V}(I, tf{-}1) \subset \mathbb{K}^{n+1}$ defined by I and $tf{-}1$ is empty. Indeed, if $(y_1,\dots,y_n,z)$ were a point of this variety, then $(y_1,\dots,y_n)$ would be a point of $\mathcal{V}(I)$. But then $f(y_1,\dots,y_n) = 0$, and so the polynomial $tf{-}1$ evaluates to 1 (and not 0) at the point $(y_1,\dots,y_n,z)$.

By the weak Nullstellensatz, $\langle I, tf{-}1\rangle = \mathbb{K}[_1,\dots,x_n,\,t]$. In particular, $1 \in \langle I, tf-1\rangle$, and so there exist polynomials $f_1,\dots,f_m \in I$ and $g_1,\dots,g_m,g \in \mathbb{K}[_1,\dots,x_n,\,t]$ such that

$$1 \;=\; f_1(x)g_1(x,t) + f_2(x)g_2(x,t) + \cdots + f_m(x)g_m(x,t) \;+\; (tf(x)-1)g(x,t)\,.$$

The substitution $t = \frac{1}{f}$ is a ring homomorphism $\mathbb{K}[x_1,\dots,x_n,\,t] \to \mathbb{K}[x_1,\dots,x_n][\frac{1}{f}] \subset \mathbb{K}(x_1,\dots,x_n)$. If we apply it to this expression, then the last term with factor $tf{-}1$ vanishes and each polynomial $g_i(x,t)$ becomes $g_i(x,\frac{1}{f})$, which is a rational function in $x_1,\dots,x_n$ whose denominator is a power of f. Clearing these denominators gives an expression of the form

$$f^N \;=\; f_1(x)G_1(x) + f_2(x)G_2(x) + \cdots + f_m(x)G_m(x)\,,$$

where $G_i(x) = f^N g_i(x,\frac{1}{f}) \in \mathbb{K}[x_1,\dots,x_n]$, for each $i = 1,\dots,m$. But this shows that $f \in \sqrt{I}$, and completes the proof of the Nullstellensatz. □

Corollary 1.2.11 (Algebra-Geometry Dictionary I). *Over any field $\mathbb{K}$, the maps $\mathcal{V}$ and $\mathcal{I}$ give an inclusion reversing correspondence*

$$\{\textit{Radical ideals } I \textit{ of } \mathbb{K}[x_1,\dots,x_n]\} \quad \underset{\mathcal{I}}{\overset{\mathcal{V}}{\rightleftarrows}} \quad \{\textit{Subvarieties } X \textit{ of } \mathbb{K}^n\} \tag{1.2.5}$$

with $\mathcal{V}(\mathcal{I}(X)) = X$. When $\mathbb{K}$ is algebraically closed, the maps $\mathcal{V}$ and $\mathcal{I}$ are inverses, and this correspondence is a bijection.

Proof. First, we already observed that $\mathcal{I}$ and $\mathcal{V}$ reverse inclusions and these maps have the domain and range indicated. Let X be a subvariety of $\mathbb{K}^n$. In Lemma 1.2.4 we showed that $X = \mathcal{V}(\mathcal{I}(X))$. Thus $\mathcal{V}$ is onto and $\mathcal{I}$ is one-to-one.

Now suppose that $\mathbb{K}$ is algebraically closed. By the Nullstellensatz, if I is radical then $\mathcal{I}(\mathcal{V}(I)) = I$, and so $\mathcal{I}$ is onto and $\mathcal{V}$ is one-to-one. Thus $\mathcal{I}$ and $\mathcal{V}$ are inverse bijections. □

Corollary 1.2.11 is only the beginning of the algebra-geometry dictionary. Many natural operations on varieties correspond to natural operations on their ideals. The *sum* $I + J$ and *product* $I \cdot J$ of ideals I and J are defined to be

$$\begin{aligned} I + J &:= \{f + g \mid f \in I \quad \text{and} \quad g \in J\} \\ I \cdot J &:= \langle fg \mid f \in I \quad \text{and} \quad g \in J\rangle\,. \end{aligned}$$

Note that $I + J$ is the ideal $\langle I, J\rangle$ generated by $I \cup J$, and that $I \cap J$ is also an ideal.

Lemma 1.2.12. *Let I, J be ideals in $\mathbb{K}[x_1,\dots,x_n]$ and set $X := \mathcal{V}(I)$ and $Y := \mathcal{V}(J)$ to be their corresponding varieties. Then*

(i) $\mathcal{V}(I + J) = X \cap Y$ and
(ii) $\mathcal{V}(I \cdot J) = \mathcal{V}(I \cap J) = X \cup Y$.

If $\mathbb{K}$ is algebraically closed, then by the Nullstellensatz we also have

(iii) $\mathcal{I}(X \cap Y) = \sqrt{I + J}$ and
(iv) $\mathcal{I}(X \cup Y) = \sqrt{I \cap J} = \sqrt{I \cdot J}$.

You are asked to prove this in Exercise 9.

Example 1.2.13. It can happen that $I \cdot J \neq I \cap J$. For example, if $\langle xy\rangle \cdot \langle yz\rangle = \langle xy^2z\rangle$, but $\langle xy\rangle \cap \langle yz\rangle = \langle xyz\rangle$. ⋄

The correspondence of Corollary 1.2.11 will be further refined in Section 1.3 to include maps between varieties. Because of this correspondence, each geometric concept has a corresponding algebraic concept, and *vice-versa*, when $\mathbb{K}$ is algebraically closed. When $\mathbb{K}$ is not algebraically closed, this correspondence is not exact. In that case we will often use algebra to guide our geometric definitions.

A polynomial $f \in \mathbb{K}[x_1,\dots,x_n]$ has an essentially unique factorization $f = f_1 \cdots f_s$ into irreducible polynomials. It is unique in that any other factorization into irreducible polynomials will have the same length, and after permuting factors, the corresponding factors in each factorization are scalar multiples of each other and hence proportional. Collecting factors proportional to each other in a given factorization and extracting a constant α if necessary, gives $f = \alpha g_1^{n_1} \cdots g_r^{n_r}$ with each $n_i \geq 1$, where, if $i \neq j$, then g_i is not proportional to g_j. The square-free part of f is $\sqrt{f} = g_1 \cdots g_r$, and we have

$$\sqrt{\langle f \rangle} \ = \ \left\langle \sqrt{f}\ \right\rangle \ = \ \langle g_1 \rangle \cap \langle g_2 \rangle \cap \cdots \cap \langle g_r \rangle \,,$$

so that $\mathcal{V}(f) = \mathcal{V}(g_1) \cup \cdots \cup \mathcal{V}(g_r)$.

Exercises for Section 1.2.

1. Show that the map $\mathcal{I}$ reverses inclusions in that $Z \subset Y$ implies $\mathcal{I}(Z) \supset \mathcal{I}(Y)$.
2. Verify the claim that the intersection of all ideals containing a set $S \subset \mathbb{K}[x_1, \ldots, x_n]$ of polynomials is an idea and that it consists of all expressions of the form

$$h_1 f_1 + \cdots + h_m f_m$$

   where $f_1, \ldots, f_m \in S$ and $h_1, \ldots, h_m \in \mathbb{K}[x_1, \ldots, x_n]$.
3. If $Y \subsetneq X$ are varieties, show that $\mathcal{I}(X) \subsetneq \mathcal{I}(Y)$.
4. Let I be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$. Show that

$$\sqrt{I} \ := \ \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid f^N \in I, \text{ for some } N \in \mathbb{N}\}$$

   is an ideal, is radical, and is the smallest radical ideal containing I.
5. Suppose that I and J are radical ideals. Show that $I \cap J$ is also a radical ideal. Is $I \cdot J$ radical?
6. Give radical ideals I and J for which $I + J$ is not radical.
7. Let $b = (b_1, \ldots, b_n) \in \mathbb{K}^n$. Show that for any $(a_1, \ldots, a_n) \in \mathbb{N}^n$, the binomial $x_1^{a_1} \cdots x_n^{a_n} - b_1^{a_1} \cdots b_n^{a_n}$ lies in $\mathfrak{m}_b$. Conclude that for any $f \in \mathbb{K}[x_1, \ldots, x_n]$, the difference $f(x) - f(b) \in \mathfrak{m}_b$, so that $f(x)$ equals $f(b)$, modulo $\mathfrak{m}_b$.
8. Let I be an ideal in $\mathbb{K}[x_1, \ldots, x_n]$, where $\mathbb{K}$ is a field. Prove and find counterexamples to the following statements. Make your assumptions clear and try to find the most general statements.
   (a) If $\mathcal{V}(I) = \mathbb{K}^n$ then $I = \langle 0 \rangle$.
   (b) If $\mathcal{V}(I) = \emptyset$ then $I = \mathbb{K}[x_1, \ldots, x_n]$.
9. Give a proof of Lemma 1.2.12. Hint: Statements *(i)* and *(ii)* are set-theoretic.
10. Give two algebraic varieties Y and Z such that $\mathcal{I}(Y \cap Z) \neq \mathcal{I}(Y) + \mathcal{I}(Z)$.
11. (a) Let I be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$. Show that if $\mathbb{K}[x_1, \ldots, x_n]/I$ is a finite-dimensional $\mathbb{K}$-vector space then $\mathcal{V}(I)$ is a finite set.
    (b) Let $J = \langle xy, yz, xz \rangle$ be an ideal in $\mathbb{K}[x, y, z]$. Find the generators of $\mathcal{I}(\mathcal{V}(J))$. Show that J cannot be generated by two polynomials in $\mathbb{K}[x, y, z]$. Describe $V(I)$ where $I = \langle xy, xz - yz \rangle$. Show that $\sqrt{I} = J$.
12. Prove that there are three points p, q, and r in $\mathbb{K}^2$ such that

$$\sqrt{\langle x^2 - 2xy^4 + y^6, y^3 - y \rangle} \ = \ I(\{p\}) \cap I(\{q\}) \cap I(\{r\}) \,.$$

    Show directly that the ideal $\langle x^2 - 2xy^4 + y^6, y^3 - y \rangle$ is not radical.
13. Deduce the weak Nullstellensatz from the statement of the Strong Nullstellensatz, showing that they are equivalent.

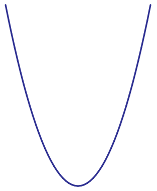
1.3. Maps and homomorphisms

We extend the algebra-geometry dictionary of Section 1.2 in two ways. We first replace affine space $\mathbb{K}^n$ by an affine variety X and the polynomial ring $\mathbb{K}[x_1,\dots,x_n]$ by the ring $\mathbb{K}[X]$ of polynomial (regular) functions on X and establish a correspondence between subvarieties of X and radical ideals of $\mathbb{K}[X]$. We next use this to enrich the algebra-geometry dictionary to a correspondence between regular maps of affine varieties and homomorphisms of their coordinate rings. We close with a nontrivial part of this dictionary concerning finite maps of varieties.

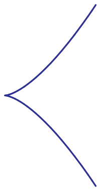
We have used that a polynomial $f \in \mathbb{K}[x_1,\dots,x_n]$ gives a function $f\colon \mathbb{K}^n \to \mathbb{K}$, defined by evaluation at points of $\mathbb{K}^n$. When $\mathbb{K}$ is infinite, the function is identically zero if and only if f is the zero polynomial, so this representation of polynomials by functions is faithful—different polynomials give different functions. When $X \subset \mathbb{K}^n$ is an affine variety, a polynomial function $f \in \mathbb{K}[x_1,\dots,x_n]$ restricts to give a *regular function* on X, $f\colon X \to \mathbb{K}$. We may add and multiply regular functions, and the set of all regular functions on X forms a ring, $\mathbb{K}[X]$, called the *coordinate ring* of the affine variety X or the ring of regular functions on X. It is called the coordinate ring because it is generated as a $\mathbb{K}$-algebra by the functions induced on X by coordinates of the ambient space $\mathbb{K}^n$. The coordinate ring of an affine variety X is a fundamental invariant of X, and when $\mathbb{K}$ is algebraically closed, it is equivalent to X itself.

The restriction of polynomial functions on $\mathbb{K}^n$ to regular functions on X defines a surjective ring homomorphism $\mathbb{K}[x_1,\dots,x_n] \twoheadrightarrow \mathbb{K}[X]$. The kernel of this restriction homomorphism is the set of polynomials that vanish identically on X, that is, the ideal $\mathcal{I}(X)$ of X. Under the correspondence between ideals, quotient rings, and homomorphisms, this restriction map gives an isomorphism between $\mathbb{K}[X]$ and the quotient ring $\mathbb{K}[x_1,\dots,x_n]/\mathcal{I}(X)$.

Example 1.3.1. The coordinate ring of the parabola $y = x^2$ is $\mathbb{K}[x,y]/\langle y-x^2\rangle$, which is isomorphic to $\mathbb{K}[x]$, the coordinate ring of $\mathbb{K}^1$. To see this, observe that substituting x^2 for y rewrites any polynomial $f(x,y) \in \mathbb{K}[x,y]$ as a polynomial $f(x,x^2)$ in x alone. The resulting map $\mathbb{K}[x,y]/\langle y-x^2\rangle \to \mathbb{K}[x]$ is well-defined and surjective. Since $y-x^2$ divides the difference $f(x,y)-f(x,x^2)$, the map is injective.



Parabola



Cuspidal cubic

On the other hand, the coordinate ring of the cuspidal cubic $y^2 = x^3$ is $\mathbb{K}[x,y]/\langle y^2-x^3\rangle$. This ring is not isomorphic to $\mathbb{K}[x,y]/\langle y-x^2\rangle$. Indeed, the element $y^2 = x^3$ has two distinct factorizations into irreducible elements, while polynomials $f(x)$ in one variable have a unique factorization into irreducible polynomials. ◇

Let $\emptyset \neq X \subset \mathbb{K}^n$ be a variety. The constant functions on X realize $\mathbb{K}$ as a subring of its coordinate ring $\mathbb{K}[X]$.

Definition 1.3.2. A $\mathbb{K}$*-algebra* is a ring that contains the field $\mathbb{K}$ as a subring. $\diamond$

A $\mathbb{K}$-algebra has the structure of a vector space over $\mathbb{K}$, given by addition of its elements and multiplication by scalars from $\mathbb{K}$. The coordinate ring $\mathbb{K}[X]$ of a variety X is a $\mathbb{K}$-algebra. As $\mathbb{K}[X] = \mathbb{K}[x_1, \dots, x_n]/\mathcal{I}(X)$, it is finitely generated as a $\mathbb{K}$-algebra by the images of the variables x_i, the coordinate functions. Since $\mathcal{I}(X)$ is radical, Exercise 5 implies that the coordinate ring $\mathbb{K}[X]$ has no nilpotent elements (elements f such that $f^N = 0$ for some N). A ring with no nilpotent elements is *reduced*. When $\mathbb{K}$ is algebraically closed, these two properties characterize coordinate rings of algebraic varieties.

Theorem 1.3.3. *Suppose that $\mathbb{K}$ is algebraically closed. A $\mathbb{K}$-algebra R is the coordinate ring of an affine variety if and only if R is finitely generated and reduced.*

Proof. We need only show that a finitely generated reduced $\mathbb{K}$-algebra R is the coordinate ring of some affine variety. Let $r_1, \dots, r_n$ be generators of a reduced $\mathbb{K}$-algebra R. Then the function $\varphi\colon x_i \to r_i$ extends to a ring homomorphism

$$\varphi \,:\, \mathbb{K}[x_1, \dots, x_n] \twoheadrightarrow R\,,$$

which is surjective as $r_1, \dots, r_n$ generate R. Let $I \subset \mathbb{K}[x_1, \dots, x_n]$ be the kernel of φ. This identifies R with $\mathbb{K}[x_1, \dots, x_n]/I$. Since R is reduced, I is a radical ideal. Indeed, a polynomial $f \notin I$ with $f^N \in I$ gives a nonzero element $\varphi(f) \in R$ with $(\varphi(f))^N = 0$.

As $\mathbb{K}$ is algebraically closed, the algebra-geometry dictionary of Corollary 1.2.11 shows that $I = \mathcal{I}(\mathcal{V}(I))$ and so $R \simeq \mathbb{K}[x_1, \dots, x_n]/I \simeq \mathbb{K}[\mathcal{V}(I)]$. $\square$

A different choice $s_1, \dots, s_m$ of generators for R in this proof will give a different affine variety with the same coordinate ring R. We seek to understand this apparent ambiguity.

Example 1.3.4. The finitely generated $\mathbb{K}$-algebra $R := \mathbb{K}[t]$ is the coordinate ring of the affine line $\mathbb{K}$. Note that if we set $x := t+1$ and $y := t^2 + 3t$, these generate R. As $y = x^2 + x - 2$, this choice of generators realizes R as $\mathbb{K}[x,y]/\langle y - x^2 - x + 2\rangle$, which is the coordinate ring of a parabola in $\mathbb{K}^2$. $\diamond$

Among the coordinate rings $\mathbb{K}[X]$ of affine varieties are the polynomial algebras $\mathbb{K}[x_1, \dots, x_n]$, when $X = \mathbb{K}^n$. Many properties of polynomial algebras, including the algebra-geometry dictionary of Corollary 1.2.11 and the Hilbert Theorems hold for these coordinate rings $\mathbb{K}[X]$.

Given regular functions $f_1, \dots, f_m \in \mathbb{K}[X]$ on an affine variety $X \subset \mathbb{K}^n$, their set of common zeroes

$$\mathcal{V}(f_1, \dots, f_m) \;:=\; \{x \in X \mid f_1(x) = \cdots = f_m(x) = 0\}\,,$$

is a subvariety of X. To see this, let $F_1, \dots, F_m \in \mathbb{K}[x_1, \dots, x_n]$ be polynomials which restrict to the functions $f_1, \dots, f_m$ on X. Then

$$\mathcal{V}(f_1, \dots, f_m) \;=\; X \,\cap\, \mathcal{V}(F_1, \dots, F_m)\,,$$

and by Lemma 1.2.12 intersections of varieties are again varieties. As in Section 1.2, we may extend this notation and define $\mathcal{V}(I)$ for an ideal I of $\mathbb{K}[X]$. If $Y \subset X$ is a subvariety of X, then $\mathcal{I}(X) \subset \mathcal{I}(Y)$ and so $\mathcal{I}(Y)/\mathcal{I}(X)$ is an ideal in the coordinate ring $\mathbb{K}[X] = \mathbb{K}[x_1, \dots, x_n]/\mathcal{I}(X)$ of X. (Recall that ideals of a quotient ring R/I have the form J/I, where J is an ideal of R which contains I.) Write $\mathcal{I}(Y) \subset \mathbb{K}[X]$ for the ideal of Y in $\mathbb{K}[X]$.

Both Hilbert's Basis Theorem and his Nullstellensätze have analogs for affine varieties X and their coordinate rings $\mathbb{K}[X]$. These consequences of the original Hilbert Theorems follow from the surjection $\mathbb{K}[x_1, \ldots, x_n] \twoheadrightarrow \mathbb{K}[X]$ and corresponding inclusion $X \hookrightarrow \mathbb{K}^n$.

Theorem 1.3.5 (Hilbert Theorems for $\mathbb{K}[X]$). *Let X be an affine variety. Then*

(i) Any ideal of $\mathbb{K}[X]$ is finitely generated.
(ii) If Y is a subvariety of X then $\mathcal{I}(Y) \subset \mathbb{K}[X]$ is a radical ideal.
(iii) Suppose that $\mathbb{K}$ is algebraically closed. An ideal I of $\mathbb{K}[X]$ defines the empty set if and only if $I = \mathbb{K}[X]$.

As in Section 1.2 we obtain a version of the algebra-geometry dictionary between subvarieties of an affine variety X and radical ideals of $\mathbb{K}[X]$. The proofs are nearly the same, and we leave them to you in Exercise 6.

Theorem 1.3.6. *Let X be an affine variety. Then the maps $\mathcal{V}$ and $\mathcal{I}$ give an inclusion reversing correspondence*

$$\{\textit{Radical ideals } I \textit{ of } \mathbb{K}[X]\} \quad \underset{\mathcal{I}}{\overset{\mathcal{V}}{\rightleftarrows}} \quad \{\textit{Subvarieties } Y \textit{ of } X\} \tag{1.3.1}$$

with $\mathcal{I}$ injective and $\mathcal{V}$ surjective. When $\mathbb{K}$ is algebraically closed, the maps $\mathcal{V}$ and $\mathcal{I}$ are inverse bijections.

We enrich this correspondence by studying maps between varieties.

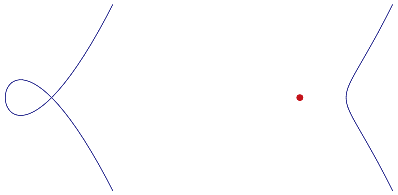
Definition 1.3.7. A list $f_1, \ldots, f_m \in \mathbb{K}[X]$ of regular functions on an affine variety X defines a function

$$\begin{array}{rccl} \varphi : & X & \longrightarrow & \mathbb{K}^m \\ & x & \longmapsto & (f_1(x), f_2(x), \ldots, f_m(x)), \end{array}$$

which we call a *regular map*. ◇

Example 1.3.8. The elements $t^2, t, -t^3 \in \mathbb{K}[t]$ define the map $\mathbb{K}^1 \to \mathbb{K}^3$ whose image is the cubic curve of Figure 1.1.1. The elements t^2, t^3 of $\mathbb{K}[t]$ define a map $\mathbb{K}^1 \to \mathbb{K}^2$ whose image is the cuspidal cubic that we saw in Example 1.3.1.

Let $x = t^2 - 1$ and $y = t^3 - t$, which are elements of $\mathbb{K}[t]$. These define a map $\mathbb{K}^1 \to \mathbb{K}^2$ whose image is the nodal cubic curve $\mathcal{V}(y^2 - (x^3 + x^2))$ on the left below. If we instead take $x = t^2 + 1$ and $y = t^3 + t$, then we get a different map $\mathbb{K}^1 \to \mathbb{K}^2$ whose image is the curve $\mathcal{V}(y^2 - (x^3 - x^2))$ on the right below. Both are singular at the origin.



In the curve on the right, the image of $\mathbb{R}^1$ is the arc, while the isolated or *solitary point* is the common image of the points $\pm\sqrt{-1}$.

Another regular map is matrix multiplication, $\mathbb{K}^{m\times n}\times\mathbb{K}^{n\times p}\to\mathbb{K}^{m\times p}$, because the product of two matrices $(a_{i,j})\in\mathbb{K}^{m\times n}$ and $(b_{k,l})\in\mathbb{K}^{n\times p}$ is the matrix in $\mathbb{K}^{m\times p}$ whose (i,l)-entry is the bilinear polynomial $\sum_{j=1}^{n}a_{i,j}b_{j,l}$. Recall from Exercise **??** in Section 1.1 that $GL_n(\mathbb{K})$ is a variety. Similarly, operation of taking the inverse of a matrix (Exercise 10) is a regular map from $GL_n(\mathbb{K})$ to itself.

Multiplication by an element $A\in\mathrm{Mat}_{m\times n}(\mathbb{K})$ gives a linear map,

$$(y_1,\dots,y_m)^T \;=\; A(x_1,\dots,x_n)^T\,,$$

which is a regular map $\mathbb{K}[x_1,\dots,x_n]\to\mathbb{K}[y_1,\dots,y_m]$. When $m=n$ and A is invertible, this is a linear change of coordinates, and its inverse is induced by A^{-1}. ◇

Suppose that X is an affine variety and we have a regular map $\varphi\colon X\to\mathbb{K}^m$ given by regular functions $f_1,\dots,f_m\in\mathbb{K}[X]$. A polynomial $g\in\mathbb{K}[y_1,\dots,y_m]$ *pulls back* along φ to give the regular function φ^*g, which is defined by composition of functions,

$$\varphi^*g \;:=\; g(f_1,\dots,f_m)\,.$$

This element of the coordinate ring $\mathbb{K}[X]$ of X is the usual pull back of a function. For $x\in X$ we have

$$(\varphi^*g)(x) \;=\; g(\varphi(x)) \;=\; g(f_1(x),\dots,f_m(x))\,.$$

The resulting map $\varphi^*\colon\mathbb{K}[y_1,\dots,y_m]\to\mathbb{K}[X]$ is a homomorphism of $\mathbb{K}$-algebras given by $\varphi^*(y_i)=f_i$. Conversely, given a homomorphism $\psi\colon\mathbb{K}[y_1,\dots,y_m]\to\mathbb{K}[X]$ of $\mathbb{K}$-algebras, if we set $f_i:=\psi(y_i)$, then $f_1,\dots,f_m\in\mathbb{K}[X]$ define a regular map $\varphi\colon X\to\mathbb{K}^m$ with $\varphi^*=\psi$.

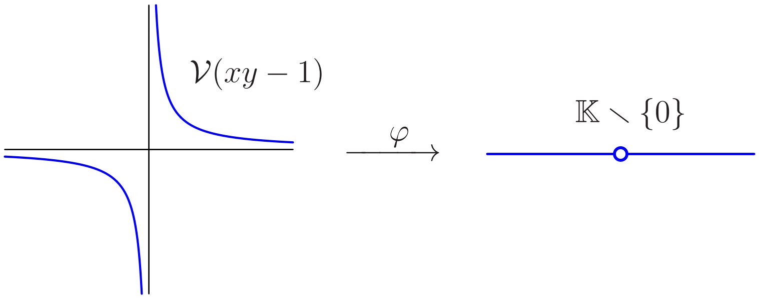
We have just shown the following basic fact.

Lemma 1.3.9. *When $\mathbb{K}$ is infinite, the association $\varphi\mapsto\varphi^*$ defines a bijection*

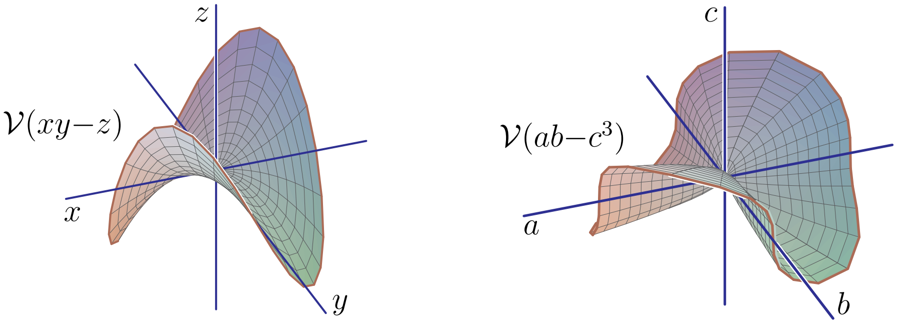
$$\left\{\begin{array}{c}\textit{Regular maps}\\ \varphi\colon X\to\mathbb{K}^m\end{array}\right\} \quad\longleftrightarrow\quad \left\{\begin{array}{c}\mathbb{K}\textit{-algebra homomorphisms}\\ \psi\colon\mathbb{K}[y_1,\dots,y_m]\to\mathbb{K}[X]\end{array}\right\}\,.$$

In each of the regular maps of Example 1.3.8, the image $\varphi(X)$ of X under φ was equal to a subvariety. This is not always the case.

Example 1.3.10. Let $X=\mathcal{V}(xy-1)$ be the hyperbola in $\mathbb{K}^2$ and $\varphi\colon\mathbb{K}^2\to\mathbb{K}$ the map which forgets the second coordinate. Then $\varphi(X)=\mathbb{K}^\times=\mathbb{K}\smallsetminus\{0\}\subsetneq\mathbb{K}$.



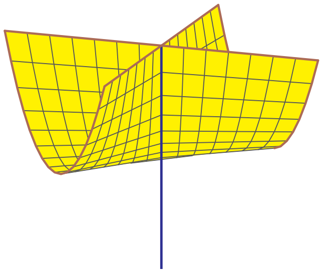
For a more interesting example, let $X = \mathcal{V}(xy-z) \subset \mathbb{K}^3$ be the hyperbolic paraboloid. Consider the map $\varphi\colon X \to \mathbb{K}^3$ given by the three regular functions on X which are the images in $\mathbb{K}[X]$ of yz, xz, xy. Let (a,b,c) be coordinates for the image $\mathbb{K}^3$. Then $\varphi^*(a) = yz$, $\varphi^*(b) = xz$, and $\varphi^*(c) = xy = z$, as $xy = z$ in $\mathbb{K}[X]$. But then $\varphi^*(ab - c^3) = xyz^2 - z^3 = 0$ as again $xy = z$ in $\mathbb{K}[X]$. Consequently, $\varphi(X) \subset \mathcal{V}(ab - c^3)$. We show these two varieties $\mathcal{V}(xy-z)$ and $\mathcal{V}(ab-c^3)$.



We do not have $\varphi(X) = \mathcal{V}(ab-c^3)$. Let $(a,b,c) \in \mathcal{V}(ab-c^3)$. If $c \neq 0$, then you may check that $(b/c, a/c, c) \in \mathcal{V}(xy-z)$, and $\varphi(b/c, a/c, c) = (a,b,c)$. However, if $c = 0$, then either $a = 0$ or $b = 0$. If $(a,b) \neq (0,0)$, then the point (a,b,c) does not lie in the image of φ. Note that we do hve $(0,0,0) = \varphi(0,0,0)$. Thus the image of X under φ is the complement of the a- and b-axes in $\mathcal{V}(ab-c^3)$, together with the origin. This image is neither a subvariety nor the complement of a subvariety. ◇

Lemma 1.3.11. *Let X be an affine variety, $\varphi\colon X \to \mathbb{K}^m$ a regular map, and $Y \subset \mathbb{K}^m$ a subvariety. Then $\varphi(X) \subset Y$ if and only if $\mathcal{I}(Y) \subset \ker\varphi^*$.*

In particular, $\mathcal{V}(\ker\varphi^*)$ is the smallest subvariety of $\mathbb{K}^m$ that contains the image $\varphi(X)$ of X. We call $\mathcal{V}(\ker\varphi^*)$ the subvariety of $\mathbb{K}^m$ parameterized by φ. Determining its ideal $\ker\varphi^* \subset \mathbb{K}[y_1,\dots,y_m]$ is called the implictization problem as it seeks implicit equations that define the the image $\varphi(X) \subset \mathbb{K}^m$. For example, consider the map $\mathbb{K}^2 \to \mathbb{K}^3$ defined by $\varphi(u,v) = (uv, u, v^2)$. Its image is the Whitney umbrella



which has implicit equation $x^2 - y^2z$, where (x,y,z) are the coordinates of $\mathbb{K}^3$. That is $\ker\varphi^* = \langle x^2 - y^2z\rangle$. In general, $\ker\varphi^*$ is the set of polynomials $g \in \mathbb{K}[y_1,\dots,y_m]$ such that $g(f_1,\dots,f_m) = 0$. Thus $\ker\varphi^*$ is the ideal of algebraic relations among the components $f_1,\dots,f_m$ of φ.

Proof of Lemma 1.3.11. First suppose that $\varphi(X) \subset Y$. If $f \in \mathcal{I}(Y)$ then f vanishes on Y and hence on $\varphi(X)$. But then φ^*f is the zero function, and so $\mathcal{I}(Y) \subset \ker\varphi^*$.

For the other direction, suppose that $\mathcal{I}(Y) \subset \ker \varphi^*$ and let $x \in X$. If $f \in \mathcal{I}(Y)$, then $\varphi^* f = 0$ and so $0 = \varphi^* f(x) = f(\varphi(x))$. This implies that $\varphi(x) \in Y$, and so we conclude that $\varphi(X) \subset Y$. $\square$

Definition 1.3.12. Affine varieties X and Y are *isomorphic* if there are regular maps $\varphi \colon X \to Y$ and $\psi \colon Y \to X$ such that both $\varphi \circ \psi$ and $\psi \circ \varphi$ are the identity maps on Y and X, respectively. In this case, we say that φ and ψ are isomorphisms. $\diamond$

Corollary 1.3.13. *Suppose that $\mathbb{K}$ is algebraically closed. Let X be an affine variety, $\varphi \colon X \to \mathbb{K}^m$ a regular map, and $Y \subset \mathbb{K}^m$ a subvariety. Then*

(i) $\ker \varphi^* \subset \mathbb{K}[y_1, \dots, y_m]$ *is a radical ideal.*

(ii) $\mathcal{V}(\ker \varphi^*)$ *is the smallest affine variety containing* $\varphi(X)$.

(iii) If $\varphi \colon X \to Y$, then $\varphi^* \colon \mathbb{K}[y_1, \dots, y_m] \to \mathbb{K}[X]$ factors through $\mathbb{K}[Y]$ inducing a homomorphism $\varphi^* \colon \mathbb{K}[Y] \to \mathbb{K}[X]$.

(iv) φ is an isomorphism of varieties if and only if $\varphi^* \colon \mathbb{K}[Y] \to \mathbb{K}[X]$ is an isomorphism of $\mathbb{K}$-algebras.

(v) $\varphi^{-1}(Y) = \mathcal{V}(\varphi^* \mathcal{I}(Y))$, and if $Z \subset X$ is a subvariety, then $\mathcal{I}(\varphi(Z)) = (\varphi^*)^{-1} \mathcal{I}(Z)$.

In particular, the fiber $\varphi^{-1}(\{y\})$ over a point $y \in Y$ is defined by the ideal $\varphi^*(\mathfrak{m}_y)$.

Proof. For *(i)*, suppose that $f^N \in \ker \varphi^*$, so that $0 = \varphi^*(f^N) = (\varphi^* f)^N$. Since $\mathbb{K}[X]$ has no nilpotent elements, we conclude that $\varphi^* f = 0$ and so $f \in \ker \varphi^*$.

Suppose that Y is an affine variety containing $\varphi(X)$. By Lemma 1.3.11, $\mathcal{I}(Y) \subset \ker \varphi^*$ and so $\mathcal{V}(\ker \varphi^*) \subset Y$. Statement *(ii)* follows as we also have $\varphi(X) \subset \mathcal{V}(\ker \varphi^*)$.

For *(iii)*, we have $\mathcal{I}(Y) \subset \ker \varphi^*$ and so the map $\varphi^* \colon \mathbb{K}[y_1, \dots, y_m] \to \mathbb{K}[X]$ factors through the quotient map $\mathbb{K}[y_1, \dots, y_m] \twoheadrightarrow \mathbb{K}[y_1, \dots, y_m]/\mathcal{I}(Y) = \mathbb{K}[Y]$.

Statement *(iv)* is immediate from the definitions.

For *(v)*, observe that $x \in \varphi^{-1}(Y)$ if and only if $\varphi(x) \in Y$, if and only if $0 = f(\varphi(x)) = \varphi^* f(x)$ for all $f \in \mathcal{I}(Y)$. By part *(ii)*, $\mathcal{I}(\varphi(Z))$ is the kernel of the composition of φ^* with the surjection $\mathbb{K}[X] \twoheadrightarrow \mathbb{K}[Z] = \mathbb{K}[X]/\mathcal{I}(Z)$, which is $\mathcal{I}(Z)$. $\square$

Thus we may refine the correspondence of Lemma 1.3.9. Let X and Y be affine varieties. Then the association $\varphi \mapsto \varphi^*$ gives a bijective correspondence

$$\left\{ \begin{matrix} \text{Regular maps} \\ \varphi : X \to Y \end{matrix} \right\} \quad \longleftrightarrow \quad \left\{ \begin{matrix} \mathbb{K}\text{-algebra homomorphisms} \\ \psi : \mathbb{K}[Y] \to \mathbb{K}[X] \end{matrix} \right\} . \tag{1.3.2}$$

This map $X \mapsto \mathbb{K}[X]$ from affine varieties to finitely generated reduced $\mathbb{K}$-algebras not only sends objects to objects, but it induces a bijection on maps between objects (reversing their direction however). Such an association is called a *contravariant equivalence of categories*. The point of this equivalence is that an affine variety and its coordinate ring are different packages for the same information. Each one determines and is determined by the other. Whether we study algebra or geometry, we are studying the same thing.

Let $\varphi \colon X \to \mathbb{K}^m$ be a map. Then $\varphi \colon X \to \mathcal{V}(\ker \varphi^*)$, by Corollary 1.3.13 *(ii)*, and so $Y := \mathcal{V}(\ker \varphi^*)$ is the smallest affine variety containing $\varphi(X)$. Also, $\varphi^* \colon \mathbb{K}[Y] \to \mathbb{K}[X]$ is an injection. When this occurs, we say that the map $\varphi \colon X \to Y$ is *dominant*.

Suppose that a regular map $\varphi\colon X \to \mathbb{K}^m$ is dominant. Then $\ker\varphi^* = \{0\}$, so that the components $f_1, \dots, f_m$ of φ satisfy no polynomial relation with coefficients in $\mathbb{K}$. In this case, $f_1, \dots, f_m$ are *algebraically independent* over $\mathbb{K}$. In Section 3.3, we use this to develop the notion of dimension of an algebraic variety. Specifically, the dimension of an affine variety X will be the maximum number m such that there is a dominant map $\varphi\colon X \to \mathbb{K}^m$. Equivalently, it is the maximum number of algebraically independent elements in the coordinate ring of X. This notion extends to subrings $R \subset \mathbb{K}[X]$; elements $f_1, \dots, f_m$ of $\mathbb{K}[X]$ are *algebraically independent* over R is there does not exist a nonzero polynomial $g \in R[y_1, \dots, y_m]$ such that $g(f_1, \dots, f_m) = 0$. Equivalently, if the map $R[y_1, \dots, y_m] \to \mathbb{K}[X]$ on the polynomial ring induced by $y_i \mapsto f_i$ is an injection.

As observed in Example 1.3.10, the image of a variety under a regular map need not be a variety. We consider a class of maps that send varieties to varieties. Let $X \subset \mathbb{K}^n$ be a variety and $\varphi\colon X \to \mathbb{K}^m$ be a regular map. When Y is the smallest variety containing $\varphi(X)$, so that $\varphi\colon X \to Y$ is dominant, we noted that the map $\varphi^*\colon \mathbb{K}[Y] \to \mathbb{K}[X]$ is an injection. We identify $\mathbb{K}[Y]$ with the image of φ^*, and consider $\mathbb{K}[Y] \subset \mathbb{K}[X]$. The map $\varphi\colon X \to Y$ is *finite* if there exist $u_1, \dots, u_n \in \mathbb{K}[X]$ such that

$$\mathbb{K}[X] \;=\; u_1\mathbb{K}[Y] + u_2\mathbb{K}[Y] + \cdots + u_n\mathbb{K}[Y]\,. \tag{1.3.3}$$

That is, every element of $\mathbb{K}[X]$ is a $\mathbb{K}[Y]$-linear combination of $u_1, \dots, u_s$. Equivalently, $\mathbb{K}[X]$ is finitely generated as a $\mathbb{K}[Y]$-module. (See Appendix A.1.4.) In contrast, note that $\mathbb{K}[x,y] = \mathbb{K}[y] + x\mathbb{K}[y] + x^2\mathbb{K}[y] + \cdots$, so that $\mathbb{K}[x,y]$ is not finitely generated as a $\mathbb{K}[y]$-module.

WHile at first glance this appears technical, finite maps are an important concept and tool in algebraic geometry. We present the main consequence of finite maps. Suppose that $\mathbb{K}$ is algebraically closed.

THEOREM 1.3.14. *A finite map $\varphi\colon X \to Y$ of affine varieties is surjective. If Z is a subvariety of X, then $\varphi(Z)$ is a subvariety of Y.*

The second statement is left to you as Exercise 8. Before proving this theorem, we explain why such a map is called finite.

COROLLARY 1.3.15. *Let $\varphi\colon X \to Y$ be a finite map. Then every fiber $\varphi^{-1}(y)$ for $y \in Y$ is a nonempty finite set.*

PROOF. Let $t \in \mathbb{K}[X]$. Since $\mathbb{K}[X]$ is finitely generated as a module over $\mathbb{K}[Y]$, it is Noetherian (see Appendix A.1.4) and there is a number $k \geq 1$ such that t^k lies in the submodule generated by $1, t, \dots, t^{k-1}$. (Indeed, for $i \in \mathbb{N}$, let M_i be the $\mathbb{K}[Y]$-submodule generated by $1, t, \dots, t^i$. Then $M_0 \subset M_1 \subset \cdots \subset \mathbb{K}[X]$ is an increasing chain of submodules. As $\mathbb{K}[X]$ is Noetherian, there is some k such that $M_k = M_{k-1}$.) This implies that there exist $c_0, c_1, \dots, c_{k-1} \in \mathbb{K}[Y]$ such that in $\mathbb{K}[X]$ we have

$$t^k + c_{k-1}t^{k-1} + \cdots + c_1 t + c_0 \;=\; 0\,.$$

For $y \in Y$ the value $t(x)$ of t at any point $x \in \varphi^{-1}(y)$ is solution of the equation

$$t^k + c_{k-1}(y)t^{k-1} + \cdots + c_1(y)t + c_0(y) \;=\; 0\,. \tag{1.3.4}$$

That is, t takes on only finitely many (in fact, k, counted with multiplicity) values on $\varphi^{-1}(y)$. As $X \subset \mathbb{K}^n$, doing this for all n coordinate functions shows that the fiber $\varphi^{-1}(y)$ is finite. $\square$

This proof illustrates a useful characterization of finite extensions $\mathbb{K}[Y] \subset \mathbb{K}[X]$. Suppose that $S \subset R$ are $\mathbb{K}$-algebras. An element $t \in R$ is *integral* over S if there are $c_1, \dots, c_k \in S$ such that

$$t^k + c_1 t^{k-1} + c_2 t^{k-2} + \cdots + c_{k-1} t + c_k \;=\; 0\,.$$

That is, t satisfies a monic polynomial equation with coefficients in S. A map $\varphi\colon X \to Y$ is finite if and only if $\varphi^*\colon \mathbb{K}[Y] \to \mathbb{K}[X]$ is an injection and every element $t \in \mathbb{K}[X]$ is integral over $\mathbb{K}[Y]$. Corollary 1.3.15 gives one direction, the other is given in Appendix A.1.4.

Another meaningful, but vague, interpretation of the adjective finite is that as y moves in Y, none of the points of $\varphi^{-1}(y)$ may disappear by going to infinity as in Example 1.3.10. Indeed, if t is a coordinate function on $\mathbb{K}^n$, then on $\varphi^{-1}(y)$ it satisfies (1.3.4), and no root of this polynomial can tend to infinity as the coefficient of the leading term is 1. Consequently, as y moves in Y, the points in the fiber may merge, but they will not disappear.

We present an elementary proof of Theorem 1.3.14. Let us first recall Cramer's rule, which is a consequence of the standard formula for determinant. Let R be a ring and $M \in \mathrm{Mat}_{n\times n}(R)$, an $n \times n$ matrix with entries from R. We have the usual formula for the determinant of $M = (m_{i,j})_{i,j=1}^n$,

$$\det(M) \;:=\; \sum_{\pi \in S_n} \mathrm{sgn}(\pi) m_{1,\pi(1)} \cdot m_{2,\pi(2)} \cdots m_{n,\pi(n)}\ , \tag{1.3.5}$$

where S_n is the group of permutations of $[n] := \{1, \dots, n\}$, and for $\pi \in S_n$, its sign is $\mathrm{sgn}(\pi) := (-1)^{\ell(\pi)}$, where

$$\ell(\pi) \;:=\; \#\{i < j \mid \pi(i) > \pi(j)\}\,.$$

For $i, j \in [n]$, let $\widehat{M_{i,j}}$ be the matrix obtained from M by deleting its ith row and jth column. Define the *adjugate* of the matrix M to be $\mathrm{adj}(M) \in \mathrm{Mat}_{n\times n}(R)$ to be the matrix whose (i, j)-th entry is

$$\mathrm{adj}(M)_{i,j} \;:=\; (-1)^{i+j} \det(\widehat{M_{j,i}})\,.$$

(Note the transpose in $\widehat{M_{j,i}}$.) Exercise 9 asks you to prove Cramer's rule,

$$\mathrm{adj}(M) \cdot M \;=\; \det(M) I_n\,. \tag{1.3.6}$$

Here I_n is the $n \times n$ identity matrix. When $\det(M) \in R$ is invertible, this gives a formula for the inverse of a matrix M.

The next step is a result from commutative algebra.

LEMMA 1.3.16. *Let $S \subset R$ be $\mathbb{K}$-algebras and suppose that R is finitely generated as an S-module. If $I \subsetneq S$ is a proper ideal of S, then $IR \neq R$.*

Proof. There exist $r_1, \ldots, r_n \in R$ such that $R = r_1S + \cdots + r_nS$. Suppose that $IR = R$. Then there are elements $m_{i,j} \in I$ for $i, j \in [n]$ such that,

$$r_i \;=\; \sum_{j=1}^{n} m_{i,j} r_j\,, \tag{1.3.7}$$

for each $i = 1, \ldots, n$. Writing M for the matrix $(m_{i,j})_{i,j=1}^{n}$ and $\vec{r}$ for the vector $(r_1, \ldots, r_n)^T$, we may express (1.3.7) as $(I_n - M)\vec{r} = 0$ in R^n.

By Cramer's rule (1.3.6) applied to the matrix $I_n - M$,

$$0 \;=\; \operatorname{adj}(I_n - M)\cdot(I_n - M)\vec{r} \;=\; \det(I_n - M)I_n\vec{r}\,.$$

Writing μ for $\det(I_n - M) \in S$, we have $\mu\vec{r} = 0$. That is, $\mu r_i = 0$ for each generator r_i of R as an S-module, and so $\mu R = 0$. As $1 \in R$ (it is a $\mathbb{K}$-algebra), this implies that $\mu = 0$. As $m_{i,j} \in I$, the formula (1.3.5) for $\det(I_n - M)$ shows that $\mu = 1 + s$ for some $s \in I$, which implies that $-1 \in I$ and so $I = S$, a contradiction. □

Proof of Theorem 1.3.14. Let $\varphi\colon X \to Y$ be a finite map of varieties. Then $\mathbb{K}[X]$ is a finitely generated $\mathbb{K}[Y]$-module. Let $y \in Y$ and $\mathfrak{m}_y \subset \mathbb{K}[Y]$ its (maximal) ideal. By Corollary 1.3.13(5), the ideal of $\varphi^{-1}(y)$ is $\mathfrak{m}_y\mathbb{K}[X]$. By Lemma 1.3.16, $\mathfrak{m}_y\mathbb{K}[X] \neq \mathbb{K}[X]$, as $\mathfrak{m}_y \neq \mathbb{K}[Y]$. By the Nullstellensatz, $\emptyset \neq \mathcal{V}(\mathfrak{m}_y\mathbb{K}[X]) = \varphi^{-1}(y)$, which completes the proof. □

Exercises for Section 1.3.

1. Suppose that $\mathbb{K}$ is an infinite field. Show that $f \in \mathbb{K}[x_1, \ldots, x_n]$ defines the zero function $f\colon \mathbb{K}^n \to \mathbb{K}$ if and only if f is the zero polynomial. (Hint: For the interesting direction, consider first the case when $n = 1$ and then use induction.)
2. Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal. Show that if $\mathbb{K}[x_1, \ldots, x_n]/I$ is a finite-dimensional $\mathbb{K}$-vector space, then $\mathcal{V}(I)$ is a finite set.
3. Suppose that $X \subset \mathbb{K}^n$ is finite. Prove that the restriction of polynomial functions to X is a surjective map from the ring of polynomials $\mathbb{K}[x_1, \ldots, x_n]$ to the finite vector space of functions from $X \to \mathbb{K}$.
4. Let $V = \mathcal{V}(y - x^2) \subset \mathbb{K}^2$ and $W = \mathcal{V}(xy - 1) \subset \mathbb{K}^2$. Show that

$$\begin{aligned} \mathbb{K}[V] &:= \mathbb{K}[x,y]/\mathcal{I}(V) \cong \mathbb{K}[t] \\ \mathbb{K}[W] &:= \mathbb{K}[x,y]/\mathcal{I}(W) \cong \mathbb{K}[t, t^{-1}] \end{aligned}$$

   Conclude that the hyperbola $V(xy - 1)$ is not isomorphic to the affine line.
5. Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal. Show that the quotient ring $\mathbb{K}[x_1, \ldots, x_n]/I$ has nilpotent elements if and only if I is not a radical ideal.
6. Give a proof of Theorem 1.3.5.
7. Verify the claims about the parameterizations in Example 1.3.8, that the image of $\mathbb{K}$ under the map $t \mapsto (t^2 - 1, t^3 - t)$ is $\mathcal{V}(y^2 - (x^3 + x^2))$ and its image under $t \mapsto (t^2 + 1, t^3 + t)$ is $\mathcal{V}(y^2 - (x^3 - x^2))$.
8. Prove the second statement of Theorem 1.3.14, using (1.3.3) and Corollary 1.3.13*(v)* to show that $\mathbb{K}[Z]$ is finitely generated as a module over an appropriate subalgebra.

9. Prove Cramer's rule (1.3.6). You may use the formula (1.3.5) for the determinant, or any other properties of determinant. Under what conditions does this give a formula for the inverse of a matrix?
10. Show that $A \mapsto A^{-1}$ is a regular map on $GL_n(\mathbb{K})$.
11. Consider the map $p\colon \mathbb{K}^{2\times 4} \to \mathbb{K}^6$ that sends a 2×4 matrix $(x_{i,j})$ to its six maximal minors $p_{i,j} := x_{1,i}x_{2,j} - x_{1,j}x_{2,i}$ for $1 \leq i < j \leq 4$. Compute the ideal $\ker p^*$ and show that $p(\mathbb{K}^{2\times 4})$ is a subvariety of $\mathbb{K}^6$. (Its image is closed.)

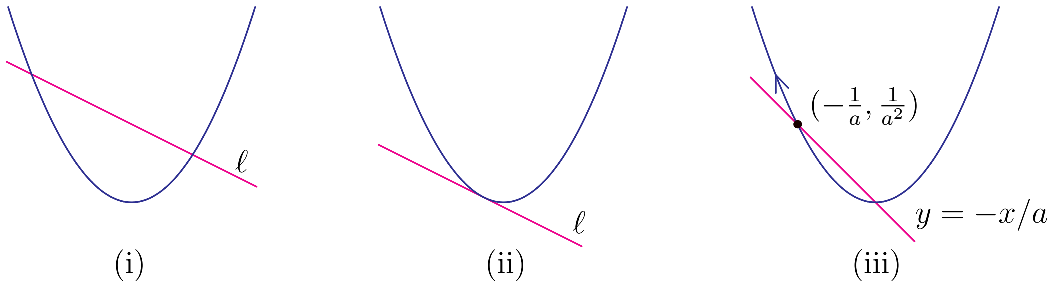
1.4. Projective varieties

Projective space and projective varieties are of central importance in algebraic geometry. We motivate projective space with an example.

Example 1.4.1. Consider the intersection of the parabola $y = x^2$ in the affine plane $\mathbb{K}^2$ with a line, $\ell := \mathcal{V}(ay + bx + c)$. Solving these implied equations gives

$$ax^2 + bx + c \;=\; 0 \qquad \text{and} \qquad y \;=\; x^2\,. \tag{1.4.1}$$

There are several cases to consider, illustrated in Figure 1.4.1.



(i) (ii) (iii)

Figure 1.4.1. The intersection of a parabola with a line in $\mathbb{R}^2$.

(i) $a \neq 0$ and $b^2 - 4ac > 0$. Then ℓ meets the parabola in two distinct real points.

(i$'$) $a \neq 0$ and $b^2 - 4ac < 0$. Then ℓ does not appear to meet the parabola, as the picture is in $\mathbb{R}^2$. In $\mathbb{C}^2$, ℓ meets it in two complex conjugate points.

When $\mathbb{K}$ is algebraically closed, then cases (i) and (i$'$) coalesce to the case of $a \neq 0$ and $b^2 - 4ac \neq 0$. These two points of intersection are predicted by Bézout's Theorem in the plane (Theorem 2.1.16).

(ii) $a \neq 0$ but $b^2 - 4ac = 0$. Then ℓ is tangent to the parabola and we solve the equations (1.4.1) to get

$$a(x - \tfrac{b}{2a})^2 \;=\; 0 \qquad \text{and} \qquad y \;=\; x^2\,.$$

Thus there is one solution, $(\frac{b}{2a}, \frac{b^2}{4a^2})$. As $x = \frac{b}{2a}$ is a root of multiplicity 2 in the first equation, it is reasonable to say that this one solution to our geometric problem occurs with multiplicity 2, agreeing with B'ezout's Theorem.

(iii) $a = 0$, so that the line ℓ is vertical. There is a single, unique solution, $x = -c/b$ and $y = c^2/b^2$.

Let us examine this passage to a vertical line. Suppose that $c = 0$ and $b = 1$. For $a \neq 0$, there are two solutions $(0,0)$ and $(-\frac{1}{a}, \frac{1}{a^2})$. In the limit as $a \to 0$, the second solution disappears off to infinity.

One purpose of projective space is to prevent this last phenomenon from occurring. ◇

Definition 1.4.2. The set of all one-dimensional linear subspaces of $\mathbb{K}^{n+1}$ is called *n-dimensional projective space* and written $\mathbb{P}^n$ or $\mathbb{P}^n_{\mathbb{K}}$. If V is a finite-dimensional vector space, then $\mathbb{P}(V)$ is the set of all one-dimensional linear subspaces of V. Note that $\mathbb{P}(V) \simeq \mathbb{P}^{\dim V - 1}$. If $V \subset \mathbb{K}^{n+1}$ is a linear subspace, then $\mathbb{P}(V) \subset \mathbb{P}^n$ is a *linear subspace* of $\mathbb{P}^n$. ◇

Example 1.4.3. The projective line $\mathbb{P}^1$ is the set of lines through the origin in $\mathbb{K}^2$. When $\mathbb{K} = \mathbb{R}$, the line $x = ay$ through the origin intersects the circle $\mathcal{V}(x^2 + (y-1)^2 - 1)$ in the origin and in the second point $(\frac{2a}{1+a^2}, \frac{2}{1+a^2})$, as shown in Figure 1.4.2. Identifying the non-horizontal line $x = ay$ with this point $(\frac{2a}{1+a^2}, \frac{2}{1+a^2})$ and the horizontal x-axis with the origin, this identifies $\mathbb{P}^1_{\mathbb{R}}$ with the circle. This map $a \mapsto (\frac{2a}{1+a^2}, \frac{2}{1+a^2})$ is Diophantus' rational parametrization of the circle. ◇

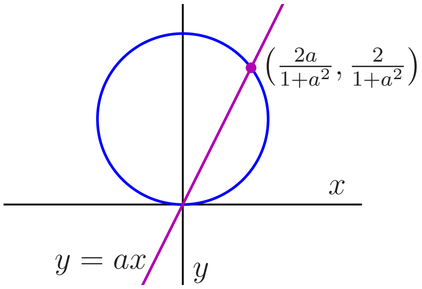


Figure 1.4.2. Lines through the origin meet the circle in a second point.

This definition of $\mathbb{P}^n$ leads to a system of 'coordinates' for $\mathbb{P}^n$. We represent a point, ℓ, of $\mathbb{P}^n$ by the coordinates $[a_0, a_1, \ldots, a_n]$ of any nonzero vector lying on the one-dimensional linear subspace $\ell \subset \mathbb{K}^{n+1}$. These coordinates are not unique. If $\lambda \neq 0$, then $[a_0, a_1, \ldots, a_n]$ and $[\lambda a_0, \lambda a_1, \ldots, \lambda a_n]$ both represent the same point. This non-uniqueness is the reason that we use rectangular brackets $[\ldots]$ for these *homogeneous coordinates*. Some authors prefer $[a_0 : a_1 : \cdots : a_n]$, emphasizing the ratios.

Example 1.4.4. When $\mathbb{K} = \mathbb{R}$, observe that a 1-dimensional subspace of $\mathbb{R}^{n+1}$ meets the unit sphere S^n in two antipodal points, v and $-v$. The group $S^0 = \{-1, 1\}$ of real numbers of absolute value 1 acts on S^n by scalar multiplication interchanging antipodal points. This identifies real projective space $\mathbb{P}^n_{\mathbb{R}}$ with the quotient $S^n/\{\pm 1\}$, showing that $\mathbb{P}^n_{\mathbb{R}}$ is a compact manifold in the usual (Euclidean) topology.

Suppose that $\mathbb{K} = \mathbb{C}$. Given a point $a \in \mathbb{P}^n_{\mathbb{C}}$, after scaling, we may assume that $|a_0|^2 + |a_1|^2 + \cdots + |a_n|^2 = 1$. Identifying $\mathbb{C}$ with $\mathbb{R}^2$, this is the set of points a on the $(2n+1)$-sphere $S^{2n+1} \subset \mathbb{R}^{2n+2}$. If $[a_0, \ldots, a_n] = [b_0, \ldots, b_n]$ with $a, b \in S^{2n+1}$, then there is some $\zeta \in S^1$, the unit circle in $\mathbb{C}$, such that $a_i = \zeta b_i$. This identifies $\mathbb{P}^n_{\mathbb{C}}$ with the quotient of S^{2n+1}/S^1, showing that $\mathbb{P}^n_{\mathbb{C}}$ is a compact manifold. This is a version of the Hopf fibration. Since $\mathbb{P}^n_{\mathbb{R}} \subset \mathbb{P}^n_{\mathbb{C}}$, we again see that $\mathbb{P}^n_{\mathbb{R}}$ is compact. ◇

Homogeneous coordinates of a point are not unique. Uniqueness may be restored, but at the price of non-uniformity. Let $A_i \subset \mathbb{P}^n$ be the set of points $[a_0, a_1, \ldots, a_n]$ in projective space $\mathbb{P}^n$ with $a_i \neq 0$, but $a_{i+1} = \cdots = a_n = 0$. Given a point $a \in A_i$, we may divide by its ith coordinate to get a representative of the form $[a_0, \ldots, a_{i-1}, 1, 0, \ldots, 0]$. These i numbers $(a_0, \ldots, a_{i-1})$ provide coordinates for A_i, identifying it with the affine space $\mathbb{K}^i$. This decomposes projective space $\mathbb{P}^n$ into a disjoint union of $n+1$ affine spaces

$$\mathbb{P}^n \;=\; \mathbb{K}^n \sqcup \cdots \sqcup \mathbb{K}^1 \sqcup \mathbb{K}^0\,,$$

one may say that $\mathbb{P}^n$ is *paved by affine spaces*.

Example 1.4.5. Figure 1.4.3 shows the possible positions of a one-dimensional linear subspace $\ell \subset \mathbb{K}^3$ with respect to the x, y-plane $z = 0$, the x-axis $z = y = 0$, and the origin in $\mathbb{K}^3$. Note that the last two charts give $\mathbb{P}^1$, so we have $\mathbb{P}^2 = \mathbb{K}^2 \sqcup \mathbb{P}^1$, which is the familiar decomposition of the projective plane as the affine plane together with the line at infinity. ◇

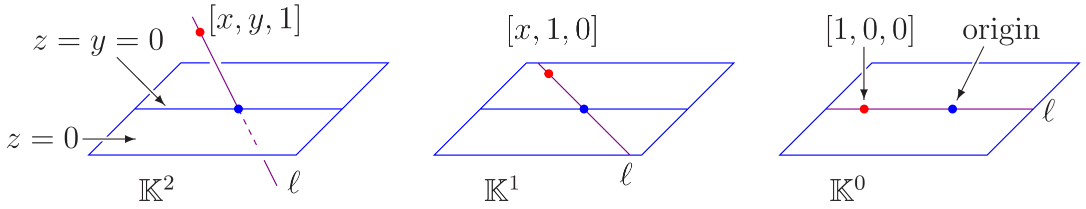


Figure 1.4.3. Paving of $\mathbb{P}^2$ by affine charts.

Projective space also admits systems of local coordinates. For each $i = 0, \ldots, n$, let U_i be the set of points $a \in \mathbb{P}^n$ in projective space whose ith coordinate is nonzero. Dividing by this ith coordinate, we obtain a representative of the point having the form

$$[a_0, \ldots, a_{i-1}, 1, a_{i+1}, \ldots, a_n]\,.$$

The n coordinates $(a_0, \ldots, a_{i-1},\; a_{i+1}, \ldots, a_n)$ determine this point, identifying U_i with affine n-space, $\mathbb{K}^n$. Geometrically, U_i is the set of lines in $\mathbb{K}^{n+1}$ that meet the affine hyperplane defined by $x_i = 1$, with the point of intersection identifying U_i with this hyperplane. Every point of $\mathbb{P}^n$ lies in some U_i, so that we have

$$\mathbb{P}^n \;=\; U_0 \cup U_1 \cup \cdots \cup U_n\,.$$

When $\mathbb{K} = \mathbb{R}$ or $\mathbb{K} = \mathbb{C}$, these U_i are coordinate charts for $\mathbb{P}^n$ as a manifold. For any field $\mathbb{K}$, these affine sets U_i provide algebraic coordinate charts for $\mathbb{P}^n$, called affine charts.

These affine charts have a coordinate-free description. Let $\Lambda\colon \mathbb{K}^{n+1} \to \mathbb{K}$ be a linear map, and let $H \subset \mathbb{K}^{n+1}$ be the set $\{x \in \mathbb{K}^{n+1} \mid \Lambda(x) = 1\}$. Then $H \simeq \mathbb{K}^n$, and the map

$$H \ni x \;\longmapsto\; [x] \in \mathbb{P}^n$$

identifies H with the complement $U_\Lambda := \mathbb{P}^n - \mathbb{P}(\mathcal{V}(\Lambda))$ of the hyperplane defined by Λ.

Example 1.4.6. This second and more general description of affine charts leads to an application of algebraic geometry to statistics. Here $\mathbb{K} = \mathbb{R}$, the real numbers and we set $\Lambda(x) := x_0 + \cdots + x_n$. If we consider those points x with $\Lambda(x) = 1$ which have nonnegative coordinates, we obtain the *probability simplex*

$$\triangle^n \ := \ \{(p_0, p_1, \ldots, p_n) \in \mathbb{R}^{n+1}_+ \mid p_0 + p_1 + \cdots + p_n = 1\}\,,$$

where $\mathbb{R}^{n+1}_+$ is the *nonnegative orthant*, the points of $\mathbb{R}^{n+1}$ with nonnegative coordinates. Here p_i represents the probability that event i occurs, and the condition $p_0 + \cdots + p_n = 1$ reflects that every event does occur. Figure 1.4.4 shows this when $n = 2$. $\diamond$

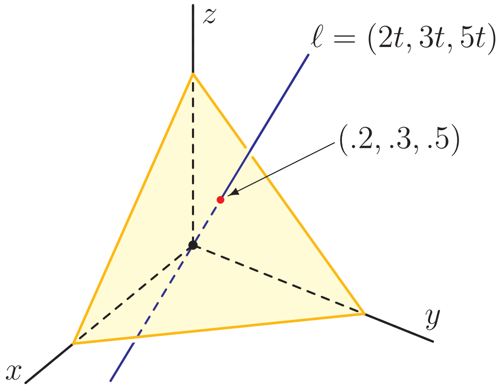


Figure 1.4.4. Probability simplex when $n = 2$.

We wish to extend the definitions and structures of affine algebraic varieties to projective space. One problem arises immediately: given a polynomial $f \in \mathbb{K}[x_0, \ldots, x_n]$ and a point $a \in \mathbb{P}^n$, we cannot in general define $f(a) \in \mathbb{K}$. To see why this is the case, for each natural number d, let f_d be the sum of the terms of f of degree d. We call f_d the dth *homogeneous component* of f. If $[a_0, \ldots, a_n]$ and $[\lambda a_0, \ldots, \lambda a_n]$ $(\lambda \neq 0)$ are two representatives of a point $a \in \mathbb{P}^n$, and f has degree m, then

$$f(\lambda a_0, \ldots, \lambda a_n) \ = \ f_0(a_0, \ldots, a_n) + \lambda f_1(a_0, \ldots, a_n) + \cdots + \lambda^m f_m(a_0, \ldots, a_n)\,, \tag{1.4.2}$$

since we can factor λ^d from every monomial $(\lambda x)^\alpha$ of degree d. Thus $f(a)$ is a well-defined number only if the polynomial (1.4.2) in λ is constant. That is, if and only if

$$f_i(a_0, \ldots, a_n) \ = \ 0 \quad \text{for} \quad i = 1, \ldots, \deg(f)\,.$$

In particular, observe that a polynomial f vanishes at a point $a \in \mathbb{P}^n$ if and only if every homogeneous component f_d of f vanishes at a. A polynomial f is *homogeneous* of degree d when $f = f_d$. We also use the term *form* for a homogeneous polynomial.

Definition 1.4.7. Let $f_1, \ldots, f_m \in \mathbb{K}[x_0, \ldots, x_n]$ be forms. These define a *projective variety*

$$\mathcal{V}(f_1, \ldots, f_m) \ := \ \{a \in \mathbb{P}^n \mid f_i(a) = 0,\ i = 1, \ldots, m\}\,. \qquad \diamond$$

An ideal $I \subset \mathbb{K}[x_0,\ldots,x_n]$ is *homogeneous* if whenever $f \in I$ then all homogeneous components of f lie in I. Thus projective varieties are defined by homogeneous ideals. Given a subset $Z \subset \mathbb{P}^n$ of projective space, its ideal is the collection of polynomials which vanish on Z,

$$\mathcal{I}(Z) \ := \ \{f \in \mathbb{K}[x_0,x_1,\ldots,x_n] \mid f(z) = 0 \text{ for all } z \in Z\}\,.$$

In Exercise 3, you are asked to show that $\mathcal{I}(Z)$ is a homogeneous ideal.

It is often convenient to work in an affine space when treating projective varieties. The *(affine) cone CZ* $\subset \mathbb{K}^{n+1}$ over a subset Z of projective space $\mathbb{P}^n$ is the union of the one-dimensional linear subspaces $\ell \subset \mathbb{K}^{n+1}$ corresponding to points of Z. The ideal $\mathcal{I}(X)$ of a projective variety X is equal to the ideal $\mathcal{I}(CX)$ of the affine cone over X.

Example 1.4.8. Let $\Lambda := a_0x_0 + a_1x_1 + \cdots + a_nx_n$ be a linear form. Then $\mathcal{V}(\Lambda)$ is a *hyperplane*. Let $V \subset \mathbb{K}^{n+1}$ be the kernel of Λ which is an n-dimensional linear subspace. It is also the affine variety defined by Λ. We have $\mathcal{V}(\Lambda) = \mathbb{P}(V) \subset \mathbb{P}^n$. ◇

Example 1.4.9. Let $[x,y,z]$ be homogeneous coordinates for the projective plane $\mathbb{P}^2$, and consider the two subvarieties $\mathcal{V}(yz - x^2)$ and $\mathcal{V}(x + ay)$. In the affine patch U_z where $z \neq 0$, these subvarieties are the parabola and the line $x = -ay$ of Example 1.4.1. Their intersection, $\mathcal{V}(x + ay, yz - x^2)$, consists of the points $[0,0,1]$ and $[-a,1,a^2]$. We see that as $a \to 0$, the second point approaches $[0,1,0]$, and does not "disappear off to infinity" as in Example 1.4.1(iii). ◇

The weak Nullstellensatz does not hold for projective space, as $\mathcal{V}(x_0,x_1,\ldots,x_n) = \emptyset$. We call this ideal, $\mathfrak{m}_0 := \langle x_0,x_1,\ldots,x_n\rangle$, the *irrelevant ideal*. Observe that every proper homogeneous ideal is a subset of $\mathfrak{m}_0$.

Lemma 1.4.10. *Suppose that $\mathbb{K}$ is algebraically closed and let $I \subsetneq \mathbb{K}[x_0,x_1,\ldots,x_n]$ be a proper homogeneous ideal. Then $\mathcal{V}(I) = \emptyset$ if and only if there is some $d \geq 0$ such that $I \supset \mathfrak{m}_0^d$.*

Proof. Note that $\mathcal{V}(I) = \emptyset$ in projective space if and only if, in the affine cone $\mathbb{K}^{n+1}$ over projective space, we have either $\mathcal{V}(I) = \emptyset$ or $\mathcal{V}(I) = \{0\}$. The first, $\mathcal{V}(I) = \emptyset$, is equivalent to $I = \mathbb{K}[x_0,\ldots,x_n]$, while the second, $\mathcal{V}(I) = \{0\}$. is equivalent to $\sqrt{I} = \mathfrak{m}_0$. This second is in turn equivalent to $I \supset \mathfrak{m}_0^d$ for some $d \geq 0$. □

The irrelevant ideal plays a special role in the projective algebra-geometry dictionary.

Theorem 1.4.11 (Projective Algebra-Geometry Dictionary). *Over any field $\mathbb{K}$, the maps $\mathcal{V}$ and $\mathcal{I}$ give an inclusion reversing correspondence*

$$\left\{\begin{matrix}\textit{Radical homogeneous ideals } I \textit{ of}\\ \mathbb{K}[x_0,\ldots,x_n] \textit{ properly contained in } \mathfrak{m}_0\end{matrix}\right\} \quad \underset{\mathcal{I}}{\overset{\mathcal{V}}{\rightleftarrows}} \quad \{\textit{Subvarieties } X \textit{ of } \mathbb{P}^n\}$$

with $\mathcal{V}(\mathcal{I}(X)) = X$. When $\mathbb{K}$ is algebraically closed, the maps $\mathcal{V}$ and $\mathcal{I}$ are inverses, and this correspondence is a bijection.

You are asked to show this in Exercise 5, deducing it from the affine version (Corollary 1.2.11).

If we relax the condition that an ideal is radical, then the corresponding geometric objects are *projective schemes*. This comes at a price, for many homogeneous ideals will define the same projective scheme (and even the same projective variety), which is not the case for their affine cousins. This non-uniqueness comes from the irrelevant ideal, $\mathfrak{m}_0$. Let us recall the construction of colon ideals from commutative algebra. Let I be an ideal and g be a polynomial. Then the colon ideal $(I : g)$ is $\{f \in \mathbb{K}[x_0,\dots,x_n] \mid fg \in I\}$. Observe that $I \subset (I : g)$. The *saturation* of I by g is

$$(I : g^\infty) \ := \ \{f \in \mathbb{K}[x_0,\dots,x_n] \mid g^m f \in I \text{ for some } m > 0\}\,.$$

If J is an ideal, then the *colon ideal* (or *ideal quotient* of I by J) is

$$(I : J) \ := \ \{f \in \mathbb{K}[x_0,\dots,x_n] \mid fJ \subset I\} \ = \ \bigcap\{(I\colon g) \mid g \in J\}\,.$$

The *saturation* of I by J is

$$(I : J^\infty) \ := \ \bigcup_{m\geq 0}(I : J^m)\ .$$

One reason for these definitions are the following results for affine varieties.

Lemma 1.4.12. *Suppose that $\mathbb{K}$ is algebraically closed. Let I be an ideal and $g \in \mathbb{K}[x_1,\dots,x_n]$ a polynomial. Then $\mathcal{V}(I : g^\infty)$ is the smallest affine variety containing $\mathcal{V}(I) \smallsetminus \mathcal{V}(g)$.*

Proof. First note that as $I \subset (I : g^\infty)$, we have $\mathcal{V}(I : g^\infty) \subset \mathcal{V}(I)$. Let $x \in \mathcal{V}(I) \smallsetminus \mathcal{V}(g)$. If $f \in (I : g^\infty)$, then there is some $m \in \mathbb{N}$ with $fg^m \in I$, so that $fg^m(x) = 0$. Since $x \notin \mathcal{V}(g)$, we conclude that $f(x) = 0$ as $g(x) \neq 0$. This establishes the inclusion $\mathcal{V}(I) \smallsetminus \mathcal{V}(g) \subset \mathcal{V}(I : g^\infty)$.

For the other inclusion, let $x \in \mathcal{V}(I : g^\infty)$. If $g(x) \neq 0$, then $x \in \mathcal{V}(I) \smallsetminus \mathcal{V}(g)$. Suppose now that $g(x) = 0$. Let $f \in \mathcal{I}(\mathcal{V}(I) \smallsetminus \mathcal{V}(g))$. Note that fg vanishes on $\mathcal{V}(I)$. By the Nullstellensatz, there is some m such that $f^m g^m \in I$, and so $f^m \in (I : g^\infty)$. But then $f^m(x) = 0$ and so $f(x) = 0$. Thus $x \in \mathcal{V}(\mathcal{I}(\mathcal{V}(I) \smallsetminus \mathcal{V}(g)))$, which completes the proof. □

Corollary 1.4.13. *Let I and J be ideals in $\mathbb{K}[x_1,\dots,x_n]$. Then $\mathcal{V}(I : J^\infty)$ is the smallest variety containing $\mathcal{V}(I) \smallsetminus \mathcal{V}(J)$.*

A homogeneous ideal $I \subset \mathbb{K}[x_0,x_1,\dots,x_n]$ is *saturated* if

$$I \ = \ (I : \mathfrak{m}_0) \ = \ \{f \mid x_i f \in I \text{ for } i = 0,1,\dots,n\}\,.$$

Applying Corollary 1.4.13 to affine cones gives the following result.

Theorem 1.4.14. *For any homogeneous ideal $I \subset \mathbb{K}[x_0,x_1,\dots,x_n]$, $\mathcal{V}(I) = \mathcal{V}(I : \mathfrak{m}_0)$ in $\mathbb{P}^n$.*

Given a projective variety $X = \mathcal{V}(I) \subset \mathbb{P}^n$, consider its intersection with an affine chart $U_i = \{x \in \mathbb{P}^n \mid x_i \neq 0\}$. For simplicity of notation, suppose that $i = 0$. Then

$$X \cap U_0 \ = \ \{x \in U_0 \mid f(x) = 0 \text{ for all } f \in I\}\,.$$

If we identify U_0 with $\mathbb{K}^n$ by $U_0 = \{[1,x_1,\dots,x_n] \mid (x_1,\dots,x_n) \in \mathbb{K}^n\}$, this is

$$X \cap U_0 \ = \ \{x \in \mathbb{K}^n \mid f(1,x_1,\dots,x_n) = 0 \text{ for all } f \in I\}\,. \tag{1.4.3}$$

We call the polynomial $f(1, x_1, \ldots, x_n)$ the *dehomogenization* of the homogeneous polynomial f with respect to x_0. The calculation (1.4.3) shows that $X \cap U_0$ is the affine variety defined by the ideal generated by the dehomogenizations of forms in I.

This proves the forward implication of the following characterization of projective varieties in terms of their intersections with these affine charts.

Lemma 1.4.15. *A subset $X \subset \mathbb{P}^n$ is a projective variety if and only if $X \cap U_i$ is an affine variety, for each $i = 0, \ldots, n$.*

Proof. We proved on implication. For the other, suppose that $X \subset \mathbb{P}^n$ is a subset such that $X \cap U_i$ is an affine variety for each $i = 0, \ldots, n$. For each i, let $H_i = \mathcal{V}(x_i)$ be the hyperplane that is the complement of U_i. Then $X \subset (X \cap U_i) \cup H_i = X \cup H_i$. We claim that $X \cup H_i$ is a projective variety. This will imply the lemma, as

$$\bigcap_{i=0}^{n} \bigl(X \cup H_i\bigr) \ = \ X \cup \bigcap_{i=0}^{n} H_i \ = \ X\,,$$

as $H_0 \cap H_1 \cap \cdots \cap H_n = \mathcal{V}(x_0, \ldots, x_n) = \emptyset$ in $\mathbb{P}^n$.

To prove the claim, let $i = 0$ for simplicity and identify U_0 with $\mathbb{K}^n$ whose coordinate ring is $\mathbb{K}[x_1, \ldots, x_n]$. For a polynomial $g \in \mathbb{K}[x_1, \ldots, x_n]$ of degree d, we have the homogeneous form g_+ of degree $d+1$ defined by

$$g_+(x_0, x_1, \ldots, x_n) \ := \ x_0^{d+1} g\bigl(\tfrac{x_1}{x_0}, \ldots, \tfrac{x_n}{x_0}\bigr)\,.$$

Let I_+ be the homogeneous ideal generated by $\{g_+ \mid g \in \mathcal{I}(X \cap U_0)\}$. Since x_0 divides g_+, we have that $H_0 \subset \mathcal{V}(I_+)$. Since the dehomogenization of g_+ is g, the dehomogenization of I_+ is $\mathcal{I}(X \cap U_0)$. Then our previous calculations show that $X \cap U_0 = \mathcal{V}(I_+) \cap U_0$, and thus $\mathcal{V}(I_+) = X \cup H_0$. This completes the proof. □

Corollary 1.4.16. *Let $X \subset \mathbb{P}^n$ be a projective variety and Λ a linear form. Then $X_\Lambda := X \smallsetminus \mathcal{V}(\Lambda)$ is an affine variety. Regular functions on X_Λ have the form f/Λ^d, where $f \in \mathbb{K}[x_0, \ldots, x_n]$ is a form of degree d.*

Proof. Applying a linear change of coordinates as in Example 1.3.8, it suffices to prove this for $\Lambda = x_0$, in which case X_Λ becomes $X_0 = X \cap U_0$, which is affine. A regular function on X_0 is the restriction of a regular function on U_0. Such a function is the dehomogenization $f(1, x_1, \ldots, x_n)$ of a form $f \in \mathbb{K}[x_0, \ldots, x_n]$. Let d be the degree of f. Then, as a function on U_0,

$$f(1, x_1, \ldots, x_n) \ = \ f\Bigl(\tfrac{x_0}{x_0}, \tfrac{x_1}{x_0}, \ldots, \tfrac{x_n}{x_0}\Bigr) \ = \ \tfrac{1}{x_0^d} f(x_0, x_1, \ldots, x_n)\,,$$

which completes the proof. □

By Lemma 1.4.15, every projective variety X is naturally a union of affine varieties

$$X \ = \ \bigcup_{i=0}^{n} \bigl(X \cap U_i\bigr)\,.$$

In fact, we may replace $U_0, \ldots, U_n$ by any collection $\{U_\Lambda \mid \Lambda \in A\}$ of linear forms such that $\mathcal{V}(\Lambda \mid \Lambda \in A) = \emptyset$. Consequently, we may often prove results for projective varieties by arguing locally on each affine set that covers it. It also illustrates a relationship between varieties and manifolds: Affine varieties are to varieties as open subsets of $\mathbb{R}^n$ are to manifolds.

We give another result relating an affine variety in U_0 to the smallest projective variety containing it. For a polynomial $f \in \mathbb{K}[x_1, \dots, x_n]$, let f_{top} be the sum of its terms of degree $\deg(f)$, its top degree homogeneous component, and let f_{hom} be its homogenization,

$$f_{\text{hom}} \ := \ x_0^{\deg(f)} f\left(\tfrac{x_1}{x_0}, \dots, \tfrac{x_n}{x_0}\right).$$

Lemma 1.4.17. *Let $X \subset \mathbb{K}^n$ be an affine variety with ideal $\mathcal{I}(X)$. Identify $\mathbb{K}^n$ with $U_0 \subset \mathbb{P}^n$ and let $Y \subset \mathbb{P}^n$ be the smallest projective variety containing X. Then*

$$\mathcal{I}(Y) \ = \ \langle f_{\text{hom}} \mid f \in \mathcal{I}(X) \rangle \ =: \ \mathcal{I}(X)_{\text{hom}}\,. \tag{1.4.4}$$

If $\mathbb{P}^{n-1} = \mathcal{V}(x_0)$ is the hyperplane at infinity, then

$$\mathcal{I}(Y \cap \mathbb{P}^{n-1}) \ = \ \langle x_0\,,\ f_{\text{top}} \mid f \in \mathcal{I}(X) \rangle\,. \tag{1.4.5}$$

In particular, if $X \neq \mathbb{K}^n$, then $Y \cap \mathbb{P}^{n-1} \neq \mathbb{P}^{n-1}$.

Proof. In the affine cone $\mathbb{K}^{n+1}$ over $\mathbb{P}^n$, the homogeneous ideal $\mathcal{I}(X)_{\text{hom}}$ is the ideal of polynomials vanishing on the cone CX over X, which proves (1.4.4). For (1.4.5), note that x_0 divides $f_{\text{hom}} - f_{\text{top}}$. □

Just as with affine varieties, projective varieties have coordinate rings. Let $X \subset \mathbb{P}^n$ be a projective variety. Its *homogeneous coordinate ring* $\mathbb{K}[X]$ is the quotient

$$\mathbb{K}[X] \ := \ \mathbb{K}[x_0, x_1, \dots, x_n]/\mathcal{I}(X)\,.$$

If we set $\mathbb{K}[X]_d$ to be the image of all degree d homogeneous polynomials, $\mathbb{K}[x_0, \dots, x_n]_d$, then this ring is graded,

$$\mathbb{K}[X] \ = \ \bigoplus_{d \geq 0} \mathbb{K}[X]_d\,,$$

where if $f \in \mathbb{K}[X]_d$ and $g \in \mathbb{K}[X]_e$, then $fg \in \mathbb{K}[X]_{d+e}$. More concretely, we have

$$\mathbb{K}[X]_d \ = \ \mathbb{K}[x_0, \dots, x_n]_d/\mathcal{I}(X)_d\,,$$

where $\mathcal{I}(X)_d = \mathcal{I}(X) \cap \mathbb{K}[x_0, \dots, x_n]_d$.

This differs from the coordinate ring of an affine variety in that its elements are not functions on X. Indeed, we already observed that, apart from constant polynomials, elements of $\mathbb{K}[x_0, \dots, x_n]$ do not give functions on any subset of $\mathbb{P}^n$. Despite this, they will be used to define maps of projective varieties, and the homogeneous coordinate ring plays another role which will be developed in Section **??**, based on the following definition.

Definition 1.4.18. Let $X \subset \mathbb{P}^n$ be a projective variety. Its *Hilbert function* is the function whose value at $d \in \mathbb{N}$ is the dimension of the d-th graded component of $\mathbb{K}[X]$,

$$\text{HF}_X(d) \ := \ \dim_{\mathbb{K}}(\mathbb{K}[X]_d)\,.$$

This is also the number of linearly independent degree d homogeneous polynomials on X.

Let Λ be a linear form on $\mathbb{P}^n$ and $X \subset \mathbb{P}^n$ a subvariety. A consequence of Corollary 1.4.16 is that elements of the coordinate ring $\mathbb{K}[X_\Lambda]$ of the affine variety X_Λ have the form $f/\Lambda^{\deg(f)}$ for f a homogeneous element of $\mathbb{K}[X]$. The ring $\mathbb{K}[X][\frac{1}{\Lambda}]$ is graded by $\deg(g/\Lambda^d) = \deg(g) - d$. This gives another description of $\mathbb{K}[X_\Lambda]$.

Corollary 1.4.19. *The coordinate ring of the affine variety X_Λ is the degree 0 homogeneous component of the graded ring $\mathbb{K}[X][\frac{1}{\Lambda}]$.*

Exercises for Section 1.4.

1. Verify the claim in Example 1.4.4 that if a, b lie on the unit sphere S^{2n+1} in $\mathbb{C}^{n+1}$ and define the same point in $\mathbb{P}^n$, then $a = \zeta b$ for some unit complex number ζ.
2. A *transition function* $\varphi_{i,j}$ expresses how to change from the local coordinates from U_i of a point $p \in U_i \cap U_j$ to the local coordinates from U_j. Write down the transition functions for $\mathbb{P}^n$ provided by the affine charts $U_0, \dots, U_n$.
3. Let $Z \subset \mathbb{P}^n$. Show that $\mathcal{I}(Z)$ is a homogeneous ideal.
4. Show that an ideal I is homogeneous if and only if it is generated by homogeneous polynomials.
5. Give a proof of Theorem 1.4.11 by replacing a projective variety by its affine cone and using the affine version, Corollary 1.2.11.
6. Show that the homogeneous ideal $\mathcal{I}(Z)$ of a subset $Z \subset \mathbb{P}^n$ is equal to the ideal $\mathcal{I}(CZ)$ of the affine cone over Z.
7. Let if $I \subset \mathbb{K}[x_1, \dots, x_n]$ be an ideal and $g \in \mathbb{K}[x_1, \dots, x_n]$ is a polynomial. Prove that $(I : g)$ is an ideal. Prove that we have an ascending chain of ideals
$$(I : g) \ \subset\ (I : g^2) \ \subset\ (I : g^3) \ \subset \cdots ,$$
and that there exists a nonnegative integer N such that $(I : g^\infty) = (I : g^N)$. Show that $(I : g^\infty) = (I : g^m)$ if and only if $(I : g^m) = (I : g^{m+1})$.

   Deduce that if $J \subset \mathbb{K}[x_1, \dots, x_n]$ is an ideal, then $(I\colon J)$ is an ideal, and that the saturation $(I\colon J^\infty)$ is an ideal.
8. Give a proof of Corollary 1.4.13.
9. Show that a radical homogeneous ideal is saturated.
10. Show that if $X \subset \mathbb{P}^n$ is a projective variety, then the smallest projective variety containing its intersection with the principal affine set U_{x_0} has ideal the saturation $(\mathcal{I}(X)\colon x_0^\infty)$.
11. Show that if I is a homogeneous ideal and $J = (I : \mathfrak{m}_0^\infty)$ is its saturation with respect to the irrelevant ideal $\mathfrak{m}_0$, then there is some integer N such that
$$J_d \ = \ I_d \qquad \text{for} \quad d \geq N\,.$$
12. Verify the claim in the text that if $X \subset \mathbb{P}^n$ is a projective variety, then its homogeneous coordinate ring is graded with
$$\mathbb{K}[X]_d \ = \ \mathbb{K}[x_0, \dots, x_n]_d / \mathcal{I}(X)_d\,.$$

1.5. Maps of projective varieties

Many properties of a projective variety X are inherited from the affine cone CX over X, but with some changes. The same is true for maps from X to a projective space.

Elements of its homogeneous coordinate ring give maps, but care must be taken for the maps to be well-defined. We explain this and describe some important maps of projective varieties. This leads to the product of projective varieties, and one of the most important properties of projective varieties; that the image of a projective variety under a map is a subvariety. We conclude by extending the notion of finite maps to projective varieties.

Suppose that $X \subset \mathbb{P}^n$ is a projective variety. Let $f_0, \dots, f_m \in \mathbb{K}[X]$ be elements of its homogeneous coordinate ring. Under what circumstances does

$$X \ \ni \ x \ \longmapsto \ [f_0(x), f_1(x), \dots, f_m(x)] \ \in \ \mathbb{P}^m$$

define a map $X \to \mathbb{P}^m$? (It always defines a map on affine cones $CX \to \mathbb{K}^{m+1}$.) The evaluation $f_i(x)$ of a form f_i at $x \in \mathbb{P}^n$ is already a problem as the value of $f_i(x)$ is ambiguous. When f is a form of degree d we saw that $f(\lambda x) = \lambda^d f(x)$ for $\lambda \in \mathbb{K}$. Thus when forms $f_0, \dots, f_m$ all have the same degree d, their values at $x \in \mathbb{P}^n$ share the same ambiguity. In fact, as long as $x \notin \mathcal{V}(f_0, \dots, f_m)$, then

$$\varphi(x) \ := \ [f_0(x), f_1(x), \dots, f_m(x)] \tag{1.5.1}$$

is a well-defined element of $\mathbb{P}^m$. Indeed, for $\lambda \in \mathbb{K}$, $\varphi(\lambda x) = \lambda^d \varphi(x)$ in $\mathbb{K}^{m+1}$, so that $\varphi(\lambda x) = \varphi(x)$ in $\mathbb{P}^m$ for $\lambda \neq 0$. For forms $f_0, \dots, f_m \in \mathbb{K}[x_0, \dots, x_n]$, if $\mathcal{V}(f_0, \dots, f_m) = \emptyset$, so that the f_i have no common zeroes on X, then (1.5.1) defines a *regular map* $\varphi \colon X \to \mathbb{P}^m$.

EXAMPLE 1.5.1. Let $[s, t]$ be homogeneous coordinates for $\mathbb{P}^1$. Then s^2, st, t^2 are forms of the same degree 2 with $\mathcal{V}(s^2, st, t^2) = \emptyset$. These define a regular map $\varphi \colon \mathbb{P}^1 \to \mathbb{P}^2$ where

$$\varphi \ : \ \mathbb{P}^1 \ \ni \ [s, t] \ \longmapsto \ [s^2, st, t^2] \ \in \ \mathbb{P}^2\,.$$

If $[x, y, z]$ are coordinates for $\mathbb{P}^2$, then the image of φ is $\mathcal{V}(xz - y^2)$. Indeed, the image is a subset of $\mathcal{V}(xz - y^2)$ as $(s^2)(t^2) - (st)^2 = 0$. Let $[x, y, z] \in \mathcal{V}(xz - y^2)$. If $x = 0$, then $y = 0$ and $[0, 0, z] = [0, 0, 1] = \varphi([0, 1])$. If $x \neq 0$, then $z = y^2/x$, and we have

$$[x, y, z] \ = \ [1, y/x, z/x] \ = \ [1, y/x, y^2/x^2] \ = \ \varphi([1, y/x]) \ = \ \varphi([x, y])\,. \tag{1.5.2}$$

Thus $\mathcal{V}(xz - y^2)$ is the image of φ. This is the parabola of Examples 1.4.1 and 1.4.9. ⋄

The map φ of Example 1.5.1 is injective, and we would like to have that $\mathbb{P}^1$ is isomorphic to its image, C. For that, we need a map $C \to \mathbb{P}^1$ that is inverse to φ. To do this, we first extend and refine our notion of regular map of projective varieties. Let X be a projective variety and suppose that $f_0, \dots, f_m \in \mathbb{K}[X]$ are forms of the same degree with $\mathcal{V}(f_0, \dots, f_m) = \emptyset$ which define a regular map $\varphi \colon X \to \mathbb{P}^m$ as in (1.5.1). A second list $g_0, \dots, g_m \in \mathbb{K}[X]$ of elements of the same degree (possible different from the degree of the f_i) with $\mathcal{V}(g_0, \dots, g_m) = \emptyset$ defines the same regular map if we have

$$\operatorname{rank}\begin{pmatrix} f_0 & f_1 & \dots & f_m \\ g_0 & g_1 & \dots & g_m \end{pmatrix} \ = \ 1\,, \quad \text{i.e., if} \ \ f_i g_j - f_j g_i \ \in \ \mathcal{I}(X) \ \ \text{for } i \neq j\,. \tag{1.5.3}$$

Indeed, the conditions $\mathcal{V}(f_0, \dots, f_m) = \mathcal{V}(g_0, \dots, g_m) = \emptyset$ and (1.5.3) imply that for any $x \in X$, $[f_0(x), \dots, f_m(x)] = [g_0(x), \dots, g_m(x)]$ in $\mathbb{P}^m$. Thus the vectors $(f_0(x), \dots, f_m(x))$ and $(g_0(x), \dots, g_m(x))$ are parallel for every $x \in X$, which implies that all 2×2 minors of the matrix of functions in (1.5.3) vanish on X, and thus lie in the ideal of X.

More interesting is when $f_0,\dots,f_m,g_0,\dots,g_m$ satisfy (1.5.3), but we do not have that $\mathcal{V}(f_0,\dots,f_m)=\mathcal{V}(g_0,\dots,g_m)=\emptyset$. In Example 1.5.1, (1.5.2) shows that if $[x,y,z]\in C=\mathcal{V}(xz-y^2)$, then $[x,y,z]=\varphi([x,y])$, but this requires that $(x,y)\neq(0,0)$. Similarly, if $(y,z)\neq(0,0)$, then $[x,y,z]=\varphi([y,z])$. We may understand this in terms of (1.5.3), at least when $xyz\neq 0$ as $\det\left(\begin{smallmatrix}x&y\\y&z\end{smallmatrix}\right)=xz-y^2$, which vanishes on C. On C, $\mathcal{V}(x)=[0,0,1]$, $\mathcal{V}(z)=[1,0,0]$, and $\mathcal{V}(y)=\{[1,0,0],[0,0,1]\}$, so that at every point of C, at least one of (x,y) or (y,z) can be used to define a map to $\mathbb{P}^1$ which is the inverse of φ.

Definition 1.5.2. A map $\varphi\colon X\to\mathbb{P}^m$ from a projective variety X is a *regular map* if for every $x\in X$, there are elements $f_0,\dots,f_m\in\mathbb{K}[X]$ of the same degree with $x\notin\mathcal{V}(f_0,\dots,f_m)$ such that for every $y\in X\smallsetminus\mathcal{V}(f_0,\dots,f_m)$,

$$\varphi(y)\ =\ [f_0(y),f_1(y),\dots,f_m(y)]\,.$$

That is, φ has the form (1.5.1), but the elements $f_0,\dots,f_m$ may change for different points of X (but any two choices satisfy (1.5.3), where both are defined). ◇

The simplest regular map is an invertible linear change of coordinates. Let $A\in GL_{n+1}\mathbb{K}$ be an invertible $(n{+}1)\times(n{+}1)$-matrix. This gives a linear map $A\colon\mathbb{K}^{n+1}\to\mathbb{K}^{n+1}$, which maps lines through the origin to lines, and thus induces a map $A\colon\mathbb{P}^n\to\mathbb{P}^n$. To understand it in coordinates, write $\Lambda_0(x),\dots,\Lambda_n(x)$ for the entries of the column vector $A(x_0,\dots,x_n)^T$. These are linear forms, and the map A is given by $[\Lambda_0(x),\dots,\Lambda_n(x)]$. Composition of these maps corresponds to matrix multiplication, and the inverse of the map given by A is given by the inverse of A. Since multiplying A by a nonzero scalar from $\mathbb{K}$ does not change the map on $\mathbb{P}^n$, we see that the quotient $PGL_{n+1}\mathbb{K}:=GL_{n+1}\mathbb{K}/\mathbb{K}^\times I_{n+1}$ acts on $\mathbb{P}^n$. Here, $\mathbb{K}^\times I_{n+1}$ is the central subgroup of invertible scalar matrices. This is the *projective general linear group*, and it is the group of automorphisms of projective space $\mathbb{P}^n$ over the field $\mathbb{K}$.

Perhaps the next simplest type of regular map of projective varieties are linear projections. Let $X\subset\mathbb{P}^n$ be a projective variety and suppose that $L\subset\mathbb{P}^n$ is a linear subspace disjoint from X. Let $\Lambda_0,\dots,\Lambda_m$ be linearly independent forms that vanish on L. Then $L=\mathcal{V}(\Lambda_0,\dots,\Lambda_m)$ and L has dimension $n-m-1$. We also have $X\cap\mathcal{V}(\Lambda_0,\dots,\Lambda_m)=\emptyset$, so that $(\Lambda_0,\dots,\Lambda_m)$ define a regular map $\pi_L\colon X\to\mathbb{P}^m$, which is called a *linear projection* with center L. If $M\simeq\mathbb{P}^m$ is a linear space disjoint from L, then $\pi_L\colon M\to\mathbb{P}^m$ is an isomorphism from M to $\mathbb{P}^m$, and we may identify the image of the linear projection π_L with M. For $p\in M$, observe that the set $\pi_L^{-1}(p)$ of preimages of p in X is the set of points in the intersection $X\cap\langle L,p\rangle$ of X with the linear span of L and p.

Projective varieties $X\subset\mathbb{P}^n$ and $Y\subset\mathbb{P}^m$ are *isomorphic* if we have regular maps $\varphi\colon X\to Y$ and $\psi\colon Y\to X$ for which the compositions $\psi\circ\varphi$ and $\varphi\circ\psi$ are the identity maps on X and Y, respectively.

The map φ of Example 1.5.1 is an isomorphism between $\mathbb{P}^1$ and its image C. We generalize this. The set $V_{n,d}$ of all $\binom{n+d}{n}$ monomials in $x_0,\dots,x_n$ of degree d is a basis for the degree d component of the irrelevant ideal, and thus generates $\mathfrak{m}_0^d$. By Lemma 1.4.10, $\mathcal{V}(V_{n,d})=\emptyset$, and thus this list of monomials gives a regular map,

$$\nu_{n,d}\ :\ \mathbb{P}^n\ \longrightarrow\ \mathbb{P}^{\binom{n+d}{n}-1}\,,$$

called the *dth Veronese map*. The map φ of Example 1.5.1 is $\nu_{1,2}$. Let us study the image of $\nu_{n,d}$. We adopt a useful convention from Section **??** and label the coordinates of $\mathbb{P}^{\binom{n+d}{n}-1}$ by the exponents of monomials in $V_{n,d}$,

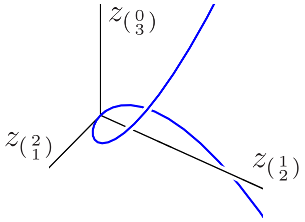
$$\mathcal{A}_{n,d} \ := \ \{(a_0,\dots,a_n) \mid a_i \in \mathbb{N} \text{ and } a_0+\dots+a_n=d\}\,.$$

Then $V_{n,d}=\{x^\alpha \mid \alpha\in\mathcal{A}_{n,d}\}$ and $[z_\alpha \mid \alpha\in\mathcal{A}_{n,d}]$ are homogeneous coordinates for $\mathbb{P}^{\binom{n+d}{n}-1}$, with the z_αth coordinate of the Veronese map $\nu_{n,d}$ equal to x^α.

Observe that if $\alpha,\beta,\gamma,\delta\in\mathcal{A}_{n,d}$ satisfy $\alpha+\beta=\gamma+\delta$ (as integer vectors), then $z_\alpha z_\beta - z_\gamma z_\delta$ vanishes on the image $\nu_d(\mathbb{P}^n)$ as $\nu_d^*(z_\alpha z_\beta - z_\gamma z_\delta) = x^\alpha x^\beta - x^\gamma x^\delta = 0$. This is the equation $xz-y^2=0$ that we found for $\nu_{1,2}$ in Example 1.5.1. When $n=1$ and $d=3$, we have $\mathcal{A}_{1,3}=\{\binom{3}{0},\binom{2}{1},\binom{1}{2},\binom{0}{3}\}$, $\nu_{1,3}([s,t])=[s^3,s^2t,st^2,t^3]$, and the quadratic polynomials that vanish on the image include

$$z_{\binom{3}{0}}z_{\binom{1}{2}} - z_{\binom{2}{1}}^2\,,\ \ z_{\binom{3}{0}}z_{\binom{0}{3}} - z_{\binom{2}{1}}z_{\binom{1}{2}}\,,\ \ \text{and}\ \ z_{\binom{2}{1}} - z_{\binom{0}{3}}z_{\binom{1}{2}}^2\,.$$

The image $\nu_{1,3}(\mathbb{P}^1)$ is the rational normal (or monomial) curve, depicted in $U_{\binom{3}{0}}$ below.



THEOREM 1.5.3. *The image $\nu_{n,d}(\mathbb{P}^n)\subset\mathbb{P}^{\binom{n+d}{n}-1}$ is the subvariety defined by the vanishing of the quadratic polynomials*

$$z_\alpha z_\beta \ - \ z_\gamma z_\delta \quad \textit{for} \quad \alpha,\beta,\gamma,\delta\in\mathcal{A}_{n,d} \quad \textit{with} \quad \alpha+\beta \ = \ \gamma+\delta\,, \tag{1.5.4}$$

and it is isomorphic to $\mathbb{P}^n$.

The image of $\nu_{n,d}$ is called the *Veronese variety*, and $\nu_{n,d}$ is the *Veronese embedding*.

PROOF. We observed that the quadratics (1.5.4) vanish on $\nu_{n,d}(\mathbb{P}^n)$.

Let $X\subset\mathbb{P}^{\binom{n+d}{n}-1}$ be the variety defined by the vanishing of the quadratics (1.5.4) and let $z\in X$. In Exercise 3, you will show that there is at least one $i=0,\dots,n$ such that $z_{de_i}\neq 0$. (Here, e_i is the ith standard basis vector so that de_i is the exponent of x_i^d. In Example 1.5.1 this observation is that one of $x=z_{\binom{2}{0}}$ or $z=z_{\binom{0}{2}}$ did not vanish.) Thus $z\in U_{de_i}$. Define φ_i on the affine patch $X\cap U_{de_i}$ by

$$\varphi_i(z) \ = \ [z_{e_j+(d-1)e_i} \mid j=0,\dots,n]\,.$$

(The subscript $e_j+(d-1)e_i$ is the exponent of $x_jx_i^{d-1}$.) Then $\varphi_i\colon X\cap U_{de_i}\to U_i\subset\mathbb{P}^n$ is an inverse to $\nu_{n,d}$ on U_i. To see this, let $y\in U_i$ be a representative with $y_i=1$. Then

$$\big(\nu_{n,d}(y)\big)_{de_i} \ = \ 1 \ \text{ and } \big(\nu_{n,d}(y)\big)_{e_j+(d-1)e_i} \ = \ y_j\,.$$

This shows that $X\cap U_{de_i}=\nu_{n,d}(U_i)=\nu_{n,d}(\mathbb{P}^n)\cap U_{de_i}$. Thus these maps φ_i piece together to define a regular map $\varphi\colon\nu_{n,d}(\mathbb{P}^n)\to\mathbb{P}^n$ which is inverse to $\nu_{n,d}$. This completes the proof. □

The value of the Veronese embedding is that if $f \in \mathbb{K}[x_0, x_1, \ldots, x_n]$ is any form of degree d, then there is a linear form Λ_f on $\mathbb{P}^{\binom{n+d}{n}-1}$ such that $f = \nu_{n,d}^*(\Lambda_f)$. More precisely,

$$f \;=\; \sum_{\alpha\in\mathcal{A}_{n,d}} c_\alpha x^\alpha \;=\; \nu_{n,d}^*\Bigl(\sum_{\alpha\in\mathcal{A}_{n,d}} c_\alpha z_\alpha\Bigr)\,. \tag{1.5.5}$$

Then $\nu_{n,d}(\mathcal{V}(f)) = \nu_{n,d}(\mathbb{P}^n) \cap \mathcal{V}(\Lambda_f)$. Extending this to a basis of $\mathcal{I}(X)_d$ for d large enough shows that any subvariety X of $\mathbb{P}^n$ is isomorphic to the intersection of a Veronese variety and a linear subspace, which is called a *linear section* (of the Veronese). Consequently, any projective variety is isomorphic to a variety defined by equations of degree at most two.

Remark 1.5.4. Suppose that f is a form of degree d on $\mathbb{P}^n$ with corresponding linear form Λ_f on $\mathbb{P}^{\binom{n+d}{n}-1}$. Then $U_f = \mathbb{P}^n \smallsetminus \mathcal{V}(f)$ is an affine variety as it is isomorphic to $\nu_{n,d}(\mathbb{P}^n) \cap U_{\Lambda_f}$. Consequently, for any projective variety $X \subset \mathbb{P}^n$ and any homogeneous element f of its coordinate ring, the set $X_f := X \smallsetminus \mathcal{V}(f) = X \cap U_f$ is an affine variety. The statement of Lemma 1.4.15 extends to these more general affine charts U_f of $\mathbb{P}^n$. These are principal affine open subsets of X. That is, a subset $X \subset \mathbb{P}^n$ is a variety if and only if $X_f \subset U_f$ is an affine variety for every homogeneous form f.

This is related to maps of projective varieties. Suppose that $\varphi\colon X \to \mathbb{P}^m$ is a regular map defined on part of X by $\varphi(x) = [f_0(x), \ldots, f_m(x)]$ for $f_0, \ldots, f_m$ homogeneous elements of $\mathbb{K}[X]$ of the same degree. Then φ is defined as a map of affine varieties on each affine patch X_{f_i} given by $\varphi\colon X_{f_i} \to U_i \subset \mathbb{P}^m$. ◇

The product of affine varieties required no special treatment as the product $\mathbb{K}^m \times \mathbb{K}^n$ of two affine spaces is again an affine space, $\mathbb{K}^{m+n}$. This is not the case with projective spaces. To remedy this, we identify $\mathbb{P}^m \times \mathbb{P}^n$ with a subvariety of the projective space $\mathbb{P}^{mn+m+n}$, and use this identification to help understand subvarieties of $\mathbb{P}^m \times \mathbb{P}^n$.

Let $x_0, \ldots, x_m$ and $y_0, \ldots, y_n$ be homogeneous coordinates for $\mathbb{P}^m$ and $\mathbb{P}^n$, respectively. Let $z_{i,j}$ for $i = 0, \ldots, m$ and $j = 0, \ldots, n$ be homogeneous coordinates for $\mathbb{P}^{mn+m+n}$. (Note that $(m+1)(n+1)-1 = mn+m+n$.) Define a map $\sigma_{m,n}\colon \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^{mn+m+n}$ by

$$\sigma_{m,n}(x, y) \;=\; z\,, \quad \text{where} \quad z_{i,j} = x_i y_j\,.$$

This map becomes more clear when lifted to the affine cones over these projective spaces, where it is the map $\mathbb{K}^{m+1} \times \mathbb{K}^{n+1} \to \mathrm{Mat}_{m+1,n+1}(\mathbb{K})$ that sends a pair of column vectors (x, y) to their outer product $xy^T \in \mathrm{Mat}_{m+1,n+1}(\mathbb{K})$. The image is the set of rank 1 matrices, which is defined by the vanishing of the quadratic polynomials,

$$\det\begin{pmatrix} z_{i,j} & z_{i,l} \\ z_{k,j} & z_{k,l}\end{pmatrix} \;=\; z_{i,j}z_{k,l} \;-\; z_{i,l}z_{k,j} \quad \text{for} \quad 0 \le i < k \le m \;\text{ and }\; 0 \le j < l \le n\,. \tag{1.5.6}$$

This is a special case of Exercise 10(a) in Section 1.1.

Theorem 1.5.5. *The image $\sigma_{m,n}(\mathbb{P}^m \times \mathbb{P}^n) \subset \mathbb{P}^{mn+m+n}$ is the subvariety defined by the vanishing of the quadratic polynomials* (1.5.6). *The map $\sigma_{m,n}$ admits an inverse.*

The map $\sigma_{m,n}$ is the *Segre map* and its image is the *Segre variety*. Exercise 6 explores the Segre variety $\mathbb{P}^1 \times \mathbb{P}^1 \subset \mathbb{P}^3$.

Proof. We sketch the proof, which is similar to that of Theorem 1.5.3, and leave the details as Exercise 7. For the inverse to $\sigma_{m,n}$, suppose that $X \subset \mathbb{P}^{mn+m+n}$ satisfies the equations (1.5.6). For each index k, l of a coordinate of $\mathbb{P}^{mn+m+n}$, we have an affine patch $U_{k,l} := \{z \in \mathbb{P}^{mn+m+n} \mid z_{k,l} \neq 0\}$. Define a map to $\mathbb{P}^m \times \mathbb{P}^n$ on the affine patch $X \cap U_{k,l}$ by

$$\varphi_{k,l}(z) \;=\; \big([z_{i,l} \mid i = 0, \ldots, m]\,,\, [z_{k,j} \mid j = 0, \ldots, n]\big)\,.$$

Then $\varphi_{k,l}$ is an isomorphism between the affine varieties $X \cap U_{k,l}$ and $U_k \times U_l$. □

This proof identifies each affine patch $X \cap U_{k,l}$ with the affine space $U_k \times U_l \simeq \mathbb{K}^m \times \mathbb{K}^n \subset \mathbb{P}^m \times \mathbb{P}^n$, and could be used to put the structure of an algebraic variety on the product $\mathbb{P}^m \times \mathbb{P}^n$, much as we do in differential geometry. Another approach is intrinsic: define subvarieties of $\mathbb{P}^m \times \mathbb{P}^n$ directly as we did with projective space. A third approach is extrinsic: use the Segre embedding to define subvarieties of $\mathbb{P}^m \times \mathbb{P}^n$. The first, using a covering by affine varieties to give $\mathbb{P}^m \times \mathbb{P}^n$ the structure of an algebraic variety, is the starting point for the general development of algebraic schemes that we do not pursue in this text.. We develop the second and third approaches and show they coincide. That they give the same notion of subvariety as the first follows from Lemma 1.4.15 applied to $\mathbb{P}^{mn+m+n}$ and $\sigma_{m,n}(\mathbb{P}^m \times \mathbb{P}^n)$.

This begins with a definition. A monomial $x^\alpha y^\beta$ in $\mathbb{K}[x_0, \ldots, x_n, y_0, \ldots, y_m] = \mathbb{K}[x; y]$ has *bidegree* (a, b) where $a = \deg(x^\alpha)$ and $b = \deg(y^\beta)$. For example, $x_0 x_1^3 y_0 y_2 y_3$ has bidegree $(4, 3)$. A polynomial $g(x; y) \in \mathbb{K}[x; y]$ is *bihomogeneous* of *bidegree* (a, b) if each of its monomials has bidegree (a, b). The same discussion from Section 1.4 that led us to understand the role of homogeneous ideals for projective varieties leads to bihomogeneous ideals defining subsets of $\mathbb{P}^m \times \mathbb{P}^n$.

We may also ask: what are the subsets X of $\mathbb{P}^m \times \mathbb{P}^n$ whose image $\sigma_{m,n}(X)$ is a subvariety of $\mathbb{P}^{mn+m+n}$? As $\sigma_{m,n}$ is given by bilinear monomials, the pullback $\sigma^*(f)$ of a form of degree d in z is a form of degree $2d$ that is bihomogeneous of bidegree (d, d). Consequently, a subset X of $\mathbb{P}^m \times \mathbb{P}^n$ whose image $\sigma_{m,n}(X)$ is a subvariety is defined by bihomogeneous polynomials $g(x; y)$ with *diagonal* bidegree (a, a).

To reconcile these two approaches, let $g(x; y)$ be a bihomogeneous polynomial with a non-diagonal bidegree (a, b) and suppose that $a = b + k$ with $k > 0$. Observe that

$$\mathcal{V}(g(x; y)) \;=\; \mathcal{V}(y_j^k g(x; y) \mid j = 0, \ldots, n)\,. \tag{1.5.7}$$

Replacing y by x when $a < b$ shows that any subset of $\mathbb{P}^m \times \mathbb{P}^n$ defined by bihomogeneous polynomials may also be defined by bihomogeneous polynomials with a diagonal bidegree, thus reconciling the two approaches to equipping $\mathbb{P}^m \times \mathbb{P}^n$ with the structure of an algebraic variety.

We follow the discussion leading up to Lemma 1.4.15 to define subvarieties of $\mathbb{P}^m \times \mathbb{K}^n$. If we restrict the second factor of $\mathbb{P}^m \times \mathbb{P}^n$ to $U_0 \simeq \mathbb{K}^n$ and dehomogenize bihomogeneous forms with respect to y_0, we see that subvarieties of $\mathbb{P}^m \times \mathbb{K}^n$ are given by polynomials $f(x; y) \in \mathbb{K}[x_0, \ldots, x_m, y_1, \ldots, y_n]$ that are homogeneous in x, but with no restriction on y. We have shown the following characterization of subvarieties of products.

Proposition 1.5.6. *A subvariety $X \subset \mathbb{P}^m \times \mathbb{P}^n$ is defined by a system of bihomogeneous polynomials $f_1(x;y), \ldots, f_r(x;y)$. A subvariety $X \subset \mathbb{P}^m \times \mathbb{K}^n$ is defined by a system of polynomials $g_1(x;y), \ldots, g_r(x;y)$ that are homogeneous in x.*

Let X, Y be varieties. Then $X \times Y$ is a variety, as it is defined by the set of polynomials $\mathcal{I}(X) \cup \mathcal{I}(Y) = \{f(x), g(y) \mid f \in \mathcal{I}(X), g \in \mathcal{I}(Y)\}$. When both X and Y are affine, this was discussed in Section 1.1, when both are projective this is a set of bihomogeneous polynomials, and if X is projective and Y affine, then these are homogeneous in the first set of variables. This description of subvarieties of products of two projective spaces or of a projective space and an affine space extends in a natural way to arbitrary finite products of projective spaces with affine space. Restricting to subvarieties in each factor, we also obtain that arbitrary finite products of algebraic varieties are algebraic varieties. We leave the details to your imagination.

In Example 1.4.4 we remarked that when $\mathbb{K} = \mathbb{C}$ or $\mathbb{K} = \mathbb{R}$, projective space is compact in the usual (Euclidean) topology, and consequently the projection maps $\mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^n$ and $\mathbb{P}^m \times \mathbb{K}^n \to \mathbb{K}^n$ are proper in that the image of a closed set is also closed. This remains true, whatever the field, if we replace the property of being closed by that of being a subvariety. This is a consequence of the following theorem.

Theorem 1.5.7. *Suppose that $\mathbb{K}$ is algebraically closed. The image of a subvariety $X \subset \mathbb{P}^m \times \mathbb{P}^n$ under the projection to $\mathbb{P}^n$ is again a subvariety, and the same for a subvariety of $\mathbb{P}^m \times \mathbb{K}^n$ under projection to $\mathbb{K}^n$.*

Before proving Theorem 1.5.7, we use it to show that the image of a projective variety under a map is a variety. That is, maps from projective varieties have the same property as finite maps of affine varieties. You will see in the proof of Theorem 1.5.7 that the reason is similar; points in a fiber cannot disappear.

A first step is to introduce a general construction. Let $\varphi\colon X \to Y$ be a regular map of algebraic varieties (projective or affine). The *graph* of φ is the set

$$\Gamma \ := \ \{(x,y) \in X \times Y \mid x \in X \text{ and } \varphi(x) = y\}\,.$$

Let π_X and π_Y be the maps that project Γ to the first and second factors of $X \times Y$, respectively, and $\iota\colon x \mapsto (x, f(x)) \in X \times Y$ the natural map from X to Γ. You are asked to prove the following in Exercise 10.

Lemma 1.5.8. *The graph Γ of φ is a subvariety of $X \times Y$. The projection π_1 to X is an isomorphism and φ is the composition $\pi_2 \circ \iota$.*

Corollary 1.5.9. *Suppose that $\mathbb{K}$ is algebraically closed. If $\varphi\colon X \to Y$ is a regular map of projective varieties, then its image $\varphi(X)$ is a subvariety of Y.*

Proof. Let $\Gamma \subset X \times Y$ be the graph of φ. Suppose that X is a subvariety of $\mathbb{P}^m$ and Y is a subvariety of $\mathbb{P}^n$. Then Γ is a subvariety of $\mathbb{P}^m \times \mathbb{P}^n$. By Theorem 1.5.7 the projection of Γ to $\mathbb{P}^n$, which is the image $\varphi(X)$, is a subvariety of $\mathbb{P}^n$, and hence of Y. □

Proof of Theorem 1.5.7. By Lemma 1.4.15, it suffices to prove the statement about projection to $\mathbb{K}^n$, as we may argue locally on the affine patches $U_0, \ldots, U_n$ of $\mathbb{P}^n$.

Let $X \subset \mathbb{P}^m \times \mathbb{K}^n$ be a subvariety. By Proposition 1.5.6, X is defined by the vanishing of finitely many polynomials

$$g_1(x;y)\,,\ g_2(x;y)\,,\ \ldots\,,\ g_r(x;y)\ \in\ \mathbb{K}[x_0,\ldots,x_m\,,\,y_1,\ldots,y_n]\,,$$

where each g_i is homogeneous of degree d_i in the x variables and with no condition on y.

Let $\pi\colon \mathbb{P}^m \times \mathbb{K}^n \to \mathbb{K}^n$ be the projection. A point $y \in \mathbb{K}^n$ lies in the image $\pi(X)$ if and only if the system of homogeneous polynomials

$$g_1(x;y)\ =\ g_2(x;y)\ =\ \cdots\ =\ g_r(x;y)\ =\ 0\,,$$

has a solution in $\mathbb{P}^m$. By Lemma 1.4.10 this holds if and only if the ideal $I(y)$ these polynomials generate does not contain $\mathfrak{m}_0(x)^d$ for any d. Since $\mathfrak{m}_0(x)^d$ is generated by the vector space $\mathbb{K}[x_0,\ldots,x_m]_d$ of all forms of degree d, this is equivalent to $I(y)_d \neq \mathbb{K}[x_0,\ldots,x_m]_d$, for all d. It is enough to show this for all d that are sufficiently large.

This degree d component $I(y)_d$ of $I(y)$ is the image of the linear map

$$\Lambda_d(y)\ :\ \mathbb{K}[x_0,\ldots,x_m]_{d-d_1}\oplus\cdots\oplus\mathbb{K}[x_0,\ldots,x_m]_{d-d_r}\ \longrightarrow\ \mathbb{K}[x_0,\ldots,x_m]_d\,,$$

given by $(f_1,\ldots,f_r) \mapsto f_1g_1(x;y)+\cdots+f_rg_r(x;y)$. If we write the linear map $\Lambda_d(y)$ in terms of the bases of monomials of $\mathbb{K}[x_0,\ldots,x_m]_d$ and $\mathbb{K}[x_0,\ldots,x_m]_{d-d_i}$, we obtain a matrix $M_d(y)$ with entries the coefficients of the monomials in x in the polynomials $g_i(x;y)$, which are polynomials in y. Thus $I(y)_d \neq \mathbb{K}[x_0,\ldots,x_m]_d$ if and only if $\Lambda_d(y)$ is not surjective.

In Exercise 11 you are asked to show that there is an integer $D > 0$ such that for any $d \geq D$, the matrix M has more columns than rows. Then for $d \geq D$, $\Lambda_d(y)$ is not surjective if and only if the maximal minors of $M_d(y)$ vanish.

We conclude that a point $y \in \mathbb{K}^n$ lies in $\pi(X)$ if and only if all the maximal minors of $M_d(y)$ vanish for all $d \geq D$. As this is a collection of polynomials in $\mathbb{K}[y_1,\ldots,y_n]$, it shows that $\pi(X)$ is an affine subvariety of $\mathbb{K}^n$. □

We close with an extension of finite maps from affine varieties to projective varieties. If $\varphi\colon X \to \mathbb{P}^m$ is a regular map from a projective variety X, then its image $\varphi(X)$ is a subvariety of $\mathbb{P}^m$. This map is *finite* if for every linear form $\Lambda \in \mathbb{K}[y_0,\ldots,y_m]$ on $\mathbb{P}^m$, the corresponding map of affine varieties

$$\varphi\ :\ X \setminus \mathcal{V}(\varphi^*(\Lambda))\ \longrightarrow\ \varphi(X)\setminus\mathcal{V}(\Lambda)$$

is a finite map[1]. We show that linear projections are finite maps.

THEOREM 1.5.10. *Suppose that $\mathbb{K}$ is algebraically closed. Let $X \subset \mathbb{P}^n$ be a projective variety and $L \subset \mathbb{P}^n$ be a linear subspace disjoint from X. Then the linear projection with center L is a finite map $\pi\colon X \to \pi(X)$.*

PROOF. Let $m := n-\dim(L)-1$, so that $\pi\colon X \to \mathbb{P}^m$, and let Λ be a linear form on $\mathbb{P}^m$. Linear forms on $\mathbb{P}^m$ pull back to linear forms on $\mathbb{P}^n$ that vanish along L. Choosing coordinates $y_0,\ldots,y_m$ on $\mathbb{P}^m$, we may assume that $\Lambda = \Lambda_0, \Lambda_1, \ldots, \Lambda_m$ are independent linear forms on $\mathbb{P}^n$ vanishing along L and that π is defined by $y_i = \Lambda_i$. We show that

$$\pi\ :\ X_{\Lambda_0} = X\setminus\mathcal{V}(\Lambda_0)\ \longrightarrow\ \pi(X)\setminus\mathcal{V}(y_0)$$

[1] We revisit this notion in Section 3.3

is a finite map. For this, we show that every element of $\mathbb{K}[X_{\Lambda_0}]$ is integral over the coordinate ring of $\pi(X)\smallsetminus\mathcal{V}(y_0)$, which is its subring generated by $\frac{\Lambda_1}{\Lambda_0},\dotsc,\frac{\Lambda_m}{\Lambda_0}$. (By Result in the appendix this implies that $\mathbb{K}[X_{\Lambda_0}]$ is integral over over the coordinate ring of $\pi(X)\smallsetminus\mathcal{V}(y_0)$.)

Let $p\in\mathbb{K}[X_{\Lambda_0}]$. By Corollary 1.4.16, there is a $d\in\mathbb{N}$ and a form f of degree d such that p is the restriction of the rational function $\frac{f}{\Lambda_0^d}$. Since $\mathcal{V}(\Lambda_0^d,\dotsc,\Lambda_m^d)=L$ is disjoint from X, the degree d forms $(\Lambda_0^d,\dotsc,\Lambda_m^d,f)$ define a regular map $\psi\colon X\to\mathbb{P}^{m+1}$. Let $g_1,\dotsc,g_r\in\mathbb{K}[z_0,\dotsc,z_{m+1}]$ be forms that define the image $\psi(X)$ as a subvariety of $\mathbb{P}^{m+1}$.

We observed that $\emptyset=L\cap X=\mathcal{V}(\Lambda_0^d,\dotsc,\Lambda_m^d)\cap X=\psi^{-1}(\mathcal{V}(z_0,\dotsc,z_m))$. This implies that $\emptyset=\mathcal{V}(z_0,\dotsc,z_m)\cap\psi(X)=\mathcal{V}(z_0,\dotsc,z_m,g_1,\dotsc,g_r)$ in $\mathbb{P}^{m+1}$. By Lemma 1.4.10, there is some $N\in\mathbb{N}$ such that $\mathfrak{m}_0^N\subset\langle z_0,\dotsc,z_m,g_1,\dotsc,g_r\rangle$, where $\mathfrak{m}_0=\langle z_0,\dotsc,z_{m+1}\rangle$ is the irrelevant ideal of $\mathbb{P}^{m+1}$. As $z_{m+1}^N\in\mathfrak{m}_0^N$, there are forms $p_0,\dotsc,p_m,q_1,\dotsc,q_r\in\mathbb{K}[z_0,\dotsc,z_{m+1}]$ such that

$$z_{m+1}^N\ =\ \sum_{i=0}^m z_ip_i\ +\ \sum_{j=1}^r g_jq_j\,.$$

Restricting to the homogeneous part of this expression of degree N, we may assume that $\deg(p_i)=N{-}1$. Set

$$F\ :=\ z_{m+1}^N\ -\ \sum_{i=0}^m z_ip_i\ \in\ \mathbb{K}[z_0,\dotsc,z_{m+1}]\,.$$

Then $F=0$ in $\mathbb{K}[\psi(X)]$, and thus $0=\psi^*(F)$ in $\mathbb{K}[X]$.

Since $\deg(p_i)=N{-}1$, z_{m+1} has degree at most $N{-}1$ in the sum $\sum_{i=0}^m z_ip_i$. Thus, if we write F as a polynomial in z_{m+1}, we obtain

$$F\ =\ z_{m+1}^N\ +\ \sum_{i=0}^{N-1} z_{m+1}^iA_{N-i}(z_0,\dotsc,z_m)\,,$$

where A_i is a form of degree i. Then the pullback $\psi^*(F)$ is

$$f^N\ +\ \sum_{i=0}^{N-1} f^iA_{N-i}(\Lambda_0^d,\dotsc,\Lambda_m^d)\,.$$

Dividing this expression by Λ_0^{Nd}, we obtain

$$\left(\tfrac{f}{\Lambda_0^d}\right)^N\ +\ \sum_{i=0}^{N-1}\left(\tfrac{f}{\Lambda_0^d}\right)^iA_{N-i}\left(1,\left(\tfrac{\Lambda_1}{\Lambda_0}\right)^d,\dotsc,\left(\tfrac{\Lambda_m}{\Lambda_0}\right)^d\right)\,.$$

As this is 0 in $\mathbb{K}[X_{\Lambda_0}]$, we have shown that $\frac{f}{\Lambda_0^d}\in\mathbb{K}[X_{\Lambda_0}]$ is integral over its subring generated by $\frac{\Lambda_1}{\Lambda_0},\dotsc,\frac{\Lambda_m}{\Lambda_0}$, which is $\mathbb{K}[\pi(X)\cap U_0]$. This completes the proof that $\pi\colon X\to\pi(X)$ is a finite map of projective varieties. □

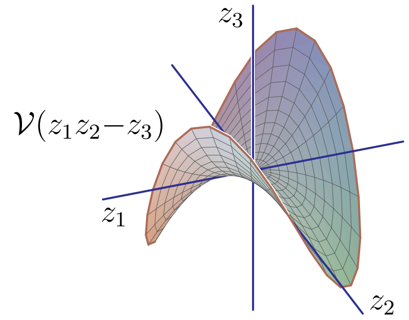
We extend this to more general regular maps.

COROLLARY 1.5.11. *Let X be a projective variety and suppose that $f_0, f_1, \ldots, f_m$ are forms of the same degree such that $\mathcal{V}(f_0, f_1, \ldots, f_m) \cap X = \emptyset$. Then the regular map $\varphi\colon X \to \mathbb{P}^m$ they define gives a finite map $\varphi\colon X \to \varphi(X)$.*

PROOF. Suppose that $X \subset \mathbb{P}^n$. As $\mathcal{V}(f_0, f_1, \ldots, f_m) \cap X = \emptyset$, the forms define a regular map (1.5.1). Let $d := \deg(f_0)$ be the common degree of each form f_i. As shown in (1.5.5), each form f_i is the composition of the dth Veronese map $\nu_{n,d}\colon \mathbb{P}^n \to \mathbb{P}^{\binom{n+d}{n}-1}$ with a linear form Λ_{f_i}. Thus φ is the composition of the isomorphism $\nu_{n,d}\colon X \to \nu_{n,d}(X)$ and the linear projection given by $\Lambda_{f_0}, \Lambda_{f_1}, \ldots, \Lambda_{f_m}$. Since $\mathcal{V}(f_0, f_1, \ldots, f_m) \cap X = \emptyset$, we have $\mathcal{V}(\Lambda_{f_0}, \Lambda_{f_1}, \ldots, \Lambda_{f_m}) \cap \nu_{n,d}(X) = \emptyset$, and the result follows from Theorem 1.5.10. □

Exercises for Section 1.5.

1. Show that if $f_0, \ldots, f_m \in \mathbb{K}[x_0, \ldots, x_n]$ are forms of the same degree that do not simultaneously vanish and if $\mathcal{V}(f_0, \ldots, f_m) = \emptyset$, then (1.5.1) defines a map $\varphi\colon \mathbb{P}^n \to \mathbb{P}^m$.
2. Show that the number of monomials in $x_0, \ldots, x_n$ of degree d is $\binom{n+d}{n} = \binom{n+d}{d}$.
3. Complete the proof of Theorem 1.5.3, verifying the claims made.
4. The quadratic Veronese map $\nu_{n,2}\colon \mathbb{P}^n \to \mathbb{P}^{\binom{n+2}{2}-1}$ may be written as $z_{i,j} = x_i x_j$ for $0 \leq i \leq j \leq n$. Identify $\mathbb{P}^{\binom{n+2}{2}-1}$ with the projective space on $(n+1) \times (n+1)$ symmetric matrices and show that the quadratic Veronese variety is the projectivization of the set of symmetric matrices of rank 1.
5. Let $X \subset \mathbb{P}^n$ be a projective variety and suppose that $f, g \in \mathbb{K}[X]$ are homogeneous forms of the same degree with $g \neq 0$. Show that the quotient f/g gives a well-defined function on $X - \mathcal{V}(g)$.
6. Show that the image of the Segre map $\sigma_{1,1}\colon \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$ is the projectivization of the hyperbolic paraboloid $z_3 = z_1 z_2$.



Show that for any $p, q \in \mathbb{P}^1$, both $\sigma_{1,1}(p \times \mathbb{P}^1)$ and $\sigma_{1,1}(\mathbb{P}^1 \times q)$ are straight lines in $\mathbb{P}^3$ whose intersection is $\sigma_{1,1}(p, q)$.

7. Complete the proof of Theorem 1.5.5.
8. Explain why the set $\mathcal{V}(f) \subset \mathbb{P}^m \times \mathbb{P}^n$ is well-defined for a bihomogeneous polynomial $f(x, y) \in \mathbb{K}[x; y]$ and prove that for any subset $Z \subset \mathbb{P}^m \times \mathbb{P}^n$ its ideal $\mathcal{I}(Z) \subset \mathbb{K}[x; y]$ is bihomogeneous.
9. Prove the equality (1.5.7). Hint: saturate with respect to $\mathfrak{m}_0(y)$.
10. Prove Lemma 1.5.8.

11. Show that if $d_1, \ldots, d_r$ are positive integers, then there is a positive integer D such that for every $d \geq D$,

$$\sum_{i=1}^{r} \dim_{\mathbb{K}} \mathbb{K}[x_0, \ldots, x_m]_{d-d_i} \;>\; \sum_{i=1}^{r} \dim_{\mathbb{K}} \mathbb{K}[x_0, \ldots, x_m]_d \,.$$

Notes

Most of the material in this chapter is standard material within courses of algebraic geometry or related courses. User-friendly, introductory texts to these topics include the books of Beltrametti, Carletti, Gallarati, and Monti Bragadin [**2**], Cox, Little, and O'Shea [**8**], Holme [**23**], Hulek [**24**], Perrin [**28**], Smith, Kahanpää, Kekäläinen, and Traves [**31**]. Advanced, in-depth treatments from the viewpoint of modern, abstract algebraic geometry can be found in the books of Eisenbud [**14**], Harris [**20**], Hartshorne [**21**], Shafarevich [**30**], and Vakil Vakil's tome? Our treatment here and in Chapter 3 is most influenced by Shafarevich, but intermediate between the introductory texts and the advanced treatments.

Our proof of the Nullstellensatz is based on notes by Allcock, which he claims is essentially equivalent to an argument of Zariski [**35**].

If the polynomials $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ over an algebraically closed field $\mathbb{K}$ do not have a common zero, then Hilbert's Nullstellensatz implies a polynomial identity of the form $\sum g_i f_i = 1$ with $g_1, \ldots, g_m \in \mathbb{K}[x_1, \ldots, x_n]$. However, the degrees of the polynomials in such a representation can grow doubly exponentially in the number n of variables, see Kollár [**25**].

CHAPTER 2

Symbolic algorithms

Symbolic algorithms, from resultants to Gröbner bases and beyond, have long been important in algebraic geometry. They are used to establish theoretical results, often providing key arguments in proofs. They are often indispensable tools for basic inquiry, as they enable the computation of key examples. The rise of computers has only increased their importance and they are now an core part of the toolkit of modern algebraic geometry, and essential in many examples. Understanding and extending symbolic algorithms is now a robust area in algebraic geometry and commutative algebra. We develop the general theory and illustrate their utility for solving systems of equations.

2.1. Resultants and Bézout's Theorem

Resultants arose in the 19th century to provide symbolic algorithms for some operations such as elimination. They offer an approach to solving systems of polynomials in two variables.

The key algorithmic step in the Euclidean algorithm for the greatest common divisor (gcd) of univariate polynomials f and g in $\mathbb{K}[x]$ with $n = \deg(g) \geq \deg(f) = m$,

$$\begin{array}{rcl} f & = & f_0x^m + f_1x^{m-1} + \cdots + f_{m-1}x + f_m \\ g & = & g_0x^n + g_1x^{n-1} + \cdots + g_{n-1}x + g_n\,, \end{array} \tag{2.1.1}$$

is to replace g by

$$g - \frac{g_0}{f_0}x^{n-m} \cdot f\,, \tag{2.1.2}$$

which has degree at most $n{-}1$. (Note that $f_0 \cdot g_0 \neq 0$.) We often want to avoid division (e.g., when $\mathbb{K}$ is a function field). Resultants detect common factors without division.

Let $\mathbb{K}[x]_\ell$ be the set of univariate polynomials of degree at most ℓ. (This differs from the notation in Chapter 1, where $\mathbb{K}[x_0, x_1, \ldots, x_n]_\ell$ consisted of all homogeneous forms of degree ℓ.) Then $\mathbb{K}[x]_\ell$ is a vector space over $\mathbb{K}$ of dimension $\ell{+}1$ that has an ordered basis of monomials $x^\ell, \ldots, x, 1$. Given f and g as in (2.1.1), consider the linear map

$$\begin{array}{rrcl} L_{f,g}\ : & \mathbb{K}[x]_{n-1} \times \mathbb{K}[x]_{m-1} & \longrightarrow & \mathbb{K}[x]_{m+n-1} \\ & (h, k) & \longmapsto & f \cdot h + g \cdot k\,. \end{array}$$

The domain and range of $L_{f,g}$ each have dimension $m + n$. We consider the linear map $L_{f,g}$ because of the following lemma.s

Lemma 2.1.1. *The polynomials f and g have a nonconstant common divisor if and only if $L_{f,g}$ has a nontrivial kernel.*

Proof. Suppose first that f and g have a nonconstant common divisor, p. Then there are polynomials h and k with $f = pk$ and $g = ph$. As p is nonconstant, $\deg(k) < \deg(f) = m$ and $\deg(h) < \deg(g) = n$ so that $(h, -k) \in \mathbb{K}[x]_{n-1} \times \mathbb{K}[x]_{m-1}$. Since

$$fh - gk \;=\; pkh - phk \;=\; 0\,,$$

we see that $(h, -k)$ is a nonzero element of the kernel of $L_{f,g}$.

Suppose that f and g are relatively prime and let $(h, k) \in \ker L_{f,g}$. Since $\langle f, g\rangle = \mathbb{K}[x]$, there exist polynomials p and q with $1 = gp + fq$. Using $0 = fh + gk$ we obtain

$$k \;=\; k \cdot 1 \;=\; k(gp + fq) \;=\; gkp + fkq \;=\; -fhp + fkq \;=\; f(kq - hp)\,.$$

This implies that $k = 0$ for otherwise $m-1 \geq \deg(k) \geq \deg(f) = m$, which is a contradiction. We similarly have $h = 0$, and so the kernel of $L_{f,g}$ is $\{(0, 0)\}$. □

The *Sylvester matrix* is the matrix of the linear map $L_{f,g}$ in the ordered bases of monomials for $\mathbb{K}[x]_{m-1} \times \mathbb{K}[x]_{n-1}$ and $\mathbb{K}[x]_{m+n-1}$ When f and g have the form (2.1.1), it is

$$\mathrm{Syl}(f, g) \;=\; \mathrm{Syl}(f, g; x) \;:=\; \left(\begin{array}{cccc|ccc}
f_0 & & & & g_0 & & 0 \\
\vdots & f_0 & 0 & & g_1 & \ddots & \\
f_{m-1} & \vdots & \ddots & & \vdots & & g_0 \\
f_m & \vdots & \ddots & & \vdots & & g_1 \\
 & f_m & & f_0 & g_{n-1} & & \vdots \\
 & & \ddots & \vdots & g_n & \ddots & \vdots \\
 & 0 & \ddots & \vdots & & \ddots & g_{n-1} \\
 & & & f_m & 0 & & g_n
\end{array}\right) . \tag{2.1.3}$$

Note that the sequence $f_0, \ldots, f_0, g_n, \ldots, g_n$ lies along the main diagonal and the left block of the matrix has n columns while the right block has m columns.

We often treat the coefficients $f_0, \ldots, f_m, g_0, \ldots, g_m$ of f and g as variables. That is, we will regard them as algebraically independent over $\mathbb{Q}$ or $\mathbb{Z}$. Any formulas proven under this assumption remain valid when the coefficients of f and g lie in any field or ring.

The (*Sylvester*) *resultant* $\mathrm{Res}(f, g)$ is the determinant of the Sylvester matrix. To emphasize that the Sylvester matrix represents the map $L_{f,g}$ in the basis of monomials in the variable x, we also write $\mathrm{Res}(f, g; x)$ for $\mathrm{Res}(f, g)$. We summarize some properties of resultants, which follow from their definition and from Lemma 2.1.1.

Theorem 2.1.2. *The resultant of nonconstant polynomials $f, g \in \mathbb{K}[x]$ is an integer polynomial in the coefficients of f and g. The resultant vanishes if and only if f and g have a nonconstant common factor.*

We give another expression for the resultant in terms of the roots of f and g.

LEMMA 2.1.3. *Suppose that $\mathbb{K}$ contains all the roots of the polynomials f and g so that*

$$f(x) \;=\; f_0\prod_{i=1}^{m}(x-a_i) \qquad \text{and} \qquad g(x) \;=\; g_0\prod_{i=1}^{n}(x-b_i)\,, \tag{2.1.4}$$

where $a_1,\dots,a_m \in \mathbb{K}$ are the roots of f and $b_1,\dots,b_n \in \mathbb{K}$ are the roots of g. Then

$$\operatorname{Res}(f,g;x) \;=\; f_0^n g_0^m \prod_{i=1}^{m}\prod_{j=1}^{n}(a_i-b_j)\,. \tag{2.1.5}$$

In Exercise 4 you are asked to show that this implies the Poisson formula,

$$\operatorname{Res}(f,g;x) \;=\; f_0^n\prod_{i=1}^{m} g(a_i) \;=\; (-1)^{mn}g_0^m\prod_{i=1}^{n} f(b_i)\,.$$

PROOF. We express the two sides of the equation (2.1.5) in the ring of polynomials in the indeterminates $f_0, g_0, a_1,\dots,a_m, b_1,\dots,b_n$ with integer coefficients, $\mathbb{Z}[f_0, g_0, a_1,\dots,a_m, b_1,\dots,b_n]$. Expanding (2.1.4) shows that the coefficients of f and g are essentially the elementary symmetric polynomials in their roots,

$$f_i \;=\; (-1)^i f_0 e_i(a_1,\dots,a_m) \qquad \text{and} \qquad g_i \;=\; (-1)^i g_0 e_i(b_1,\dots,b_n)\,. \tag{2.1.6}$$

We claim that both sides of (2.1.5) are homogeneous polynomials of degree mn in the variables $a_1,\dots,b_n$. This is immediate for the right hand side. For the resultant, we extend our notation, setting $f_i := 0$ when $i<0$ or $i>m$ and $g_i := 0$ when $i<0$ or $i>n$. Then the entry in row i and column j of the Sylvester matrix is

$$\operatorname{Syl}(f,g;x)_{i,j} \;=\; \begin{cases} f_{i-j} & \text{if } j \le n\,,\\ g_{n+i-j} & \text{if } n<j\le m+n\,. \end{cases}$$

The determinant is a signed sum over permutations w of $\{1,\dots,m{+}n\}$ of terms

$$\prod_{j=1}^{n} f_{w(j)-j} \;\cdot\; \prod_{j=n+1}^{m+n} g_{n+w(j)-j}\,.$$

This term is homogeneous of degree mn. Indeed, as f_i and g_i are each homogeneous of degree i in the variables $a_1,\dots,b_n$ and 0 is homogeneous of any degree, the sum of the degrees of the factors is

$$\sum_{j=1}^{n} w(j){-}j \quad + \quad \sum_{j=n+1}^{m+n} n+w(j){-}j \;=\; mn+\sum_{j=1}^{m+n} w(j){-}j \;=\; mn\,.$$

The resultant Res vanishes whenever $a_i=b_j$ for some $i=1,\dots,m$ and $j=1,\dots,n$. This implies that Res lies in the ideal $\langle a_i-b_j\rangle$ for every i and j. Thus the resultant is a multiple of the double product in (2.1.5). As its degree is mn, it is a scalar multiple. We determine this scalar. The term in $\operatorname{Res}(f,g)$ which is the product of diagonal entries of the Sylvester matrix is

$$f_0^n g_n^m \;=\; (-1)^{mn} f_0^n g_0^m e_n(b_1,\dots,b_n)^m \;=\; (-1)^{mn} f_0^n g_0^m b_1^m\cdots b_n^m\,.$$

This is the only term of $\mathrm{Res}(f,g)$ involving the monomial $b_1^m\cdots b_n^m$. The corresponding term on the right hand side of (2.1.5) is

$$f_0^n g_0^m(-b_1)^m\cdots(-b_n)^m \;=\; (-1)^{mn}f_0^n g_0^m b_1^m\cdots b_n^m\,,$$

which completes the proof. □

Remark 3.3.16 uses geometric arguments to show that the resultant is irreducible and gives another characterization of resultants, which we give below. check this!

THEOREM 2.1.4. *The resultant polynomial is irreducible in $\mathbb{Z}[f_0,\dots,f_m,g_0,\dots,g_m]$. It is the unique (up to sign) irreducible integer polynomial in the coefficients of f and g that vanishes on the set of pairs of polynomials (f,g) which have a common root.*

EXAMPLE 2.1.5. We give an application of resultants. A polynomial $f\in\mathbb{K}[x]$ of degree n has fewer than n distinct roots in the algebraic closure of $\mathbb{K}$ when it has a factor in $\mathbb{K}[x]$ of multiplicity greater than 1, and in that case f and its derivative f' have a factor in common. The *discriminant* of f is a polynomial in the coefficients of f which vanishes precisely when f has a repeated factor. It is defined to be

$$\mathrm{disc}_n(f) \;:=\; (-1)^{\binom{n}{2}}\frac{1}{f_0}\mathrm{Res}(f,f') \;=\; f_0^{2n-2}\prod_{i<j}(a_i-a_j)^2\,,$$

where $a_1,\dots,a_n$ are the roots of $f(x)$. ◇

Resultants may also be used to eliminate variables from multivariate equations. The first step towards this is another interesting formula involving the Sylvester resultant, a canonical expression for it as a polynomial linear combination of f and g.

LEMMA 2.1.6. *Given polynomials $f,g\in\mathbb{K}[x]$, there are polynomials $h,k\in\mathbb{K}[x]$ whose coefficients are universal integer polynomials in the coefficients of f and g such that*

$$f(x)h(x)+g(x)k(x) \;=\; \mathrm{Res}(f,g)\,. \tag{2.1.7}$$

PROOF. Set $\mathbb{K}:=\mathbb{Q}(f_0,\dots,f_m,g_0,\dots,g_n)$, the field of rational functions (quotients of integer polynomials) in the variables $f_0,\dots,f_m,g_0,\dots,g_n$ and let $f,g\in\mathbb{K}[x]$ be univariate polynomials as in (2.1.1). Then $\gcd(f,g)=1$ and so the map $L_{f,g}$ is invertible.

Set $(h,k):=L_{f,g}^{-1}(\mathrm{Res}(f,g))$ so that

$$f(x)h(x) \;+\; g(x)k(x) \;=\; \mathrm{Res}(f,g)\,,$$

with $h\in\mathbb{K}[x]_{n-1}$ and $k\in\mathbb{K}[x]_{m-1}$.

Recall Cramer's formula (1.3.6) for the inverse of a $n\times n$ matrix M,

$$\det(M)\cdot M^{-1} \;=\; \mathrm{adj}M\,, \tag{2.1.8}$$

where $\mathrm{adj}M$ is the *adjugate* of M. Its (i,j)-entry is $(-1)^{i+j}\cdot\det(\widehat{M_{j,i}})$, where $M_{j,i}$ is the $(n-1)\times(n-1)$ matrix obtained from M by deleting its jth row and ith column.

Since $\det(L_{f,g})=\mathrm{Res}(f,g)\in\mathbb{K}$ and $L_{f,g}$ is $\mathbb{K}$-linear, we have

$$L_{f,g}^{-1}(\mathrm{Res}(f,g)) \;=\; \mathrm{Res}(f,g)\cdot L_{f,g}^{-1}(1) \;=\; \det(L_{f,g})\cdot L_{f,g}^{-1}(1) \;=\; \mathrm{adj}(\mathrm{Syl}(f,g))(1)\,.$$

In the monomial basis of $\mathbb{K}[x]_{m+n-1}$ the polynomial 1 is the vector $(0,\ldots,0,1)^T$. Thus, the coefficients of $L_{f,g}^{-1}(\mathrm{Res}(f,g))$ are the entries of the last column of $\mathrm{ad}(\mathrm{Syl}(f,g))$, which are ± the minors of the Sylvester matrix $\mathrm{Syl}(f,g)$ with its last row removed. In particular, they are integer polynomials in the variables $f_0,\ldots,f_m,g_0,\ldots,g_n$. □

This proof shows that $h,k \in \mathbb{Z}[f_0,\ldots,f_m,g_0,\ldots,g_n][x]$ and that (2.1.7) holds as an expression in this polynomial ring with $m{+}n{+}3$ variables. It leads to a method to eliminate variables. Suppose that $f,g \in \mathbb{K}[x_1,\ldots,x_n]$ are multivariate polynomials. We may consider them as polynomials in the variable x_n whose coefficients are polynomials in the other variables, that is, as polynomials in $\mathbb{K}(x_1,\ldots,x_{n-1})[x_n]$. Then the resultant $\mathrm{Res}(f,g;x_n)$ both lies in the ideal generated by f and g and in the subring $\mathbb{K}[x_1,\ldots,x_{n-1}]$. We examine the geometry of this elimination of variables.

Suppose that $1 \leq m < n$ and let $\pi\colon \mathbb{K}^n \to \mathbb{K}^m$ be the coordinate projection

$$\pi \;:\; (a_1,\ldots,a_n) \longmapsto (a_1,\ldots,a_m)\,.$$

Also, for $I \subset \mathbb{K}[x_1,\ldots,x_n]$ set $I_m := I \cap \mathbb{K}[x_1,\ldots,x_m]$.

Lemma 2.1.7. *Let $I \subset \mathbb{K}[x_1,\ldots,x_n]$ be an ideal. Then $\pi(\mathcal{V}(I)) \subset \mathcal{V}(I_m)$. When $\mathbb{K}$ is algebraically closed, $\mathcal{V}(I_m)$ is the smallest variety in $\mathbb{K}^m$ containing $\pi(\mathcal{V}(I))$.*

Proof. Let us set $X := \mathcal{V}(I)$. For the first statement, suppose that $a = (a_1,\ldots,a_n) \in X$. If $f \in I_m = I \cap \mathbb{K}[x_1,\ldots,x_m]$, then

$$0 \;=\; f(a) \;=\; f(a_1,\ldots,a_m) \;=\; f(\pi(a))\,,$$

which establishes the inclusion $\pi(X) \subset \mathcal{V}(I_m)$. (For this we view f as a polynomial in either $x_1,\ldots,x_n$ or in $x_1,\ldots,x_m$.) This implies that $\mathcal{V}(\mathcal{I}(\pi(X))) \subset \mathcal{V}(I_m)$.

Now suppose that $\mathbb{K}$ is algebraically closed. Let $f \in \mathcal{I}(\pi(X))$. Then $f \in \mathbb{K}[x_1,\ldots,x_m]$ has the property that $f(a_1,\ldots,a_m) = 0$ for all $(a_1,\ldots,a_m) \in \pi(X)$. But then f is an element of $\mathbb{K}[x_1,\ldots,x_n]$ that vanishes on $X = \mathcal{V}(I)$. By the Nullstellensatz, there is a positive integer N such that $f^N \in I$ (as elements of $\mathbb{K}[x_1,\ldots,x_n]$). But then $f^N \in I \cap \mathbb{K}[x_1,\ldots,x_m] = I_m$, which implies that $f \in \sqrt{I_m}$. Thus $\mathcal{I}(\pi(X)) \subset \sqrt{I_m}$, so that

$$\mathcal{V}(\mathcal{I}(\pi(X))) \;\supset\; \mathcal{V}(\sqrt{I_m}) \;=\; \mathcal{V}(I_m)\,,$$

which completes the proof. □

The ideal $I_m = I \cap \mathbb{K}[x_1,\ldots,x_m]$ is called an *elimination ideal* as the variables $x_{m+1},\ldots,x_n$ have been eliminated from the ideal I. By Lemma 2.1.7, elimination is the algebraic counterpart to coordinate projection, but the correspondence is not exact. For example, the inclusion $\pi(\mathcal{V}(I)) \subset \mathcal{V}(I \cap \mathbb{K}[x_1,\ldots,x_m])$ may be strict. We saw this in Example 1.3.10 where the projection of the hyperbola $\mathcal{V}(xy-1)$ to the x-axis has image $\mathbb{K}-\{0\} \subsetneq \mathbb{K} = V(0)$, but $\langle 0\rangle = \langle xy-1\rangle \cap \mathbb{K}[x]$. The missing point $\{0\}$ of $\mathbb{K}^1$ corresponds to the coefficient x of the highest power of y in $xy-1$.

Let $\pi\colon \mathbb{K}^{n+1} \to \mathbb{K}^n$ be the projection forgetting the last coordinate. Letting $x_1,\ldots,x_n,t$ be the coordinates of $\mathbb{K}^{n+1}$, then $\pi(x_1,\ldots,x_n,t) = (x_1,\ldots,x_n)$. Let $f,g \in \mathbb{K}[x_1,\ldots,x_n,t]$

and set $I := \langle f, g\rangle \cap \mathbb{K}[x_1,\ldots,x_n]$. By Lemma 2.1.6, the resultant $\mathrm{Res}(f,g;t)$ lies in I. Combining this with Lemma 2.1.7 gives the chain of inclusions

$$\pi(\mathcal{V}(f,g)) \;\subset\; \mathcal{V}(I) \;\subset\; \mathcal{V}(\mathrm{Res}(f,g;t))\,, \tag{2.1.9}$$

with the first inclusion an equality if $\mathbb{K}$ is algebraically closed and $\pi(\mathcal{V}(f,g))$ is a variety.

We now suppose that $\mathbb{K}$ is algebraically closed. Let $f,g \in \mathbb{K}[x_1,\ldots,x_n,t]$ and write each as a polynomial in t with coefficients in $\mathbb{K}[x_1,\ldots,x_n]$,

$$\begin{aligned} f &= f_0t^m + f_1t^{m-1} + \cdots + f_{m-1}t + f_m \\ g &= g_0t^n + g_1t^{n-1} + \cdots + g_{n-1}t + g_n\,, \end{aligned}$$

where $f_i, g_j \in \mathbb{K}[x_1,\ldots,x_n]$ and neither f_0 nor g_0 is the zero polynomial.

Theorem 2.1.8 (Extension Theorem). *Let $\mathbb{K}$ be algebraically closed. If $a \in \mathbb{K}^n$ is an element of $\mathcal{V}(\langle f,g\rangle \cap \mathbb{K}[x_1,\ldots,x_n]) \smallsetminus \mathcal{V}(f_0,g_0)$, then there is some $b \in \mathbb{K}$ with $(a,b) \in \mathcal{V}(f,g)$.*

With $I = \langle f,g\rangle \cap \mathbb{K}[x_1,\ldots,x_n]$ as in (2.1.9), this establishes the chain of inclusions of subvarieties of $\mathbb{K}^n$,

$$\mathcal{V}(I) \smallsetminus \mathcal{V}(f_0,g_0) \;\subset\; \pi(\mathcal{V}(f,g)) \;\subset\; \mathcal{V}(I) \subset\; \mathcal{V}(\mathrm{Res}(f,g;t))\,.$$

If either of f_0 or g_0 are constant, or if $\gcd(f,g) = 1$, then $\mathcal{V}(I) = \mathcal{V}(\mathrm{Res}(f,g;t))$.

Proof. Let $a \in \mathbb{K}^n$ be an element of $\mathcal{V}(I)\smallsetminus\mathcal{V}(f_0,g_0)$. Suppose first that $f_0(a)\cdot g_0(a) \neq 0$. Then $f(a,t)$ and $g(a,t)$ are univariate polynomials in t of degrees m and n, respectively. It follows that the Sylvester matrix $\mathrm{Syl}(f(a,t),g(a,t))$ has the same format (2.1.3) as the Sylvester matrix $\mathrm{Syl}(f,g;t)$, whose entries are the coefficients of f and g, which are polynomials in $x_1,\ldots,x_n$. In fact, $\mathrm{Syl}(f(a,t),g(a,t))$ is obtained from $\mathrm{Syl}(f,g;t)$ by the substitution $x = a$.

This implies that $\mathrm{Res}(f(a,t),g(a,t))$ is the evaluation of the resultant $\mathrm{Res}(f,g;t)$ at $x = a$. Since $\mathrm{Res}(f,g;t) \in I$ and $a \in \mathcal{V}(I)$, this evaluation is 0. By Theorem 2.1.2, the univariate polynomials $f(a,t)$ and $g(a,t)$ have a nonconstant common factor. As $\mathbb{K}$ is algebraically closed, they have a common root, say b. But then $(a,b) \in \mathcal{V}(f,g)$, and so $a \in \pi(\mathcal{V}(f,g))$.

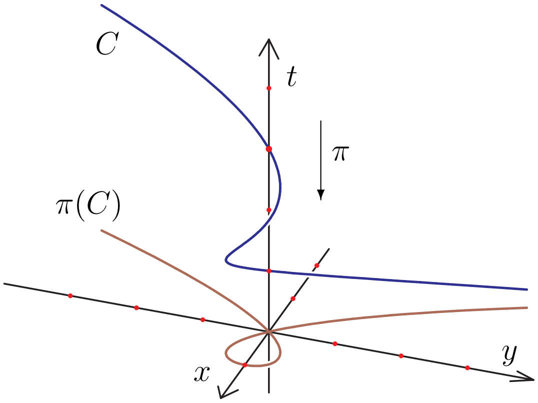
Now suppose that $f_0(a) \neq 0$ but $g_0(a) = 0$. Since $\langle f,g\rangle = \langle f, g + t^\ell f\rangle$, if we replace g by $g + t^\ell f$ where $\ell + m > n$, then we are in the previous case. □

We solve the implicitization problem for plane curves using elimination.

Example 2.1.9. Consider the parametric plane curve from Example 1.3.8,

$$x \;=\; 1 - t^2, \qquad y \;=\; t^3 - t\,. \tag{2.1.10}$$

This is the image of the space curve $C := \mathcal{V}(t^2 - 1 + x, t^3 - t - y)$ under the projection $(x,y,t) \mapsto (x,y)$. Indeed, C is the graph of the map $t \mapsto (1 - t^2, t^3 - t)$ We display this with the t-axis vertical and the xy-plane at $t = -2$.



By Lemma 2.1.7, the plane curve is defined by $\langle t^2 - 1 + x, t^3 - t - y\rangle \cap \mathbb{K}[x, y]$. If we set

$$f(t) \;:=\; t^2 - 1 + x \qquad\text{and}\qquad g(t) \;:=\; t^3 - t - y\,,$$

then the Sylvester resultant $\operatorname{Res}(f, g; t)$ is

$$\det\left(\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0 & 1\\ x{-}1 & 0 & 1 & -1 & 0\\ 0 & x{-}1 & 0 & -y & -1\\ 0 & 0 & x{-}1 & 0 & -y \end{array}\right) \;=\; y^2 - x^2 + x^3\,,$$

which is the implicit equation of the parameterized cubic $\pi(C)$ (2.1.10). ⋄

The ring $\mathbb{K}[x, y]$ of bivariate polynomials is a subring of the ring $\mathbb{K}(x)[y]$ of polynomials in y whose coefficients are rational functions in x. Suppose that $f, g \in \mathbb{K}[x, y]$. Considering f and g as elements of $\mathbb{K}(x)[y]$, the resultant $\operatorname{Res}(f, g; y)$ is the determinant of their Sylvester matrix expressed in the basis of monomials in y. By Theorem 2.1.2, $\operatorname{Res}(f, g; y)$ is a univariate polynomial in x which vanishes if and only if f and g have a common factor in $\mathbb{K}(x)[y]$. In fact it vanishes if and only if $f(x, y)$ and $g(x, y)$ have a common factor in $\mathbb{K}[x, y]$ with positive degree in y, by the following version of Gauss's lemma for $\mathbb{K}[x, y]$.

Lemma 2.1.10. *Polynomials f and g in $\mathbb{K}[x, y]$ have a common factor of positive degree in y if and only if they have a common factor in $\mathbb{K}(x)[y]$.*

Proof. The forward implication is clear, as such a factorization in $\mathbb{K}[x, y]$ is also a factorization in $\mathbb{K}(x)[y]$. For the reverse implication, suppose that

$$f \;=\; h \cdot \overline{f} \qquad\text{and}\qquad g \;=\; h \cdot \overline{g} \tag{2.1.11}$$

is a factorization in $\mathbb{K}(x)[y]$ where h has positive degree in y.

There is a polynomial $d \in \mathbb{K}[x]$ which is divisible by every denominator of a coefficient of h, $\overline{f}$, and $\overline{g}$. Multiplying the expressions (2.1.11) by d^2 gives

$$d^2 f \;=\; (dh) \cdot (d\overline{f}) \qquad\text{and}\qquad d^2 g \;=\; (dh) \cdot (d\overline{g})\,,$$

where dh, $d\overline{f}$, and $d\overline{g}$ are polynomials in $\mathbb{K}[x,y]$. Let $p(x,y) \in \mathbb{K}[x,y]$ be an irreducible polynomial factor of dh having positive degree in y. Then p divides both $d^2 f$ and $d^2 g$. However, p cannot divide d as $d \in \mathbb{K}[x]$ and p has positive degree in y. Therefore $p(x,y)$ is a common polynomial factor of f and g. □

Example 2.1.11. Suppose that $f, g \in \mathbb{C}[x,y]$ are the polynomials,

$$\begin{aligned} f &= (5-10x+5x^2)y^2 + (-14+42x-24x^2)y + (5-28x+19x^2) \\ g &= (5-10x+5x^2)y^2 + (-16+46x-26x^2)y + (19-36x+21x^2) \end{aligned}$$

Figure 2.1.1 shows the curves $\mathcal{V}(f)$ and $\mathcal{V}(g)$, which meet in three points,

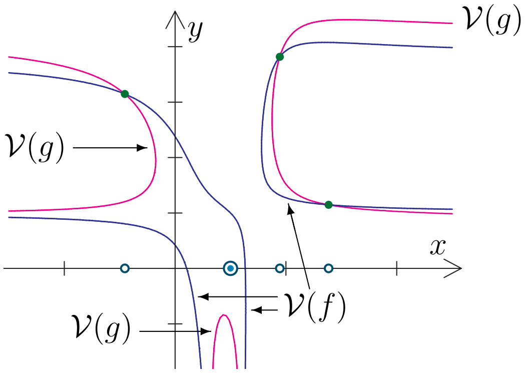


Figure 2.1.1. Comparing resultants to elimination.

$$\mathcal{V}(f,g) = \{ (-0.9081601, 3.146707),\ (1.888332, 3.817437),\ (2.769828, 1.146967) \} .$$

Thus $\pi(\mathcal{V}(f,g))$ consists of three points which are roots of $h = 4x^3 - 15x^2 + 4x + 19$, where $\langle h \rangle = \langle f, g \rangle \cap \mathbb{K}[x]$. However, the resultant is

$$\mathrm{Res}(f,g;y) = 160(4x^3 - 15x^2 + 4x + 19)(x-1)^4 ,$$

whose roots are shown on the x-axis, including the point $x = 1$ with multiplicity four. ⋄

We single out a special case of the Extension Theorem 2.1.8 when $n = 1$ and f_0, g_0 are constants.

Corollary 2.1.12. *If the coefficients of the highest powers of y in f and g do not involve x and if* $\gcd(f,g) = 1$, *then* $\mathcal{V}(\langle f,g\rangle \cap \mathbb{K}[x]) = \mathcal{V}(\mathrm{Res}(f,g;x))$.

Lemma 2.1.13. *When $\mathbb{K}$ is algebraically closed, the system of bivariate polynomials*

$$f(x,y) = g(x,y) = 0$$

has finitely many solutions in $\mathbb{K}^2$ if and only if f and g have no common factor.

Proof. We instead show that $\mathcal{V}(f,g)$ is infinite if and only if f and g do have a common factor. If f and g have a common factor $h(x,y)$ then their common zeroes $\mathcal{V}(f,g)$ include $\mathcal{V}(h)$ which is infinite as h is nonconstant and $\mathbb{K}$ is algebraically closed.

Now suppose that $\mathcal{V}(f,g)$ is infinite. Its projection to at least one of the two coordinate axes is infinite. Suppose that the projection π onto the x-axis is infinite. Set $I := \langle f,g\rangle \cap \mathbb{K}[x]$, the elimination ideal. By the Theorem 2.1.8, we have $\pi(\mathcal{V}(f,g)) \subset \mathcal{V}(I) \subset \mathcal{V}(\mathrm{Res}(f,g;y))$. Since $\pi(\mathcal{V}(f,g))$ is infinite, $\mathcal{V}(\mathrm{Res}(f,g;y)) = \mathbb{K}$, which implies that $\mathrm{Res}(f,g;y)$ is the zero polynomial. By Theorem 2.1.2 and Lemma 2.1.10, f and g have a common factor. □

Let $f,g \in \mathbb{K}[x,y]$ and suppose that neither $\mathrm{Res}(f,g;x)$ nor $\mathrm{Res}(f,g;y)$ vanishes so that f and g have no common factor. Then $\mathcal{V}(f,g)$ consists of finitely many points. The Extension Theorem 2.1.8 gives the following algorithm to compute $\mathcal{V}(f,g)$.

Algorithm 2.1.14 (Elimination Algorithm).
Input: Polynomials $f,g \in \mathbb{K}[x,y]$ with $\gcd(f,g) = 1$.
Output: $\mathcal{V}(f,g)$.

First, compute the resultant $\mathrm{Res}(f,g;x)$, which is not the zero polynomial. Then, for every root a of $\mathrm{Res}(f,g;y)$, find all common roots b of $f(a,y)$ and $g(a,y)$. The finitely many pairs (a,b) computed are the points of $\mathcal{V}(f,g)$. ⋄

The Elimination Algorithm reduces the problem of solving a bivariate system

$$f(x,y) \;=\; g(x,y) \;=\; 0\,, \tag{2.1.12}$$

to that of sequentially finding the roots of univariate polynomials.

Often we only want to count the number of solutions to a system (2.1.12), or give a realistic bound for this number which is attained when f and g are sufficiently general (we explain this in Section **??**). The most basic such bound was given by Etienne Bézout in 1779. Our first step toward establishing Bézout's Theorem is an exercise in algebra and some bookkeeping. The monomials in a polynomial of degree n in the variables x,y are indexed by the set

$$n\text{◺} \;:=\; \{(i,j) \in \mathbb{N}^2 \mid i+j \leq n\}\,.$$

Let $F := \{f_{i,j} \mid (i,j) \in m\text{◺}\}$ and $G := \{g_{i,j} \mid (i,j) \in n\text{◺}\}$ be variables and consider polynomials f and g of respective degrees m and n in $\mathbb{Z}[F,G][x,y]$,

$$f(x,y) \;:=\; \sum_{(i,j)\in m\text{◺}} f_{i,j}x^iy^j \qquad \text{and} \qquad g(x,y) \;:=\; \sum_{(i,j)\in n\text{◺}} g_{i,j}x^iy^j\;.$$

Lemma 2.1.15. *This resultant* $\mathrm{Res}(f,g;y) \in \mathbb{Z}[F,G][x]$ *is a polynomial in* x *of degree* mn.

Proof. Write

$$f \;:=\; \sum_{j=0}^{m} f_j(x)y^{m-j} \qquad \text{and} \qquad g \;:=\; \sum_{j=0}^{n} g_j(x)y^{n-j}\,,$$

where the coefficients are univariate polynomials in x,

$$f_j(x) \;:=\; \sum_{i=0}^{j} f_{i,m-j}x^i \qquad \text{and} \qquad g_j(x) \;:=\; \sum_{i=0}^{j} g_{i,n-j}x^i\,.$$

Then the Sylvester matrix $\mathrm{Syl}(f,g;y)$ (2.1.3) has entries the polynomials $f_i(x)$ and $g_j(x)$, and so the resultant $\mathrm{Res}(f,g;y)=\det(\mathrm{Syl}(f,g;y))$ is a univariate polynomial in x.

As in the proof of Lemma 2.1.3, if we set $f_j := 0$ when $j<0$ or $j>m$ and $g_j := 0$ when $j<0$ or $j>n$, then the entry in row i and column j of the Sylvester matrix is

$$\mathrm{Syl}(f,g;y)_{i,j} \;=\; \begin{cases} f_{i-j}(x) & \text{if } j\leq n\\ g_{n+i-j}(x) & \text{if } n<j\leq m+n \end{cases} .$$

The determinant is a signed sum over permutations w of $\{1,\dots,m{+}n\}$ of terms

$$\prod_{j=1}^{n} f_{w(j)-j}(x) \;\cdot\; \prod_{j=n+1}^{m+n} g_{n+w(j)-j}(x)\,.$$

This is a polynomial in x of degree at most

$$\sum_{j=1}^{n} w(j){-}j \quad+\quad \sum_{j=n+1}^{m+n} n+w(j){-}j \;=\; mn+\sum_{j=1}^{m+n} w(j){-}j \;=\; mn\,.$$

Thus $\mathrm{Res}(f,g;y)$ is a polynomial of degree at most mn in x.

We complete the proof by showing that the resultant does indeed have degree mn. The product $f_0(x)^n\cdot g_n(x)^m$ of the entries along the main diagonal of the Sylvester matrix has leading term $f_{0,m}^n\cdot g_{n,0}^m\,x^{mn}$ and constant term $f_{0,m}^n\cdot g_{0,n}^m$, and these are the only terms in the expansion of the determinant of the Sylvester matrix involving either of these monomials in the coefficients $f_{i,j},g_{k,l}$. □

We now state and prove Bézout's Theorem. By general, we mean an element of the complement of a proper subvariety. This notion is covered in more detail on Section **??**.

THEOREM 2.1.16 (Bézout's Theorem). *Two polynomials $f,g\in\mathbb{K}[x,y]$ either have a common factor or else $|\mathcal{V}(f,g)|\leq\deg(f)\cdot\deg(g)$.*

When $|\mathbb{K}|$ is at least $\max\{\deg(f),\deg(g)\}$, this inequality is sharp in that the bound is attained for some f,g. When $\mathbb{K}$ is algebraically closed, the bound is attained when f and g are general polynomials of the given degrees.

PROOF. Suppose that $m:=\deg(f)$ and $n:=\deg(g)$. By Lemma 2.1.13, if f and g are relatively prime, then $\mathcal{V}(f,g)$ is finite. Let us extend $\mathbb{K}$ to its algebraic closure $\overline{\mathbb{K}}$, which in infinite. We may change coordinates, replacing f by $f(A(x,y))$ and g by $g(A(x,y))$, where A is an invertible affine transformation,

$$A(x,y) \;=\; (ax+by+c,\;\alpha x+\beta y+\gamma)\,, \tag{2.1.13}$$

with $a,b,c,\alpha,\beta,\gamma\in\overline{\mathbb{K}}$ and $a\beta-\alpha b\neq 0$. As $\overline{\mathbb{K}}$ is infinite, we can choose these parameters so that the constant terms and terms with highest power of x in each of f and g are nonzero. By Lemma 2.1.15, this implies that the resultant $\mathrm{Res}(f,g;y)$ has degree at most mn and thus at most mn zeroes. If we set $I:=\langle f,g\rangle\cap\overline{\mathbb{K}}[x]$, then this also implies that $\mathcal{V}(I)=\mathcal{V}(\mathrm{Res}(f,g;x))$, by Corollary 2.1.12.

We can furthermore choose the parameters in A so that the projection $\pi\colon (x,y)\mapsto x$ is 1-1 on $\mathcal{V}(f,g)$, as $\mathcal{V}(f,g)$ is finite and $\overline{\mathbb{K}}$ infinite. Thus

$$\pi(\mathcal{V}(f,g)) \;=\; \mathcal{V}(I) \;=\; \mathcal{V}(\mathrm{Res}(f,g;x))\,,$$

which implies the inequality of the theorem as $|\mathcal{V}(\mathrm{Res}(f,g;y))| \leq mn$.

To see that the bound is sharp when $|\mathbb{K}|$ is large enough, let $a_1,\dots,a_m$ and $b_1,\dots,b_n$ be distinct elements of $\mathbb{K}$. Note that the system

$$f \ :=\ \prod_{i=1}^{m}(x-a_i) \ =\ 0 \qquad \text{and} \qquad g \ :=\ \prod_{i=1}^{n}(y-b_i) \ =\ 0 \tag{2.1.14}$$

has mn solutions $\{(a_i,b_j) \mid 1 \leq i \leq m, 1 \leq j \leq n\}$, so the inequality is sharp.

Suppose now that $\mathbb{K}$ is algebraically closed. If the resultant $\mathrm{Res}(f,g;y)$ has fewer than mn distinct roots, then either it has degree strictly less than mn or else it has a multiple root. In the first case, its leading coefficient vanishes and in the second case, its discriminant vanishes. But the leading coefficient and the discriminant of $\mathrm{Res}(f,g;y)$ are polynomials in the $\binom{m+2}{2}+\binom{n+2}{2}$ coefficients of f and g. Neither is the zero polynomial, as they do not vanish when evaluated at the coefficients of the polynomials (2.1.14). Thus the set of pairs of polynomials (f,g) with $\mathcal{V}(f,g)$ consisting of mn points in $\mathbb{K}^2$ is the complement of a proper subvariety of $\mathbb{K}^{\binom{m+2}{2}+\binom{n+2}{2}}$. □

Exercises for Section 2.1.

1. Prove the formula (2.1.6) for the coefficients of a polynomial in terms of its roots.
2. Verify the claims in the proof of Lemma 2.1.3. This may involve unique factorization in polynomial rings and the Nullstellensatz.
3. What happens to the Sylvester matrix if $m \geq n$ and f is replaced by the first remainder (2.1.2) in the Euclidean Algorithm?
4. Using the formula (2.1.5) deduce the Poisson formula for the resultant of univariate polynomials f and g,
$$\mathrm{Res}(f,g;x) \ =\ f_0^n \prod_{i=1}^{m} g(a_i)\,,$$
where $a_1,\dots,a_m$ are the roots of f.
5. Suppose that the polynomial $g = g_1 \cdot g_2$ factors. Show that the resultant also factors, $\mathrm{Res}(f,g;x) = \mathrm{Res}(f,g_1;x)\cdot\mathrm{Res}(f,g_2;x)$.
6. Prove the equality of the two formulas for the discriminant in Example 2.1.5. Hint: First prove the formula: $f'(a_i) = f_0(a_i-a_1)\cdots\widehat{(a_i-a_i)}\cdots(a_i-a_m)$, where $a_1,\dots,a_m$ are the roots of f and $\widehat{(a_i-a_i)}$ indicates that this term is omitted.
7. Compute the discriminant of a general cubic x^3+ax^2+bx+c by taking the determinant of a 5×5 matrix. Show that the discriminant of the depressed quartic x^4+ax^2+bx+c is
$$16a^4c - 4a^3b^2 - 128a^2c^2 + 144ab^2c - 27b^4 + 256c^3\,.$$
8. Suppose that $f = x^2+y^2+z^2-4$ and $g = 4x^2-4y^2+(2z-3)^2-1$. Use a resultant to compute $\pi(\mathcal{V}(f,g))$ where $\pi\colon (x,y,z) \mapsto (x,y)$.

   Suppose that f and g are general polynomials in $\mathbb{C}[x,y,z]$ of degrees a and b, respectively, what do you expect is the degree of $\mathrm{Res}(f,g;z)$? Why?
9. Find the implicit equation for the parametric curve given by $x = t^4-2t^3+3t^2-6t+3$, $y = t^3-4t^2+3t+1$.

10. Suppose that a curve C is given parametrically by $x = f(t)$ and $g = y(t)$. What do you expect is the degree of C? When does this expectation occur?

2.2. Gröbner basics

Gröbner bases are a foundation for many algorithms to represent and manipulate varieties on a computer. While these algorithms are important in applications, Gröbner bases are also a useful theoretical tool. They will reappear in later chapters in both guises.

A motivating problem is that of recognizing when a polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$ lies in an ideal I. When I is radical and $\mathbb{K}$ is algebraically closed, this is equivalent to asking whether or not f vanishes on $\mathcal{V}(I)$. For example, we may ask which of the polynomials $x^3z - xz^3$, $x^2yz - y^2z^2 - x^2y^2$, and/or $x^2y - x^2z + y^2z$ lies in the ideal

$$\langle x^2y{-}xz^2{+}y^2z,\ y^2{-}xz{+}yz\rangle \ ?$$

This *ideal membership problem* is easy for univariate polynomials. Suppose that $I = \langle f(x), g(x), \ldots, h(x)\rangle$ is an ideal and $F(x)$ is a polynomial in $\mathbb{K}[x]$, the ring of polynomials in a single variable x. We determine if $F(x) \in I$ via a two-step process.

(i) Use the Euclidean Algorithm to compute $p(x) := \gcd(f(x), g(x), \ldots, h(x))$.
(ii) Use the Division Algorithm to determine if $p(x)$ divides $F(x)$.

This is valid, as $I = \langle p(x)\rangle$. The first step is a simplification, where we find a simpler (lower-degree) polynomial which generates I, while the second step is a reduction, where we compute F modulo I. Both steps proceed systematically, operating on the terms of the polynomials involving the highest power of x. A good description for I is a prerequisite for solving our ideal membership problem.

We shall see how Gröbner bases give algorithms which extend this procedure to multivariate polynomials. In particular, a Gröbner basis of an ideal I gives a sufficiently good description of I to solve the ideal membership problem. Gröbner bases are also the foundation of algorithms that solve many other problems.

A *monomial* is a product of powers of the variables $x_1, \ldots, x_n$. The *exponent* of a monomial $x^\alpha := x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$ is a vector $\alpha \in \mathbb{N}^n$. If we identify monomials with their exponent vectors, then multiplication of monomials corresponds to vector addition, and divisibility of monomials corresponds to the partial order on $\mathbb{N}^n$ of componentwise comparison.

Definition 2.2.1. A *monomial ideal* $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is an ideal which satisfies the following two equivalent conditions.

(i) I is generated by monomials.
(ii) If $f \in I$, then every monomial of f lies in I. ◇

One advantage of monomial ideals is that they are essentially combinatorial objects. By Condition (*ii*), a monomial ideal is determined by the set of monomials which it contains. Under the correspondence between monomials and their exponents, divisibility of monomials corresponds to componentwise comparison of vectors.

$$x^\alpha | x^\beta \iff \alpha_i \leq \beta_i\,,\ i = 1, \ldots, n \iff \alpha \leq \beta\,,$$

which defines a partial order on $\mathbb{N}^n$. Thus

$$(1,1,1) \leq (3,1,2) \qquad \text{but} \qquad (3,1,2) \not\leq (2,3,1)\,.$$

The set $O(I)$ of exponent vectors of monomials in a monomial ideal I has the property that if $\alpha \leq \beta$ with $\alpha \in O(I)$, then $\beta \in O(I)$. Thus $O(I)$ is an (upper) *order ideal* of the *poset* (*p*artially *o*rdered *set*) $\mathbb{N}^n$.

A set of monomials $G \subset I$ generates I if and only if every monomial in I is divisible by at least one monomial of G. A monomial ideal I has a unique minimal set of generators—these are the monomials x^α in I which are not divisible by any other monomial in I.

Let us look at some examples. When $n = 1$, monomials have the form x^d for some natural number $d \geq 0$. If d is the minimal exponent of a monomial in I, then $I = \langle x^d \rangle$. Thus all univariate monomial ideals have the form $\langle x^d \rangle$ for some $d \geq 0$.

When $n = 2$, we identify monomials with their exponents and identify the monomial ideal I with the set of exponents of monomials in I. We may then plot the exponents in the order ideal associated to a monomial ideal. For example, the lattice points in the shaded region of Figure 2.2.1 represent the monomials in the ideal $I := \langle y^4,\, x^2y^4,\, x^3y^3,\, x^5y,\, x^6y^2 \rangle$,

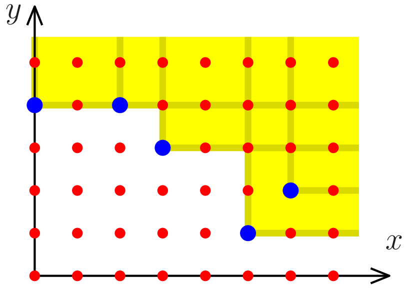


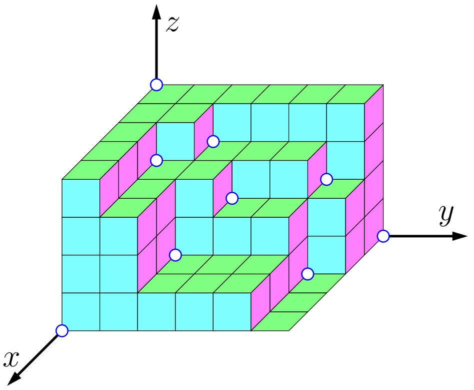
FIGURE 2.2.1. Exponents of monomials in the ideal $\langle y^4,\, x^2y^4,\, x^3y^3,\, x^5y,\, x^6y^2 \rangle$.

with the generators marked. From this picture we see that I is minimally generated by y^4, x^3y^3, and x^5y.

Since $x^ay^b \in I$ implies that $x^{a+c}y^{b+d} \in I$ for any $(c,d) \in \mathbb{N}^2$, a monomial ideal $I \subset \mathbb{K}[x,y]$ is the union of the shifted positive quadrants $(a,b) + \mathbb{N}^2$ for every monomial $x^ay^b \in I$. It follows that the monomials in I are those above the staircase shape that is the boundary of the shaded region. The monomials not in I lie under the staircase, and they form a vector space basis for the quotient ring $\mathbb{K}[x,y]/I$.

This notion of staircase for two variables makes sense when there are more variables. The *staircase* of an ideal I consists of the monomials which are on the boundary of $O(I)$.

Here is the staircase for the ideal $\langle x^5,\, x^2y^5,\, y^6,\, x^3y^2z,\, x^2y^3z^2,\, xy^5z^2,\, x^2yz^3,\, xy^2z^3,\, z^4\rangle$.



We offer a purely combinatorial proof that monomial ideals are finitely generated.

Lemma 2.2.2 (Dickson's Lemma). *Every monomial ideal is finitely generated.*

Proof. We use induction on n. The case $n = 1$ was covered in the preceding examples. Let $I \subset \mathbb{K}[x_1,\ldots,x_n,y]$ be a monomial ideal. For each $d \in \mathbb{N}$, observe that the set

$$\{x^\alpha \mid x^\alpha y^d \in I\}\,,$$

generates a monomial ideal I_d of $\mathbb{K}[x_1,\ldots,x_n]$, and the union of all such monomials,

$$\{x^\alpha \mid x^\alpha y^d \in I \text{ for some } d \geq 0\}\,,$$

generates a monomial ideal I_∞ of $\mathbb{K}[x_1,\ldots,x_n]$. By our induction hypothesis, I_d has a finite generating set G_d, for each $d = 0, 1, \ldots, \infty$.

Note that $I_0 \subset I_1 \subset \cdots \subset I_\infty$. We must have $I_\infty = I_d$ for some $d < \infty$. Indeed, each generator $x^\alpha \in G_\infty$ of I_∞ comes from a monomial $x^\alpha y^b$ in I, and we may let d be the maximum of the numbers b which occur among the finitely many generators of I_∞. Since $I_\infty = I_d$, we have $I_b = I_d$ for any $b > d$. Note that if $b > d$, then we may assume that $G_b = G_d$ as $I_b = I_d$.

We claim that the finite set

$$G \;=\; \bigcup_{b=0}^{d} \{x^\alpha y^b \mid x^\alpha \in G_b\}$$

generates I. Indeed, let $x^\alpha y^b$ be a monomial in I. Since $x^\alpha \in I_b$, there is a generator $x^\gamma \in G_b$ which divides x^α. If $b \leq d$, then $x^\gamma y^b \in G$ is a monomial dividing $x^\alpha y^b$. If $b > d$, then as $G_b = G_d$, we have $x^\gamma y^d \in G$ and $x^\gamma y^d$ divides $x^\alpha y^b$. Thus G generates I. □

A consequence of Dickson's Lemma is that any strictly increasing chain of monomial ideals is finite. Suppose that we have an increasing chain of monomial ideals,

$$I_1 \;\subset\; I_2 \;\subset\; I_3 \;\subset\; \cdots$$

Let I_∞ be their union, which is another monomial ideal. Since I_∞ is finitely generated, there is some ideal I_d which contains all generators of I_∞, and so $I_d = I_{d+1} = \cdots = I_\infty$. We used this technique to prove Dickson's lemma.

The key idea behind Gröbner bases is to determine what is meant by 'term of highest power' in a polynomial having two or more variables. It turns out that there is no canonical way to do this, so we must make a choice, which is encoded in the notion of a monomial order. An order $\succ$ on monomials in $\mathbb{K}[x_1,\dots,x_n]$ is *total* if for monomials x^α and x^β exactly one of the following holds

$$x^\alpha \ \succ\ x^\beta \qquad \text{or} \qquad x^\alpha \ =\ x^\beta \qquad \text{or} \qquad x^\alpha \ \prec\ x^\beta\,.$$

(Note that we use both $\succ$ and $\prec$, where $x^\alpha \prec x^\beta$ if and only if $x^\beta \succ x^\alpha$.)

Definition 2.2.3. A *monomial order* on $\mathbb{K}[x_1,\dots,x_n]$ is a total order $\succ$ on the monomials in $\mathbb{K}[x_1,\dots,x_n]$ such that

(i) 1 is the minimal element under $\succ$.

(ii) $\succ$ respects multiplication by monomials: If $x^\alpha \succ x^\beta$ then $x^\alpha\cdot x^\gamma \succ x^\beta\cdot x^\gamma$, for any monomial x^γ.

Conditions (*i*) and (*ii*) in Definition 2.2.3 imply that if x^α is divisible by x^β, then $x^\alpha \succ x^\beta$. A *well-ordering* is a total order with no infinite descending chain, equivalently, one in which every subset has a minimal element.

Lemma 2.2.4. *Monomial orders on $\mathbb{K}[x_1,\dots,x_n]$ are exactly the well-orderings $\succ$ on monomials that satisfy Condition (ii) of Definition* 2.2.3.

Proof. Let $\succ$ be a well-ordering on monomials in $\mathbb{K}[x_1,\dots,x_n]$ that satisfies Condition (*ii*) of Definition 2.2.3. Suppose that $\succ$ is not a monomial order. Then there is some monomial x^α with $1 \succ x^\alpha$. By Condition (*ii*), we have $1 \succ x^\alpha \succ x^{2\alpha} \succ x^{3\alpha} \succ \cdots$, which contradicts $\succ$ being a well-order. Thus 1 is the $\succ$-minimal monomial.

Let $\succ$ be a monomial order and M be any set of monomials. Let I be the ideal generated by M. By Dickson's Lemma, I is generated by a finite set G of monomials. We may assume that $G\subset M$, for if $x^\alpha \in G\smallsetminus M$, then as M generates I, there is some $x^\beta\in M$ that divides x^α, and so we may replace x^α by x^β in G. After finitely many such replacements, we will have that $G\subset M$. Since G is finite, let x^γ be the minimal monomial in G under $\succ$. We claim that x^γ is the minimal monomial in M.

Let $x^\alpha\in M$. Since G generates I and $M\subset I$, there is some $x^\beta\in G$ which divides x^α and thus $x^\alpha \succ x^\beta$. But x^γ is the minimal monomial in G, so $x^\alpha \succ x^\beta \succ x^\gamma$. □

The well-ordering property of monomials orders is key to what follows, as many proofs use induction on $\succ$, which requires that $\succ$ be a well-ordering.

Example 2.2.5. Recall that the *(total) degree*, $\deg(x^\alpha)$, of a monomial $x^\alpha = x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ is $\alpha_1+\cdots+\alpha_n$. We describe four important monomial orders.

(i) The *lexicographic order* $\succ_{\text{lex}}$ on $\mathbb{K}[x_1,\dots,x_n]$ is defined by

$$x^\alpha \succ_{\text{lex}} x^\beta \iff \left\{\begin{matrix}\text{The first nonzero entry of the}\\ \text{vector } \alpha-\beta \text{ in } \mathbb{Z}^n \text{ is positive.}\end{matrix}\right\}$$

(ii) The *degree lexicographic order* $\succ_{\text{dlx}}$ on $\mathbb{K}[x_1,\dots,x_n]$ is defined by

$$x^\alpha \succ_{\text{dlx}} x^\beta \iff \left\{\begin{array}{ll}\deg(x^\alpha) > \deg(x^\beta) & \text{or}\,,\\ \deg(x^\alpha) = \deg(x^\beta) & \text{and}\ \ x^\alpha \succ_{\text{lex}} x^\beta\,.\end{array}\right.$$

(iii) The *degree reverse lexicographic order* $\succ_{drl}$ $\mathbb{K}[x_1,\dots,x_n]$ is defined by

$$x^\alpha \succ_{\rm drl} x^\beta \iff \begin{cases} \deg(x^\alpha) > \deg(x^\beta) & \text{or ,} \\ \deg(x^\alpha) = \deg(x^\beta) & \text{and the last nonzero entry of the} \\ & \text{vector } \alpha-\beta \text{ in } \mathbb{Z}^n \text{ is negative .} \end{cases}$$

(iv) Let $w \in \mathbb{R}^n_{\geq}$ be a vector with nonnegative components, called a weight. This defines a partial order $\succ_w$ on monomials

$$x^\alpha \ \succ_w \ x^\beta \iff w\cdot\alpha > w\cdot\beta\,.$$

If all components of w are positive, then $\succ_w$ satisfies the two conditions of Definition 2.2.3. Its only failure to be a monomial order is that it may not be a total order on monomials. (For example, consider $w=(1,1,\dots,1)$, then $w\cdot\alpha$ is the total degree of x^α.) This may be remedied by picking a monomial order to break ties. For example, if we use $\succ_{\rm lex}$, then we get a monomial order

$$x^\alpha \ \succ_{w,{\rm lex}} \ x^\beta \iff \begin{cases} w\cdot\alpha > w\cdot\beta & \text{or ,} \\ w\cdot\alpha = w\cdot\beta & \text{and } x^\alpha \succ_{\rm lex} x^\beta \end{cases}$$

Another way to do this is to break the ties with a different monomial order, or a different weight, and this may be done recursively. We call all of these $\succ_w$, $\succ_{w,\succ_{\rm lex}}$, and etc. *weighted orders* for the weight w.

A monomial order is *graded* if it refines the total degree partial order $\succ_{(1,1,\dots,1)}$. The orders $\succ$ dlx and $\succ_{\rm drl}$ are graded monomial orders. They are sometimes called graded lexicographic and graded reverse lexicographic orders, and $\succ_{\rm drl}$ is also called grevlex. ◇

You are asked to prove these are monomial orders in Exercise 7.

Remark 2.2.6. We compare the first three orders on monomials of degrees 1 and 2 in $\mathbb{K}[x,y,z]$ where the variables are ordered $x\succ y\succ z$.

$$\begin{gathered} x^2 \succ_{\rm lex} xy \succ_{\rm lex} xz \succ_{\rm lex} x \succ_{\rm lex} y^2 \succ_{\rm lex} yz \succ_{\rm lex} y \succ_{\rm lex} z^2 \succ_{\rm lex} z \\ x^2 \succ_{\rm dlx} xy \succ_{\rm dlx} xz \succ_{\rm dlx} y^2 \succ_{\rm dlx} yz \succ_{\rm dlx} z^2 \succ_{\rm dlx} x \succ_{\rm dlx} y \succ_{\rm dlx} z \\ x^2 \succ_{\rm drl} xy \succ_{\rm drl} y^2 \succ_{\rm drl} xz \succ_{\rm drl} yz \succ_{\rm drl} z^2 \succ_{\rm drl} x \succ_{\rm drl} y \succ_{\rm drl} z \end{gathered}$$ ◇

Quite often the order of the variables in $\mathbb{K}[x_1,\dots,x_n]$ is compatible with the monomial order in that $x_1\succ x_2\succ\cdots\succ x_n$.

A *term* is a product ax^α of a nonzero scalar $a\in\mathbb{K}^\times$ with a monomial x^α. Any monomial order $\succ$ extends to terms by setting $ax^\alpha\succ bx^\beta$ if $x^\alpha\succ x^\beta$ and $ab\neq 0$. We also write $ax^\alpha\succeq bx^\beta$ when $ab\neq0$ and $x^\alpha\succeq x^\beta$. This *term order* is not a partial order, for if $a\neq0$, then $ax^\alpha\succeq x^\alpha$ and $x^\alpha\succ ax^\alpha$, but these are not equal when $a\neq1$. This term order is however *well-founded* in that it does not admit an infinite strictly decreasing chain. By convention 0 is the $\succ$-minimal term.

The *initial term* $\text{in}_\succ(f)$ of a polynomial $f\in\mathbb{K}[x_1,\dots,x_n]$ is the term of f that is maximal with respect to $\succ$. If $\succ$ is lexicographic order with $x\succ y$, then

$$\text{in}_\succ(3x^3y - 7x^2y^{11} + 13y^{31}) \;=\; 3x^3y\,.$$

When $\succ$ is understood, we may write in(f). In Exercise 9, you will show that taking initial terms is multiplicative, which is a consequence of (ii) in Definition 2.2.3, that $\succ$ respects the multiplication of monomials.

EXAMPLE 2.2.7. The initial terms of a polynomial f with a weighted partial order $\succ_w$ have a geometric interpretation in terms of the Newton polytope (see Section A.1.1) of f. For example, suppose that f is

$$x^2 + 2x^3 + 3y + 5x^2y + 7y^2 + 11xy^2 + 13x^2y^2 + 17y^3 + 19xy^3 + 23y^4 .$$

Figure 2.2.2 shows the exponent vectors of terms of f, along with their convex hull, Newton polygon of f. Then $\text{in}_{(1,1)} f = 13x^2y^2 + 19xy^3 + 23y^4$, the terms of f of total degree 4. Also, $\text{in}_{(2,1)} f = 2x^3 + 13x^2y^2$. Other choices for $w \in \mathbb{R}^2_{\geq}$ give a single term of f, as shown on the right in Figure 2.2.2, where we label the cones with the corresponding terms. ◇

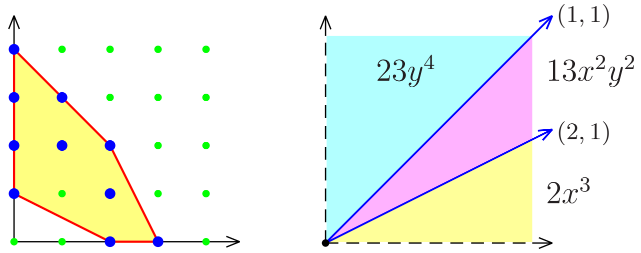


FIGURE 2.2.2. Newton polygon and weights.

The *initial ideal* $\text{in}_\succ(I)$ (or in(I)) of an ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is the ideal generated by the initial terms of polynomials in I,

$$\text{in}_\succ(I) \;=\; \langle \text{in}_\succ(f) \mid f \in I \rangle .$$

This is a monomial ideal, and observe that every monomial in $\text{in}_\succ(I)$ arises as $\text{in}_\succ(f)$ for some $f \in I$.

We make the most important definition of this section.

DEFINITION 2.2.8. Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal and $\succ$ a monomial order. A set $G \subset I$ is a *Gröbner basis* for I with respect to the monomial order $\succ$ if the initial ideal $\text{in}_\succ(I)$ is generated by the initial terms of polynomials in G, that is, if

$$\text{in}_\succ(I) \;=\; \langle \text{in}_\succ(g) \mid g \in G \rangle .$$

Notice that if G is a Gröbner basis and $G \subset G'$, then G' is also a Gröbner basis. Note also that I is a Gröbner basis for I, and every Gröbner basis contains a finite subset that is also a Gröbner basis, by Dickson's Lemma.

We justify our use of the term 'basis' in 'Gröbner basis'.

LEMMA 2.2.9. *If G is a Gröbner basis for I with respect to a monomial order $\succ$, then G generates I.*

Proof. Let $f \in I$. Since $\{\mathrm{in}(g) \mid g \in G\}$ generates $\mathrm{in}(I)$, there is a polynomial $g \in G$ whose initial term $\mathrm{in}(g)$ divides the initial term $\mathrm{in}(f)$ of f. Thus there is some term ax^α so that

$$\mathrm{in}(f) \;=\; ax^\alpha\,\mathrm{in}(g) \;=\; \mathrm{in}(ax^\alpha g)\,,$$

as $\succ$ respects multiplication. If we set $f_1 := f - cx^\alpha g$, then $\mathrm{in}(f) \succ \mathrm{in}(f_1)$ and $f_1 \in I$.

We will prove the lemma by induction on $\mathrm{in}(f)$ for $f \in I$. Suppose first that $f \in I$ is a polynomial whose initial term $\mathrm{in}(f)$ is the $\succ$-minimal monomial in $\mathrm{in}(I)$. As $\mathrm{in}(f) \succ \mathrm{in}(f_1)$ and $f_1 \in I$, we must have that $f_1 = 0$, by the minimality of $\mathrm{in}(f)$. Thus $f \in \langle G\rangle$. Suppose now that $I \neq \langle G\rangle$, and let $f \in I$ be a polynomial with $\mathrm{in}(f)$ is $\succ$-minimal among all $f \in I \smallsetminus \langle G\rangle$. But then $f_1 = f - cx^\alpha g \in I$ and as $\mathrm{in}(f) \succ \mathrm{in}(f_1)$, we must have that $f_1 \in \langle G\rangle$, which implies that $f \in \langle G\rangle$, a contradiction. □

An immediate consequence of Dickson's Lemma and Lemma 2.2.9 is the following Gröbner basis version (strengthening) of the Hilbert Basis Theorem.

Theorem 2.2.10 (Hilbert Basis Theorem). *Every ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ has a finite Gröbner basis with respect to any given monomial order.*

Example 2.2.11. Different monomial orderings give different Gröbner bases, and the sizes of the Gröbner bases can vary. Consider the ideal generated by the three polynomials

$$xy^3 + xz^3 + x - 1, \quad yz^3 + yx^3 + y - 1, \quad zx^3 + zy^3 + z - 1$$

In the degree reverse lexicographic order, where $x \succ y \succ z$, this has a Gröbner basis

$$\begin{array}{l}
x^3z + y^3z + z - 1,\\
xy^3 + xz^3 + x - 1,\\
x^3y + yz^3 + y - 1,\\
y^4z - yz^4 - y + z,\\
2xyz^4 + xyz + xy - xz - yz,\\
2y^3z^3 - x^3 + y^3 + z^3 + x^2 - y^2 - z^2,\\
y^6 - z^6 - y^5 + y^3z^2 - 2x^2z^3 - y^2z^3 + z^5 + y^3 - z^3 - x^2 - y^2 + z^2 + x,\\
x^6 - z^6 - x^5 - y^3z^2 - x^2z^3 - 2y^2z^3 + z^5 + x^3 - z^3 - x^2 - y^2 + y + z,\\
2z^7+4x^2z^4+4y^2z^4-2z^6+3z^4-x^3-y^3+3x^2z+3y^2z-2z^3+x^2+y^2-2xz-2yz-z^2+z-1,\\
2yz^6 + y^4 + 2yz^3 + x^2y - y^3 + yz^2 - 2z^3 + y - 1,\\
2xz^6 + x^4 + 2xz^3 - x^3 + xy^2 + xz^2 - 2z^3 + x - 1,
\end{array}$$

consisting of 11 polynomials with largest coefficient 4 and highest degree 7. If we consider instead the lexicographic monomial order, then this ideal has a larger Gröbner basis

$$\begin{array}{l}
64z^{34} - 64z^{33} + 384z^{31} - 192z^{30} - 192z^{29} + 1008z^{28} + 48z^{27} - 816z^{26} + 1408z^{25} + 976z^{24}\\
-1296z^{23} + 916z^{22} + 1964z^{21} - 792z^{20} - 36z^{19} + 1944z^{18} + 372z^{17} - 405z^{16} + 1003z^{15}\\
+879z^{14} - 183z^{13} + 192z^{12} + 498z^{11} + 7z^{10} - 94z^9 + 78z^8 + 27z^7 - 47z^6 - 31z^5 + 4z^3\\
-3z^2 - 4z - 1,
\end{array}$$

$$\begin{array}{l}
64yz^{21} + 288yz^{18} + 96yz^{17} + 528yz^{15} + 384yz^{14} + 48yz^{13} + 504yz^{12} + 600yz^{11} + 168yz^{10}\\
+200yz^9 + 456yz^8 + 216yz^7 + 120yz^5 + 120yz^4 - 8yz^2 + 16yz + 8y - 64z^{33} + 128z^{32}\\
-128z^{31} - 320z^{30} + 576z^{29} - 384z^{28} - 976z^{27} + 1120z^{26} - 144z^{25} - 2096z^{24} + 1152z^{23}\\
+784z^{22} - 2772z^{21} + 232z^{20} + 1520z^{19} - 2248z^{18} - 900z^{17} + 1128z^{16} - 1073z^{15} - 1274z^{14}\\
+229z^{13} - 294z^{12} - 966z^{11} - 88z^{10} - 81z^9 - 463z^8 - 69z^7 + 26z^6 - 141z^5 - 32z^4 + 24z^3
\end{array}$$

$-12z^2 - 11z + 1$

$$\begin{gathered}
589311934509212912y^2 - 1178623869018425824 0yz^{20} - 9428990952147406592yz^{19} \\
-2357247738036851648yz^{18} - 4832357862975545878 4yz^{17} - 48323578629755458784yz^{16} \\
-20036605773313239008yz^{15} - 81914358896780594768yz^{14} - 97825781128529343392yz^{13} \\
-53038074105829162080yz^{12} - 78673143256979923752yz^{11} - 99888372899311588584yz^{10} \\
-63645688926994994496yz^9 - 37126651874080413456yz^8 - 43903739120936361944yz^7 \\
-34474748168788955352yz^6 - 9134334984892800136yz^5 - 5893119345092129120yz^4 \\
-4125183541564490384yz^3 - 1178623869018425824yz^2 - 2062591770782245192yz \\
-1178623869018425824y + 4666564515534984633 6z^{33} - 5256138633033865068 8z^{32} \\
+25195872352020329920z^{31} + 28156769162372952723 2z^{30} - 19392177430724378694 4z^{29} \\
-22383823960598695936z^{28} + 81706533724600969099 2z^{27} - 16308104685758723524 8z^{26} \\
-42770559036883403033 6z^{25} + 13905781683718208538 08z^{24} + 39000434368484674580 8z^{23} \\
-98032219788785598166 4z^{22} + 13454251172212979738 76z^{21} + 12879560659390367316 76z^{20} \\
-95338316228249822884 4z^{19} + 63120234731058122985 6z^{18} + 17043019678692273960 24z^{17} \\
-1552085677865551499 88z^{16} - 1676406686225739650 5z^{15} + 1257475403277150700 961z^{14} \\
+5266859689013671695 98z^{13} - 1647515300005562648 80z^{12} + 4912495316392756540 50z^{11} \\
+4571263088711868823 06z^{10} - 8700839618951356274 7z^9 + 1580376890718582875 0z^8 \\
+1393206815639441012 73z^7 - 1735591958638331796 1z^6 - 5077736523391081905 4z^5 \\
-4630862847055988750z^4 + 8085080238139562826z^3 + 1366850803924776890z^2 \\
-3824545208919673161z - 2755936363893486164,
\end{gathered}$$

$$\begin{gathered}
589311934509212912x + 589311934509212912y - 8796637839650931859 2z^{33} \\
+1333834025316714664 96z^{32} - 5911531214172776755 2z^{31} - 5069268076485932801 28z^{30} \\
+5221417718101723342 72z^{29} + 4828643400945003264 0z^{28} - 1434725988338736388 752z^{27} \\
+6299718117668695917 12z^{26} + 9179860027743916652 64z^{25} - 2389871198974843205 136z^{24} \\
-2469823148310669418 88z^{23} + 2038968926105271519 536z^{22} - 2174896389643343086 620z^{21} \\
-1758138782546221156 976z^{20} + 2025390185406562798 552z^{19} - 7745426414203638283 64z^{18} \\
-2365390641451278278 484z^{17} + 6278248355593633049 92z^{16} + 3984846332328591159 07z^{15} \\
-1548683110130934220 322z^{14} - 5001926667100915104 19z^{13} + 5519214279984747585 10z^{12} \\
-4903687943451022864 10z^{11} - 4805040048418990573 84z^{10} + 2205140074544011756 15z^9 \\
+3851598490198004730 5z^8 - 1366443016356866846 09z^7 + 1741071269413252079 4z^6 \\
+5872455235409422580 3z^5 + 1570234197189530735 6z^4 - 7440058907697789332z^3 \\
-1398341089468668912z^2 + 3913205630531612397z + 2689145244006168857,
\end{gathered}$$

consisting of 4 polynomials with largest degree 34 and significantly larger coefficients. ◇

Exercises for Section 2.2.

1. Prove the equivalence of conditions (i) and (ii) in Definition 2.2.1.
2. Show that the radical of a monomial ideal is a monomial ideal, and that a monomial ideal is radical if and only if it is square-free. (Square-free means that in each of its minimal generators no variable occurs to a power greater than 1.)
3. Show that the elements of a monomial ideal I which are minimal with respect to division form a minimal set of generators of I in that they generate I and are a subset of any monomial generating set of I.

4. Let $I \subset \mathbb{K}[x_1,\dots,x_n]$ be a monomial ideal. Show that the set $S(I) := \{x^\alpha \mid x^\alpha \notin I\}$ of monomials not in I forms a vector space basis for $\mathbb{K}[x_1,\dots,x_n]/I$.
5. Which of the polynomials $x^3z - xz^3$, $x^2yz - y^2z^2 - x^2y^2$, and/or $x^2y - x^2z + y^2z$ lies in the ideal
$$\langle x^2y{-}xz^2{+}y^2z,\ y^2{-}xz{+}yz\rangle\ ?$$
6. Using Definition 2.2.1, show that a monomial order is a linear extension of the divisibility partial order on monomials.
7. Show that each of the order relations $\succ_{\rm lex}$, $\succ_{\rm dlx}$, and $\succ_{\rm drl}$, are monomial orders.
8. Show that if the coordinates of $w \in \mathbb{R}^n_>$ are linearly independent over $\mathbb{Q}$, then $\succ_w$ is a monomial order. Show that each of $\succ_{\rm lex}$, $\succ_{\rm dlx}$, and $\succ_{\rm drl}$ are weighted orders, by giving a sequence of weights $w_1,\dots,w_m \in \mathbb{R}^n$ where w_i is used to break any ties among $w_1,\dots,w_{i-1}$.
9. Suppose that $\succ$ is a monomial order. Prove that for any two nonzero polynomials f, g, we have $\mathrm{in}_\succ(fg) = \mathrm{in}_\succ(f)\,\mathrm{in}_\succ(g)$.
10. Show that if an ideal I has a square-free initial ideal, then I is radical. Give an example to show that the converse of this statement is false.
11. Show that for a monomial order $\succ$, $\mathrm{in}(I)\,\mathrm{in}(J) \subset \mathrm{in}(IJ)$ for any two ideals I and J. Find I and J such that the inclusion is proper.

2.3. Algorithmic aspects of Gröbner bases

Many practical algorithms to study and manipulate ideals and varieties are based on Gröbner bases. The foundations for algorithms involving Gröbner bases are the multivariate division algorithm and Buchberger's algorithm to compute Gröbner bases.

Both steps in the algorithm for ideal membership in one variable rely on the same elementary procedure: using a polynomial of low degree to simplify a polynomial of higher degree. This same procedure was also used in the proof of Lemma 2.2.9. This leads to the *multivariate division algorithm*, which is a cornerstone of the theory of Gröbner bases.

ALGORITHM 2.3.1 (Multivariate division algorithm).
INPUT: Polynomials $g_1,\dots,g_m, f$ in $\mathbb{K}[x_1,\dots,x_n]$ and a monomial order $\succ$.
OUTPUT: Polynomials $q_1,\dots,q_m$ and r such that

$$f \;=\; q_1g_1 + q_2g_2 + \cdots + q_mg_m + r\,, \tag{2.3.1}$$

where $\mathrm{in}(f) \succeq \mathrm{in}(r)$, no term of r is divisible by an initial term of any polynomial g_i, and $\mathrm{in}(f) \succeq \mathrm{in}(q_ig_i)$, for each $i = 1,\dots,m$.
INITIALIZE: Set $r := f$ and $q_1 := 0, \dots, q_m := 0$. Perform the following steps.

(1) If no term of r is divisible by an initial term of some g_i, then exit.
(2) Otherwise, let ax^α be the largest (with respect to $\succ$) term of r divisible by some $\mathrm{in}(g_i)$. Choose j minimal such that $\mathrm{in}(g_j)$ divides x^α and set $bx^\beta := ax^\alpha/\mathrm{in}(g_j)$. Replace r by $r - bx^\beta g_j$ and q_j by $q_j + bx^\beta$, and return to step (1).

PROOF OF CORRECTNESS. Each iteration of (2) is a *reduction* of r by the polynomials $g_1,\dots,g_m$. With each reduction, the largest term in r divisible by some $\mathrm{in}(g_i)$ decreases with respect to $\succ$. Since the term order $\succ$ is well-founded, the algorithm terminates after a finite number of steps. Every time the algorithm executes step (1), condition (2.3.1) holds. We also always have $\mathrm{in}(f) \succeq \mathrm{in}(r)$ because it holds initially, and with every reduction any new terms of r are less than the term that was canceled. Lastly, $\mathrm{in}(f) \succeq \mathrm{in}(q_i g_i)$ holds, because $\mathrm{in}(q_i g_i)$ is a term of r in some previous step of the algorithm. □

Given a list $G = (g_1, \ldots, g_m)$ of polynomials and a polynomial f, let r be the remainder obtained by the multivariate division algorithm applied to G and f. Since $f - r$ lies in the ideal generated by G, we write $f \bmod G$ for this remainder r. While $f \bmod G$ depends on the monomial order $\succ$, in general it will also depend upon the order of the polynomials $(g_1, \ldots, g_m)$. For example, in the degree lexicographic order

$$\begin{array}{rcl} x^2y \ \bmod \ (x^2,\, xy + y^2) & = & 0\,, \qquad \text{but} \\ x^2y \ \bmod \ (xy + y^2,\, x^2) & = & y^3\,. \end{array}$$

Thus we cannot reliably use the multivariate division algorithm to test when f is in the ideal generated by G. However, this does not occur when G is a Gröbner basis.

Lemma 2.3.2 (Ideal membership test). *Let G be a finite Gröbner basis for an ideal I with respect to a monomial order $\succ$. Then a polynomial $f \in I$ if and only if $f \bmod G = 0$.*

Proof. Set $r := f \bmod G$. If $r = 0$, then $f \in I$. Suppose $r \neq 0$. Since no term of r is divisible any initial term of a polynomial in G, its initial term $\mathrm{in}(r)$ is not in the initial ideal of I, as G is a Gröbner basis for I. But then $r \notin I$, and so $f \notin I$. □

Corollary 2.3.3. *A finite set G of polynomials is a Gröbner basis for the ideal $\langle G \rangle$ it generates if and only if for all $f \in \langle G \rangle$, $f \ \bmod G = 0$.*

When G is a Gröbner basis for an ideal I and $f \in \mathbb{K}[x_1, \ldots, x_n]$, no term of the remainder $f \bmod G$ lies in the initial ideal of I. A monomial x^α is standard if $x^\alpha \notin \mathrm{in}(I)$. The images of standard monomials in the ring $\mathbb{K}[x_1, \ldots, x_n]/\mathrm{in}(I)$ form a vector space basis, by Exercise 4 in Section **??**. Much more interesting is the following theorem.

Theorem 2.3.4. *Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal and $\succ$ a monomial order. Then the images of standard monomials in $\mathbb{K}[x_1, \ldots, x_n]/I$ form a vector space basis.*

Proof. Let G be a finite Gröbner basis for I with respect to $\succ$. Given a polynomial f, both f and $f \bmod G$ represent the same element of $\mathbb{K}[x_1, \ldots, x_n]/I$. Since $f \bmod G$ is a linear combination of standard monomials, the standard monomials span $\mathbb{K}[x_1, \ldots, x_n]/I$.

A linear combination f of standard monomials is zero in $\mathbb{K}[x_1, \ldots, x_n]/I$ only if $f \in I$. But then $\mathrm{in}(f)$ is both standard and lies in $\mathrm{in}(I)$, and so we conclude that $f = 0$. Thus the standard monomials are linearly independent in $\mathbb{K}[x_1, \ldots, x_n]/I$. □

By Theorem 2.3.4, if we have a monomial order $\succ$ and an ideal I, then for every polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$, there is a unique polynomial $\overline{f}$ which is a linear combination of standard monomials such that f and $\overline{f}$ have the same image in the quotient ring $\mathbb{K}[x_1, \ldots, x_n]/I$. Moreover, $\overline{f} = f \bmod G$, where G is any finite Gröbner basis of I with respect to the monomial order $\succ$, and thus $\overline{f}$ may be computed from f and G using the division algorithm. This unique representative $\overline{f}$ of f is called the *normal form* of

f modulo I and the division algorithm with a Gröbner basis for I is called *normal form reduction*.

A Gröbner basis enables computation in the quotient ring $\mathbb{K}[x_1,\dots,x_n]/I$ using the operations of the polynomial ring and linear algebra, by Theorem 2.3.4. Indeed, let G be a finite Gröbner basis for an ideal I with respect to a monomial order $\succ$ and suppose that $f,g\in\mathbb{K}[x_1,\dots,x_n]/I$ are in normal form, as a linear combination of standard monomials. Then $f+g$ is a linear combination of standard monomials and we can compute the product fg in the quotient ring as $fg \bmod G$, where the product is taken in the polynomial ring.

Theorem 2.2.10, which asserts the existence of a finite Gröbner basis, is purely existential. To use Gröbner bases, we need methods to detect and generate them. Such methods were given by Bruno Buchberger in his 1965 Ph.D. thesis.

A given set G of generators for an ideal will fail to be a Gröbner basis if the initial terms of the generators fail to generate the initial ideal. That is, if there are polynomials in the ideal whose initial terms are not divisible by the initial terms of the generators. A necessary step towards a Gröbner basis is some method to generate polynomials in the ideal with 'new' initial terms. This is the *raison d'etre* for the following definition.

Definition 2.3.5. The *least common multiple*, $\mathrm{lcm}\{ax^\alpha, bx^\beta\}$ of two terms ax^α and bx^β is the minimal monomial x^γ divisible by both x^α and x^β. Consequently, the exponent vector γ is the componentwise maximum of α and β.

Let $0\neq f,g\in\mathbb{K}[x_1,\dots,x_n]$ and suppose $\succ$ is a monomial order. The *S-polynomial* of f and g, $\mathrm{Spol}(f,g)$, is the polynomial linear combination of f and g,

$$\mathrm{Spol}(f,g) \ :=\ \frac{\mathrm{lcm}\{\mathrm{in}(f),\mathrm{in}(g)\}}{\mathrm{in}(f)}f \ -\ \frac{\mathrm{lcm}\{\mathrm{in}(f),\mathrm{in}(g)\}}{\mathrm{in}(g)}g\,.$$

Note that both terms in this expression have the same initial term, which is the monomial $\mathrm{lcm}\{\mathrm{in}(f),\mathrm{in}(g)\}$, so that we have $\mathrm{in}(\mathrm{Spol}(f,g))\prec\mathrm{lcm}\{\mathrm{in}(f),\mathrm{in}(g)\}$. ◇

Buchberger gave the following simple criterion to detect when a set G of polynomials is a Gröbner basis for the ideal $\langle G\rangle$ it generates.

Theorem 2.3.6 (Buchberger's Criterion). *A set G of polynomials is a Gröbner basis for the ideal $\langle G\rangle$ with respect to a monomial order $\succ$ if and only if for for all pairs $f,g\in G$,*

$$\mathrm{Spol}(f,g) \bmod G \ =\ 0\,.$$

Proof. First, observe that Buchberger's criterion is necessary. Suppose that G is a Gröbner basis for an ideal I with respect to $\succ$. Then for $f,g\in G$, their S-polynomial $\mathrm{Spol}(f,g)$ lies in I and the ideal membership test implies that $\mathrm{Spol}(f,g) \bmod G=0$.

For sufficiency, suppose that $G=\{g_1,\dots,g_m\}$ satisfies Buchberger's criterion and let I be the ideal generated by G. Let $f\in I$. We will show that there is some $g\in G$, such that $\mathrm{in}(f)$ is divisible by $\mathrm{in}(g)$. This implies that G is a Gröbner basis for I.

Given a list $h=(h_1,\dots,h_m)$ of polynomials in $\mathbb{K}[x_1,\dots,x_n]$, let $\mathrm{mm}(h)$ be the largest monomial appearing in one of $h_1g_1,\dots,h_mg_m$. This will be the monomial in at least one of the initial terms $\mathrm{in}(h_1g_1),\dots,\mathrm{in}(h_mg_m)$. Let $j(h)$ be the least index i for which $\mathrm{mm}(h)$ is the monomial of $\mathrm{in}(h_ig_i)$.

Consider lists $h = (h_1, \ldots, h_m)$ of polynomials with

$$f \;=\; h_1 g_1 + \cdots + h_m g_m \tag{2.3.2}$$

for which $\mathrm{mm}(h)$ minimal among all lists satisfying (2.3.2). Of these, let h be a list with $j := j(h)$ maximal. We claim that $\mathrm{mm}(h)$ is the monomial underlying $\mathrm{in}(f)$, which implies that $\mathrm{in}(g_j)$ divides $\mathrm{in}(f)$, and completes the proof.

To prove the claim, we assume that it does not hold. Then $\mathrm{mm}(h) \succ \mathrm{in}(f)$, and thus the initial term $\mathrm{in}(h_j g_j)$ is canceled in the sum (2.3.2). Thus there is some index $k \neq j$ such that $\mathrm{mm}(h)$ is a monomial in $h_k g_k$. Since $\mathrm{mm}(h)$ is the maximal monomial appearing in $h_1 g_1, \ldots, h_m g_m$, it is the maximal monomial in $g_k h_k$, and thus is the monomial underlying $\mathrm{in}(h_k g_k)$. Since $j = j(h)$ is the least index i such that $\mathrm{mm}(h)$ underlies $\mathrm{in}(h_i g_i)$, we have $j < k$. Let $x^\beta := \mathrm{lcm}\{\mathrm{in}(g_j), \mathrm{in}(g_k)\}$, the monomial which is canceled in $\mathrm{Spol}(g_j, g_k)$. Since $\mathrm{in}(g_k)$ divides $\mathrm{mm}(h)$, it divides $\mathrm{in}(h_j g_j)$ and thus x^β divides $\mathrm{in}(h_j g_j)$. Let $a x^\alpha$ be the term such that $a x^\alpha x^\beta = \mathrm{in}(h_j g_j) = \mathrm{in}(h_j) \cdot \mathrm{in}(g_j)$. Set $c x^\gamma := \mathrm{in}(h_j g_j) / \mathrm{in}(g_k)$. Then

$$a x^\alpha \mathrm{Spol}(g_j, g_k) \;=\; a x^\alpha \frac{x^\beta}{\mathrm{in}(g_j)} g_j \;-\; a x^\alpha \frac{x^\beta}{\mathrm{in}(g_k)} g_k \;=\; \mathrm{in}(h_j) g_j \;-\; c x^\gamma g_k \,. \tag{2.3.3}$$

By the construction of $\mathrm{Spol}(g_j, g_k)$, the initial terms of $\mathrm{in}(h_j) g_j$ and $c x^\gamma g_k$ cancel in (2.3.3). Since $\mathrm{mm}(h)$ is the monomial underlying $\mathrm{in}(h_j g_j) = \mathrm{in}(\mathrm{in}(h_j) g_j)$, and these initial terms cancel, we have $\mathrm{in}(a x^\alpha \mathrm{Spol}(g_j, g_k)) \prec \mathrm{mm}(h)$. By Buchberger's criterion for G, there are polynomials $q_1, \ldots, q_m$ with

$$\mathrm{Spol}(g_j, g_k) \;=\; q_1 g_1 + \cdots + q_m g_m \,,$$

and we may assume that $\mathrm{in}(q_i g_i) \preceq \mathrm{in}(\mathrm{Spol}(g_j, g_k)) \prec x^\beta$, by the Division Algorithm and the construction of $\mathrm{Spol}(g_j, g_k)$.

Define a new list $h' = (h'_1, \ldots, h'_m)$ of polynomials where

$$h'_i \;:=\; \left\{ \begin{array}{rl} h_i + a x^\alpha q_i & \quad i \neq j, k \\ h_j + a x^\alpha q_j - \mathrm{in}(h_j) & \quad i = j \\ h_k + a x^\alpha q_k + c x^\gamma & \quad i = k \end{array} \right. \,.$$

Consider the sum $\sum h'_i g_i$, which is

$$\begin{aligned} &\sum_i h_i g_i + \Bigl(a x^\alpha \sum_i q_i g_i \Bigr) - \mathrm{in}(h_j) g_j + c x^\gamma g_k \\ &\qquad\qquad \;=\; f + a x^\alpha \mathrm{Spol}(g_j, g_k) - a x^\alpha \mathrm{Spol}(g_j, g_k) \;=\; f \,, \end{aligned}$$

so h' is a list satisfying (2.3.2).

We have $\mathrm{in}(q_i g_i) \preceq \mathrm{in}(\mathrm{Spol}(g_j, g_k)) \prec x^\beta$, so $\mathrm{in}(a x^\alpha q_i g_i) \prec x^\alpha x^\beta = \mathrm{mm}(h)$. This implies that $\mathrm{in}(h'_i g_i) \preceq \mathrm{in}(h_i g_i)$ for every $i = 1, \ldots, m$, and thus $\mathrm{mm}(h') \preceq \mathrm{mm}(h) = \max\{\mathrm{in}(h_i g_i) \mid i = 1, \ldots, m\}$. By the minimality of $\mathrm{mm}(h)$, we have $\mathrm{mm}(h') = \mathrm{mm}(h)$. Since

$$\begin{aligned} \mathrm{in}(h'_j g_j) &\;=\; \mathrm{in}((h_j + a x^\alpha q_j - \mathrm{in}(h_j)) \cdot g_j) \\ &\;=\; \max\bigl\{\mathrm{in}(x^\alpha q_j g_j)\,,\, \mathrm{in}((h_j - \mathrm{in}(h_j)) g_j)\bigr\} \;\prec\; \mathrm{in}(h_j g_j)\,. \end{aligned}$$

Thus $j(h) = j < j(h')$, which contradicts our choice of h. □

Buchberger's algorithm to compute a Gröbner basis begins with a list of polynomials and augments that list by adding reductions of S-polynomials. It halts when the list of polynomials satisfies Buchberger's Criterion.

ALGORITHM 2.3.7 (Buchberger's Algorithm). Let $G = (g_1, \dots, g_m)$ be generators for an ideal I and $\succ$ a monomial order. For each $1 \leq i < j \leq m$, let $h_{ij} := \mathrm{Spol}(g_i, g_j) \bmod G$. If each reduction vanishes, so that $\mathrm{Spol}(g_i, g_j) \bmod G = 0$ for each $1 \leq i < j \leq m$, then by Buchberger's Criterion, G is a Gröbner basis for I with respect to $\succ$. Otherwise append all the nonzero h_{ij} to the list G and repeat this process.

PROOF OF CORRECTNESS. Let $J(G) := \langle \mathrm{in}(g) \mid g \in G \rangle$, the monomial ideal generated by the initial terms of polynomials in G. If there is a pair $g_i, g_j \in G$ such that $0 \neq h_{ij} := \mathrm{Spol}(g_i, g_j) \bmod G$ and $G' \subset G \cup \{h_{ij}\}$, then $J(G') \supsetneq J(G)$. Since there does not exist an infinite ascending chain of monomial ideals (as we showed in Dickson's Lemma), the algorithm will only find finitely many such nonzero reductions h_{ij} of S-polynomials and therefore must halt. □

Since the manipulations in Buchberger's algorithm involve only algebraic operations using the coefficients of the input polynomials, we deduce the following corollary. Let $\Bbbk$ be any subfield of $\mathbb{K}$.

COROLLARY 2.3.8. *Let $f_1, \dots, f_m \in \Bbbk[x_1, \dots, x_n]$ be polynomials and $\succ$ a monomial order. Then there is a Gröbner basis $G \subset \Bbbk[x_1, \dots, x_n]$ for the ideal $\langle f_1, \dots, f_m \rangle$ in $\mathbb{K}[x_1, \dots, x_n]$ with respect to the monomial order $\succ$.*

EXAMPLE 2.3.9. Consider applying the Buchberger algorithm to $G = (x^2, xy + y^2)$ with any monomial order where $x \succ y$. First

$$\mathrm{Spol}(x^2, xy + y^2) \;=\; y \cdot x^2 - x(xy + y^2) \;=\; -xy^2 \,.$$

Then

$$-xy^2 \bmod (x^2, xy + y^2) \;=\; -xy^2 + y(xy + y^2) \;=\; y^3 \,.$$

Since all S-polynomials of $(x^2, xy + y^2, y^3)$ reduce to zero, this is a Gröbner basis. ◇

Among the polynomials h_{ij} computed at each stage of Buchberger's algorithm are those where one of $\mathrm{in}(g_i)$ or $\mathrm{in}(g_j)$ divides the other. Suppose that $\mathrm{in}(g_i)$ divides $\mathrm{in}(g_j)$ with $i \neq j$. Then $\mathrm{Spol}(g_i, g_j) = g_j - ax^\alpha g_i$, where ax^α is some term. This has strictly smaller initial term than does g_j and so we never use g_j to compute $h_{ij} := \mathrm{Spol}(g_i, g_j) \bmod G$. It follows that $g_j - h_{ij}$ lies in the ideal generated by $G \smallsetminus \{g_j\}$, and so we may replace g_j by h_{ij} in G without changing the ideal generated by G, and only possibly increasing the ideal generated by the initial terms of polynomials in G.

This gives the following elementary improvement to Buchberger's algorithm:

(2.3.4) In each step, initially compute h_{ij} for those $i \neq j$ where $\mathrm{in}(g_i)$ divides $\mathrm{in}(g_j)$, and replace g_j by h_{ij}.

In some cases this computes the Gröbner basis. Another improvement, identifying S-polynomials that reduce to zero and therefore need not be computed, is given in Exercise 4.

A Gröbner basis G is *reduced* if the initial terms of polynomials in G have coefficient 1 and if for each $g \in G$, no monomial of g is divisible by an initial term of another element of G. A reduced Gröbner basis for an ideal is uniquely determined by the monomial order. Reduced Gröbner bases are the multivariate analog of unique monic polynomial generators of ideals in the univariate polynomial ring $\mathbb{K}[x]$. Elements g of a reduced Gröbner basis have the form,

$$x^\alpha - \sum_{\beta\in\mathcal{B}} a_\beta x^\beta\,, \tag{2.3.5}$$

where $x^\alpha = \text{in}(g)$ is the initial term and $\mathcal{B}$ consists of exponent vectors of standard monomials. This rewrites the nonstandard initial monomial in terms of standard monomials. In this way, a Gröbner basis is a system of rewriting rules for polynomials. A reduced Gröbner basis has one generator for every generator of the initial ideal.

Example 2.3.10. Let M be a $m \times n$ matrix which is the matrix of coefficients of m linear forms $g_1, \ldots, g_m$ in $\mathbb{K}[x_1, \ldots, x_n]$, and suppose that $x_1 \succ x_2 \succ \cdots \succ x_n$. We can apply (2.3.4) to two forms g_i and g_j when their initial terms have the same variable. Then the S-polynomial and subsequent reductions are equivalent to the steps in the algorithm of Gaussian elimination applied to the matrix M. If we iterate our applications of (2.3.4) until the initial terms of the forms g_i have distinct variables, then the forms $g_1, \ldots, g_m$ are a Gröbner basis for the ideal they generate.

If the forms g_i are a reduced Gröbner basis and are sorted in decreasing order according to their initial terms, then the resulting matrix $\overline{M}$ of their coefficients is an *echelon matrix*: The initial nonzero entry in each row is 1, it is the only nonzero entry in its column, and these columns increase with row number.

Gaussian elimination produces the same echelon matrix from M. Thus the Buchberger algorithm is a generalization of Gaussian elimination to nonlinear polynomials. ◇

The form (2.3.5) of elements in a reduced Gröbner basis G for an ideal I with respect to a given monomial order $\succ$ implies that G depends on the monomial ideal $\text{in}_\succ(I)$, and thus only indirectly on $\succ$. That is, if $\succ'$ is a second monomial order with $\text{in}_{\succ'}(I) = \text{in}_\succ(I)$, then G is also a Gröbner basis for I with respect to $\succ'$. While there are uncountably many monomial orders, any given ideal has only finitely many initial ideals.

Theorem 2.3.11. *An ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ has only finitely many initial ideals.*

Proof. Let $\text{In}(I)$ be the set of initial ideals of I. For each initial ideal M of I, choose a monomial order $\succ_M$ with $M = \text{in}_{\succ_M}(I)$. Let

$$T \;:=\; \{\succ_M \mid M \in \text{In}(I)\}$$

be this set of monomial orders, one for each initial ideal of I.

Suppose that $\text{In}(I)$ is infinite. Then T is infinite. Let $g_1, \ldots, g_m \in \mathbb{K}[x_1, \ldots, x_n]$ be generators for I. Since each polynomial g_i has only finitely many terms, there is an infinite subset T_0 of T with the property that any two monomial orders $\succ, \succ'$ in T_0 will select the same initial terms from each of the g_i,

$$\text{in}_\succ(g_i) \;=\; \text{in}_{\succ'}(g_i) \qquad \text{for } i = 1, \ldots, m\,.$$

Choose a term order $\succ$ from T_0. Set $M_0 := \langle \text{in}_\succ(g_1), \ldots, \text{in}_\succ(g_m)\rangle$, the monomial ideal generated by the initial terms of the polynomials $g_1, \ldots, g_m$. Note that M_0 depends only upon T_0 and not $\succ$. Either $(g_1,\dots,g_m)$ is a Gröbner basis for I with respect to $\succ$ or else there is a some polynomial g_{m+1} in I whose $\succ$-initial term does not lie in M_0. Replacing g_{m+1} by g_{m+1} mod $(g_1,\dots,g_m)$ (computed with respect to $\succ$), we may assume that g_{m+1} has no term in M_0.

Then there is an infinite subset T_1 of T_0 such that any two monomial orders $\succ,\succ'$ in T_1 will select the same initial term of g_{m+1}, $\mathrm{in}_\succ(g_{m+1})=\mathrm{in}_{\succ'}(g_{m+1})$. Choose a monomial order $\succ$ from T_1 and let M_1 be the monomial ideal generated by M_0 and $\mathrm{in}_\succ(g_{m+1})$. Again, M_1 depends only upon T_1 and not $\succ$. As before, either $(g_1,\dots,g_m,g_{m+1})$ is a Gröbner basis for I with respect to $\succ$, or else there is an element g_{m+2} of I having no term in M_1.

Continuing in this fashion constructs an increasing chain $M_0\subsetneq M_1\subsetneq\cdots$ of monomial ideals in $\mathbb{K}[x_1,\dots,x_n]$. By Dickson's Lemma, this process must terminate after finitely many, say r steps. At this point we will have an infinite subset T_r of T and polynomials $g_1,\dots,g_{m+r}$ that form a Gröbner basis for I with respect to a monomial order $\succ$ in T_r, with the property that for any other monomial order $\succ'$ in T_r, we have

$$\mathrm{in}_\succ(g_i) \;=\; \mathrm{in}_{\succ'}(g_i) \qquad \text{for } i=1,\dots,m{+}r\,.$$

But this implies that $\mathrm{in}_\succ(I)=\mathrm{in}_{\succ'}(I)$ is an initial ideal for two distinct monomial orders in the infinite set $T_r\subset T$, which contradicts the construction of the set T. □

Definition 2.3.12. A consequence of Theorem 2.3.11 that an ideal I has only finitely many initial ideals is that an ideal I has only finitely many reduced Gröbner bases. The union of this finite set of reduced Gröbner bases is a finite generating set for I that is a Gröbner basis for I with respect to any monomial order. Such a generating set is called a *universal Gröbner basis* for the ideal I.

Exercises for Section 2.3.

1. Describe how Buchberger's algorithm behaves when it computes a Gröbner basis from a list of monomials. What if we use the elementary improvement (2.3.4)?
2. Given an ideal I and a monomial order $\succ$, show that I has a reduced Gröbner basis with respect to $\succ$, and that the reduced Gröbner basis is unique.
3. Use Buchberger's algorithm to compute by hand the reduced Gröbner basis of $\langle y^2-xz+yz,\ x^2y-xz^2+y^2z\rangle$ in the degree reverse lexicographic order where $x\succ y\succ z$.
4. Let $f,g\in\mathbb{K}[x_1,\dots,x_n]$ be polynomials with relatively prime initial terms, and suppose that their initial coefficients are 1.
   (a) Show that
   $$\mathrm{Spol}(f,g) \;=\; -(g-\mathrm{in}(g))f+(f-\mathrm{in}(f))g\,.$$
   Deduce that the initial monomial of $\mathrm{Spol}(f,g)$ is a multiple of either the initial monomial of f or the initial monomial of g.
   (b) Analyze the steps of the reduction computing $\mathrm{Spol}(f,g)$ mod (f,g) using the division algorithm to show that this is zero.

   This gives another improvement to Buchberger's algorithm: avoid computing and reducing those S-polynomials of polynomials with relatively prime initial terms.
5. Prove that when $n>1$, there are uncountably many distinct monomial orderings for $\mathbb{K}[x_1,\dots,x_n]$.

6. Let U be a universal Gröbner basis for an ideal I in $\mathbb{K}[x_1,\ldots,x_n]$. Show that for every subset $Y \subset \{x_1,\ldots,x_n\}$ the elimination ideal $I \cap \mathbb{K}[Y]$ is generated by $U \cap \mathbb{K}[Y]$.
7. Let $\succ$ be any monomial order and G be a list of homogeneous polynomials. Then for any homogeneous polynomial f, its reduction modulo G is also homogeneous.

   Show that the reduced Gröbner basis computed by Buchberger's algorithm from G consists of homogeneous polynomials. Deduce that the reduced Gröbner basis of a homogeneous ideal consists of homogeneous polynomials.
8. Let I be a ideal generated by homogeneous linear polynomials. A nonzero linear form f in I is a *circuit* of I if f has minimal support (with respect to inclusion) among all polynomials in I. Prove that the set of all circuits of I is a universal Gröbner basis of I.
9. Let $I := \langle x^2+y^2, x^3+y^3\rangle \subset \mathbb{Q}[x,y]$ and suppose that the monomial order $\succ$ is the lexicographic order with $x \succ y$.
   (a) Show that $y^4 \in I$.
   (b) Show that the reduced Gröbner basis for I is $\{y^4, xy^2-y^3, x^2+y^2\}$.
   (c) Show that $\{x^2+y^2, x^3+y^3\}$ cannot be a Gröbner basis for I for any monomial ordering.
10. (a) Prove that the ideal $\langle x,y\rangle \subset \mathbb{Q}[x,y]$ is not a principal ideal.
    (b) Is $\langle x^2+y, x+y\rangle$ already a Gröbner basis with respect to some term ordering?
    (c) Use Buchberger's algorithm to compute by hand Gröbner bases of the ideal $I = \langle y-z^2, z-x^3\rangle \in \mathbb{Q}[x,y,z]$ with respect to the lexicographic and to the degree reverse lexicographic monomial orders.
11. Let $I \subset \mathbb{K}[x_0,\ldots,x_n]$ be a homogeneous ideal. Fix the degree reverse lexicographic order $\succ$ where $x_0 \succ x_1 \succ \cdots \succ x_n$ and let G be the reduced Gröbner basis of I. Show that the set

$$\{f \in G \mid x_n \text{ does not divide } f\} \ \cup\ \{f/x_n \mid f \in G \text{ and } x_n \text{ divides } f\}$$

    is a Gröbner basis of $(I : x_n)$. Show that a Gröbner basis of $(I : x_n^\infty)$ is obtained by dividing each element $f \in G$ by the highest power of x_n that divides f.

2.4. Solving equations with Gröbner bases

Algorithm 2.1.14 reduced the problem of solving two equations in two variables to that of solving univariate polynomials, using resultants to eliminate a variable and put the system into triangular form. For an ideal $I \subset \mathbb{K}[x_1,\ldots,x_n]$ whose variety $\mathcal{V}(I)$ consists of finitely many points, this same idea leads to an algorithm to compute $\mathcal{V}(I)$, provided we can compute the elimination ideals $I \cap \mathbb{K}[x_i]$. Gröbner bases provide a universal algorithm for computing elimination ideals. More generally, ideas from the theory of Gröbner bases can help to understand solutions to systems of equations.

Suppose that we have N polynomial equations in n variables $x_1,\ldots,x_n$

$$f_1(x_1,\ldots,x_n) \ =\ \cdots\ =\ f_N(x_1,\ldots,x_n) \ =\ 0\,, \tag{2.4.1}$$

and we want to understand the solutions to this system. By understand, we mean answering (any of) the following questions.

(i) Does (2.4.1) have finitely many solutions?
(ii) Can we count them, or give (good) upper bounds on their number?
(iii) Can we *solve* the system (2.4.1) and find all solutions?
(iv) When the polynomials have real coefficients, can we count (or bound) the number of real solutions to (2.4.1)? Or simply find them?

The solutions to (2.4.1) in $\mathbb{K}^n$ constitute the affine variety $\mathcal{V}(I)$, where I is the ideal generated by the polynomials $f_1, \dots, f_N$. Algorithms based on Gröbner bases to address Questions (i)-(iv) involve studying I. An ideal I is zero-dimensional if, over the algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$, $\mathcal{V}(I)$ is finite. Thus I is zero-dimensional if and only if its radical $\sqrt{I}$ is zero-dimensional.

Theorem 2.4.1. *An ideal $I \subset \mathbb{K}[x_1, \dots, x_n]$ is zero-dimensional if and only if the quotient ring $\mathbb{K}[x_1, \dots, x_n]/I$ is a finite-dimensional $\mathbb{K}$-vector space.*

When an ideal I is zero-dimensional, we will call the points of $\mathcal{V}(I)$ the roots of I.

Proof. We may assume the $\mathbb{K}$ is algebraically closed, as this does not change the dimension of quotient rings.

We prove this first in the case that I is radical. Then $I = \mathcal{I}(\mathcal{V}(I))$, by the Nullstellensatz and $\mathbb{K}[x_1, \dots, x_n]/I$ is the coordinate ring $\mathbb{K}[X]$ of $X := \mathcal{V}(I)$. This consists of all functions obtained by restricting polynomials to $\mathcal{V}(I)$, and is therefore a subring of the ring of functions on X. If X is finite, then $\mathbb{K}[X]$ is finite-dimensional as the space of functions on X has dimension equal to the number of points in X. Conversely, suppose that X is infinite. Then there is some coordinate, say x_1, such that the projection of X to the x_1-axis is infinite. In particular, no polynomial in x_1, except the zero polynomial, vanishes on X. Restriction of polynomials in x_1 to X is therefore an injective map from $\mathbb{K}[x_1] \hookrightarrow \mathbb{K}[X]$ which shows that $\mathbb{K}[X]$ is infinite-dimensional.

We complete the proof by showing that $\mathbb{K}[x_1, \dots, x_n]/I$ is finite-dimensional if and only if $\mathbb{K}[x_1, \dots, x_n]/\sqrt{I}$ is finite-dimensional. Let I be any ideal. If $\mathbb{K}[x_1, \dots, x_n]/I$ is finite-dimensional, then so is $\mathbb{K}[x_1, \dots, x_n]/\sqrt{I}$ as $I \subset \sqrt{I}$. For the other direction, suppose that $\mathbb{K}[x_1, \dots, x_n]/\sqrt{I}$ is finite-dimensional. For each variable x_i, there is some linear combination of $1, x_i, x_i^2, \dots$ which is zero in $\mathbb{K}[x_1, \dots, x_n]/\sqrt{I}$ and hence lies in $\sqrt{I}$. But this is a univariate polynomial $g_i(x_i) \in \sqrt{I}$, so there is some power $g_i(x_i)^{M_i}$ of g_i which lies in I. But then we have $\langle g_1(x_1)^{M_1}, \dots, g_n(x_n)^{M_n} \rangle \subset I$, and so the map

$$\mathbb{K}[x_1, \dots, x_n]/\langle g_1(x_1)^{M_1}, \dots, g_n(x_n)^{M_n} \rangle \quad \longrightarrow \quad \mathbb{K}[x_1, \dots, x_n]/I$$

is a surjection. But $\mathbb{K}[x_1, \dots, x_n]/\langle g_1(x_1)^{M_1}, \dots, g_n(x_n)^{M_n} \rangle$ has dimension $\prod_i M_i \deg(g_i)$, which implies that $\mathbb{K}[x_1, \dots, x_n]/I$ is finite-dimensional. □

A consequence of this proof is the following criterion for an ideal to be zero-dimensional.

Corollary 2.4.2. *An ideal $I \subset \mathbb{K}[x_1, \dots, x_n]$ is zero-dimensional if and only if for every variable x_i, there is a univariate polynomial $g_i(x_i)$ which lies in I.*

Together with Theorem 2.3.4, Theorem 2.4.1 leads to an algorithm to solve Question (i), based on Gröbner bases.

COROLLARY 2.4.3. *An ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is zero-dimensional if and only if for any monomial order $\succ$, the initial ideal $\mathrm{in}_\succ I$ of I contains some power of every variable.*

Thus we can determine if I is zero-dimensional and thereby answer Question (i) by computing a Gröbner basis for I and checking that the initial terms of elements of the Gröbner basis include pure powers of all variables.

When I is zero-dimensional, its *degree*, $\deg(I)$, is the dimension of $\mathbb{K}[x_1, \ldots, x_n]/I$ as a $\mathbb{K}$-vector space, which is the number of standard monomials, by Theorem 2.3.4. A Gröbner basis for I gives generators of the initial ideal which we can use to count the number of standard monomials to determine its degree.

When I is a zero-dimensional radical ideal and $\mathbb{K}$ is algebraically closed, the degree of I equals the number of points in $\mathcal{V}(I) \subset \mathbb{K}^n$ (see Exercise 3 from Section 1.3) and thus we obtain an answer to Question (ii).

THEOREM 2.4.4. *Let I be the ideal generated by the polynomials f_i of* (2.4.1)*. If I is zero-dimensional, then the number of solutions to the system* (2.4.1) *is bounded by the degree of I. When $\mathbb{K}$ is algebraically closed, the number of solutions is equal to this degree if and only if I is radical.*

In many important cases, there are sharp upper bounds for the number of isolated solutions to the system (2.4.1) which do not require a Gröbner basis. For example, Theorem 2.1.16 (Bézout's Theorem in the plane) gives such bounds when $N = n = 2$. Suppose that $N = n$ so that the number of equations equals the number of variables. This is called a *square system*. Bézout's Theorem in the plane has a natural extension in this case, which we will prove in Section **??**. A common solution a to a square system of equations is *simple* if the differentials of the equations are linearly independent at a.

THEOREM 2.4.5 (Bézout's Theorem). *Given polynomials $f_1, \ldots, f_n \in \mathbb{K}[x_1, \ldots, x_n]$ with $d_i = \deg(f_i)$, the number of simple solutions to the system*

$$f_1(x_1, \ldots, x_n) \;=\; \cdots \;=\; f_n(x_1, \ldots, x_n) \;=\; 0$$

in $\mathbb{K}^n$ is at most $d_1 \cdots d_n$. When $\mathbb{K}$ is algebraically closed, this is a bound for the number of isolated solutions, and it is attained for generic choices of the polynomials f_i.

This product of degrees $d_1 \cdots d_n$ is the *Bézout bound* for such a system. While sharp for generic square systems, few practical problems involve generic systems and other bounds are often needed (see Exercise 5). We study such bounds in Chapter **??**, where we establish the polyhedral bounds of Kushnirenko's and Bernsteins's Theorems.

We discuss a symbolic method to solve systems of polynomial equations (2.4.1) based upon elimination theory and the Shape Lemma, which describes an optimal form of a Gröbner basis of a zero-dimensional ideal I with respect to a lexicographic monomial order. Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal. A univariate polynomial $g(x_i)$ is an *eliminant for I* if g generates the elimination ideal $I \cap \mathbb{K}[x_i]$.

THEOREM 2.4.6. *Suppose that $g(x_i)$ is an eliminant for an ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$. Then $g(a_i) = 0$ for every $a = (a_1, \ldots, a_n) \in \mathcal{V}(I) \in \mathbb{K}^n$. When $\mathbb{K}$ is algebraically closed, every root of g is the ith coordinate of a point of $\mathcal{V}(I)$.*

Proof. Let $a \in \mathcal{V}(I)$. Then $g(a_i) = 0$ as this is the value of g at the point a. Suppose that $\mathbb{K}$ is algebraically closed and that ξ is a root of $g(x_i)$ but there is no point $a \in \mathcal{V}(I)$ whose ith coordinate is ξ. Let $h(x_i)$ be a polynomial whose roots are the other roots of g. Then h vanishes on $\mathcal{V}(I)$ and so $h \in \sqrt{I}$. But then some power, h^N, of h lies in I. Thus $h^N \in I \cap \mathbb{K}[x_i] = \langle g \rangle$. But this is a contradiction as $h(\xi) \neq 0$ while $g(\xi) = 0$. □

Theorem 2.4.7. *If $g(x_i)$ is a monic eliminant for an ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$, then g lies in the reduced Gröbner basis for I with respect to any monomial order in which the pure powers x_i^m of x_i precede variables x_j with $j \neq i$.*

Proof. Suppose that $\succ$ is such a monomial order. Then its minimal monomials are $1, x_i, x_i^2, \ldots$. Since g generates the elimination ideal $I \cap \mathbb{K}[x_i]$, it is the lowest degree monic polynomial in x_i lying in I. As $g \in I$, we have that $x_i^{\deg(g)} \in \mathrm{in}_\prec(I)$. Let x_i^m be the generator of $\mathrm{in}_\prec(I) \cap \mathbb{K}[x_i]$. Then $m \leq \deg(g)$. Let f be the polynomial in the reduced Gröbner basis of I with respect to $\prec$ whose initial term is x_i^m. Then its remaining terms involve smaller standard monomials and are thus pure powers of x_i. We conclude that $f \in I \cap \mathbb{K}[x_i] = \langle g \rangle$, and so g divides f, so $m = \deg(g)$. As $f - g$ is a polynomial in x_i which lies in I but has degree less than $\deg(g)$, the minimality of f and g implies that $f - g = 0$. This proves that g lies in the reduced Gröbner basis. □

The following theorem relating Gröbner bases and elimination ideals is proven in the exercises.

Theorem 2.4.8. *Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal and let $\prec$ be the lexicographic monomial order with $x_1 \prec x_2 \prec \cdots \prec x_n$ and suppose that G is a Gröbner basis for I with respect to $\prec$. Then, for each $m = 1, \ldots, n$, the polynomials in G that lie in $\mathbb{K}[x_1, \ldots, x_m]$ form a Gröbner basis for the elimination ideal $I_m = I \cap \mathbb{K}[x_1, \ldots, x_m]$.*

These theorems give an algorithm to compute eliminants—simply compute a lexicographic Gröbner basis. This is not recommended, as lexicographic Gröbner bases appear to be the most expensive to compute. As we saw in Example 2.2.11, their size can be significantly larger than other Gröbner bases. It is even expensive to compute a univariate eliminant $g(x_i)$ using an *elimination order*, (a monomial order $\prec$ where any pure power x_i^d of x_i precedes any monomial involving any other variable x_j for $j \neq i$ as in Theorem 2.4.7). We instead offer the following algorithm.

Algorithm 2.4.9.
Input: A zero-dimensional ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ and a variable x_i.
Output: A univariate eliminant $g(x_i) \in I$.

(i) Compute a Gröbner basis G for I with respect to any monomial order.
(ii) Compute the sequence $1 \bmod G$, $x_i \bmod G$, $x_i^2 \bmod G$, …, until a linear dependence is found,

$$\sum_{j=0}^{m} a_j (x_i^j \bmod G) \;=\; 0\,, \tag{2.4.2}$$

where m is minimal. Then

$$g(x_i) \;=\; \sum_{j=0}^{m} a_j x_i^j$$

is a univariate eliminant.

Proof of correctness. Since I is zero-dimensional, by Corollary 2.4.2 it has an eliminant $g(x_i) \in I$. If $g = \sum_{i=0}^{N} b_j x_i^j$ then by the ideal membership test (Lemma 2.3.2),

$$0 \;=\; g \bmod G \;=\; \Big(\sum_{j=0}^{N} b_j x_i^j\Big) \bmod G \;=\; \sum_{j=0}^{N} b_j (x_i^j \bmod G)\,,$$

which is a linear dependence among the elements of the sequence 1 mod G, x_i mod G, x_i^2 mod G, ... Thus the algorithm halts during Step (2). The minimality of the degree of g implies that $N = m$ and the uniqueness of such minimal linear combinations implies that the coefficients b_j and a_j are proportional, which shows that the algorithm computes a scalar multiple of g, which is also an eliminant. □

Elimination using Gröbner bases gives algorithms for Questions (iii) and (iv). The first step is to understand the optimal form of a Gröbner basis of a zero-dimensional ideal.

Lemma 2.4.10 (Shape Lemma). *Suppose $g = g(x_i)$ is an eliminant of a zero-dimensional ideal I with $\deg(g) = \deg(I)$. Then I is radical if and only if g has no multiple factors.*

Suppose that $i = 1$ so that $g = g(x_1)$. Then in the lexicographic monomial order with $x_1 \prec x_2 \prec \cdots \prec x_n$, the ideal I has a Gröbner basis of the form:

$$g(x_1)\,,\quad x_2 - g_2(x_1)\,,\quad \ldots\,,\quad x_n - g_n(x_1)\,, \tag{2.4.3}$$

where $\deg(g) > \deg(g_i)$ for $i = 2, \ldots, n$.

If I is generated by polynomials with coefficients in a subfield $\mathbb{k}$ of $\mathbb{K}$, then the number of points of $\mathcal{V}(I)$ in $\mathbb{k}^n$ equals the number of roots of g in $\mathbb{k}$.

This is a simplified version of the Shape Lemma, which describes the form of a reduced Gröbner basis for any zero-dimensional ideal in the lexicographic order. Example 2.2.11 gives a zero-dimensional ideal which does not satisfy the hypotheses of Lemma 2.4.10 and suggests the form of the general shape lemma.

Proof. Replacing $\mathbb{K}$ by its algebraic closure does not affect these algebraic statements, as the polynomials g and g_i have coefficients in $\mathbb{k}$, by Corollary 2.3.8. Suppose that $g = g(x_i)$ is an eliminant. We have

$$\#\text{roots of } g \;\le\; \#\mathcal{V}(I) \;\le\; \deg(I) \;=\; \deg(g)\,,$$

the first inequality is by Theorem 2.4.6 and the second by Theorem 2.4.4. If the roots of g are distinct, then their number is $\deg(g)$ and so these inequalities are equalities. This implies that I is radical, by Theorem 2.4.4. Conversely, if g has multiple roots, then there is a polynomial h with the same roots as g but with smaller degree. (We may select h to be the square-free part of g.) Since $\langle g\rangle = I \cap \mathbb{K}[x_i]$, we have that $h \notin I$, but since $h^{\deg(g)}$ is divisible by g, $h^{\deg(g)} \in I$, so I is not radical.

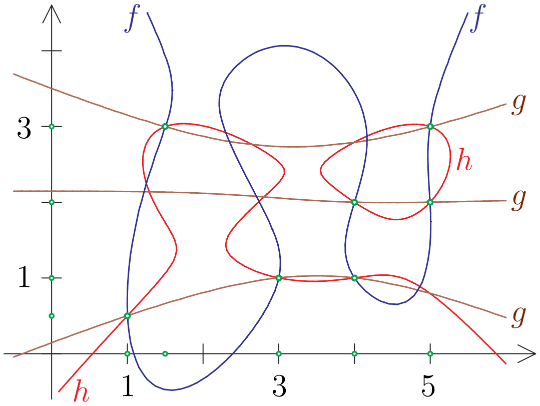


FIGURE 2.4.1. The seven points of $\mathcal{V}(f, g, h)$ and their projections.

To prove the second statement, let d be the degree of the eliminant $g(x_1)$. Then $1, x_1, \ldots, x_1^{d-1}$ are standard monomials, and since $\deg(g) = \deg(I)$, there are no others. Thus the lexicographic initial ideal is $\langle x_1^d, x_2, \ldots, x_n\rangle$. Each element of the reduced Gröbner basis for I expresses a generator of the initial ideal as a $\mathbb{K}$-linear combination of standard monomials. It follows that the reduced Gröbner basis has the form claimed.

For the last statement, observe that the common zeroes of the polynomials (2.4.3) are

$$\{(a_1, \ldots, a_n) \mid g(a_1) = 0 \text{ and } a_i = g_i(a_1)\,,\ i = 2, \ldots, n\}\,.$$

By Corollary 2.3.8, the polynomials $g, g_2, \ldots, g_n$ all have coefficients from $\Bbbk$, and so a component a_i lies in $\Bbbk$ if the root a_1 of $g(x_1)$ lies in $\Bbbk$. □

Not all ideals I have an eliminant g with $\deg(g) = \deg(I)$. For example, let $\mathfrak{m}_0 := \langle x, y\rangle$ be the maximal ideal corresponding to the origin $\{(0,0)\} \in \mathbb{K}^2$. Then its square $\mathfrak{m}_0^2 = \langle x^2, xy, y^2\rangle$ has degree three (there are three standard monomials), but any eliminant has degree two.

Failure of the condition $\deg(g) = \deg(I)$ in the Shape Lemma may occur even when I is radical. Indeed, when I is radical, $\deg(g(x_i)) = \deg(I)$ if and only if the projection map π_i to the coordinate x_i-axis is one-to-one.

EXAMPLE 2.4.11. Suppose that the ideal I is generated by the three polynomials,

$$\begin{aligned} f &:= 1574y^2 - 625yx - 1234y + 334x^4 - 4317x^3 + 19471x^2 \\ &\qquad - 34708x + 19764 + 45x^2y - 244y^3\,, \\ g &:= 45x^2y - 305yx - 2034y - 244y^3 - 95x^2 + 655x + 264 + 1414y^2\,, \quad \text{and} \\ h &:= -33x^2y + 197yx + 2274y + 38x^4 - 497x^3 + 2361x^2 - 4754x \\ &\qquad + 1956 + 244y^3 - 1414y^2\,. \end{aligned}$$

Then $\mathcal{V}(I)$ is the seven nondegenerate points of Figure 2.4.1. There are only five points in the projection to the x-axis and four in the projection to the y-axis. The corresponding eliminants have degrees five and four,

$$2x^5 - 29x^4 + 157x^3 - 391x^2 + 441x - 180 \qquad 2y^4 - 13y^3 + 28y^2 - 23y + 6$$ ◇

Nevertheless, when I is radical, $\deg(g) = \deg(I)$ will hold after a generic change of coordinates, as we saw in Example 2.4.11 and as was used in the proof of Bézout's Theorem in the plane (Theorem 2.1.16). In this case, the Gröbner basis (2.4.3) has the form, and we may find all roots of I over an algebraically closed field by finding all roots to g_1 and then substituting them into $g_2, \ldots, g_n$, solving Question (iii). It also gives a symbolic algorithm to count the number of real solutions to a system of equations whose ideal satisfies the hypotheses of the Shape Lemma and solves Question (iv). It requires an algorithm to count the number of real roots of a univariate polynomial. The classical algorithm involving Sturm sequences is given in Section **??**.

Algorithm 2.4.12 (Counting real roots).
Input: An ideal $I \subset \mathbb{R}[x_1, \ldots, x_n]$.
Output: The number of real points in $\mathcal{V}(I)$, if I satisfies the hypotheses of the Shape Lemma, or else "I does not satisfy the hypotheses of the Shape Lemma".

Compute $\dim(I)$ and $\deg(I)$. If I does not have dimension 0, then exit with "I is not zero-dimensional", else set $i := 1$.

(i) Compute an eliminant $g(x_i)$ for I. If $\deg(g) = \deg(I)$ and $\gcd(g, g') = 1$, then output the number of real roots of g. Else if $i < n$, set $i := i + 1$ and return to (1).

(ii) If no eliminant has been computed and $i = n$, then output "I does not satisfy the hypotheses of the Shape Lemma".

While this algorithm will not always successfully compute the number of real points in $\mathcal{V}(I)$ (it would fail for the ideal of Figure 2.4.1), it may be combined with more sophisticated methods to accomplish that task, see ?????.

The Shape Lemma describes an optimal form of a Gröbner basis for a zero-dimensional ideal, we remarked that it is typically not optimal to compute a lexicographic Gröbner basis directly, and offered Algorithm 2.4.9 to compute eliminants. The idea behind Algorithm 2.4.9 extends to the *FGLM algorithm* for Gröbner basis conversion. This takes a Gröbner basis for a zero-dimensional ideal with respect to one monomial order $\rhd$ and computes a Gröbner basis with respect to a different monomial order $\succ$.

Algorithm 2.4.13 (FGLM).
Input: A Gröbner basis G for a zero-dimensional ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ with respect to a monomial order $\rhd$, and a different monomial order $\succ$.
Output: A Gröbner basis H for I with respect to $\succ$.
Initialize: Set $H := \{\}$, $x^\alpha := 1$, and $S := \{\}$.

(i) Compute $\overline{x^\alpha} := x^\alpha \mod G$.

(ii) If $\overline{x^\alpha}$ does not lie in the linear span of S, then set $S := S \cup \{\overline{x^\alpha}\}$.

Otherwise, there is a (unique) linear combination of elements of S such that

$$\overline{x^\alpha} \;=\; \sum_{\overline{x^\beta} \in S} c_\beta \overline{x^\beta}\,.$$

Set $H := H \cup \{x^\alpha - \sum_\beta c_\beta x^\beta\}$.

(3) If $\{x^\gamma \mid x^\gamma \succ x^\alpha\} \subset \mathrm{in}_\succ(H) := \langle \mathrm{in}_\succ(h) \mid h \in H\rangle$, then halt and output H. Otherwise, set x^α to be the $\succ$-minimal monomial in $\{x^\gamma \not\in \mathrm{in}_\succ(H) \mid x^\gamma \succ x^\alpha\}$ and return to (1).

Proof of correctness. By construction, H always consists of elements of I, and elements of S are linearly independent in the quotient ring $\mathbb{K}[x_1,\dots,x_n]/I$. Thus $\mathrm{in}_\succ(H)$ is a subset of the initial ideal $\mathrm{in}_\succ(I)$, and we always have the inequalities

$$|S| \;\leq\; \dim_{\mathbb{K}}(\mathbb{K}[x_1,\dots,x_n]/I) \qquad \text{and} \qquad \mathrm{in}_\succ(H) \;\subset\; \mathrm{in}_\succ(I)\,.$$

Every time we return to (1) either the set S or the set H (and also $\mathrm{in}_\succ(H)$) increases. Since the cardinality of S is bounded by $\deg(I)$ and the monomial ideals $\mathrm{in}_\succ(H)$ form a strictly increasing chain, the algorithm must halt.

When the algorithm halts, every monomial is either in the set $\mathrm{SM} := \{\mathrm{x}^\beta \mid \overline{\mathrm{x}^\beta} \in \mathrm{S}\}$ or else in the monomial ideal $\mathrm{in}_\succ(H)$. By our choice of x^α in (3), these two sets are disjoint, so that SM is the set of standard monomials for $\mathrm{in}_\succ(H)$. Since

$$\mathrm{in}_\succ(H) \;\subset\; \mathrm{in}_\succ\langle H\rangle \;\subset\; \mathrm{in}_\succ(I)\,,$$

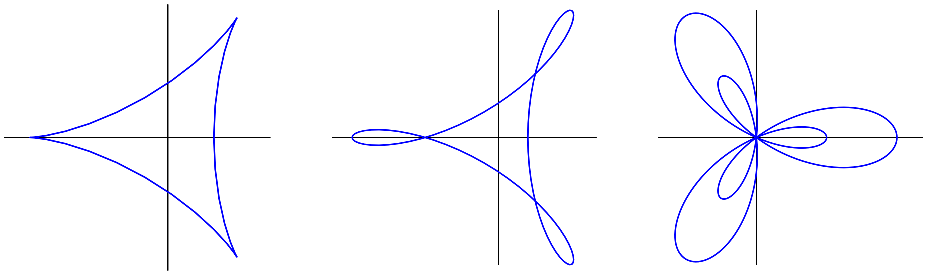
and elements of S are linearly independent in $\mathbb{K}[x_1,\dots,x_n]/I$, we have

$$\begin{aligned}|S| \;\leq\; \dim_{\mathbb{K}}(\mathbb{K}[x_1,\dots,x_n]/I) \;&=\; \dim_{\mathbb{K}}(\mathbb{K}[x_1,\dots,x_n]/\,\mathrm{in}_\succ(I))\\ &\leq\; \dim_{\mathbb{K}}(\mathbb{K}[x_1,\dots,x_n]/\,\mathrm{in}_\succ(H)) \;=\; |S|\,.\end{aligned}$$

Thus $\mathrm{in}_\succ(I) = \mathrm{in}_\succ(H)$, which proves that H is a Gröbner basis for I with respect to the monomial order $\succ$. By the form of the elements of H, it is the reduced Gröbner basis. □

Exercises for Section 2.4. find more appropriate problems

1. Verify the claim in the proof of Theorem 2.4.1 that
$$\mathbb{K}[x_1,\dots,x_n]/\langle g_1(x_1)^{M_1},\dots,g_n(x_n)^{M_n}\rangle$$
has dimension $\prod_i M_i \deg(g_i)$.
2. The trigonometric curves parameterized by $(\cos(\theta) - \frac{1}{2}\cos(2\theta), \sin(\theta) + \frac{1}{2}\sin(2\theta))$, $(\cos(\theta) - \frac{2}{3}\cos(2\theta), \sin(\theta) + \frac{2}{3}\sin(2\theta))$, and the polar curve $r = 1 + 3\cos(3\theta)$ are the cuspidal and trinodal plane quartics, and the rose with three petals, respectively.



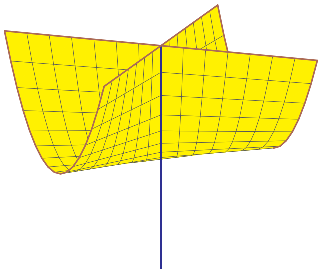
Use elimination to find their implicit equations: Write each as the projection to the (x,y)-plane of an algebraic variety in $\mathbb{K}^4$. Hint: These are images of the circle

$c^2+s^2=1$ under maps to the (x,y) plane, where the variables (c,s) correspond to $(\cos(\theta),\sin(\theta))$. The graph of the first is given by the three polynomials

$$c^2+s^2-1\,,\ x-(c-\tfrac{1}{2}(c^2-s^2))\,,\ y-(s+sc)\,,$$

using the identities $\cos(2\theta)=\cos^2(\theta)-\sin^2(\theta)$ and $\sin(2\theta)=2\sin(\theta)\cos(\theta)$.

3. The Whitney umbrella is the image in $\mathbb{K}^3$ of the map $(u,v)\mapsto(uv,u,v^2)$. Use elimination to find an implicit equation for the Whitney umbrella.



Which points in $\mathbb{K}^2$ give the handle of the Whitney umbrella?

4. Show that every eliminant of $\mathfrak{m}_0^2=\langle x^2,xy,y^2\rangle$ has degree two, even after a linear change of coordinates.
5. Compute the number of solutions to the system of polynomials

$$1+2x+3y+5xy \;=\; 7+11xy+13xy^2+17x^2y \;=\; 0\,.$$

Show that each is nondegenerate and compare this to the Bézout bound for this system. How many solutions are real?

6. In this and subsequent exercises, you are asked to use computer experimentation to study the number of solutions to certain structured polynomial systems. This is a good opportunity to become acquainted with symbolic software.

For several small values of n and d, generate n random polynomials in n variables of degree d, and compute their numbers of isolated solutions. Does your answer agree with Bézout's Theorem?

7. A polynomial is *multilinear* if all exponents are 0 or 1. For example,

$$3xyz-17xy+29xz-37yz+43x-53y+61z-71$$

is a multilinear polynomial in the variables x,y,z. For several small values of n generate n random multilinear polynomials and compute their numbers of common zeroes, Does your answer agree with Bézout's Theorem?

8. Let $\mathcal{A}\subset\mathbb{N}^n$ be a finite set of integer vectors, which we regard as exponents of monomials in $\mathbb{K}[x_1,\dots,x_n]$. A polynomial with support $\mathcal{A}$ is a linear combination of monomials whose exponents are from $\mathcal{A}$. For example

$$1+3x+9x^2+27y+81xy+243xy^2$$

is a polynomial whose support is the column vectors of $\mathcal{A}=\left(\begin{smallmatrix}0&1&2&0&1&1\\0&0&0&1&1&2\end{smallmatrix}\right)$.

For $n=2,3$ and many $\mathcal{A}$ with $|\mathcal{A}|>n$ and $0\in\mathcal{A}$, generate random systems of polynomials with support $\mathcal{A}$ and determine their numbers of isolated solutions. Try to formulate a conjecture about this number of solutions as a function of $\mathcal{A}$.

9. Fix $m, p \geq 2$. For $\alpha\colon 1 \leq \alpha_1 < \cdots < \alpha_p \leq m{+}p$, let E_α be a $p \times (m{+}p)$ matrix whose entries in the columns indexed by α form the identity matrix, and the entries in position i, j are either variables if $j < \alpha_i$ or 0 if $\alpha_i < j$. For example, when $m = p = 3$, here are E_{245} and E_{356},

$$E_{245} \;=\; \begin{pmatrix} x_{1,1} & 1 & 0 & 0 & 0 & 0 \\ x_{2,1} & 0 & x_{2,3} & 1 & 0 & 0 \\ x_{3,1} & 0 & x_{3,3} & 0 & 1 & 0 \end{pmatrix} \qquad E_{356} \;=\; \begin{pmatrix} x_{1,1} & x_{1,2} & 1 & 0 & 0 & 0 \\ x_{2,1} & x_{2,2} & 0 & x_{2,4} & 1 & 0 \\ x_{3,1} & x_{3,2} & 0 & x_{3,4} & 0 & 1 \end{pmatrix}\,.$$

Set $|\alpha| := \alpha_1 - 1 + \alpha_2 - 2 + \cdots + \alpha_p - p$ be the number of variables in E_α. For all small m, p, and α, generate $|\alpha|$ random $m \times (m{+}p)$ matrices $M_1, \ldots, M_{|\alpha|}$ and determine the number of isolated solutions to the system of equations

$$\det\begin{pmatrix} E_\alpha \\ M_1 \end{pmatrix} \;=\; \det\begin{pmatrix} E_\alpha \\ M_2 \end{pmatrix} \;=\; \cdots \;=\; \det\begin{pmatrix} E_\alpha \\ M_{|\alpha|} \end{pmatrix} \;=\; 0\,.$$

Formulate a conjecture for the number of solutions as a function of m, p, and α.

2.5. Gröbner bases for modules

By the ideal-variety correspondence of Section 1.2 and its refinement in Section 1.3, a radical ideal $I \subset \mathbb{K}[x_1,\dots,x_n]$ contains the same information as its variety $\mathcal{V}(I) \subset \mathbb{K}^n$. Homological algebra—the study of modules over $\mathbb{K}[x_1,\dots,x_n]$ and maps between them—is a theoretical tool for accessing the information encoded in an ideal.

For example, suppose that $I \subset \mathbb{K}[x_1,\dots,x_n]$ is an ideal with generators $g_1,\dots,g_r$. We have a sequence of maps,

$$(\mathbb{K}[x_1,\dots,x_n])^r \xrightarrow{\varphi} \mathbb{K}[x_1,\dots,x_n] \longrightarrow \mathbb{K}[x_1,\dots,x_n]/I \longrightarrow 0\,,$$

where $\varphi(f_1,\dots,f_r) = f_1g_2 + \cdots + f_rg_r$. The image of φ is the ideal I, so the sequence is exact. To extend this sequence and determine the homological invariants of I, we need to understand the kernel of φ. This will give a presentation of the ideal I in terms of generators and relations (called *syzygies* of the generators). The module of those relations is called the *syzygy module* for $g_1,\dots,g_r$. This syzygy module, as well as extensions of this presentation, is part of the information encoded in the ideal I.

Gröbner bases for modules are an algorithmic tool for computing homological invariants of an ideal I, and therefore information about $\mathcal{V}(I)$. Fortunately, Gröbner bases for modules require only mild extensions of the theory we developed for ideals.

We present a quick review of modules in the Appendix A.1.2. We will write R for the polynomial ring $\mathbb{K}[x_1,\dots,x_n]$. A (finitely) generated free module over R is an R-module isomorphic to R^r for a positive integer r, called its *rank*. The polynomial ring $\mathbb{K}[x_1,\dots,x_n]$ is a free R-module of rank 1. We represent elements of R^r as ordered lists $\mathbf{f} = (f_1,\dots,f_r)$ of polynomials. We will let $\mathbf{e}_1,\dots,\mathbf{e}_r \in R^r$ be the standard basis elements, e.g. $\mathbf{e}_1 := (1,0,\dots,0)$, $\mathbf{e}_1 = 2 := (0,1,\dots,0)$, and etc. Then $R^r = \bigoplus_{i=1}^r R\mathbf{e}_i$. We have

$$(f_1, f_2, \dots, f_r) \;=\; f_1\mathbf{e}_1 + f_2\mathbf{e}_2 + \cdots + f_r\mathbf{e}_r\,.$$

We will study submodules M of free R-modules R^r, as they are universal in the following sense. Suppose that $A = \langle a_1,\dots,a_r\rangle$ is a finitely generated R-module. Then the map $\varphi\colon R^r \to A$ defined by $\varphi(\mathbf{e}_i) = a_i$ is a surjection. Writing $M \subset R^r$ for its kernel, we obtain the presentation $A \simeq R^r/M$ of A as the quotient of a free module R^r by a submodule.

A *monomial* in R^r is an element of the form $x^\alpha\mathbf{e}_i$, where $x^\alpha \in \mathbb{K}[x_1,\dots,x_n]$ is a monomial, and a *term* is an element of the form $ax^\alpha\mathbf{e}_i$, for some $a \in \mathbb{K}^\times$. Given two monomials $x^\alpha\mathbf{e}_i$ and $x^\beta\mathbf{e}_j$, we say that $x^\alpha\mathbf{e}_i$ *divides* $x^\beta\mathbf{e}_j$ if $i = j$ (so they have the same basis element of R^r) and x^α divides x^β. If $x^\alpha\mathbf{e}_i$ divides $x^\beta\mathbf{e}_i$, then we write the fraction $x^\beta\mathbf{e}_i/x^\alpha\mathbf{e}_i$ for the monomial $x^{\alpha-\beta} = x^\alpha/x^\beta$. The *least common multiple* of monomials $x^\alpha\mathbf{e}_i$ and $x^\beta\mathbf{e}_j$, $\operatorname{lcm}(x^\alpha\mathbf{e}_i, x^\beta\mathbf{e}_j)$, is $\mathbf{0}$ unless $i = j$, and when $i = j$ it is $x^\gamma\mathbf{e}_i$, where x^γ is the least common multiple of x^α and x^β. As with polynomials, we define the least common multiple of two terms to be the least common multiple of their underlying monomials.

A *monomial (sub)module* $M \subset R^r$ is one generated by monomials. Equivalently, if $\mathbf{f} \in M$, then every monomial in $\mathbf{f}$ lies in M. Dickson's Lemma holds for monomial submodules.

LEMMA 2.5.1. *Every monomial submodule is finitely generated.*

Proof. As each monomial in a monomial submodule $M \subset R^r$ lies in some summand $R\mathbf{e}_i$, we have

$$M \;=\; (M \cap R\mathbf{e}_1) \oplus (M \cap R\mathbf{e}_2) \oplus \cdots \oplus (M \cap R\mathbf{e}_r)\,.$$

Under the identification $R \xrightarrow{\sim} R\mathbf{e}_i$ $(1 \mapsto 1\mathbf{e}_i)$, each summand is identified with a monomial ideal of R. The lemma follows from Dickson's Lemma (Lemma 2.2.2) for ideals. □

We note two consequences of this lemma. A monomial submodule has a unique set of minimal generators—these are its monomials which are minimal under divisibility. Also, any increasing chain

$$M_1 \;\subset\; M_2 \;\subset\; M_2 \;\subset\; \cdots \;\subset\; R^r \tag{2.5.1}$$

of monomial submodules is finite. Given a weakly increasing chain (2.5.1) of monomial submodules of R^r, there is some $\ell \geq 1$ such that $M_\ell = M_{\ell+1} = \cdots$.

Let $M \subset R^r$ be a monomial submodule and suppose that the monomials $\mathbf{g}_1, \ldots, \mathbf{g}_m$ are its minimal generators. Let R^m be the free R-module with basis $\boldsymbol{\varepsilon}_1, \ldots, \boldsymbol{\varepsilon}_m$, and consider the map with image M

$$\varphi \,:\, R^m \;\longrightarrow\; R^r \qquad \varphi(\boldsymbol{\varepsilon}_i) \;=\; \mathbf{g}_i \quad i = 1, \ldots, m\,.$$

The kernel of φ is the *syzygy module* of $\mathbf{g}_1, \ldots, \mathbf{g}_m$.

For indices $i \neq j$ such that $\mathbf{g}_i$ and $\mathbf{g}_j$ have the same basis element of R^r, define

$$x_{ij} \;:=\; \frac{\mathrm{lcm}(\mathbf{g}_i, \mathbf{g}_j)}{\mathbf{g}_i}\;,$$

which is a monomial of R. Define $\boldsymbol{\sigma}_{ij} := x_{ij}\boldsymbol{\varepsilon}_i - x_{ji}\boldsymbol{\varepsilon}_j$. If $\mathbf{g}_i$ and $\mathbf{g}_j$ do not have the same basis element of R^r, then set $\boldsymbol{\sigma}_{ij} := \mathbf{0}$. In either case, $\varphi(\boldsymbol{\sigma}_{ij}) = \mathbf{0}$, as $x_{ij}\mathbf{g}_i = x_{ji}\mathbf{g}_j = \mathrm{lcm}(\mathbf{g}_i, \mathbf{g}_j)$.

Lemma 2.5.2. *With these definitions, the syzygy module* $\ker\varphi$ *is generated as an R-module by the elements $\boldsymbol{\sigma}_{ij}$ for $i < j$.*

Proof. As a $\mathbb{K}$-linear map, φ sends monomials in R^m to monomials in M. For a monomial $x^\gamma\mathbf{e}_k \in M$, the (finite) set of monomials $\mathbf{f}$ of R^m such that $\varphi(\mathbf{f}) = x^\gamma\mathbf{e}_k$ is a basis for a $\mathbb{K}$-vector subspace $R^m(x^\gamma\mathbf{e}_k)$ of R^m. Observe that R^m is the direct sum of these subspaces $R^m(x^\gamma\mathbf{e}_k)$, and $\ker\varphi$ is the direct sum of its intersections with the $R^m(x^\gamma\mathbf{e}_k)$.

Fix a monomial $x^\gamma\mathbf{e}_k \in M$ and suppose that $\boldsymbol{\sigma} = \sum_i a_i x^{\beta_i}\boldsymbol{\varepsilon}_i \in R^m(x^\gamma\mathbf{e}_k) \cap \ker\varphi$. We argue that $\boldsymbol{\sigma}$ lies in the R-module generated by the elements $\boldsymbol{\sigma}_{ij}$ by induction on the number of nonzero terms in $\boldsymbol{\sigma}$. Note that if $a_i \neq 0$, then $\varphi(x^{\beta_i}\boldsymbol{\varepsilon}_i) = x^{\beta_i}\mathbf{g}_i = x^\gamma\mathbf{e}_k$. Since

$$\mathbf{0} \;=\; \varphi\big(\sum_i a_i x^{\beta_i}\boldsymbol{\varepsilon}_i\big) \;=\; \sum_i a_i x^{\beta_i}\mathbf{g}_i \;=\; \big(\sum_i a_i\big)x^\gamma\mathbf{e}_k\,,$$

we have $\sum_i a_i = 0$. If $\boldsymbol{\sigma} \neq \mathbf{0}$, then there are two indices $i < j$ with $a_i a_j \neq 0$. Since $x^{\beta_i}\mathbf{g}_i = x^\gamma\mathbf{e}_k = x^{\beta_j}\mathbf{g}_j$, if we set $x^\alpha := x^\gamma\mathbf{e}_k/\mathrm{lcm}(\mathbf{g}_i, \mathbf{g}_j)$, then $a_j x^\alpha\boldsymbol{\sigma}_{ij} \;=\; a_j x^{\beta_i}\boldsymbol{\varepsilon}_i - a_j x^{\beta_j}\boldsymbol{\varepsilon}_j$. It follows that $\boldsymbol{\sigma} + a_j x^\alpha\boldsymbol{\sigma}_{ij}$ cancels the term $a_j x^{\beta_j}\boldsymbol{\varepsilon}_j$ from $\boldsymbol{\sigma}$, and is thus an element of $R^m(x^\gamma\mathbf{e}_k) \cap \ker\varphi$ involving fewer nonzero terms than $\boldsymbol{\sigma}$. This completes the proof. □

Definition 2.5.3. A *monomial order* on a free module R^r over $R = \mathbb{K}[x_1, \ldots, x_n]$ is a well-ordering $\succ$ on the monomials in R^r that is compatible with multiplication by monomials of R, in the following sense. If $x^\alpha \mathbf{e}_i \succ x^\beta \mathbf{e}_j$, then for any monomial x^γ of R. $x^\gamma \cdot x^\alpha \mathbf{e}_i \succ x^\gamma \cdot x^\beta \mathbf{e}_j \succ x^\beta \mathbf{e}_j$. ◇

Just as we often have $x_1 \succ x_2 \succ \cdots \succ x_n$ for a monomial order $\succ$ on $\mathbb{K}[x_1, \ldots, x_n]$, for a monomial order $\succ$ on R^r, it is common to have

$$\mathbf{e}_1 \ \succ\ \mathbf{e}_2 \ \succ\ \cdots \ \succ\ \mathbf{e}_r\,.$$

Example 2.5.4. We describe two schema for extending a monomial order $\succ$ on $R = \mathbb{K}[x_1, \ldots, x_n]$ to R^r.

(i) (Term over position) $x^\alpha \mathbf{e}_i \succ_{\text{top}} x^\beta \mathbf{e}_j$ if $x^\alpha \succ x^\beta$ or if $x^\alpha = x^\beta$ and $i < j$.

(ii) (Position over term) $x^\alpha \mathbf{e}_i \succ_{\text{pot}} x^\beta \mathbf{e}_j$ if $i < j$ or if $i = j$ and $x^\alpha \succ x^\beta$.

These do not exhaust possible monomial orders, as we will see when we study syzygies.◇

Given a monomial order $\succ$ on R^r, we may extend it to the terms of R^r, obtaining a *term order*. This is not a partial order, but it is well-founded in that all decreasing chains are finite. Elements of R^r are the sum of terms, and the *initial term* $\text{in}_\succ(\mathbf{f})$ (or $\text{in}(\mathbf{f})$ when $\succ$ is understood) of an element $\mathbf{f} \in R^r$ is the $\succ$-maximal term of $\mathbf{f}$. It is important in what follows that $\text{in}(\mathbf{f})$ is the initial term and not the initial monomial. Let $M \subset R^r$ be a submodule. Its *initial module* is

$$\text{in}(M) \ :=\ \langle \text{in}(\mathbf{f}) \mid \mathbf{f} \in M \rangle\,,$$

which is a monomial submodule of R^r.

Definition 2.5.5. A *Gröbner basis* for a module $M \subset R^r$ with respect to a monomial order $\succ$ is a subset G of M such that the initial module $\text{in}(M)$ is generated by the initial terms of elements of G. That is, $\text{in}(M) = \langle \text{in}(\mathbf{f}) \mid \mathbf{f} \in G \rangle$. ◇

define a reduced GrÖbner basis and explain that you always have them.

Theorem 2.5.6. *A Gröbner basis for a module $M \subset R^r$ generates M.*

Proof. See Exercise 2. □

Corollary 2.5.7. *Every submodule $M \subset R^r$ is finitely generated.*

Proof. See Exercise 3. □

Corollary 2.5.8. *Let M be a finitely generated $\mathbb{K}[x_1, \ldots, x_n]$-module. Then any submodule of M is finitely generated. Any increasing chain $M_1 \subset M_2 \subset \cdots$ of submodules of M is finite.*

This may be restated that a finitely generated $\mathbb{K}[x_1, \ldots, x_n]$-module is noetherian.

Proof. As M is finitely generated, there is a free module R^r and a surjection $\varphi\colon R^r \to M$. The preimage $\varphi^{-1}(N)$ a submodule $N \subset M$ is a submodule of R^r. By Corollary 2.5.7, $\varphi^{-1}(N)$ has a finite generating set $\{\mathbf{g}_1, \ldots, \mathbf{g}_m\}$. Then $\{\varphi(\mathbf{g}_1), \ldots, \varphi(\mathbf{g}_m)\}$ generates N, which proves the first assertion.

The second assertion follows by arguments similar to that given for the same assertion for monomial ideals following the proof of Dickson's Lemma. □

The division algorithm plays an important role in Gröbner bases for modules.

Algorithm 2.5.9 (Division algorithm for modules).
Input: Elements $\mathbf{g}_1, \ldots, \mathbf{g}_m, \mathbf{f}$ in R^r and a monomial order $\succ$.
Output: Polynomials $q_1, \ldots, q_m$ in $\mathbb{K}[x_1, \ldots, x_n]$ and an element $\mathbf{r} \in R^r$ such that

$$\mathbf{f} \ = \ q_1\mathbf{g}_1 + q_2\mathbf{g}_2 + \cdots + q_m\mathbf{g}_m + \mathbf{r}\,, \tag{2.5.2}$$

where $\mathrm{in}(\mathbf{f}) \succ \mathrm{in}(\mathbf{r})$, no term of $\mathbf{r}$ is divisible by an initial term of any element $\mathbf{g}_i$, and we have $\mathrm{in}(\mathbf{f}) \succeq \mathrm{in}(q_i\mathbf{g}_i)$, for each $i = 1, \ldots, m$.
Initialize: Set $\mathbf{r} := \mathbf{f}$ and $q_1 := 0, \ldots, q_m := 0$. Perform the following steps.

(i) If no term of $\mathbf{r}$ is divisible by an initial term of some $\mathbf{g}_i$, then exit.
(ii) Otherwise, let $ax^\alpha\mathbf{e}_k$ be the $\succ$-greatest term of $\mathbf{r}$ divisible by some $\mathrm{in}(\mathbf{g}_i)$. Choose j minimal such that $\mathrm{in}(\mathbf{g}_j)$ divides $x^\alpha\mathbf{e}_k$ and set $bx^\beta := ax^\alpha\mathbf{e}_k/\,\mathrm{in}(\mathbf{g}_j)$. Replace $\mathbf{r}$ by $\mathbf{r} - bx^\beta\mathbf{g}_j$, q_j by $q_j + bx^\beta$, and return to step (1).

The element $\mathbf{r}$ computed by Algorithm 2.5.9 is the remainder of $\mathbf{f}$ upon division by the set $\{\mathbf{g}_1, \ldots, \mathbf{g}_m\}$. The proof of correctness of Algorithm 2.5.9 is the same as that for Algorithm 2.3.1. As with ideals, a Gröbner basis for a submodule $M \subset R^r$ gives an algorithm for testing membership, and the proof is the same as that for ideals.

Corollary 2.5.10. *Suppose that $M \subset R^r$ is a submodule and that G is a finite Gröbner basis for M with respect to a monomial order $\succ$ on R^r. An element $\mathbf{f} \in R^r$ lies in M if and only if the remainder of $\mathbf{f}$ upon division by G is $\mathbf{0}$.*

Let $M \subset R^r$ be a submodule and $\succ$ a monomial order on R^r. A monomial $x^\alpha\mathbf{e}_i$ of R^r is standard if $x^\alpha\mathbf{e}_i \not\in \mathrm{in}(M)$. The same proof given for ideals shows that standard monomials form a vector space basis for R^r/M.

Theorem 2.5.11. *Let $M \subset R^r$ be a submodule and $\succ$ a monomial order. Then the images of standard monomials in R^r/M form a vector space basis.*

A Gröbner basis G for a submodule M of R^r is reduced if for each element $\mathbf{g} \in G$, its initial term $\mathrm{in}(\mathbf{g})$ is a monomial and ts, we may iteratively replace each element does not divide any term in any other element of G.

We need an analog of S-polynomials. Let $\succ$ be a monomial order on R^r and suppose that $\mathbf{f}, \mathbf{g} \in R^r$. The S-vector of $\mathbf{f}$ and $\mathbf{g}$, written $\mathbf{S}(\mathbf{f}, \mathbf{g})$, is the following element of R^r,

$$\mathbf{S}(\mathbf{f},\mathbf{g}) \ := \ \frac{\mathrm{lcm}(\mathrm{in}(\mathbf{f}), \mathrm{in}(\mathbf{g}))}{\mathrm{in}(\mathbf{f})}\mathbf{f} \ - \ \frac{\mathrm{lcm}(\mathrm{in}(\mathbf{f}), \mathrm{in}(\mathbf{g}))}{\mathrm{in}(\mathbf{g})}\mathbf{g}\ .$$

This is nonzero if and only if $\mathrm{in}(\mathbf{f})$ and $\mathrm{in}(\mathbf{g})$ have the same basis element of R^r and if $\mathbf{f}$ and $\mathbf{g}$ are not both monomials.

Theorem 2.5.12 (Buchberger's criterion for submodules). *A set $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_m\} \subset R^r$ is a Gröbner basis for the submodule it generates if and only if the remainder upon division by G of each S-vector $\mathbf{S}(\mathbf{g}_i, \mathbf{g}_j)$ is $\mathbf{0}$.*

The proof of this is essentially the same as that for Buchberger's criterion for ideals (Theorem 2.3.6), and Buchberger's algorithm for computing a Gröbner basis given a finite generating set is also essentially the same as that for ideals, and we omit both. As with ideals, given a Gröbner basis G for a module $M \subset R^r$, we may assume that if $\mathbf{f} \neq \mathbf{g}$ are two elements of G, then $\mathrm{in}(\mathbf{f})$ does not divide $\mathrm{in}(\mathbf{g})$. We will also assume that elements of G are monic in that their initial terms are monomials.

Let us return to syzygies. Suppose that $M \neq \{\mathbf{0}\}$ is a finitely generated R-module. It has a presentation $M \simeq R^{r_0}/N$ for a positive integer r_0 and a submodule $N \subset R^{r_0}$. As N is finitely generated, it is the image of a map $\varphi_1 \colon R^{r_1} \to R^{r_0}$ from a free module with $R^{r_1} \xrightarrow{\varphi_1} R^{r_0} \to M \to 0$ exact. The kernel of φ_1 is finitely generated, and it is the image of a map from a free module. Continuing in this fashion constructs a sequence of maps of free modules,

$$\cdots \xrightarrow{\varphi_{i+1}} R^{r_i} \xrightarrow{\varphi_i} \cdots \xrightarrow{\varphi_2} R^{r_1} \xrightarrow{\varphi_1} R^{r_0}\ , \tag{2.5.3}$$

with M the cokernel of the last map $R^{r_1} \to R^{r_0}$. As $\mathrm{image}(\varphi_i) = \ker(\varphi_{i-1})$ (by construction), this sequence is exact. We call (2.5.3) a free resolution of $M = \mathrm{coker}\,\varphi_1$. When the resolution (2.5.3) is finite, that is, there is some d with φ_d injective and if $j > d$, then $R^{r_j} = \mathbf{0}$ and $\varphi_j = 0$, then we say that it is a free resolution of *length* d. We apply the theory of Gröbner bases for modules to the problem of computing and studying free resolutions of finitely generated R-modules.

Suppose that $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_m\}$ is a Gröbner basis for a submodule $M \subset R^r$ with respect to a monomial order $\succ$ on R^r. We assume that all initial terms $\mathrm{in}(\mathbf{g}_i)$ are monomials. Suppose that $i \neq j$ are indices such that $\mathrm{in}(\mathbf{g}_i)$ and $\mathrm{in}(\mathbf{g}_j)$ have the same basis element of R^r. Define the monomial x_{ij} of R by

$$x_{ij} \ := \ \frac{\mathrm{lcm}(\mathrm{in}(\mathbf{g}_i), \mathrm{in}(\mathbf{g}_j))}{\mathrm{in}(\mathbf{g}_i)}\ .$$

By Buchberger's criterion, $\mathbf{S}(\mathbf{g}_i, \mathbf{g}_j) = x_{ij}\mathbf{g}_i - x_{ji}\mathbf{g}_j$ has remainder $\mathbf{0}$ when divided by the Gröbner basis G. That is, there is an expression

$$x_{ij}\mathbf{g}_i \ - \ x_{ji}\mathbf{g}_j \ = \ \sum_k q_k^{ij}\mathbf{g}_k\ , \tag{2.5.4}$$

where $\mathrm{in}(x_{ij}\mathbf{g}_i) \succ \mathrm{in}(\mathbf{S}(\mathbf{g}_i, \mathbf{g}_j)) \succeq \mathrm{in}(q_k^{ij}\mathbf{g}_k)$ (a consequence of the Division Algorithm). Let $\boldsymbol{\varepsilon}_1, \ldots, \boldsymbol{\varepsilon}_m$ be the standard basis elements of R^m. Define the element $\boldsymbol{\tau}_{ij}$ of R^m by

$$\boldsymbol{\tau}_{ij} \ := \ x_{ij}\boldsymbol{\varepsilon}_i \ - \ x_{ji}\boldsymbol{\varepsilon}_j \ - \ \sum_k q_k^{ij}\boldsymbol{\varepsilon}_k\ . \tag{2.5.5}$$

If $i < j$ but $\mathrm{in}(\mathbf{g}_i)$ and $\mathrm{in}(\mathbf{g}_j)$ have different basis elements, then we set $\boldsymbol{\tau}_{ij} := \mathbf{0}$.

Let $\varphi \colon R^m \to M$ be the map defined by $\varphi(\boldsymbol{\varepsilon}_i) = \mathbf{g}_i$. Then for all $i < j$, $\varphi(\boldsymbol{\tau}_{ij}) = \mathbf{0}$ by (2.5.4), so that $\boldsymbol{\tau}_{ij}$ lies in the syzygy module $\ker\varphi$. We will show that these syzygies $\{\boldsymbol{\tau}_{ij} \mid i < j\}$ generate the syzygy module by showing that they form a Gröbner basis for it with respect to a particular monomial order on R^m. To that end, define the *Schreyer order* $\succ_S$ on R^m by $x^\alpha\boldsymbol{\varepsilon}_i \succ_S x^\beta\boldsymbol{\varepsilon}_j$ if

$$\begin{array}{lcll} \mathrm{in}_\succ(x^\alpha\mathbf{g}_i) & \succ & \mathrm{in}_\succ(x^\beta\mathbf{g}_j) & \text{in } R^r\,, \text{ or if} \\ \mathrm{in}_\succ(x^\alpha\mathbf{g}_i) & = & \mathrm{in}_\succ(x^\beta\mathbf{g}_j) & \text{and } i \ < \ j\,. \end{array} \tag{2.5.6}$$

By our assumption that the $\mathbf{g}_i$ are monic, $\mathrm{in}_\succ(x^\alpha\mathbf{g}_i)$ and $\mathrm{in}_\succ(x^\beta\mathbf{g}_j)$ are both monomials. In Exercise 7, you are asked to show that $\succ_S$ is a monomial order on R^m.

THEOREM 2.5.13. *With these definitions, the syzygies* $\{\boldsymbol{\tau}_{ij} \mid i < j\}$ *form a Gröbner basis for* $\ker\varphi$ *with respect to* $\succ_S$, *and* $\mathrm{in}_{\succ_S}(\tau_{ij}) = x_{ij}\boldsymbol{\varepsilon}_i$.

PROOF. The expression (2.5.5) for $\boldsymbol{\tau}_{ij}$, (2.5.4), and the Division Algorithm imply that $\mathrm{in}_\succ(x_{ij}\mathbf{g}_i)(=\mathrm{in}_\succ(x_{ji}\mathbf{g}_j))$ is $\succ$-greater than every term in the remaining summands $q_k^{ij}\mathbf{g}_k$. Thus $\mathrm{in}_{\succ_S}(\boldsymbol{\tau}_{ij})$ is either $x_{ij}\boldsymbol{\varepsilon}_i$ or $-x_{ji}\boldsymbol{\varepsilon}_j$. Since $i<j$, it is $x_{ij}\boldsymbol{\varepsilon}_i$.

Let $\boldsymbol{\tau} = \sum f_j\boldsymbol{\varepsilon}_j$ be an element of $\ker\varphi$. We complete the proof by showing that there is a syzygy $\boldsymbol{\tau}_{ij}$ such that $\mathrm{in}_{\succ_S}(\boldsymbol{\tau}_{ij})$ divides $\mathrm{in}_{\succ_S}(\boldsymbol{\tau})$.

For each index j, let y_j be the term in R such that $\mathrm{in}_{\succ_S}(f_j\boldsymbol{\varepsilon}_j) = y_j\boldsymbol{\varepsilon}_j$, and note that $\mathrm{in}_\succ(f_j\mathbf{g}_j) = \mathrm{in}_\succ(y_j\mathbf{g}_j)$. Let i be the index such that $\mathrm{in}_{\succ_S}(\boldsymbol{\tau}) = \mathrm{in}_{\succ_S}(f_i\boldsymbol{\varepsilon}_i) = y_i\boldsymbol{\varepsilon}_i$. Define J to be the set of indices j such that the term $\mathrm{in}_\succ(y_j\mathbf{g}_j)$ has the same monomial as $\mathrm{in}_\succ(y_i\mathbf{g}_i)$. By the definition (2.5.6) of $\succ_S$, i is the minimal element of J.

Set $\boldsymbol{\sigma} := \sum_{j\in J} y_j\boldsymbol{\varepsilon}_j$ and note that $\mathrm{in}_{\succ_S}(\boldsymbol{\sigma}) = y_i\boldsymbol{\varepsilon}_i$. Since $\mathbf{0} = \varphi(\boldsymbol{\tau}) = \sum f_j\mathbf{g}_j$, the sum of the terms of the $f_j\mathbf{g}_j$ having the monomial of $\mathrm{in}_\succ(y_i\mathbf{g}_i)$ must be $\mathbf{0}$. By the construction of the set J, this sum is $\sum_{j\in J} y_j\,\mathrm{in}_\succ(\mathbf{g}_j) = \varphi(\boldsymbol{\sigma})$, so $\boldsymbol{\sigma}$ lies in the module of syzygies of the monomials $\{\mathrm{in}_\succ(\mathbf{g}_j) \mid j \in J\}$. By Lemma 2.5.2, this module is generated by the syzygies $\boldsymbol{\sigma}_{k\ell}$ for $k<\ell$ in J. Those syzygies which include the standard basis element $\boldsymbol{\varepsilon}_i$ are $\boldsymbol{\sigma}_{ij} := x_{ij}\boldsymbol{\varepsilon}_i - x_{ji}\boldsymbol{\varepsilon}_j$ with $j \in J \smallsetminus \{i\}$.

In particular, there is some $j \in J\smallsetminus\{i\}$ such that $x_{ij}\boldsymbol{\varepsilon}_i$ divides $y_i\boldsymbol{\varepsilon}_i = \mathrm{in}_{\succ_S}(\boldsymbol{\tau})$. As we showed that $x_{ij}\boldsymbol{\varepsilon}_i = \mathrm{in}_{\succ_S}(\boldsymbol{\tau}_{ij})$, this completes the proof. □

While Theorem 2.5.13 provides an algorithm for computing a Gröbner basis for the module of syzygies of a Gröbner basis of a module, and therefore may be used to compute further syzygy modules, it does not give an algorithm to compute a free resolution (2.5.3). This is because it does not have a stopping criterion. There is however a mild modification for which the computed resolution halts after at most n steps.

Suppose that we are in the same situation as that preceding Theorem 2.5.13, except that we have ordered the Gröbner basis elements $\{\mathbf{g}_1,\dots,\mathbf{g}_m\}$ as follows: For all $i<j$, if $\mathrm{in}(\mathbf{g}_i)$ and $\mathrm{in}(\mathbf{g}_j)$ have the same standard basis element of R^r, so that $\mathrm{in}(\mathbf{g}_i) = x^\alpha\mathbf{e}_k$ and $\mathrm{in}(\mathbf{g}_j) = x^\beta\mathbf{e}_k$, then we require that $x^\alpha \succ_{\mathrm{lex}} x^\beta$. Thus the monomials of R that appear in the initial terms of elements of the Gröbner basis with the same standard basis element of R^r appear in decreasing lexicographic order. Note that the monomial order $\succ$ on R^r is not necessarily related to the lexicographic order $\succ_{\succ_{\mathrm{lex}}}$ on R.

LEMMA 2.5.14. *With this ordering of the Gröbner basis* $\{\mathbf{g}_1,\dots,\mathbf{g}_m\}$ *and the hypotheses of Theorem 2.5.13, suppose that no variable* $x_1,\dots,x_s$ *appears in any of the initial monomials* $\mathrm{in}_\succ(\mathbf{g}_1),\dots,\mathrm{in}_\succ(\mathbf{g}_m)$. *Then no variable* $x_1,\dots,x_{s+1}$ *appears in any initial term* $\mathrm{in}_{\succ_S}(\boldsymbol{\tau}_{ij})$ *of a syzygy.*

PROOF. Let $\boldsymbol{\tau}_{ij}$ with $i<j$ be a syzygy so that $\mathrm{in}_{\succ_S}(\boldsymbol{\tau}_{ij}) = x_{ij}\boldsymbol{\varepsilon}_i$. Suppose that $\mathrm{in}_\succ(\mathbf{g}_i) = ax^\alpha\mathbf{e}_k$ and $\mathrm{in}_\succ(\mathbf{g}_j) = x^\beta\mathbf{e}_k$. By assumption, no variable $x_1,\dots,x_s$ appears in x^α or in x^β, but x_{s+1} may occur. By the choice of ordering of $\mathbf{g}_1,\dots,\mathbf{g}_m$ as $i<j$, we have $x^\alpha \succ_{\mathrm{lex}} x^\beta$ so that the power of x_{s+1} in x^β is at most that in x^α, which is its power

in $\mathrm{lcm}(x^\alpha, x^\beta)$. Thus x_{s+1} does not appear in $x_{ij} = \mathrm{lcm}(x^\alpha, x^\beta)/x^\alpha$, which completes the proof. □

We use this to deduce a famous result of Hilbert.

Corollary 2.5.15 (Hilbert Syzygy Theorem). *Any finitely generated $\mathbb{K}[x_1, \dots, x_n]$-module has a free resolution of length at most n.*

Proof. Recall that a finitely generated $R = \mathbb{K}[x_1, \dots, x_n]$-module is isomorphic to a quotient R^r/M of a free module. The corollary is the case $s = 0$ of the following statement:
Claim: Under the hypotheses of Lemma 2.5.14, if $M = \langle \mathbf{g}_1, \dots, \mathbf{g}_m \rangle \subset R^r$, then R^r/M has a free resolution of length $n - s$.

We prove this by downward induction on s. When $s = n$, the assumption of the claim is that each initial monomial $\mathrm{in}_\succ(\mathbf{g}_i)$ is one of the standard basis elements of R^r. Thus $\mathrm{in}_\succ(M)$ is the free module spanned by those basis elements. Let $M' \subset R^r$ be the free submodule spanned by the remaining basis elements. We claim that the composition of the map of R-modules

$$M' \longrightarrow R^r \longrightarrow R^r/M$$

is an isomorphism, which implies that R^r/M is free, and thus it has a free resolution of length 0. By Theorem 2.5.11, the standard monomials of M form a $\mathbb{K}$-vector space basis for R^r/M. By the form of the initial monomials $\mathrm{in}_\succ(\mathbf{g}_i)$, the standard monomials are exactly the monomials that do not involve the basis elements appearing in any of the $\mathrm{in}_\succ(\mathbf{g}_i)$. But these are the monomials of M', which shows that the composition is an isomorphism of $\mathbb{K}$-vector spaces, which proves the claim.

Let $s < n$ and suppose that $M := \langle \mathbf{g}_1, \dots, \mathbf{g}_m \rangle \subset R^r$ with $\mathbf{g}_1, \dots, \mathbf{g}_m$ satisfying the hypotheses of Lemma 2.5.14 for s, including that they are monic and ordered as described before Lemma 2.5.14. Let $N := \langle \boldsymbol{\tau}_{ij} \mid i < j \rangle \subset R^m$ be the module of syzygies of $\mathbf{g}_1, \dots, \mathbf{g}_m$. By Lemma 2.5.14, no variable $x_1, \dots, x_{s+1}$ appears in any initial term $\mathrm{in}_{\succ_S}(\boldsymbol{\tau}_{Ij})$. We may also assume that the $\boldsymbol{\tau}_{ij}$ and monic and ordered as described before Lemma 2.5.14. Then by our induction hypothesis, $R^m/N \simeq M$ has a free resolution of length $n - s - 1$,

$$R^a \longrightarrow \cdots \longrightarrow R^b \twoheadrightarrow R^m/N \,.$$

Splicing this together with $R^m/N \simeq M \hookrightarrow R^r \twoheadrightarrow R^r/M$ gives a free resolution of R^r/M of length $n - s$,

$$R^a \longrightarrow \cdots \longrightarrow R^b \longrightarrow R^r \twoheadrightarrow R^r/M \,,$$

which completes this algorithmic proof of Hilbert's Syzygy Theorem. □

Needed: Examples and more exercises

Perhaps needed: Minimal free resolutions (definition, existence), graded modules and Hilbert functions.

Exercises for Section 2.5.

1. Prove the claims in the proof of Lemma 2.5.2 that R^m is the direct sum of the subspace $R^m(x^\gamma \mathbf{e}_k)$, and $\ker\varphi$ is the direct sum of its intersections with the $R^m(x^\gamma \mathbf{e}_k)$.
2. Prove Theorem 2.5.6.
3. Prove Corollary 2.5.7.

4. Let $M \subset R^r$ be a submodule and $\succ$ a monomial order on R^r. Give an algorithm to convert any Gröbner basis G for M with respect to $\succ$ to a reduced Gröbner basis, and prove that this is unique as well as the analog of (2.3.5).
5. Give a proof of Buchberger's Criterion for Gröbner bases of submodules.
6. Describe Buchberger's algorithm for submodules.
7. Show that a Schreyer order $\succ_S$ is a monomial order.

2.6. Notes

Resultants were developed in the nineteenth century by Sylvester, were part of the computational toolkit of algebra from that century, and have remained a fundamental symbolic tool in algebra and its applications. Even more classical is Bézout's Theorem, stated by Etienne Bézout in his 1779 treatise *Théorie Générale des Équations Algébriques* [**3, 4**]. Perhaps mention that Chinese mathematicians could eliminate up to 4 variables?

The subject of Gröbner bases began with Buchberger's 1965 Ph.D. thesis which contained his algorithm to compute Gröbner bases [**5, 6**]. The term "Gröbner basis" honors Buchberger's doctoral advisor Wolfgang Gröbner. Key ideas about Gröbner bases had appeared earlier in work of Gordan and of Macaulay, and in Hironaka's resolution of singularities [**22**]. Hironaka called Gröbner bases "standard bases", a term which persists. For example, in the computer algebra package `Singular` [**11**] the command `std(I);` computes the Gröbner basis of an ideal `I`. Despite these precedents, the theory of Gröbner bases rightly begins with Buchberger's contributions.

Chinese had a method of elimination to reduce a system to triangular form and thus to solving univariate equations.

Theorem 2.3.4 was proven by Macaulay [**27**], who the Gröbner basis package `Macaulay 2` [**19**] is named after.

There are additional improvements in Buchberger's algorithm (see Ch. 2.9 in [**8**] for a discussion), and even a series of completely different algorithms due to Jean-Charles Faugère [**16**] based on linear algebra with vastly improved performance.

The FGLM Gröbner basis conversion algorithm for zero-dimensional ideals is due to Faugère, Gianni, Lazard, and Mora [**17**].

For further information on techniques for solving systems of polynomial equations see the books of Cox, Little, and O'Shea [**10, 8**], Sturmfels [**33**] as well as Emiris and Dickenstein [**13**].

The word syzygy come from astronomy, referring to an alignment of heavenly bodies. Page 44 of Eisenbud

Schreyer.

Move this all to Chapter 5

In Section **??**, a further refinement of the eigenvalue techniques will be used to study real roots.

Where is a reference to Stickelberger's Theorem? David Cox is chasing this down.

CHAPTER 3

Structure of varieties

Outline:

In Chapter 1 we introduced varieties and ideals and established the algebra-geometry dictionary, and then developed basic symbolic algorithms in Chapter 2. We now turn to important structural properties of varieties which we will need in subsequent chapters. This begins with the Zariski topology and the notion of genericity, and then the analog of unique factorization for varieties. We introduce rational functions and study maps of projective varieties. After discussing smooth and singular points and tangent spaces, we introduce the notion of dimension. This sets the stage for the fundamental theorems of Bertini-type which deal with the dimension and smoothness of intersections of varieties and their images under maps. This chapter finishes with the Hilbert function and degree of a projective variety and Bézout's Theorem. Revise this paragraph.

3.1. Generic properties of varieties

Many properties in algebraic geometry hold for almost all points of a variety or for almost all objects of a given type. For example, matrices are almost always invertible, univariate polynomials of degree d almost always have d distinct roots, and multivariate polynomials are almost always irreducible. Here, "almost always" means that there is a nonzero polynomial in the parameters which vanishes when these properties do not hold. This notion is much stronger than elsewhere in geometry, where 'almost always' may mean the complement of a set of Lesbegue measure zero or the complement of a meager set (as in Sard's Theorem). We develop the terminology 'generic' and 'Zariski open' to formalize this notion of almost always in algebraic geometry. We use this to define quasi-projective varieties, a common generalization of affine and projective variety, and we show that the image $\varphi(X)$ of a map $\varphi\colon X \to Y$ of algebraic varieties contains a Zariski open subset of its closure $\overline{\varphi(X)}$.

A starting point is the behavior of intersections and unions of affine varieties, which has already had cameo appearances in Chapter 1.

Theorem 3.1.1. *The intersection of any collection of affine varieties in $\mathbb{K}^n$ is an affine variety. The union of any finite collection of affine varieties is an affine variety.*

Proof. The first statement generalizes Lemma 1.2.12(1). Let $\{I_t \mid t \in T\}$ be a collection of ideals in $\mathbb{K}[x_1, \ldots, x_n]$. As both containments are straightforward, we have

$$\bigcap_{t\in T} \mathcal{V}(I_t) \;=\; \mathcal{V}\Bigl(\bigcup_{t\in T} I_t\Bigr)\,.$$

Arguing by induction on the number of varieties shows that it suffices to establish the second statement for the union of two varieties, which is Lemma 1.2.12 (2). □

Theorem 3.1.1 shows that affine varieties in $\mathbb{K}^n$ have the same properties as the closed sets of a topology on $\mathbb{K}^n$. (See Section A.2 of the Appendix.)

Definition 3.1.2. An affine variety is a *Zariski closed set*. The complement of a Zariski closed set is a *Zariski open set*. The *Zariski topology* on $\mathbb{K}^n$ is the topology whose closed sets are the affine varieties in $\mathbb{K}^n$. The *Zariski closure* of a subset $Z \subset \mathbb{K}^n$ is the smallest variety containing Z, which is $\overline{Z} := \mathcal{V}(\mathcal{I}(Z))$, by Lemma 1.2.4. A subvariety X of $\mathbb{K}^n$ inherits its Zariski topology from $\mathbb{K}^n$: the closed subsets of X are its subvarieties. A subset of a variety X is *Zariski dense* in X if its Zariski closure is X. ⋄

Remark 3.1.3. We used these notions implicitly in Chapter 1. It is useful to reconsider some of that chapter in light of Zariski open and Zariski closed sets. Lemma 1.2.4 shows that $Z \mapsto \overline{Z} = \mathcal{V}(\mathcal{I}(Z))$ is a closure operation. We may now reinterpret the second statement of Theorem 1.3.14 about finite maps: A finite map is *proper*, as it maps closed sets to closed sets. Similarly, Theorem 1.5.7 asserts that maps of projective varieties are proper, as is the projection $\mathbb{P}^n \times \mathbb{K}^m \to \mathbb{K}^m$. ⋄

This Zariski topology behaves quite differently from the usual, *Euclidean*, topology on $\mathbb{R}^n$ or $\mathbb{C}^n$ with which we are familiar, and which is reviewed in Appendix A.2. A topology on a space may be defined by giving a generating collection of basic open sets. In the Euclidean topology, the basic open sets are (Euclidean) balls. Let $\mathbb{K} = \mathbb{R}$ or $\mathbb{K} = \mathbb{C}$. The *ball* with radius $\epsilon > 0$ centered at $z \in \mathbb{K}^n$ is

$$B(z, \epsilon) \;:=\; \{a \in \mathbb{K}^n \mid \sum (z_i - a_i)^2 \;<\; \epsilon\}\,.$$

In the Zariski topology, the basic open sets are complements of hypersurfaces, called *principal open sets*. Let $f \in \mathbb{K}[x_1, \ldots, x_n]$ and set

$$U_f \;:=\; \{a \in \mathbb{K}^n \mid f(a) \neq 0\}\,. \tag{3.1.1}$$

In Exercise 3, you are to show that this is an affine variety and to determine its coordinate ring. Such sets occurred in Chapter 1 when discussing local coordinates on projective varieties. In both the Zariski topology and the Euclidean topology the open sets are unions of basic open sets. For the Zariski topology, this is a consequence of Lemma 3.1.12 below. We give two examples to illustrate the Zariski topology.

Example 3.1.4. The Zariski closed subsets of $\mathbb{K}^1$ consist of the empty set, finite collections of points, and $\mathbb{K}^1$ itself. Thus when $\mathbb{K}$ is infinite the familiar separation property of

Hausdorff spaces (any two points are covered by two disjoint open sets) fails spectacularly as any two nonempty open sets meet.

For any field $\mathbb{K}$, every permutation of $\mathbb{K}$ (bijection $\varphi\colon \mathbb{K} \to \mathbb{K}$) is continuous in the Zariski topology. When $\mathbb{K}$ is infinite there are far more Zariski-continuous function f than the polynomials. A deeper development of algebraic geometry than we pursue here leverages the algebraic-geometric dictionary to simultaneously consider Zariski open subsets together with the polynomial functions on them. This is the realm of schemes, locally-ringed spaces, and sheaves of algebras. ◇

Example 3.1.5. The Zariski topology on a product $X \times Y$ of affine varieties X and Y is significantly richer than the product Zariski topology. In the product Zariski topology on $\mathbb{K}^2$, the closed sets are finite unions of sets of the following form: the empty set, points, vertical and horizontal lines $\{a\} \times \mathbb{K}^1$ and $\mathbb{K}^1 \times \{a\}$ for $a \in \mathbb{K}$, and the whole space $\mathbb{K}^2$. On the other hand, $\mathbb{K}^2$ contains many other other subvarieties (called *plane curves*), such as the cubic plane curves of Section 1.1.

More generally, let X and Y be infinite varieties. If $W \subset X$ and $Z \subset Y$ are Zariski closed subsets, then $W \times Z$ is closed in the product Zariski topology on $X \times Y$, and the same is true for products of Zariski open sets. However, the diagonal $\{(x, x) \mid x \in X\}$ is a subvariety of $X \times X$ that is not closed in the product Zariski topology. ◇

We compare the Zariski topology with the Euclidean topology. Recall that a set is nowhere dense in the Euclidean topology if its closure does not contain a ball.

Theorem 3.1.6. *Suppose that $\mathbb{K}$ is one of $\mathbb{R}$ or $\mathbb{C}$. Then*

1. *A Zariski closed set is closed in the Euclidean topology on $\mathbb{K}^n$.*
2. *A Zariski open set is open in the Euclidean topology on $\mathbb{K}^n$.*
3. *A nonempty Euclidean open set is dense in the Zariski topology on $\mathbb{K}^n$.*
4. *$\mathbb{R}^n$ is dense in the Zariski topology on $\mathbb{C}^n$.*
5. *A proper Zariski closed set is nowhere dense in the Euclidean topology on $\mathbb{K}^n$.*
6. *A nonempty Zariski open set is dense in the the Euclidean topology on $\mathbb{K}^n$.*

Proof. For statements 1 and 2, observe that a Zariski closed set $\mathcal{V}(I)$ is the intersection of the hypersurfaces $\mathcal{V}(f)$ for $f \in I$, so it suffices to show this for a hypersurface $\mathcal{V}(f)$. But then Statement 1 (and hence also 2) follows as the polynomial function $f\colon \mathbb{K}^n \to \mathbb{K}$ is continuous in the Euclidean topology, and $\mathcal{V}(f) = f^{-1}(0)$.

Any ball $B(z, \epsilon)$ is dense in the Zariski topology. If a polynomial f vanishes identically on $B(z, \epsilon)$, then all of its partial derivatives do as well. Thus its Taylor series expansion at z is identically zero. But then f is the zero polynomial. This shows that $\mathcal{I}(B(z, \epsilon)) = \{0\}$, and so $\mathcal{V}(\mathcal{I}(B(z, \epsilon))) = \mathbb{K}^n$, that is, $B(z, \epsilon)$ is dense in the Zariski topology on $\mathbb{K}^n$.

Statement 4 uses the same argument. If a polynomial vanishes on $\mathbb{R}^n$, then all of its partial derivatives vanish and so f must be the zero polynomial. Thus $\mathcal{I}(\mathbb{R}^n) = \{0\}$ and $\mathcal{V}(\mathcal{I}(\mathbb{R}^n)) = \mathbb{C}^n$. In fact, we may replace $\mathbb{R}^n$ by any set containing a Euclidean ball.

For Statements 5 and 6, observe that if f is nonconstant, then by Statement 3, the Euclidean closed set $\mathcal{V}(f)$ does not contain a Euclidean ball so $\mathcal{V}(f)$ is nowhere dense. A variety is an intersection of nowhere dense hypersurfaces, so varieties (Zariski closed sets) are nowhere dense. The complement of a nowhere dense set is dense, so nonempty Zariski open sets are dense in $\mathbb{K}^n$. □

Theorem 3.1.6(6) leads to the useful notions of genericity and generic sets and properties. We will use the term "Zariski dense" for dense in the Zariski topology.

Definition 3.1.7. Let X be a variety. A subset $Y \subset X$ is *generic* if it contains a Zariski dense open subset U of X. That is, Y contains a Zariski open set U that is dense in X, $\overline{U} = X$. A property is *generic* if the set of points on which it holds is a generic set. Points of a generic set are called *general* points. ◇

The notion of which points are general depends on the context, and so care must be exercised when using these terms. For example, we may identify $\mathbb{K}^2$ with the set of monic quadratic polynomials in x via

$$(b, c) \longmapsto x^2 + bx + c\,.$$

Then the general quadratic polynomial does not vanish when $x = 0$. (We just need to avoid quadratics with $c = 0$.) On the other hand, the general quadratic polynomial has two roots, as we need only avoid quadratics with $b^2 - 4c = 0$. The quadratic $x^2 - 2x + 1$ is general in the first sense, but not in the second, while the quadratic $x^2 + x$ is general in the second sense, but not in the first. Despite this ambiguity due to its reliance on context, general is a very useful concept.

When $\mathbb{K}$ is $\mathbb{R}$ or $\mathbb{C}$, generic sets in $\mathbb{K}^n$ are dense in the Euclidean topology, by Theorem 3.1.6(6). Thus generic properties hold almost everywhere, in the standard sense.

Example 3.1.8. A general $n \times n$ matrix is invertible, as invertible matrices form a nonempty principal open subset of $\mathrm{Mat}_{n\times n}(\mathbb{K})$. It is the complement of the variety $\mathcal{V}(\det)$ of singular matrices. The *general linear group GL_n* is the set of all invertible matrices,

$$GL_n := \{M \in \mathrm{Mat}_{n\times n} \mid \det(M) \neq 0\} = U_{\det}\,. \qquad ◇$$

Example 3.1.9. A general univariate polynomial of degree n has n distinct complex roots. Identify $\mathbb{K}^n$ with the set of monic univariate polynomials of degree n via

$$(a_1, \dots, a_n) \in \mathbb{K}^n \longleftrightarrow x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{K}[x]\,. \tag{3.1.2}$$

The classical discriminant $\mathrm{disc}_n \in \mathbb{K}[a_1, \dots, a_n]$ (see Example 2.1.5) is a polynomial of degree $2n-2$ which vanishes exactly when the polynomial (3.1.2) has a repeated factor. This identifies the set of polynomials with n distinct complex roots as the set U_{disc}. The discriminant of the quadratic $x^2 + bx + c$ is b^2-4c. ◇

Example 3.1.10. A general complex $n \times n$ matrix is semisimple (diagonalizable). We do not show this by providing an algebraic characterization of semisimplicity. Instead we observe that if a matrix $M \in \mathrm{Mat}_{n\times n}$ has n distinct eigenvalues, then it is semisimple. Let $M \in \mathrm{Mat}_{n\times n}$ and consider the (monic) characteristic polynomial of M

$$\chi(x) := \det(xI_n - M)\,,$$

whose roots are the eigenvalues of M. The coefficients of the characteristic polynomial $\chi(x)$ are polynomials in the entries of M. Evaluating the discriminant at these coefficients gives a polynomial ψ which vanishes when the characteristic polynomial $\chi(x)$ of M has a repeated root. Consequently, the set of matrices with distinct eigenvalues equals the nonempty principal open set U_ψ. Thus the set of semisimple matrices contains an Zariski open dense subset of $\mathrm{Mat}_{n\times n}$ and is therefore generic.

When $n = 2$, the characteristic polynomial of a generic matrix is

$$\det\left(xI_2 \;-\; \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\right) \;=\; x^2 - x(a_{11} + a_{22}) + a_{11}a_{22} - a_{12}a_{21}\,,$$

and so the polynomial ψ is $(a_{11} + a_{22})^2 - 4(a_{11}a_{22} - a_{12}a_{21})\,.$ ⋄

In each of these examples, we used the following easy fact.

Proposition 3.1.11. *A set $V \subset \mathbb{K}^n$ is generic if and only if there is a nonconstant polynomial that vanishes on its complement, if and only if it contains a principal open set.*

In Section 1.5, we showed that the complement of a hypersurface in a projective variety is an affine variety. We consider the same construction for an affine variety. If $X \subset \mathbb{K}^n$ is a variety and $f \in \mathbb{K}[x_1, \dots, x_n]$ is a polynomial which is not identically zero on X ($f \notin \mathcal{I}(X)$), then we have the principal open subset of X,

$$X_f \;:=\; X \smallsetminus \mathcal{V}(f) \;=\; \{x \in X \mid f(x) \neq 0\}\,. \tag{3.1.3}$$

We may also take $f \in \mathbb{K}[X] \smallsetminus \{0\}$, a nonzero element of the coordinate ring of X. In Exercise 3, you are asked to show that X_f is an affine variety and to compute its coordinate ring.

Lemma 3.1.12. *Any Zariski open subset U of a variety X is a finite union of principal open subsets.*

Proof. The complement $Y := X \smallsetminus U$ of a Zariski open subset U of X is a Zariski closed subset. The ideal $\mathcal{I}(Y)$ of Y in $\mathbb{K}^n$ contains the ideal $\mathcal{I}(X)$ of X. By the Hilbert Basis Theorem, there are polynomials $f_1, \dots, f_m \in \mathcal{I}(Y)$ such that

$$\mathcal{I}(Y) \;=\; \langle \mathcal{I}(X),\; f_1, \dots, f_m\rangle\,.$$

Then $X_{f_1} \cup \cdots \cup X_{f_m}$ is equal to

$$(X \smallsetminus \mathcal{V}(f_1)) \cup \cdots \cup (X \smallsetminus \mathcal{V}(f_m)) \;=\; X \smallsetminus (\mathcal{V}(f_1) \cap \cdots \cap \mathcal{V}(f_m)) \;=\; X \smallsetminus Y \;=\; U\,. \qquad \square$$

In Section 1.4, we introduced the cover of projective space $\mathbb{P}^n = U_0 \cup U_1 \cup \cdots \cup U_n$ by affine charts, where for each $i = 0, \dots, n$, U_i is the principal open set U_{x_i},

$$U_{x_i} \;:=\; \{a = [a_0, a_1, \dots, a_n] \in \mathbb{P}^n \mid a_i \neq 0\} \;\simeq\; \mathbb{K}^n\,.$$

By Lemma 1.4.15, a subset $X \subset \mathbb{P}^n$ is a projective variety if and only if each intersection $X \cap U_{x_i}$ is an affine variety, for each $i = 0, \dots, n$. Thus every projective variety X is covered by affine varieties, $X = X_0 \cup X_1 \cup \cdots \cup X_n$, where $X_i := X \cap U_{x_i}$. In Section 1.5 we introduced principal affine subsets U_f and X_f for f a homogeneous form. We may define the Zariski topology on projective varieties in two equivalent ways: Either extend the definition of Zariski topology to projective space (projective varieties are the closed sets) or use the cover of a projective variety by affine varieties to define basic affine open subsets to generate the topology. These are equivalent by Lemma 1.4.15. A subset $Z \subset X$

of a projective variety X is Zariski closed if and only if it is closed in each principal affine set $X_i = X \cap U_i$ of X. Note that Lemma 3.1.12 holds for projective varieties.

We expand our notion of a variety. A subset $X \subset \mathbb{P}^n$ is a *quasi-projective variety* if it is a Zariski open subset of its closure in $\mathbb{P}^n$. That is, if there are projective subvarieties Y, Z of $\mathbb{P}^n$ with $X = Y \smallsetminus Z$. A quasi-projective variety inherits its Zariski topology from that of projective space. A Zariski closed subset of a quasi-projective variety X is its intersection with a projective subvariety Y, and the same for a Zariski open subset of X. A subvariety of a quasi-projective variety X is a Zariski closed subset $Y \subset X$; this will also be a quasi-projective variety. The notion of generic introduced for affine varieties also makes sense for quasi-projective varieties, and it has the same properties. We henceforth often drop the adjective quasi-projective and simply refer to these as varieties.

An *affine cover* of a variety X is a collection $\{U_i \mid i \in I\}$ of Zariski open subsets of X whose union is X, and where each U_i is an affine variety. Any property of a variety that holds under restriction to affine open subsets and which may be detected through such restrictions is called *a local property*. We observed that being closed is a local property. The property that a function is regular is a local property.

Lemma 3.1.13. *Suppose that $\mathbb{K}$ is algebraically closed and let X be an affine variety. Suppose that $f\colon X \to \mathbb{K}$ is a function such that every point $x \in X$ has an affine open neighborhood $U_x \subset X$ with $f|_{U_x} \in \mathbb{K}[U_x]$. Then $f \in \mathbb{K}[X]$ is a regular function.*

Proof. Since the restriction of a regular function to an affine open subset is a regular function and each U_x is covered by principal open sets, we may replace each U_x by a principal open set X_{g_x} where $g_x \in \mathbb{K}[X]$ with $g_x(x) \neq 0$ such that $f|_{X_{g_x}} \in \mathbb{K}[X_{g_x}]$. By Hilbert's Basis Theorem, there are $x_1, \ldots, x_r$ such that $g_{x_1}, \ldots, g_{x_r}$ generates the ideal $\mathcal{I}(\{g_x \mid x \in X\})$. Write g_i for g_{x_i}. Then $\emptyset = \mathcal{V}(\{g_x \mid x \in X\}) = \mathcal{V}(g_1, \ldots, g_r)$, so that $X = X_{g_1} \cup \cdots \cup X_{g_r}$. Thus we may replace our original cover $\{U_x \mid x \in X\}$ by the finite subcover $X_{g_1}, \ldots, X_{g_r}$ consisting of principal open subsets of X.

Let $1 \leq i \leq r$. By assumption, $f|_{X_{g_i}} \in \mathbb{K}[X_{g_i}] = \mathbb{K}[X][\frac{1}{g_i}]$, the second equality by Exer1cise 3. Thus there is a regular function $h_i \in \mathbb{K}[X]$ and nonnegative integer n_i such that $f|_{X_{g_i}} = h_i/g_i^{n_i}$. If we clear the denominator and multiply by g_i, we have $g_i^{1+n_i} f = g_i h_i$. This also holds on X, as both sides vanish on $X \smallsetminus X_{g_i} = \mathcal{V}(g_i)$.

Since $\emptyset = \mathcal{V}(g_1, \ldots, g_r)$, we have $\emptyset = \mathcal{V}(g_1^{1+n_1}, \ldots, g_r^{1+n_r})$. As $\mathbb{K}$ is algebraically closed, by the weak Nullstellensatz there exist $k_1, \ldots, k_r \in \mathbb{K}[X]$ such that $1 = \sum_i k_i g_i^{1+n_i}$. But then $f = \sum_i k_i g_i^{1+n_i} f = \sum_i k_i g_i h_i$ is a regular function on X. □

We record a corollary of this proof.

Corollary 3.1.14. *Suppose that $\mathbb{K}$ is algebraically closed and $\{U_i \mid i \in I\}$ is an affine cover of an affine variety X. Then there exits a finite subset $J \subset I$ of I and for each $j \in J$ a principal open subset U_{g_j} of X such that $U_{g_j} \subset U_j$ with the property that $\{U_{g_j} \mid j \in J\}$ forms an affine cover of X.*

We will say that the finite cover $\{U_{g_j} \mid j \in J\}$ of X by principal affine open sets *refines* the original cover $\{U_i \mid i \in I\}$ of X. Corollary 3.1.14 extends to quasi-projective and even to projective varieties. We show this when $X \subset \mathbb{P}^n$ is projective. Suppose that

$\{U_i \mid i \in I\}$ is a cover of X by affine open subsets. First replace each U_i by its intersection $U_i \cap U_{x_j}$ with each of the principal affine charts $U_{x_j} := \{x \in \mathbb{P}^n \mid x_j \neq 0\} \simeq \mathbb{K}^n$ for $j = 0, \ldots, n$. For each j, $\{U_i \cap U_{x_j} \mid i \in I\}$ form an affine cover of the principal affine open subset $X_{x_j} = X \cap U_{x_j}$ of X. By Corollary 3.1.14 this may be refined to a finite cover of $X \cap U_{x_j}$ by principal affine open subsets, and the union of these for all $j = 0, \ldots, n$ gives a finite cover of X by principal open subsets which refine the original affine cover $\{X_i \mid i \in I\}$ of X. We will use such finite principal affine covers to define and establish properties of varieties.

Observe that if $\varphi\colon X \to Y$ is a regular map of affine varieties and $g \in \mathbb{K}[Y]$ is a regular function on Y, then we may restrict $\varphi^*\colon \mathbb{K}[Y] \to \mathbb{K}[X]$ to $\mathbb{K}[Y_g]$, where Y_g is the principal affine open subset of Y. Indeed, the pullback $\varphi^*(g)$ is a regular function on X, and we have an induced homomorphism

$$\varphi^* \;:\; \mathbb{K}[Y_g] = \mathbb{K}[Y][\tfrac{1}{g}] \;\longrightarrow\; \mathbb{K}[X_{\varphi^*(g)}] = \mathbb{K}[X][\tfrac{1}{\varphi^*(g)}]\,.$$

Being a regular map of affine varieties is a local property.

Corollary 3.1.15. *Suppose that $\mathbb{K}$ is algebraically closed and let X and Y be affine varieties. Suppose that $\varphi\colon X \to Y$ is a map such that every point $x \in X$ has an affine open neighborhood $U_x \subset X$ with $\varphi|_{U_x}\colon U_x \to Y$ a regular map. Then φ is a regular map.*

Proof. Suppose that $Y \subset \mathbb{K}^m$ and apply Lemma 3.1.13 to each of the m coordinate functions defining φ. □

Affine covers afford a uniform definition of a regular map between varieties (affine, projective, or quasi-projective). Suppose that $\mathbb{K}$ is algebraically closed, and that X and Y are varieties. A regular map is a function $\varphi\colon X \to Y$ such that there exists an affine cover $\{V_i \mid i \in I\}$ of Y, and for each $i \in I$ an affine cover $\{U_{i,j} \mid j \in J_i\}$ of $\varphi^{-1}(V_i)$ such that for every i, j, the restriction $\varphi\colon U_{i,j} \to V_i$ is a regular map of affine varieties.

Finiteness is another local property.

Lemma 3.1.16. *Let $\mathbb{K}$ be algebraically closed and suppose that $\varphi\colon X \to Y$ is a regular map of affine varieties with the property that every $y \in Y$ has an affine neighborhood U such that $\varphi^{-1}(U) \subset X$ is affine and the restriction $\varphi|_{\varphi^{-1}(U)}\colon \varphi^{-1}(U) \to U$ is a finite map. Then φ is a finite map.*

Proof. Note that $\varphi(X) = Y$ as finite maps are surjective. We regard $\mathbb{K}[Y]$ as a subring of $\mathbb{K}[X]$ under φ^*. As before, Y has a finite cover $Y_{g_1}, \ldots, Y_{g_r}$ by principal affine sets with $g_i \in \mathbb{K}[Y]$ such that for each i, $\varphi\colon X_{g_i} \to Y_{g_i}$ is finite, as $\varphi^{-1}(Y_{g_i}) = X_{g_i}$.

That is, $\mathbb{K}[X_{g_i}] = \mathbb{K}[X][\frac{1}{g_i}]$ is finitely generated as a module over $\mathbb{K}[Y_{g_i}] = \mathbb{K}[Y][\frac{1}{g_i}]$. Let $u_{i,1}, \ldots, u_{i,m_i} \in \mathbb{K}[X_{g_i}]$ be generators. Since g_i is invertible in $\mathbb{K}[X_{g_i}]$, we may assume that $u_{i,j} \in \mathbb{K}[X]$. We claim that the union of all these $u_{i,j}$ generates $\mathbb{K}[X]$ over $\mathbb{K}[Y]$.

Let $f \in \mathbb{K}[X]$. Then for each i, we have an expression $g_i f = \sum_j u_{i,j} h'_j / g_i^{a_{i,j}}$ with $h'_j \in \mathbb{K}[Y]$ which holds on X_{g_i}. Multiplying through by a sufficient power of g_i and absorbing extra factors of g_i into h'_j, we have $g_i^{n_i} f = \sum_j u_{i,j} h_j$ with $n_i > 0$. Since $\emptyset = \mathcal{V}(g_1^{n_1}, \ldots, g_r^{n_r})$, by the Nullstellensatz there are $k_1, \ldots, k_r \in \mathbb{K}[Y]$ such that $1 = \sum_i k_i g_i^{n_i}$, and thus $f = \sum_i k_i g_i^{n_i} f = \sum_i \sum_j u_{i,j} k_i h_j$, which completes the proof of the lemma. □

Lemma 3.1.16 motivates and explains our definition of a finite map of projective varieties which we gave in Section 1.5. It also justifies the following definition. A regular map $\varphi\colon X \to Y$ of quasi-projective varieties is finite if every $y \in Y$ has an affine neighborhood U such that $\varphi^{-1}(U) \subset X$ is affine and the restriction $\varphi|_{\varphi^{-1}(U)}\colon \varphi^{-1}(U) \to U$ is a finite map of affine varieties.

We prove a very useful property of maps of varieties.

Theorem 3.1.17. *Suppose that $\varphi\colon X \to Y$ is a dominant map. Then $\varphi(X)$ contains a non-empty Zariski open subset of Y.*

Recall that X and Y have finite affine covers, $\{U_{i,j}\}$ for X and $\{V_j\}$ for Y such that $\{U_{i,j} \mid j \in J_i\}$ is an affine cover of $\varphi^{-1}(V_i)$ with $\varphi\colon U_{i,j} \to V_i$ a regular map of affine varieties. Thus it suffices to prove the theorem for dominant maps of affine varieties. When $\varphi\colon X \to Y$ is dominant, the map $\varphi^*\colon \mathbb{K}[Y] \hookrightarrow \mathbb{K}[X]$ is injective, by Corollary 1.3.13(2). We will regard $\mathbb{K}[Y]$ as a subalgebra of $\mathbb{K}[X]$.

As in Section 1.3, elements $u_1, \dots, u_r \in \mathbb{K}[X]$ are algebraically independent over $\mathbb{K}[Y]$ if the map $\mathbb{K}[Y][z_1, \dots, z_r] \to \mathbb{K}[X]$ from the ring of polynomials in $z_1, \dots, z_r$ over $\mathbb{K}[Y]$ to $\mathbb{K}[X]$ given by $z_i \mapsto u_i$ is injective. By Corollary 1.3.13(2), this is equivalent to the map $\psi\colon X \to Y \times \mathbb{K}^r$ given by $x \mapsto (\varphi(x), u_1(x), \dots, u_r(x))$ being dominant.

Lemma 3.1.18. *There exist $r \geq 0$ and elements $u_1, \dots, u_r \in \mathbb{K}[X]$ such that*

(1) $u_1, \dots, u_r$ are algebraically independent over $\mathbb{K}[Y]$.
(2) Every element of $\mathbb{K}[X]$ is algebraically dependent on $\mathbb{K}[Y]$ and $u_1, \dots, u_r$.

Proof. Since X is affine, $\mathbb{K}[X]$ is finitely generated over $\mathbb{K}$, and hence finitely generated over $\mathbb{K}[Y]$. Let $u_1, \dots, u_s$ be a set of generators. Consider subsets $U \subset \{u_1, \dots, u_s\}$ of these generators that are algebraically independent over $\mathbb{K}[Y]$. Of all such subsets, let U be one of maximal cardinality. Relabeling the generators, we may assume that $U = \{u_1, \dots, u_r\}$. This gives the first statement.

By the maximality of U, for any $r < i \leq s$, there exists a nonzero polynomial $g \in \mathbb{K}[Y][z_1, \dots, z_r][t] = \mathbb{K}[Y][t; z_1, \dots, z_t]$ such that $0 = g(u_i; u_1, \dots, u_r)$. Let us expand g as a polynomial in t,

$$g(t; z_1, \dots, z_r) \ = \ \sum_{i=0}^{m} t^i g_i(z_1, \dots, z_r)\,,$$

where $g_i \in \mathbb{K}[Y][z_1, \dots, z_r]$ and $g_m \neq 0$. Since $u_1, \dots, u_r$ are algebraically independent, we have that $g_m(z_1, \dots, z_r) \neq 0$. Furthermore, we have $m > 0$ for otherwise $0 = g(u_i; z_1, \dots, z_r) = g_0(z_1, \dots, z_r)$, a contradiction. Thus the remaining generators $u_{r+1}, \dots, u_s$ are each algebraically dependent on $\mathbb{K}[Y]$ and $u_1, \dots, u_r$. The second statement follows from this and from Lemma 3.1.19 below. □

Lemma 3.1.19. *Suppose that $R \subset S$ are finitely generated $\mathbb{K}$-algebras with $u, v \in S$. If both u and v are algebraically dependent over R, then so are both $u + v$ and uv. If both u and v are integral over R, then so are both $u + v$ and uv.*

The proof of this is Exercise 11.

Proof of Theorem 3.1.17. Let $u_1, \ldots, u_r \in \mathbb{K}[X]$ be the elements we construcrted in Lemma 3.1.18. Then the map $\varphi \colon X \to Y$ factors as $X \xrightarrow{\psi} Y \times \mathbb{K}^r \xrightarrow{\pi} Y$. We exploit this factorization to prove Theorem 3.1.17. Let $v_1, \ldots, v_s$ generate $\mathbb{K}[X]$ over $\mathbb{K}[Y \times \mathbb{K}^r]$ as an algebra. By Lemma 3.1.18, each v_i is algebraic over $\mathbb{K}[Y \times \mathbb{K}^r]$ and thus is the root of a polynomial $g_i(t) \in \mathbb{K}[Y \times \mathbb{K}^r][t]$. Suppose that the leading term of $g_i(t)$ is $c_i t^{d_i}$ qwith $c_i \in \mathbb{K}[Y \times \mathbb{K}^r]$, so that in particular $c_i \neq 0$ and $d_i > 0$.

Write $f := c_1 \cdots c_s$ for the product of these leading coefficients and let $U_f := (Y \times \mathbb{K}^r) \smallsetminus \mathcal{V}(f)$ and $X_f := X \smallsetminus \mathcal{V}(f)$ be the principal affine open subsets of $Y \times \mathbb{K}^r$ and X on which f (and each a_i) is invertible. Then $\mathbb{K}[X_f] = \mathbb{K}[X][\frac{1}{f}]$ is finitely generated over $\mathbb{K}[U_f] = \mathbb{K}[Y \times \mathbb{K}^r][\frac{1}{f}]$ by $v_1, \ldots, v_s$ and each v_i satisfies a monic polynomial of degree d_i over $\mathbb{K}[U_f]$. That is,

$$v_i^{d_i} \ \in \ \mathbb{K}[U_f] + v_i \mathbb{K}[U_f] + \cdots + v_i^{d_i - 1} \mathbb{K}[U_f]\,.$$

But this implies that $\mathbb{K}[X_f]$ is a finitely generated module over $\mathbb{K}[U_f]$ (with generators $\{v_1^{a_1} \cdots v_s^{a_s} \mid 0 \leq a_i < d_i\}$), and thus the map $\psi_f \colon X_f \to U_f$ is finite. By Theorem 1.3.14 it is surjective, and thus $\psi(X)$ contains the principal affine open subset U_f of $Y \times \mathbb{K}^r$.

We complete the proof by showing that the image of U_f in Y under the projection contains an affine open subset of Y. We have that $f \in \mathbb{K}[Y \times \mathbb{K}^r] = \mathbb{K}[Y][z_1, \ldots, z_r]$. Let cz^α with $c \in \mathbb{K}[Y]$ be a nonzero term of f, and set $V := Y \smallsetminus \mathcal{V}(c)$, a nonempty principal affine open subset of Y. Then, over points $v \in V$, the polynomial $f(v)$ is nonzero, and thus $U_f \cap \{v\} \times \mathbb{K}^r \neq \emptyset$. But this implies that $V \subset \pi(U_f)$ and thus $V \subset \varphi(X)$, which completes the proof of Theorem 3.1.17. □

After the exercises for this section, the Zariski topology is the default topology; “open” means Zariski open and “closed” means Zariski closed.

Exercises for Section 3.1.

1. Verify the claim that the collection of affine subvarieties of $\mathbb{K}^n$ form the closed sets in a topology on $\mathbb{K}^n$. (See Section A.2 of the Appendix for definitions.)
2. Prove that a closed set in the Zariski topology on $\mathbb{K}^1$ is either the empty set, a finite collection of points, or $\mathbb{K}^1$ itself.
3. Show that the principal open subset U_f (3.1.1) is an affine variety by identifying it with $\mathcal{V}(yf - 1) \subset \mathbb{K}^{n+1}$. Show that its coordinate ring is $\mathbb{K}[x][\frac{1}{f}]$, the localization of the polynomial ring at f. Deduce that a principal open subset X_f (3.1.3) of an affine variety is an affine variety and show that $\mathbb{K}[X_f] = \mathbb{K}[X][\frac{1}{f}]$.
4. Zariski topology of a product vs. product Zariski topology.
   (a) Verify the claim in Example 3.1.5 about the closed sets in the product Zariski topology on $\mathbb{K}^1 \times \mathbb{K}^1$. This requires the statement of Exercise 2.
   (b) Show that any open set in the product Zariski topology on $\mathbb{K}^1 \times \mathbb{K}^1$ is Zariski open in $\mathbb{K}^2$.
   (c) Find a Zariski open set in $\mathbb{K}^2$ which is not open in the product topology on $\mathbb{K}^1 \times \mathbb{K}^1$, and verify these claims.
5. Prove that if $W \subset X$ and $Z \subset Y$ are subvarieties of the varieties X and Y, respectively, then $W \times Z$ is closed in the product Zariski topology on $X \times Y$, and that

$W \times Z$ is a subvariety of $X \times Y$. Prove that if X is an affine variety, then the diagonal $\{(x,x) \mid x \in X\}$ is a subvariety of $X \times X$.

6. (a) Show that the Zariski topology in $\mathbb{K}^n$ is not Hausdorff if $\mathbb{K}$ is infinite.
   (b) Prove that any nonempty Zariski open subset of $\mathbb{K}^n$ is dense.
   (c) Prove that $\mathbb{K}^n$ is compact in the Zariski topology.
7. Let $f(x,y)$ be a polynomial of total degree n. Show that there is a non-empty Zariski open subset of parameters $(a,b,c,\alpha,\beta,\gamma) \in \mathbb{K}^6$ with $a\beta - \alpha b \neq 0$ such that if A is the affine transformation (2.1.13), then every monomial $x^i y^j$ with $0 \leq i, j$ and $i + j \leq n$ appears in the polynomial $f(A(x,y))$ with a nonzero coefficient.
8. Prove that the general triple of points in $\mathbb{R}^2$ are the vertices of a triangle.
9. Suppose that $n \leq m$. Prove that a general $n \times m$ matrix has rank n.
10. Show that $\mathbb{K}^2 \smallsetminus \{(0,0\}$ and $\mathbb{P}^2 \smallsetminus \{(0,0\}$ are quasiprojective varieties that are neither affine nor projective.
11. Give a proof of Lemma 3.1.19. Hint: Let $f, g \in R[x]$ be polynomials with $f(u) = g(v) = 0$. Set $h := g(y-x)$ and show that $u+v$ is a root of the resultant $\operatorname{Res}(f,h;x)$. Similarly, uv is a root of the resultant $\operatorname{Res}(f,k;x)$, where $k = x^{\deg(g)} g(y/x)$.

3.2. Unique factorization for varieties

The polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$ has unique factorization; Every polynomial factors uniquely as a product of irreducible polynomials. A basic structural result about algebraic varieties is an analog of this unique factorization. Any algebraic variety is the finite union of irreducible varieties, and this decomposition is unique. The coordinate ring of an irreducible variety X is a domain whose quotient field is the field $\mathbb{K}(X)$ of rational functions on X. While $\mathbb{K}(X)$ does not determine X, it determines X up to removing proper subvarieties.

A polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$ is *reducible* if we may factor f nontrivially, that is, if $f = gh$ with neither g nor h a constant polynomial. Otherwise f is *irreducible*. Any polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$ may be factored

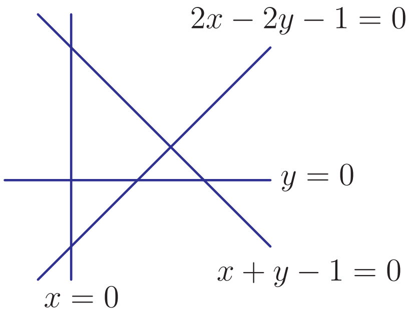
$$f \;=\; c g_1^{d_1} g_2^{d_2} \cdots g_m^{d_m} \tag{3.2.1}$$

where $c \in \mathbb{K}$ is a nonzero constant, the exponents $d_1, \ldots, d_m$ are positive integers, each polynomial g_i is irreducible and non-constant, *and* when $i \neq j$ the polynomials g_i and g_j are not proportional. The factorization (3.2.1) is essentially unique as any other such factorization is obtained from it by permuting the factors, possibly multiplying each polynomial g_i by a constant, and changing the constant c. The polynomials g_j are the *irreducible factors* of f.

When $\mathbb{K}$ is algebraically closed, this algebraic property has a consequence for the geometry of hypersurfaces in $\mathbb{K}^n$. Suppose that a polynomial f has a factorization (3.2.1) into irreducible polynomials. Then the hypersurface $X = \mathcal{V}(f)$ is the union of hypersurfaces $X_i := \mathcal{V}(g_i)$, for $i = 1, \ldots, m$,

$$X \;=\; X_1 \cup X_2 \cup \cdots \cup X_m\,. \tag{3.2.2}$$

For example, $\mathcal{V}(xy^2(x{+}y{-}1)^3(2x{-}2y{-}1))$ is the union of four lines in $\mathbb{K}^2$.



We will show that this decomposition property is shared by general varieties.

Definition 3.2.1. A variety X is *reducible* if it is the union $X = Y \cup Z$ of proper closed subvarieties $Y, Z \subsetneq X$. Otherwise X is *irreducible*. If an irreducible variety X is written as a union of subvarieties $X = Y \cup Z$, then either $X = Y$ or $X = Z$. ⋄

Example 3.2.2. Figure 1.1.1 in Section 1.1 shows that $\mathcal{V}(xy + z,\, x^2 - x + y^2 + yz)$ consists of two space curves, each of which is a variety in its own right. Thus it is reducible.

To see this, we solve the two equations $xy+z=x^2-x+y^2+yz=0$. First note that

$$x^2-x+y^2+yz \ - \ y(xy+z) \ = \ x^2-x+y^2-xy^2 \ = \ (x-1)(x-y^2)\,.$$

Thus either $x=1$ or else $x=y^2$. When $x=1$, we have $y+z=0$ and these equations define the line in Figure 1.1.1. When $x=y^2$, the polynomial relation $xy+z=0$ implies that $z=-y^3$, and these equations define the cubic curve parameterized by $(t^2,t,-t^3)$.

Figure 3.2.1 shows another reducible variety. It has six components, one is a surface, two are space curves, and three are points. ◇

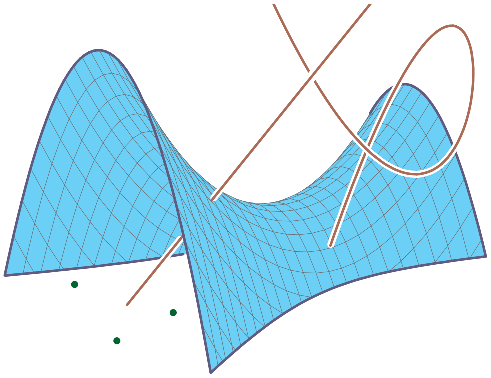


FIGURE 3.2.1. A reducible variety.

THEOREM 3.2.3. *A product $X\times Y$ of irreducible varieties is irreducible.*

PROOF. Suppose that $Z_1,Z_2\subset X\times Y$ are subvarieties with $Z_1\cup Z_2=X\times Y$. We assume that $Z_2\neq X\times Y$ and use this to show that $Z_1=X\times Y$. For each $x\in X$, identify the subvariety $\{x\}\times Y$ with Y. This irreducible variety is the union of two subvarieties,

$$\{x\}\times Y \ = \ \big((\{x\}\times Y)\cap Z_1\big) \ \cup \ \big((\{x\}\times Y)\cap Z_2\big)\,,$$

and so one of these must equal $\{x\}\times Y$. In particular, we must either have $\{x\}\times Y\subset Z_1$ or else $\{x\}\times Y\subset Z_2$. If we define

$$\begin{aligned} x[X_1 \ &= \ \{x\in X\mid \{x\}\times Y\subset Z_1\}\,, \quad \text{and}\\ X_2 \ &= \ \{x\in X\mid \{x\}\times Y\subset Z_2\}\,,\end{aligned}$$

then we have just shown that $X=X_1\cup X_2$. Since $Z_2\neq X\times Y$, we have $X_2\neq X$. We claim that both X_1 and X_2 are subvarieties of X. Then the irreducibility of X implies that $X=X_1$ and thus $X\times Y=Z_1$.

It suffices to show that X_1 is a subvariety of X, as the argument for X_2 is similar. For $y\in Y$, set

$$X_y \ := \ \{x\in X\mid (x,y)\in Z_1\}\,.$$

Since $X_y\times\{y\}=(X\times\{y\})\cap Z_1$, we see that X_y is a subvariety of X. But we have

$$X_1 \ = \ \bigcap_{y\in Y} X_y\,,$$

which shows that X_1 is a subvariety of X and completes the proof. □

The geometric notion of an irreducible variety corresponds to the algebraic notion of a prime ideal. An ideal $I \subset \mathbb{K}[x_1, \dots, x_n]$ is *prime* if whenever $fg \in I$ with $f \notin I$, then we have $g \in I$. Equivalently, if whenever $f, g \notin I$ then $fg \notin I$.

Theorem 3.2.4. *An affine variety X is irreducible if and only if its ideal $\mathcal{I}(X)$ is prime.*

Working in the affine cone $CX \subset \mathbb{K}^{n+1}$ over a projective variety $X \subset \mathbb{P}^n$ shows that X is irreducible if and only if its homogeneous ideal is prime.

Proof. Let $X \subset \mathbb{K}^n$ be an affine variety. First suppose that X is irreducible. Let $f, g \notin \mathcal{I}(X)$. Then neither f nor g vanishes identically on X. Thus $Y := X \cap \mathcal{V}(f)$ and $Z := X \cap \mathcal{V}(g)$ are proper subvarieties of X. Since X is irreducible, $Y \cup Z = X \cap \mathcal{V}(fg)$ is also a proper subvariety of X, and thus $fg \notin \mathcal{I}(X)$. This shows that $\mathcal{I}(X)$ is a prime ideal.

Suppose now that X is reducible. Then $X = Y \cup Z$ is the union of proper subvarieties Y, Z of X. Since $Y \subsetneq X$ is a subvariety, we have $\mathcal{I}(X) \subsetneq \mathcal{I}(Y)$. Let $f \in \mathcal{I}(Y) \smallsetminus \mathcal{I}(X)$ be a polynomial which vanishes on Y but not on X. Similarly, let $g \in \mathcal{I}(Z) \smallsetminus \mathcal{I}(X)$ be a polynomial which vanishes on Z but not on X. Since $X = Y \cup Z$, fg vanishes on X and therefore lies in $\mathcal{I}(X)$. Thus $\mathcal{I}(X)$ is not prime. □

Let us justify the observation about hypersurfaces with which we began this section. We first record an algebraic fact.

Lemma 3.2.5. *A principal ideal $\langle f \rangle$ for $f \in \mathbb{K}[x_1, \dots, x_n]$ is prime if and only if f is irreducible.*

By Exercise 1, a hypersurface $\mathcal{V}(f)$ is defined by the square-free part $\sqrt{f}$ of f. (This was observed at the end of Section 1.2.) If $\sqrt{f}$ is reducible, then $\mathcal{V}(f)$ is reducible. This observation, together with Theorem 3.2.4 and Lemma 3.2.5 give the following characterization of irreducibility for hypersurfaces.

Corollary 3.2.6. *A hypersurface $\mathcal{V}(f)$ is irreducible if and only if the square-free part $\sqrt{f}$ of f is irreducible.*

By Theorem 3.2.4, if $f = g^d$ is a power of an irreducible polynomial g, then $\mathcal{V}(f) = \mathcal{V}(g)$ is irreducible. Thus (3.2.2) exhibits a hypersurface as a union of irreducible hypersurfaces, and this is unique, due to the uniqueness of factorization of polynomials. Notice that irreducibility depends on the field. For example $\mathcal{V}(x^2 + y^2)$ is irreducible over $\mathbb{R}$, bur reducible over $\mathbb{C}$ as $x^2 + y^2 = (x + \sqrt{-1}y)(x - \sqrt{-1}y)$. In the literature, a variety is *absolutely irreducible* or *gemetrically irreducible* if it is irreducible over the algebraic closure $\overline{\mathbb{K}}$.

Proof of Lemma 3.2.5. If $f = gh$ with neither g nor h constant, so that f is reducible, then $g, h \notin \langle f \rangle$, but $gh \in \langle f \rangle$. As $gh \in \langle f \rangle$, we have that $f|gh$. Unique factorization and the irreducibility of f implies that f divides one of g or h. □

We have seen examples of varieties with one, two, four, and six irreducible components. Taking products of distinct irreducible polynomials (or unions of distinct hypersurfaces), yields varieties having any finite number of irreducible components. This is all that may occur as Hilbert's Basis Theorem implies that a variety is a union of finitely many irreducible varieties.

Lemma 3.2.7. *Any affine variety is a finite union of irreducible closed subvarieties.*

Proof. An affine variety X either is irreducible or else we have $X = Y \cup Z$, with both Y and Z proper subvarieties of X. We may similarly decompose whichever of Y and Z is reducible, and continue this process, stopping only when all subvarieties obtained are irreducible. *A priori*, this process could continue indefinitely. We show that it must stop after a finite number of steps.

If this process never stops, then X must contain an infinite chain of subvarieties, each properly contained in the previous one,

$$X \supsetneqq X_1 \supsetneqq X_2 \supsetneqq \cdots .$$

Their ideals form an infinite increasing chain of ideals in $\mathbb{K}[x_1, \ldots, x_n]$,

$$\mathcal{I}(X) \subsetneqq \mathcal{I}(X_1) \subsetneqq \mathcal{I}(X_2) \subsetneqq \cdots .$$

The union I of these ideals is again an ideal. No ideal $\mathcal{I}(X_m)$ is equal to I as the chain of ideals is strict. By the Hilbert Basis Theorem, I is finitely generated, and thus there is some integer m for which $\mathcal{I}(X_m)$ contains these generators. But then $I = \mathcal{I}(X_m)$, a contradiction. □

Lemma 3.2.8. *Let X be a variety and $U \subset X$ a quasiprojective variety that is dense in X. Then X is irreducible if and only if U is irreducible.*

Proof. Assume that U is irreducible and suppose that $X = Y \cup Z$ is the union of two closed subvarieties. Then $U = (U \cap Y) \cup (U \cap Z)$ is the union of two closed subvarieties. As U is irreducible, we may assume that $U = U \cap Y$, but then $X = \overline{U} \subset Y$, which implies that X is irreducible.

Now assume that X is irreducible and suppose that $U = V \cup W$ is union of two closed subvarieties of U. Then $X = \overline{U} = \overline{V} \cup \overline{W}$ is the union of two closed subvarieties. As X is irreducible, we may assume that $X = \overline{V}$, but then $U = U \cap \overline{V} = V$. □

Corollary 3.2.9. *A variety X is a finite union of irreducible subvarieties.*

Proof. Suppose that $X \subset \mathbb{P}^n$ is a projective variety. Then $X = X_0 \cup X_1 \cup \cdots \cup X_n$ where $X_i = X \cap U_i$. Each affine variety X_i is a finite union of irreducible closed subvarieties $U_{i,1}, \ldots, U_{i,m_i}$. By Lemma 3.2.8, the closure in $\mathbb{P}^n$ of each $U_{i,j}$ is irreducible. Since X is the union of these closures, it is a finite union of irreducible closed subvarieties.

If $X \subset \mathbb{P}^n$ is quasi-projective, then its Zariski closure $\overline{X}$ is a projective variety, and is thus a finite union of irreducible closed subvarieties. The intersection of each of these with X is an irreducible closed subvariety of X, by Lemma 3.2.8. Noting that X is the union of these intersections completes the proof. □

A consequence of the proof of Lemma 3.2.7 and of Corollary 3.2.9 is that any decreasing chain of subvarieties of a given variety must have finite length. When $\mathbb{K}$ is infinite, there are such decreasing chains of arbitrary length, as youo are asked to show in Exercise 2.

By Corollary 3.2.9, a variety X may be written as a finite union

$$X \;=\; X_1 \,\cup\, X_2 \,\cup\, \cdots \,\cup\, X_m \tag{3.2.3}$$

of irreducible closed subvarieties. We may assume this is *irredundant* in that if $i \neq j$ then $X_i \not\subseteq X_j$. If we did have $i \neq j$ with $X_i \subset X_j$, then we may remove X_i from the decomposition. We demonstrated that when $X = \mathcal{V}(f)$ is a hypersurface, it has a unique irredundant irreducible decomposition given by the irreducible factors of f. The main result of this section—a basic structural result about varieties—shows that this holds for arbitrary varieties.

THEOREM 3.2.10 (Unique Decomposition of Varieties). *Any variety X is a finite union (3.2.3) of irreducible subvarieties $X_1, \dots, X_m$ such that $X_i \subset X_j$ implies that $i = j$. Furthermore, given any irredundant irreducible decomposition, $X = Y_1 \cup \cdots \cup Y_n$, we have $m = n$ and $\{Y_1, \dots, Y_n\} = \{X_1, \dots, X_m\}$.*

Call these distinguished subvarieties $X_1, \dots, X_m$ the *irreducible components* of X.

PROOF. Suppose that X has another irredundant decomposition,

$$X \;=\; Y_1 \,\cup\, Y_2 \,\cup\, \cdots \,\cup\, Y_n\,,$$

where each Y_j is irreducible and closed in X. Then for each $i = 1, \dots, m$,

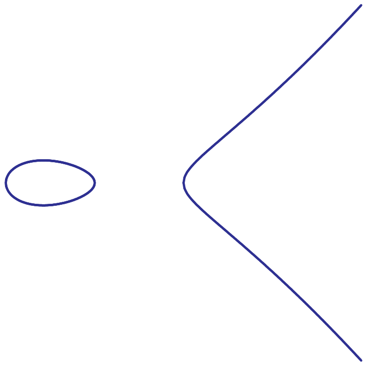
$$X_i \;=\; (X_i \cap Y_1) \,\cup\, (X_i \cap Y_2) \,\cup\, \cdots \,\cup\, (X_i \cap Y_n)\,.$$

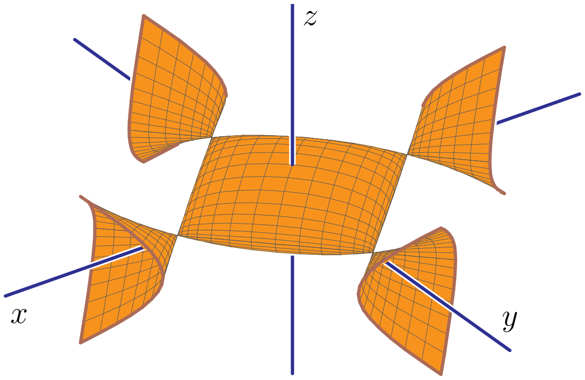
Since X_i is irreducible, one of these must equal X_i, which means that there is some index j with $X_i \subset Y_j$. Similarly, there is some index k with $Y_j \subset X_k$, so that $X_i \subset X_k$. But then $i = k$, and so $X_i = Y_j$. This implies that $n = m$ and that the second decomposition differs from the first solely by permuting the terms. □

REMARK 3.2.11. When $\mathbb{K} = \mathbb{C}$, we will show[†] that an irreducible variety is connected in the Euclidean topology. We will even show that the smooth points of an irreducible variety are connected. Neither of these facts are true over $\mathbb{R}$. Below, we display the cubic plane curve $\mathcal{V}(y^2 - x^3 + x)$ in $\mathbb{R}^2$ and the surface $\mathcal{V}((x^2 - y^2)^2 - 2x^2 - 2y^2 - 16z^2 + 1)$ in

[†] When and where will we show this?

$\mathbb{R}^3$.





Both are irreducible hypersurfaces. The first has two connected components in the Euclidean topology, while in the second, the five components of smooth points meet at the four singular points. (Smooth and singular points will be defined in Section 3.4.) $\diamond$

THEOREM 3.2.12. *Suppose that X is irreducible and $\varphi\colon X \to Y$ is a map of varieties. Then $\overline{\varphi(X)}$ is an irreducible subvariety of Y.*

PROOF. Suppose that the closure Z of $\varphi(X)$ is the union of two subvarieties, $Z = Z_1 \cup Z_2$, with $Z_2 \neq Z$. For each $i = 1, 2$, set $X_i := \varphi^{-1}(Z_i)$, which is closed in X and thus a subvariety. Then $X = X_1 \cup X_2$. Since $Z_2 \neq Z$, we have $X_2 \neq X$. As X is irreducible, this implies that $X = X_1$, and therefore that $Z = Z_1$. $\square$

We introduce another algebraic invariant of an irreducible variety X, its function field $\mathbb{K}(X)$. We investigate to what extent elements of $\mathbb{K}(X)$ are functions on X, and to what extent $\mathbb{K}(X)$ determines X.

Suppose that X is an irreducible affine variety. By Theorem 3.2.4, its ideal $\mathcal{I}(X)$ is prime, so its coordinate ring $\mathbb{K}[X]$ has no zero divisors ($0 \neq f, g \in \mathbb{K}[X]$ with $fg = 0$). A ring without zero divisors is an *(integral) domain*. In exact analogy with the construction of the rational numbers $\mathbb{Q}$ as quotients of integers $\mathbb{Z}$, we may form the *function field* $\mathbb{K}(X)$ of X as quotients of regular functions in $\mathbb{K}[X]$. Formally, $\mathbb{K}(X)$ is the collection of all quotients f/g with $f, g \in \mathbb{K}[X]$ and $g \neq 0$, where we identify

$$\frac{f_1}{g_1} = \frac{f_2}{g_2} \iff f_1g_2 - f_2g_1 = 0 \text{ in } \mathbb{K}[X]\,.$$

The map $f \mapsto \frac{f}{1}$ embeds $\mathbb{K}[X]$ into the function field $\mathbb{K}(X)$. Indeed, as $\mathbb{K}[X]$ is a domain, $\frac{f}{g} = \frac{0}{1}$ implies that $f = 0$.

EXAMPLE 3.2.13. The function field of affine space $\mathbb{K}^n$ consists of quotients of polynomials P/Q with $P, Q \in \mathbb{K}[x_1, \ldots, x_n]$ and $Q \neq 0$. This field $\mathbb{K}(x_1, \ldots, x_n)$ is called the *field of rational functions* in the variables $x_1, \ldots, x_n$. $\diamond$

Given an irreducible affine variety $X \subset \mathbb{K}^n$, we may also express $\mathbb{K}(X)$ as the collection of quotients f/g of polynomials $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ with $g \notin \mathcal{I}(X)$, where we identify

$$\frac{f_1}{g_1} = \frac{f_2}{g_2} \iff f_1g_2 - f_2g_1 \in \mathcal{I}(X)\,.$$

Rational functions on an affine variety X do not in general have unique representatives as quotients of polynomials or even as quotients of regular functions.

EXAMPLE 3.2.14. Let $X := \mathcal{V}(x^2+y^2+2y) \subset \mathbb{K}^2$ be the circle of radius 1 centered at $(0,-1)$. In $\mathbb{K}(X)$ we have

$$-\frac{x}{y} \;=\; \frac{y+2}{x}\,. \qquad \diamond$$

In Chapter 1, we showed that an affine variety is determined up to embedding in affine space by its coordinate ring, and that there is an equivalence of categories between affine varieties and finitely generated reduced $\mathbb{K}$-algebras. The correspondence between irreducible varieties and their fields of rational functions is looser. This however enables us to define fields of rational functions for arbitrary irreducible varieties.

PROPOSITION-DEFINITION 3.2.15. *Let X be an irreducible variety and $U, V \subset X$ nonempty affine open subsets of X. Then their function fields are equal, $\mathbb{K}(U) = \mathbb{K}(V)$, and we define the function field $\mathbb{K}(X)$ to be this common field.*

Thus the function field of an irreducible variety X depends rather weakly on X as any affine open subset has the same function field. Irreducible varieties X and Y are *birationally equivalent* if their function fields are isomorphic, $\mathbb{K}(X) \simeq \mathbb{K}(Y)$.

PROOF. Suppose first that $X \subset \mathbb{K}^n$ is is affine. As U is open, there is some $f \in \mathbb{K}[X]$ with $X \smallsetminus U \subset \mathcal{V}(f)$, so that $X_f = X \smallsetminus \mathcal{V}(f) \subset U$. By Exercise 7, $\mathbb{K}(X) = \mathbb{K}(X_f)$. Since $U_f = X_f$, we have $\mathbb{K}(U) = \mathbb{K}(U_f) = \mathbb{K}(X_f) = \mathbb{K}(X)$.

This does not quite prove the general case, as $U \cap V$ need not be affine. Let $f \in \mathbb{K}[U]$ be such that $U_f \subset U \cap V$, which is an affine subset of both U and V. Then $\mathbb{K}(U) = \mathbb{K}(U_f)$, and as $U_f \subset V$, we deduce that $\mathbb{K}(V) = \mathbb{K}(U_f) = \mathbb{K}(U)$. □

A rational function $\varphi \in \mathbb{K}(X)$ is *regular* at $x \in X$ if φ has a representative f/g with $f, g \in \mathbb{K}[U]$ where $U \subset X$ is affine, $x \in U$, and $g(x) \neq 0$. Then all points of U_g, which is a neighborhood of x in X, are regular points of φ. Thus the set of regular points of φ is a nonempty open subset of X. This is the *domain of regularity of φ*.

When $x \in X$ is a regular point of a rational function $\varphi \in \mathbb{K}(X)$, we set $\varphi(x) := f(x)/g(x) \in \mathbb{K}$, where φ has a representative f/g with $g(x) \neq 0$. The value of $\varphi(x)$ does not depend upon the choice of representative f/g of φ. In this way, φ gives a function from a dense subset of X (its domain of regularity) to $\mathbb{K}$. We write this as

$$\varphi\colon X \dashrightarrow \mathbb{K}$$

with the dashed arrow indicating that φ is not necessarily defined at all points of X.

The rational function φ of Example 3.2.14 has domain of regularity $X \smallsetminus \{(0,0)\}$. Here $\varphi\colon X \dashrightarrow \mathbb{K}$ is stereographic projection of the circle onto the line $y = -1$ from the origin.

EXAMPLE 3.2.16. Let $X = \mathbb{R}$ and $\varphi = 1/(1+x^2) \in \mathbb{R}(X)$. Then every point of X is a regular point of φ, but $\varphi \notin \mathbb{R}[x] = \mathbb{R}[X]$. The existence of rational functions which are everywhere regular, but are not elements of the coordinate ring, is a special feature of real algebraic geometry. Observe that φ is not regular at the points $\pm\sqrt{-1} \in \mathbb{C}$. $\diamond$

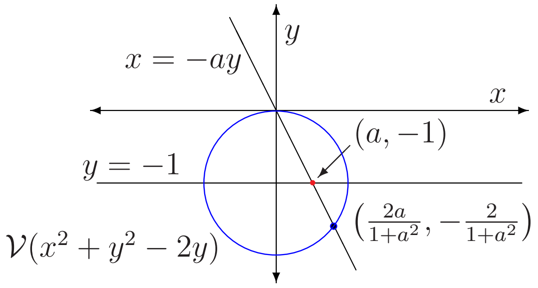

y
$x = -ay$
x
$(a, -1)$
$y = -1$
$\left(\frac{2a}{1+a^2}, -\frac{2}{1+a^2}\right)$
$\mathcal{V}(x^2 + y^2 - 2y)$

FIGURE 3.2.2. Projection of the circle $\mathcal{V}(x^2 + (y-1)^2 - 1)$ from the origin.

THEOREM 3.2.17. *When $\mathbb{K}$ is algebraically closed, a rational function that is regular at all points of an irreducible affine variety X is a regular function in $\mathbb{K}[X]$.*

PROOF. This is a special case of Lemma 3.1.13 For each point $x \in X$, there are regular functions $f_x, g_x \in \mathbb{K}[X]$ with $\varphi = f_x/g_x$ and $g_x(x) \neq 0$. Let $\mathcal{I}$ be the ideal generated by the denominators g_x of φ for $x \in X$. Then $\mathcal{V}(\mathcal{I}) = \emptyset$, as φ is regular at all points of X.

If we let $g_1, \ldots, g_s$ be generators of $\mathcal{I}$ that are denominators of φ and let $f_1, \ldots, f_s$ be regular functions such that $\varphi = f_i/g_i$ for each i. Then by the Weak Nullstellensatz for X (Theorem 1.3.5(3)), there are regular functions $h_1, \ldots, h_s \in \mathbb{K}[X]$ such that in $\mathbb{K}[X]$,

$$1 \;=\; h_1 g_1 + \cdots + h_s g_s\,.$$

Multiplying this equation by φ, we obtain

$$\varphi \;=\; h_1 f_1 + \cdots + h_s f_s\,,$$

which proves the theorem. □

REMARK 3.2.18. The proof of Theorem 3.2.17 uses an 'algebraic partition of unity' which is afforded to us by the Weak Nullstellensatz. ◇

Cut the Proof of the Theorem. Move the Remark to Section 3.1. Add material on rational maps and linear projections.

Exercises for Section 3.2.

1. Show that the ideal of a hypersurface $\mathcal{V}(f)$ is generated by the square-free part of f, which is the product of the irreducible factors of f, each with exponent 1.
2. Suppose that $\mathbb{K}$ is infinite. For every positive integer n, give a decreasing chain of subvarieties of $\mathbb{K}^1$ of length $n{+}1$.
3. Suppose that $I_1 \subset I_2 \subset \cdots$ is an increasing chain of ideals in $\mathbb{K}[x_1, \ldots, x_n]$. Show that its union is an ideal of $\mathbb{K}[x_1, \ldots, x_n]$.
4. Write the ideal $\langle x^3 - x, x^2 - y\rangle$ as the intersection of three prime ideals. Describe the corresponding geometry.
5. Show that $f(x,y) = y^2 + x^2(x-1)^2 \in \mathbb{R}[x,y]$ is an irreducible polynomial but that $V(f)$ is reducible.
6. Verify the claim in Example 3.2.14.

7. Suppose that X is an irreducible affine variety and $0 \neq f \in \mathbb{K}[X]$. Show that the map $K[X] \to \mathbb{K}[X_f]$ is an inclusion and that $\mathbb{K}(X) = \mathbb{K}(X_f)$. (By Exercise (3.1.3) of Section 3.1, $\mathbb{K}[X_f] = \mathbb{K}[X][\frac{1}{f}]$.)
8. Show that irreducible affine varieties X and Y are birationally equivalent if and only if they have isomorphic open sets.
9. We observed that quotients f/g of homogeneous polynomials of the same degree define a function on the principal open set $U_g = \mathbb{P}^n \smallsetminus \mathcal{V}(g)$. The quotient field of the homogeneous coordinate ring of $\mathbb{P}^n$ is graded, and these quotients have degree 0. Show that the degree 0 component of this quotient field is isomorphic to the rational function field $\mathbb{K}(x_1, \ldots, x_n)$.

3.3. Dimension

Dimension is a fundamental concept in algebraic geometry. It has both algebraic and geometric manifestations and several equivalent, but very different definitions. While these different perspectives illuminate the concept, justifying its main properties is subtle. While our definition is motivated by vivid geometric ideas, its justification is ultimately algebraic, and we invoke some algebra from the theory of field extensions in our development of dimension. This algebraic formulation of dimension is powerful—it enables us to prove several equivalent formulations of dimension and establish the main properties of dimension. In Sections 3.4 and 3.6 we give two further formulations of dimension.

Both affine n-space $\mathbb{K}^n$ and projective n-space $\mathbb{P}^n$ should have dimension n. We would similarly expect that a dense open subset $U \subset X$ of a variety X has the same dimension as X. Finite sets of points will then have dimension 0 (a point is a $\mathbb{K}^0$), and we would expect that if $\varphi\colon X \to Y$ is dominant with finite fibers, then X and Y have the same dimension. The following application of Theorem 1.5.10 relates projective (affine) varieties to projective (affine) space, and inspires our definition of dimension. It uses Exercise 1, that the composition of finite maps is a finite map. Also, as we give an algebraic justification of our notion of dimension, it should come as no surprise that we will need for our field $\mathbb{K}$ to be algebraically closed. Recall also that finite maps are surjective.

Theorem 3.3.1 (Noether Normalization). *An irreducible projective variety $X \subset \mathbb{P}^n$ has a finite map $\varphi\colon X \to \mathbb{P}^m$ to a projective space. An irreducible affine variety $X \subset \mathbb{K}^n$ has a finite map $\varphi\colon X \to \mathbb{K}^m$ to an affine space.*

Proof. Let $X \subset \mathbb{P}^n$ be an irreducible projective variety. If $X \neq \mathbb{P}^n$, then let $p \in \mathbb{P}^n \smallsetminus X$ be a point not lying on X and let $\mathbb{P}^{n-1} \subset \mathbb{P}^n$ be a hyperplane disjoint from p. By Theorem 1.5.10, the linear projection π_p with center p is a finite map $\pi_p\colon X \to \pi_p(X) \subset \mathbb{P}^{n-1}$, and by Theorem 3.2.12, its image $\pi_p(X)$ is irreducible. If $\pi_p(X) \neq \mathbb{P}^{n-1}$, then we choose a point $q \in \mathbb{P}^{n-1} \smallsetminus \pi_p(X)$ as a center from which to project $\pi_p(X)$. Continue in this fashion until the image of X is a linear subspace $\mathbb{P}^m$ of $\mathbb{P}^n$. The composition of these linear projections is linear projection π_L with center $L \simeq \mathbb{P}^{n-m-1}$ disjoint from both X and the image $\mathbb{P}^m$ with $\pi_L\colon X \to \mathbb{P}^m$ a finite map.

If $X \subset \mathbb{K}^n$ is an irreducible affine variety, identify $\mathbb{K}^n$ with $U_0 \subset \mathbb{P}^n$ and let $\overline{X}$ be the closure of X, an irreducible projective variety. Repeat the previous construction, but choose the point p in the hyperplane $\mathcal{V}(x_0) = \mathbb{P}^n \smallsetminus \mathbb{K}^n$ at infinity (which is not contained in $\overline{X}$, by Lemma 1.4.17). Then the image of X under π_p lies in $\mathbb{K}^n \cap \mathbb{P}^{n-1} \simeq \mathbb{K}^{n-1}$, and $\pi_p\colon X \to \pi_p(X)$ is a finite map. Continuing, we obtain $L \subset \mathcal{V}(x_0)$ which is disjoint from $\overline{X}$ with $\pi_L\colon X \to \mathbb{K}^m = \mathbb{K}^n \cap \mathbb{P}^m$ a finite map. □

Recall that every fiber of a finite map is finite. Consequently, it would make sense to define the dimension m of an irreducible projective or affine variety X to be the dimension of a projective or affine linear space such that X admits a finite map to that linear space. However, it is not clear that this notion is well-defined, e.g. why would such an m be unique? We instead make a more flexible definition.

Definition 3.3.2. The *dimension*, $\dim X$, of a variety X is the maximum integer m such that there is a dominant rational map $\varphi\colon X \to \mathbb{P}^m$.

To show that this definition is valid, (e.g. why is the set of dimensions of projective spaces that admit dominant maps from X bounded?), we recast this property in terms of algebra. Replacing $\mathbb{P}^m$ by an affine chart U isomorphic to $\mathbb{K}^m$ and X by a dense affine open subset of $\varphi^{-1}(U)$, we obtain a dominant map $\varphi\colon X \to \mathbb{K}^m$ of affine varieties. As observed in Section 1.3, the images of the coordinate functions on $\mathbb{K}^m$ in the coordinate ring $\mathbb{K}[X]$ of X are algebraically independent. Conversely, m algebraically independent elements in $\mathbb{K}[X]$ give a dominant map $X \to \mathbb{K}^m$. Thus the dimension of an affine variety is the maximum number of algebraically independent elements in its coordinate ring.

Suppose that X is an irreducible affine variety and $u_1, \dots, u_m \in \mathbb{K}[X]$ are algebraically independent. Then $u_1, \dots, u_m$ form a set of elements in the function field $\mathbb{K}(X)$ of X that algebraically independent over $\mathbb{K}$. As explained in Appendix A.1.5, algebraic independence of elements in a field extension behaves like linear independence in a vector space, with the analog of the dimension of a vector space the transcendence degree of the field extension. The transcendence degree of $\mathbb{K}(X)$ over $\mathbb{K}$ is the maximum number of elements in a set of elements of $\mathbb{K}(X)$ that are algebraically independent over $\mathbb{K}$, and every maximal set of independent elements has the same number of elements. Call such a maximally independent set a *transcendence basis*. Since $\mathbb{K}(X)$ is the quotient field of the coordinate ring $\mathbb{K}[X]$, we may assume that we have a transcendence basis of $\mathbb{K}(X)$ consisting of elements $u_1, \dots, u_m$ of $\mathbb{K}[X]$. We summarize this discussion.

Theorem 3.3.3. *The dimension of an irreducible variety X is the transcendence degree of its function field.*

When X is affine or projective, this is the dimension of a linear space that is the image of X under a finite map.

Proof. The first statement is a consequence of the discussion preceeding the statement of the theorem.

Suppose that X is an affine variety and $\varphi\colon X \to \mathbb{K}^m$ is a finite map. Then the coordinate functions on $\mathbb{K}^m$ are algebraically indepedent over $\mathbb{K}$, as elements of the coordinate ring of X, and every element in the coordinate ring is algebraically depedent on those coordinate functions. This shows that the dimension of X is m. The same argument holds when X is projective. □

By Exercise 2, the dimension of a variety is the maximum of the dimensions of its irreducible components, and by Exercise 3, the dimension of a variety is equal to the dimension of any dense open subset. In particular, if $X \subset \mathbb{P}^n$ is quasiprojective, then X and its closure $\overline{X}$ have the same dimension. Thus we may study dimension of varieties one irreducible component at a time, and on such a component, dimension is a local property. We develop some elementary properties of dimension, showing that dimension behaves as expected under maps and under taking subvarieties.

Theorem 3.3.4. *Let $\varphi\colon X \to Y$ be a dominant map of varieties. Then* $\dim X \geq \dim Y$. *If φ is a finite map, then* $\dim X = \dim Y$.

Proof. It suffices to prove this when X and Y are irreducible. Indeed, if $Y_0 \subset Y$ is an irreducible component of Y with $\dim Y = \dim Y_0$ and X_0 is an irreducible component of X in $\varphi^{-1}(Y_0)$, then we may replace Y by Y_0 and X by X_0. Let $\psi\colon Y \to \mathbb{P}^m$ be a dominant map with $m = \dim Y$. Then $\psi \circ \varphi\colon X \to \mathbb{P}^m$ is dominant, which implies that $\dim X \geq m = \dim Y$.

If φ is finite, then we may replace X and Y by affine open subsets so that $\varphi\colon X \to Y$ is a finite map of affine varieties. If $\psi\colon Y \to \mathbb{K}^m$ is a finite map (so that $m = \dim Y$), then by Exercise 1, the composition $\psi \circ \varphi\colon X \to \mathbb{K}^m$ is finite, which completes the proof. □

Theorem 3.3.5. *Suppose that X and Y are varieties with $X \subset Y$. Then $\dim X \leq \dim Y$. If Y is irreducible and X is a subvariety of Y with $\dim X = \dim Y$, then $X = Y$.*

Proof. It suffices to prove this when both X and Y are irreducible. We may also replace Y by an affine open subset meeting X. If X is not closed in Y, then we may replace X and Y by the affine varieties X_f and Y_f where $f \in \mathbb{K}[Y]$ vanishes on $\overline{X} \smallsetminus X$ but not on X. Thus we may assume that X is a subvariety of Y, and both are affine and irreducible.

If $\dim Y = m$, then any $m+1$ elements of $\mathbb{K}[Y]$ are algebraically dependent. They remain dependent when restricted to X. This implies that $\dim X \leq \dim Y$, as elements of $\mathbb{K}[X]$ are restrictions of elements of $\mathbb{K}[Y]$.

Now suppose that $\dim X = \dim Y = m$. Let $u_1, \dots, u_m \in \mathbb{K}[Y]$ be elements whose images in $\mathbb{K}[X]$ are algebraically independent over $\mathbb{K}$. Then they are also independent over $\mathbb{K}$ as elements in $\mathbb{K}[Y]$. For any $y \in \mathbb{K}[Y]$, $y, u_1, \dots, u_m$ are algebraically dependent and satisfy a polynomial relation in $\mathbb{K}[Y]$,

$$0 \;=\; f(y, u_1, \dots, u_m) \;=\; y^d c_0(u_1, \dots, u_m) + \cdots + c_d(u_1, \dots, u_m)\,, \tag{3.3.1}$$

where $f \in \mathbb{K}[z, t_1, \dots, t_m]$ and $c_i \in \mathbb{K}[t_1, \dots, t_m]$ are polynomials in indeterminates $z, t_1, \dots, t_m$. If f is reducible, let $f = a g_1^{\alpha_1} \cdots g_m^{\alpha_m}$ with $a \in \mathbb{K}$ be its irreducible factorization in $\mathbb{K}[z, t_1, \dots, t_m]$, then

$$0 \;=\; f(y, u_1, \dots, u_m) \;=\; a(g_1(y, u_1, \dots, u_m))^{\alpha_1} \cdots (g_m(y, u_1, \dots, u_m))^{\alpha_m}\,.$$

Since Y is irreducible, $\mathbb{K}[Y]$ is a domain, and one of the functions $g_i(y, u_1, \dots, u_m)$ vanishes on Y. Thus we may assume that f is irreducible, which further implies that $c_d \in \mathbb{K}[t_1, \dots, t_m]$ is not the zero polynomial.

If $X \neq Y$, choose $y \in \mathcal{I}(X)$. Then y vanishes on X. If we let $f \in \mathbb{K}[z, t_1, \dots, t_m]$ be an irreducible polynomial relation among $y, u_1, \dots, u_m$ as in (3.3.1). Restricting this to X, as y vanishes on X, we have $c_d(u_1, \dots, u_m) = 0$, which contradicts the algebraic independence of $u_1, \dots, u_m$ in $\mathbb{K}[X]$. □

If $X \subset Y$ are varieties, then the codimension of X in Y is $\dim Y - \dim X$.

Corollary 3.3.6. *Every irreducible component of a hypersurface in $\mathbb{P}^n$ or in $\mathbb{K}^n$ has codimension* 1.

Proof. Passing to affine open subsets, it is enough to prove this for an irreducible hypersurface $X = \mathcal{V}(f)$ in $\mathbb{K}^n$, where $f \in \mathbb{K}[x_1, \dots, x_n]$ is an irreducible polynomial by

Corollary 3.2.6. Renumbering the variables, we may assume that x_n appears in f. Let us write f as a polynomial in x_n,

$$f \;=\; x_n^d c_0(x_1,\dots,x_{n-1}) + \cdots + x_n c_{d-1}(x_1,\dots,x_{n-1}) + c_d(x_1,\dots,x_{n-1})\,,$$

with $c_i \in \mathbb{K}[x_1,\dots,x_{n-1}]$, $d>0$, and $c_0 \neq 0$. If $a := (a_1,\dots,a_{n-1}) \notin \mathcal{V}(c_0) \subset \mathbb{K}^{n-1}$, then $f(a;x_n)$ is a nonconstant polynomial in x_n, and therefore it has a root.

Since $X = \mathcal{V}(f)$, this implies that the image $\pi(X) \subset \mathbb{K}^{n-1}$ under the projection $\pi\colon \mathbb{K}^n \to \mathbb{K}^{n-1}$ to the first $n{-}1$ coordinates contains the principal open set U_{c_0}, and is therefore dominant. Thus $\dim X \geq n{-}1$. Since $X \subsetneq \mathbb{K}^n$, Theorem 3.3.5 implies that $\dim X = n{-}1$. □

We complete our study of hypersurfaces in affine or projective space.

Corollary 3.3.7. *Suppose that $X \subset \mathbb{K}^n$ and every irreducible component of X has codimension* 1. *Then X is a hypersurface and $\mathcal{I}(X)$ is a principal ideal.*

Proof. It suffices to prove this when X is irreducible. Since $X \neq \mathbb{K}^n$, there is a nonzero polynomial f that vanishes on X. As X is irreducible and $X \subset \mathcal{V}(f)$, the irreducible decomposition of $\mathcal{V}(f)$ (3.2.2) given by the irreducible factorization of f implies that there is an irreducible factor g of f with $X \subset \mathcal{V}(g)$. Since $\mathcal{V}(g)$ is irreducible and has the same dimension, $n{-}1$, as X, Theorem 3.3.5 implies that $X = \mathcal{V}(g)$ is a hypersurface whose ideal is the prime principal ideal $\langle g\rangle$. □

We extend our study of dimension to the intersection of a variety and a hypersurface, and show that a variety of dimension m has subvarieties of every dimension between 0 and m, ibclusive, wich leads to an inductive or combinatorial definition of dimension. We begin with projective varieties, for their behavior is the most regular.

Let $X \subset \mathbb{P}^n$ be a projective variety. Choose a point in each irreducible component of X and let Λ be a linear form that does not vanish at any of these finitely many chosen points. For any positive integer d, Λ^d a form of degree d that does not vanish on any irreducible component of X, in particular, there exist forms of every degree $d>0$ that do not vanish on any irreducible componenta of X.

Suppose that f is a form of degree d that does not vanish on any irreducible component of X. By Theorem 3.3.5, $\dim X \cap \mathcal{V}(f) < \dim X$, as $\mathcal{V}(f)$ does not contain any irreducible component of X. Set $X_1 := X \cap \mathcal{V}(f)$ and apply the previous argument to obtain a form f_1 of degree d that does not vanish on any irreducible component of X_1. Setting $X_2 := X_1 \cap \mathcal{V}(f_1)$, and continuing in this fashion, we obtain a chain of subvarieties,

$$X_0 \;\supsetneq\; X_1 \;\supsetneq\; X_2 \;\supsetneq\; \cdots \qquad\qquad \text{with } X_{i+1} := X_i \cap \mathcal{V}(f_i)\,, \tag{3.3.2}$$

(we set $X_0 := X$ and $f_0 := f$), where $\dim X_i > \dim X_{i+1}$ for all i, by Theorem 3.3.5.

Theorem 3.3.8. *If an irreducible projective variety X has dimension m and f is a form that does not vanish on X, then* $\dim(X \cap \mathcal{V}(f)) = m{-}1$.

Proof. Suppose that $\dim(X \cap \mathcal{V}(f)) < m{-}1$. Construct a chain of subvarieties (3.3.2) and forms $f_0 = f, f_1, \dots$ of the same degree as f with $X_0 = X$ and $X_{i+1} = X_i \cap \mathcal{V}(f_i)$.

Then $\dim X_i < m-i$, so that $X_m = \emptyset$. Consequently, $\mathcal{V}(f_0, f_1, \dots, f_{m-1}) \cap X = \emptyset$, and therefore the forms $(f_0, f_1, \dots, f_{m-1})$ define a regular map as in (1.5.1),

$$\varphi \, : \, X \longrightarrow \mathbb{P}^{m-1} \, .$$

By Corollary 1.5.11, $\varphi \colon X \to \varphi(X)$ is finite and thus $\dim X \leq m-1$, a contradiction. □

Consequently, in (3.3.2), $\dim X_i = m - i$, which implies that a projective variety X has subvarieties of every dimension between 0 and $\dim X$. This holds more generally.

Corollary 3.3.9. *A quasiprojective variety X has a subvariety of of every dimension between* 0 *and* $\dim X$.

Proof. It suffices to show this when $X \subset \mathbb{P}^n$ is irreducible. Let g be a form that vanishes on the complement $\overline{X} \smallsetminus X$, but is not identically zero on X. Recall that X and $\overline{X}$ have the same dimension as does $\overline{X}_g = \overline{X} \smallsetminus \mathcal{V}(G)$, which is an o0en subset of X. When constructing the chain (3.3.2) for $\overline{X}$, we may choose forms f_i so that $\mathcal{V}(f_i) \not\subset \mathcal{V}(g)$. Intersecting members of the chain with the affine open subset $\overline{X}_g$ gives a chain of affine subvarieties of all possible dimensions between 0 and $\dim X$. Replacing these subvarieties by their closures in X completes the proof. □

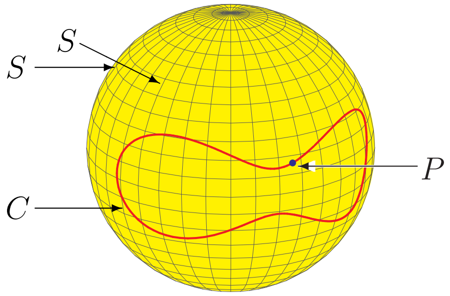
These results imply the following inductive characterization of dimension: The dimension of an irreducible variety X is one more than the supremum of the dimensions of all proper subvarieties of X.

In constructing the chain (3.3.2), we may at each step replace X_i by an irreducible component Y_i with $\dim Y_i = \dim X_i$. This gives another vividly geometric and combinatorial definition of dimension: The dimension of a variety X is the maximum integer m such that there is a strictly decreasing chain

$$Y_0 \supsetneq Y_1 \supsetneq Y_2 \supsetneq \cdots \supsetneq Y_m \supsetneq \emptyset$$

of irreducible subvarieties Y_i of X.

Example 3.3.10. The sphere $S \subset \mathbb{R}^3$ has dimension two, as it is a hypersurface. It has a chain of irreducible subvarieties $S \supsetneq C \supsetneq P$ as shown below.



◇

In Theorem 3.3.8, $\dim(X \cap \mathcal{V}(f)) = \dim X - 1$ means that at least one of the irreducible components of $X \cap \mathcal{V}(f)$ has codimension 1 in X, and every irreducible component has codimension at least 1. We prove a much stronger result, which is one of the most important facts concerning dimension.

THEOREM 3.3.11. *If a form f does not vanish identically on an irreducible projective variety X, then every component of $X \cap \mathcal{V}(f)$ has dimension* $\dim X-1$.

PROOF. Let $d := \deg f$, $m := \dim X$, and suppose that $f_0 = f, f_1, \dots, f_m$ are forms of degree d which give a chain as in (3.3.2) of subvarieties of X where $X_0 = X$, and for $i = 0, \dots, m-1$, $X_{i+1} = X_i \cap \mathcal{V}(f_i)$. The variety X has an affine cover given by the sets $X_{f_i} := X \smallsetminus \mathcal{V}(f_i)$. Note that $X_1 = \mathcal{V}(f)$. We work locally, proving that every component of $X_{f_i} \cap \mathcal{V}(f)$ is either empty or has dimension $m-1$, for each i. Since this is empty when $i = 0$, we only need to consider $i > 0$.

Since $X \cap \mathcal{V}(f_0, \dots, f_m) = \emptyset$, these forms $f_0, \dots, f_m$ define a finite map $\varphi\colon X \to \mathbb{P}^m$, by Corollary 1.5.11. Let $x_0, \dots, x_m$ be homogeneous coordinates for $\mathbb{P}^m$, so that $\varphi^{-1}(x_i) = f_i$. Then for each i, the map φ restricts to give a finite map of affine varieties $\varphi\colon X_{f_i} \to U_{x_i} \simeq \mathbb{K}^m$. If we define $y_j := f_{j-1}/f_i$ for $j = 1, \dots, i$ and $y_j := f_j/f_i$ for $j = i+1, \dots, m$, then $y_1, \dots, y_m$ are regular functions on X_{f_i} that give the map $\varphi\colon X_{f_i} \to \mathbb{K}^m$, and on X_{f_i}, $\mathcal{V}(f) = \mathcal{V}(y_1)$.

Let us replace X by X_{f_i}. Then we may assume that X is an irreducible affine variety with a finite map $X \to \mathbb{K}^m$ given by regular functions $y_1, \dots, y_m$ that are also the coordinates of $\mathbb{K}^m$. Then $\mathbb{K}[X]$ is integral over the polynomial ring $\mathbb{K}[y_1, \dots, y_m]$. To show that every component of $\mathcal{V}(y_1)$ in X has dimension $n-1$, we will prove that $y_2, \dots, y_m$ are algebraically independent on each component, which implies that the component has dimension at least $m-1$. With Theorem 3.3.8, this will complete the proof.

For this, let $p = p(y_2, \dots, y_m) \in \mathbb{K}[y_2, \dots, y_m]$ be a nonzero polynomial. We show that p does not vanish on any component of $\mathcal{V}(y_1)$ in X, using the insightful reformulation:

$$\text{(3.3.3)} \qquad p \text{ does not vanish on any component of } \mathcal{V}(y_1) \iff$$
$$\text{for any } u \in \mathbb{K}[X], \text{ if } pu = 0 \text{ on } \mathcal{V}(y_1), \text{ then } u = 0 \text{ on } \mathcal{V}(y_1).$$

To understand why this is a biequivalence, let $\mathcal{V}(y_1) = Y_1 \cup \cdots \cup Y_t$ be the irredundant irreducible decomposition of $\mathcal{V}(y_1)$. Suppose that p vanishes on Y_1, and let $u \in \mathbb{K}[X]$ be any regular function that vanishes on $Y_2, \dots, Y_t$, but not on Y_1. Then $pu = 0$ on $\mathcal{V}(y_1)$ but $u \neq 0$ on $\mathcal{V}(y_1)$.

By the Nullstellensatz, (3.3.3) is equivalent to the following: if $y_1|(pu)^N$ for some $N > 0$, then $y_1|u^d$ for some $d > 0$. Since y_1 and p are relatively prime in $\mathbb{K}[y_1, y_2, \dots, y_m]$, y_1 and p^N are relatively prime. Replacing y_1, p^N, and u^N by r, s, and v, respectively, this claim (the right hand side of (3.3.3)) follows from the technical Lemma 3.3.12 below (where $R = \mathbb{K}[X]$), and that completes the proof. □

LEMMA 3.3.12. *Let R be a domain containing $S = \mathbb{K}[y_1, \dots, y_m]$ in which every element of R is integral over S. Let $r, s \in S$ be relatively prime. Then for every $v \in R$, if $r|sv$, then there is some $d > 0$ with $r|v^d$.*

PROOF. Let $K = \mathbb{K}(y_1, \dots, y_m)$ be the field of fractions of S. An element $u \in R$ is integral over S, so there is a monic polynomial $f(t) \in S[t]$ that vanishes at u, $f(u) = 0$. Let $g(t) \in K[t]$ be the minimal polynomial of u, the monic polynomial of minimal degree in t such that $g(u) = 0$. Then $f \in \langle g \rangle$, so there is a polynomial $h \in K[t]$ with $f = gh$. By

Gauss's Lemma[1], $g \in S[t]$. Thus the mininmal polynomial in $K[t]$ of any element $u \in R$ lies in $S[t]$.

As $r|sv$, let $u \in R$ be the element such that $ru = sv$. In the quotient field of R, $u = sv/r$ so that a polynomial $f(t) \in K(t)$ vanishes at $t = u$ if and only if the polynomial $g(t) := (r/s)^{\deg(f)} f(st/r) \in K[t]$ vanishes at v. Note that f and g have the same degree in t and that f is monic if and only if g is monic. Let $f = t^d + c_1 t^{d-1} + \cdots + c_{d-1}t + c_d$ be the minimal polynomial of u. As we observed, $f \in S[t]$ and thus each of its coefficients c_i is an element of S. These arguments imply that

$$g(t) \;=\; \left(\frac{r}{s}\right)^d f\left(\frac{st}{r}\right) \;=\; t^d + \frac{rc_1}{s}t^{d-1} + \cdots + \frac{r^{d-1}c_{d-1}}{s^{d-1}}t + \frac{r^d c_d}{s^d}c_d$$

is the minimal polynomial of $v \in R$. (If a monicx polynomail $h \in S[t]$ of lower degree vanished at v, then $(s/r)^{\deg(h)}h(rt/s)$ vanishes when $t = u$, a contradiction.) Again, $g \in S[t]$ so that $r^i c_i/s^i \in S$ for all i. As r and s are relatively prime, s^i divides c_i in S, so that $b_i := r^{i-1}c_i/s^i \in R$. Rewriting $g(v) = 0$, we obtain

$$v^d \;=\; -r(b_1 v^{d-1} + \cdots + b_{d-1}v + b_d)\,.$$

As the second factor lies in R, we see that $r|v^d$ as desired. □

In linear algebra, we know that that r linear forms on $\mathbb{K}^n$ define a linear subspace of dimension at least $n-r$ (and that the rank of a $n \times r$ matrix is at most r). The same holds in the nonlinear algebra of algebraic geometry, and is an important existence result about solutions to systems of equations.

COROLLARY 3.3.13. *The variety of common zeroes of r forms (regular functions) on an m-dimensional irreducible quasiprojective (affine) variety $X \subset \mathbb{P}^n$ is either empty or every component has dimension at least $m-r$. If X is projective, then this is nonempty if $m \geq r$. If $r \leq n$, then r forms on $\mathbb{P}^n$ define a nonempty variety.*

PROOF. For a projective variety X of dimension m, applying Theorem 3.3.11 r times shows that every irreducible component of the variety Z defined by r forms has dimension at least $m-r$, and therefore Z is nonempty when $m \geq r$. This also implies the last statement. For the first, as X is quasiprojective or affine, it is an open subset of a projective variety Y, which is also irreducible of dimension m. Let $Z \subset Y$ be the set of common zeroes of the forms (or homogenizations of regular functions if X is affine). Then $Z \cap X$ is the set of their common zeroes on X, and each irreducible component W of Z has dimension at least $m-r$. Either W does not meet X or $W \cap X$ is nonempty and open in W, and therefore has the same dimension as W. □

In linear algebra, if $\varphi\colon V \to W$ is a surjective linear map of vector spaces, then rank-nullity implies that

$$\dim\ker\varphi \;+\; \dim W \;=\; \dim V\,.$$

Since, for $w \in W$, $\varphi^{-1}(w)$ is a coset of $\ker\varphi$, the dimension of every fiber of φ is equal to $\dim V - \dim W$. A similar, but weaker result holds for nonlinear maps of varieties, which is an important structure theorem about the dimensions of fibers of a map of varieties.

[1] Appendix??

THEOREM 3.3.14. *Suppose that $\varphi\colon X \to Y$ is a surjective map of varieties with X irreducible. Set $m := \dim(X)$ and $n := \dim(Y)$. Then $n \leq m$. For any $y \in Y$, every irreducible component of the fiber $\varphi^{-1}(y)$ has dimension at least $m-n$. There is a nonempty open subset U of Y such that for every $y \in U$, $\dim \varphi^{-1}(y) = m - n$.*

PROOF. By Theorem 3.2.12, Y is irreducible, and by Theorem 3.3.4, $n \leq m$, proving the first assertion. Let $y \in Y$, and note that if $Y = \{y\}$, so that Y has dimension zero then the result is immediate. Replacing Y by an affine open subset containing y and X by the inverse image of that set, we may assume that $Y \subset \mathbb{K}^N$ is affine. Construct a decreasing chain of subvarieties of Y as in (3.3.2), except that each f_i is a regular function on Y, and it vanishes at y. Exercise 6 shows that this is possible. This gives regular functions $f_1, \dots, f_n \in \mathbb{K}[Y]$ and a chain of subvarieties

$$Y = Y_0 \supsetneq Y_1 \supsetneq \cdots \supsetneq Y_n\,,$$

where $Y_{i-1} \cap \mathcal{V}(f_i) = Y_i$ and $\dim Y_i = n-i$. This is because $y \in Y_n$, so that $Y_i \neq \emptyset$.

Since $\dim Y_n = 0$, it is the union of finitely many points. By Exercise 4, there is a polynomial $g \in \mathbb{K}[x_1, \dots, x_N]$ on Y that vanishes on the finite set $Y_n \smallsetminus \{y\}$, but not at y. Then on $U_g := Y \smallsetminus \mathcal{V}(g)$, $\mathcal{V}(f_1, \dots, f_n) = \{y\}$. Replacing Y by U_g and X by $\varphi^{-1}(U_g)$, we see that $\varphi^{-1}(y)$ is defined by the n functions $\varphi^*(f_1), \dots, \varphi^*(f_n)$ on X, and therefore has dimension at least $m-n$, by Corollary 3.3.13. This proves the second assertion.

For the last assertion, again assume that Y is affine. Let $V \subset X$ be an affine open subset. As $\varphi(X) = Y$, the map $\varphi\colon V \to Y$ is dominant. As in Lemma 3.1.18, we may assume that $\mathbb{K}[Y] \subset \mathbb{K}[V]$ and $\mathbb{K}[V]$ is generated over $\mathbb{K}[Y]$ by elements $u_1, \dots, u_s$ with $u_1, \dots, u_r$ algebraically independent over $\mathbb{K}[Y]$ and each of $u_{r+1}, \dots, u_s$ are algebraically dependent on $\mathbb{K}[Y]$ and $u_1, \dots, u_r$.

We argue that $r = m - n$. In the proof of Theorem 3.1.17, we showed that the map $\varphi\colon V \to Y$ factors through a map $\psi\colon V \to Y \times \mathbb{K}^r$, and that there exists a principal affine open subset U_h of $Y \times \mathbb{K}^r$ such that the map $\psi^{-1}(U_h) \to U_h$ is finite. Thus

$$m \;=\; \dim X \;=\; \dim V \;=\; \dim \psi^{-1}(U_h) \;=\; \dim U_h \;=\; \dim Y \times \mathbb{K}^r \;=\; n+r\,,$$

proving the claim that $r = m - n$.

For each $m-n < i \leq s$, let $g_i(t)$ be a nonzero univariate polynomial with coefficients in $\mathbb{K}[Y][u_1, \dots, u_{m-n}]$ such that $g_i(u_i) = 0$. Since $u_1, \dots, u_{m-n}$ are algebraically independent over $\mathbb{K}[Y]$, for each $m-n < i \leq s$, the polynomial $g_i(t)$ has positive degree in t. Let $a_i \in \mathbb{K}[Y][u_1, \dots, u_{m-n}]$ be the coefficient of its leading term, which is itself a nonzero polynomial in $u_1, \dots, u_{m-n}$ with coefficients in $\mathbb{K}[Y]$. Let $Z_i \subset Y$ be the variety where all the coefficients of a_i vanish.

Define $U := Y \smallsetminus \bigcup Z_i$. We claim that for $y \in U$, the fiber $\varphi^{-1}(y)$ in V has dimension $m-n$. Since we have shown that the fiber has dimension at least $m-n$, we will show that its dimension is at most $m-n$. Evaluating functions in $\mathbb{K}[Y]$ at the point y identifies $\mathbb{K}[Y]/\mathfrak{m}_y$ with $\mathbb{K}$. Let $v_1, \dots, v_s$ be the images of $u_1, \dots, u_s$ in $\mathbb{K}[\varphi^{-1}(y)] = \mathbb{K}[v_1, \dots, v_s]$, and for $m-n < i \leq s$, let $h_i(t) \in \mathbb{K}[v_1, \dots, v_{m-n}][t]$ be the image of $g_i(t)$. As $\mathbb{K}[\varphi^{-1}(y)] = \mathbb{K}[v_1, \dots, v_s]$, we see that $\varphi^{-1}(y)$ is the subvariety of $\mathbb{K}^s$ given by the algebraic relations among $v_1, \dots, v_s$.

By our construction of Z_i and U, $h_i(t)$ is a non-constant polynomial in t (as the coefficient a_i of the leading term of g_i does not vanish on U), and we have $h_i(v_i) = 0$. Thus, in $\mathbb{K}[\varphi^{-1}(y)]$, $v_{m-n+1}, \dots, v_s$ are algebraically dependent on $v_1, \dots, v_{m-n}$, and so $\varphi^{-1}(y) \subset W$, where W is defined by the polynomials $h_i(v_i)$ (we treat $v_1, \dots, v_s$ as coordinate functions on $\mathbb{K}^s$). Consider the map $\psi\colon W \to \mathbb{K}^{m-n}$ given by $v_1, \dots, v_{m-n}$. Let a be the product of the leading coefficients of $h_{m-n+1}, \dots, h_s$.[†] Then on U_a the leading coefficients of $h_{m-n+1}, \dots, h_s$ are invertible, we may assume that they are monic. This implies that the restriction map $\psi\colon \psi^{-1}(U_a) \to U_a$ is finite and proves that $\dim W \leq m-n$, and in particular $\dim \varphi^{-1}(y) \leq m-n$. Thus fibers of $\varphi^{-1}(y)$ in V, for $y \in U_a$ have dimension $m-n$.

Since X is irreducible and $X \smallsetminus V$ is a closed subvariety, its dimension is less than $m = \dim(X)$. For each irreducible component Z of $X \smallsetminus V$, if $\varphi\colon Z \to Y$ is not dominant, then we set $U_Z := Y \smallsetminus \overline{\varphi(Z)}$. If $\varphi\colon Z \to Y$ is dominant, let U_Z be a dense open subset of Y such that if $y \in U_Z$, then $\varphi^{-1}(y) \cap Z$ has dimension $\dim Z - \dim Y < m - n$. In particular, $\varphi^{-1}(y) \cap Z$ is proper subvariety of $\varphi^{-1}(y) \subset X$. Let U be the intersection of U_a and U_Z for Z an irreducible component of $X \smallsetminus V$. The n U is our set Say this better. □

We use the theorem on dimension of fibers to deduce a useful criterion for a variety to be irreducible.

THEOREM 3.3.15. *Let $\varphi\colon X \to Y$ be a surjective regular map of projective varieties. Suppose that Y is irreducible and every fiber $\varphi^{-1}(y)$ of the map φ is irreducible and they all have the same dimension. Then X is irreducible.*

PROOF. Suppose that n is the dimension of the fibers of φ. Consider the irredundant irreducible decomposition of X. Since $\varphi(X) = Y$, at least one component has image Y under φ.

For each component Z of X with $\varphi(Z) = Y$, let $U_Z \subset Y$ be a dense open subset such that for $y \in U$, $\dim \varphi^{-1}(y) \cap Z = \dim Z - \dim Y =: n_Z$. If $\varphi(Z) \neq Y$, then set $U_Z := Y \smallsetminus \varphi(Z)$.

Let U be the intersection of the U_Z and suppose that $y \in U$. If $\varphi^{-1}(y)$ is irreducible, is is contained in some irreducible component Z of X. Let $\psi\colon Z \to Y$ be the restriction of φ to Z. As $\varphi^{-1}(y) \subset \psi^{-1}(y) \subset \varphi^{-1}(y)$, the fibers are equal, and $n = n_Z$. By our construction, ψ is surjective, so that if $y \in Y$, then $\psi^{-1}(y) \subset \varphi^{-1}(y)$. Also, $\dim \psi^{-1}(y) \geq n_Z = n = \dim \varphi^{-1}(y)$, which implies that $\psi^{-1}(y) \subset \varphi^{-1}(y)$ as $\varphi^{-1}(y)$ is irreducible. But this implies that $Z = X$. □

We close this section with a proof that the resultant polynomial of Section **??** is irreducible. We should also be able to do the discriminant. (Exercise)

REMARK 3.3.16. Suppose that $\mathbb{K}$ is algebraically closed and consider the variety of all triples consisting of a pair of univariate polynomials with a common root, together with a common root,

$$\Sigma \;:=\; \{(f,g,a) \in \mathbb{K}_m[x] \times \mathbb{K}_n[x] \times \mathbb{K} \mid f(a) = g(a) = 0\}\,,$$

[†] Wasn't a already nonzero?

where $\mathbb{K}_d[x]$ is the $(d+1)$-dimensional vector space of polynomials of degree d. This has projections $p\colon \Sigma \to \mathbb{K}_m[x] \times \mathbb{K}_n[x]$ and $\pi\colon \Sigma \to \mathbb{K}$. The image $p(\Sigma)$ is the set of pairs of polynomials having a common root, which is the variety $\mathcal{V}(\mathrm{Res})$ of the resultant polynomial, $\mathrm{Res} \in \mathbb{Z}[f_0, \ldots, f_m, g_0, \ldots, g_n]$, where $f_0, \ldots, g_n$ are the coefficients of f and g,

$$f \;=\; f_0x^m + f_1x^{m-1} + \cdots + f_m \quad \text{and} \quad g \;=\; g_0x^n + g_1x^{n-1} + \cdots + g_n\,.$$

The fiber of π over a point $a \in \mathbb{K}$ consists all pairs of polynomials f, g with $f(a) = g(a) = 0$. Since each equation is linear in the coefficients of the polynomials f and g, this fiber is isomorphic to $\mathbb{K}^m \times \mathbb{K}^n$. Since $\pi\colon \Sigma \to \mathbb{K}$ has irreducible image ($\mathbb{K}$) and irreducible fibers, we see that Σ is irreducible by Theorem 3.3.15, and has dimension $1 + m + n$.

This implies that $p(\Sigma)$ is irreducible. Furthermore, the fiber $p^{-1}(f, g)$ is the set of common roots of f and g. This is a finite set when $f, g \neq (0, 0)$. Thus $p(\Sigma)$ has[†] dimension $1+m+n$, and is thus an irreducible hypersurface in $\mathbb{K}_m[x] \times \mathbb{K}_n[x]$. Let F be a polynomial generating the ideal $\mathcal{I}(p(\Sigma))$, which is necessarily irreducible. As $\mathcal{V}(\mathrm{Res}) = p(\Sigma)$, we must have $\mathrm{Res} = F^N$ for some positive integer N. The formula (2.1.5) shows that $N = 1$ as the resultant polynomial is square-free.

We only need to show that the greatest common divisor of the coefficients of the integer polynomial Res is 1. But this is clear as Res contains the term $f_0^n g_n^m$ with coefficient 1, as we showed in the proof of Lemma 2.1.3. ◇

Exercises for Section 3.3. These need to be updated, as we now have the correct and sophisticated definition of dimension.

1. Prove that the composition $\psi\colon \varphi$ of finite maps $\varphi\colon X \to Y$ and $\psi\colon Y \to Z$ of finite maps is a finite map. (First prove this for affine varieties.)
2. Using the definition of dimension, show that the dimension of a variety is the maximum dimension of its irreducible components.
3. Show that if X is irreducible, and $U \subset X$ is a nonempty open affine subset, then $\dim X = \dim U$.
4. Show that given any finite set $S \subset \mathbb{K}^n$ of points and a point $x \in \mathbb{K}^n$ with $x \notin S$, there is a polynomial that vanishes on S but not at x.
5. Formulate and prove an analog of Corollary 3.3.7 for subvarieties of projective space $\mathbb{P}^n$. Do the same for subvarieties of products $\mathbb{P}^n \times \mathbb{P}^m$ of projective spaces. These may be deduced from Corollary 3.3.7.
6. Show that if X is a projective variety and $x \in X$ lies on an irreducible component Y of X with $Y \neq \{x\}$, then there is a linear form Λ that vanishes at x, but does not canish identically on any irreducible component of X. Deduce that for any posiive integer d there is a form of degree d that vanishes at x, but is not identically zero on any irreducible component of X.
7. Define degree and use the statement of Bézout's theorem in Chapter 2 to deduce the general version of Bézout's theorem.
8. Suppose that f and g are two polynomials on $\mathbb{K}^n$ that are relatively prime. Show that every component of $\mathcal{V}(f, g)$ has dimension $n - 2$.

[†] Appeal to dimension of fibers

9. Use Lemma 2.1.13 to show that $\mathbb{K}^2$ has dimension 2, in the sense of the combinatorial definition of dimension
10. Use Lemma 2.1.13 and induction on the number of polynomials defining a proper subvariety X of $\mathbb{K}^2$ to show that X consists of finitely many irreducible curves and finitely many isolated points.

3.4. Smooth and singular points

Algebraic varieties are not manifolds—the very first example of this book ((1.1.1) in Section 1.1) included the cubic plane curve $\mathcal{V}(y^2 - x^2 - x^3)$. In a neighborhood of the origin, this curve is not a manifold; it has two branches crossing at there. Many other examples likewise have points that do not have a neighborhood in the Euclidean topology which are manifolds, either differentiable or topological. Algebraic varieties have points at which they are differentiable manifolds (smooth points) and others at which they are not manifolds (singular points). We develop some of the basic properties of these smooth and singular points.

Given a polynomial $f \in \mathbb{K}[x]$ and a point $a = (a_1, \ldots, a_n) \in \mathbb{K}^n$, we may write f as a polynomial in new variables $v = (v_1, \ldots, v_n)$, with $v_i := x_i - a_i$ to obtain

$$f \;=\; f(a) \;+\; \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(a) \cdot v_i \;+\; \cdots\,, \tag{3.4.1}$$

where the remaining terms have degrees greater than 1 in the variables v. When $\mathbb{K}$ has characteristic zero, this is the usual multivariate Taylor expansion of f at the point a (and the 'derivatives' in (3.4.1) are derivatives). The coefficient of the monomial v^α in this expansion is the mixed partial derivative of f evaluated at a,

$$\frac{1}{\alpha_1!\alpha_2!\cdots\alpha_n!}\left(\left(\frac{\partial}{\partial x_1}\right)^{\alpha_1}\left(\frac{\partial}{\partial x_2}\right)^{\alpha_2}\cdots\left(\frac{\partial}{\partial x_n}\right)^{\alpha_n} f\right)(a)\,.$$

In the coordinates v for $\mathbb{K}^n$, the degree one term in the expansion (3.4.1) is a linear map

$$d_a f \;:\; \mathbb{K}^n \;\longrightarrow\; \mathbb{K}$$

called the *differential* of f at the point a. Note that for any constant $c \in \mathbb{K}$, we have $d_a(c) = 0$ and $d_a(f + c) = d_a f$.

Definition 3.4.1. Let $X \subset \mathbb{K}^n$ be an affine variety with ideal $\mathcal{I}(X)$. The *(Zariski) tangent space T_aX* to X at the point $a \in X$ is the subspace of $\mathbb{K}^n$ annihilated by the collection $\{d_a f \mid f \in \mathcal{I}(X)\}$ of linear maps. Since

$$\begin{aligned} d_a(f+g) \;&=\; d_a f + d_a g \\ d_a(fg) \;&=\; f(a) d_a g + g(a) d_a f \end{aligned} \tag{3.4.2}$$

we do not need all the polynomials in $\mathcal{I}(X)$ to define T_aX, but may instead take any finite generating set. ◇

Suppose that $X \subset \mathbb{K}^n$ is an affine variety and $a \in X$. Given a nonzero vector $v \in \mathbb{K}^n$, the map $\ell\colon t \mapsto a + tv$ parameterizes the line through a with direction v. For $f \in \mathcal{I}(X)$, if we expand the composition $f(\ell(t))$ in powers of t, we obtain

$$f(\ell(t)) \;=\; 0 \;+\; t(d_a f \cdot v) \;+\; t^2(\cdots)\,,$$

where we suppress the coefficients of t^2 and of higher powers in t. Here, $d_a f \cdot v$ is the usual dot product. When $d_a f \cdot v = 0$, the function $f(\ell(t))$ of t vanishes to order at least 2 at $t = 0$. Thus the nonzero vectors in T_aX are the directions of lines through a whose algebraic order of contact with every hypersurface containing X is at least 2. If X is a manifold in $\mathbb{K}^n$ (real or complex as $\mathbb{K}=\mathbb{R}$ or $\mathbb{K}=\mathbb{C}$), then the Zariski tangent space T_aX is the extrinsic tangent space of X at a. (Extrinsic as it is a linear subspace of $\mathbb{K}^n$.)

Example 3.4.2. Consider the cuspidal cubic $C=\mathcal{V}(f)\subset\mathbb{K}^2$, where $f:=y^2-x^3$. This contains the origin $(0,0)$, and $d_{(0,0)}f$ is the zero linear functional, so that $T_{(0,0)}C=\mathbb{K}^2$, which has dimension two. At every other point $a\in C$, we have $d_af\neq 0$, so that T_aC is one-dimensional. Figure 3.4.1 shows the cubic, its tangent space at the origin and its tangent space at $(\frac{1}{4},\frac{1}{8})$. As is customary, we translate the linear subspace T_aC so that its origin is at the point a, to indicate its relation to the variety. ◇

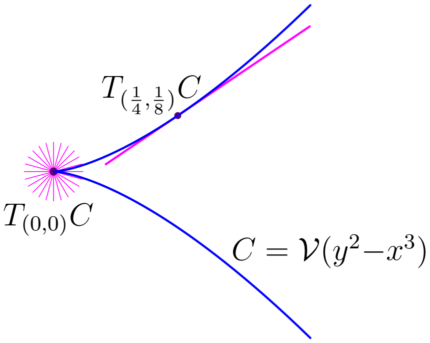


Figure 3.4.1. Zariski tangent spaces of the cuspidal cubic.

Theorem 3.4.3. *Let X be an affine variety and suppose that $\mathbb{K}$ is algebraically closed. Then the set of points of X whose tangent space has minimal dimension is a nonempty Zariski open subset of X.*

Proof. Let $f_1,\dots,f_m$ be generators of $\mathcal{I}(X)$. Writing $F=(f_1,\dots,f_m)$, we let $DF\in\mathrm{Mat}_{m\times n}(\mathbb{K}[x])$ be the matrix whose entry in row i and column j is the partial derivative $\partial f_i/\partial x_j$. For $a\in\mathbb{K}^n$, the components of the vector-valued function

$$\begin{array}{rcl} DF\,:\,\mathbb{K}^n & \longrightarrow & \mathbb{K}^m \\ v & \longmapsto & DF(a)v \end{array}$$

are the dot products $d_af_1\cdot v,\dots,d_af_m\cdot v$ and its kernel is T_aX when $a\in X$.

For each $i=1,\dots,\min\{n,m\}$, the degeneracy locus $\Delta_i\subset\mathbb{K}^n$ is the variety defined by all $i\times i$ subdeterminants (minors) of the matrix DF, and we set $\Delta_{\min\{n,m\}+1}:=\mathbb{K}^n$. Since we may expand any $(i+1)\times(i+1)$ minor along a row or column and express it in terms of $i\times i$ minors, these varieties are nested

$$\Delta_1\ \subset\ \Delta_2\ \subset\ \cdots\ \subset\ \Delta_{\min\{n,m\}}\ \subset\ \Delta_{\min\{n,m\}+1}\ =\ \mathbb{K}^n\,.$$

By definition, a point $a\in\mathbb{K}^n$ lies in $\Delta_{i+1}\smallsetminus\Delta_i$ if and only if the matrix $DF(a)$ has rank i. In particular, if $a\in\Delta_{i+1}\smallsetminus\Delta_i$, then the kernel of $DF(a)$ has dimension $n-i$.

Let i be the minimal index with $X\subset\Delta_{i+1}$. Then

$$X\setminus(X\cap\Delta_i)\ =\ \{a\in X\mid \dim T_aX=n-i\}$$

is a nonempty open subset of X and $n-i$ is the minimum dimension of a tangent space at a point of X. □

The Zariski tangent space of an affine variety $X \subset \mathbb{K}^n$ is defined extrinsically via a given embedding in affine space. We used this to show that there is a nonempty open subset of X where its tangent space has this minimal dimension. The Zariski tangent space also has an intrinsic definition. For any point $a \in X$ and polynomial $f \in \mathbb{K}[x]$, the differential $d_a f$ is a linear map on $\mathbb{K}^n$ that we may restrict to the Zariski tangent space T_aX of X at a. By the formulas (3.4.2) and the definition of T_aX, this linear map is well-defined for elements $f \in \mathbb{K}[X]$ of the coordinate ring of X. Recall that $\mathfrak{m}_a$ is the maximal ideal of $\mathbb{K}[X]$ consisting of regular functions that vanish at a. Since $d_af = d_a(f - f(a))$, the formulas (3.4.2) show that the differential is a linear map from $\mathfrak{m}_a$ to $T_a^*X := \mathrm{Hom}(T_aX, \mathbb{K})$, the space of linear functions on T_aX. By the Leibniz formula for d_a (3.4.2), elements of the square $\mathfrak{m}_a^2$ of $\mathfrak{m}_a$ have zero differential.

Lemma 3.4.4. *For a point $a \in X$, there is a canonical isomorphism $d_a \colon \mathfrak{m}_a/\mathfrak{m}_a^2 \xrightarrow{\sim} T_a^*X$.*

Proof. For a linear form Λ on $\mathbb{K}^n$ and $a \in \mathbb{K}^n$, $d_a(\Lambda - \Lambda(a)) = \Lambda$ on $T_a\mathbb{K}^n = \mathbb{K}^n$. Consequently, if $\ell \in \mathbb{K}[X]$ is the image of $\Lambda - \Lambda(a)$, then $\ell \in \mathfrak{m}_a$ and $d_a\ell$ is the restriction of Λ to $T_aX \subset \mathbb{K}^n$. As every linear form on T_aX is the restriction of a linear form on $\mathbb{K}^n$, we conclude that the map $d_a \colon \mathfrak{m}_a \to T_a^*X$ is surjective.

Suppose that $g \in \mathfrak{m}_a$ and d_ag vanishes on T_aX. Let h be a polynomial whose image in $\mathbb{K}[X]$ is g, and let $f_1, \dots, f_m$ be polynomials that generate $\mathcal{I}(X)$. Since T_aX is defined by the vanishing of $d_af_1, \dots, d_af_m$, and d_ah vanishes on T_aX, there are $\lambda_1, \dots, \lambda_m \in \mathbb{K}$ such that

$$d_ah \;=\; \lambda_1 d_af_1 \;+\; \lambda_2 d_af_2 \;+\; \cdots \;+\; \lambda_m d_af_m\,. \tag{3.4.3}$$

Set $h_1 := h - (\lambda_1 f_1 + \cdots + \lambda_m f_m)$. If we expand h_1 in the parameters $v_1, \dots, v_n$, where $v_i = x_i - a_i$ (as in (3.4.1)), then its constant term vanishes (as h and each f_i vanish at a) and its linear terms also vanish, by (3.4.3). Thus h_1 lies in the ideal $\langle v_1, \dots, v_n\rangle^2$. Since $g \in \mathbb{K}[X]$ is the image of h_1 and $\mathfrak{m}_a \subset \mathbb{K}[X]$ is the image of $\langle v_1, \dots, v_n\rangle$, we conclude that $g \in \mathfrak{m}_a^2$. This completes the proof. □

Let $a \in X$. We may therefore define the Zariski tangent space T_aX independent of any embedding of X to be the vector space $(\mathfrak{m}_a/\mathfrak{m}_a^2)^*$. Suppose that we have a regular map $\varphi \colon X \to Y$ of affine varieties and point $a \in X$. The functorial pullback map $\varphi^* \colon \mathbb{K}[Y] \to \mathbb{K}[X]$ sends $\mathfrak{m}_{\varphi(a)}$ to $\mathfrak{m}_a$ as a regular function $g \in \mathbb{K}[Y]$ that vanishes at $\varphi(a)$ has pullback that vanishes at a. This also induces a map $\varphi^* \colon \mathfrak{m}_{\varphi(a)}/\mathfrak{m}_{\varphi(a)}^2 \to \mathfrak{m}_a/\mathfrak{m}_a^2$. Taking linear duals, we obtain a functorial linear map between tangent spaces $d_a\varphi \colon T_aX \to T_{\varphi(a)}Y$.

By Exercise 2, tangent spaces of affine varieties are unchanged in passing to principal affine open subsets. We use this to define Zariski tangent spaces for any variety. Given a variety X and a point $a \in X$, define T_aX to be the Zariski tangent space T_aU for any affine open subset $U \subset X$ containing a.

Suppose that X is irreducible and let m be the minimum dimension of a tangent space of X. By Theorem 3.4.3, the points of X whose tangent space has this minimum dimension form a nonempty open and hence dense subset of X. Call these points of X *smooth* points and write X_{sm} for the nonempty open subset of smooth points. The complement $X \smallsetminus X_{\mathrm{sm}}$ is the set X_{sing} of *singular* points of X. The set of smooth points is dense in X, for otherwise we may write the irreducible variety X as a union $\overline{X_{\mathrm{sm}}} \cup X_{\mathrm{sing}}$ of two proper closed subsets.

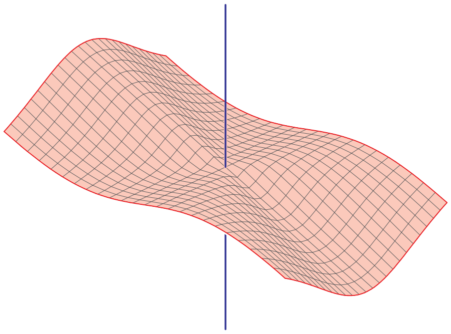
When $\mathbb{K} = \mathbb{C}$, the set of smooth points of X forms a complex manifold of whose dimension at a point $a \in X_{\mathrm{sm}}$ is $\dim_{\mathbb{C}} T_aX$. This is a consequence of standard results about differential manifolds. Similarly, when $\mathbb{K} = \mathbb{R}$, if X has a smooth real point, then the set of smooth points of X is nonempty and forms a manifold whose dimension at a point $a \in X_{\mathrm{sm}}$ is $\dim_{\mathbb{R}} T_aX$. This restriction is necessary, for it is possible that $X_{\mathrm{sm}} = \emptyset$ for a real variety. For example, the real algebraic variety $X = \mathcal{V}(y^2 + x^2)$ has only one real point, the origin, where it is singular as $d_{(0,0)}(y^2 + x^2) = 0$.

Thus when X is smooth and irreducible and $\mathbb{K} = \mathbb{C}$, the dimension of the tangent space to X at a smooth point is equal to its dimension as a manifold. This remains true for any irreducible variety, smooth or not, and for any algebraically closed field. This gives a second definition of dimension which is distinct from the combinatorial definition of Definition.

We have the following facts concerning the locus of smooth and singular points on a real or complex variety. this needs expansion/explanation.

Proposition 3.4.5. *The set of smooth points of an irreducible complex affine subvariety X of dimension d whose complex local dimension in the Euclidean topology is d is dense in the Euclidean topology.*

Example 3.4.6. Irreducible real algebraic varieties need not have this property. The Cartan umbrella $\mathcal{V}(z(x^2 + y^2) - x^3)$



is a connected irreducible surface in $\mathbb{R}^3$ where the local dimension of its smooth points is either 1 (along the z axis or 'handle') or 2 (along the 'canopy' of the umbrella). ⋄

Use this relation of dimension to tangent space to prove some of the theorems about dimension of varieties and then images under maps. This will be a precursor to the Bertini Theorems. These are needed in later sections in Toric varieties and in numerical algebraic geometry. There is also scope to add a couple of pages to this section.

Exercises for Section 3.4.

1. Using the consequence of Lemma 3.4.4 that the Zariski tangent spaces of an affine variety are intrinsic to give another proof that the cuspidal cubic $\mathcal{V}(y^2 - x^3)$ is not

isomorphic to either the parabola $\mathcal{V}(y-x^2)$ or to the line $\mathbb{K}^1$. (This was shown in Example 1.3.1 of Section 1.3 by other means.)

2. Let $X \subset \mathbb{K}^n$ be an affine variety, $a \in X$, and $f \in \mathbb{K}[X]$ a regular function that does not vanish at a. Using the embedding $X_f \hookrightarrow \mathbb{K}^{n+1}$ given by $x \mapsto (x, f(x))$, show that the two tangent spaces T_aX and $T_{(a,f(a))}X_f$ are isomorphic. We recommend using the definition of T_aX as given in Definition 3.4.1.
3. What is the dimension of the Zariski tangent space along the handle of the Cartan umbrella (the locus of points $(0,0,z)$ for $z \in \mathbb{C}$).
4. Compute some examples of Zariski tangent spaces of differing dimensions.

3.5. Bertini's Theorem

An essential result in algebraic geometry is that the intersection of a smooth variety with a general hypersurface is a smooth subvariety of codimension 1. Another is that the general fiber of a map from a smooth variety is smooth. This is an algebraic counterpart of Sard's Theorem. These results refine what we have shown about dimension and underlie numerical algorithms that we present in Chapter 4 for studying complex varieties on a computer. This result was only proven in the 20th century, and we present it here.

THEOREM 3.5.1 (Bertini's Theorem). *Suppose that X and Y are varieties over an algebraically closed field of characteristic zero with X smooth, and that $\varphi\colon X \to Y$ is a regular map with $\varphi(X)$ dense in Y. Then there is a dense open subset $U \subset Y$ such that the fiber $\varphi^{-1}(y)$ is smooth for all $y \in U$.*

We let $m := \dim X$ and $n := \dim Y$. To prove this, assume that X is a smooth variety, and let us replace Y by an open subset such that every component of a fiber $\varphi^{-1}(y)$ has dimension $m-n$, and then replace X by the preimage of this open subset. The existence of such a subset is guaranteed by Theorem 3.3.14. We may also assume that Y is smooth.

LEMMA 3.5.2. *With X ands Y as above, for any point $y \in Y$, the fiber $\varphi^{-1}(y)$ is nonsingular if and only if for all $x \in \varphi^{-1}(y)$, the differential map $d_x\varphi\colon T_xX \to T_yY$ is surjective.*

PROOF. Let $y \in Y$ and $x \in \varphi^{-1}(y)$. We show that the tangent space at x to the fiber $\varphi^{-1}(y)$ has dimension equal to $m-n$. As this is the dimension of the fiber, we conclude that the fiber is smooth at x.

We claim that the tangent space $T_x\varphi^{-1}(y)$ to the fiber is a linear subspace of the kernel of $d_x\varphi$, that is, the composition $T_x\varphi^{-1}(y) \hookrightarrow T_xX \xrightarrow{d_x\varphi} T_yY$ is zero. This is a local statement, so we may assume that X and Y and $\varphi^{-1}(y)$ are all affine varieties, and let us consider the corresponding maps on the maximal ideals of the point. Recall that the fiber $\varphi^{-1}(y)$ is defined in X by $\varphi^*\mathfrak{m}_y$. Thus the composition

$$\mathfrak{m}_y \xrightarrow{\varphi^*} \mathfrak{m}_x \longrightarrow \mathfrak{m}_x/\mathfrak{m}_y \subset \mathfrak{m}_{x,\varphi^{-1}(y)}$$

is zero. The last term, $\mathfrak{m}_{x,\varphi^{-1}(y)}$ is the maximal ideal at x in the fiber $\varphi^{-1}(y)$. Write $\overline{\mathfrak{m}}_x$ for this maximal ideal. Thus the composition

$$\mathfrak{m}_y/\mathfrak{m}_y^2 \longrightarrow \mathfrak{m}_x/\mathfrak{m}_x^2 \longrightarrow \overline{\mathfrak{m}}_x/\overline{\mathfrak{m}}_x^2$$

is zero. Taking linear duals implies the result about the tangent spaces.

Suppose that $d_x\varphi$ is surjective. Then

$$\dim T_x\varphi^{-1}(y) \;\leq\; \dim\ker d_x\varphi \;=\; \dim T_xX - \dim T_yY \;=\; m-n\,,$$

as X and Y are smooth. Since all components of the fiber $\varphi^{-1}(y)$ have dimension $m-n$, we have that $\dim T_x\varphi^{-1}(y) \geq m-n$, which implies equality. Thus $\varphi^{-1}(y)$ is nonsingular at x when $d_x\varphi$ is surjective. □

LEMMA 3.5.3. *Let X and Y be irreducible smooth varitеties over an algebraically closed field of charateristic zero and suppose that the $\varphi\colon X \to Y$ is a map with $\varphi(X)$ dense in Y. Then there is a nonempty open subset V of X such that $d_x\varphi$ is surjective for all $x \in V$.*

Proof. Replacing X and Y by affine open subsets, we may assume that they are both affine and that $\varphi(X) = Y$. Taking linear duals, the surjectivity of $d_x\varphi$ is equivalent to the injectivity of the map $f^*\colon \mathfrak{m}_y/\mathfrak{m}_y^2 \to \mathfrak{m}_x/\mathfrak{m}_x^2$, where $y = \varphi(x)$.

Let $u_1, \dots, u_n \in \mathbb{K}[Y]$ be local parameters[†] at $\varphi(x) = y$. These are algebraically independent in $\mathbb{K}[Y]$ and as $\varphi^*\colon \mathbb{K}[Y] \hookrightarrow \mathbb{K}[X]$ is an injection, they may be regarded as algebraically independent elements of $\mathbb{K}[X]$. Complete these to $u_1, \dots, u_m \in \mathbb{K}[X]$, a maximal set of algebraically independent elements of $\mathbb{K}[X]$.

Let us assume that $X \subset \mathbb{K}^M$ with coordinate functions $x_1, \dots, x_M$, which generate $\mathbb{K}[X]$. At every point $x \in X$, their differentials $d_x x_1, \dots, d_x x_M$ generate $\mathfrak{m}_x/\mathfrak{m}_x^2$. We show that there is a nonempty Zariski open subset $V \subset X$ such that for $a \in V$ we have $d_a x_i \in \operatorname{span}\{d_a u_1, \dots, d_a u_m\}$, for each $i = 1, \dots, M$. This implies that $\dim T_a X \leq m$, with equality when these differentials are linearly independent. Since $\dim T_a X \geq \dim X = m$, these differentials $\{d_a u_1, \dots, d_a u_m\}$ form a basis for $\mathfrak{m}_x/\mathfrak{m}_x^2$. In particular $\{d_a u_1, \dots, d_a u_n\}$ are linearly independent. If $b = f(a)$, this implies that $f^*\colon \mathfrak{m}_b/\mathfrak{m}_b^2 \to \mathfrak{m}_a/\mathfrak{m}_a^2$ is injective and so $d_a f\colon T_a X \to T_b Y$ is surjective.

Let i satisfy $1 \leq i \leq M$. Then the coordinate function x_i is algebraic over $\mathbb{K}[u_1, \dots, u_m]$, so there is a nonzero polynomial $g_i \in \mathbb{K}[z, t_1, \dots, t_m]$ such that $g_i(x_i, u_1, \dots, u_m) = 0$ in $\mathbb{K}[X]$. We may assume that g_i is irreducible (as X is irreducible) and of minimal degree in x_i.

Write $g_i = z^r c_0 + \cdots z c_{r-1} + c_r$ with $c_j \in \mathbb{K}[t_1, \dots, t_m]$ and $r \geq 1$. Since $\mathbb{K}$ has characteristic zero $\partial g_i/\partial z$ is not the zero polynomial, and we have that $\partial g_i/\partial z(x_i, u_1, \dots, u_m) \neq 0$ in $\mathbb{K}[X]$ by the minimality of g_i. Since $g_i(x_i, u_1, \dots, u_m) = 0$, its differential at a point $a \in X$ vanishes, and thus by the properties of d_a we have

$$0 \;=\; \frac{\partial g_i}{\partial z}(a) d_a x_i + x_i^r d_a c_0(u_1, \dots, u_m) + \cdots + d_a c_r(u_1, \dots, u_m)\,.$$

The properties of d_a also imply that $x_i^s d_a c_{r-s}(u_1, \dots, u_m)$ lies in the span of $\{d_a u_1, \dots, d_a u_m\}$. If $\partial g_i/\partial z(a) \neq 0$, then this computation implies that $d_a x_i \in \operatorname{span}\{d_a u_1, \dots, d_a u_m\}$. Let $V \subset X$ be the complement of the union of proper subvarieties $\mathcal{V}(\partial g_i/\partial z)$ for $i = 1, \dots, M$. As X is irreducible and for each i, $\partial g_i/\partial z \neq 0$, V is nonempty. □

Proof of Bertini's Theorem. Let $Z \subset X$ be the set of points $x \in X$ such that $d_x\varphi$ is not surjective. Then Z is a subvariety of X, as the non-surjectivity of $d_x\varphi$ is given by the vanishing of some minors. make this explicit earlier, perhaps in the section on tangent spaces. By Lemma 3.5.2 Bertini's Theorem is equivalent to the statement that $\varphi(Z)$ lies in a proper subvariety of Y.

Otherwise, $\varphi(Z)$ is dense in Y. Applying Lemma 3.5.3, there is a nonempty open subset $V \subset Z$ such that if $a \in V$ then the map $d_a\varphi\colon T_a Z \to T_{\varphi(a)} Y$ is surjective. As $T_a Z \subset T_a X$, this implies that $d_a\varphi\colon T_a X \to T_{\varphi(a)} Y$ is surjective, which is a contradiction. □

Exercises for Section 3.5.

[†] Need to define local paramters in Section on tangent spaces.

3.6. Hilbert functions

The homogeneous coordinate ring $\mathbb{K}[X]$ of a projective variety $X \subset \mathbb{P}^n$ is an invariant of the variety X which determines it up to a linear automorphisms of $\mathbb{P}^n$. Basic numerical invariants, such as the dimension of X, are encoded in the combinatorics of $\mathbb{K}[X]$ and expressed through its Hilbert function. The coordinate ring of an affine variety $Y \subset \mathbb{K}^n$ also has a Hilbert function which encodes its dimension, and it equals the Hilbert function of its projective closure $\overline{Y} \subset \mathbb{P}^n$.

In Section 1.4, we introduced the homogeneous coordinate ring $\mathbb{K}[X] = \mathbb{K}[x_0, \ldots, x_n]/\mathcal{I}(X)$ of a projective variety X. This ring is graded,

$$\mathbb{K}[X] \;=\; \bigoplus_{r=0}^{\infty} \mathbb{K}[X]_r\,,$$

and its degree r component $\mathbb{K}[X]_r$ consists of images of all degree r homogeneous polynomials, that is, it is the quotient $\mathbb{K}[x_0, \ldots, x_n]_r/\mathcal{I}(X)_r$. This is a finite-dimensional $\mathbb{K}$-vector space as $\dim_{\mathbb{K}} \mathbb{K}[x_0, \ldots, x_n]_r = \binom{n+r}{n}$. The most basic numerical invariant of this ring is the *Hilbert function* of X, whose value at $r \in \mathbb{N}$ is the dimension of the r-th graded component of $\mathbb{K}[X]$,

$$\mathrm{HF}_X(r) \;:=\; \dim_{\mathbb{K}}(\mathbb{K}[X]_r)\,.$$

This is also the number of linearly independent degree r homogeneous polynomials on X. We may also define the Hilbert function of a homogeneous ideal $I \subset \mathbb{K}[x_0, \ldots, x_n]$,

$$\mathrm{HF}_I(r) \;:=\; \dim_{\mathbb{K}}\bigl(\mathbb{K}[x_0, \ldots, x_n]_r/I_r\bigr)\,.$$

Note that $\mathrm{HF}_X = \mathrm{HF}_{\mathcal{I}(X)}$.

EXAMPLE 3.6.1. The space curve C of Figure???[2] is the image of $\mathbb{P}^1$ under the map

$$\varphi \,:\; \mathbb{P}^1 \ni [s,t] \;\longmapsto\; [s^3, s^2t, st^2, 2t^3{-}2s^2t] \in \mathbb{P}^3\,.$$

If $\mathbb{P}^3$ has coordinates $[w,x,y,z]$, then $C = \mathcal{V}(2y^2 - xz - 2yw,\ 2xy - 2xw - zw,\ x^2 - yw)$. This map has the property that the pullback $\varphi^*(f)$ of a homogeneous form f of degree r is a homogeneous polynomial of degree $3r$ in the variables s,t, and all homogeneous forms of degree $3r$ in s,t occur as pullbacks. Since there are $3r+1$ forms of degree $3r$ in s,t, we see that $\mathrm{HF}_C(r) = 3r+1$. ◇

The Hilbert function of a homogeneous ideal I may be computed using Gröbner bases. First observe that any reduced Gröbner basis of I consists of homogeneous polynomials.

THEOREM 3.6.2. *Any reduced Gröbner basis for a homogeneous ideal I consists of homogeneous polynomials.*

PROOF. Buchberger's algorithm is friendly to homogeneous polynomials. That is, if f and g are homogeneous, then so is $\mathrm{Spol}(f,g)$. Similarly, the reduction of one homogeneous polynomial by another is a homogeneous polynomial. Since Buchberger's algorithm consists of forming S-polynomials and their reductions, if given homogeneous generators of an ideal, it will compute a reduced Gröbner basis consisting of homogeneous polynomials.

[2] Need a different space cubic

A homogeneous ideal I has a finite generating set B consisting of homogeneous polynomials. Therefore, given a monomial order, Buchberger's algorithm will transform B into a reduced Gröbner basis G consisting of homogeneous polynomials. As reduced Gröbner bases are uniquely determined by the term order, Buchberger's algorithm will transform any generating set into G. □

A consequence of Theorem 3.6.2 is that it is no loss of generality to use graded term orders when computing a Gröbner basis of a homogeneous ideal. Theorem 3.6.2 also implies that the linear isomorphism of Theorem **??** between $\mathbb{K}[x_0,\dots,x_n]/I$ and $\mathbb{K}[x_0,\dots,x_n]/\operatorname{in}(I)$ respects degree and so the Hilbert functions of I and of $\operatorname{in}(I)$ agree.

Corollary 3.6.3. *Let I be a homogeneous ideal. Then for any term order, $\mathrm{HF}_I(r) = \mathrm{HF}_{\operatorname{in}(I)}(r)$, the number of standard monomials of degree r.*

Proof. The image in $\mathbb{K}[x_0,\dots,x_n]/I$ of a standard monomial of degree r lies in the rth graded component. Since the images of standard monomials are linearly independent, we only need to show that they span the degree r graded component of this ring. Let $f \in \mathbb{K}[x_0,\dots,x_n]$ be a homogeneous form of degree r and let G be a reduced Gröbner basis for I. Then the reduction $f \bmod G$ is a linear combination of standard monomials. Each of these will have degree r as G consists of homogeneous polynomials and the division algorithm is homogeneous-friendly. □

Example 3.6.4. In the degree-reverse lexicographic monomial order with $x \succ y \succ z \succ w$, the polynomials

$$\underline{2y^2} - xz - 2yw\,,\ \underline{2xy} - 2xw - zw\,,\ \underline{x^2} - yw\,,$$

form the reduced Gröbner basis for the ideal of the cubic space curve C of Example 3.6.1. The initial terms are underlined, so the initial ideal is the monomial ideal $\langle y^2, xy, x^2\rangle$.

The standard monomials of degree r are exactly the set

$$\{z^aw^b,\ xz^cw^d,\ yz^cw^d \mid a+b=r,\ c+d=r-1\}$$

and so there are exactly $r+1+r+r = 3r+1$ standard monomials of degree r. This agrees with the Hilbert function of C, as computed in Example 3.6.1. ◇

By Corollary 3.6.3 we need only consider monomial ideals when studying Hilbert functions of arbitrary homogeneous ideals. Once again we see how some questions about arbitrary ideals may be reduced to the same questions about monomial ideals, which may be answered using combinatorial arguments.

Because an ideal and its saturation both define the same projective scheme, and because Hilbert functions are difficult to compute, we introduce the Hilbert polynomial.

Definition 3.6.5. Two functions $f, g\colon \mathbb{N} \to \mathbb{N}$ are *stably equivalent* if $f(r) = g(r)$ for r sufficiently large. ◇

We prove the following result at the end of this section.

Proposition-Definition 3.6.6. *The Hilbert function of a homogeneous ideal I is stably equivalent to a polynomial, HP_I, called the Hilbert polynomial of I.*

The Hilbert polynomial of a projective variety encodes many of its numerical invariants. We explore two such invariants.

DEFINITION 3.6.7. Let $X \subset \mathbb{P}^n$ be a projective variety and suppose that the initial term of its Hilbert polynomial is

$$\mathrm{in}(\mathrm{HP}_X(r)) \ = \ d\frac{r^m}{m!}\,.$$

Then the *dimension of X* is the degree, m, of the Hilbert polynomial and the coefficient d is the *degree of X*. This is the third, and so far, independent definition we have given of dimension. ◇

We computed the Hilbert function of the curve $C \subset \mathbb{P}^3$ of Example 3.6.1 to be $3r + 1$. This is also its Hilbert polynomial, and we see that C has dimension 1 and degree 3, which justifies our calling it a cubic space curve.

We may similarly define the dimension and degree of a homogeneous ideal I, using the leading term of its Hilbert polynomial.

EXAMPLE 3.6.8. In Exercise 3 you are asked to show that if X consists of d distinct points, then the Hilbert polynomial of X is the constant, d. Thus X has dimension 0 and degree d.

Suppose that X is a linear space, $\mathbb{P}(V)$, where $V \subset \mathbb{K}^{n+1}$ has dimension $m{+}1$. We may choose coordinates $x_0, \dots, x_n$ on $\mathbb{P}^n$ so that V is defined by $x_{m+1} = \cdots = x_n = 0$, and so $\mathbb{K}[X] \simeq \mathbb{K}[x_0, \dots, x_m]$. Then $\mathrm{HF}_X(r) = \binom{r+m}{m}$. As a polynomial in r this has initial term $\frac{r^m}{m!}$ and so X has dimension m and degree 1.

Suppose that $I = \langle f \rangle$, where f is a homogeneous polynomial of degree d. Then

$$\bigl(\mathbb{K}[x_0, \dots, x_n]/I\bigr)_r \ = \ \frac{\mathbb{K}[x_0, \dots, x_n]_r}{f \cdot \mathbb{K}[x_0, \dots, x_n]_{r-d}}\,.$$

Since multiplication by f is injective, it follows that $\mathrm{HF}_I(r) = \binom{r+n}{n} - \binom{r-d+n}{n}$, where if $a < n$, then $\binom{a}{n} = 0$. This is a polynomial in r for $r + n \geq d$. By Exercise 4, the leading term of the Hilbert polynomial of I is $d\frac{r^{n-1}}{(n-1)!}$, and so I has dimension $n{-}1$ and degree d. When f is square-free, we have that $I = \mathcal{I}(\mathcal{V}(f))$. Thus the hypersurface defined by f has dimension $n{-}1$ and degree equal to the degree of f. ◇

REMARK 3.6.9. Suppose that $Y \subset \mathbb{K}^n$ is an affine variety with coordinate ring $\mathbb{K}[Y]$. This ring is not graded, but it does have an increasing sequence of finite-dimensional subspaces $\mathbb{K}[Y]_{\leq r}$ for $r \in \mathbb{N}$, where $\mathbb{K}[Y]_{\leq r}$ is image in $\mathbb{K}[Y]$ of the linear span of polynomials in $\mathbb{K}[x_1, \dots, x_n]$ of degree at most r. We define the Hilbert function HF_Y of the affine variety Y to be the function whose value at $r \in \mathbb{N}$ is $\dim_{\mathbb{K}} \mathbb{K}[Y]_{\leq r}$. If $I \subset \mathbb{K}[x_1, \dots, x_n]$ is an ideal, then we may define its Hilbert function in the same way.

As in Section 1.4, if $U_0 = \{x \in \mathbb{P}^n \mid x_0 \neq 0\}$, then $U_0 \simeq \mathbb{K}^n$ and we may regard Y as a subvariety of U_0. Let $X \subset \mathbb{P}^n$ be its Zariski closure. In Exercise 5 you will show that for any $r \geq 0$, dehomogenization induces a linear isomorphism $\mathbb{K}[X]_r \xrightarrow{\sim} \mathbb{K}[Y]_{\leq r}$, which implies that $\mathrm{HF}_Y = HF_X$, and thus the equality of affine and projective Hilbert functions. ◇

We need some additional results on inequalities of Hilbert functions and Hilbert polynomials. You are asked to prove the following lemma in Exercise 6

Lemma 3.6.10. *Suppose that $f, g\colon \mathbb{N} \to \mathbb{N}$ are functions that satisfy $f(r) \leq g(r)$ for all $r \in \mathbb{N}$. If, for $r \geq r_0$, f and g are equal to polynomials F and G, respectively, then $\deg F \leq \deg G$. If additionally there is an integer $a \geq 0$ with $g(r-a) \leq f(r)$ for $r \geq a$, then $\deg F = \deg G$ and their leading coefficients are equal.*

Theorem 3.6.11. *Suppose that X is a projective variety of dimension m. Every subvariety of X has dimension at most m, at least one irreducible component of X has dimension m, and the degree of X is the sum of the degrees of its irreducible components of dimension m.*

Proof. Let Y be a subvariety of X. Then the coordinate ring of Y is a quotient of the coordinate ring of X, so $HF_Y(r) \leq HF_X(r)$ for all r. By Lemma 3.6.10, the degree of the Hilbert polynomial of Y is at most the degree of the Hilbert polynomial of X, and thus $\dim Y \leq \dim X$.

Suppose that $X = X_1 \cup \cdots \cup X_k$ is the decomposition of X into irreducible components. Consider the map of graded vector spaces which is induced by restriction

$$\mathbb{K}[X] \ \longrightarrow\ \mathbb{K}[X_1] \oplus \mathbb{K}[X_2] \oplus \cdots \oplus \mathbb{K}[X_k]\,.$$

This is injective, which implies the inequality

$$\mathrm{HF}_X(r) \ \leq\ \sum_{i=1}^{r} \mathrm{HF}_{X_i}(r)\,. \tag{3.6.1}$$

Passing to Hilbert polynomials, Lemma 3.6.10 implies there is a component X_i of X whose Hilbert polynomial has degree at least m, which implies that $\dim X_i = \dim X$.

A consequence of Lemma 3.6.12, which is stated below, is that there is a number $a \geq 0$ such that when $r > a$, we have

$$\sum_{i=1}^{r} \mathrm{HF}_{X_i}(r-a) \ \leq\ \mathrm{HF}_X(r)\,. \tag{3.6.2}$$

Each Hilbert function is eventually equal to the corresponding Hilbert polynomial, so that the sum in (3.6.1) is eventually equal to the sum, $\sum_i \mathrm{HP}_{x_i}(r)$ of Hilbert polynomials of the components. By Lemma 3.6.10 and the inequalities (3.6.1) and (3.6.2), the polynomial $\sum_i \mathrm{HP}_{x_i}(r)$ has the same degree and leading term as does the Hilbert polynomial of X. But this leading term is the sum of leading terms of the Hilbert polynomials of its components of dimension m, which completes the proof. □

Lemma 3.6.12. *Suppose that $X = X_1 \cup \cdots \cup X_k$ is the decomposition of X into irreducible components. There is a positive integer a such that when $r \geq a$, we have*

$$\sum_{i=1}^{k} \mathrm{HF}_{X_i}(r-a) \ \leq\ \mathrm{HF}_X(r)\,.$$

Proof. For each $i = 1, \ldots, k$, let $f_i \in \mathbb{K}[X]$ be a nonzero element that vanishes on $X \smallsetminus X_i$. As $0 \neq f_i$, it also does not vanish on X_i (for otherwise it would be identically zero on X), so it has nonzero image in the domain $\mathbb{K}[X_i]$. Consider the map $\mu\colon g \mapsto f_i g$ on $\mathbb{K}[X]$. If $g \in \mathcal{I}(X_i)$, then $f_i g$ is identically zero on X, and hence 0 in $\mathbb{K}[X]$, so that $\mathcal{I}(X_i) \subset \ker \mu$, and thus multiplication by f_i gives a well-defined map $\mathbb{K}[X_i] \to \mathbb{K}[X]$.

Consequently, the expression $(g_1, \ldots, g_k) \mapsto f_1 g_1 + \cdots + f_k g_k$ induces a map

$$\varphi \,:\, \mathbb{K}[X_1] \oplus \cdots \oplus \mathbb{K}[X_k] \;\longrightarrow\; \mathbb{K}[X]\,.$$

This is an injection because if $f_1 g_1 + \cdots + f_k g_k = 0$, then $g_i = 0$ for all i. Indeed, the image of $f_1 g_1 + \cdots + f_k g_k$ in $\mathbb{K}[X_i]$, which is $f_i g_i$, is also zero. But this implies that $g_i = 0$ as f_i is a nonzero element of the integral domain $\mathbb{K}[X_i]$.

To complete the proof, let a be any number so that $a \geq \deg(f_i)$ for all i. If for each i we replace f_i by $f_i g_i$ where $0 \neq g_i \in \mathbb{K}[X_i]$ has degree $a - \deg(f_i)$, then we may assume that each f_i has degree a. This the map φ restricts to an injection

$$\varphi \,:\, \mathbb{K}[X_1]_{r-a} \oplus \cdots \oplus \mathbb{K}[X_k]_{r-a} \;\longrightarrow\; \mathbb{K}[X]_r\,.$$

which proves the inequality of the corollary. □

We use combinatorics to prove the following at the end of the section. Do it

Theorem 3.6.13. *When I is a monomial ideal, the degree of HP_I is the dimension of the largest linear subspace contained in $\mathcal{V}(I) \subset \mathbb{P}^n$.*

As $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$, we deduce the following corollary.

Corollary 3.6.14. *If I is a monomial ideal, then the Hilbert polynomials HP_I and $\mathrm{HP}_{\sqrt{I}}$ have the same degree.*

Theorem 3.6.15. *Let X be a subvariety of $\mathbb{P}^n$ and suppose that $f \in \mathbb{K}[X]$ has degree d and is not a zero divisor. Then the ideal $\langle \mathcal{I}(X), f\rangle$ has dimension $\dim(X) - 1$ and degree $d \cdot \deg(X)$.*

If X is irreducible, then every proper subvariety of X has dimension at most $m-1$ and X has a subvariety of dimension $m-1$.

Proof. For $r \geq d$, the degree r component of the quotient ring $\mathbb{K}[x_0, \ldots, x_n]/\langle \mathcal{I}(X), f\rangle$ is

$$\mathbb{K}[X]_r / f \cdot \mathbb{K}[X]_{r-d}\,, \tag{3.6.3}$$

and so it has dimension $\dim_{\mathbb{K}}(\mathbb{K}[X]_r) - \dim_{\mathbb{K}}(f \cdot \mathbb{K}[X]_{r-d})$.

Suppose that r is large enough so that the Hilbert function of X is equal to its Hilbert polynomial at $r-d$ and all larger integers. Since f is not a zero divisor, multiplication by f is injective. Thus the dimension of the quotient (3.6.3) is

$$\mathrm{HP}_X(r) - \mathrm{HP}_X(r-d)\,.$$

which is a polynomial of degree $\dim(X)-1$ and leading coefficient $d\cdot\deg(X)/(\dim(X)-1)!$, which is a consequence of Exercise 4.

Suppose now that X is irreducible. Let Y be a proper subvariety of X, and let $0 \neq f \in \mathcal{I}(Y) \subset \mathbb{K}[X]$. Since $\mathbb{K}[X]/\langle f\rangle \twoheadrightarrow \mathbb{K}[X]/\mathcal{I}(Y) = \mathbb{K}[Y]$, we see that the Hilbert polynomial of $\mathbb{K}[Y]$ has degree at most that of $\mathbb{K}[X]/\langle f\rangle$, which is $d-1$.

Suppose that $0 \neq f \in \mathbb{K}[X]$ and let $I = \langle \mathcal{I}(X), f\rangle$, where we write f both for the element $f \in \mathbb{K}(X)$ and for a homogeneous polynomial which restricts to it. If I is radical, then we have just shown that $\mathcal{V}(I) \subset X$ is a subvariety of dimension $d{-}1$. Otherwise, let $\succ$ be a monomial order, and observe that we have the chain of inclusions

$$\text{in}(I) \ \subset\ \text{in}(\sqrt{I}) \ \subset\ \sqrt{\text{in}(I)}\ . \tag{3.6.4}$$

Indeed, $I \subset \sqrt{I}$, which implies that $\text{in}(I) \subset \text{in}(\sqrt{I})$. For the other inclusion, let $f \in \sqrt{I}$. Then $f^N \in I$ for some $N \in \mathbb{N}$. But then $\text{in}(f)^N = \text{in}(f^N) \in \text{in}(I)$, and so $\text{in}(f) \in \sqrt{\text{in}(I)}$.

This chain of inclusions (3.6.4) implies surjections of the corresponding coordinate rings, and therefore the inequalities of Hilbert functions, $\text{HF}_{\text{in}(I)}(r) \geq \text{HF}_{\text{in}(\sqrt{I})}(r) \geq \text{HF}_{\sqrt{\text{in}(I)}}(r)$. This we deduce the corresponding chain of inequalities of degrees of Hilbert polynomials,

$$\deg(\text{HP}_{\text{in}(I)}) \ \geq\ \deg(\text{HP}_{\text{in}(\sqrt{I})}) \ \geq\ \deg(\text{HP}_{\sqrt{\text{in}(I)}})\,.$$

By Corollary 3.6.14, $\deg(\text{HP}_{\text{in}(I)}) = \deg(\text{HP}_{\sqrt{\text{in}(I)}})$, so all three degrees are equal. As $\text{HP}_I = \text{HP}_{\text{in}(I)}$, and the same for $\sqrt{I}$, which is the ideal of $\mathcal{V}(I)$, we conclude that $\mathcal{V}(I)$ is a subvariety of X having dimension $d{-}1$. □

We may now show that the combinatorial definition of dimension agrees with the definition given in terms of Hilbert function.

Corollary 3.6.16 (Combinatorial definition of dimension). *The dimension of a variety X is the length of the longest decreasing chain of irreducible subvarieties of X. If*

$$X \ \supset\ X_0 \ \supsetneq\ X_1 \ \supsetneq\ X_2 \ \supsetneq\ \cdots \ \supsetneq\ X_m \ \supsetneq\ \emptyset\,,$$

is such a chain of maximal length, then X has dimension m.

Proof. Suppose that

$$X \ \supset\ X_0 \ \supsetneq\ X_1 \ \supsetneq\ X_2 \ \supsetneq\ \cdots \ \supsetneq\ X_m \ \supsetneq\ \emptyset$$

is a chain of irreducible subvarieties of a variety X. By Theorem 3.6.11, $\dim(X_{i-1}) > \dim(X_i)$ for $i = 1, \ldots, m$, and so $\dim(X) \geq \dim(X_0) \geq m$.

For the other inequality, we may assume that X_0 is an irreducible component of X with $\dim(X) = \dim(X_0)$. Since X_0 has a subvariety X_1' with dimension $\dim(X_0) - 1$, we may let X_1 be an irreducible component of X_1' with the same dimension. In the same fashion, for each $i = 2, \ldots, \dim(X)$, we may construct an irreducible subvariety X_i of dimension $\dim(X){-}i$. This gives a chain of irreducible subvarieties of X of length $\dim(X){+}1$, which proves the combinatorial definition of dimension. □

Similarly, the definition of dimension in terms of tangent spaces (Definition ??????) agrees with the definition given in terms of Hilbert function. For this, I think that we should appeal to differential geometry, such as if $d_x\varphi \neq 0$, and $x \in X$ is a smooth point, then $\mathcal{V}(f)$ is smooth in a neighborhood of x in X.

We now turn to the proof of Hilbert's Theorem 3.6.6, that the Hilbert function of a projective variety or homogeneous ideal is stably equivalent to a polynomial. We prove this for Hilbert functions of a more general class of objects, finitely generated graded modules over a polynomial ring.

A *module* over $\mathbb{K}[x] = \mathbb{K}[x_0, x_1, \ldots, x_n]$ (*$\mathbb{K}[x]$-module*) is a vector space M over $\mathbb{K}$, together with a ring homomorphism $\psi\colon \mathbb{K}[x] \to \mathrm{End}(M)$. Here, $\mathrm{End}(M)$ is the set of linear transformations $M \to M$. This is a $\mathbb{K}$-vector space with a multiplication is induced by composition, and $\mathrm{End}(M)$ is a noncommutative ring. Through ψ, polynomials in $\mathbb{K}[x]$ act as $\mathbb{K}$-linear transformations of the vector space M. We suppress the map ψ; simply writing $f.u$ for $\psi(f)(u)$, the image of $u \in M$ under the linear map $\psi(f)$, for $f \in \mathbb{K}[x]$.

The polynomial ring $\mathbb{K}[x]$ is a $\mathbb{K}[x]$-module, as $\mathbb{K}[x]$ acts linearly on itself by multiplication. An ideal I of $\mathbb{K}[x]$ is a $\mathbb{K}[x]$-module, and ideals are exactly the $\mathbb{K}[x]$-submodules of $\mathbb{K}[x]$. Quotients of modules are also modules, so that a quotient ring $\mathbb{K}[x]/I$ is a $\mathbb{K}[x]$-module. A module M is *finitely generated* if there exist finitely many elements $u_1, \ldots, u_k \in M$ such that every element u of M has an expression

$$u \;=\; f_1.u_1 \;+\; f_2.u_2 \;+\; \cdots \;+\; f_k.u_k$$

as a $\mathbb{K}[x]$-linear combination of $u_1, \ldots, u_k$ ($f_1, \ldots, f_k \in \mathbb{K}[x]$).

A module M is *graded* if it has a decomposition

$$M \;=\; \bigoplus_{s\in\mathbb{Z}} M_s\,,$$

where for each $s \in \mathbb{Z}$, M_s is a vector subspace of M and the $\mathbb{K}[x]$-action respects this decomposition. That is, for all $r \in \mathbb{N}$ and $s \in \mathbb{Z}$, if $f \in \mathbb{K}[x]_r$ is homogeneous of degree r and $u \in M_s$, then $f.u \in M_{r+s}$.

LEMMA 3.6.17. *If M is a finitely generated graded $\mathbb{K}[x]$-module, then each graded component of M is a finite-dimensional vector space.*

PROOF. Let $u_1, \ldots, u_k$ be generators of M with $u_i \in M_{s_i}$. For $s \in \mathbb{Z}$, every element $u \in M_s$ has an expression

$$u \;=\; f_1.u_1 \;+\; f_2.u_2 \;+\; \cdots \;+\; f_k.u_k$$

as a $\mathbb{K}[x]$-linear combination of $u_1, \ldots, u_k$. Here $f_i \in \mathbb{K}[x]_{s-s_i}$. Thus there is a surjection

$$\bigoplus_{i=1}^{k} \mathbb{K}[x]_{s-s_i} \;\twoheadrightarrow\; M_s\,.$$

This completes the proof, as the graded components of $\mathbb{K}[x]$ are finite-dimensional. □

The main consequence of Lemma 3.6.17 is that a finitely generated graded module M has a Hilbert function, defined by $HF_M(s) = \dim_{\mathbb{K}} M_s$.

THEOREM 3.6.18. *If M is a finitely generated graded $\mathbb{K}[x_0, x_1, \ldots, x_n]$-module, then its Hilbert function is stably equivalent to a polynomial of degree $m \leq n$. If as^m is the leading term of this polynomial, then $m!a$ is a nonnegative integer.*

Our proof will use induction on the number of variables, as well as maps of graded modules. A map $\varphi\colon M \to N$ of graded modules is a collection of linear maps

$$\varphi_s \ : \ M_s \ \longrightarrow \ N_s \qquad \text{for } s \in \mathbb{Z}$$

such that for every homogeneous polynomial $f \in \mathbb{K}[x]_r$ and $u \in M_s$ we have

$$\varphi_{r+s}(f.u) \ = \ f.\varphi_s(u) \qquad \text{in } N_{r+s}\,.$$

That is, the map φ is a map of modules that respects the grading (f has degree 0).

A consequence of this definition is that if $f \in \mathbb{K}[x]_r$ and M is a graded module, then multiplication by f is a linear map that sends M_s to M_{r+s}, but it is not *a priori* a map of graded modules. This is remedied by changing the grading in the domain of this multiplication map. Define a new graded module $M(-r)$ by $M(-r)_s := M_{s-r}$. Then multiplication by $f \in \mathbb{K}[x]_r$ is a map of graded modules $M(-r) \to M$.

Proof. When there are no variables, M is a finite-dimensional vector space, and so there is an integer s_0 with $M_s = 0$ for all $s \geq s_0$. In this case, HF_M is stably equivalent to 0, a polynomial of degree -1.

Now suppose that $r \geq 0$ and assume that the theorem holds when there are r variables, that is, for finitely generated $\mathbb{K}[x_0, \ldots, x_{r-1}]$-modules. Let M be a finitely generated graded $\mathbb{K}[x_0, \ldots, x_r]$-module, and let $K \subset M$ be the kernel of the linear map induced by multiplication by x_r. This gives an exact sequence of graded vector spaces,

$$0 \ \longrightarrow \ K(-1) \ \longrightarrow \ M(-1) \ \xrightarrow{x_r\cdot} \ M \ \longrightarrow \ M/x_r.M \ \longrightarrow \ 0\,.$$

For any $s \in \mathbb{Z}$, if we take the dimension of the sth graded components, then the rank-nullity theorem implies that

$$0 \ = \ \dim_{\mathbb{K}} K(-1)_s \ - \ \dim_{\mathbb{K}} M(-1)_s \ + \ \dim_{\mathbb{K}} M_s \ - \ \dim_{\mathbb{K}}(M/x_r.M)_s\,.$$

Using that $M(-1)s = M_{s-1}$, this becomes,

$$\dim_{\mathbb{K}} M_s \ - \ \dim_{\mathbb{K}} M_{s-1} \ = \ \dim_{\mathbb{K}}(M/x_r.M)_s \ - \ \dim_{\mathbb{K}} K(-1)_s\,.$$

Observe that both $K(-1)$ and $M/x_r.M$ are finitely generated modules over $\mathbb{K}[x_0, \ldots, x_{r-1}]$. By our induction hypothesis, the Hilbert function of each is stably equivalent to a polynomial of degree at most $r{-}1$. If m is the degree of the polynomial, then the coefficient a of its leading term as^m has $m!a$ a nonnegative integer. The same is true for their difference, (but the integer could be negative). Let $P(s)$ be this polynomial and s_0 the integer such that for $s \geq s_0$, $P(s) = \dim_{\mathbb{K}}(M/x_r.M)_s - \dim_{\mathbb{K}} K(-1)_s$. Suppose that P has degree m and leading coefficient ad^m.

Then, for $s \geq s_0$, $P(s) = \mathrm{HF}_M(s) - \mathrm{HF}_M(s-1)$, and we have

$$\mathrm{HF}_M(s) \ = \ \mathrm{HF}_M(s_0) \ + \ \sum_{t=s_0}^{s} P(t)\,.$$

By Exercise 4 the right hand side is a polynomial in s of degree $m{+}1$ with leading term $\frac{a}{m+1}s^{m+1}$. This completes the proof. □

Still need to prove the theorem about monomial ideals

Exercises for Section 3.6.

1. Show that the dimension of the space $\mathbb{K}[x_0,\dots,x_n]_m$ of homogeneous polynomials of degree m is $\binom{m+n}{n} = \frac{m^n}{n!}$ + lower order terms in m.
2. Let I be a homogeneous ideal. Show that the Hilbert functions HF_I, $HF_{(I\colon \mathfrak{m}_0)}$, and $HF_{I_{\geq d}}$ are stably equivalent.
3. Show that if $X \subset \mathbb{P}^n$ consists of d points, then, for r sufficiently large, we have $\mathbb{K}[X]_r \simeq \mathbb{K}^d$, and so $HP_X(r) = d$.
4. Suppose that $f(t)$ is a polynomial of degree d with initial term a_0t^m.
   (a) Show that $f(t) - f(t-1)$ has initial term ma_0t^{m-1}.
   (b) Show that $f(t) - f(t-b)$ has initial term mba_0t^{m-1}.
   (c) Show that for $t \geq t_0$ the sum
$$\sum_{s=t_0}^{t} f(s)$$
   is a polynomial of degree $m{+}1$ in t with initial term $\frac{a_0}{m+1}t^{m+1}$.
5. Let $Y \subset \mathbb{K}^n$ be an affine variety, embedded into projective space $\mathbb{P}^n$ via the identification of U_0 with $\mathbb{K}^n$ as in Remark 3.6.9, and let X be its projective closure. Show that for $r \geq 0$ dehomogenization induces a linear isomorphism of $\mathbb{K}[X]_r$ and $\mathbb{K}[Y]_{\leq r}$.
6. Prove Lemma 3.6.10
7. Compute the Hilbert functions and polynomials the following projective varieties. What are their dimensions and degrees?
   (a) The union of three skew lines in P^3, say $\mathcal{V}(x-w, y-z) \cup \mathcal{V}(x+w, y+z) \cup \mathcal{V}(y-w, x+z)$, whose ideal has reduced Gröbner basis
$$\langle \underline{x^2} + y^2 - z^2 - w^2,\ \underline{y^2z} - xz^2 - z^3 + xyw + yzw - zw^2,\ \underline{xyz} - y^2w - xzw + yw^2,$$
$$\underline{y^3} - yz^2 - y^2w + z^2w,\ \underline{xy^2} - xyw - yzw + zw^2\rangle$$
   (b) The union of two coplanar lines and a third line not meeting the first two, say the x- and y-axes and the line $x = y = 1$.
   (c) The union of three lines where the first meets the second but not the third and the second meets the third. For example $\mathcal{V}(wy, wz, xz)$.
   (d) The union of three coincident lines, say the x-, y-, and z- axes.
   Draw a picture of these?
8. Show that if $A \subset \mathbb{K}^n$ and $B \subset \mathbb{K}^m$ are subvarieties of degrees a and b, respectively, then $A \times B \subset \mathbb{K}^n \times \mathbb{K}^m$ has degree ab.

A consequence of a Bertini's Theorem[†] is that if X is a projective variety, then for almost all homogeneous polynomials f of a fixed degree, $\langle \mathcal{I}(X), f\rangle$ is radical and f is not a zero-divisor in $\mathbb{K}[X]$.

Consequently, if Λ is a generic linear form and set $Y := \mathcal{V}(\Lambda) \cap X$, then $\mathcal{I}(Y) = \langle \mathcal{I}(X), \Lambda\rangle$, and so

$$\mathrm{HP}_Y \;=\; \mathrm{HP}_{\langle \mathcal{I}(X),\Lambda\rangle}\,,$$

[†] Not formulated here, yet!

and so by Theorem 3.6.15, $\deg(Y) = \deg(X)$. If $Y \subset \mathbb{P}^n$ has dimension d, then we say that Y has codimension $n - d$.

Corollary 3.6.19 (Geometric meaning of degree). *The degree of a projective variety $X \subset \mathbb{P}^n$ of dimension d is the number of points in an intersection*

$$X \cap L\,,$$

where $L \subset \mathbb{P}^n$ is a generic linear subspaces of codimension d.

For example, the cubic curve of Figure ????[3] has degree 3, and we see in that figure that it meets the plane $z = 0$ in 3 points.

Does this belong anywhere? Suppose that the ideal I generated by the polynomials f_i of (2.4.1) is not zero-dimensional, and we still want to count the isolated solutions to (2.4.1). In this case, there are symbolic algorithms that compute a zero-dimensional ideal J with $J \supset I$ having the property that $\mathcal{V}(J)$ consists of all isolated points in $\mathcal{V}(I)$, that is all isolated solutions to (2.4.1). These algorithms successively compute the ideal of all components of $\mathcal{V}(I)$ of maximal dimension, and then strip them off. One such method would be to compute the primary decomposition of an ideal. Another method, when the non-isolated solutions are known to lie on a variety $\mathcal{V}(J)$, is to saturate I by J to remove the excess intersection.[†]

3.7. Notes

Mention about the origin of Zariski topology.

[3] Need a different picture

[†] Develop this further, either here or somewhere else, and then refer to that place.

CHAPTER 4

Numerical Algebraic Geometry

Outline:

Chapter 2 presented fundamental symbolic algorithms, including the classical resultant and general methods based on Gröbner bases. Those algorithms operate on the algebraic side of the algebraic-geometric dictionary underlying algebraic geometry. This chapter develops the fundamental algorithms of numerical algebraic geometry, which uses tools from numerical analysis to represent and study algebraic varieties on a computer. As we will see, this field primarily operates on the geometric side of our dictionary. Since numerical algebraic geometry involves numerical computation, we will work over the complex numbers.

4.1. Core Numerical Algorithms

Numerical algebraic geometry rests on two core numerical algorithms, which go back at least to Newton and Euler. Newton's method refines approximations to solutions to systems of polynomial equations. A careful study of its convergence leads to methods for certifying numerical output, which we describe in Section 4.5. The other core algorithm comes from Euler's method for computing a solution to an initial value problem. This is a first-order iterative method, and more sophisticated higher-order methods are used in practice for they have better convergence. These two algorithms are used together for path-tracking in numerical homotopy continuation, which we develop in subsequent sections as a tool for solving systems of polynomial equations and for manipulating varieties on a computer. While these algorithms are standard in introductory numerical analysis, they are less familiar to algebraists. Our approach is intended to be friendly to algebraists.

By the Fundamental Theorem of Algebra, a univariate polynomial $f(x)$ of degree n has n complex zeroes. When the degree of f is at most four, there are algorithmic formulas for these zeroes that involve arithmetic operations and extracting roots. Zeroes of linear polynomials go back to the earliest mathematical writing, such as the Rhind Papyrus, and the Babylonians had a method for the zeroes of quadratic polynomials that is the precursor of the familiar quadratic formula, which was made explicit by Bramagupta c. 600

CE. The 16th century Italians del Ferro, Tartaglia, Cardano, and Ferrari colorfully gave formulas for the zeroes of cubic and quartic polynomials. It was only in 1823 that Niels Hendrik Abel proved there is no universal such formula for the zeroes of polynomials of degree five and higher.

It was later shown that the zeroes of a general polynomial cannot be expressed in terms of the coefficients using only arithmetic operations on its coefficients and extracting roots. For example, the zeroes of this sextic

$$f \ := \ x^6 \ + \ 2x^5 \ + \ 3x^4 \ + \ 5x^3 \ + \ 7x^2 \ + \ 11x \ - \ 13 \tag{4.1.1}$$

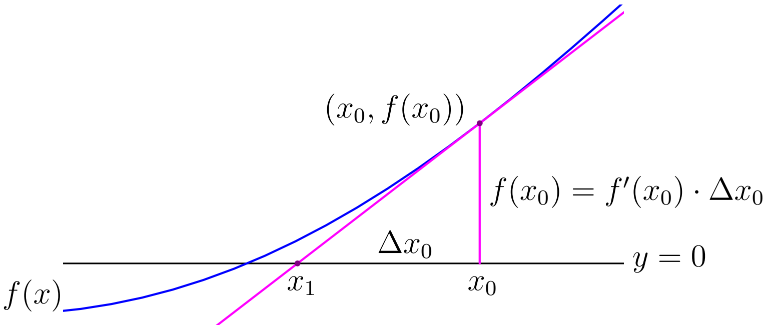
admit no such expression. This is not to say there is no formula for the zeroes of polynomials of degree five or more. For example, there are hypergeometric power series for those zeroes that depend upon the coefficients.

Numerical methods offer another path to the roots of univariate polynomials. While numerical linear algebra may be combined with the eigenvalue approaches to solving of Section 5.3, we will discuss algorithms based on Newton's method.

Newton's method uses the tangent-line approximation to the graph of a differentiable function $f(x)$ to refine an approximation x_0 to a zero of f. The tangent line to the graph of $f(x)$ at the point $(x_0, f(x_0))$ has equation

$$y \ = \ f'(x_0)(x - x_0) \ + \ f(x_0)\,.$$

If $f'(x_0) \neq 0$, we solve this for $y = 0$ to get the formula $x_1 := x_0 - (f'(x_0))^{-1} f(x_0)$ for the refinement of x_0. This may also be read from the graph.



Using operator notation Df for the derivative of f, we obtain the expression

$$N_f(x) \ := \ x \ - \ (Df(x))^{-1} f(x) \tag{4.1.2}$$

for the passage from x_0 to x_1 above. This *Newton iteration* (4.1.2) is the basis for Newton's method to compute a zero of a function $f(x)$:

- Start with an initial value x_0, and
- While $Df(x_i) \neq 0$, compute the sequence $\{x_i \mid i \in \mathbb{N}\}$ using the recurrence $x_{i+1} = N_f(x_i)$.

For $f(x) = x^2 - 2$ with $x_0 = 1$, if we compute the first seven terms of the sequence,

$$\begin{aligned}
x_1 &= 1.5\\
x_2 &= 1.416\overline{6}\\
x_3 &= 1.4142156862745098039\overline{2156862745098039}\\
x_4 &= 1.4142135623746899106262955788901349101165596221157440445849050192000\\
x_5 &= 1.4142135623730950488016896235025302436149819257761974284982894986231\\
x_6 &= 1.4142135623730950488016887242096980785696718753772340015610131331132\\
x_7 &= 1.4142135623730950488016887242096980785696718753769480731766797379907\,,
\end{aligned}$$

then the 58 displayed digits of x_7 are also the first 58 digits of $\sqrt{2}$.

This example suggests that Newton's method may converge rapidly to a solution. It is not always so well-behaved. For example, if $f(x) = x^3 - 2x + 2$, then $N_f(0) = 1$ and $N_f(1) = 0$, and so the sequence $\{x_i\}$ of Newton iterates with $x_0 = 0$ is periodic with period 2, and does not converge to a root of f.

In fact Newton's method is about as badly behaved as it can be, even for polynomials. The *basin of attraction* for a zero x^* of f is the set of all complex numbers x_0 such that Newton's method starting at x_0 converges to x^*. In general, the boundary of a basin of attraction is a fractal Julia set. Figure 4.1.1 shows basins of attraction for two univariate cubic polynomials. On the left are those for the polynomial $f(x) = x^3 - 1$, in the region $|\Re(x)|, |\Im(x)| \leq 1.3$. This polynomial vanishes at the cubic roots of unity, and each is a fixed point of a Newton iteration. There are three basins, one for each root of f, and their union is dense in the complex plane. Each basin is drawn in a different color.

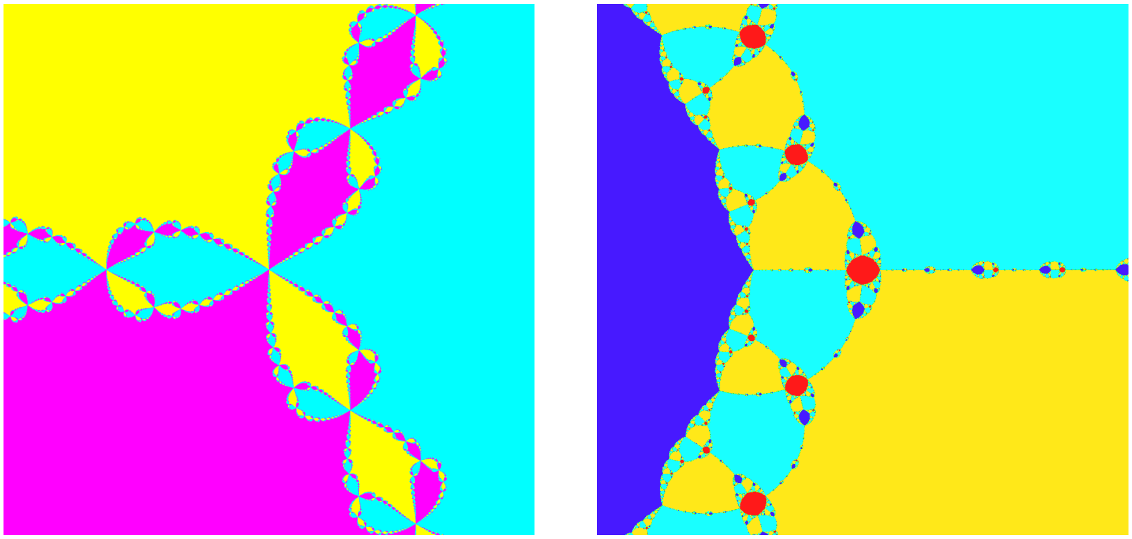


FIGURE 4.1.1. Basins of attraction for two cubics

On the right of Figure 4.1.1 are basins for the polynomial $f(x) = x^3 - 2x + 2$. The roots of f give three fixed points of a Newton iteration, and we noted there is an orbit of period 2. The roots and the orbit each have a basin of attraction and each basin is drawn in a different color. The basin of attraction for the orbit of period 2 is in red.

Despite this complicated behaviour, Newton's method is a foundation for numerical algebraic geometry, and it may be used to certify the results of numerical computation. To understand why this is so, we investigate its convergence.

Suppose that f is twice continuously differentiable in a neighborhood of a zero ζ of f and that $Df(\zeta)^{-1}$ exists. Differentiating the expression (4.1.2) for $N_f(x)$ gives

$$\begin{aligned} DN_f(x) &= 1 - Df(x)^{-1}Df(x) + Df(x)^{-1}D^{(2)}f(x)Df(x)^{-1}f(x) \\ &= Df(x)^{-1}D^{(2)}f(x)Df(x)^{-1}f(x)\,. \end{aligned}$$

As $f(\zeta)=0$, we have $DN_f(\zeta)=0$ and $N_f(\zeta)=\zeta$. The first order Taylor expansion of $N_f(x)$ about the point $x=\zeta$ with remainder is then

$$N_f(x) = \zeta + \frac{1}{2}D^{(2)}N_f(a)(x-\zeta)^2\,,$$

where a is some point with $|a-\zeta| < |x-\zeta|$, and we used that $N_f(\zeta)=\zeta$. If we set $c := \max\{\frac{1}{2}|D^{(2)}N_f(a)| \mid |a-\zeta|<r\}$, for some $r>0$, then we have

$$|N_f(x)-\zeta| \leq c|x-\zeta|^2\,,$$

whenever $|x-\zeta|\leq r$. Suppose now that $|x-\zeta| < \min\{\frac{1}{2c}, r\}$. Then,

$$\begin{aligned} |N_f(x)-\zeta| &< c\cdot\left(\frac{1}{2c}\right)^2 = \frac{1}{4c}\,, \qquad \text{and} \\ |N_f^2(x)-\zeta| &< c\cdot\left(\frac{1}{4c}\right)^2 = \frac{1}{16c}\,, \end{aligned}$$

and in general, if $N_f^i(x)$ is the ith iteration of N_f applied to z, we have

$$|N_f^i(x)-\zeta| < 2^{1-2^i}\frac{1}{2c}\,.$$

This implies that the number of digits of ζ that have been computed in x_{i+1} (the number of significant digits in x_{i+1}) will be approximately twice the number of significant digits in x_i. We saw this when computing $\sqrt{2}$ using Newton's method as $x_1, x_2, \dots, x_6$ had 1, 3, 6, 12, 24, and 48 correct decimal digits of $\sqrt{2}$.

This has a straightforward extension to the problem of approximating zeroes to a square system of multivariate polynomials,

$$F : f_1 = f_2 = \cdots = f_n = 0\,, \tag{4.1.3}$$

where each f_i is a polynomial in n variables. Here square means that the number of equations equals the number of variables and (4.1.3) defines a zero-dimensional variety. It is useful to consider F to be a polynomial map,

$$F = (f_1,\dots,f_n) : \mathbb{C}^n \longrightarrow \mathbb{C}^n\,,$$

and write the solutions $\mathcal{V}(F)$ as $F^{-1}(0)$. Given a point $x\in\mathbb{C}^n$ where the Jacobian matrix $DF(x)$ of partial derivatives of $f_1,\dots,f_n$ with respect to the components of x is invertible, the *Newton iteration* of F applied to x is

$$NF(x) \;:=\; x - DF(x)^{-1}F(x)\,.$$

The geometry of this map is the same as for univariate polynomials: $NF(x)$ is the unique zero of the linear approximation of F at x. This is the solution $\zeta \in \mathbb{C}^n$ to

$$0 \;=\; F(x) + DF(x)(\zeta - x)\,.$$

The elementary analysis of iterating Newton steps is also the same. As before, Newton steps define a chaotic dynamical system on $\mathbb{C}^n$, but if x is sufficiently close to a zero ζ of F, then Newton iterations starting at x converge rapidly to ζ.

We quantify this. A sequence $\{x_i \mid i \in \mathbb{N}\} \subset \mathbb{C}^n$ *converges quadratically* to a point $\zeta \in \mathbb{C}^n$ if for all $i \in \mathbb{N}$,

$$\|x_i - \zeta\| \;\leq\; 2^{1-2^i}\|x_0 - \zeta\|\,. \tag{4.1.4}$$

For example, the sequence of Newton iterations for $x^2 - 2$ beginning with $x_0 = 1$ that we computed converges quadratically to $\sqrt{2}$. A point $x \in \mathbb{C}^n$ is an *approximate zero* of F with *associated zero* $\zeta \in \mathbb{C}^n$ if $F(\zeta) = 0$ and if the sequence of Newton iterates defined by $x_0 := x$ and $x_{i+1} := NF(x_i)$ for $i \geq 0$ converges quadratically to ζ.

Knowing an approximate zero x to a system F is a well-behaved relaxation of the problem of knowing its associated zero ζ. Indeed, the sequence of Newton iterations starting with x reveals as many digits of ζ as desired, in a controlled manner.

At this point, one should ask for methods to determine if x is an approximate zero to F. A heuristic that is used in practice is to treat the length of a Newton step

$$\beta(F,x) \;:=\; \|x - NF(x)\| \;=\; \|DF(x)^{-1}F(x)\|\,, \tag{4.1.5}$$

as a proxy for the distance $\|x - \zeta\|$ to the zero ζ of F. If we are in the basin of quadratic convergence to ζ, then we expect that

$$\tfrac{1}{2}\|x - \zeta\| \;\lesssim\; \beta(F,x) \;\lesssim\; \|x - \zeta\|\,.$$

For the heuristic, compute two Newton iterations, $NF(x)$ and $NF^2(x)$. If we have that

$$\beta(F, NF(x)) \;\leq\; \beta(F,x)^2\,, \tag{4.1.6}$$

with $\beta(F,x)$ below some threshold $\beta \ll 1$, then we replace x by $NF^2(x)$, and declare it to be an approximate zero of F with some certitude. The condition (4.1.6) implies that the number of digits common to $NF(x)$ and $NF^2(x)$ is at least twice the number of digits common to x and $NF(x)$. See Exercise 5 for potential limitations of this heuristic.

We can do much better than this heuristic. Smale studied the convergence of Newton's method and developed what is now called *α-theory* after a computable constant $\alpha = \alpha(F,x)$ such that if α is sufficiently small, then x is an approximate zero of F. We present this theory in Section 4.5. For now, we define $\alpha(F,x)$ and state Smale's theorem.

The constant $\alpha(F,x)$ is the product of two numbers. The first is the length $\beta(F,x)$ (4.1.5) of a Newton step at x. For the second, recall the Taylor expansion of F at x, Relate this to /eqrefEq:Taylor.

$$F(w) \;=\; F(x) + DF(x)(w-x) + D^2F(x)(w-x)^2 + \cdots + D^NF(x)(w-x)^N\,,$$

where the polynomial map F has degree N. Let is describe the meaning of the terms in this Taylor expansion. For $v \in \mathbb{C}^n$, v^k is the symmetric tensor indexed by all exponents $a \in \mathbb{N}^n$ of degree k, where

$$(v^k)_a \;=\; \tfrac{1}{a_1!}\tfrac{1}{a_2!}\cdots\tfrac{1}{a_n!}v_1^{a_1}v_2^{a_2}\cdots v_n^{a_n} \;=:\; \tfrac{1}{a!}v^a\,.$$

Let $S^k\mathbb{C}^n$ be this vector space of symmetric tensors. Writing $x = (x_1,\dots,x_n) \in \mathbb{C}^n$, the ith component of $D^kF(x)$ is the vector of partial derivatives of F_i of order k,

$$(D^kF_i(x))_a \;=\; \left(\tfrac{\partial}{\partial x_1}\right)^{a_1}\left(\tfrac{\partial}{\partial x_2}\right)^{a_2}\cdots\left(\tfrac{\partial}{\partial x_n}\right)^{a_n} F_i(x)\,,$$

for $a \in \mathbb{N}^n$ of degree k. Then the ith component of $D^kF(x)(w-x)^k$ is the sum

$$\sum_{|a|=k} D^aF_i(x)\tfrac{1}{a!}(w-x)^a\,.$$

Thus $D^kF(x)$ is a linear map from the space $S^k\mathbb{C}^n$ of symmetric tensors to $\mathbb{C}^n$. The same is true for the composition $DF(x)^{-1}\circ D^kF(x)$. If we use the standard norm for vectors $z \in \mathbb{C}^n$ and $v \in S^k\mathbb{C}^n$,

$$\|z\| \;:=\; \Bigl(\sum_{i=1}^n |z_i|^2\Bigr)^{1/2} \qquad\text{and}\qquad \|v\| \;:=\; \Bigl(\sum_{|a|=k} |v_a|^2\Bigr)^{1/2},$$

then the operator norm of this composition is

$$\bigl\|DF(x)^{-1}\circ D^kF(x)\bigr\| \;:=\; \max_{\|v\|=1}\bigl\|DF(x)^{-1}\circ D^kF(x)(v^k)\bigr\|\,.$$

With these definitions, set

$$\gamma(F,x) \;:=\; \max_{k\geq 2}\tfrac{1}{k!}\bigl\|DF(x)^{-1}\circ D^kF(x)\bigr\|^{\frac{1}{k-1}}\,,$$

and then define

$$\alpha(F,x) \;:=\; \beta(F,x)\cdot\gamma(F,x)\,.$$

THEOREM 4.1.1. *If $\alpha(F,x) < \frac14(13-3\sqrt{17}) \simeq 0.15767\dots$, then x is an approximate zero of F. The distance from x to its associated zero is at most $2\beta(F,x)$.*

We prove Theorem 4.1.1 and some extensions in Section 4.5. Note the similarity between the formula for $\gamma(F,x)$ and the root test/formula for the radius of convergence of a power series. The shift in the radical from $\frac1k$ to $\frac{1}{k-1}$ is because this is applied to the expansion of DF.

We apply this to the quadratic polynomial $f(x) = x^2-2$. When $x \in \mathbb{C}$ is nonzero, $f'(x) \neq 0$, and we have

$$\beta(f,x) \;=\; \left|\frac{f(x)}{f'(x)}\right| \qquad\text{and}\qquad \gamma(f,x) \;=\; \frac12\left|\frac{f''(x)}{f'(x)}\right|\,.$$

Then $\alpha(f,x) = \frac12|f(x)f''(x)/(f'(x))^2| = |\frac{x^2-2}{4x^2}|$.

Observe that $\alpha(f,1) = \frac14 > \frac14(13-3\sqrt{17})$. Thus, while Newton iterations starting at $x_0 = 1$ converge quadratically to $\sqrt2$, this quadratic convergence is not detected with

Smale's α-theory. Note that $\alpha(f, 3/2) = \frac{1}{36} < \frac{1}{4}(13 - 3\sqrt{17})$, so that α-theory certifies the quadratic convergence of Newton iterations starting with $x_0 = 3/2$.

Consider the regions of convergence of Newton's method for the zeroes of $x^2 - 2$ in the complex plane. First, when $\Re(x) > 0$, Newton iterations beginning with x converge to $\sqrt{2}$ and when $\Re(x) < 0$, iterations beginning with x converge to $-\sqrt{2}$. In Figure 4.1.2, a point $x \in \mathbb{C}$ is yellow if Newton iterations converge quadratically, and magenta otherwise. The zeroes $\pm\sqrt{(2)}$ are as indicated and the convex regions enclosing them indicate the points whose quadratic convergence is certified using α-theory ($\alpha(f, z) < \frac{1}{4}(13 - 3\sqrt{17})$).

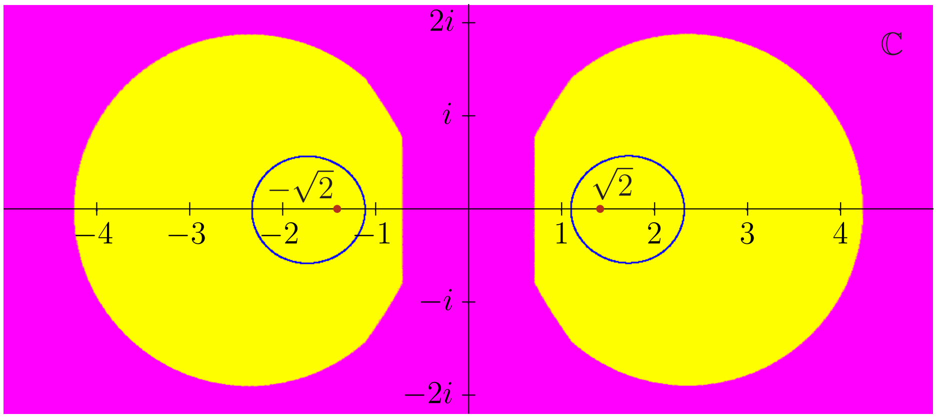


Figure 4.1.2. Basins of quadratic convergence for $x^2 - 2$.

On the positive real line, the interval of quadratic convergence is $(\sqrt{2}/2, 3\sqrt{2})$, while the interval where $\alpha(f, x) < \frac{1}{4}(13 - 3\sqrt{17})$ is $(1.10746, 2.32710)$, which is much smaller.

Euler's method was developed to solve the initial value problem for a first-order ordinary linear differential equation,

$$y' = f(x, y), \qquad y(x_0) = y_0,$$

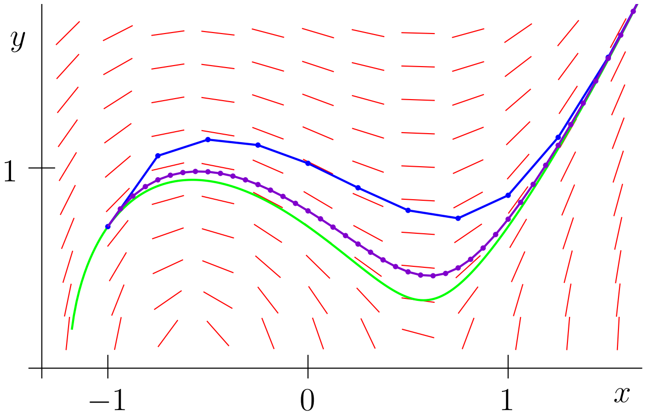
where the function $f(x, y)$ is continuous near (x_0, y_0) in $\mathbb{R}^2$. Given a *stepsize* $h > 0$, Euler's method approximates the value of $y(x)$ at $x_1 = x_0 + h$ using the linear approximation given by the differential equation, $y_1 := y_0 + hf(x_0, y_0)$. Euler's method recursively computes a sequence $\{(x_i, y_i) \mid i = 0, \ldots, N\}$ of points where

$$x_{i+1} := x_i + h \quad \text{and} \quad y_{i+1} := y_i + hf(x_i, y_i).$$

Let us consider the initial value problem,

$$y' = \frac{3x^2 - 1}{2y}, \qquad y(-1) = \frac{1}{\sqrt{2}}. \tag{4.1.7}$$

The solution to this initial value problem is $y = \sqrt{x^3 - 3 + \frac{1}{2}}$. The picture below shows the slope field and the solution curve, and two approximations using Euler's method starting at $(-1, \frac{1}{\sqrt{2}})$ with respective stepsizes $h = \frac{1}{4}$ and $h = \frac{1}{16}$.



Like Newton's method, Euler's method extends to solving the intial value problem for a system of first order linear differential equations, so that y is a vector.

Let us investigate the accuracy of Euler's method, assuming that y (and hence $f(x, y)$) has sufficiently many derivatives. The second order Taylor expansion of $y(x)$ at $x = x_0$, together with the differential equation $y'(x) = f(y, x)$ gives

$$y(x+h) \;=\; y_0 + hf(x_0, y_0) + \tfrac{h^2}{2}y''(x_0) + \tfrac{h^3}{6}y'''(x^*)\,,$$

where x^* lies between x_0 and $x_0 + h$. We estimate

$$|y(x+h) - (y_0 + hf(x_0, y_0))| \;\le\; h^2\big(\tfrac{1}{2}|y''(x_0)| + \tfrac{|h|}{6}|y'''(x^*)|\big)\,.$$

When y''' is bounded near (x_0, y_0), the error in a single step of Euler's method is at most a constant mutiple of h^2.

To compute $y(x)$ for a fixed x using Euler's method, choose a stepsize h and then perform $\lceil |x - x_0|/h \rceil$ iterations. Each iteration introduces an error at most a constant multiple of h^2 so the difference between $y(x)$ and the computed value will be at most a constant multiple of h. That the global error is at most a constant multiple of the stepsize h, marks Euler's method as a *first-order* iterative method.

The primary value of Euler's method is to illustrate the idea of an iterative solver for initial value problems, as first order accuracy is typically insufficient. A simple higher-order method is the *midpoint rule*, in which the successive values of y are computed using the more complicated formula

$$x_{i+1} = \; x_i + h\,, \quad \text{and} \quad y_{i+1} = \; y_i + hf\left(x_i + \tfrac{1}{2}h\,,\, y_i + \tfrac{1}{2}hf(x_i, y_i)\right)\,,$$

which is second-order.

The classical *Runge-Kutta* method, also called RK4, is a common fourth-order method. For this,

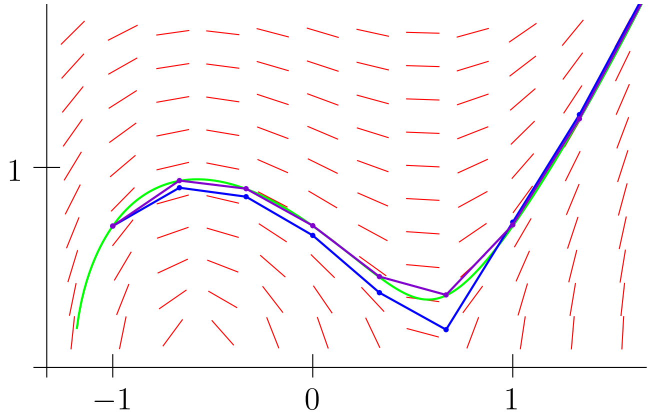
$$x_{i+1} = \; x_i + h\,, \quad \text{and} \quad y_{i+1} = \; y_i + \tfrac{1}{6}h(z_1 + 2z_2 + 2z_3 + z_4)\,,$$

where

$$\begin{array}{lllllll} z_1 & = & f(x_i, y_i)\,, & & z_2 & = & f(x_i + \tfrac{1}{2}h\,,\, y_i + \tfrac{1}{2}hz_1)\,, \\ z_3 & = & f(x_i + \tfrac{1}{2}h\,,\, y_i + \tfrac{1}{2}hz_2)\,, & \text{and} & z_4 & = & f(x_i + h\,,\, y_i + hz_3)\,. \end{array}$$

In Exercise 9 you are asked to relate this to Simpson's rule.

We display the two piecewise linear curves obtained from the midpoint and Runge-Kutta methods with stepsize $\frac{1}{3}$ for the initial value problem (4.1.7) with solution $y = \sqrt{x^3 - 3 + \frac{1}{2}}$ on the same slope field as we used to illustrate Euler's method.



There is a vast literature on iterative methods for solving ordinary differential equations.

Exercises.

(1) Consider a depressed cubic equation, one of the form $x^3 + bx = c$. Show that

$$x \;=\; \sqrt[3]{\tfrac{c}{2} + \sqrt{\tfrac{c^2}{4} + \tfrac{b^3}{27}}} \;+\; \sqrt[3]{\tfrac{c}{2} - \sqrt{\tfrac{c^2}{4} + \tfrac{b^3}{27}}}$$

is a solution. What are the other two solutions? How about the solutions to a general cubic equation $\alpha x^3 + \beta x^2 + \gamma x + \delta = 0$?

(2) Prove the assertion about (4.1.1) using Galois theory. Specifically show that the polynomial f has Galois group the full symmetric group S_6 by factoring f modulo sufficiently many primes, and use lifts of Frobenius elements.

(3) Consider the following iterative algorithm used by the Babylonians to compute $\sqrt{x}$ for $x > 0$. Observe that if $x_i > 0$ and $x_i \neq \sqrt{x}$, then the interval with endpoints x_i and x/x_i contains $\sqrt{x}$ in its interior. Set $x_{i+1} = \frac{1}{2}(x_i + \frac{x}{x_i})$ and repeat. Compare this method of computing square roots to Newton's Method.

(4) Let $f(x) = x^3 - 2x + 2$ and compute some iterates of Newton's method beginning with the following values of x_0,

$$x_0 \;\in\; \{0.1\,,\; 0.9\,,\; \tfrac{1}{2} + \frac{1}{10}\sqrt{-1}\,,\; 1 - \frac{1}{10}\sqrt{-1}\,,\; -1\}\,.$$

(5) Newton's method for $f(x) = x^2 - 2$ converges quadratically for x_0 in the interval $[\sqrt{2}/2, 3\sqrt{2}]$. Prove that Newton iterations beginning with these endpoints converge quadratically. Investigate the failure of quadratic convergence for $x > 3\sqrt{2}$: at which step of Newton's method does quadratic convergence fail (the condition (4.1.4) does not hold) for each of the following starting points for Newton's method.

$$5.2\,,\;4.53\,,\;4.36\,,\;4.298\,,\;4.256\,,\;4.25\,,\;4.246\,,\;4.245\,,\;4.2427\,.$$

(6) Prove that the midpoint rule is a second-order method.

(7) Give some examples of Euler's method. If you cannot find something more interesting, start with the exponential function. Have them study its global convergence and the dependence on stepsize.

(8) Compare Euler, midpoint, and Runge-Kutta on some examples.

(9) Have the students prove the equivalence of Runge-Kutta with Simpson's rule.

4.2. Numerical Homotopy Continuation

The core numerical algorithms introduced in Section 4.1—Newton's method to refine an approximation to a solution of a system of polynomial equations and iterative methods to solve an initial value problem—are the building blocks of higher-level predictor-corrector methods that track smooth implicitly defined paths. Numerical homotopy continuation uses path tracking to compute the zeroes of a system of polynomials, given the zeroes of a different, but related system. The Bézout Homotopy Algorithm, which is based on numerical homotopy continuation, computes the isolated zeroes of any system of multivariate polynomials and is optimal for generic systems. Algorithms based on numerical homotopy continuation have the added virtue of being inherently parallelizable.

To motivate and illustrate these ideas, consider a toy problem. Suppose we want to compute the (four) solutions to the system of equations

$$z(y-1)-1 \;=\; y^2+2z^2-9 \;=\; 0\,. \tag{4.2.1}$$

Consider instead the system

$$z(y-1) \;=\; y^2+2z^2-9 \;=\; 0\,, \tag{4.2.2}$$

whose solutions are found by inspection to be

$$(\pm 3, 0) \qquad \text{and} \qquad (1, \pm 2)\,. \tag{4.2.3}$$

Figure 4.2.1 shows the plane curves defined by the polynomials in these systems. The first system (4.2.1) seeks the intersection of the hyperbola with the ellipse, while the second, simpler, system (4.2.2) replaces the hyperbola by the two lines.

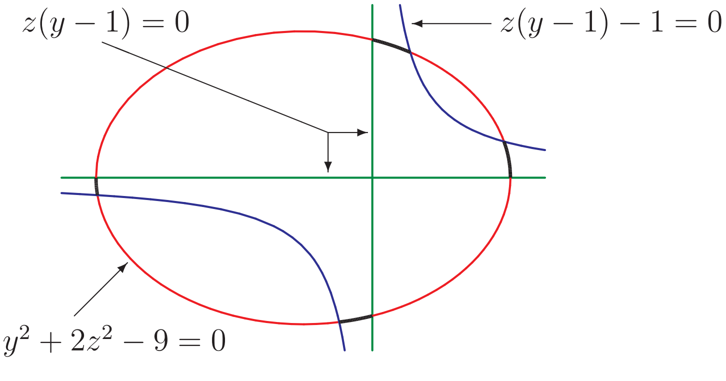


FIGURE 4.2.1. The intersection of a hyperbola with an ellipse.

These systems are connected by the one-parameter (in t) family of systems

$$z(y-1)-(1-t) \;=\; y^2+2z^2-9 \;=\; 0\,. \tag{4.2.4}$$

This defines a space curve C in $\mathbb{C}^2_{yz}\times\mathbb{C}_t$. Restricting C to $t\in[0,1]$ gives four paths that connect the known solutions to (4.2.2) at $t=1$ to the unknown solutions to (4.2.1) at $t=0$. These paths are shown in Figure 4.2.2. To find the unknown solutions at $t=0$, we need to track these four paths, starting from the known solutions at $t=1$.

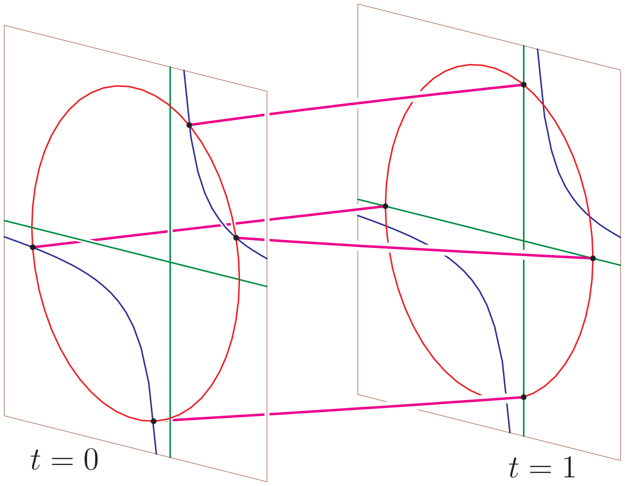


FIGURE 4.2.2. Paths connecting solutions.

Let $H(y,z;t)$ be the system of two polynomials in (4.2.4) that define the space curve C, and let $x(t) := (y(t),z(t))$ for $t\in[0,1]$ be the projection of one of the paths in Figure 4.2.2, which is a parametrization of one of the thickened arcs in Figure 4.2.1.

Then $H(y(t),z(t);t)\equiv 0$ for $t\in[0,1]$. Differentiating this gives

$$\frac{\partial H}{\partial y}\cdot\frac{dx}{dt} \;+\; \frac{\partial H}{\partial z}\cdot\frac{dy}{dt} \;+\; \frac{\partial H}{\partial t} \;=\; 0\,.$$

Solving, shows that $x(t)$ satisfies the *Davidenko differential equation*

$$x' \;=\; -(D_xH)^{-1}\frac{\partial H}{\partial t}\,. \tag{4.2.5}$$

Here, D_xH is the Jacobian matrix of H with respect to its first two (y,z) variables. Thus each of the four paths in Figure 4.2.2 is a solution of an initial value problem for this differential equation, one for each of the four points (4.2.3). Using an iterative method to solve these initial value problems computes approximations to the solutions of (4.2.1).

This is dramatically improved when combined with Newton's method. Fix a sequence of points $1=t_0>t_1>\cdots>t_m=0$ in $[0,1]$, let z_0 be one of the four solutions (4.2.3) to the system (4.2.2) and $x(t)$ the corresponding path. Having computed x_i for some $i<m$, apply one step of any iterative method (Euler, midpoint, RK4, ...) with stepsize $t_{i+1}-t_i$ to get a prediction x^*_{i+1} for $x(t_{i+1})$. Next, perform Newton iterations for $H(x;t_{i+1})$

starting at x^*_{i+1}, until some stopping criterion is reached, obtaining x_{i+1}. If each x_i lies in the basin of attraction of $x(t_i)$ for Newton iterations, then x_m converges to $x(0)$ under Newton iterations. Better is when the x_i are approximate solutions, for then x_m is an approximate solution to $H(x;0) = 0$ with associated zero $x(0)$.

This discussion about the system (4.2.4) is in fact quite general. Let $H(x;t)$ be a system of n polynomials in $n+1$ variables ($x \in \mathbb{C}^n$ and $t \in \mathbb{C}_t$). Then every component of the affine variety $\mathcal{V}(H)$ has dimension at least 1. Let C be the union of all components of dimension 1 whose projection to $\mathbb{C}_t$ is dense.Then A point $(x;t) \in \mathcal{V}(H)$ is *nondegenerate* if the Jacobian matrix D_xH with respect to its x-variables is invertible at $(x;t)$. A nondegenerate point is isolated from other points of $\mathcal{V}(H)$ in its fiber $\mathbb{C}^n \times \{t\}$ and the nondegenerate points are exactly the points where the Davidenko differential equation (4.2.5) is defined. You are asked to prove the following lemma in Exercise 2.

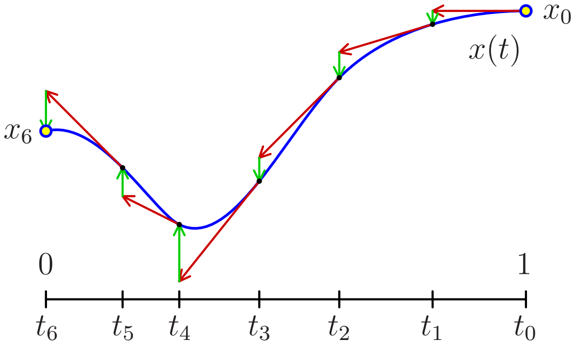
LEMMA 4.2.1. *The curve C contains every point $(x;t)$ of $\mathcal{V}(H)$ that is isolated from other points of $\mathcal{V}(H)$ in its fiber. If C is nonempty, then there is a positive integer d and a nonempty Zariski-open subset U of $\mathbb{C}_t$ consisting of all points u such that $H(x;u) = 0$ has d nondegenerate solutions. Above every point b of the complement $B := \mathbb{C}_t \smallsetminus U$ there is some point where either the curve C meets another component of $\mathcal{V}(H)$ or the map $C \to \mathbb{C}_t$ is ramified or C has a branch tending to infinity near C.*

We call $H(x;t)$ a *homotopy* if C is nonempty and $1 \in U$. Suppose further that

$$\text{the interval } [0,1] \text{ of } \mathbb{R} \text{ is a subset of } U. \tag{4.2.6}$$

Then the restriction $C|_{[0,1]}$ of C to $t \in [0,1]$ is a collection of d smooth paths. The *start system* is $H(x;1) = 0$ and the *target system* is $H(x;0) = 0$, and both have d nondegenerate solutions. Each path in $C|_{[0,1]}$ connects one nondegenerate solution to the start system to one nondegenerate solution to the target system.

Given a nondegenerate solution x_0 to the start system, let $x(t)$ be the path in $C|_{[0,1]}$ with $x_0 = x(1)$. It satisfies the Davidenko differential equation (4.2.5). Choosing a sequence of points $1 = t_0 > t_1 > \cdots > t_m = 0$ in $[0,1]$, a *predictor-corrector method* constructs a sequence $x_1, \ldots, x_m$ of approximations to the points $x(t_i)$ along the path alternately applying an iterative method to x_i to get a prediction x^*_{i+1} to $x(t_{i+1})$, which is refined using Newton iterations to get the next point x_{i+1}. Here is a schematic of the predictor-corrector method using Euler predictions to trace a smooth path $x(t)$.



A predictor-corrector method only computes refinable approximations to a sequence of points on an implicitly defined path $x(t)$ for $t \in [0,1]$. We will largely ignore this distinction and refer to the computed points as lying on the path with $x(1)$ the starting point and $x(0)$ the output, and use the term *path tracking* for this process.

The algorithm of *numerical homotopy continuation* begins with a homotopy $H(x;t)$ satisfying (4.2.6) and the set of nondegenerate solutions to the start system $H(x;1) = 0$. By assumption (4.2.6), each solution x is the starting point $x(1)$ of a smooth path $x(t)$ defined implicitly by $H(x;t) = 0$ for $t \in [0,1]$. For each solution x to the start system, the algorithm tracks the path $x(t)$ from $t = 1$ to $t = 0$ to obtain $x(0)$, a solution to the target system.

Theorem 4.2.2. *Numerical homotopy continuation under assumption* (4.2.6) *computes all nondegenerate solutions to the start system $H(x;0) = 0$.*

Proof. For each solution x to the start system, the path $x(t)$ is smooth, so that path tracking starting from $x = x(1)$ will compute its endpoint $x(0)$. By assumption (4.2.6), each nondegenerate solution of the target system is connected to a nondegenerate solution of the start system along one of these paths. This completes the proof. □

The Bézout homotopy is one of the simplest homotopies. Suppose that $F = (f_1, \dots, f_n)$ is a system of n polynomials in n variables with $\deg f_i = d_i$. By Bézout's Theorem ????, $\mathcal{V}(F)$ has at most $d := d_1 d_2 \cdots d_n$ isolated solutions, and if F is generic, it has exactly d solutions, all nondegenerate. Given the degrees $d_1, \dots, d_n$, for each $i = 1, \dots, n$, set

$$g_i(x) \ := \ x_i^{d_i} - 1\,. \tag{4.2.7}$$

Then the system $G = (g_1, \dots, g_n)$ has the d solutions,

$$\{(\zeta_1, \dots, \zeta_n) \ \mid \ \zeta_i = e^{\frac{2\pi k}{d_i}\sqrt{-1}} \text{ for } k = 0, \dots, d_i \text{ and } i = 1, \dots, n\}\,.$$

The *Bézout homotopy* is the convex combination of F and G,

$$H(x;t) \ := \ tG \ + \ (1-t)F\,. \tag{4.2.8}$$

For any $t \in \mathbb{C}_t$, $H(x;t) = 0$ has at most d isolated solutions. As there are d nondegenerate solutions when $t = 1$, the curve C of Lemma 4.2.1 is nonempty and $1 \in U$. Thus (4.2.8) is a homotopy with start system G having known solutions and target system F.

Proposition 4.2.3. *If the system F is general, then numerical homotopy continuation using the Bézout homotopy will compute all d solutions to $F = 0$.*

This follows from Theorem 4.2.2, once we see that F general implies that assumption (4.2.6) holds. While this follows from the discussion below, our goal is to modify the homotopy (4.2.8) and our path-tracking algorithm to prove the stronger result that the modified Bézout homotopy computes all isolated solutions to the system F.

Let us examine condition (4.2.6) for the Bézout homotopy. At the endpoints $t = 0, 1$, (4.2.6) is ensured if the target system is general. To help understand what may happen for $t \in (0,1)$, consider the Bézout homotopy in one variable

$$H(x;t) \ := \ t(x^2 - 1) + (1-t)(x^2 + x + 1) \ = \ x^2 + (1-t)x + 1 - 2t\,. \tag{4.2.9}$$

The zeroes of $H(x;t)=0$ as a function of t are found using the quadratic formula

$$x(t) \;=\; \frac{t-1}{2} \pm \frac{\sqrt{t^2+6t-3}}{2}\,.$$

The system $H(x;2\sqrt{3}-3)$ has a single root $\sqrt{3}-1$ of multiplicity 2. At that point, $\frac{\partial H}{\partial x}=0$ and so assumption (4.2.6) fails as $2\sqrt{3}-3\approx 0.464$ is a branch point in $[0,1]$.

The Bézout homotopy is a *straight-line homotopy*, which is a convex combination

$$H(x;t) \;:=\; tG+(1-t)F \tag{4.2.10}$$

of two polynomial systems that forms a homotopy (defines a curve C with $t=1$ not a branch point). When both F and G are real as in (4.2.9), the branch locus likely contains real points that meet the interval $[0,1]$ even when 0 is not a branch point. A simple modification gives smooth paths above $[0,1]$. Let γ be any nonzero complex number, and set

$$H_\gamma(x;t) \;:=\; \gamma tG \;+\; (1-t)F\,. \tag{4.2.11}$$

The modification (4.2.11) is called the 'γ-trick'.

THEOREM 4.2.4. *Let F,G be as above. For any nonzero $\gamma\in\mathbb{C}$, $H_\gamma(x;t)$ is a homotopy with start system G and target system F. When 0 is not a branch point of* (4.2.10)*, there is a finite set Θ of arguments such that if* $\arg(\gamma)\notin\Theta$*, then $H_\gamma(x;t)$ satisfies* (4.2.6)*.*

PROOF. For the first statement, substitute $t=1,0$ into the formula for $H_\gamma(x;t)$. To understand the modification (4.2.11) and prove the second statement, note that

$$\frac{\gamma t}{\gamma t+(1-t)}A+\Bigl(1-\frac{\gamma t}{\gamma t+(1-t)}\Bigr)B \;=\; \frac{1}{\gamma t+(1-t)}\bigl(\gamma tA+(1-t)B\bigr)\,,$$

for indeterminates A,B,t. Consequently, if we define $\tau_\gamma(t):=\gamma t/(\gamma t+(1-t))$ and if $\gamma t+(1-t)\neq 0$ for $t\in[0,1]$, then for every $t\in[0,1]$,

$$\gamma tF+(1-t)G \qquad\text{and}\qquad \tau_\gamma(t)F+(1-\tau_\gamma(t))G$$

have the same solutions. That is, if $\gamma t+(1-t)\neq 0$ for $t\in[0,1]$, then the homotopy $H_\gamma(x;t)$ (4.2.11) for $t\in[0,1]$ is a straight-line homotopy (4.2.10), but over the image of $\tau_\gamma\colon[0,1]\to\mathbb{C}$. Solving $\gamma t+(1-t)=0$ gives $\gamma=1-\frac{1}{t}$, so γ cannot be a negative real number, $\arg\gamma\neq\pi$. Identifying $\mathbb{C}$ with $\mathbb{R}^2$ where $(x,y)\leftrightarrow x+y\sqrt{-1}$ and writing $\gamma=a+b\sqrt{-1}$, the path $\tau_\gamma(t)$ for $t\in[0,1]$ lies on the circle $x^2-x+y^2+\frac{a}{b}y=0$ with center $(\frac{1}{2},-\frac{a}{2b})$ and radius $\frac{a^2+b^2}{4b^2}$. This circle contains the points 0 and 1, and the path $\tau_\gamma(t)$ for $t\in[0,1]$ traces the arc of that circle lying in the same half-plane as γ.

The paths defined by $H_\gamma(x;t)=0$ for $t\in[0,1]$ are those in the curve C lying above the image $\tau_\gamma[0,1]$. They will be continuous and satisfy the Davidenko differential equation exactly when $\tau_\gamma[0,1]$ does not meet the branch locus B. As B is finite, τ_γ depends only upon the argument of γ, and the arcs $\tau_\gamma(0,1)$ foliate $\mathbb{C}_t\smallsetminus\mathbb{R}$, there are only finitely many arguments for γ such that $\tau_\gamma[0,1]$ meets B. This completes the proof. □

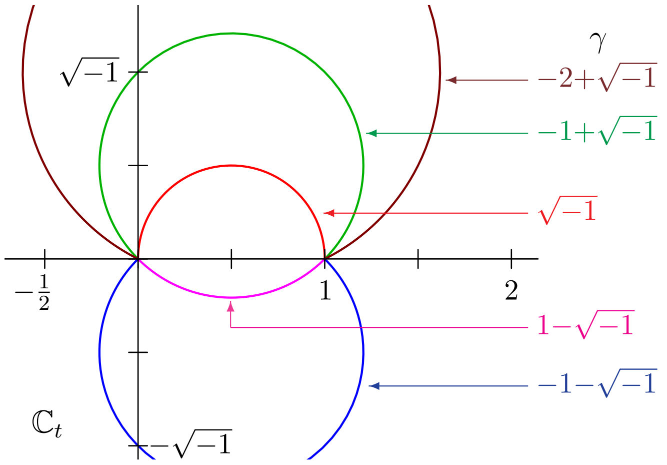


FIGURE 4.2.3. Paths τ_γ for $\gamma = -1-\sqrt{-1}, 1-\sqrt{-1}, \sqrt{-1}, -1+\sqrt{-1}, -2+\sqrt{-1}$

For the Bézout homotopy and any other straight-line homotopy, we use the γ-trick for a general $\gamma \in \mathbb{C} \smallsetminus \mathbb{R}$. This γ-trick is a systematic (and easy) way to choose a smooth path in $\mathbb{C}_t \smallsetminus B$ between 0 and 1, but any such path will suffice. For a general homotopy, we will assume that the tracking is done over a general smooth path $\tau \subset \mathbb{C}_t$ between 0 and 1. These assumptions imply that branch points in $\mathbb{C}_t \smallsetminus \{0\}$ may be avoided. This is commonly expressed as "the homotopy defines smooth paths, *with probability one*". That is, the set of paths between 0 and 1 in $\mathbb{C}_t$ that meet the base locus has measure zero in the collection of all paths considered.

Suppose that we have a homotopy $H(x;t)$ and assume for simplicity that the interval $(0,1] \subset \mathbb{C}_t$ does not meet the branch locus B. (In general choose a smooth path τ in $(\mathbb{C}_t \smallsetminus B) \cup \{0\}$ between 0 and 1.) Then $C|_{(0,1]}$ is a collection of d half-open smooth paths, and at each point of every path the Jacobian matrix DH_x is invertible. When $0 \notin B$, the homotopy satisfies (4.2.6) and by Theorem 4.2.2 numerical homotopy continuation computes all solutions to the target system, given the solutions to the start system. When $0 \in B$, by Lemma 4.2.1 there are several cases for a path $x(t)$ in $C|_{(0,1]}$ in the limit as $t \to 0$.

(1) The path $x(t)$ does not have a limit as it becomes unbounded as $t \to 0$.
(2) The path $x(t)$ has a limit $x(0)$ and D_xH is invertible at $x(0)$.
(3) The path $x(t)$ has a limit $x(0)$ that lies on another component of $\mathcal{V}(H)$ so that D_xH is not invertible at $x(0)$.
(4) The path $x(t)$ has a limit $x(0)$ that is a branch point of $C \to \mathbb{C}_t$, so that D_xH is not invertible at $x(0)$ and at least one other path also ends at $x(0)$.

Figure 4.2.4 is a schematic showing these four cases.

In Case (2), when D_xH is invertible at the endpoint $x(0)$ of the path $x(t)$, this path may be successfully tracked from $x(1)$ to $x(0)$. In all other cases, simple path-tracking will fail, as D_xH is not invertible at $x(0)$. and alternatives to simple path-tracking, called *endgames*, are needed.

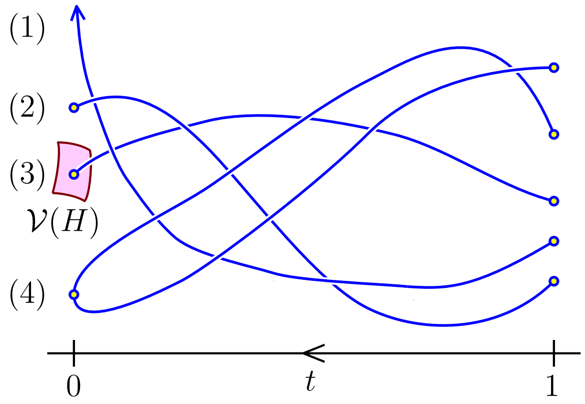


FIGURE 4.2.4. Possible behavior of homotopy paths near $t = 0$.

Case (1) There are at least two endgames when $x(t)$ becomes unbounded as $t \to 0$. For one, when $\|x(t)\|$ exceeds a heuristic threshold, tracking is halted and the path is declared to diverge. The other applies, for example, when the homotopy $H(x;t)$ for $x \in \mathbb{C}^n_x$ and $t \in \mathbb{C}_t$ is the restriction of a homotopy $\widetilde{H}(z;t)$ for $z \in \P^n$ to an affine patch $\mathbb{C}^n_x \subset \P^n$. Choosing a different affine patch $\mathbb{C}^n_y$ and applying a change of coordinates expresses the homotopy and the computed points on the path $x(t)$ in the coordinates y of $\mathbb{C}^n_y$. If $\mathbb{C}^n_y$ is chosen propitiously (e.g. at random), then the resulting path $y(t)$ converges in $\mathbb{C}^n_y$ to a point $y(0)$ as $t \to 0$, and this path falls into one of cases (2), (3), or (4).

Case (3) While geometrically distinct from Case (4), this is treated in the same way as Case (4).

Case (4) The curve C is either singular at $x(0)$ or the map to $\mathbb{C}_t$ is ramified at $x(0)$, or both. Let us examine in detail its geometry near $x(0)$ before describing the Cauchy endgame, which also applies to the other cases (2) and (3).

Let $f\colon \widetilde{C} \to C$ be the normalization of C, so that $\widetilde{C}$ is smooth. The *ramification index* $r = r(x')$ of a preimage $x' \in f^{-1}(x(0))$ is the order of vanishing at x' of the (rational) function t that is the composition $\pi\colon \widetilde{C} \to C \to \mathbb{C}_t$, with the second map the projection onto the t-coordinate. If s is a nonconstant rational function on $\widetilde{C}$ that vanishes to order 1 at x', then $t = s^r g$, for some rational function g with $g(x') \neq 0$.

Suppose that $\Delta \subset \mathbb{C}_t$ is a disc centered at the origin small enough so that 0 is the only branch point in Δ. Then each component of its preimage $\pi^{-1}(\Delta)$ in $\widetilde{C}$ contains a unique point $x' \in \pi^{-1}(0)$. On the component Δ' containing x', the map $\pi\colon \Delta' \smallsetminus \{x'\} \to \Delta \smallsetminus \{0\}$ of punctured neighborhoods is an r-fold covering space, analytically isomorphic to the map $s \mapsto s^r$. Over the punctured disc $\Delta \smallsetminus \{0\}$, the two curves $\widetilde{C}$ and C agree, and the image in C of a component of $\pi^{-1}(\Delta)$ is a *branch* of C at the corresponding point above 0. Figure 4.2.5 shows some possibilities near a ramification point. The map $C \to \mathbb{C}_t$ is the vertical projection and only one veritcal real dimension is shown. (The self-intersections, except at $x(0)$, are artifacts of this.) In (a), C is singular at $x(0)$ with two smooth

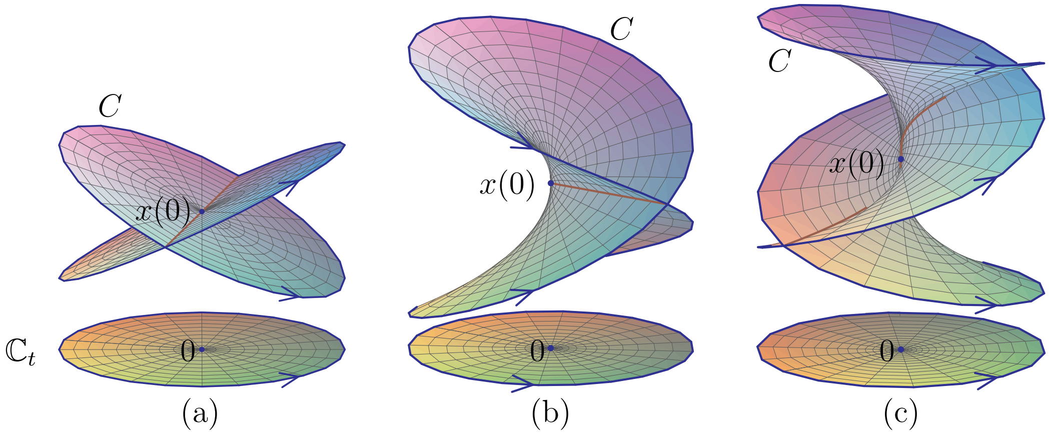


FIGURE 4.2.5. Local behaviour near a ramification point.

branches, each with ramification index 1. In (b), C is smooth with one branch at $x(0)$ and ramification index 2. In (c), the ramification index is 3.

The ramification index is also a winding number. Given a point $x(\epsilon) \in C$ for $\epsilon > 0$ in the disc $\Delta \subset \mathbb{C}_t$, analytic continuation on C starting at $x(\epsilon)$ above the circle $\epsilon e^{2\pi\theta\sqrt{-1}}$ for $\theta \geq 0$ gives a closed path $(y(\theta), \epsilon e^{2\pi\theta\sqrt{-1}})$ in C which is parametrized by $\theta \in [0, r]$. The path $(y(\theta), \epsilon e^{2\pi\theta\sqrt{-1}})$ encircling $x(0)$ in C has image in $\mathbb{C}_t$ winding r times around 0. Figure 4.2.5 shows the circle and these paths. The ramification index may be computed numerically by tracking the path $(y(\theta), \epsilon e^{2\pi\theta\sqrt{-1}})$ for $\theta \geq 0$.

We may compute the endpoint $x(0)$ of the path $x(t)$ in C without tracking the path $x(t)$ to $t = 0$ using Cauchy's integral formula. Recall that if g is a function that is holomorphic in a neighborhood of closed disc D centered at the origin, then

$$g(0) \;=\; \frac{1}{2\pi\sqrt{-1}} \oint_{\partial D} \frac{g(z)}{z} dz \;.$$

This holds also when g is vector-valued. In our case, let D be the unit disc and consider the map $D \to \Delta$ where $z \mapsto \epsilon z^r =: t$. This lifts to a map $g\colon D \to C$ with $g(0) = x(0)$ and $g(e^{2\pi\alpha\sqrt{-1}}) = (y(r\alpha), e^{2\pi\alpha\sqrt{-1}})$ to which we may apply the Cauchy integral formula. After a change of coordinates, we obtain

$$x(0) \;=\; \Big(\frac{1}{\sqrt{-1}} \int_0^1 \frac{y(r\alpha)}{e^{2\pi\alpha\sqrt{-1}}}\, d\alpha \;,\; 0\Big) \;. \tag{4.2.12}$$

The *Cauchy endgame* is a numerical algorithm using this.

ALGORITHM 4.2.5 (Cauchy Endgame).
<u>INPUT:</u> A homotopy $H(x;t)$, curve C as in Lemma 4.2.1, a path $x(t)$ on C with limit $x(0)$ as $t \to 0$, and a point $x(\epsilon)$ on the path with $\epsilon > 0$.
<u>OUTPUT:</u> A numerical approximation to $x(0)$ and the ramification index.

(1) Starting at $x(\epsilon) = (y(0), \epsilon)$, track the path $y(\theta)$ above the circle $\epsilon e^{2\pi\theta\sqrt{-1}}$ from $\theta = 0$ until the first integer $r > 0$ with $y(r) = y(0)$.

(2) Using the computed intermediate values of θ and $y(\theta)$, estimate $x(0)$, using numerical integration for the integral (4.2.12).

(3) Track $x(t)$ from $x(\epsilon)$ to $x(\epsilon/2)$, replace ϵ by $\epsilon/2$, and repeat steps (1) and (2), obtaining another estimate for $x(0)$.

If successive estimates agree up to a tolerance, or do so after it repeating (3), then exit and return the computed value of $x(0)$, along with r.

Remark 4.2.6. The Cauchy endgame applies in each of the cases (1)—(4) above. (In (1), first change coordinates in $\P^n$ so that the path has a finite limit.) Simply stop the tracking of $x(t)$ at some fixed ϵ (e.g. $\epsilon = 0.1$), and then apply the Cauchy endgame. There will be r paths that converge to the endpoint $x(0)$. An additional check verifies that there are indeed $r-1$ other paths with this endpoint.

We deduce a strengthening of Theorem 4.2.2.

Theorem 4.2.2′ *Numerical homotopy continuation with endgames computes all isolated solutions to the start system $H(x;0) = 0$.*

A homotopy is *optimal* if every isolated solution of the target system is connected to a unique solution of the start system along a path of $C|_\tau$, for $\tau \subset \mathbb{C}_t \smallsetminus B$ a path connecting 0 to 1. By Proposition 4.2.3, the Bézout homotopy is optimal, for a general target system F. In a non-optimal homotopy some paths either diverge (Case(1)) or become singular (Cases (3) and (4)), all of which require expensive endgames.

The cost of using numerical homotopy continuation to solve a system of polynomials is dominated by path-tracking and engames, and is therefore minimized for optimal or near optimal homotopies. A significant advantage is that homotopy continuation algorithms are inherently massively parallelizable—once the initial precomputation of solving the start system and setting up the homotopies is completed, then each solution curve may be followed independently of all other solution curves.

Given a specific target system $F = (f_1, \ldots, f_n)$ with $\deg F_i = d_i$, using the Bézout homotopy (4.2.8) to compute its solutions may be problematic as neither the start (4.2.7) nor the target systems are necessarily generic. In practice the more robust Bézout homotopy algorithm overcomes this by using a two-step process.

Algorithm 4.2.7 (Bézout Homotopy Algorithm).
Input: A target system $F = (f_1, \ldots, f_n)$ with $\deg f_i = d_i$.
Output: Numerical approximations to the isolated zeroes of $\mathcal{V}(F)$.

(1) Generate a random system $E = (e_1, \ldots, e_n)$ of polynomials with $\deg e_i = d_i$.

(2) Use the Bézout homotopy (4.2.8) with start system (4.2.7) to compute all $d = d_1 \cdots d_n$ solutions to $\mathcal{V}(E)$.

(3) Use the straight-line homotopy $tE + (1-t)F$ starting with the solutions to E to compute the isolated solutions to $\mathcal{V}(F)$, possibly employing endgames.

Theorem 4.2.8. *The Bézout homotopy algorithm computes all isolated zeroes of F.*

This is a probability one algorithm, as it requires that $\mathcal{V}(E)$ consist of d isolated solutions, which holds on an open dense set of such systems.

Proof. As E is generic, Proposition 4.2.3 implies that the first homotopy is optimal and it will compute all d solutions to $\mathcal{V}(E)$. For every t, the second homotopy is a system of polynomials in x of degrees $d_1, \dots, d_n$ and so by Bézout's Theorem it has at most d isolated solutions, and when there are d solutions, all are nondegenerate. Since the start system has d solutions, this implies that $C|_{(0,1]}$ consists of d half-open paths beginning at $t = 1$ with $\mathcal{V}(E)$. By our discussion of endgames (and possibly using projective coordinates in Case (1)), all isolated solutions of $\mathcal{V}(F)$ will be found. □

Example 4.2.9. One source of homotopies are polynomial systems that depend upon parameters. For example, a bivariate polynomial $F_d(x; c)$ of degree d ($x \in \mathbb{C}^2$) has coefficients $c \in \mathbb{C}^{\binom{d+2}{2}}$. Thus a system consisting of a quadratic $F_2(x; a)$ and a cubic $F_3(x; b)$ depends upon $\binom{4}{2} + \binom{5}{2} = 6 + 10 = 16$ parameters. This gives a family

$$\Gamma \ := \ \{(x; a, b) \in \mathbb{C}^2 \times \mathbb{C}^6 \times \mathbb{C}^{10} \mid F_2(x; a) = F_3(x; b) = 0\}\,,$$

with a map $\Gamma \to \mathbb{C}^{16}$ whose fiber over $(a, b) \in \mathbb{C}^{16}$ is the set of common zeroes to $F_2(x; a)$ and $F_3(x; b)$. There is a non-empty Zariski open set $U \subset \mathbb{C}^{16}$ consisting of pairs (a, b) for which the fiber has six solutions and its complement is the branch locus B. We call U the set of regular values of $\Gamma \to \mathbb{C}^{16}$. For a and b general, this has six solutions by Bézout's Theorem. We obtain a homotopy by parametrizing a line ℓ in the base, $f\colon \mathbb{C} \to \ell \subset \mathbb{C}^{16}$ where $f(t) = (a(t), b(t))$ with each component linear, and where $(a(1), b(1))$ gives a system with six solutions. Then $\Gamma|_\ell = f^{-1}(\Gamma)$ is given by the homotopy $H(x; t) := (F_2(x; a(t)), F_3(x; b(t)))$.

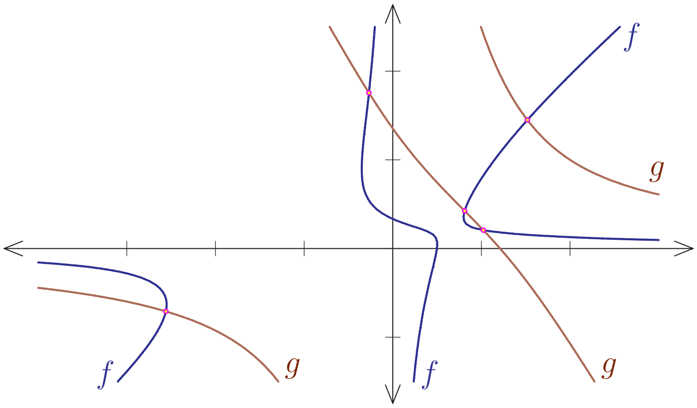
A homotopy arising from such a family where the start and target systems lie in the open set of regular values is a *parameter homotopy*. The Bézout homotopy for a general target system is a parameter homotopy. Nearly every homotopy we use will be a parameter homotopy, often with a propitious choice of line (or a rational curve) in the base.

Polynomial systems arising 'in nature' are rarely generic dense systems. The bound from Bézout's Theorem for the number of isolated solutions is typically not achieved.

For example, consider the system of cubic polynomials,

$$\begin{array}{rrcrcrcrcrcrcl} f\colon & 1 & - & 2x & - & 3y & + & 4xy & + & 5x^2y & - & 6xy^2 & = & 0 \\ g\colon & 23 & - & 17x & - & 19y & - & 13xy & + & 11x^2y & + & 7xy^2 & = & 0 \end{array} \tag{4.2.13}$$

This has the five solutions shown below, and not the 9 predicted by Bézout's Theorem.



Section ????? describes a method to solve structured systems of equations that are either not square or have fewer solutions than expected from Bézout's Theorem. Square systems of the form 4.2.13 which are general given the monomials in each polynomial are called *sparse*, and the polyhedral homotopy, based on ideas from the study of toric varieties, is an optimal homotopy for sparse systems. This will be developed in Section **??**.

Exercises.

(1) Find the solutions to the system of equations (4.2.1) directly, and also by solving the initial value problem for the differential equation 4.2.5 starting at the solutions (4.2.3) using any of the iterative methods of Section 4.1.
(2) Give a proof of Lemma 4.2.1.
(3) Let $\gamma = a + b\sqrt{-1}$ with a, b real and $b \neq 0$. Show that the path in the complex plane $\tau_\gamma(t) := \gamma t/(\gamma t + (1-t))$ for $t \in [0,1]$ lies on the circle with centre $(\frac{1}{2}, -\frac{a}{2b})$ and radius $\frac{a^2+b^2}{4b^2}$, which contains the points 0 and 1. Show that the tangent direction of τ_γ at $t = 0$ is γ and that $\tau_\gamma[0,1]$ lies in the same half-plane as γ.
(4) Discuss how to get equations for the branch locus in Example 4.2.9.
(5) Explain the ramification of $y^2 = x^3$ in each coordinate projection.
(6) Verify the claim in the text that the system (4.2.13) has exactly five solutions.
(7) Needs more exercises.

4.3. Numerical Algebraic Geometry

In Section 4.2 on numerical homotopy continuation, we discussed path-tracking, presented the Bézout homotopy to compute all isolated solutions to a square system of polynomial equations, and mentioned improvements that are covered elsewhere in this text. Numerical algebraic geometry uses this ability to solve systems of polynomial equations to represent and study algebraic varieties on a computer. We first discuss overdetermined and undetermined systems of equations before introducing the notion of a witness set, which is one of the fundamental ideas in numerical algebraic geometry.

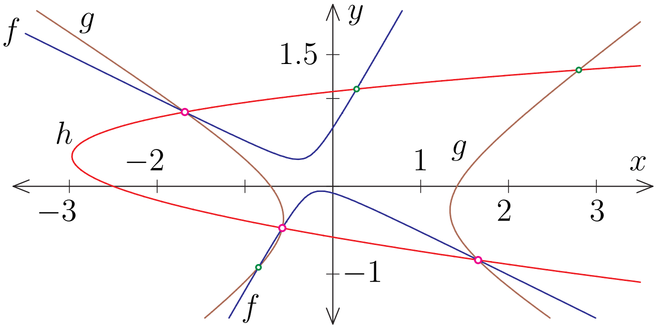
EXAMPLE 4.3.1. Consider the following problem. For which values of (x, y) does the following matrix of linear polynomials have rank one?

$$M(x,y) := \begin{pmatrix} 4-4x+8y & 3-7x-y & 9-7x+8y \\ 6+6x+y & 5+2x-5y & 5+2x-8y \end{pmatrix} \tag{4.3.1}$$

A nonzero 2×3 matrix has rank one if and only if all three of its 2×2 minors vanish. This gives the following system of three polynomial equations,

$$\begin{array}{rlcl} f: & (4-4x+8y)(5+2x-5y) & - & (3-7x-y)(6+6x+y) = 0 \\ g: & (4-4x+8y)(5+2x-8y) & - & (9-7x+8y)(6+6x+y) = 0 \\ h: & (3-7x-y)(5+2x-8y) & - & (9-7x+8y)(5+2x-5y) = 0 \end{array} \tag{4.3.2}$$

These minors define three curves in the plane



which appear to have three common solutions. We may verify this by computing a lexicographic Gröbner basis with $y < x$ from the minors (4.3.2),

$$G \;=\; \{213y^3 + 100y^2 - 152y - 72\,,\; 213y^2 - 136y - 68x - 152\}\,.$$

The eliminant in y has degree three. Finding its roots, substituting into the second polynomial, and solving for x gives the three solutions

$$(4.3.3)\quad (1.654564, -0.8399545)\,,\; (-0.5754011, -0.4756340)\,,\; (-1.685073, 0.8461049)\,.$$

Each pair of minors vanishes at four points. The fourth point is where the column common to the two minors vanishes. It may be pruned from the other three by evaluating the third minor at all four points and retaining only those where the evaluation is below a predetermined threshold. For example, the minors f and g also vanish at $(-11/13, -12/13)$. Evaluating the third minor h at these four points gives the values $(-4.5 \times 10^{-6}, -1.3 \times 10^{-7}, 9.2 \times 10^{-7}, 45.6)$. The value of h at three of the points is approximately the working precision, so we (correctly) discard the fourth. [†]

As in Example 4.3.1, meaningful systems of equations are not necessarily square; they may have more equations than variables (are *overdetermined*), and yet define a zero-dimensional ideal. There may be no reasonable way to select a square subsystem whose solutions are only those of the original system. When faced with an overdetermined system, one approach is to randomly select a square subsystem ('squaring up' the original system). This square system is solved and polynomials from the original system are used to prune the excess solutions found in the square subsystem.

ALGORITHM 4.3.2 (Squaring up).
INPUT: An overdetermined system $F\colon \mathbb{C}^n \to \mathbb{C}^m$ $(m > n)$ of polynomials.
OUTPUT: A square system $G\colon \mathbb{C}^n \to \mathbb{C}^n$ whose solutions $\mathcal{V}(G)$ contain the solutions $\mathcal{V}(F)$ of F, with the nondegenerate solutions of F remaining nondegenerate for G.[§]
DO: Select a random linear map $\Lambda\colon \mathbb{C}^m \to \mathbb{C}^n$ and return $G := \Lambda \circ F$.

Algorithm 4.3.2 is a 'probablility one' algorithm. We give a proof of its correctness.

[†] This needs to refer to an algorithm for solving in Chapter 2.

[§] Strengthen this to isolated solutions.

THEOREM 4.3.3. *For any linear map $\Lambda\colon \mathbb{C}^m \to \mathbb{C}^n$, we have the containment $\mathcal{V}(F) \subset \mathcal{V}(G)$ of solutions in Algorithm* 4.3.2. *There is a nonempty Zariski open subset U of $n \times m$ complex matrices consisting of linear maps Λ such that the nondegenerate solutions of F remain nondegenerate soutions of $G = \Lambda \circ F$.*

PROOF. As Λ is linear, if $F(x) = 0$, then $\Lambda \circ F(x) = 0$, which proves the first statement.

For the second statement, let $x \in \mathcal{V}(F) \subset \mathbb{C}^n$ be nondegenerate. Then the Jacobian matrix $DF(x)$ at x gives an injective linear map from $\mathbb{C}^n = T_x\mathbb{C}^n \to \mathbb{C}^m$. A point $x \in \mathcal{V}(G)$ is nondegenerate if the composition $DG(x) = \Lambda \circ DF(x)\colon \mathbb{C}^n \to \mathbb{C}^n$ is injective. Geometrically, this means that the kernel of Λ is transverse to the image of $DF(x)$. This condition defines a nonempty open subset in the space of linear maps. Since $\mathcal{V}(F)$ has finitely many nondegenerate solutions, the set U is the intersection of these nonempty open subsets, one for each nondegenerate solution $x \in \mathcal{V}(F)$. □

REMARK 4.3.4. Choosing a random linear map $\Lambda\colon \mathbb{C}^m \to \mathbb{C}^{n-d}$ gives a subsystem $G = \Lambda \circ F$ of F with the following properites: Every component of $\mathcal{V}(G)$ has dimension at least d. These include all irreducible components of $\mathcal{V}(F)$ of dimension d or greater, together with possibly some other components of dimension d.

EXAMPLE 4.3.5. Let us view Example 4.3.1 in a different light. Suppose that we want a rank one 2×3 matrix M, that is, a solution to the equations

$$M_{1,1}M_{2,2} - M_{1,2}M_{2,1} \;=\; M_{1,2}M_{2,3} - M_{1,3}M_{2,2} \;=\; M_{1,1}M_{2,3} - M_{1,3}M_{2,1} \;=\; 0\,. \tag{4.3.4}$$

With three linearly independent equations on a six-dimensional space, this defines a subvariety of either of dimension three or of dimension four. We reduce this to a zero-dimensional problem by slicing the set of solutions to (4.3.4), adding the (successive) linear equations

$$\begin{array}{rcr} 5M_{1,1} - 2M_{1,3} + 3M_{2,3} &=& 17 \\ 40M_{1,2} - 58M_{1,3} - 63M_{2,3} &=& -717 \\ 8M_{2,1} + 10M_{1,3} + 11M_{2,3} &=& 193 \\ 40M_{2,2} + 6M_{1,3} - 19M_{2,3} &=& 159 \end{array} \tag{4.3.5}$$

Only after these four linear equations are added to (4.3.4) do we obtain a zero-dimensional system with three solutions. This shows that the dimension of the set of rank one 2×3 matrices is four. The local dimension test, which we will describe later, is another way to determine the dimension of a variety, given a point on it and its defining equations.

A system of equations as in (4.3.4) that defines a positive-dimensional variety V whose points are of interest is an underdetermined system. As in Example 4.3.5, adding further equations to reduce its dimension to zero will give a system of polynomials to solve, obtaining points of V. By Bézout's Theorem, this system is expected to have the fewest number of solutions when the additional equations are linear. In this case, the linear equations define a linear subspace L whose codimension equals the dimension of V (L is complimentary to V), and the points are the linear section $V \cap L$.

These two techniques of squaring up and slicing down reduce any system of equations to a square system whose solutions may be further processed to obtain solutions to the original problem. When the system is underdetermined and defines a variety $V = \mathcal{V}(F)$, we obtain points of V in the complimentary linear section $V \cap L$. Numerical algebraic geometry uses this to study the algebraic variety V.

Remark 4.3.6. In Examples 4.3.1 and 4.3.5, the variety of rank one 2×3 matrices were sliced by the same linear subspace. The linear equations (4.3.5) define a four-dimensional linear subspace L of $\mathrm{Mat}_{2\times 3}\mathbb{C}$, and the family of matrices $M(x,y)$ (4.3.1) for $x,y \in \mathbb{C}$ is a parametrization of L. You are asked to verify this in Exercise 1.

Any linear subspace of $\mathbb{C}^n$ has an extrinsic description as the vanishing set of some linear equations, and an intrinsic description as the image of a linear map (a parametrization). Either description may be used for slicing. This flexibility may be used to improve the efficiency of an algorithm.

The first question numerical algebraic geometry addresses is how to represent an algebraic variety $V \subset \mathbb{C}^n$ on a computer? In symbolic computation, this is answered by giving a finite set of polynomials $F = \{f_1, \ldots, f_m\}$ such that $V = \mathcal{V}(F)$, perhaps with the good algorithmic property of being a Gröbner basis for the ideal of V. In numerical algebraic geometry, if V is zero-dimensional, then the list V of (approximations to) its points, together with the polynomials that define V is a reasonable representation. When the dimension of V is at least one, we will slice V to obtain a collection of points and use these points and the slice as our representation.

Definition 4.3.7. Let $V \subset \mathbb{C}^n$ be an irreducible variety of dimension d. A *witness set* for V is a set W of the form $V \cap L$, where L is a general linear subspace of $\mathbb{C}^n$ complimentary to V, so that it has codimension d. The generality of V ensures that the intersection is transverse and by Bézout's Theorem[†], W consists of $\deg V$ points. For computational/algorithmic purposes, we will represent a witness set for V by a triple (W, F, L). Here, $W = V \cap L$ with V an irreducible component of $\mathcal{V}(F)$ where $F = \{f_1, \ldots, f_m\}$ a system of polynomials on $\mathbb{C}^n$ and $L = \{\ell_1, \ldots, \ell_d\}$ is d general linear polynomials. (We write L for both the linear subspace and its given equations.)

The same definition makes sense when V is a reducible variety, all of whose components have the same dimension d. While a witness set is certainly a representation of a variety, this definition is justified by its utility. We shall see that a witness sets is the central notion in numerical algebraic geometry and is the input for many of its algorithms. We describe some of the more elementary algorithms that use witness sets. (Needs Examples)

Sampling. A witness set (W, F, L) for a variety $V \subset \mathbb{C}^n$ includes a collection of points of V. If $L' = \{\ell'_1, \ldots, \ell'_d\}$ is another collection of d linear polynomials, we may form the straight-line homotopy

$$H(x;t) \;:=\; (F(x)\,,\, tL(x) + (1-t)L'(x))\,. \tag{4.3.6}$$

For almost all $t \in \mathbb{C}$, the d linear polynomials $tL(x) + (1-t)L'(x)$ define a codimension d linear subspace $L_t \subset \mathbb{C}^n$ with $L_1 = L$ and $L_0 = L'$. As $V \cap L$ is transverse, for any point $w \in W = V \cap L$, the homotopy (4.3.6) defines a path $w(t)$ in V for $t \in (0,1]$ with

[†] Make sure to state it this way in Chapter 3

$w(1) = w$ and well-defined endpoint $w(0) = \lim_{t\to 0} w(t)$ (perhaps lying at infinity in V). We may use a witness set as the input for an algorithm to sample points of V.

Algorithm 4.3.8 (Sampling).
Input: A witness set (W, F, L) for $V \subset \mathbb{C}^n$.
Output: Point(s) of V.
Do:
(1) Choose d linear polynomials $L' = \{\ell'_1, \ldots, \ell'_d\}$ and form the homotopy $H(x; t)$ (4.3.6).
(2) Follow one or more points w of W along the homotopy $H(x; t)$ from $t = 1$ to $t = 0$ and return the endpoints $w(0)$ of the homotopy paths.

Proof of correctness. By the generality of L, all homotopy paths $w(t)$ for $w \in W$ are smooth for $t \in (0, 1]$. In particular, each lies in the smooth locus of $\mathcal{V}(F)$. As the initial point $w(1)$ of each path is a point of $W = V \cap L$, the path lies on V, and in particular, its endpoint $w(0)$ is a point of V (possibly singular in $\mathcal{V}(F)$ or at infinity). □

Moving a witness set. If the linear polynomials $L' = \{\ell'_1, \ldots, \ell'_d\}$ in (4.3.6) are general, then $V \cap L'$ is transverse and consists of $\deg(V)$ points, by Corollary 3.6.19. Thus $W' = (V \cap L', F, L')$ is another witness set for V. This justifies the following algorithm.

Algorithm 4.3.9 (Moving a Witness Set).
Input: A witness set (W, F, L) for $V \subset \mathbb{C}^n$.
Output: A second witness set $(V \cap L', F, L')$ for V.
Do: Choose general linear polynomials $L' = (\ell'_1, \ldots, \ell'_d\}$ on $\mathbb{C}^n$. Run Algorithm 4.3.8 on all points $w \in W$, using this choice of L'. Set W' to be the collection of endpoints obtained and output (W, F, L').

Remark 4.3.10. Note that this algorithm only needs that $W = V \cap L$ is transverse and consists of $\deg(V)$ points, for then (4.3.6) is a homotopy defining paths that start at points w of W. It is only needed that L' be a general complimentary linear subspace.

Similarly, the Sampling Algorithm 4.3.8 only needs a complimentary linear space L and a point $w \in V \cap L$ where $V \cap L$ is transverse at w to sample points of V.

Membership. Suppose that $x \in \mathbb{C}^n$ is a point of $\mathcal{V}(F)$. We may use a witness set (W, F, L) for a variety V that is a component of $\mathcal{V}(F)$ to determine if $x \in V$.

Algorithm 4.3.11 (Membership Test).
Input: A witness set (W, F, L) for $V \subset \mathbb{C}^n$ and a point $x \in \mathcal{V}(F)$.
Output: True (if $x \in V$) or False (if $x \notin V$).
Do:
(1) Choose d linear polynomials $L' = \{\ell'_1, \ldots, \ell'_d\}$ that are general given that $\ell'_i(x) = 0$.
(2) Call Algorithm 4.3.8 using L' in the homotopy (4.3.6) and follow homotopy paths from every point $w \in W$.
(3) If x is an endpoint of one of these paths, return True, otherwise, return False.

Proof of correctness. By the genericity of L', the set $W' := V \cap L'$ consists of $\deg(V)$ points, counted with multiplicity. All points of W', except possibly x (if $x \in W$), are smooth points of V with none at infinity, and all points of W' are endpoints of homotopy paths.[†] Thus $x \in V$ if and only if it is an endpoint of a path given by the homotopy (4.3.6) that starts at some point of W. □

Inclusion. Suppose that X and V are irreducible subvarieties of $\mathbb{C}^n$. If $X \not\subset V$, then their set-theoretic difference $X \smallsetminus V$ is open and dense in X. Furthermore, if L is a general linear subspace complimentary to X, then $X \cap L \subset X \smallsetminus V$. This observation leads to the following probability one algorithm to test if $X \subset V$.

ALGORITHM 4.3.12 (Inclusion).
INPUT: Witness sets (W_X, F_X, L_X) for $X \subset \mathbb{C}^n$ and (W_V, F_V, L_V) for $V \subset \mathbb{C}^n$.
OUTPUT: True (if $X \subset V$) or False (if $X \not\subset V$).
DO:
(1) Call the Sampling Algorithm 4.3.8 using the witness set (W_X, F_X, L_X) for X to obtain a point $x \in X \cap L'$, where L' is a general linear subspace complimentary to X.
(2) Call the Membership Test Algorithm 4.3.11 to test if $x \in V$.

PROOF OF CORRECTNESS. The point $x \in X$ lies in $X \cap L'$, where L' is a general linear subspace complimentary to X. If $X \subset V$, then $x \in V$, and the algorithm returns True. If $X \not\subset V$, then with probability one $(X \cap L') \cap V = \emptyset$, so that $x \notin V$ and the algorithm returns False. □

The first step in this algorithm is precautionary because L_X may not be sufficiently general to avoid points of $X \cap V$ when $X \not\subset V$.

Witness set of a product. Suppose that $A \subset \mathbb{C}^n$ and $B \subset \mathbb{C}^m$ are irreducible varieties and that (W_A, F_A, L_A) and (W_B, F_B, L_B) are witness sets for A and B, respectively. Here $F_A = F_A(x)$ is a system of polynomials on $\mathbb{C}^n$ and $F_B = F_B(y)$ is a system of polynomials on $\mathbb{C}^m$. The product $A \times B$ is an irreducible component of the concatenation $F = F(x, y) = (F_A(x), F_B(y))$ of the two systems. Also, the degree of $A \times B$ is the product of the degree of A and the degree of B. Furthermore, $L_A \times L_B$ is a linear subspace of $\mathbb{C}^n \times \mathbb{C}^m$ complimentary to $A \times B$ and $W_A \times W_B = (A \times B) \cap (L_A \times L_B)$ is transverse and consists of $\deg(A) \cdot \deg(B)$ points. While we would like for $(W_A \times W_B, (F_A, F_B), L_A \times L_B)$ to be a witness set for $A \times B$, it is not a witness set as $L_A \times L_B$ is not a general linear subspace of $\mathbb{C}^n \times \mathbb{C}^m$. For example, $L_A \times L_B$ is not in general position with respect to the coordinate projections to $\mathbb{C}^n$ and to $\mathbb{C}^m$.

ALGORITHM 4.3.13 (Witness Set of a Product).
INPUT: Witness sets (W_A, F_A, L_A) for $A \subset \mathbb{C}^n$ and (W_B, F_B, L_B) for $B \subset \mathbb{C}^m$.
OUTPUT: A witness set (W, F, L) for the product $A \times B \subset \mathbb{C}^n \times \mathbb{C}^m$.
DO:
(1) Set $F := (F_A, F_B)$ and choose general linear forms $L = (\ell_1, \ldots, \ell_d)$ on $\mathbb{C}^n \times \mathbb{C}^m$ where $d = \dim(A) + \dim(B)$.
(2) Call the Moving Algorithm 4.3.9 with input $(W_A \times W_B, F, (L_A, L_B))$ to move the set $W_A \times W_B$ to the set $W := (A \times B) \cap L$.

PROOF OF CORRECTNESS. The collection (L_A, L_B) defines $L_A \times L_B$. We observed that while $W_A \times W_B = (A \times B) \cap (L_A \times L_B)$ is transverse and consists of $\deg(A \times B) =$

[†] There is something to prove here that should have been proved earlier

$\deg(A) \cdot \deg(B)$ points, it is not a witness set as $L_A \times L_B$ is not a general complimentary linear subspace. By Remark 4.3.10, the Moving Algorithm 4.3.9 only needs its input to be a transverse intersection with a complimentary linear subspace to compute a witness set. This implies that (W, F, L) will be a witness set for the product $A \times B$. □

Witness sets for projections. Suppose that $X \subset \mathbb{C}^n \times \mathbb{C}^k$ is a variety that is an irreducible component of a system $F = F(x, y)$ of polynomials with $x \in \mathbb{C}^n$ and $y \in \mathbb{C}^k$. Let $\pi\colon \mathbb{C}^n \times \mathbb{C}^k \to \mathbb{C}^n$ be the coordinate projection and set $V := \overline{\pi(X)}$, and irreducible subvariety of $\mathbb{C}^n$. By Lemma 2.1.7, this coordinate projection corresponds to the elimination of the y variables from $F(x, y)$, which may be accomplished by resultants or Gröbner bases. Besides the potential complexity of this computation, there is a very real and practical problem with symbolic elimination: If X' is an irreducible component of $\mathcal{V}(F)$, eliminating y from F gives polynomials that vanish on $\pi(X')$. If it happens that $\overline{\pi(X)} \subset\neq \overline{\pi(X')}$, then we could not study $V = \overline{\pi(X)}$ using an eliminant.

In this setting of a projection, we instead use a variant of a witness set for V. For this, let $M \subset \mathbb{C}^k$ be a general linear subspace complimentary to V. As M is general, $V \cap M$ is transverse and each of its $\deg(V)$ points lies in $\pi(X)$. The intersection $X \cap (\mathbb{C}^n \times M)$ is a collection of $\deg(V)$ fibers of the projection $X \to V$. Write X_v for the fiber over a point $v \in V \cap M$. The genericity of M implies that these fibers all have the same dimension, $\dim(X) - \dim(V)$, and they all have the same degree.

Let $L \subset \mathbb{C}^n$ be a general linear subspace of codimension $\dim(X) - \dim(V)$. As it is general, L meets each of the fibers X_v for $v \in V \cap M$ transversally in $\deg(X_v)$ points, and we have

$$X \cap (L \times M) \;=\; \bigcup \{X_v \cap L \mid v \in V \cap M\}\,.$$

The quadruple $(X \cap (L \times M), F, L, M)$ is a *pseudowitness set* for $V = \overline{\pi(X)}$. This representation of V does not require knowing polynomials that vanish on V.

A pseudowitness set for the image $\overline{\pi(X)}$ of a projection may be computed from a witness set (W, F, L_X) for X in the same way as Algorithm 4.3.13, but run in reverse. That is, given L and M, we compute $X \cap (L \times M)$ from $X \cap L_X$ using a homotopy between the general linear subspace L_X and the linear subspace $L \times M$.

As the complimentary linear subspace $L \times M$ in a pseudowitness set is not in general position, algorithms that involve manipulating a pseudowitness set for V to obtain a pseudowitness set for another variety $V' = \overline{\pi(X')}$ will have two additional steps (1 and 3 below) as described in the following outline.

(1) Use the pseudowitness set $(X \cap (L \times M), F, L, M)$ for $\overline{\pi(X)}$ to compute a witness set (W, F, L_X) for X (using Algorithm 4.3.13).
(2) Apply an appropriate construction or algorithm on X using (W, F, L_X) to obtain a witness set (W', F', L'_X) for a variety X' with projection $\overline{\pi(X')} = V'$.
(3) Using Algorithm 4.3.13 move the witness set (W', F', L'_X) for X' to a pseudowitness set $(X' \cap (L' \times M'), F', L', M')$ for $V' = \overline{\pi(X')}$.

Studying $V = \overline{\pi(X)}$ using a pseudowitness set is a numerical version of elimination theory.

Local dimension test. Suppose that x is a point lying on a variety V that is an irreducible component of $\mathcal{V}(F)$ where $F = \{f_1, \dots, f_m\}$ is a system of polynomials on $\mathbb{C}^n$. We would like a numerical method to compute the dimension of V. We discuss one that assumes V is smooth at x. While this does not use a witness set as an input, it has a similar flavor and is needed in subsequent sections.

As explained in Section 3.4, given a point $x \in \mathcal{V}(F)$, the differentials $d_x f_i$ of the polynomials $f_i \in F$ at x define the Zariski tangent space $T_x\mathcal{V}(F)$ of $\mathcal{V}(F)$ at x. Thus $\dim T_x\mathcal{V}(F) = n - \operatorname{rank}(DF(x))$, the corank of the Jacobian matrix of F at x. When x is a smooth point of $\mathcal{V}(F)$, the Zariski tangent space is the ordinary tangent space and its dimension is the dimension of V.

The problem with this calculation is that in practice x is only a numerical approximation to a point of $\mathcal{V}(F)$ and the Jacobian may likely have full rank $\min\{m, n\}$ at x. The notion of numerical rank from numerical analysis suggests a resolution of this problem. We begin with an example.

Example 4.3.14. If we solve the linear equations (4.3.5) on the set of 2×3 rank one matrices, as in Example 4.3.5, there are three solutions. Here is one,

$$M \;=\; \begin{pmatrix} -9.33788 & -7.74194 & -9.30154 \\ 15.0874 & 12.5089 & 15.0288 \end{pmatrix} .$$

This corresponds to the first solution in (4.3.3), substituted into the matrix $M(x, y)$. The Jacobian matrix of the three 2×2 minors (4.3.4) is

$$\begin{pmatrix} M_{2,2} & -M_{2,1} & 0 & -M_{1,2} & M_{1,1} & 0 \\ 0 & M_{2,3} & -M_{2,2} & 0 & -M_{1,3} & M_{1,2} \\ M_{2,3} & 0 & -M_{2,1} & -M_{1,3} & 0 & M_{1,1} \end{pmatrix} ,$$

and evaluating it at the point M gives

$$\begin{pmatrix} 12.5089 & -15.0874 & 0 & 7.74194 & -9.33788 & 0 \\ 0 & 15.0288 & -12.5089 & 0 & 9.30154 & -7.74194 \\ 15.0288 & 0 & -15.0874 & 9.30154 & 0 & -9.33788 \end{pmatrix} . \tag{4.3.7}$$

This has full rank 3, but the 3×3-minors are all at most 0.026 in absolute value, so the Jacobian matrix is nearly singular.

Numerical analysis furnishes a method to estimate the rank of such a matrix, by determining a nearby singular matrix. A *singular value decomposition* of a complex $m \times n$ matrix M is a factorization $M = UDV^*$, where U and V are unitary matrices of sizes $m \times m$ and $n \times n$, respectively, and D is a $m \times n$ matrix whose only nonzero entries are nonnegative real numbers on the diagonal. The diagonal entries of D are the *singular values* of M. The columns of U are orthonormal eigenvectors of MM^*, the columns of V are the orthonormal eigenvectors of M^*M, and the nonzero singular values are the square roots of the nonzero eigenvalues of both M^*M and MM^*. The *numerical rank* of M is the number of singular values that, when divided by the maximum singular value, exceed a pre-determined thershold.

For example, the matrix (4.3.7) has singular values $29.045, 29.045, 8.35 \times 10^{-5}$. As the ratios are $1, 1$, and 2.6×10^{-6} with the third about the working precision, we declare its numerical rank to be 2. The singular values for the Jacobian matrices at the other two solutions are $36.12, 36.12$, and 3.85×10^{-5} and $15.79, 15.79$, and 3.06×10^{-5}, so these likewise have numerical rank 2. Refining the approximate solutions to 12 significant digits does not affect the first two singular values, but the third shrinks to about 10^{-11}, so the ratio is again the working precision.

ALGORITHM 4.3.15 (Local Dimension Test).
INPUT: A point x on an irreducible component V of $\mathcal{V}(F) \subset \mathbb{C}^n$ and a threshold ϵ.
OUTPUT: An estimate for $\dim(V)$.
DO: Compute the singular value decomposition of the Jacobiaan $DF(x)$ of F at x. Let $\sigma_{\max}$ be the maximal singular value and return

$$n \;-\; \#\{\sigma \text{ is a singular value of } DF(x) \text{ with } \sigma > \epsilon\sigma_{\max}\}\,.$$

Explain how this can be used to determine the dimension of an image.
Make an exercise involving 2×4 matrices ?

Exercises.

(1) Verify the claim in Example 4.3.5 that the system of minors and four linear equations has three solutions. Relate this to Example 4.3.1: Show that the matrix $M(x, y)$ of linear polynomials parametrizes the zero locus of the linear equations (4.3.5), and that the three rank one matrices obtained in each example are the same.
(2) Explain why three linearly independent equations on a six-dimensional space define a subvariety either of dimension three or of dimension four.
(3) Verify the claim that in Example 4.3.1 and Example 4.3.5, the variety of rank-one 2×3 matrices was sliced by the same linear subspace.
(4) More exercises

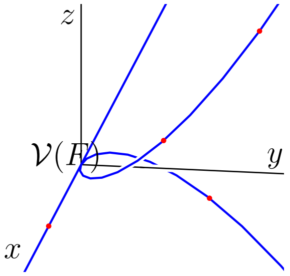
4.4. Numerical Irreducible Decomposition

Section 4.3 introduced witness sets to represent varieties numerically and discussed some algorithms that use witness sets to manipulate varieties. It did not address how to compute a witness set. We offer one method in this section. Here, we explain numerical irreducible decomposition, which begins with a witness set for a (possibly) reducible but equidimensional variety V, decomposing that witness set into witness sets for each irreducible component of V.

Example 4.4.1. Suppose that F is the system of polynomials

$$xy - z \;=\; xz - y^2 \;=\; 0\,,$$

in variables x, y, z for $\mathbb{C}^3$. Substituting the first into the second gives $x^2y - y^2 = 0$ or $y(x^2 - y) = 0$. If $y = 0$ then $z = 0$ and we see that the x-axis $\mathcal{V}(y, z)$ is a subset of $\mathcal{V}(F)$. If $y \neq 0$, then $y = x^2$ so that $z = x^3$, which shows that the moment curve is also a subset of $\mathcal{V}(F)$. In fact, $\langle F\rangle = \langle y, z\rangle \cap \langle x^2 - y, x^3 - z\rangle$, so that $\mathcal{V}(F)$ is the union of these two curves.



Suppose that we were not able to decompose $\mathcal{V}(F)$ by hand, but only had access to a witness set for it. To be specific, as the two polynomials in F are each irreducible, Exercise 8 of Section 3.2 implies that that $\dim(\mathcal{V}(F)) = 1$. If we add the linear equation $x + 2y - 2z = 1$ to F and solve, we obtain the four points

$$(1,0,0)\,,\quad (1,1,1)\,,\ (\tfrac{1}{\sqrt{2}}, \tfrac{1}{2}, \tfrac{1}{2\sqrt{2}})\,,\ (-\tfrac{1}{\sqrt{2}}, \tfrac{1}{2}, -\tfrac{1}{2\sqrt{2}})\,,$$

which constitute a witness set W for $\mathcal{V}(F)$. A numerical irreducible decomposition of $\mathcal{V}(F)$ is the partition of these points

$$\{(1,0,0)\} \;\sqcup\; \{(1,1,1)\,,\ (\tfrac{1}{\sqrt{2}}, \tfrac{1}{2}, \tfrac{1}{2\sqrt{2}})\,,\ (-\tfrac{1}{\sqrt{2}}, \tfrac{1}{2}, -\tfrac{1}{2\sqrt{2}})\}$$

into two parts with each part being a witness set for one component of $\mathcal{V}(F)$.

Suppose that $V \subset \mathbb{C}^n$ is a (possibly) reducible variety, all of whose irreducible components have the same dimension, and that (W, F, L) is a witness set for V. Let $V = V_1 \cup V_2 \cup \cdots \cup V_s$ be the decomposition of V into irreducible components. This induces a partition

$$W \;=\; W_1 \sqcup W_2 \sqcup \cdots \sqcup W_s \tag{4.4.1}$$

of the witness set W with each part the witness set of the corresponding component of W, $W_i = V_i \cap L$. We call this partition (4.4.1) of a witness set W for V a *numerical irreducible decomposition* of V. We will describe methods to compute and verify a numerical irreducible decomposition for V, given a witness set (W, F, L) for V.

Before describing these methods, let us briefly discuss an algorithm to obtain such a witness set. (We will describe more sophisticated methods in the nest section.) Let $F = \{f_1, \ldots, f_m\}$ be a system of polynomials on $\mathbb{C}^n$. The variety $\mathcal{V}(F)$ many have many components of different dimensions, and we would like to obtain a witness set for the union V of its components of a given dimension d. The following algorithm furnishes such a method.

Algorithm 4.4.2.
Input: A system $F = \{f_1, \ldots, f_m\}$ of polynomials on $\mathbb{C}^n$ and a positive intgeger $d < n$.
Output: A witness set for the union V of components of $\mathcal{V}(F)$ of dimension d.
Do:
(1) Select a random subsystem F' of F consisting of $n-d$ polynomials. This uses a variant of Algorithm 4.3.2.
(2) Choose d general linear polynomials, L.
(3) Use the Bézout Homotopy Algorithm 4.2.7 (or any other method) to compute all isolated solutions W' to the square system $\mathcal{V}(F', L)$.
(4) Let $W \subset W'$ be those points of W' that lie on $\mathcal{V}(F)$ and have local dimension d in $\mathcal{V}(F)$. Return (W, F, L).

Proof of correctness. Rewrite this As F' consists of $n - d$ polynomials, the components of $\mathcal{V}(F')$ all havbe dimension d or more. As this is a subsystem of F, $\mathcal{V}(F) \subset \mathcal{V}(F')$, and as it is a random subsystem, with probability one, the components of $\mathcal{V}(F')$ of dimension more than d are components of $\mathcal{V}(F)$ Need a proof of this. Thus every d-dimensional component of $\mathcal{V}(F)$ is a component of $\mathcal{V}(F')$.

The endpoints of the homotopy paths in Step (3) will all be points of $'calV(F') \cap L$, and will include all isolated points. As L is general, it will meet the union of all d-dimensional components of $\mathcal{V}(F')$ transversally in the set of isolated points. Those points that lie in $\mathcal{V}(F)$ anbds for which $\mathcal{V}(F)$ has local dimension d will thus be the points of a witness set $W = V \cap L$ of the union V of the d-dimensional components of $\mathcal{V}(F)$. □

• **Monodromy** Explain how to apply to the example. Find a single loop that permutes the three points.

Lemma Homotopy paths remain on the same irreducible component.

Theorem Monodromy on an irreducible component = full symmetric group.

⟶ The idea is that connectivity of smooth points implies that monodromy is transitive, and the existence of a simple tangent (reduce to plane curves) implies a simple transposition.

Discuss the coarsening algorithm using monodromy, but note that it lacks a stopping criterion when V has two or more components.

• **Trace Test**

Explain the need, apply to the example, and then perhaps to the example from Frank's paper with Anton and Jose.

Prove that trace is linear on a witness set, and it is not linear if the wotness set is incomplete.

Discuss how there is currently no way to certify linearity.

Give the numerical irreducible decomposition algorithm, together with a proof of its correctness.

Perhaps give a meatier example ?

• Witness set of an intersection.

Exercises.

4.5. Smale's α-theory

There are some notes on this from Frank's last Math 648 class
Need to get Smale's book where this is done carefully.
There is a paper improving Smale's threshold for α

Exercises.

4.6. Notes

mention formulas for zeroes of univariate polynomials ? e.g. hypergeometric? Need to mention Davidenko, as well as possible the origins of both Newton and Euler's methods. Do explain that numerical homotopy contiunation originated outside of mathematics.

Cut Material. May need to explain parameter homotopies somewhere

Another source of optimal homotopies are *Parameter homotopies* [**26**],

Parameter homotopies provide a method to solve such a system. We illustrate this with this example. Each polynomial in (4.2.13) has six monomials, and we may identify the space of polynomial systems consisting of two such polynomials (f, g) with $\mathbb{C}^{12}$,

$$\begin{aligned} f &:= f_1 + f_2x + f_3y + f_4xy + f_5x^2y + f_6xy^2\,, \\ g &:= g_1 + g_2x + g_3y + g_4xy + g_5x^2y + g_6xy^2\,. \end{aligned}$$

The total space of the polynomial system $f(x, y) = g(x, y) = 0$

$$U := \{(x, y, f, g) \in \mathbb{C}^{14} \mid f(x, y) = g(x, y) = 0\}$$

has dimension 12, and for a general $(f, g) \in \mathbb{C}^{12}$, there are 5 solutions (x, y) to the equations.

Suppose that we have a system $G := (f^*, g^*)$ in this family whose solutions are known. Given any other system $F = (f, g)$, the straight-line parameter homotopy

$$H(x, t) := tG + (1 - t)F$$

allows us to use the solutions to G to find the isolated solutions to F, as in ????

CHAPTER 5

Real Algebraic Geometry

Outline:

Algebraic geometry for applications includes a treatment of real number aspects, as applications of mathematics typically require real-number answers. These needs really require a full text. Here, we give a treatment of some aspects of real algebraic geometry that are concerned with real solutions to systems of equations. Let this serve as an appetizer for other aspects of real algebraic geometry related to applications.

5.1. Real roots of univariate polynomials.

Classical underpinnings of real algebraic geometry include Descartes' Rule of Signs (1637) and Sturm's Theorem (1829). Each gives different information on the number of real roots of a univariate polynomial $f \in \mathbb{R}[x]$. Both admit strengthenings. For Descartes' Rule, this is the Budan-Fourier Theorem which bounds the number of real roots of f in an interval, counted with multiplicity, and consequently has an algebraic nature. For Sturm's Theorem, this is Sylvester's Theorem, which counts the number of real roots of f in an interval, according to the sign of a second polynomial g at the root. This is more topological in nature and such a signed count is a recurring theme in real algebraic geometry, which we will see again in Section 5.4.

We begin with Descartes' Rule. Let $f \in \mathbb{R}[x]$ be a univariate polynomial. Express f as a sum of terms,

$$f(x) \;=\; c_0x^{a_0} + c_1x^{a_1} + \cdots + c_kx^{a_k}\,,$$

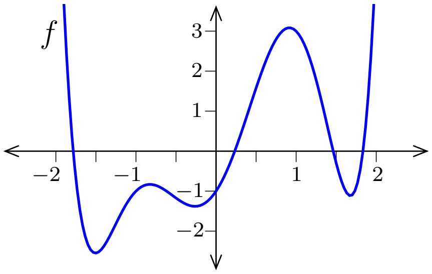
where $a_0 < a_1 < \cdots < a_k$ and each coefficient c_i is nonzero.

THEOREM 5.1.1 (Descartes' Rule of Signs). *The number of positive roots of f, counted with multiplicity, is at most the number of changes in sign of its coefficients,*

$$\#\{i = 1, \ldots, k \mid c_{i-1}c_i < 0\}\,, \tag{5.1.1}$$

and the difference is even.

EXAMPLE 5.1.2. The real roots of the polynomial $f = x^6 - 5x^4 - x^3 + 6x^2 + 3x - 1$ are approximately -1.7834, 0.23346, 1.4629, and 1.8340. Three are positive, and f has three changes in sign among its coefficients.



Note that $f(-x) = x^6 - 5x^4 + x^3 + 6x^2 - 3x - 1$ also has three changes in the sign of its coefficients, but only one positive root (corresponding to the negative root of $f(x)$). ◇

A consequence of Descartes' Rule of Signs and the trick of considering $f(-x)$ to examine negative roots is his bound on the number of real roots of a univariate polynomial.

COROLLARY 5.1.3 (Descartes' Bound). *A real univariate polynomial with $k+1$ terms has at most*

(1) k positive roots,
(2) $2k$ non-zero roots, and
(3) $2k+1$ real roots.

This bound is sharp, as exhibited by $f(x) = x(x^2-1)(x^2-4)\cdots(x^2-k^2)$.

A first step towards Descartes' Rule is to observe that the sum $\rho_+(f)$ of the multiplicities of the positive roots of f has the same parity as $\mathrm{var}(f)$, the number of changes in sign of its coefficients. Indeed, dividing by $c_k x^{a_0}$, we may assume that the leading coefficient of f is positive and $a_0 = 0$. If $c_0 = f(0)$ is also positive, then $\mathrm{var}(f)$ is even. Similarly, as $f(0) > 0$, the graph of f crosses the positive x-axis an even number of times. As $f(x)$ changes sign only at a root of odd multiplicity, $\rho_+(f)$ is also even. The same arguments show that when $c_0 < 0$ both $\mathrm{var}(f)$ and $\rho_+(f)$ are odd.

PROOF OF DESCARTES' RULE. We show this by induction on the degree d of f. When $d = 1$, the result is easy. Suppose that $d > 1$ and consider f'. By Rolle's Theorem between any two real roots of f, there is a root of f'. Also, if f has a root ζ of multiplicity r, then ζ is a root of f' of multiplicity $r-1$. Thus $\rho_+(f) \leq \rho_+(f') + 1$. The rules of differentiation show that $\mathrm{var}(f') \leq \mathrm{var}(f)$. Hence,

$$\rho_+(f) \;\leq\; \rho_+(f') + 1 \;\leq\; \mathrm{var}(f') + 1 \;\leq\; \mathrm{var}(f) + 1\,.$$

As $\rho_+(f)$ and $\mathrm{var}(f)$ have the same parity, the result follows. □

Let us formalize the ingredients in Descartes' Rule. The *variation*, $\mathrm{var}(c)$ of a sequence $c = (c_0, c_1, \ldots, c_k)$ of nonzero real numbers is the quantity (5.1.1) in Descartes' Rule of Signs, the number of changes in sign of its coefficients. For an arbitrary sequence c of real numbers, $\mathrm{var}(c)$ is the variation in the sequence obtained by removing all 0s from c. Thus $\mathrm{var}(3, -1, 0, -2, 1, 0, 0, 3) = \mathrm{var}(3, -1, -2, 1, 3) = 2$.

Given a sequence $F = (f_0, f_1, \ldots, f_k)$ of polynomials and a real number $a \in \mathbb{R}$, let $\mathrm{var}(F(a))$ be the variation in the sequence $(f_0(a), f_1(a), \ldots, f_k(a))$ obtained by evaluating elements of F at a. We extend this to $a \in \{\pm\infty\}$ as follows. Let $F(\infty)$ be the sequence of leading coefficients of the polynomials $f_i(x)$ in F and $F(-\infty)$ the leading coefficients of the polynomials $f_i(-x)$. Then $\mathrm{var}(F(\infty))$ is the variation in the sequence of the leading coefficients of the polynomials $f_i(x)$ and let $\mathrm{var}(F(-\infty))$ is the variation in the leading coefficients of the polynomials $f_i(-x)$. These are equal to $\mathrm{var}(F(a))$ for any number a greater than (respectively less than) any root of any polynomial in F.

Descartes' Rule is a special case of a more refined theorem due to Budan and Fourier. For a univariate polynomial $f(x)$, let δf be the sequence of its derivatives,

$$\delta f \ := \ f\,,\, f'\,,\, f''\,,\, \ldots\,,\, f^{(k)}\,,$$

where k is the degree of f. We will call this the *derivative sequence* of f.

The multiplicity of a root ζ of f is the largest integer m such that $(x-\zeta)^m$ divides f. That is, $(x-\zeta)^m$ divides f but $(x-\zeta)^{m+1}$ does not divide f, which we write as $(x-\zeta)^m \| f$. When $f(\zeta) \neq 0$, the multiplicity of ζ is $m = 0$. For $a < b$ in $\mathbb{R} \cup \{\pm\infty\}$, let $\rho(f, a, b)$ be the number of roots of f in the interval $(a, b]$, counted with multiplicity.

Theorem 5.1.4 (Budan-Fourier). *Let $f \in \mathbb{R}[x]$ be a real univariate polynomial and $a < b$ in $\mathbb{R} \cup \{\pm\infty\}$. Then*

$$\rho(f, a, b) \ \leq \ \mathrm{var}(\delta f(a)) \ - \ \mathrm{var}(\delta f(b))\,,$$

and the difference is even.

Example 5.1.5. Consider the derivative sequence for the polynomial of Example 5.1.2, factors,

$$\begin{aligned}
f &= x^6 - 5x^4 - x^3 + 6x^2 + 3x - 1\,,\\
f' &= 6x^5 - 20x^3 - 3x^2 + 12x + 3\,,\\
f'' &= 30x^4 - 60x^2 - 6x + 12\,,\\
f^{(3)} &= 120x^3 - 120x - 6\,,\\
f^{(4)} &= 360x^2 - 120\,, \qquad f^{(5)} \ = \ 720x\,, \qquad f^{(6)} \ = \ 720\,.
\end{aligned}$$

Its values at 1 are

$$\delta f(1) \ = \ (3, -2, -24, -6, 240, 720, 720)$$

and at -1 are

$$\delta f(-1) \ = \ (-1, 2, -12, -6, 240, -720, 720)\,.$$

Thus $\mathrm{var}(\delta f(-1)) - \mathrm{var}(\delta f(1)) = 5 - 2 = 3$, and f has one real root in $[-1, 1]$. ◇

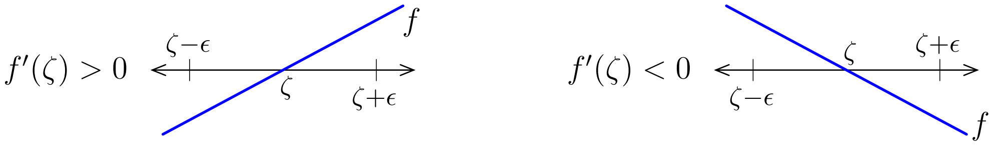
Descartes' Rule follows from Theorem 5.1.4 once we observe that $\mathrm{var}(\delta f(0))$ is the variation in the coefficients of f and $\mathrm{var}(\delta f(\infty))$ is zero, as the leading coefficients of polynomials in δf all have the same sign.

Proof of the Budan-Fourier Theorem. Consider the function $\mathrm{var}(\delta f(t))$ for $t \in \mathbb{R}$. This is constant on intervals containing no root of any derivative of f. We study how $\mathrm{var}(\delta f(t))$ changes when t passes such a root, ζ. Let $\epsilon > 0$ be a number such that ζ is the only root of any derivative of f in the interval $[\zeta-\epsilon, \zeta+\epsilon]$. Let m be the order of vanishing of f at ζ. We will prove that

$$\begin{array}{lrcl} & (1)\quad \mathrm{var}(\delta f(\zeta)) & = & \mathrm{var}(\delta f(\zeta+\epsilon)),\ \text{ and} \\ (5.1.2) & & & \\ & (2)\quad \mathrm{var}(\delta f(\zeta-\epsilon)) & \geq & \mathrm{var}(\delta f(\zeta)) + m, \quad \text{and the difference is even.} \end{array}$$

Assuming (5.1.2), consider how the sum $\mathrm{var}(\delta f(t)) + \rho(f; a, t)$ changes as t ranges from a to b. When t passes a root ζ of f or of one of its derivatives, $\rho(f; a, t)$ jumps by the multiplicity m of that root ζ of f, while $\mathrm{var}(\delta f(t))$ drops by m, and possibly also by a non-negative even integer. Thus the Budan-Fourier Theorem follows from (5.1.2).

We prove (5.1.2) by induction on the degree of f. There are two cases when $\deg(f) = 1$



For each, we have $\mathrm{var}(\delta f(\zeta-\epsilon)) = 1$ and $\mathrm{var}(\delta f(\zeta+\epsilon)) = 0$, which proves the claim (5.1.2) when f has degree 1.

Suppose now that f has degree at least 2 and let m be the multiplicity of a root ζ of f. When $f(\zeta) = 0$, so that $m > 0$, let us apply our induction hypothesis to f':

$$\begin{array}{rcl} (1)\quad \mathrm{var}(\delta f'(\zeta)) & = & \mathrm{var}(\delta f'(\zeta+\epsilon)),\ \text{ and} \\ (2)\quad \mathrm{var}(\delta f'(\zeta-\epsilon)) & \geq & \mathrm{var}(\delta f'(\zeta)) + (m{-}1), \quad \text{and the difference is even.} \end{array}$$

Since $f(\zeta) = 0$, $\mathrm{var}(\delta f(\zeta)) = \mathrm{var}(\delta f'(\zeta))$. By Lagrange's Mean Value Theorem, f and f' have opposite signs on $[\zeta-\epsilon, \zeta)$, but the same sign on $(\zeta, \zeta+\epsilon]$. Thus

$$\begin{array}{rcl} \mathrm{var}(\delta f(\zeta-\epsilon)) & = & \mathrm{var}(\delta f'(\zeta-\epsilon)) + 1\,, \\ \mathrm{var}(\delta f(\zeta)) & = & \mathrm{var}(\delta f'(\zeta))\,,\ \text{and} \\ \mathrm{var}(\delta f(\zeta+\epsilon)) & = & \mathrm{var}(\delta f'(\zeta+\epsilon))\,, \end{array}$$

which proves this case, as

$$\mathrm{var}(\delta f(\zeta-\epsilon)) \;=\; \mathrm{var}(\delta f'(\zeta-\epsilon)) + 1 \;\leq\; \mathrm{var}(\delta f'(\zeta)) + m - 1 + 1 \;=\; \mathrm{var}(\delta f(\zeta)) + m\,,$$

and the difference is even.

We are left with the case when $f(\zeta) \neq 0$ and some other member of δf vanishes at ζ. Let $n \geq 0$ be the order of vanishing of f' at ζ. By our induction hypothesis applied to f', we have

$$\begin{array}{rcl} (1)\quad \mathrm{var}(\delta f'(\zeta)) & = & \mathrm{var}(\delta f'(\zeta+\epsilon)),\ \text{ and} \\ (2)\quad \mathrm{var}(\delta f'(\zeta-\epsilon)) & \geq & \mathrm{var}(\delta f'(\zeta)) + n, \quad \text{and the difference is even.} \end{array}$$

We have $f'(\zeta) = f^{(2)}(\zeta) = \cdots = f^{(n)}(\zeta) = 0$, but $f^{(n+1)}(\zeta) \neq 0$. Multiplying by -1 if necessary, we may assume that $f^{(n+1)}(\zeta) > 0$. Considering the Taylor expansion

$$f'(x) \;=\; \frac{f^{(n+1)}(\zeta)}{n!}(x-\zeta)^n + \frac{f^{(n+2)}(\zeta)}{(n+1)!}(x-\zeta)^{n+1} + \cdots$$

of $f'(x)$ at $x = \zeta$, we see that $f'(x)$ has the same sign as $(x-\zeta)^k$ for $x \in [\zeta-\epsilon, \zeta+\epsilon]$. There are four cases depending upon the parity of n and the sign of $f(\zeta)$.

If n is even then both $f'(\zeta-\epsilon)$ and $f'(\zeta+\epsilon)$ are positive, so that for t one of $\{\zeta-\epsilon, \zeta, \zeta+\epsilon\}$, the first term in the sequence $\text{var}(\delta f(t))$ is positive. If $f(\zeta) > 0$, then $\text{var}(\delta f(t)) = \text{var}(\delta f'(t))$, and if $f(\zeta) < 0$, then $\text{var}(\delta f(t)) = \text{var}(\delta f'(t)) + 1$. In either case, the claim follows as n is even (and is absorbed into the difference).

Now suppose that n is odd. Then

$$f'(\zeta-\epsilon) \;<\; 0 \;=\; f'(\zeta) \;<\; f'(\zeta+\epsilon)\,,$$

and the first non-zero term in $\delta f'(t)$ has sign $-,+,+$, for $t = \zeta-\epsilon, \zeta, \zeta+\epsilon$, respectively. If $f(\zeta) > 0$, then $\text{var}(\delta f(\zeta-\epsilon)) = \text{var}(\delta f'(\zeta-\epsilon)) + 1$ and the variations at ζ and $\zeta+\epsilon$ are the same for δf and $\delta f'$. If $f(\zeta) < 0$, then the variation at $\zeta-\epsilon$ is the same for δf and $\delta f'$, but the variations of δf at ζ and $\zeta+\epsilon$ are one more than those of $\delta f'$.

In either case, $\text{var}(\delta f(\zeta)) = \text{var}(\delta f(\zeta+\epsilon))$ and

$$\text{var}(\delta f(\zeta-\epsilon)) \;-\; \text{var}(\delta f(\zeta)) \;=\; \text{var}(\delta f'(\zeta-\epsilon)) \;-\; \text{var}(\delta f'(\zeta)) \;\pm 1\,. \tag{5.1.3}$$

As $\text{var}(\delta f'(\zeta-\epsilon)) \;-\; \text{var}(\delta f'(\zeta)) = n$ plus a nonnegative even integer and $n \geq 1$ is odd, the difference in (5.1.3) is a nonnegative even integer. □

Remark 5.1.6. Budan's original theorem was formulated as follows: For a univariate polynomial $f \in \mathbb{R}[x]$ and $a \in \mathbb{R}$, let $\text{var}_a f$ be the sign variation among the coefficients of $f(x+a) \in \mathbb{R}[x]$ (that is, expanded as a polynomial in x). Then for real numbers $a < b$,

$$\text{var}_a f \;-\; \text{var}_b f \;\geq\; \rho(f, a, b)\,,$$

and the difference is even. ◇

The Budan-Fourier Theorem may enable the isolation of simple roots.

Corollary 5.1.7. *Suppose that $a < b$ and $f \in \mathbb{R}[x]$.*
If $\text{var}(\delta f(a)) = \text{var}(\delta f(b))$, then f has no roots in $(a, b]$.
If $\text{var}(\delta f(a)) = \text{var}(\delta f(b)) + 1$, then f has exactly one simple root in $(a, b]$

Note that it may not be possible to use Corollary 5.1.7 to isolate a simple root of a polynomial. For example $f = x^3 + x$ has a simple root at $x = 0$. Its derivative sequence is

$$\delta f \;=\; (\,x^3 + x\,,\; 3x^2 + 1\,,\; 6x\,,\; 6\,)\,,$$

and $\delta f(-1) = (-2, 4, -6, 6)$ while $\delta f(1) = (2, 4, 6, 6)$, so that $\text{var}(\delta f(-1)) - \text{var}(\delta f(1)) = 3$, and not 1. In fact, if $a < 0$ and $b > 0$, then $\text{var}(\delta f(a)) - \text{var}(\delta f(b)) = 3$, so that Corollary 5.1.7 cannot be used to isolate the unique simple root of f.

The Budan-Fourier Theorem is algebraic in that it gives a bound for the number of roots of a univariate polynomial counted with multiplicity. Sturm's Theorem is inherently topological in that it just counts roots. It is also a fundamental algorithmic result—it gives a symbolic method to isolate and count the roots of a univariate polynomial $f \in \mathbb{R}[x]$. Like Descartes' Rule, it is now seen as a special case of a more general result.

Let $f, g \in \mathbb{R}[x]$ be real polynomials. Their *Sylvester sequence* $\mathrm{Sy}(f, g)$ is the sequence $f_0, f_1, f_2, \ldots$ of polynomials where $f_0 := f$, $f_1 := g$, and for $i \geq 1$, we have

$$f_{i+1} \ := \ -1 \cdot \mathrm{remainder}(f_{i-1}, f_i)\,,$$

the *negative* remainder in the division of f_{i-1} by f_i, as given by the Division Algorithm A.1.9. That is, there are unique polynomials $q_i(x)$ and $f_{i+1}(x)$ such that

$$f_{i-1}(x) \ = \ q_i(x) f_i(x) \ - \ f_{i+1}(x)\,, \tag{5.1.4}$$

where $\deg f_{i+1}(x) < \deg f_i(x)$. The last nonzero element f_k of this sequence is a greatest common divisor of f, g, $\gcd(f, g)$.

The *Sturm sequence* of a polynomial $f \in \mathbb{R}[x]$ is the Sylvester sequence $\mathrm{Sy}(f, f')$.

THEOREM 5.1.8 (Sturm's Theorem). *Let $f \in \mathbb{R}[x]$ be a real univariate polynomial with Sturm sequence $F := \mathrm{Sy}(f, f')$. For any $a < b$ in $\mathbb{R} \cup \{\pm\infty\}$, $\mathrm{var}(F, a) - \mathrm{var}(F, b)$ is equal to the number of roots of f in the half-open interval $(a, b]$.*

EXAMPLE 5.1.9. The sextic of Example 5.1.2 has Sturm sequence F:

$$\begin{aligned}
f_0 &= x^6 - 5x^4 - x^3 + 6x^2 + 3x - 1\\
f_1 &= 6x^5 - 20x^3 - 3x^2 + 12x + 3\\
f_2 &= 5/3x^4 + 1/2x^3 - 4x^2 - 5/2x + 1\\
f_3 &= 253/50x^3 - 42/25x^2 - 57/10x - 102/25\\
f_4 &= 113475/64009x^2 - 1950/64009x - 118375/64009\\
f_5 &= 77066836/171687675x + 985802609/171687675\\
f_6 &= -26779786317275/92788470544\,.
\end{aligned}$$

We have

$$F(-1) \ = \ (-1\,,\ 2\,,\ \tfrac{2}{3}\,,\ -\tfrac{128}{25}\,,\ -\tfrac{2950}{64009}\,,\ \tfrac{908735773}{171687675}\,,\ -\tfrac{26779786317275}{92788470544})\,.$$

and

$$F(1) \ = \ (3\,,\ -2\,,\ -\tfrac{10}{3}\,,\ -\tfrac{32}{5}\,,\ -\tfrac{6850}{64009}\,,\ \tfrac{70857963}{11445845}\,,\ -\tfrac{26779786317275}{92788470544})\,.$$

and thus $\mathrm{var}(F(-1)) = \mathrm{var}(F(1)) = 4 - 3 = 1$, which agrees with f having a single root 0.23346 in $(-1, 1]$. ◇

The *reduced Sylvester sequence* of polynomials $f, g \in \mathbb{R}[x]$ is obtained by dividing each term of their Sylvester sequence $\mathrm{Sy}(f, g)$ by its last nonzero term, $f_k = \gcd(f, g)$. If $g_0, g_1, \ldots, g_k$ is the reduced Sylvester sequence, then $g_k = 1$ and (5.1.4) holds with f_j replaced by g_j. In fact, $(g_0, g_1, \ldots, g_{k-1}, 1) = \mathrm{Syl}(g_0, g_1)$.

THEOREM 5.1.10 (Sylvester's Theorem). *Let $f, g \in \mathbb{R}[x]$ and suppose that G is the reduced Sylvester sequence of f and $f'g$. For $a < b$ in $\mathbb{R} \cup \{\pm\infty\}$ we have,*

$$\begin{aligned}
\mathrm{var}(G, a) - \mathrm{var}(G, b) \ &= \ \#\{\zeta \in (a, b] \mid f(\zeta) = 0 \textit{ and } g(\zeta) > 0\}\\
&\qquad - \ \#\{\zeta \in [a, b) \mid f(\zeta) = 0 \textit{ and } g(\zeta) < 0\}\,.
\end{aligned}$$

The expression on the right is a mildly subtle (note the role of the endpoints) signed sum of the roots of f in the interval $[a, b]$ with signs given by the sign of g at the corresponding root of f.

Example 5.1.11. Consider the (reduced) Sylvester sequence $G = \mathrm{Syl}(f, xf')$, where f is the sextic of Example 5.1.2:

$$\begin{array}{rcl}
g_0 &=& x^6 - 5x^4 - x^3 + 6x^2 + 3x - 1 \\
g_1 &=& 6x^6 - 20x^4 - 3x^3 + 12x^2 + 3x \\
g_2 &=& 5/3x^4 + 1/2x^3 - 4x^2 - 5/2x + 1 \\
g_3 &=& -1599/500x^3 + 1611/250x^2 + 351/100x - 759/250 \\
g_4 &=& -1592000/284089x^2 - 10000/65559x + 756500/284089 \\
g_5 &=& -107669731/59401500x - 85510789/1267232000 \\
g_6 &=& -6949069627125/2611636995136
\end{array}$$

We have that

$$G(\infty) \;=\; (1\,,\ 6\,,\ \tfrac{5}{3}\,,\ -\tfrac{1599}{500}\,,\ -\tfrac{1592000}{284089}\,,\ -\tfrac{107669731}{59401500}\,,\ -\tfrac{6949069627125}{2611636995136})$$

and

$$G(-\infty) \;=\; (1\,,\ 6\,,\ \tfrac{5}{3}\,,\ \tfrac{1599}{500}\,,\ -\tfrac{1592000}{284089}\,,\ \tfrac{107669731}{59401500}\,,\ -\tfrac{6949069627125}{2611636995136})\,.$$

Thus $\mathrm{var}(G(-\infty)) - \mathrm{var}(G(\infty)) = 3 - 1 = 2$, which agrees with f having three positive roots and one negative root. ◇

The coefficient growth in a Sylvester sequence may be significant. For rational polynomials $f \in \mathbb{Q}[x]$, replacing each polynomial $f_{i+1}(x)$ obtained in (5.1.4) by its primitive part (clearing positive denominators and dividing by positive common factors of its coefficients) will give smaller coefficients. For example, here is the resulting *primitive Sylvester sequence* for f, f' from Example 5.1.9.

$$\begin{array}{rcl}
f_0 &=& x^6 - 5x^4 - x^3 + 6x^2 + 3x - 1 \\
f_1 &=& 6x^5 - 20x^3 - 3x^2 + 12x + 3 \\
f_2 &=& 10x^4 + 3x^3 - 24x^2 - 15x + 6 \\
f_3 &=& 253x^3 - 84x^2 - 285x - 204 \\
f_4 &=& 14539x^2 - 78x - 4735 \\
f_5 &=& 1204x + 15401 \\
f_6 &=& -1\,.
\end{array}$$

Proof. Let $f, g \in \mathbb{R}[x]$ and suppose that $G = (g_0, g_1, \ldots, g_{k-1}, 1)$ is the reduced Sylvester sequence of f and $f'g$. That is, if $(f_0, f_1, \ldots, f_k) = \mathrm{Sy}(f, f'g)$ is the Sylvester sequence ($f_0 = f$, $f_1 = f'g$, and $f_k = \gcd(f, f'g)$), then $g_i := f_i/f_k$ for $i = 0, \ldots, k$. We consider the variation $\mathrm{var}(G, t)$ as t increases from a to b. This can only change when t passes a root $\zeta \in (a, b)$ of some polynomial g_i in G, or possibly when that root ζ is an endpoint of $[a, b]$.

Observe first that ζ cannot be a root of two consecutive elements of G. If it were, then by (5.1.4) and an induction, it is a root of all elements of G, and thus of $g_k = 1$, which is a contradiction. Suppose that $g_i(\zeta) = 0$ for some $i \geq 1$. By (5.1.4) again, $g_{i-1}(\zeta)$ and $g_{i+1}(\zeta)$ have opposite signs in a neighborhood of ζ and thus g_{i-1}, g_i, g_{i+1} do not contribute to any change in $\mathrm{var}(G, t)$ for t in a neighborhood of ζ. This in particular remains true if $\zeta = a$ and t increases from a or if $\zeta = b$ and t approaches b.

We are left with the case that $g_0(\zeta) = 0$ (and $g_1(\zeta) \neq 0$). This implies that $f(\zeta) = 0$ but $g(\zeta) \neq 0$, and is in fact equivalent to these two conditions. Indeed, suppose that $f(\zeta) = 0$. Then there exist $m > 0$ and $n \geq 0$ such that $(x-\zeta)^m || f$ and $(x-\zeta)^n || g$. Then $(x-\zeta)^{m-1} || f'$. If $n > 0$ so that $g(\zeta) = 0$, then $(x-\zeta)^m$ divides $f'g$, which implies that $(x-\zeta)^m$ divides f_k. Dividing $\mathrm{Syl}(f, f'g)$ by $(x-\zeta)^m$ gives $h_0, \ldots, h_k$ with $h_0(\zeta), h_k(\zeta) \neq 0$, and thus $g_0(\zeta) = h_0(\zeta)/h_k(\zeta) \neq 0$.

Thus when $g_0(\zeta) = 0$, there is an integer $m > 0$ with $(x-\zeta)^m || f$ and $(x-\zeta)^{m-1} || f'g$, so that $(x-\zeta)^{m-1} || f_k$. Then $f_k/(x-\zeta)^{m-1}$ is nonzero in a neighborhood of ζ. Since multiplying a sequence by a nonzero number does not change its variation, we multiply the reduced Sylvester sequence G by $f_k/(x-\zeta)^{m-1}$ and study the change in variation of this new sequence H near ζ. This sequence $H = (h_0, h_1, \ldots, h_k)$ is obtained by dividing each element in the Sylvester sequence $\mathrm{Sy}(f, f'g)$ by $(x-\zeta)^{m-1}$.

We have that $f = (x-\zeta)^m \cdot h$ with $h(\zeta) \neq 0$ and $g(\zeta) \neq 0$. Then $h_0(x) = (x-\zeta)h(x)$ and h_1 is

$$\begin{aligned} \frac{f'g}{(x-\zeta)^{m-1}} &= \frac{1}{(x-\zeta)^{m-1}} \left(m(x-\zeta)^{m-1}h(x) + (x-\zeta)^m h'(x) \right) g(x) \\ &= mh(x)g(x) + (x-\zeta)h'(x)g(x)\,. \end{aligned}$$

Let $\epsilon > 0$ be a real number such that ζ is the only root of any element in H lying in the interval $[\zeta{-}\epsilon, \zeta{+}\epsilon]$. We evaluate the first two terms of H at ζ and the endpoints $\zeta_\pm$ of this interval.

x	$h_0(x)$	$h_1(x)$
$\zeta{-}\epsilon$	$-\epsilon h(\zeta{-}\epsilon)$	$mh(\zeta{-}\epsilon)g(\zeta{-}\epsilon) - \epsilon h'(\zeta{-}\epsilon)g(\zeta{-}\epsilon)$
ζ	0	$mh(\zeta)g(\zeta)$
ζ_+	$\epsilon h(\zeta{+}\epsilon)$	$mh(\zeta{+}\epsilon)g(\zeta{+}\epsilon)) + \epsilon h'(\zeta{+}\epsilon)g(\zeta{+}\epsilon)$

Suppose that $g(\zeta) > 0$. Then the sign of h_1 on $[\zeta{-}\epsilon, \zeta{+}\epsilon]$ is opposite to the sign of $h_0(\zeta{-}\epsilon)$, but the same as the sign of $h_0(\zeta{+}\epsilon)$. We conclude that $\mathrm{var}(H, t)(= \mathrm{var}(G, t))$ decreases by 1 as t passes from $\zeta{-}\epsilon$ to ζ, but is unchanged as t passes from ζ to $\zeta{+}\epsilon$,

$$\mathrm{var}(G, \zeta{-}\epsilon) - 1 \;=\; \mathrm{var}(G, \zeta) \;=\; \mathrm{var}(G, \zeta{+}\epsilon)\,.$$

Suppose that $g(\zeta) < 0$. Then the sign of h_1 on $[\zeta{-}\epsilon, \zeta{+}\epsilon]$ is the same as the sign of $h_0(\zeta - \epsilon)$, but opposite to the sign of $h_0(\zeta{+}\epsilon)$. We conclude that $\mathrm{var}(H, t)(= \mathrm{var}(G, t))$ is unchanged as t passes from $\zeta{-}\epsilon$ to ζ, but increases by 1 as t passes from ζ to $\zeta{+}\epsilon$,

$$\mathrm{var}(G, \zeta{-}\epsilon) \;=\; \mathrm{var}(G, \zeta) \;=\; \mathrm{var}(G, \zeta{+}\epsilon) - 1\,.$$

Now consider the variation $\mathrm{var}(G, t)$ for $t \in [a, b]$. This may only change at a number $\zeta \in [a, b]$ if $f(\zeta) = 0$. If $g(\zeta) > 0$ and $\zeta \neq b$, then it decreases by 1. If $g(\zeta) < 0$ and $\zeta \neq a$, then it increases by 1. It is unchanged in all other cases. This completes the proof of the Theorem. □

Discuss counting with multiplicity

What else here?

Mention the algorithm for counting real solutions in section on Stickelberger.

Exercises for Section 5.1.

1. Deduce Descartes's Bound from his Rule of Signs, and verify its sharpness for the $f(x) = x(x^2-1)(x^2-4)\cdots(x^2-k^2)$.
2. Deduce from the Budan-Fourier Theorem 5.1.4 Budan's formulation described in Remark 5.1.6.
3. Verify the assertion made just before Sylvester's Theorem about a reduced Sylvester sequence being a Sylvester sequence.

5.2. Stable univariate polynomials.

There is a long-standing classical interest in the location of the roots of a univariate polynomial, much more than simply studying real roots. Some of the results we discuss are Hermite stability and the Gauß-Lucas Theorem on the roots of a polynomial and its derivatives, as well as the useful Hermite-Biehler Theorem characterizing stability. Our goal is the Routh-Hurwitz Problem and Hurwitz-stability, results motivated by the stability of systems of ordinary differential equations.

Let us write $\mathcal{H} := \{z \in \mathbb{C} \mid \Im(z) > 0\}$ for the upper half-plane in $\mathbb{C}$. A polynomial $f \in \mathbb{C}[x]$ is *stable* if it has no roots in $\mathcal{H}$. It is *strictly stable* if it is stable and has no real roots, as well. If a polynomial $f \in \mathbb{R}[x]$ is stable, then it has only real roots. Such a polynomial is also called *hyperbolic*. For example, the characteristic polynomial of a symmetric matrix is hyperbolic.

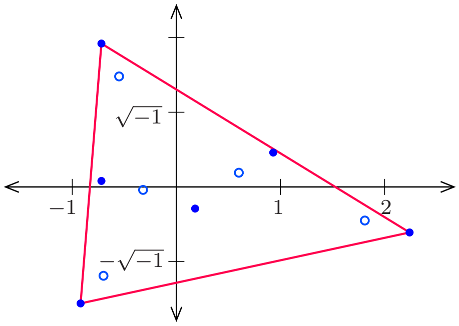
Recall that Rolle's Theorem asserts that between any two roots of a real univariate polynomial there is a root of its derivative. This is significantly extended by the Gauß-Lucas Theorem, a famous result on locating the roots of polynomials.

Theorem 5.2.1 (Gauß-Lucas). *Let $f \in \mathbb{C}[x]$ be a complex univariate polynomial. Then the roots of f' lie within the convex hull of the roots of f.*

Example 5.2.2. Suppose that

$$f(x) \;=\; x^6 - x^5 + \sqrt{-1}x^4 + (-7+3\sqrt{-1})x^3 + 4x^2 + 5x - 1 + 2\sqrt{-1}\,.$$

Then $f'(x) = 6x^5 - 5x^4 + 4\sqrt{-1}x^3 + (-21+9\sqrt{-1})x^2 + 8x + 5$. We plot the roots of f (dots) and f' (circles) in the complex plane below



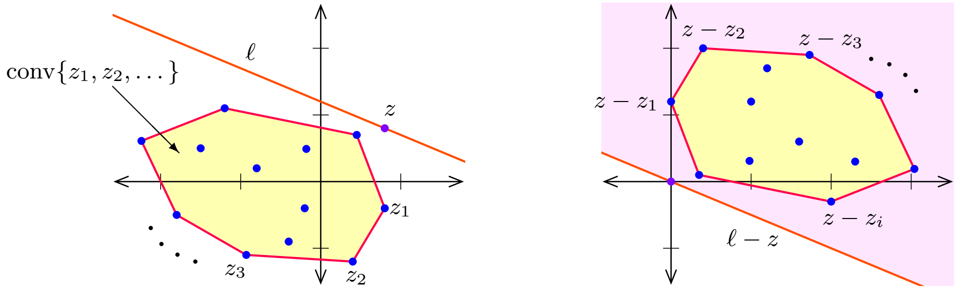
◇

Proof. Suppose that $z_1, \dots, z_n$ are the roots of f, where we repeat multiple roots. Writing $f = \alpha\prod_{i=1}^{n}(x - z_i)$, we have that

$$\frac{f'}{f} \;=\; \frac{1}{x - z_1} \;+\; \cdots \;+\; \frac{1}{x - z_n}\,. \tag{5.2.1}$$

Suppose that z does not lie in the convex hull of $\{z_1, \dots, z_n\}$. Then $f(z) \neq 0$ and by the separating property of convex sets (see Section A.3 in the Appendix), there is a line $\ell \subset \mathbb{C}$ containing z and disjoint from the convex hull of $\{z_1, \dots, z_n\}$. Consequently, the differences $z - z_1, \dots, z - z_n$ lie in a common half-plane with boundary the line $\ell - z$

through the origin.



For a non-zero complex number w, we have that $\frac{1}{w} = \frac{\overline{w}}{|w|^2}$. Consequently, all of $\frac{1}{z-z_1}, \dots, \frac{1}{z-z_n}$ lie in a common open half-plane bounded by $\overline{\ell - z}$. By the expression (5.2.1) and the convexity of half-spaces, we conclude that $f'(z)/f(z)$ lies in the same half-plane, and is thus non-zero. □

By the classical Rolle's Theorem, the derivative of a hyperbolic polynomial is hyperbolic. As both the upper-half plane $\mathcal{H}$ and its complement are convex, we deduce the following generalization of this fact to stable polynomials.

Corollary 5.2.3. *The derivative of a stable polynomial is stable.*

As the derivative is a linear map on the vector space of polynomials, Corollary 5.2.3 is an example of a linear map on polynomials that preserves the polynomial not vanishing on a subset of $\mathbb{C}$.

Given a univariate polynomial $h \in \mathbb{C}[x]$, there are real polynomials $f, g \in \mathbb{R}[x]$ such that $h = g + \sqrt{-1} \cdot f$. The Hermite-Biehler Theorem characterizes the stability of h in terms of the roots of f and g.

Suppose that f and g are hyperbolic (real stable) univariate polynomials. Write the roots of f as $z_1 \le z_2 \le \cdots \le z_n$ and those of g as $y_1 \le y_2 \le \cdots \le y_m$. These roots are *interlaced* if either

$$z_1 \le y_1 \le z_2 \le y_2 \le z_3 \le \cdots \qquad \text{or} \qquad y_1 \le z_1 \le y_2 \le z_2 \le y_3 \le \cdots$$

Necessarily we must have that $|m - n| \le 1$ for this to occur. We will say that the roots *strictly interlace* if all inequalities are strict. Note that this implies that the product fg has only simple roots.

For now, and for many of our proofs, we assume that the polynomials f and g have only simple roots. We later[1] provide a limiting argument which shows this assumption will imply the general case of multiple roots. Do it here

Suppose now that g is a real stable polynomial with distinct roots $b_1 < \cdots < b_\ell$. Let us define

$$\widehat{g}_j \;:=\; \frac{g}{x - b_j} \qquad \text{for } 1 \le j \le \ell, .$$

The reader will recognize these polynomials $\hat{g}_j$ as (unnormalized) Lagrange polynomials for interpolating polynomials with specified values at the roots of g. In particular, $\hat{g}_j(b_i) \neq 0$ if and only if $i = j$. They are linearly independent.

[1] Do not neglect to do this, properly.

Lemma 5.2.4. *The polynomials $\hat{g}_1, \dots, \hat{g}_\ell$, and g form a basis for the space of polynomials of degree at most ℓ.*

Proof. We show that the polynomials $\hat{g}_1, \dots, \hat{g}_\ell, g$ are linearly independent. As they are $\ell + 1$ polynomials of degree at most ℓ the result follows. Consider a general linear combination of the polynomials

$$f \;=\; \alpha g \;+\; \sum_{j=1}^{\ell} \beta_j \hat{g}_j \;. \tag{5.2.2}$$

Observe that for each $1 \leq j \leq \ell$, $f(b_j) = \beta_j \hat{g}_j(b_j)$ and if $g(b) \neq 0$, then

$$\alpha \;=\; \frac{1}{g(b)} \Bigl(f(b) - \sum_{j=1}^{\ell} \beta_j \hat{g}_j(b) \Bigr) \,.$$

In particular, if f is the zero polynomial, then $\beta_j = 0$ for all $1 \leq j \leq \ell$ and also $\alpha = 0$. □

We will often write a polynomial f of degree at most that of g in the normal form (5.2.2). The signs of the coefficients in this expression are related to the interlacing of the roots of f and g.

Lemma 5.2.5. *Suppose that f and g are nonzero real stable polynomials with* $\deg f \leq \deg g$, *and let us assume that fg has only simple roots. The following are equivalent.*

(1) The roots of f and g are strictly interlaced.
(2) In the representation (5.2.2), *the coefficients $\beta_1, \dots, \beta_\ell$ are nonzero and have the same sign.*

We should modify this statement to weakly interlace....

Proof. For the forward direction, note that as the roots of f and g are simple and strictly interlace, the sequence $f(b_1), \dots, f(b_\ell)$ of nonzero numbers alternates in sign (this is Exercise 1). Similarly, the sequence of nonzero numbers

$$\hat{g}_j(b_j) \;=\; c \cdot (b_j - b_1) \cdots (b_j - b_{j-1}) \widehat{(b_j - b_j)} (b_j - b_{j+1}) \cdots (b_j - b_\ell)$$

alternates in sign (here, c is the leading coefficient of c). As $f(b_j) = \beta_j \hat{g}_j(b_j)$, we see that the coefficients $\beta_1, \dots, \beta_\ell$ are nonzero and have the same sign.

For the reverse direction, reverse the arguments in the previous paragraph. □

The Wronskian of univariate polynomials f and g is $W_{f,g} := f'g - g'f$. Our next lemma relates interlacing of roots to the (non-)vanishing of the Wronskian.

Lemma 5.2.6. *Real stable polynomials $f, g \in \mathbb{R}[x]$ have interlaced roots if and only if their Wronskian $W_{f,g}$ is either nonnegative on $\mathbb{R}$ or nonpositive on $\mathbb{R}$.*

Proof. Suppose that the roots of fg are simple[2]. Without loss of generality, we may assume that $\deg f \leq \deg g$ and use the representation (5.2.2). Then

$$W_{f,g} \;=\; f'g - g'f \;=\; g^2 \frac{d}{dx}\frac{f}{g} \;=\; g^2 \sum_{j=1}^{\ell} -\frac{\beta_j}{(x-b_j)^2}\,. \tag{5.2.3}$$

By Lemma 5.2.5, the roots of f and g interlace if and only if the coefficients $\beta_1, \ldots, \beta_\ell$ are nonzero and have the same sign. Assuming that $\beta_1, \ldots, \beta_\ell$ are nonzero and have the same sign, the expression (5.2.3) for $W_{f,g}$ shows that its sign is the sign of $-\beta_j$ (any j). For the reverse direction, note that $W_{f,g}(b_j) = -\beta_j$. □

We formalize this last condition. Two real univariate polynomials f and g are in *proper position*, written $f \ll g$, if they are real stable, if $\deg f \leq \deg g$, and if $W_{f,g}$ is nonpositive on $\mathbb{R}$. Note that $f \ll g$ implies that the coefficients β_j in the representation (5.2.2) are nonnegative. With these preliminaries, we may state the first main theorem of this subsection, characterizing stable polynomials.

Theorem 5.2.7 (Hermite-Biehler). *Let f, g be nonconstant real polynomials. Then $g + \sqrt{-1} \cdot f$ is stable if and only if $f \ll g$.*

Proof. Let us suppose that fg has only simple roots. The general case follows by a limiting argument.

Suppose that f and g are real stable and that $f \ll g$. Let $z \in \mathcal{H}$ lie in the upper half plane and fix $\tau \in \mathbb{R}$. As $z - \tau \in H$ and $\frac{1}{w} = \frac{\overline{w}}{|w|^2}$, we see that $1/(z-\tau)$ has negative imginary part. Using the representation (5.2.2), we have

$$\frac{f(z)}{g(z)} \;=\; \alpha \;+\; \sum_{j=1}^{\ell} \frac{\beta_j}{z - b_j}\,, \tag{5.2.4}$$

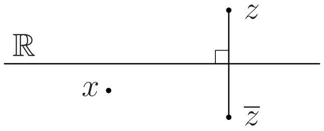
where $b_1, \ldots, b_\ell$ are the roots of g, $\alpha, \beta_j \in \mathbb{R}$, and as $f \ll g$ each $\beta_j > 0$. This expression and the observations that preceeded it imply that the quotient (5.2.4) has negative imaginary part.

Now suppose that x is a root of the polynomial $h = g + \sqrt{-1} \cdot f$. Then

$$0 \;=\; g(x) + \sqrt{-1} \cdot f(x) \quad \text{which implies that} \quad \sqrt{-1} \;=\; \frac{f(x)}{g(x)}\,.$$

This implies that $x \notin \mathcal{H}$ and we conclude that $g + \sqrt{-1} \cdot f$ is stable.

For the other direction, suppose that $h = g + \sqrt{-1} \cdot f$ is stable, so that if $h(x) = 0$, then the imaginary part of x is negative. Let $z \in \mathcal{H}$, and observe that the real axis is the perpendicular bisector of the line between z and its complex conjugate $\overline{z}$.



[2] need the limiting argument

Consequently, $|z-x| > |\overline{z}-x|$.

Let us write $h(z) = c \cdot \prod_i (z-x_i)$ as a product of linear factors with $\{x_i\}$ the roots of h. As these roots all have negative imaginary part, the inequality $|z-x| > |\overline{z}-x|$ implies that $|h(z)| > |h(\overline{z})|$ when $z \in \mathcal{H}$ lies in the upper half plane. Squaring and subtracting gives $0 < |h(z)|^2 - |h(\overline{z})|^2$. Expand this to obtain

$$\begin{aligned} 0 &< h(z)\overline{h(z)} - h(\overline{z})\overline{h(\overline{z})} \\ &= (g(z)+\sqrt{-1}\,f(z))(g(\overline{z})-\sqrt{-1}\,f(\overline{z})) \qquad (5.2.5) \\ &\qquad - \ (g(\overline{z})+\sqrt{-1}\,f(\overline{z}))(g(z)-\sqrt{-1}\,f(z)) \\ &= 2\sqrt{-1}\big(g(\overline{z})f(z) \ - \ g(z)f(\overline{z})\big)\ . \qquad (5.2.6) \end{aligned}$$

As f and g are real polynomials, their non-real roots occur in complex conjugate pairs. The last line (5.2.6) shows that neither f nor g has a non-real root. Consequently, both f and g are hyperbolic.

To complete the proof, let $z \in \mathcal{H}$, so that its imaginary part $\Im(z)$ is positive. As $z - \overline{z} = 2\sqrt{-1}\,\Im(z)$, we have that $2\sqrt{-1}(z-\overline{z}) < 0$. Using (5.2.6), we have that

$$\begin{aligned} 0 &> \frac{2\sqrt{-1}}{2\sqrt{-1}(z-\overline{z})}\Big(g(\overline{z})f(z) \ - \ g(z)f(\overline{z})\Big) \\ &= \frac{f(z)-f(\overline{z})}{z-\overline{z}}g(\overline{z}) \ - \ \frac{g(z)-g(\overline{z})}{z-\overline{z}}f(\overline{z})\,. \end{aligned}$$

Fix $x \in \mathbb{R}$ and consider the limit of this expression as $z \to x$. As you will show in Exercise 2, the difference quotients become derivatives at x, so that

$$W_{f,g}(x) \ = \ f'(x)g(x) - f(x)g'(x) \leq 0\,.$$

By Lemma 5.2.6, f and g have interlaced roots, so that $f \ll g$. □

Example?

The Routh-Hurwitz problem asks for an algorithm to decide if a univariate polynomial has all of its roots z satisfying $\Re(z) < 0$, this is, it lies in the left half plane. This is similar to stable polynomials, but the roots are constrained to a different half plane in $\mathbb{C}$. The motivation for this problem goes back to Euler, who studied linear ordinary differential equations,

$$y^{(n)} \ + \ a_1 y^{(n-1)} \ + \ \cdots \ + \ a_{n-1}y' \ + \ a_n y \ = \ 0\,. \qquad (5.2.7)$$

Assuming that the companion polynomial $x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ has distinct roots $\lambda_1, \dots, \lambda_n$, then the solutions to (5.2.7) have the form $y(t) = \sum_i c_i e^{\lambda_i t}$. We see that all solutions to (5.2.7) converge to zero if and only if $\Re(\lambda_i) < 0$ for all i. In Exercise 3, you are asked to show that this conclusion still holds when the companion polynomial has multiple roots.

Can you relate this to stability of dynamical systems.

Inspired by this, we define a real polynomial f to be *Hurwitz-stable* if all of its roots have negative real part. We note a simple consequence of Hurwitz-stability.

PROPOSITION 5.2.8 (Stodola's Criterion). *All coefficients of a Hurwitz stable polynomial have the same sign.*

Note that if the coefficients of a polynomial all have the same sign, then by Descartes' rule it has no positive roots. Stodola's Criterion is a partial converse to Descartes' rule.

PROOF. Without any loss, we assume that f is a monic Hurwirtz stable polynomial. Write $a_1, \dots, a_r$ for the real roots of f and $b_j \pm \sqrt{-1}c_j$ for $j = 1, \dots, s$ the non-real roots of f. Thus

$$f(x) \;=\; \prod_{i=1}^{r}(x - a_i) \;\cdot\; \prod_{j=1}^{s}\left((x - b_j)^2 + c_j^2\right) \;.$$

As each a_i and b_j are negative, all coefficients of f are positive. □

In Exercise 4 you are asked to show that a polynomial $f \in \mathbb{R}[x]$ is Hurwitz stable if and only if and only if $f(x/\sqrt{-1}) = f(-\sqrt{-1} \cdot x)$ is stable. To exploit this observation, we introduce some notation.

Given $f \in \mathbb{R}[x]$, let us write $(\sqrt{-1})^n \cdot f(x/\sqrt{-1}) = f_0(x) + \sqrt{-1}f_1(x)$, where f_0, f_1 are real polynomials. Suppose that $f(x) = \sum_{j=0}^{n} a_{n-j}x^j$ then

$$\begin{aligned}(\sqrt{-1})^n \cdot f(x/\sqrt{-1}) \;&=\; \sum_{j=0}^{n} a_{n-j}(\sqrt{-1})^{n-j}x^j\\ &=\; a_0x^n \qquad\qquad - \;\; a_2x^{n-2} \qquad\qquad\qquad + \;\cdots\\ &\qquad + \;\sqrt{-1}a_1x^{n-1} \qquad\qquad - \;\sqrt{-1}a_3x^{n-3} \;\; + \;\cdots\end{aligned} \tag{5.2.8}$$

Thus f_0 consists of the terms of f whose power of x has the same parity as the degree of f, but with alteration in sign, and f_1 are those terms with the opposite parity and again with alteration in sign.

We note that if $f \in \mathbb{R}[x]$ has degree n and is Hurwitz stable, then $\deg f_0 = n$ and $\deg f_1 = n - 1$ as $a_1/a_0 = -\sum \text{roots of } f \;> 0$. In particular, the leding coefficients of f, f_0, and f_1 all have the same sign.

LEMMA 5.2.9. *Let $f \in \mathbb{R}[x]$ have degree $n \geq 2$. Then the following are equivalent.*

(1) f is Hurwitz stable.
(2) $(\sqrt{-1})^n \cdot f(x/\sqrt{-1}) = f_0 + \sqrt{-1} \cdot f_1(x)$ is strictly stable.
(3) Let $f_2 \in \mathbb{R}[x]$ be the negative remainder in the Eucliden Algorithm,

$$f_0 \;=\; qf_1 \;-\; f_2\,. \tag{5.2.9}$$

Then $\deg f_2 = n-2$, the leading coefficients of f_0 and f_2 have the same sign, and $f_1 + \sqrt{-1} \cdot f_2$ is stable.

PROOF. The equivalence of the first two points is Exercise 4. Let us consider the implication (2) ⇒ (3). Assume without any loss of generality that the leading coefficient of f (and thus also of f_0) is positive. By the Hermite-Biehler Theorem, the polynomials f_0 and f_1 are hyperbolic with strictly interlaced roots.

We claim that f_1 and f_2 have strictly interlaced roots. To see this, let $b_1 < \dots, b_{n-1}$ be the roots of f_1. As the roots of f_0 interlace those of f_1, the sequence $f_0(b_1), \dots, f_0(b_{n-1})$

alternate in sign, by Exercise 1. As f_0 has a root greater than b_{n-1} and its leading coefficient is positive—so that $\lim_{x\to\infty} f_0(x) = \infty$, we conclude that $f_0(b_{n-1}) < 0$.

Let us evaluate the identity (5.2.9) at a root b_i of f_1,

$$f_0(b_i) \;=\; q(b_i)f_1(b_i) \;-\; f_2(b_i) \;=\; -f_2(b_i)\,.$$

Thus $f_1(b_1), \dots, f_2(b_{n-1})$ alternates in sign with $f_2(b_{n-1}) > 0$. By the Intermediate Value Theorem, this implies that f_2 has at least $n-2$ real roots (between each consecutive root b_i and b_{i+1} of f_1). Since $\deg f_2 \leq n-2$ (it is a remainder in the Euclidean Algorithm), we conclude that $\deg f_2 = n-2$, that it is real-rooted with positive leading coefficient, and finally that roots of f_1 and f_2 strictly interlace. This completes the proof of the claim.

Let us evaluate the Wronskian of f_2, f_1 at the last root b_{n-1} of f_1,

$$W_{f_2,f_1}(b_{n-1}) \;=\; f_2'(b_{n-1})f_1(b_{n-1}) \;-\; f_2(b_{n-1})f_1'(b_{n-1}) \;=\; f_2(b_{n-1})f_1'(b_{n-1})\,.$$

As a_0 and a_1 have the same sign and $a_0 > 0$, we have that $a_1 > 0$. This is the leading coefficient of f_1, so we conclude that $f_1'(b_{n-1}) > 0$, as f_1 is hyperbolic and b_{n-1} is the last root of f_1. This implies that $W_{f_2,f_1}(b_{n-1}) < 0$, so that the Wronskian is negative. By the Hermite-Biehler Theorem, $f_1 + \sqrt{-1}\cdot f_2$ is strictly stable.

These arguments are reversable. Reversing them establishes (3) ⇒ (2) and completes the proof. □

Example 5.2.10. Suppose that $f = 2x^3 + 10x^2 + 16x + 12$, whose roots are -3 and $-1 \pm \sqrt{-1}$, so that f is Hurwitz stable. Following (5.2.8), we have that $f_0 = 2x^3 - 16x$ and $f_1 = 10x^2 - 12$. We write

$$f_0(x) \;=\; \frac{x}{5}f_1(x) \;-\; \frac{68}{5}x\,,$$

so that $f_2 = \frac{68}{5}x$. Then

$$f_2(x) + \sqrt{-1}f_2(x) \;=\; 10x^2 + \sqrt{-1}\frac{68}{5}x - 12\,.$$

Using the quadratic formula, we determine its roots to be

$$-\sqrt{-1}\frac{68}{100} \;\pm\; \frac{1}{20}\Big(-\frac{68^2}{25} \;+\; 4\cdot 120\Big)^{1/2}\,.$$

Since $\frac{68^2}{25} < 480$, the second term is real, so that the roots have negative imaginary part. We conclude that $f_2(x) + \sqrt{-1}f_2(x)$ is stable. ⋄

Lemma 5.2.9 gives the following symbolic algorithm for Hurwitz stability.

Algorithm 5.2.11.
Input: A polynomial $f \in \mathbb{R}[x]$.
Output: f is/is not Hurwitz-stable.

Let n be the degree of f and compute $(\sqrt{-1})^n f(x/\sqrt{-1}) = f_0(x) + \sqrt{-1}\cdot f_1(x)$ with $f_0, f_1 \in \mathbb{R}[x]$. This is done by insection.

Form the Sylvester sequence $\mathrm{Sy}(f_0, f_1) = (f_0, f_1, \dots, f_k, 0)$, where f_k is nonzero. If we have

- $k = n$, so that f_k is a nonzero constant,

- All leading coefficients of polynomials in $\mathrm{Sy}(f_0, f_1)$ have the same sign, and
- $f_{n-1} + \sqrt{-1} f_n$ is stable,

then f is Hurwitz-stable. Otherwise, f is not Hurwitz-stable. ◇

Example 5.2.12. We finish computing $\mathrm{Syl}(f_0, f_1)$ from Example 5.2.10. We have

$$\begin{array}{rcl} 10x^2 \ - \ 12 & = & \frac{50}{68}x \cdot (\frac{68}{5}x) \ - \ 12 \\ f_1(x) & = & q_2(x) f_2(x) \ - \ f_3(x)\,. \end{array}$$

Thus $f_3 = 12$. We have

$$f_2 + \sqrt{-1} f_3 \ = \ \frac{68}{5}x + \sqrt{-1} \cdot 12\,,$$

whose root has negative imaginary part and is thus stable. We again conclude that $f = 2x^3 + 10x^2 + 16x + 12$ is Hurwitz-stable. ◇

Remark 5.2.13. Example 5.2.10 suggests a simplification when computing the Sylvester sequence in Algorithm 5.2.11, as well as a more direct version of Lemma 5.2.9. As the powers of x in both f_0 and f_1 are all of the same parity, in the first step of constructing their Sylvester sequence,

$$f_0(x) \ = \ q_1(x) f_1(x) \ - \ f_2(x)\,,$$

the polynomial $q_1(x)$ is the monomial $\frac{a_0}{a_1}x$, and $f_2(x) = \frac{a_0}{a_1} x f_1(x) - f_0(x)$. Let us define a polynomial g by

$$\begin{array}{rcl} (\sqrt{-1})^{n-1} \cdot g(x/\sqrt{-1}) & = & f_1(x) + \sqrt{-1} \cdot f_2(x) \\ & = & f_1(x) + \sqrt{-1}\big(\frac{c_0}{c_1}x \cdot f_1(x) \ - \ f_0(x)\big)\,. \end{array}$$

By Lemma 5.2.9, we have that f is Hurwitz-stable if and only if g is Hurwitz-stable. ◇

The polynomial g of Remark 5.2.13 has an explicit formula, which we give in the following corollary.

Corollary 5.2.14. *A real polynomial $f = \sum_{i=0}^{n} a_i x^{n-i}$ with $a_0 \cdot a_1 \neq 0$ is Hurwitz-stable if and only if*

$$g(x) \ = \ sum_{j\geq 0} a_{2j+1} x^{n-1-2j} \ + \ \sum_{j\geq 1} \big(a_{2j} - \tfrac{a_0}{a_1} a_{2j+1}\big) x^{n-2j}$$

is Hurwitz-stable

The proof of Corollary 5.2.14 is left as Exercise 5.

Corollary 5.2.14 and the role of the Sylvester sequence from Algorithm 5.2.11 leads to the classical solution to the Routh-Hurwitz problem involving Hurwitz matrices.

Definition 5.2.15. Let $f = \sum_{j=0}^{n} a_j x^{n-j}$ be a real univariate polynomial. For each $1 \leq k \leq n$, the kth *Hurwitz matrix* $\mathcal{H}_k$ is the $k \times k$ matrix

$$\mathcal{H}_k \ := \ \begin{pmatrix} a_1 & a_3 & a_5 & \cdots & \cdots & a_{2k-1} \\ a_0 & a_2 & a_4 & \cdots & \cdots & a_{2k-2} \\ 0 & a_1 & a_3 & \cdots & \cdots & a_{2k-3} \\ 0 & a_0 & a_2 & \cdots & \cdots & \vdots \\ 0 & 0 & a_1 & \cdots & \cdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \cdots & \vdots \\ 0 & 0 & \cdots & a_1/a_0 & \cdots & a_k \end{pmatrix} \ = \ \Bigl(a_{2j-i}\Bigr)_{i,j=1}^{k} .$$

Set $\delta_k := \det(\mathcal{H}_k)$ be the kth Hurwitz determinant.

For the polynomial f of Example 5.2.10, we have

$$\mathcal{H}_3 \ = \ \begin{pmatrix} 10 & 12 & 0 \\ 2 & 16 & 0 \\ 0 & 10 & 12 \end{pmatrix} .$$

Theorem 5.2.16. *Let $f = \sum_{j=0}^{n} a_j x^{n-j}$ be a real univariate polynomial with positive leading coefficient $a_0 > 0$ and $n \geq 1$. Then f is Hurwitz-stable if and only if all the Hurwitz determinants $\delta_1, \ldots, \delta_n$ are positive.*

The Hurwitz determinants δ_k are the principal minors of the nth Hurwitz matrix $\mathcal{H}_n$.

Proof. When $n = 1$, $\mathcal{H}_1 = (a_1)$, so that $\delta_1 = a_1$. As the root of f is $-a_1/a_0$, this is negative if and nly if $\delta_1 > 0$.

Suppose that $n > 1$ and suppose that the statement of the theorem is true for all $k < n$. Consider the Hurwitz matrix $\mathcal{H}_n$. To each even-numbered row, apply the row operation

$$R_{2j} \ \longleftarrow \ R_{2j} - \frac{a_0}{a_1} R_{2j-1} .$$

This gives a matrix whose lower right $(n-1) \times (n-1)$ block is the Hurwitz matrix $\mathcal{H}(g)$ for the polynomial g of Corollary 5.2.14.

Suppose that f is Hurwitz-stable, then $a_1 > 0$ (as $a_0 > 0$) and also g is Hurwitz-stable. Then for each $k = 1, \ldots, n$ we have

$$\delta_k \ = \ \det \mathcal{H}_k \ = \ c_1 \cdot \det(\mathcal{H}_{k-1}(g)) \ > \ 0 .$$

(Here, we take $\det(\mathcal{H}_0) := 1$.)

Conversely, if $\delta_1, \ldots, \delta_n > 0$, then $\delta_1 = c_1 > 0$. This implies that $\det(\mathcal{H}_{k-1}(g)) > 0$ for all k. Thus g is Hurwitz-stable by our induction hypothesis, which implies that f is Hurwitz-stable, byCorollary 5.2.14. □

Exercises for Section 5.2.

1. Prove the assertion that is the roots of f and g are simple and strictly interlace, then the values of f at the roots of g alternate in sign.
2. Verify the assertion at the end of the Hermite Biehler Theorem that for an analytic function f,
$$\lim_{z\to x} \frac{f(z)-f(\overline{z})}{z-\overline{z}} \;=\; f'(x)\,,$$
where $x \in \mathbb{R}$ and the limit is over those $z \in \mathcal{H}$ with $\Im(z) \to 0$ as $z \to x$. (Hint: write $z = x+\sqrt{-1}\cdot\epsilon$ and use the definition of derivative, $f'(x) := \lim_{h\to 0}(f(x+h)-f(x))/h$.)
3. Recall the general solution to a linear ordinary differential equation (5.2.7), that is, when its characteristic polynomial $x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ may have roots of ultipicity greater than 1. Using this, show that all solutions to (5.2.7) converge to zero if and only if every root has negative real part.
4. Prove the assertion that a polynomial $f(x)$ is Hurwitz stable if and only if the polynomial $f(x/\sqrt{-1})$ is stable.
5. Verify that the formula for the polynomial g in Corollary 5.2.14 gives the formula of Remark 5.2.13.

5.3. Solving equations with linear algebra

We discuss a connection between the solutions to systems of polynomial equations and eigenvalues from linear algebra. This leads to further methods to compute and analyze the roots of a zero-dimensional ideal. The techniques are based on classical results, but their computational aspects have only recently been systematically developed.

Let $\mathbb{K}$ be a field with algebraic closure $\overline{\mathbb{K}}$ and suppose that $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is a zero-dimensional ideal. Our goal is to interpret the coordinates of points in $\mathcal{V}_{\overline{\mathbb{K}}}(I)$ in terms of eigenvalues of suitable matrices. Then numerical linear algebra provides efficient methods to numerically determine the eigenvalues of a complex matrix, and the matrices we use are readily computed using Gröbner basis algorithms.

It is instructive to start with univariate polynomials. Given a monic univariate polynomial $p = c_0 + c_1 t + \cdots + c_{d-1}t^{d-1} + t^d \in \mathbb{K}[t]$, its companion matrix is

$$C_p \;:=\; \begin{pmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -c_{d-1} \end{pmatrix} \;\in\; \mathbb{K}^{d\times d}\,. \tag{5.3.1}$$

The eigenvalues of a square matrix M are the roots of its characteristic polynomial $\chi_M(t) \;:=\; \det(t\,\mathrm{Id} - M)$, where Id is the appropriately-sized identity matrix. The roots of a polynomial p are the eigenvalues of its companion matrix C_p.

Theorem 5.3.1. *Let $p = c_0 + \cdots + c_{d-1}t^{d-1} + t^d \in \mathbb{K}[t]$ be a monic univariate polynomial of degree $d \geq 1$. Then $p(t) = \chi_{C_p}(t)$, the characteristic polynomial of its companion matrix C_p. Its companion matrix expresses multiplication by t in the ring $\mathbb{K}[t]/\langle p\rangle$ in the basis $1, t, \ldots, t^{d-1}$ of standard monomials.*

Proof. For $d = 1$, the statement is clear, and for $d > 1$, expanding the determinant along the first row of $t\,\mathrm{Id} - C_p$ yields

$$\det(t\,\mathrm{Id} - C_p) \;=\; t\det(t\,\mathrm{Id} - C_q) + (-1)^{d+1}(-1)^{d-1}c_0\,,$$

where C_q is the companion matrix of the polynomial

$$q \;:=\; c_1 + c_2 t + \cdots + c_{d-1}t^{d-2} + t^{d-1} \;=\; (p(t) - c_0)/t\,.$$

Applying the induction hypothesis gives the result.

The claim that the matrix C_p expresses multiplication by t in $\mathbb{K}[t]/\langle p\rangle$ in the basis $1, t, \ldots, t^{d-1}$ of standard monomials is Exercise 1 below. □

Theorem 5.3.1 is well-known—companion matrices underlie the rational canonical form of a matrix or linear transformation. It is equally instructive to reprise the structure of $\overline{\mathbb{K}}[t]/\langle p\rangle$ that underlines the Jordan canonical form. Let $\lambda_1, \ldots, \lambda_r \in \overline{\mathbb{K}}$ be the roots of $p(t)$ with respective multiplicities $\mu_1, \ldots, \mu_r$, so that in $\overline{\mathbb{K}}[t]$, we have

$$p(t) \;=\; \prod_{i=1}^{r}(t-\lambda_i)^{\mu_i}\,.$$

As the factors $(t-\lambda_i)^{\mu_i}$ are pairwise comaximal, the Chinese Remainder r Theorem A.1.1 implies that we have the product decomposition

$$\overline{\mathbb{K}}[t]/\langle p\rangle \ \simeq\ \prod_{i=1}^{r}\overline{\mathbb{K}}[t]/\langle (t{-}\lambda_i)^{\mu_i}\rangle\,. \tag{5.3.2}$$

Let is drop indices and consider one factor $A_\lambda = \overline{\mathbb{K}}[t]/\langle (t{-}\lambda)^{\mu}\rangle$. This is a local ring with unique maximal ideal $\mathfrak{m}_\lambda = \langle t{-}\lambda\rangle$. A more propitious basis than the monomial basis is $\mathcal{B}_\lambda := \{1, (t{-}\lambda), \ldots, (t{-}\lambda)^{\mu-1}\}$. Let $h\in\mathbb{K}[t]$ (or $h\in A$) and consider its expansion in this basis,

$$h \ =\ h(\lambda)\ +\ h_1(\lambda)(t{-}\lambda)\ +\ \cdots\ +\ h_{\mu-1}(\lambda)(t{-}\lambda)^{\mu-1} \qquad \mathrm{mod}(t-\lambda)^{\mu}\,. \tag{5.3.3}$$

(In characteristic zero, $h_k(\lambda) = h^{(k)}(\lambda)/k!$.)

Multiplication by h induces the endomorphism $m_h\colon A_\lambda \to A_\lambda$. Multiplying the expression (5.3.3) for h by elements of the basis $\mathcal{B}_\lambda$ and expressing it in this basis gives the (Toeplitz) matrix of m_h in this basis:

$$\begin{pmatrix} h(\lambda) & 0 & \cdots & 0\\ h_1(\lambda) & h(\lambda) & & \vdots\\ \vdots & \ddots & \ddots & 0\\ h_{\mu-1}(\lambda) & \cdots & h_1(\lambda) & h(\lambda)\end{pmatrix}\,. \tag{5.3.4}$$

Thus $h(\lambda)$ is the only (generalized) eigenvalue of m_h and its algebraic multiplicity is $\mu = \dim_{\mathbb{K}} A_\lambda$. Observe that if h is not a constant in A_λ, then the only eigenvector of m_h is $(t{-}\lambda)^{\mu-1}$.

Consequently, if $\overline{\mathbb{K}}[t]/\langle p\rangle$ has the decomposition (5.3.2) with factors A_{λ_i}, and $h\in\overline{\mathbb{K}}[t]$, then $m_h(A_{\lambda_i})\subset A_{\lambda_i}$ and $m_h|_{A_{\lambda_i}}$ has only one eigenvalue $h(\lambda_i)$ with multiplicity μ_i. In the basis $\mathcal{B} = \mathcal{B}_{\lambda_i}\sqcup\cdots\sqcup\mathcal{B}_{\lambda_r}$ for $\overline{\mathbb{K}}[t]/\langle p\rangle$, m_h is block diagonal with blocks of the form (5.3.4).

THEOREM 5.3.2. *With these definitions, the eigenvalues of m_h are its evaluations $h(\lambda_i)$ at the roots of p, and the eigenvalue $h(\lambda_i)$ has algebraic multiplicity μ_i. Consequently, the trace of m_h is $\sum_i \mu_i h(\lambda_i)$.*

The images of $(t-\lambda_i)^{\mu_i-1}$ in $\overline{\mathbb{K}}[t]/\langle p\rangle$ under the isomorphism (5.3.2) *are the common eigenvectors for all multiplication operators m_h.*

We extend some of this to finite-dimensional quotients of multivariate polynomial rings. Let $I\subset\mathbb{K}[x_1,\ldots,x_n]$ be a zero-dimensional ideal. By Theorems 2.4.1 and 2.4.4, the $\mathbb{K}$-vector space $\mathbb{K}[x_1,\ldots,x_n]/I$ is finite-dimensional, and the cardinality of the variety $\mathcal{V}(I)$ is bounded from above by the dimension of $\mathbb{K}[x_1,\ldots,x_n]/I$. Given a polynomial $f\in\mathbb{K}[x_1,\ldots,x_n]$, write $\overline{f}$ for its residue class in the quotient ring $\mathbb{K}[x_1,\ldots,x_n]/I$.

For any $i=1,\ldots,n$, multiplication of an element in $\mathbb{K}[x_1,\ldots,x_n]/I$ with the residue class $\overline{x_i}$ of a variable x_i defines an endomorphism m_i,

$$\begin{aligned} m_i\ :\ \mathbb{K}[x_1,\ldots,x_n]/I\ &\longrightarrow\ \mathbb{K}[x_1,\ldots,x_n]/I\,,\\ \overline{f}\ &\longmapsto\ \overline{x_i}\cdot\overline{f}\ =\ \overline{x_i f}\,. \end{aligned}$$

Lemma 5.3.3. *The map $x_i \mapsto m_i$ induces an injection*

$$\mathbb{K}[x_1,\dots,x_n]/I \ \hookrightarrow\ \mathrm{End}(\mathbb{K}[x_1,\dots,x_n]/I)\,.$$

Proof. The map $x_i \mapsto m_i$ induces a map φ from $\mathbb{K}[x_1,\dots,x_n]$ to the endomorphism ring. For polynomials $p, f \in \mathbb{K}[x_1,\dots,x_n]$, we have that

$$\varphi(p).\overline{f} \ = \ p(m_1,\dots,m_n).\overline{f} \ = \ \overline{p(x_1,\dots,x_n)f}\,.$$

This implies that $I \subset \ker\varphi$. Setting $f = 1$ shows that $\ker\varphi \subset I$. □

This map $\mathbb{K}[x_1,\dots,x_n]/I \hookrightarrow \mathrm{End}(\mathbb{K}[x_1,\dots,x_n]/I)$ is the regular representation of $\mathbb{K}[x_1,\dots,x_n]/I$. We will use it to study the variety $\mathcal{V}(I)$. Since $\mathbb{K}[x_1,\dots,x_n]/I$ is a finite-dimensional vector space with dimension $d = \deg(I)$, we may represent each linear multiplication map m_i as a $d \times d$-matrix with respect to a fixed basis of $\mathbb{K}[x_1,\dots,x_n]/I$. For this, a basis of standard monomials is both convenient and readily computed.

Let $\mathcal{B}$ be the set of standard monomials for I with respect to a monomial order $\prec$. Let G be a Gröbner basis for I with respect to $\prec$. For each $i = 1,\dots,n$, let $M_i \in \mathrm{Mat}_{\mathcal{B}\times\mathcal{B}}(K)$ be the matrix representing the endomorphism m_i of multiplication by the variable x_i with respect to the basis $\mathcal{B}$, which we call the *i-th companion matrix* of the ideal I with respect to $\mathcal{B}$. The rows and the columns of M_i are indexed by the monomials in $\mathcal{B}$. For a pair of monomials $x^\alpha, x^\beta \in \mathcal{B}$, the entry of M_i in the row corresponding to x^α and column corresponding to x^β is the coefficient of x^α in $x_i \cdot x^\beta$ mod G, the normal form of $x_i \cdot x^\beta$.

Lemma 5.3.4. *The companion matrices commute,*

$$M_i \cdot M_j \ = \ M_j \cdot M_i \quad \textit{for } 1 \le i < j \le n\,.$$

Proof. Let $1 \le i < j \le n$. The matrices M_iM_j and M_jM_i represent the compositions $m_i \circ m_j$ and $m_j \circ m_i$, respectively. These compositions are the endomorphisms of multiplication by x_ix_j and x_jx_i on $\mathbb{K}[x_1,\dots,x_n]/I$. The lemma follows as multiplication in $\mathbb{K}[x_1,\dots,x_n]/I$ is commutative. □

The companion matrices $M_1,\dots,M_n$ generate a subalgebra of $\mathrm{Mat}_{\mathcal{B}\times\mathcal{B}}(\mathbb{K})$ isomorphic to $\mathbb{K}[x_1,\dots,x_n]/I$, by Lemma 5.3.3. As $\mathbb{K}[x_1,\dots,x_n]/I$ is commutative, when $\mathbb{K}$ is algebraically closed, this subalgebra has a collection of common eigenvectors whose eigenvalues are characters (homomorphisms to $\mathbb{K}$) of $\mathbb{K}[x_1,\dots,x_n]/I$. We have the following fundamental result about the eigenvalues of an element $h \in \mathbb{K}[x_1,\dots,x_n]/I$.

Theorem 5.3.5 (Eigenvalue Theorem). *Suppose that $\mathbb{K}$ is algebraically closed, $I \subset \mathbb{K}[x_1,\dots,x_n]$ is a zero-dimensional ideal, and $h \in \mathbb{K}[x_1,\dots,x_n]$. Then the eigenvalues of m_h are the values of h at points of $\mathcal{V}(I)$.*

While this shows that each joint eigenvector of A corresponds to a point of $\mathcal{V}(I)$, and all points of $\mathcal{V}(I)$ arise in this way, the correspondence is is not an injection.

EXAMPLE 5.3.6. Consider the quotient $A = \mathbb{K}[x,y]/\langle x^2, xy, y^2\rangle$, and note that $\mathcal{V}(x^2,xy,y^2) = \{(0,0)\}$. This has dimension 3 with standard basis $\{1,x,y\}$. In this bases, the multiplication endomorphisms become

$$m_1 \;=\; \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix} \qquad m_x \;=\; \begin{pmatrix}0&0&0\\1&0&0\\0&0&0\end{pmatrix} \qquad m_y \;=\; \begin{pmatrix}0&0&0\\0&0&0\\1&0&0\end{pmatrix}$$

Thus the joint eigenvectors of the action of A are the set of the nonzero vectors in the 2-dimensional subspace generated by the images $\overline{x}, \overline{y}$ of x and y in A. Thus the correspondence between eigenvectors and points of $\mathcal{V}(I)$ is not..... ◇

Let us now suppose that $\mathbb{K} = \overline{\mathbb{K}}$ is algebraically closed. We will give a proof Theorem 5.3.5 using the structure of the finite-dimensional (Artinian) ring $A := \mathbb{K}[x_1,\dots,x_n]/I$, which will lead to a strengthening.

Let $\mathcal{V}(I) = \{a_1,\dots,a_r\}$ be the points in the variety of I. These have corresponding maximal ideals $\mathfrak{m}_{a_1},\dots,\mathfrak{m}_{a_r}$, which are exactly the maximal ideals of $\mathbb{K}[x_1,\dots,x_n]$ containing I. As they are pairwise comaximal, the Chinese Remainder Theorem A.1.1 implies that their intersection $J := \mathfrak{m}_{a_1} \bigcap \cdots \bigcap \mathfrak{m}_{a_r}$ equals their product $\mathfrak{m}_{a_1}\cdots\mathfrak{m}_{a_r}$. An element $g \in J$ vanishes on $\mathcal{V}(I)$, so the Nullstellensatz implies that there is an integer $N > 0$ with $g^N \in I$. As J is finitely generated, there is an integer $k > 0$ with $J^k = \mathfrak{m}_{a_1}^k \cdots \mathfrak{m}_{a_r}^k \subset I$. Since $\mathfrak{m}_{a_1}^k,\dots,\mathfrak{m}_{a_r}^k$ are pairwise comaximal, the Chinese Remainder Theorem A.1.1 implies the decomposition $\mathbb{K}[x_1,\dots,x_n]/J^k \simeq \prod_{i=1}^r \mathbb{K}[x_1,\dots,x_n]/\mathfrak{m}_{a_i}^k$.

Since $J^k \subset I$, we have the following decomposition of A,

$$A \;=\; \mathbb{K}[x_1,\dots,x_n]/I \;\simeq\; \prod_{i=1}^{r} \mathbb{K}[x_1,\dots,x_n]/\overline{\mathfrak{m}}_{a_i}^k\ , \tag{5.3.5}$$

where $\overline{\mathfrak{m}}_{a_i}$ is the image of the maximal ideal $\mathfrak{m}_{a_i}$ in A, which is a maximal ideal of A. For $a \in \mathcal{V}(I)$, let A_a be the corresponding factor of A in (5.3.5). This is a local ring with unique maximal ideal $\overline{\mathfrak{m}}_a$. The (*algebraic*) *multiplicity* of the point $a \in \mathcal{V}(I)$, $\text{mult}_I(a)$, is the dimension of A_a as a $\mathbb{K}$-vector space.

As extending scalars to the algebraic closure does not change the dimension of a finite-dimensional vector space, we deduce the following corollary.

COROLLARY 5.3.7. *For any field* $\mathbb{K}$ *and zero-dimensional ideal* $I \subset \mathbb{K}[x_1,\dots,x_n]$,

$$\dim_{\mathbb{K}} \mathbb{K}[x_1,\dots,x_n]/I \;=\; \sum_{a\in\mathcal{V}(I)} \text{mult}_I(a)\,.$$

We prove a theorem that strengthens the statement of the Eigenvalue Theorem.

THEOREM 5.3.8. **??**. *Suppose that* $\mathbb{K}$ *is algebraically closed,* $I \subset \mathbb{K}[x_1,\dots,x_n]$ *is zero-dimensional and* $h \in \mathbb{K}[x_1,\dots,x_n]$. *Then for every* $a \in \mathcal{V}(I)$, *we have* $m_h(A_a) \subset A_a$, *and the restriction of* m_a *to* A_a *has only one eigenvalue* $h(a)$ *of algebraic multiplicity* $\mu(a)$.

By the decomposition (5.3.5) ($A = \prod A_a$), this proves the Eigenvalue Theorem 5.3.5.

PROOF. Let us use the notation of the decomposition (5.3.5). By the Corollary A.1.2 to the Chinese Remainder Theorem, we have elements $\{e_a \mid a \in \mathcal{V}(I)\} \subset \mathbb{K}[x_1,\dots,x_n]$

such that if $a \neq b$ are points of $\mathcal{V}(I)$, then $e_a \in \mathfrak{m}_a^k$, and their images $\{\overline{e_a} \mid a \in \mathcal{V}(I)\}$ in $\mathbb{K}[x_1, \dots, x_n]/I$ satisfy

$$1 \;=\; \sum_{a \in \mathcal{V}(I)} \overline{e_a} \qquad \overline{e_a}^2 = \overline{e_a} \qquad \text{if } a \neq b \;\; \overline{e_a} \cdot \overline{e_b} = 0\,.$$

Observe that as $e_a \in \mathfrak{m}_b$ for $a \neq b$ and the sum of the $\overline{e_a}$ is 1, we have $e_a(b) = \delta_{a,b}$, the Kronecker delta function.

Another consequence of Corollary A.1.2 it that $e_a A = A_a$. Let $h \in \mathbb{K}[x_1, \dots, x_n]$. Then $m_h(A_a) = h(A_a) = h e_a A = e_a h A \subset e_a A = A_a$. For the second statement, note that the restriction of m_h to A_a is multiplication by $e_a h$. Observe that $e_a(h - h(a))$ vanishes on $\mathcal{V}(I)$. By the Nullstellensatz, there is some N such that $(e_a(h-h(a))^N$ lies in I. But then $e_a(h-h(a))^N$ is 0 in A, which shows that $m_{h-h(a)}$ is nilpotent on A_a, which completes the proof. □

Proof of Theorem **??**. Let λ be an eigenvalue of the multiplication endomorphism m_i on $\mathbb{K}[x_1, \dots, x_n]/I$ with corresponding eigenvector $\overline{v}$. That is, $\overline{x_i v} = \lambda \overline{v}$ and thus $\overline{(x_i - \lambda) \cdot v} = 0$ in the vector space $\mathbb{K}[x_1, \dots, x_n]/I$ so that $(x_i - \lambda)v \in I$. Let us assume by way of contradiction that there is no point $a \in \mathcal{V}(I)$ with ith coordinate λ.

This implies that $x_i - \lambda$ vanishes at no point of $\mathcal{V}(I)$. We will use this to show that $\overline{x_i - \lambda}$ is invertible in $\mathbb{K}[x_1, \dots, x_n]/I$. Multiplying the equation $\overline{(x_i - \lambda) \cdot v} = 0$ by this inverse implies that $\overline{v} = 0$, which is a contradiction as eigenvectors are nonzero.

By Exercise 3 of Section 1.3, the map $\mathbb{K}[x_1, \dots, x_n] \to \mathbb{K}^{\mathcal{V}(I)}$ is surjective, where $\mathbb{K}^{\mathcal{V}(I)}$ is the ring of functions on the finite set $\mathcal{V}(I)$. Its kernel is $\sqrt{I}$ by Hilbert's Nullstellensatz. Thus there exists a polynomial $f \in \mathbb{K}[x_1, \dots, x_n]$ with image

$$\overline{f} \;=\; \sum_{a \in \mathcal{V}(I)} \frac{1}{a_i - \lambda} \delta_a$$

in $\mathbb{K}^{\mathcal{V}(I)} \simeq \mathbb{K}[x_1, \dots, x_n]/\sqrt{I}$, where δ_a is the Kronecker delta function, whose value at a point b is zero unless $b = a$, and then its value is 1. Then $f(a) = 1/(a_i - \lambda)$ for $a \in \mathcal{V}(I)$, from which we obtain

$$(1 \;-\; (x_i - \lambda) f(x)) \;\in\; \mathcal{I}(\mathcal{V}(I)) \;=\; \sqrt{I}\,.$$

By Hilbert's Nullstellensatz, there is a positive integer N such that $(1 - (x_i - \lambda) f(x))^N \in I$. Expanding this, we obtain

$$1 \;-\; N(x_i - \lambda) f \;+\; \tbinom{N}{2} (x_i - \lambda)^2 f^2 \;-\; \cdots \;\in\; I\,,$$

and so there exists a polynomial g such that $1 - (x_i - \lambda) g \in I$. Then $\overline{g}$ is the desired inverse to $\overline{x_i - \lambda}$ in $\mathbb{K}[x_1, \dots, x_n]/I$.

Conversely, let $a \in \mathcal{V}(I)$ with $a_i = \lambda$. Let h_i be the minimal polynomial of m_i. By Lemma **??** we need only show that $h_i(\lambda) = 0$. By the definition of minimal polynomial, the function $h_i(m_i)$ is the zero endomorphism on $\mathbb{K}[x_1, \dots, x_n]/I$. In particular, $h_i(\overline{x_i}) = h_i(m_i)(\overline{1}) = 0$ in $\mathbb{K}[x_1, \dots, x_n]/I$, which implies that the polynomial $h_i(x_i) \in \mathbb{K}[x_1, \dots, x_n]$ lies in I. Evaluating this at a point $a \in \mathcal{V}(I)$ gives $0 = h(a) = h(a_i) = h(\lambda)$. □

EXAMPLE 5.3.9. Let $I = \langle x^2y+1, y^2-1\rangle$. Then $\{x^4-1, y+x^2\}$ is a lexicographic Gröbner basis of I. Hence $\{1, x, x^2, x^3\}$ is a basis of $\mathbb{K}[x,y]/I$. With respect to this basis, the representing matrices of the endomorphisms m_x and m_y are

$$M_x \;=\; \begin{pmatrix} 0&0&0&1\\ 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0 \end{pmatrix} \qquad\text{and}\qquad M_y \;=\; \begin{pmatrix} 0&0&-1&0\\ 0&0&0&-1\\ -1&0&0&0\\ 0&-1&0&0 \end{pmatrix}.$$

The eigenvalues of M_x are $-1, 1, -i, i$ and the eigenvalues of M_y are -1 (twice) and 1 (twice). Indeed, we have $\mathcal{V}(I) = \{(i,1), (-i,1), (1,-1), (-1,-1)\}$. ⋄

While we used a Gröbner basis and basis $\mathcal{B}$ of standard monomials to compute companion matrices, Stickelberger's Theorem **??** only requires that we know a basis of the coordinate ring $\mathbb{K}[x_1,\dots,x_n]/I$ and the companion matrices in this basis. Given these data, the computational complexity of finding solutions depends on the dimension, $d = \deg(I)$, of $\mathbb{K}[x_1,\dots,x_n]/I$.

These methods simplify when there exists a joint basis of eigenvectors. That is, if there exists an invertible matrix $S \in \mathbb{K}^{d\times d}$ and diagonal matrices $D_i \in \mathbb{K}^{d\times d}$ for $i = 1,\dots,n$ with

$$M_iS \;=\; SD_i\,, \quad \text{for } i = 1,\dots,n\,. \tag{5.3.6}$$

Then the columns of S are eigenvectors for each multiplication operator, with the eigenvalues given by the entries of the matrices D_i. When (5.3.6) occurs, then $S^{-1}M_iS = D_i$, so that the companion matrices M_i are *simultaneously diagonalizable*.

THEOREM 5.3.10. *The companion matrices $M_1,\dots,M_n$ are simultaneously diagonalizable if and only if I is radical.*

PROOF. Suppose that I is radical. Let $a = (a_1,\dots,a_n)$ be a point in $\mathcal{V}(I)$. As in the proof of Theorem **??**, there exists a polynomial $g_a \in \mathbb{K}[x_1,\dots,x_n]$ with $g_a(a) = 1$ and $g_a(b) = 0$ for all $b \in \mathcal{V}(I) \smallsetminus \{a\}$. Hence, the polynomial $(x_i - a_i)g_a$ vanishes on $\mathcal{V}(I)$. Hilbert's Nullstellensatz then implies $(x_i - a_i)g_a \in \sqrt{I} = I$, and thus $\overline{g_a} \in \mathbb{K}[x_1,\dots,x_n]/I$ is a joint eigenvector of $M_1,\dots,M_n$, with the eigenvalue of M_i equal to the coordinate a_i as in Corollary **??**. As I is radical, $\mathcal{V}(I)$ consists of $d = \deg(I) = \dim(\mathbb{K}[x_1,\dots,x_n]/I)$ points, and so we have found a joint basis of eigenvectors for the companion matrices M_i.

Conversely, if the companion matrices $M_1,\dots,M_n$ are simultaneously diagonalizable, then for every every polynomial $f \in \mathbb{K}[x_1,\dots,x_n]$, the matrix $f(M_1,\dots,M_n)$ is simultaneously diagonalizable, as $f(M_1,\dots,M_n)S = Sf(D_1,\dots,D_n)$. Thus $f(M_1,\dots,M_n)$ is nilpotent only if it is the zero matrix. By Lemma 5.3.3, this implies that I is radical. Explain this □

Stickelberger's Theorem **??** not only connects classical linear algebra to the problem of finding the common zeroes of a zero-dimensional ideal, but it leads to another method to compute eliminants.

COROLLARY 5.3.11. *Suppose that $I \subset \mathbb{K}[x_1,\dots,x_n]$ is a zero-dimensional ideal. The eliminant $g(x_i)$ is the minimal polynomial of the operator m_i of multiplication by x_i on*

$\mathbb{K}[x_1, \ldots, x_n]/I$. *It is a factor of the characteristic polynomial* χ_{m_i} *of* m_i *which contains all its roots.*

This leads to an algorithm to compute the eliminant $g(x_i)$ of the radical of I.

Algorithm 5.3.12.
Input: A zero-dimensional ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ and an index i with $1 \leq i \leq n$.
Output: The eliminant $g(x_i)$ of the radical of I.

Compute a Gröbner basis G for I with respect to any monomial order $\prec$. If $\dim(I) \neq 0$, then exit, else let $\mathcal{B}$ be the corresponding finite set of standard monomials.

Construct M_i, the matrix in $\mathrm{Mat}_{\mathcal{B}\times\mathcal{B}}(\mathbb{K})$ representing multiplication by x_i in the quotient ring $\mathbb{K}[x_1, \ldots, x_n]/I$ in the basis of standard monomials. Let χ_{m_i} be the characteristic polynomial of M_i, and set $g(x_i)$ to be the square-free part of χ_{m_i}, $\chi_{m_i}/\gcd(\chi_{m_i}, \chi'_{m_i})$.

The proof of correctness of this algorithm is Exercise 7.

Exercises.

(1) Let $p = c_0 + \cdots + c_{d-1}t^{d-1} + t^d$ be a monic, univariate polynomial. Show that the matrix M_t representing the endomorphism $m_t \colon \mathbb{K}[t]/\langle p\rangle \to \mathbb{K}[t]/\langle p\rangle$, $\overline{f} \mapsto \overline{tf}$ with respect to a natural basis coincides with the companion matrix C_p (5.3.1).

(2) Let $G := \{x^4-3x^2-2x+1, y+x^3-3x-1\}$ and $I := \langle G\rangle$ be an ideal in $\mathbb{C}[x, y]$. Show that G is a Gröbner basis of I for the lexicographic order $x \prec y$, determine the set of standard monomials of $\mathbb{C}[x, y]/I$ and compute the multiplication matrices M_x and M_y.

(3) Let $f \in \mathbb{K}[x_1, \ldots, x_n]$. Show that $m_f \colon \mathbb{K}[x_1, \ldots, x_n]/I \to \mathbb{K}[x_1, \ldots, x_n]/I$, where $m_f \colon \overline{g} \mapsto \overline{f} \cdot \overline{g}$ is an endomorphism.

(4) In a computer algebra system, use the method of Stickelberger's Theorem to determine the common complex zeroes of $x^2 + 3xy + y^2 - 1$ and $x^2 + 2xy + y + 3$.

(5) If two endomorphisms f and g on a finite-dimensional vector space V are diagonalizable and $f \circ g = g \circ f$, then they are jointly diagonalizable. Conclude that for Stickelberger's Theorem for the ring $\mathbb{K}[x, y]$ with only two variables, there always exist a basis of joint eigenvectors.

(6) Perform the following computational experiment in a computer algebra system.

Generate two bivariate polynomials $f, g \in \mathbb{K}[x, y]$.

(a) Compute their resultant $\mathrm{Res}(f, g; x) \in \mathbb{K}[y]$.

(b) Compute their eliminant $\langle f, g\rangle \cap \mathbb{K}[y]$, using a lexicographic Gröbner basis.

(c) Compute the characteristic polynomial of the companion matrix M_y.

Compare the timings for these three operations for a number of polynomial pairs of moderate to extreme order. Which is more efficient ?

(7) Prove the correctness of Algorithm 5.3.12.

5.4. Root location via quadratic forms

In Section 5.1, we not only gave methods to count and isolate real roots of univariate polynomials, but also how to count the roots of one polynomial by the sign of another polynomial(Theorem ???). We describe another classical method, using the signature and rank of a quadratic trace form, to also count the roots of one polynomial by the sign of another. That method generalizes to multivariate polynomials. We begin with some background on quadratic forms.

A square $n \times n$ matrix $M = (m_{ij})$ is *symmetric* if it is equal to its transpose, $M^T = M$. Equivalently, if $m_{ij} = m_{ji}$ for all $i, j \in [n]$. Recall the classical Spectral Theorem.

THEOREM 5.4.1. *A real symmetric matrix has only real eigenvalues.*

PROOF. Let M be a real $n \times n$ symmetric matrix, and $0 \neq \lambda \in \mathbb{C}$ be a nonzero eigenvalue of M and $v \in \mathbb{C}^n$ is the corresponding eigenvector. Then $v \neq 0$ and $\lambda v = Mv$. Taking complex conjugation gives $\overline{\lambda}\overline{v} = \overline{Mv} = M\overline{v}$. Note that $(M\overline{v})^T = \overline{v}^T M$.

We compute $\overline{v}^T Mv$ in two ways,

$$\begin{aligned} \overline{v}^T Mv &= v^T \cdot (\lambda v) = \lambda(\overline{v}^T \cdot v) \\ \overline{v}^T Mv &= (M\overline{v})^T \cdot v = (\overline{\lambda}\overline{v})^T \cdot v = \overline{\lambda}(\overline{v}^T \cdot v)\,. \end{aligned}$$

Since $0 \neq \|v\|^2 = \overline{v}^T \cdot v$, we conclude that $\lambda = \overline{\lambda}$ is real. □

A *quadratic form* $q = q(x_1, \ldots, x_n)$ is a homogeneous polynomial of degree two in $\mathbb{K}[x_1, \ldots, x_n]$. Consider its monomial expansion

$$q(x_1, \ldots, x_n) = \sum_{i \leq j} a_{ij} x_i x_j\,, \tag{5.4.1}$$

where the coefficients $a_{ij} \in \mathbb{K}$. Suppose that $\mathbb{K}$ does not have characteristic 2. We define a symmetric matrix $Q = (q_{ij})$ by $q_{ii} = a_{ii}$ for $i \in [n]$, and for $i \neq j$ in $[n]$,

$$q_{ij} = \begin{cases} \frac{1}{2} a_{ij} & \text{if } i < j \\ \frac{1}{2} a_{ji} & \text{if } j < i \end{cases}.$$

If we write x for the vector $(x_1, \ldots, x_n)^T$ of variables, then $q = x^T Q x$.

This reversible transformation $q \leftrightsquigarrow Q$ between quadratic forms $q \in \mathbb{K}[x_1, \ldots, x_n]$ and $n \times n$ symmetric matrices over $\mathbb{K}$ identifies the two sets and enables us to transfer results and definitions between quadratic forms and symmetric matrices. For example, the rank, rank(q), of a quadratic form q is the rank of the associated symmetric matrix Q. We establish a fundamental result about quadratic forms and symmetric matrices.

THEOREM 5.4.2. *Let $q \in \mathbb{K}[x_1, \ldots, x_n]$ be a quadratic form over a field $\mathbb{K}$ not of characteristic two. Then there exist nonzero constants $d_1, \ldots, d_r \in \mathbb{K}$, and independent linear forms $\ell_1, \ldots, \ell_r \in \mathbb{K}[x_1, \ldots, x_n]$ such that*

$$q(x_1, \ldots, x_n) = \sum_{i=1}^{r} d_i (\ell_i(x_1, \ldots, x_n))^2\,. \tag{5.4.2}$$

When $\mathbb{K} = \mathbb{R}$, the difference between the number of the constants d_i that are positive and the number that are negative depends upon q and not on the decomposition (5.4.2).

Let $\Lambda \in \mathbb{K}^{r\times n}$ be the matrix of coefficients of the linear forms; its ith row consists of the coefficients of ℓ_i), and $D = \operatorname{diag}(d_1, \dots, d_r)$, and $r \times r$ diagonal matrix. Then the diagonal decomposition (5.4.2) of q corresponds to the factorization of its associated symmetric matrix, $Q = \Lambda^T D\Lambda$. This is a diagonalization of Q, and an expression (5.4.2) is a *diagonalization* of the quadratic form q. As the ℓ_i are linearly independent, both $Lambda$ and D have rank r, showing that the number r in (5.4.2) is the rank of q.

Proof. Let $Q = (q_{ij}) \in \mathbb{K}^{n\times n}$ be the symmetric matrix associated to the quadratic form q, so that $q(x) = x^T Qx$. We prove that q has the form (5.4.2) by induction on the number n of variables.

Observe that if $n = 1$ or $Q = 0$, then q may be diagonalized (5.4.2). Assume that $n > 1$, $Q \neq 0$, and that any quadratic form in $n-1$ variables may be diagonalized.

Suppose first that some diagonal entry q_{ii} in Q is nonzero. Reindexing if necessary, we may assume that $q_{nn} \neq 0$. Let $\ell(x) = \sum_i q_{in}x_i$ be the last entry of the vector Qx, and set $p(x) := q(x) - (\ell(x))^2/q_{nn}$. This quadratic form does not depend upon x_n. Indeed,

$$p(x) \;=\; \sum_{i,j=1}^{n} \bigl(q_{ij} - \frac{q_{in}q_{nj}}{q_{nn}}\bigr) x_i x_j\,,$$

and observe that all terms with i or j equal to n vanish.

By induction, there are independent linear forms $\ell_1, \dots, \ell_r \in \mathbb{K}[x_1, \dots, x_{n-1}]$ and nonzero constants $d_1, \dots, d_r \in \mathbb{K}$ with

$$p \;=\; d_1(\ell_1(x))^2 \;+\; \cdots \;+\; d_r(\ell_r(x))^2\,.$$

Then

$$q \;=\; p \;+\; \frac{1}{q_{nn}}(\ell(x))^2 \;=\; d_1(\ell_1(x))^2 \;+\; \cdots \;+\; d_r(\ell_r(x))^2 \;+\; \frac{1}{q_{nn}}(\ell(x))^2\,.$$

Since x_n occurs in $\ell(x)$, but not in $\ell_1, \dots, \ell_r$, this is a diagonalization of q.

It remains to treat the case when $Q \neq 0$ but all of its diagonal entries q_{ii} vanish. After possibly reindexing, we may assume that $q_{n-1,n} \neq 0$. Thus $q(0, \dots, x_{n-1}, x_n) = 2q_{n-1,n}$. Consider the linear change of variables

$$y_1 \;:=\; x_1\,, \;\dots\;, \; y_{n-2} \;:=\; x_{n-2}\,,\; y_{n-1} \;:=\; \frac{x_{n-1} + x_n}{2}\;,\; y_n \;:=\; \frac{x_{n-1} - x_n}{2}\;.$$

Since $y_{n-1}^2 - y_n^2 = 4x_{n-1}x_n$, we see that if we expand q in terms of $y = (y_1, \dots, y_n)^T$ as $q = y^T My$ with M symmetric,

$$q(y_1, \dots, y_n) \;=\; \sum_{i,j=1}^{n} m_{ij} y_i y_j\,,$$

then $m_{n-1,n} = m_{n,n-1} = 0$ and $m_{n-1,n-1} = 2q_{n-1,n}$ and $m_{n,n} = -q_{n-1,n}$. Thus M has nonzero diagonal entries, and returns us to the previous case when Q has a nonzero diagonal entry.

For the second statement, suppose that $\mathbb{K} = \mathbb{R}$ and suppose that

$$q(x_1, \ldots, x_n) \;=\; \sum_{i=1}^{r} \delta_i(\lambda_i(x))^2 \tag{5.4.3}$$

is a second diagonalization of q—$\delta_1, \ldots, \delta_r \in \mathbb{R}$ are nonzero and $\lambda_1(x), \ldots, \lambda_r(x)$ are linearly independent linear forms. Need to use something other than λ Let s count the number of terms in (5.4.2) with positive coefficients d_i and σ the number of terms in (5.4.3) with positive coefficients, and without loss of generality suppose that $s \leq \sigma$. Suppose further that these sums are indexed so that

$$d_1, \ldots, d_s \;>\; 0 \;>\; d_{s+1}, \ldots, d_r \qquad \text{and} \qquad \delta_1, \ldots, \delta_\sigma \;>\; 0 \;>\; \delta_{\sigma+1}, \ldots, \delta_r\,.$$

Let us suppose by way of contradiction that $s < \sigma$. Write V for the linear space defined by the vanishing of $\ell_1, \ldots, \ell_s\,, \lambda_{\sigma+1}, \ldots, \lambda_r$, and W be defined by $\ell_1, \ldots, \ell_r$. Then

$$\dim V \;\geq\; n - s - (r - \sigma) \;=\; n{-}r \;+\; (\sigma - s) \;>\; n{-}r \;=\; \dim W\,.$$

Let $x \in V \smallsetminus W (\neq \emptyset)$. At least one of the linear forms $\ell_{s+1}, \ldots, \ell_r$ is nonzero at x. Using (5.4.3), we have

$$q(x) \;=\; \sum_{i=1}^{r} \delta_i(\lambda_i(x))^2 \;=\; \delta_{s+1}(\ell_{s+1}(x))^2 \;+\; \cdots \;+\; \delta_\sigma(\lambda_\sigma(x))^2 \;\geq\; 0\,,$$

but using (5.4.2), we have

$$q(x) \;=\; \sum_{i=1}^{r} d_i(\ell_i(x))^2 \;=\; d_{s+1}(\ell_{s+1}(x))^2 \;+\; \cdots \;+\; d_r(\ell_r(x))^2 \;<\; 0\,,$$

which is a contradiction. □

5.5. Craciun's Theorem

5.6. Notes

Descartes' rule of sign [**12**]

In 1807, Ferdinand François Désiré Budan de Boislaurent [**7**] published a generalization of Descartes' Rule to any interval, by considering the expansion of a polynomial $f(x+1)$. In 1820 Joseph Fourier [**18**] independently gave the equivalent form that we presented.

Sturm's Theorem [**32**]

Make remark about the Branden-Borcea theorem (and cite their paper, which is in Ch5/

Theorem **??** is commonly attributed to Stickelberger. A fascinating, scholarly account of that attribution and of Stickelberger's actual work is given in the paper of David Cox [**9**]. Stickelberger he described the form of the trace for a finite-dimensional algebra over a not necessarily algebraically closed field, using a decomposition as a product of local rings, similar to the approach we take to establish both the trace and eigenvalue theorems.

Real algebraic geometry, and especially its relation to applications, is a much larger subject that one may infer from the topics covered in this chapter. A crisp, modern treatment is found in the book of Theobald [**34**], which is particularly focused toward optimization. For a significantly more algorithmic approach is the encyclopedic [**1**].

CHAPTER 6

Schubert Calculus

Outline:

XXX

Grassmannians and flag varieties (and their Schubert varieties) are some of the more common and fundamental objects encountered in algebraic geometry and its applications. Like toric varieties, they posses strong combinatorial structures which facilitate their study. This study involves nontrivial applications of ideas developed elsewhere in this text, and further extensions of these ideas which have been useful in applications. Together with toric varieties, Grassmannians and flag varieties form the foundation of combinatorial algebraic geometry.

6.1. Grassmannians.

Let V be a finite-dimensional $\mathbb{K}$-vector space and k a positive integer less than $\dim(V)$. The set of Grassmannian k-dimensional linear subspaces of V is the *Grassmannian* $G(k,V)$. When $V \simeq \mathbb{K}^n$, we will simply write $G(k,n)$ for the Grassmannian. When $k=1$, this is $\mathbb{P}(V)$ (Definition 1.4.2), which shows that Grassmannians are a generalization of projective spaces.

Let V be an n-dimensional vector space and write V^* for the vector space of linear funcrtions on V (the linear dual V). A nonzero linear form $\ell \in V^*$ on V vanishes on a hyperplane in V (a linear subspace of V of dimension $n{-}1$), and scalar multiples of ℓ give the same hyperplane. This identifies $\mathbb{P}(V^*)$ with $G(n{-}1,V)$. More generally, if $H \in G(k,V)$, then the space $H^\perp$ of linear forms on V that vanish on H has dimension $n{-}k$, which identifies $G(k,V)$ with $G(n{-}k,V^*)$. Choosing a basis for V and the dual basis for V^*, this identifies $G(k,n)$ with $G(n{-}k,n)$, and this identification is called Grassmann duality.

Other than these cases when the Grassmannian is a projective space, we have not yet given the Grassmannian the structure of an algebraic variety. This is a goal of this section. The general linear group $GL(V)$ acts transitively on nonzero-vectors in V, and more generally on k-dimensional linear subspaces of V. That is, given $H, H' \in G(k,V)$, there is an invertible linear transformation on V such that $gH = H'$. If we let $G_H =$

$\{g \in GL(V) \mid gH = H\}$ be the stabilizer of H in $GL(V)$, then we have an identification $G(k, V) = GL(V)/G_H$.

APPENDIX A

Appendix

Basic material should go here, with references. Complete explainations are not necessary, but care should be taken to not abuse the reader.

A.1. Algebra

Algebra is the foundation of algebraic geometry here we collect some of the basic algebra on which we rely and develop some needed algebraic background. This may not be an adequate substitute for a course in abstract algebra. Proofs can be found in standard algebra texts, such as give some useful texts.

A.1.1. Rings. We are all familiar with the real numbers, $\mathbb{R}$, with the rational numbers $\mathbb{Q}$, and with the complex numbers $\mathbb{C}$. These are the most common examples of *fields*, which are the basic building blocks of both the algebra and the geometry that we study. Formally and briefly, a field is a set $\mathbb{K}$ equipped with operations of addition and multiplication and distinguished elements 0 and 1 (the additive and multiplicative identities), and we have that $0 \neq 1$. Every number $a \in \mathbb{K}$ has an additive inverse $-a$ and every nonzero number $a \in \mathbb{K}^\times := \mathbb{K} - \{0\}$ has a multiplicative inverse $a^{-1} =: \frac{1}{a}$. Addition and multiplication are commutative and associative and multiplication distributes over addition, $a(b+c) = ab + ac$.

The set $\mathbb{Z}$ of integers is not a field as $\frac{1}{2}$ is not an integer. While we will mostly be working over $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, at times we will need to discuss other fields. These include the field $\mathbb{K}(t)$ of rational functions, which consists of quotients of univariate polynomials in t or the function field $\mathbb{K}(x_1, \ldots, x_n)$, whose elements are quotients of multivariate polynomials. Most of what we do in algebraic geometry makes sense over any field, including the finite fields. In particular, linear algebra (except numerical linear algebra) works over any field.

Linear algebra concerns itself with *vector spaces*. A vector space V over a field $\mathbb{K}$ comes equipped with an operation of addition—we may add vectors and an operation of multiplication—we may multiply a vector by an element of the field. A linear combination of vectors $v_1, \ldots, v_n \in V$ is any vector of the form

$$a_1v_1 + a_2v_2 + \cdots + a_nv_n\,,$$

where $a_1, \ldots, a_n \in \mathbb{K}$. A collection S of vectors *spans* V if every vector in V is a linear combination of vectors from S. A collection S of vectors is *linearly independent* if zero is not nontrivial linear combination of vectors from S. A *basis* S of V is a linearly independent spanning set. When a vector space V has a finite basis, every other basis has the same number of elements, and this common number is called the *dimension* of V.

A (commutative) *ring* R is a set equipped with an addition and a multiplication which satisfy many of the properties of a field, except that we do not necessarily have multiplicative inverses. While the integers $\mathbb{Z}$ do not form a field, they do form a ring. An *ideal* I of a ring R is a subset which is closed under addition and under multiplication by elements of R. Every ring has two trivial ideals, the zero ideal $\{0\}$ and the unit ideal consisting of R itself. Given a set $S \subset R$ of elements, the smallest ideal containing S, also called the ideal *generated by S*, is

$$\langle S\rangle \ := \ \{r_1s_1 + r_2s_2 + \cdots + r_ms_m \mid r_1, \ldots, r_m \in R \text{ and } s_1, \ldots, s_m \in S\}\,.$$

Given ideals I and J, their sum, $I + J$, is the ideal generated by I and J, which is also the set of elements of the form $a+b$ in R with $a \in I$ and $b \in J$. Their product, $I \cdot J$, is the ideal generated by all products $a \cdot b$ where $a \in I$ and $b \in J$. While we have $I \cdot J \subset I \cap J$, we do not necessarily have equality (for example, when $I = J$, or more concretely, for the ideals $I = 6\mathbb{Z}$ and $J = 10\mathbb{Z}$ of the integers $\mathbb{Z}$, as $I \cdot J = 60\mathbb{Z}$, but $I \cap J = 30\mathbb{Z}$).

A primary use of ideals in algebra is through the construction of quotient rings. Let $I \subset R$ be an ideal. Formally, the *quotient ring R/I* is the collection of all sets of the form

$$[r] \ := \ r + I \ = \ \{r + s \mid s \in I\}\,,$$

as r ranges over R. Addition and multiplication of these sets are defined in the usual way

$$\begin{aligned} [r] + [s] \ &= \ \{r' + s' \mid r' \in [r] \text{ and } s' \in [s]\} \ = \ [r + s], \quad \text{and} \\ [r] \cdot [s] \ &= \ \{r' \cdot s' \mid r' \in [r] \text{ and } s' \in [s]\} \ = \ [rs]\,. \end{aligned}$$

The last equality in each line is meant to be surprising, they are theorems due to I being an ideal. Thus addition and multiplication on R/I are inherited from R. With these definitions (and also $-[r] = [-r]$, $0 := [0]$, and $1 := [1]$), the set R/I becomes a ring.

We say 'R-mod-I' for R/I because the arithmetic in R/I is just the arithmetic in R, but considered modulo the ideal I, as $[r] = [s]$ in R/I if and only if $r - s \in I$. Oftentimes, we will write $\overline{r}$ or even r itself for the image $[r]$ of a ring element $r \in R$ in a quotient ring R/I.

Ideals arise naturally as kernels of homomorphisms. A *homomorphism* $\varphi\colon R \to S$ from the ring R to the ring S is a function that preserves the ring structure. Thus for $r, s \in R$, $\varphi(r + s) = \varphi(r) + \varphi(s)$ and $\varphi(rs) = \varphi(r)\varphi(s)$. We also require that $\varphi(1) = 1$. The *kernel* of a homomorphism $\varphi\colon R \to S$,

$$\ker\varphi \ := \ \{r \in R \mid \varphi(r) = 0\}$$

is an ideal: If $r, s \in \ker\varphi$ and $t \in R$, then

$$\varphi(r + s) \ = \ \varphi(r) + \varphi(s) \ = \ 0 \ = \ t\varphi(r) \ = \ \varphi(tr)\,.$$

Homomorphisms are deeply intertwined with ideals. If I is an ideal of a ring R, then the association $r \mapsto [r]$ defines a homomorphism $\varphi\colon R \to R/I$ whose kernel is I. Dually, given a homomorphism $\varphi\colon R \to S$, the image of R in S is identified with $R/\ker\varphi$. More generally, if $\varphi\colon R \to S$ is a homomorphism and $I \subset R$ is an ideal with $I \subset \ker\varphi$ (that is, $\varphi(I) = 0$), then φ induces a homomorphism $\varphi\colon R/I \to S$.

Properties of ideals induce natural properties in the associated quotient rings. For example, the ideals of R/I all have the form J/I, where J is an ideal of R that contains

I. An element r of a ring R is *nilpotent* if $r \neq 0$, but some power of r vanishes. A ring R is *reduced* if it has no nilpotent elements, that is, whenever $r \in R$ and n is a natural number with $r^n = 0$, then we must have $r = 0$. An ideal *radical* if whenever $r \in R$ and n is a natural number with $r^n \in I$, then we must have $r \in I$. It follows that a quotient ring R/I is reduced if and only if I is radical.

A ring R is a *domain* if whenever we have $r \cdot s = 0$ with $r \neq 0$, then we must have $s = 0$. An ideal is *prime* if whenever $r \cdot s \in I$ with $r \notin I$, then we must have $s \in I$. It follows that a quotient ring R/I is a domain if and only if I is prime.

Given a domain R, we have its field of fractions or quotient field. This generalizes the construction of the rational numbers $\mathbb{Q}$ from the integers $\mathbb{Z}$. As a set, it is the collection of fractions r/s, where $r, s \in R$ and $s \neq 0$, where we identify r/s with ρ/σ if and only if $r\sigma = s\rho$. Addition and multiplication of fractions is the same as addition and mutiplication of rational numbers. The function fields $\mathbb{K}(t)$ and $\mathbb{K}(x_1, \ldots, x_n)$ are the fields of fractions of the polynomial rings $\mathbb{K}[t]$ and $\mathbb{K}[x_1, \ldots, x_n]$, respectively.

A ring R with no nontrivial ideals must be a field. Indeed, if $0 \neq r \in R$, then the ideal rR of R generated by r is not the zero ideal, and so it must equal R. But then $1 = rs$ for some $s \in R$, and so r is invertible. Conversely, if R is a field and $0 \neq r \in R$, then $1 = r \cdot r^{-1} \in rR$, so the only ideals of R are $\{0\}$ and R. An ideal $\mathfrak{m}$ of R is *maximal* if $\mathfrak{m} \subsetneq R$, but there is no ideal I strictly contained between $\mathfrak{m}$ and R; if $\mathfrak{m} \subset I \subset R$ and $I \neq R$, then $I = \mathfrak{m}$. It follows that a quotient ring R/I is a field if and only if I is maximal. As a field is a domain, maximal ideals are also prime.

We remark that any ideal I of R with $I \neq R$ is contained in some maximal ideal. This is a standard application of Zorn's Lemma. Let $\mathcal{I}$ be the set of proper ideals J of R with $I \subset J$. This is partially ordered by inclusion. Consider a chain of ideals in $\mathcal{I}$,

$$I \ \subset \ I_1 \ \subset \ I_2 \ \subset \ \cdots$$

We claim that the union $J := \bigcup_n I_n$ of these ideals is a proper ideal in R. First, $1 \neq J$ as $1 \neq I_i$ for all i. Suppose that $r, s \in J$. Then there are indices i, j with $r \in I_i$ and $s \in I_j$. Since $I_i, I_j \subset I_{\max(i,j)}$, we have $r + s \in I_{\max(i,j)} \subset J$. Also, $t \in R$, then $tr \in I_i \subset J$. Thus $J \in \mathcal{I}$. By Zorn's Lemma, there are maximal elements of $\mathcal{I}$, and any such maximal element is necessarily a maximal ideal in R.

Ideals I, J of a ring R are *comaximal* is there is no maximal ideal containing both. Equivalently, if $I + J = R$. Observe that if I and J are comaximal, then for any $k > 0$, I^k and J^k are comaximal. We show the contrapositive of this statement. If $\mathfrak{m}$ is a maximal ideal containing both I^k and J^k, then as $\mathfrak{m}$ is prime, $I, J \subset \mathfrak{m}$. The Chinese Remainder Theorem describes the structure of a ring modulo a product of comaximal ideals.

Theorem A.1.1. *Suppose that $I_1, \ldots, I_n \subset R$ are pairwise comaximal ideals of a ring R (for all $i \neq j$, I_i and I_j are comaximal). Then the diagonal map $r \mapsto (r, \ldots, r)$ from $R \to R^n$ induces an isomorphism of rings*

$$R/(I_1 \cdot I_2 \cdots I_n) \ \xrightarrow{\ \sim\ } \ R/I_1 \times R/I_2 \times \ \cdots \ \times R/I_n \,.$$

The intersection $I_1 \cap I_2 \cap \cdots \cap I_n$ of these ideal is equal to their product $I_1 \cdot I_2 \cdots I_n$.

Proof. Suppose first that $n = 2$. Let $I, J \subset R$ be comaximal ideals. The diagonal map $r \mapsto (r, r)$ from $R \to R \times R$ induces a ring homomorphism $R \to R/I \times R/J$ with kernel $I \cap J$, and thus a homomorphism

$$\varphi \colon\ R/I \cap J \ \longrightarrow\ R/I \times R/J\,.$$

As I and J are comaximal, $I + J = R$. Thus there exist $a \in I$ and $b \in J$ with $a + b = 1$. Thus $(\overline{1}, \overline{1}) = \varphi(1) = \varphi(a + b) = (\overline{b}, \overline{a})$. Let $(\overline{p}, \overline{q}) \in R/I \times R/J$. Then

$$\varphi(pb + qa) \ =\ (\overline{pb}, \overline{qa}) \ =\ (\overline{p}, \overline{q}) \cdot (\overline{b}, \overline{a}) \ =\ (\overline{p}, \overline{q}) \cdot (\overline{1}, \overline{1}) \ =\ (\overline{p}, \overline{q})\,.$$

Thus φ is surjective. Recall that $I \cdot J \subset I \cap J$. Let $c \in I \cap J$. Then $c = c \cdot (a + b) = ca + cb \in I \cdot J$, so that $I \cap J = I \cdot J$. This completes the proof when $n = 2$.

The general case follows by induction on n. Set $I := I_1$ and $J = I_2 \cdots I_n$. We claim these are comaximal. For each $j = 2, \ldots, n$, I_1 and I_j are comaximal, so there exist $a_j \in I_1$ and $b_j \in I_j$ with $a_j + b_j = 1$. Then

$$1 \ =\ (a_2 + b_2) \cdot (a_3 + b_3) \cdots (a_n + b_n) \ \in\ I_1 + I_2 \cdots I_n \ =\ I + J\,.$$

Applying the result for $n = 2$ to I, J and the induction hypothesis for $I_2, \ldots, I_n$ completes the proof. □

Corollary A.1.2. *Let $I_1, \ldots, I_n \subset R$ are pairwise comaximal ideals of a ring R. Then there*

Note that $e_i R/I = R/I_i$.
Define local ring somewhere?

Theorem A.1.3. *See if this can be removed. Let I be an ideal of a ring R. Then:*

(1) $\sqrt{I}$ is the intersection of all prime ideals containing I.
(2) For every prime ideal P containing I there exists a minimal prime ideal $P' \subset P$ containing I.
(3) If P is a minimal prime ideal containing I and $a \in P$ then there exists $b \in R \setminus P$ and $n \geq 0$ with $a^n b \in I$.

A.1.2. Modules. A *module* over a commutative ring R is an abelian group M (the group operation on M is addition and is written '$+$'), together with an action of R on M. That is, for $f \in R$ and $g \in M$, we have $f.m \in M$, and this satisfies the following properties: For $f, g \in R$ and $m, n \in M$,

$$\begin{array}{rclcrcl} (f+g).m & = & f.m + g.m & \qquad & f.(m+n) & = & f.m + f.n \\ f.(g.m) & = & (fg).m & & 1.m & = & 1\,. \end{array}$$

Here, 1 is the identity of R. These properties imply that $0.m = f.0 = 0$. Technically, an action is a ring homomorphism $\varphi\colon R \to \mathrm{End}(M)$, and we write $f.m$ for $\varphi(f)(m)$.

Example A.1.4. Any abelian group A is a $\mathbb{Z}$-module, where for $a \in A$ and $n \in \mathbb{Z}$, if $n > 0$, then $n.a := a + \cdots + a$ (n times), and if $n < 0$, then $n.a := -(-n.a)$.

Suppose that $R = \mathbb{K}[x_1, \ldots, x_n]$ is a polynomial ring over a field $\mathbb{K}$. Then R is an R-module—the action is simply multiplication, $f.g := fg$. An ideal $I \subset R$ is also an R-module, as is the quotient ring R/I. ◇

A *submodule* of an R-module M is a subgroup N of M that is closed under the action of R: for all $f \in R$ and $n \in N$, we have $f.n \in N$. Ideals of R are exactly the R-submodules of R. Given an R-submodule N of M, the quotient M/N of abelian groups is also an R-module. Given R-modules M, N an R-module map is a homomorphism $\varphi\colon M \to N$ of abelian groups that commutes with the R-action, for all $f \in R$ and $m \in M$, we have $\varphi(f.m) = f.\varphi(m)$. The *kernel* $\ker\varphi$ and *image* $\varphi(M)$ are the kernel and image of φ as a map of abelian groups. We have $\ker\varphi \subset M$ and $\varphi(M) \subset N$, and they are R-submodules. The quotient $N/\varphi(M)$ is called the *cokernel* of φ and written as $\operatorname{coker}\varphi$. If $A \subset N$ is an R-submodule, then its inverse image $\varphi^{-1}(A) = \{m \in M \mid \varphi(m) \in A\}$ is an R-submodule of M called the preimage of A under φ.

A sequence of R-modules and maps, $L \xrightarrow{\varphi} M \xrightarrow{\psi} N$ is *exact* at M if $\varphi(L) = \ker\psi$. A longer sequence

$$M_{r+1} \xrightarrow{\varphi_{r+1}} M_r \xrightarrow{\varphi_r} \cdots \xrightarrow{\varphi_2} M_1 \xrightarrow{\varphi_1} M_0$$

is *exact* if it is exact at each of $M_1, \ldots, M_r$.

An R module M is *finitely generated* if there is a finite set $S = \{m_1, \ldots, m_r\} \subset M$ such that M is the only submodule of M that contains S. Equivalently, for any $m \in M$, there are $f_1, \ldots, f_r \in R$ such that $m = f_1 m_1 + \cdots + f_r m_r$.

An R-module M is *free* if it is isomorphic to a direct sum of copies of R. The number(cardinality) of summands is an invariant of M, called its *rank*. When this is finite, we will write $M = R^r$, where $r = \mathrm{rank}(M)$, and express an element $\mathbf{f}$ of R^r as an ordered list $\mathbf{f} = (f_1, \ldots, f_r)$ of elements $f_i \in R$. Canonical generators of R^r are its *standard basis* $\mathbf{e}_1, \ldots, \mathbf{e}_r$, where $\mathbf{e}_i$ is the list $(0, \ldots, 1, \ldots, 0)$, which every entry is 0 except the ith, which is 1.

A.1.3. Fields and polynomials. Our basic algebraic objects are polynomials. Make sure to define Laurent polynomials. A *univariate polynomial* p is an expression of the form

$$p \;=\; p(x) \;:=\; a_0 + a_1x + a_2x^2 + \cdots + a_mx^m\,, \tag{A.1.1}$$

where m is a nonnegative integer and the coefficients $a_0, a_1, \dots, a_m$ lie in $\mathbb{K}$. Write $\mathbb{K}[x]$ for the set of all polynomials in the variable x with coefficients in $\mathbb{K}$. We may add, subtract, and multiply polynomials and $\mathbb{K}[x]$ is a ring.

While a polynomial p may be regarded as a formal expression (A.1.1), evaluation of a polynomial defines a function $p\colon \mathbb{K} \to \mathbb{K}$: The value of the function p at a point $a \in \mathbb{K}$ is simply $p(a)$. When $\mathbb{K}$ is infinite, the polynomial and the function determine each other, but this is not the case when $\mathbb{K}$ is finite.

For polynomials with more than one variable, we begin with multivariate monomials.

Definition A.1.5. A *monomial* in the variables $x_1, \dots, x_n$ is a product of the form

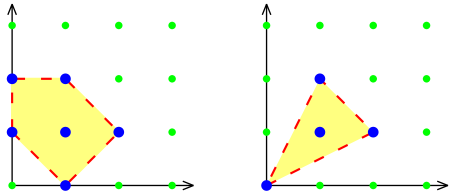
$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}\,,$$

where the exponents $\alpha_1, \dots, \alpha_n$ are nonnegative integers. For notational convenience, set $\alpha := (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$[†] and write x^α for the expression $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. The (*total*) *degree* of the monomial x^α is $|\alpha| := \alpha_1 + \cdots + \alpha_n$. ◇

A *polynomial* $f = f(x_1, \dots, x_n)$ in the variables $x_1, \dots, x_n$ is a linear combination of monomials, that is, a sum of the form

$$f \;=\; \sum_{\alpha\in\mathbb{N}^n} a_\alpha x^\alpha\,,$$

where each *coefficient* a_α lies in $\mathbb{K}$ and all but finitely many coefficients vanish. The product $a_\alpha x^\alpha$ of an element a_α of $\mathbb{K}$ and a monomial x^α is a *term*. The *support* $\mathcal{A} \subset \mathbb{N}^n$ of a polynomial f is the set of all exponent vectors that appear in f with a nonzero coefficient. For example, the bivariate polynomial $p := 1 - 2xy + 4xy^2 - 8x^2y$ has support $\{(0,0), (1,1), (1,2), (2,1)\}$. Writing the elements of the support as the columns of a matrix, this is $\left(\begin{smallmatrix} 0&1&1&2\\ 0&1&2&1\end{smallmatrix}\right)$. The polynomial $q := x + 2y + 3xy + 5y^2 + 7xy^2 + 11x^2y$ has support $\left(\begin{smallmatrix} 1&0&1&0&1&2\\ 0&1&1&2&2&1\end{smallmatrix}\right)$. The *Newton polytope*, $\mathrm{New}(f)$ of a polynomial f is the convex hull of its support. (See Section A.3.) Here are the Newton polytopes of p and q (which are polygons), respectively.



We will say that f has support $\mathcal{A}$ to mean that the support of f is a subset of $\mathcal{A}$. With this definition, the set of all polynomials with support a finite set $\mathcal{A} \subset \mathbb{N}^n$ is the vector space $\mathbb{K}^{\mathcal{A}}$, consisting of all coefficient vectors $(a_\alpha \mid \alpha \in \mathcal{A})$ for polynomials with support $\mathcal{A}$. Here, as elsewhere, we the finite set $\mathcal{A}$ as a natural index set.

[†] Where have we defined $\mathbb{N}$?

After 0 and 1 (the additive and multiplicative identities), the most distinguished integers are the prime numbers, those $p > 1$ whose only divisors are 1 and themselves. These are the numbers $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$ Every integer $n > 1$ has a unique factorization into prime numbers

$$n \;=\; p_1^{\alpha_1} p_1^{\alpha_2} \cdots p_n^{\alpha_n}\,,$$

where $p_1 < \cdots < p_n$ are distinct primes, and $\alpha_1, \ldots, \alpha_n$ are (strictly) positive integers. For example, $999 = 3^3 \cdot 37$. Polynomials also have unique factorization.

Definition A.1.6. A nonconstant polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$ is *irreducible* if whenever we have $f = gh$ with g, h polynomials, then either g or h is a constant. That is, f has no nontrivial factors.

Theorem A.1.7. *Every polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$ is a product of irreducible polynomials*

$$f \;=\; p_1 \cdot p_2 \cdots p_m\,,$$

where the polynomials $p_1, \ldots, p_m$ are irreducible and nonconstant. Moreover, this factorization is essentially unique. That is, if

$$f \;=\; q_1 \cdot q_2 \cdots q_s\,,$$

is another such factorization, then $m = s$, and after permuting the order of the factors, each polynomial q_i is a scalar multiple of the corresponding polynomial p_i.

A.1.4. Polynomials in one variable. While rings of polynomials have many properties in common with the integers, the relation is the closest for univariate polynomials. The *degree*, $\deg(f)$ of a univariate polynomial f is the largest degree of a monomial appearing in f. If this monomial has coefficient 1, then the polynomial is *monic*. This allows us to remove the ambiguity in the uniqueness of factorizations in Theorem A.1.7. A polynomial $f(x) \in \mathbb{K}[x]$ has a unique factorization of the form

$$f \;=\; f_m \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_s^{\alpha_s}\,,$$

where $f_m \in \mathbb{K}^\times$ is the leading coefficient of f, the polynomials $p_1, \ldots, p_s$ are monic and irreducible, and the exponents α_i are positive integers.

Definition A.1.8. A *greatest common divisor* of two polynomials $f, g \in \mathbb{K}[x]$ (or $\gcd(f, g)$) is a polynomial h such that h divides each of f and g, and if there is another polynomial k which divides both f and g, then k divides h.

Any two polynomials f and g have a monic greatest common divisor which is the product of the common monic irreducible factors of f and g, each raised to the highest power that divides both f and g. Finding greatest common divisor would seem challenging as factoring polynomials is not an easy task. There is, however, a very fast and efficient algorithm for computing the greatest common divisor of two polynomials.

Suppose that we have polynomials f and g in $\mathbb{K}[x]$ with $\deg(g) \geq \deg(f)$,

$$\begin{aligned} f &= f_0 + f_1 x + f_2 x^2 + \cdots + f_m x^m \\ g &= g_0 + g_1 x + g_2 x^2 + \cdots + g_m x^m + \cdots + g_n x^n\,, \end{aligned}$$

where f_m and g_n are nonzero. Then the polynomial

$$S(f,g) \ := \ g - \frac{g_n}{f_m} x^{n-m} \cdot f$$

has degree strictly less than $n = \deg(g)$. This simple operation of *reducing* f by the polynomial g forms the basis of the Division Algorithm and the Euclidean Algorithm for computing the greatest common divisor of two polynomials.

We describe the *Division Algorithm* in *pseudocode*, which is a common way to explain algorithms without reference to a specific programming language.

Algorithm A.1.9 (Division Algorithm).

```
INPUT: Polynomials $f, g \in \mathbb{K}[x]$.
OUTPUT: Polynomials $q, r \in \mathbb{K}[x]$ with $g = qf + r$ and $\deg(r) < \deg(f)$.
Set $r := g$ and $q := 0$.
(1) If $\deg(r) < \deg(f)$, then exit.
(2) Otherwise, reduce $r$ by $f$ to get the expression
        $r \ = \ \frac{r_n}{f_m} x^{n-m} \cdot f \ + \ S(f,r)\,,$
    where $n = \deg(r)$ and $m = \deg(f)$. Set $q := q + \frac{r_n}{f_m} x^{n-m}$ and $r := S(f,r)$, and return to step (1).
```

To see that this algorithm does produce the desired expression $g = qf + r$ with the degree of r less than the degree of f, note first that whenever we are at step (1), we will always have $g = qf + r$. Also, every time step (2) is executed, the degree of r must drop, and so after at most $\deg(g) - \deg(f) + 1$ steps, the algorithm will halt with the correct answer.

The *Euclidean Algorithm* computes the greatest common divisor of two polynomials f and g.

Algorithm A.1.10 (Euclidean Algorithm).

```
INPUT: Polynomials $f, g \in \mathbb{K}[x]$.
OUTPUT: The greatest common divisor $h$ of $f$ and $g$.
(1) Call the Division Algorithm to write $g = qf + r$ where $\deg(r) < \deg(f)$.
(2) If $r = 0$ then set $h := f$ and exit.
    Otherwise, set $g := f$ and $f := r$ and return to step (1).
```

To see that the Euclidean algorithm performs as claimed, first note that if $g = qf + r$ with $r = 0$, then $f = \gcd(f,g)$. If $r \neq 0$, then $\gcd(f,g) = \gcd(f,r)$. Thus the greatest common divisor h of f and g is always the same whenever step (1) is executed. Since the degree of r must drop upon each iteration, r will eventually become 0, which shows that the algorithm will halt and return h.[†]

An ideal is *principal* if it has the form

$$\langle f \rangle \ = \ \{h \cdot f \mid h \in \mathbb{K}[x]\}\,,$$

[†] This is poorly written!

for some $f \in \mathbb{K}[x]$. We say that f *generates* $\langle f\rangle$. Since $\langle f\rangle = \langle \alpha f\rangle$ for any $\alpha \in \mathbb{K}$, the principal ideal has a unique monic generator.

THEOREM A.1.11. *Every ideal I of $\mathbb{K}[x]$ is principal.*

PROOF. Suppose that I is a nonzero ideal of $\mathbb{K}[x]$, and let f be a nonzero polynomial of minimal degree in I. If $g \in I$, then we may apply the Division Algorithm and obtain polynomials $q, r \in \mathbb{K}[x]$ with

$$g \;=\; qf + r \qquad \text{with} \qquad \deg(r) < \deg(f)\,.$$

Since $r = g - qf$, we have $r \in I$, and since $\deg(r) < \deg(f)$, but f had minimal degree in I, we conclude that f divides g, and thus $I = \langle f\rangle$. □

The ideal generated by univariate polynomials $f_1, \ldots, f_s$ is the principal ideal $\langle p\rangle$, where p is the greatest common divisor of $f_1, \ldots, f_s$.

For univariate polynomials p the quotient ring $\mathbb{K}[x]/\langle p\rangle$ has a concrete interpretation. Given $f \in \mathbb{K}[x]$, we may call the Division Algorithm to obtain polynomials q, r with

$$f \;=\; q\cdot p + r, \text{ where } \deg(r) < \deg(q)\,.$$

Then $[f] = f + \langle p\rangle = r + \langle p\rangle = [r]$ and in fact r is the unique polynomial of minimal degree in the coset $f + \langle p\rangle$. We call this the *normal form* of f in $\mathbb{K}[x]/\langle p\rangle$.

Since, if $\deg(r), \deg(s) < \deg(p)$, we cannot have $r - s \in \langle p\rangle$ unless $r = s$, we see that the monomials $1, x, x^2, \ldots, x^{\deg(p)-1}$ form a basis for the $\mathbb{K}$-vector space $\mathbb{K}[x]/\langle p\rangle$. This describes the additive structure on $\mathbb{K}[x]/\langle p\rangle$.

To describe its multiplicative structure, we only need to show how to write a product of monomials $x^a \cdot x^b$ with $a, b < \deg(p)$ in this basis. Suppose that p is monic with $\deg(p) = n$ and write $p(x) = x^n - q(x)$, where q has degree strictly less than p. Since $x^a \cdot x^b = (x^a \cdot x)\cdot x^{b-1}$, we may assume that $b = 1$. When $a < n$, we have $x^a \cdot x^1 = x^{a+1}$. When $a = n-1$, then $x^{n-1}\cdot x^1 = x^n = q(x)$,

Here are some things that we may need.

- Gauss's lemma (as used in Section 3.3): K is the quotient field of a UFD R if $f \in R[t]$ is monic and $f = gh$ in $K[t]$ with g monic, then $g \in R[t]$.
- Relate algebraic properties of $p(x)$ to properties of R, for example, zero divisors and domain. What is meant by this?
- Prove that a field is a ring with only trivial ideals.

  Prove $I \subset J \subset R$ are ideals, then J/I is an ideal of R/I, and deduce that $R = \mathbb{K}[x]/p(x)$ is a field only if $p(x)$ is irreducible.

  Example $\mathbb{Q}[x]/(x^2-2)$ and explore $\mathbb{Q}(\sqrt{2})$.

  Example $\mathbb{R}[x]/(x^2+1)$ and show how it is isomorphic to $\mathbb{C}$.

  Work up to algebraically closed fields, the fundamental theorem of algebra (both over $\mathbb{C}$ and over $\mathbb{R}$).

  Explain that an algebraically closed field has no algebraic extensions (hence the name).
- We will need to develop briefly Noetherian modules over a commutative ring, and state that a finitely generated module over a Noetherian ring is Noetherian. Also

that a ring extension is finite if and only if every element of the bigger ring is integral over the smaller one.

- For this, we show that every element of $\mathbb{K}[X_{\Lambda_0}]$ is integral over the coordinate ring of $\pi(X) \smallsetminus \mathcal{V}(y_0)$, which is its subring generated by $\frac{\Lambda_1}{\Lambda_0}, \dots, \frac{\Lambda_m}{\Lambda_0}$. (By Result in the appendix this implies that $\mathbb{K}[X_{\Lambda_0}]$ is integral over over the coordinate ring of $\pi(X) \smallsetminus \mathcal{V}(y_0)$.)
- A map $\varphi\colon X \to Y$ is finite if and only if $\varphi^*\colon \mathbb{K}[Y] \to \mathbb{K}[X]$ is an injection and every element $t \in \mathbb{K}[X]$ is integral over $\mathbb{K}[Y]$. Corollary 1.3.15 gives one direction, the other needs to be discussed in Appendix A.1.4.
- Need every ideal of a ring is contained in a maximal ideal.

A.1.5. Some field theory? Algebra needed for the Nullstellensatz

In Chapter 1, we deduced the Nullstellensatz from Lemma 1.2.7, but only gave a proof when the base field $\mathbb{K}$ was uncountable. Because of its importance, we give a proof of the full statement.

Lemma 1.2.7 *Let $\mathbb{K}$ be a field and $L \supset \mathbb{K}$ a field extension that is finitely generated over $\mathbb{K}$. Then L is an algebraic extension of $\mathbb{K}$.*

Proof. Our proof relies on transcendental extensions. Can this be turned into a direct proof?

Suppose that L is finitely generated as a $\mathbb{K}$-algebra, but L is not an algebraic extension of $\mathbb{K}$. Then L has an element t that is not algebraic over $\mathbb{K}$, so that $\mathbb{K}(t) \subset L$ is isomorphic to the field of rational functions over $\mathbb{K}$ in one variable.

We first suppose that L is algebraic over $\mathbb{K}(t)$. Since it is also finitely generated, this implies that it has finite dimension as a $\mathbb{K}(t)$-vector space.[†] Let $\mathbf{e}_1, \dots, \mathbf{e}_m \in L$ be a $\mathbb{K}(t)$-basis. We may assume that $\mathbf{e}_1 = 1$. Consider the multiplication table for L,

$$\mathbf{e}_i \cdot \mathbf{e}_j \;=\; \sum_{k=1}^{m} \frac{\alpha_{ijk}(t)}{\beta_{ijk}(t)} \mathbf{e}_k \ , \tag{A.1.2}$$

where $\alpha_{ijk}, \beta_{ijk}$ are polynomials in $L[t]$. Let $R = \mathbb{K}[r_2, \dots, r_n] \subset L$ be a finitely generated $\mathbb{K}$-algebra. We will show that $R \neq L$, which contradicts our assumption that L is finitely generated.

Let $r_1 := 1$, and let us expand $r_1, \dots, r_n$ in terms of the basis $\mathbf{e}_1, \dots, \mathbf{e}_m$,

$$r_i \;=\; \sum_{j=1}^{m} \frac{\gamma_{ij}(t)}{\delta_{ij}(t)} \mathbf{e}_j \ , \tag{A.1.3}$$

where γ_{ij}, δ_{ij} are polynomials in $L[t]$. Any element $r \in R$ is a $\mathbb{K}$-linear combination of $r_0 = 1 = \mathbf{e}_1$ and monomials in the $r_1, \dots, r_n$. Write each r_i in terms of the basis

[†] Maybe we need to make this argument somewhere.

using (A.1.3), and then use (A.1.2) to express products of the basis elements in terms of the basis. This gives an expression

$$r \;=\; \sum_{i=1}^{m} \frac{f_i(t)}{g_i(t)}\mathbf{e}_i$$

of r as a $\mathbb{K}(t)$-linear combination of $\mathbf{e}_1, \ldots, \mathbf{e}_m$. Note that in this expression, the denominators $g_i(t)$ only involve products of the denominators β_{ijk} and δ_{ij} from (A.1.2) and (A.1.3).

Since $\mathbb{K}[t]$ is a unique factorization domain and it has infinitely many primes,[†], we may let $p(t) \in \mathbb{K}[t]$ be a prime that does mot divide any of the polynomials γ_{ij}, δ_{ij}. Then $1/p(t) = \mathbf{e}_1/p(t) \in L$ is not an element of R, which completes the proof in this case.

Let us consider the general case. We may assume that L is generated over $\mathbb{K}$ by $t_1, \ldots, t_a, x_1, \ldots, x_b$, where $t_1, \ldots, t_a$ are algebraically independent[§] over $\mathbb{K}$ so that the function field $\mathbb{K}(t_1, \ldots, t_a)$ of $t_1, \ldots, t_a$ is a subfield of L, and each x_i is algebraic over $\mathbb{K}(t_1, \ldots, t_a)$. Thus L is an algebraic extension of $\mathbb{K}(t_1, \ldots, t_a)$. By our assumption that L is not an algebraic extension of $\mathbb{K}$, we have $a \geq 1$. Since L is finitely generated as an algebra over $\mathbb{K}$, it is finitely generated as an algebra over $M = \mathbb{K}(t_1, \ldots, t_{a-1})$. Replacing $\mathbb{K}$ by M and t by t_a puts us in the previous case, which completes the proof. □

Remark A.1.12. We may appeal to field theory to justify the algebraic version of our definition of dimension. Let X be an irreducible variety and $U \subset X$ a dense affine open subset. These have the same field of rational functions, $\mathbb{K}(X) = \mathbb{K}(U)$. If $\{u_1, \ldots, u_m\} \subset \mathbb{K}[U]$ is a maximal set of algebraically independent elements, then every element of $\mathbb{K}[U]$ is algebraic over $\mathbb{K}[u_1, \ldots, u_m]$, and therefore $\mathbb{K}(X)$ is an algebraic extension of $\mathbb{K}(u_1, \ldots, u_m)$. In field theory, such a set $\{u_1, \ldots, u_m\} \subset \mathbb{K}(X)$ of algebraically independent elements is a *transcendence basis* for $\mathbb{K}(X)$. Arguments similar to those from linear algebra about bases imply that the number, m of elements in a transcendence basis for $\mathbb{K}(X)$ is an invariant called the transcendence degree. Please develop these arguments here. Thus we may appeal to field theory for the definition of dimension in algebraic geometry.

A.1.6. Multilinear algebra.

This may be needed in the section on the Grassmannian.

A.2. Topology

Topology concerns the most basic properties of shape and space. A fundamental notion is that of continuity that many of us first encountered in calculus. It begins quite formally. A topology on a set X is a collection of subsets of X, called *open sets*, that satisfy the following properties.

(1) Both the empty set and X itself are open.
(2) Any union of open sets are open.
(3) Any finite intersection of open sets is open.

[†] Prove this somewhere

[§] Define algebraically (in)dependent somewhere? Prove some properties in the exercises.

A set X with a topology is called a *topological space*. The complement of an open set is a *closed set*. A topology is dually specified by its collection of closed sets. Closed sets satisfy corresponding properties: Both X and are closed, any intersection of closed sets is closed, and any finite union of closed sets is closed.

The *closure* $\overline{Z}$ of a subset $Z \subset X$ of a topologoical space is the intersection of all closed subsets that contain Z. It is the smallest closed subset of X that contains Z. A topology on X can be specified by giving a collection of subsets of X called *basic open sets*, and then taking the open sets to be the smallest collection of subsets containing these basic open sets and that satisfies the three given properties.

The standard examples of topological spaces are $\mathbb{R}^n$ and $\mathbb{C}^n$ with what we call their *Euclidean topology*. Here, the basic open sets are Euclidean balls. For $x \in \mathbb{R}^n$ and $\epsilon > 0$

$$B(x, \epsilon) \ := \ \{a \in \mathbb{R}^n \mid \sum |a_i - x_i|^2 \ < \ \epsilon\}\,.$$

The same formula gives a Euclidean ball in $\mathbb{C}^n$, where for a complex number $z \in \mathbb{C}$, we have $|z|^2 = z\overline{z}$, where $\overline{z}$ is the complex cojugate of z.

A subset $Y \subset X$ of a topological space has an induced *subspace topology*. A subset of Y is open if it is the intersection of Y with an open subset of X. A subset Y of X with this topology is a (topological) subspace of X.

Contiuous functions are the functions between topological spaces that preserve their structures. More formally, a function $f\colon X \to Y$ between topological spaces X and Y is continous if for any open subset U of Y, $f^{-1}(U)$ is an open subset of X. Dually, for any closed subset Z of Y, $f^{-1}(Z)$ is closed in X.

The standard topology on $\mathbb{R}^n$ or $\mathbb{C}^n$, along with the subspace topology on their subsets, is common in mathematics. Algebraic geometry uses a weaker topology, called the *Zariski topology*. Its basis of open sets have the form $U_f := \{x \in \mathbb{C}^n \mid f(x) \neq 0\}$, where $f \in \mathbb{C}[x_1, \dots, x_n]$ is a polynomial, and its closed subsets are varieties $\mathcal{V}(S) := \{x \in \mathbb{C}^n \mid f(x) = 0 \ \forall f \in S\}$, where $S \subset \mathbb{C}[x_1, \dots, x_n]$ is a set of polynomials. This is introduced in Section **??**.

A.3. Convex geometry

Need the separating property: if K is convex and $x \notin K$, then there is a hyperplane H containing x that does not meet K.

A.3.1. Polytopes and polyhedra. Polytopes and polyhedra are important semialgebraic sets that are fundamental to toric varieties and tropical geometry. For more information see the books of Ewald [**15**] and Ziegler [**36**]. Let $\{v_1, \dots, v_m\} \subset \mathbb{R}^n$ be a finite set of points. A sum

$$\sum_{i=1}^{m} \lambda_i v_i \qquad \text{where} \qquad \lambda_1, \dots, \lambda_m \ \geq \ 0 \quad \text{and} \quad \sum_{i=1}^{m} \lambda_i \ = \ 1$$

is a *convex combination* of the points $v_1, \dots, v_m$. The *convex hull* of $\{v_1, \dots, v_m\}$ is the set of all their convex combinations,

$$\text{(A.3.1)} \qquad \operatorname{conv}\{v_1, \dots, v_m\} \ := \ \Big\{\sum_{i=1}^{m} \lambda_i v_i \mid \lambda_1, \dots, \lambda_m \ \geq \ 0 \quad \text{and} \quad \sum_{i=1}^{m} \lambda_i \ = \ 1\Big\}.$$

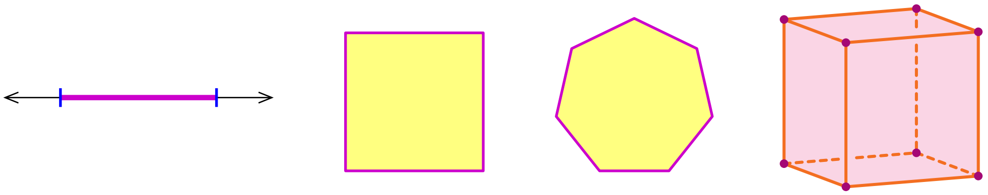
A convex hull of a finite set of points is a *polytope*. If this representation is irredundant in that no point v_i lies in the convex hull of the others, then each point v_i is a *vertex* of the polytope.

A translate $x + L$ of a linear subspace L by a vector $x \in \mathbb{R}^n$ is an affine subspace. The dimension of $x + L$ is the dimension of L. The *affine span*, $\operatorname{Aff}(X)$ of a set X is the intersection of all affine subspaces that contain X. For any $x \in X$, it has the form $x + \operatorname{span}\{y - x \mid y \in X\}$. It is also the set of all affine combinations of points of X,

$$\text{(A.3.2)} \qquad \operatorname{Aff} X \ = \ \Big\{\sum_{i=1}^{m} \lambda_i x_i \mid x_1, \dots, x_m \in X \quad \text{and} \quad \sum_{i=1}^{m} \lambda_i = 1\Big\}.$$

(This differs fronm the convex hull in that the coefficients λ_i may be negative.) The dimension of a polytope P is the dimension of its affine span.

There is only one polytope (a point) of dimension 0. Polytopes of dimension 1 are line segments, two-dimensional polytopes are polygons, and three-dimensional polytopes are familiar objects such as the cube in $\mathbb{R}^3$.



A polytope P with m vertices has dimension at most $m{-}1$. When it has dimension $m{-}1$, it is a *simplex*. For example, the *standard*, or probability, n-dimensional simplex $\triangle^n$ is the convex hull of the $n{+}1$ linearly independent standard basis vectors $e_1, \dots, e_{n+1}$ in $\mathbb{R}^{n+1}$. It is the intersection of the affine hyperplane $\{\lambda \in \mathbb{R}^{n+1} \mid \lambda_1 + \cdots + \lambda_{n+1} = 1\}$ and the positive orthant,

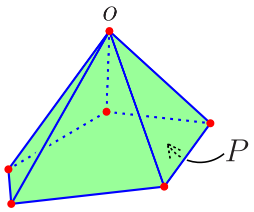
$$\triangle^n \ = \ \{\lambda \ \in \ \mathbb{R}^{n+1} \ \mid \ \lambda_i \ \geq \ 0 \quad \text{and} \quad \lambda_1 + \cdots + \lambda_{n+1} \ = \ 1\}.$$

A polytope with m vertices $\operatorname{conv}\{v_1, \dots, v_m\}$ (A.3.1) is the image of the standard $m{-}1$ simplex under the linear map that sends $e_i \in \mathbb{R}^m$ to $v_i \in \mathbb{R}^n$, for $i = 1, \dots, m$. This is evident as points in the simplex parametrize convex combinations under this map. More generally, the image of any polytope under a linear or an affine map is another polytope—simply take the convex hull of the images of the vertices.

As a polytope P is closed and bounded, for $w \in \mathbb{R}^n$, the linear function $x \mapsto w^T x$ is bounded below and achieves its minimum value, $h_P(w)$, on P. The function $w \mapsto h_P(w)$ is the *support function* of P, and the subset $P_w := \{x \in P \mid w^T x = h_P(w)\}$ of P where this minimum is attained is the face of P *exposed* by w. A *face* of P is a set of the form P_w for some $w \in \mathbb{R}^n$. Faces are themselves polytopes; if $P = \operatorname{conv}\{v_1, \dots, v_m\}$, then $P_w = \operatorname{conv}\{v_i \mid w^T v_i = h_P(w)\}$. The polytope P is itself a face; it is exposed by the zero vector $0 \in \mathbb{R}^n$. Vertices are faces of dimension zero and edges are faces of dimension one. A *facet* of P is a face F of codimension one, $\dim F = \dim P - 1$. As its faces are convex hulls of subsets of its vertices, a polytope P has only finitely many faces.

Perhaps this is where it would be useful to point out that the set of w which expose a face of a polytope is a cone, giving equations and inequations, and note that there are integer points in this cone if the polytope is integral. This is used in Chapter 8. It would also be used in defining the Gröbner fan, which might be useful in tropical geometry ?

Example A.3.1. A useful construction of one polytope from another is a pyramid. Suppose that a polytope $P \subset \mathbb{R}^n$ has dimension $n-1$. Then its affine span is a hyperplane H. For any point $o \in \mathbb{R}^n \smallsetminus H$, the *pyramid* with base P and *apex* o is the convex hull of the polytope P and the point o.



◇

By the definition of the support functions, for every $w \in \mathbb{R}^n$ we have that

$$P \;\subset\; \{x \in \mathbb{R}^n \mid w^T x \geq h_P(w)\}\,.$$

When $w \neq 0$, the set $\{x \in \mathbb{R}^n \mid w^T x \geq h_P(w)\}$ is a *half space* and its boundary $H := \{x \in \mathbb{R}^n \mid w^T x = h_P(w)\}$ is a *supporting hyperplane* of P. The intersection of P with this supporting hyperplane is the face P_w of P exposed by w. Also note that a face P_w of a polytope is the intersection of P with the affine span of P_w.

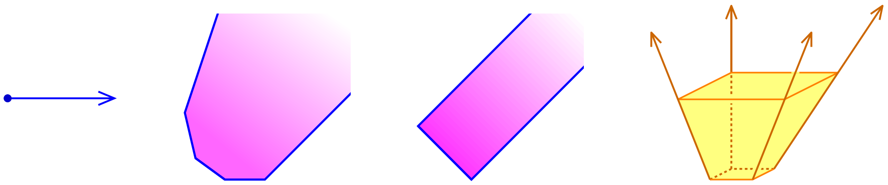
As a closed, convex body, P is the intersection of all half-spaces that contain it,

$$P \;=\; \bigcap_{w \in \mathbb{R}^n} \{x \in \mathbb{R}^n \mid w^T x \geq h_P(w)\}\,. \tag{A.3.3}$$

This intersection may be taken to be finite, there is a finite set $w_1, \dots, w_d \in \mathbb{R}^n$ such that

$$P \;=\; \{x \in \mathbb{R}^n \mid w_i^T x \geq h_P(w_i) \quad \text{for } i = 1, \dots, d\}\,. \tag{A.3.4}$$

A *polyhedron* is the intersection of finitely many half spaces. In general, a polyhedron may be unbounded. Here are four unbounded polyhedra in $\mathbb{R}$, $\mathbb{R}^2$, $\mathbb{R}^2$, and $\mathbb{R}^3$, respectively.



A polyhedron P has a support function $h_P(w)$ that takes values in $\mathbb{R} \cup \{-\infty\}$. When P is unbounded in the direction opposite w, then $h_P(w) = -\infty$. With this definition, the description (A.3.3) holds for P. Polytopes are exactly the bounded polyhedra.

Given the facet description (A.3.4) of a polyhedron, let A be the $d \times n$ matrix whose rows are the facet normals w_i^T for $i = 1, \ldots, d$ and let $b \in \mathbb{R}^d$ be the column vector with ith entry $-h_P(w_i)$. Then (A.3.4) becomes

$$P \;=\; \{x \in \mathbb{R}^n \mid Ax + b \geq 0\}\,, \tag{A.3.5}$$

where $\geq$ is coordinatewise comparison.

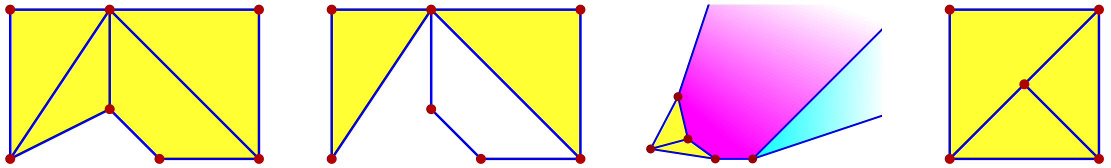
This leads to another description. The affine map $\Lambda\colon x \mapsto Ax + b$ sends $\mathbb{R}^n$ to the affine subspace $L := A\mathbb{R}^n + b$ of $\mathbb{R}^d$, and by (A.3.5) the image $\Lambda(P)$ of P under this map is the intersection $L \cap \mathbb{R}^d_+$ of L with the nonnegative orthant $\mathbb{R}^d_+ := \{y \in \mathbb{R}^d \mid y_i \geq 0\}$. Thus P is the inverse image of the polyhedron $\mathbb{R}^d_+$ under the affine map Λ.

Suppose that an affine subspace $L \subset \mathbb{R}^n$ is defined by the affine equations $Ax = b$ where $A\colon \mathbb{R}^n \to \mathbb{R}^d$ is a linear map and $b \in \mathbb{R}^d$. Then the polyhedron $L \cap \mathbb{R}^n_+$ is

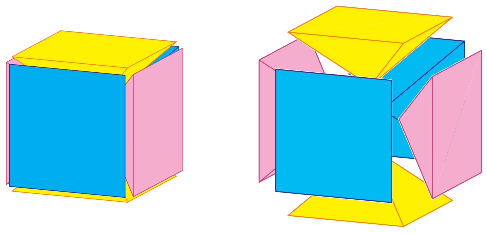
$$\{x \in \mathbb{R}^n \mid Ax = b \ \text{ and } \ x \geq 0\}\,.$$

More generally, any section $L \cap P$ of a polyhedron P by an affine subspace L is again a polyhedron, as is the inverse image of a polyhedron under an affine map. By Fourier-Motzkin elimination (Need to justify this) the image of a polyhedron under an affine map is again a polyhedron.

A *polyhedral complex* is a collection $\mathcal{P}$ of polyhedra in $\mathbb{R}^n$ such that every face of a polyhedron P in $\mathcal{P}$ is another polyhedron in $\mathcal{P}$ and the intersection of any two polyhedra P, P' in $\mathcal{P}$ is a common face of each. For example, of the four collections of vertices, line segments and polyhedra shown below, the first three are polyhedral complexes, while the last is not; the large triangle does not meet either smaller triangle in one of its faces.

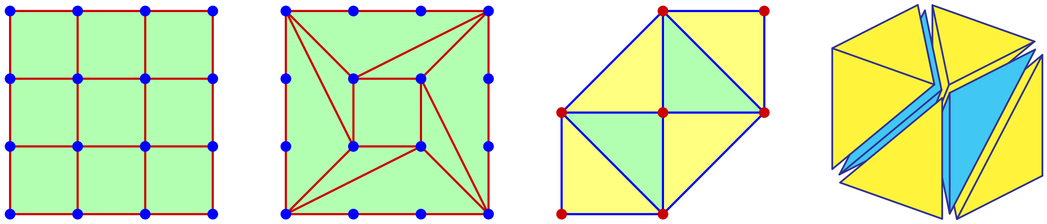


The collection of all faces of a polyhedron is a polyhedral complex, as is the collection of its proper faces. For a less trivial example, suppose that $o \in P$ is any point of a polytope P. For every face F of P that does not contain o we may consider the pyramid with base F and apex o. This collection of pyramids, their bases, and the apex forms a polyhedral complex. For example, consider the cube in $\mathbb{R}^3$ with o its center. The resulting polyhedral complex has six square pyramids, which we show in both slightly and exaggerated exploded views.



The *support* of a polyhedral complex $\mathcal{P}$ is the union of the polyhedra in $\mathcal{P}$. When the support of a polyhedral complex is a polyhedron P, the complex is a *subdivision* of P.

When every polytope in a polyhedral complex $\mathcal{P}$ is a simplex, $\mathcal{P}$ is a *triangulation* of its support. Of the four polyhedral subdivisions below, the last two are triangulations.



A.3.2. Minkowski sum and mixed volumes. Polytopes in the vector space $\mathbb{R}^n$ inherit two operations of sum and scalar multiplication, and they also have an intrinsic metric invariant, their volume. The interplay of these structures leads to the notion of mixed volume, which is important in the application of algebraic geometry. A standard reference is [**29**], see also [**15**].

Addition of vectors in $\mathbb{R}^n$ induces the operation of *Minkowski sum* on polytopes, where

$$P + Q \ := \ \{x + y \mid x \in P, y \in Q\}\,.$$

We may similarly multiply a polytope P by a positive scalar λ to get λP. When λ is an integer, these operations coincide, for example $P + P = 2P$. We may combine them. Given polytopes $P_1, \ldots, P_r \subset \mathbb{R}^n$ and nonnegative real numbers $\lambda_1, \ldots, \lambda_r$, define

$$P(\lambda) \ := \ \lambda_1 P_1 + \cdots + \lambda_r P_r\,. \tag{A.3.6}$$

Lemma A.3.2. *The Minkowski sum $P(\lambda)$ (A.3.6) is a polytope. For any vector $w \in \mathbb{R}^n$, its support function $h_{P(\lambda)}(w)$ is the sum $\lambda_1 h_{P_1}(w) + \cdots + \lambda_r h_{P_r}(w)$, and*

$$P(\lambda)_w \ = \ \lambda_1 P_{1,w} + \cdots + \lambda_r P_{r,w}\,.$$

If $P(\lambda)_w$ is a facet of $P(\lambda)$ for one choice of $\lambda_1, \ldots, \lambda_r$ with all $\lambda_i > 0$, then $P(\lambda)_w$ is a facet of $P(\lambda)$ for any $\lambda_1, \ldots, \lambda_r$ with all $\lambda_i > 0$.

Example A.3.3. Suppose that $P \subset \mathbb{R}^2$ is the convex hull of the column vectors of the matrix $\left(\begin{smallmatrix}1&0&1&2&1\\0&1&1&1&2\end{smallmatrix}\right)$ and Q is the convex hull of the column vectors of the matrix $\left(\begin{smallmatrix}0&1&2&1&1\\0&0&0&1&2\end{smallmatrix}\right)$. Then $P + Q$ is the convex hull of the column vectors of the matrix $\left(\begin{smallmatrix}1&3&0&4&1&3&2\\0&0&1&1&3&3&4\end{smallmatrix}\right)$. We display these polygons and their Minkowski sum in Figure A.3.1.

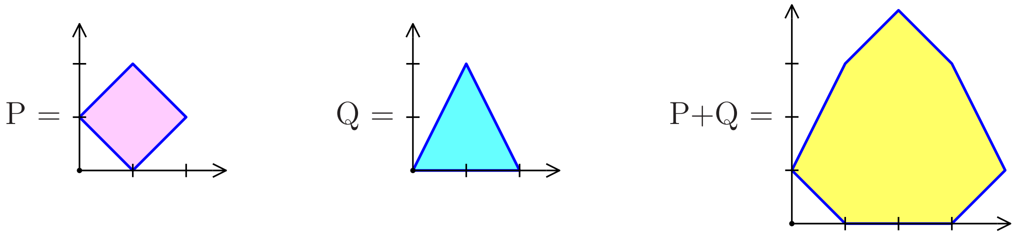


Figure A.3.1. Minkowski sum of two polygons.

Proof. Let $\{v_1, \ldots, v_m\}$ and $\{u_1, \ldots, u_d\}$ be finite subsets of $\mathbb{R}^n$. The sum of a convex combination of each is a convex combination of their sum,

$$\sum_{i=1}^{m} \lambda_i v_i + \sum_{j=1}^{d} \mu_j u_j \;=\; \sum_{i,j} \lambda_i \mu_j (v_i + u_j)\,, \tag{A.3.7}$$

as $\sum_i \lambda_i = \sum_j \mu_j = 1$, which implies that $\sum_{i,j} \lambda_i \mu_j = 1$. The same is true for a scalar multiple of a convex combination. Thus the Minkowski sum of polytopes is a polytope and a scalar multiple of a polytope is a polytope.

If λ, μ are nonnegative, then

$$\min\{(\lambda v_i + \mu u_j) w^T\}_{i,j} \;=\; \lambda \min\{v_i w^T\}_i + \mu \min\{u_j w^T\}_j\,,$$

which implies the linearity of the support function, and that the face of $P(\lambda)$ exposed by w is the scaled sum of faces of the P_i exposed by w. Finally, the statement about facets follows as the affine span of a nonnegative scalar multiple μX of a set X is the scalar multiple of the affine span of X, and the affine span of a Minkowski sum is the Minkowski sum of the affine span, again by (A.3.7). □

We prove Minkowski's result about the volume of the scaled sum (A.3.6).

Theorem A.3.4. *Let $P_1, \ldots, P_r \subset \mathbb{R}^n$ be polytopes. For nonnegative $\lambda_1, \ldots, \lambda_r$, $\mathrm{vol}_n(P(\lambda))$ is a homogeneous polynomial of degree n in $\lambda_1, \ldots, \lambda_r$.*

Proof. Suppose first that $n = 1$. Then each P_i is an interval $[a_i, b_i]$ with $a_i \leq b_i$ so that $P(\lambda) = [\lambda_1 a_1 + \cdots + \lambda_r a_r, \lambda_1 b_1 + \cdots + \lambda_r b_r]$, and we have

$$\mathrm{vol}_1(P(\lambda)) \;=\; \sum_{i=1}^{r} \lambda_i b_i - \sum_{i=1}^{r} \lambda_i a_i \;=\; \sum_{i=1}^{r} \lambda_i (b_i - a_i) \;=\; \sum_{i=1}^{r} \lambda_i \, \mathrm{vol}_1(P_i)\,,$$

which is homogeneous of degree 1 in $\lambda_1, \ldots, \lambda_r$.

Now suppose that $n > 1$. As volume is invariant under translation, we make some assumptions for the purpose of computation. For a given $w \in \mathbb{R}^n$ and all i, we may assume that 0 lies in the face $P_{i,w}$ of P_i exposed by w. Then each $P_{i,w}$ as well as $P(\lambda)_w$ lies in the hyperplane annihilated by w, which is isomorphic to $\mathbb{R}^{n-1}$. By induction on dimension, we may assume that $\mathrm{vol}_{n-1}(P(\lambda)_w) = \mathrm{vol}_{n-1}(\lambda_1 P_{1,w} + \cdots + \lambda_r P_{r,w})$ is a homogeneous polynomial of degree $n-1$ in $\lambda_1, \ldots, \lambda_r$. This conclusion about $\mathrm{vol}_{n-1}(P(\lambda)_w)$ remains true even if 0 does not lie in any face $P_{i,w}$.

Again translating $P(\lambda)$ if necessary, we may assume that $h_{P(\lambda)}(w) > 0$. Then the pyramid C_w with apex $0 \in \mathbb{R}^n$ over the facet $P(\lambda)_w$ of $P(\lambda)$ has height $\frac{1}{\|w\|} h_{P(\lambda)}(w)$ and therefore has volume

$$\frac{1}{n} \cdot \frac{1}{\|w\|} h_{P(\lambda)}(w) \cdot \mathrm{vol}_{n-1}(P(\lambda)_w)$$

which is a homogeneous polynomial of degree n in $\lambda_1, \ldots, \lambda_r$, as $h_{P(\lambda)}(w)$ is linear in $\lambda_1, \ldots, \lambda_r$. Again using that volume is invariant under translation, now suppose that $0 \in P(\lambda)$, and thus the support function of $P(\lambda)$ is nonnegative for all $w \in \mathbb{R}^n$. Then the pyramids over facets of $P(\lambda)$ form a polyhedral subdivision of $P(\lambda)$, so that $\mathrm{vol}(P(\lambda))$ is the sum of the volumes of these pyramids. This completes the proof. □

Let us write the polynomial $\mathrm{vol}(P(\lambda))$ as a tensor (nonsymmetric in $\lambda_1, \ldots, \lambda_r$),

$$\text{(A.3.8)} \qquad \mathrm{vol}(P(\lambda)) \;=\; \sum_{a_1,\ldots,a_n=1}^{r} \mathrm{MV}(P_{a_1}, P_{a_2}, \ldots, P_{a_n})\lambda_{a_1}\lambda_{a_2}\cdots\lambda_{a_n}\,,$$

where the coefficients are chosen to be symmetric—for any permutation $\pi \in S_n$, we have

$$\mathrm{MV}(P_{a_1}, P_{a_2}, \ldots, P_{a_n}) \;=\; \mathrm{MV}(P_{\pi(a_1)}, P_{\pi(a_2)}, \ldots, P_{\pi(a_n)})\,.$$

The coefficient $\mathrm{MV}(P_{a_1} \ldots, P_{a_n})$ is the *mixed volume* of the polytopes $P_{a_1}, \ldots, P_{a_n}$.

Lemma A.3.5. *Mixed volumes satisfy the following properties. Let $P, Q, P_1, \ldots, P_n \subset \mathbb{R}^n$ be polytopes.*

(1) Symmetry. $\mathrm{MV}(P_{a_1}, \ldots, P_{a_n}) = \mathrm{MV}(P_{\pi(a_1)}, \ldots, P_{\pi(a_n)})$ *for any permutation* $\pi \in S_n$.

(2) Multilinearity. For any nonnegative λ, μ, we have

$$\mathrm{MV}(\lambda P + \mu Q, P_2, \ldots, P_n) \;=\; \lambda\,\mathrm{MV}(P, P_2, \ldots, P_n) \;+\; \mu\,\mathrm{MV}(Q, P_2, \ldots, P_n)\,.$$

(3) Normalization. $\mathrm{MV}(P, \ldots, P) = \mathrm{vol}_n(P)$.

Proof. Symmetry follows from the definition of mixed volume. For multilinearity, equate the coefficient of $\lambda_1 \cdots \lambda_n$ in the nonsymmetric expansions (A.3.8) of

$$\mathrm{vol}(\lambda_1(\lambda P + \mu Q) + P_2 + \cdots + P_n) \;=\; \mathrm{vol}(\lambda_1\lambda P + \lambda_1\mu Q + P_2 + \cdots + P_n)\,.$$

(For the first, $r = n$ and for the second, $r = n{+}1$ in (A.3.8).) Finally, for normalization, note that for $\lambda \geq 0$, $\lambda^n \mathrm{vol}(P) = \mathrm{vol}(\lambda P) = \lambda^n \mathrm{MV}(P, \ldots, P)$, with the first equality coming from the definition of volume and the second from the expansion (A.3.8) defining mixed volume. □

These three properties characterize mixed volumes.

Corollary A.3.6. *Mixed volume is the unique function of n-tuples of polytopes in $\mathbb{R}^n$ that satisfies the properties of symmetry, multilinearity, and normalization of Lemma A.3.5.*

Proof. Let L be a function of n-tuples of polytopes in $\mathbb{R}^n$ that satisfies the three properties of symmetry, multilinearity, and normalization of Lemma A.3.5. For any polytopes $P_1, \ldots, P_n \subset \mathbb{R}^n$ and nonnegative $\lambda_1, \ldots, \lambda_n$, we have $\mathrm{vol}(P(\lambda)) = L(P(\lambda), \ldots, P(\lambda))$ by normalization. Expanding this using (A.3.6) and the multilinearity of L, we obtain

$$L(P(\lambda), \ldots, P(\lambda)) \;=\; \sum_{a_1,\ldots,a_n=1}^{n} L(P_{a_1}, P_{a_2}, \ldots, P_{a_n})\lambda_{a_1}\lambda_{a_2}\cdots\lambda_{a_n}\,.$$

The equality of this sum with the sum (A.3.8) and the symmetry of both L and MV in their arguments completes the proof. □

We give another formula for mixed volume and prove a stronger version of Corollary A.3.6. Given polytopes $P_1, \ldots, P_n$ and $\emptyset \neq A \subset [n]$ write $P(A)$ for the Minkowski sum $\sum_{i\in A} P_i$.

Theorem A.3.7. *Let $\mathcal{P}$ be a collection of polytopes in $\mathbb{R}^n$ that is closed under Minkowski sum. Suppose that L is a function of n-tuples of polytopes in $\mathcal{P}$ that is symmetric in its arguments and normalized (as in Lemma A.3.5), and that L is multilinear under Minkowski sum ($\lambda = \mu = 1$ in Lemma A.3.5). Then for any polytopes $P_1, \ldots, P_n \in \mathcal{P}$, we have*

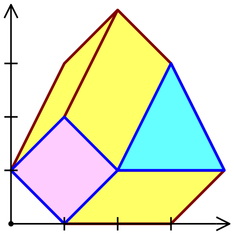
$$n!L(P_1, \ldots, P_n) \;=\; \sum_{\emptyset \neq A \subset [n]} (-1)^{n-|A|} \operatorname{vol}(P(A))\,. \tag{A.3.9}$$

In particular, L equals mixed volume, $L(P_1, \ldots, P_n) = \operatorname{MV}(P_1, \ldots, P_n)$.

Example A.3.8. If P, Q, R are polytopes in $\mathbb{R}^3$, then $6\,\operatorname{MV}(P,Q,R)$ equals

$$\operatorname{vol}(P+Q+R) - \operatorname{vol}(P+Q) - \operatorname{vol}(P+R) - \operatorname{vol}(Q+R) + \operatorname{vol}(P) + \operatorname{vol}(Q) + \operatorname{vol}(R)\,.$$

For polygons P, Q, we have $2\,\operatorname{MV}(P,Q) = \operatorname{vol}(P+Q) - \operatorname{vol}(P) - \operatorname{vol}(Q)$. For the polygons in Figure A.3.1, if we subdivide $P+Q$ as shown,



then $2\,\operatorname{MV}(P,Q)$ equals the combined areas of the four parallelograms, which is six.

Proof of Theorem A.3.7. Let $\emptyset \neq A \subset [n]$. Since L is normalized, $L(P(A), \ldots, P(A))$ equals $\operatorname{vol}(P(A))$. Expand $L(P(A), \ldots, P(A))$ using the multilinearity of L to obtain

$$\operatorname{vol}(P(A)) \;=\; \sum_{a_1, \ldots, a_n \in A} L(P_{a_1}, \ldots, P_{a_n})\,. \tag{A.3.10}$$

Let $b_1, \ldots, b_n$ be any sequence with $b_i \in [n]$ and set $B := \{b_1, \ldots, b_n\}$. Then $L(P_{b_1}, \ldots, P_{b_n})$ occurs in the sum (A.3.10) if and only if $B \subset A$, and in that case, it appears with coefficient 1.

Expand the right hand side of (A.3.9) in terms of the function L using (A.3.10). Then for $b_1, \ldots, b_n \in [n]$ the term $L(P_{b_1}, \ldots, P_{b_n})$ occurs with coefficient

$$\sum_{B \subset A \subset [n]} (-1)^{n-|A|} \;=\; (1-1)^{n-|B|} \;=\; \begin{cases} 0 & \text{if } B \neq [n] \\ 1 & \text{if } B = [n] \end{cases}\,.$$

Thus the right hand side of (A.3.9) reduces to the sum of $L(P_{b_1}, \ldots, P_{b_n})$ for $b_1, \ldots, b_n$ distinct. Each of these $n!$ terms are equal by symmetry, which completes the proof. □

A.4. Complex analysis

We might need a little bit of this for Routh Hurwicz.

Bibliography

1. Saugata Basu, Richard Pollack, and Marie-Françoise Roy, *Algorithms in real algebraic geometry*, second ed., Algorithms and Computation in Mathematics, vol. 10, Springer-Verlag, Berlin, 2006.
2. M.C. Beltrametti, E. Carletti, D. Gallarati, and G. Monti Bragadin, *Lectures on curves, surfaces and projective varieties*, EMS Textbooks in Mathematics, European Mathematical Society (EMS), Zürich, 2009.
3. E. Bézout, *Théorie générale des équations algébriques*, Ph.-D. Pierres, 1779.
4. ———, *General theory of algebraic equations*, Princeton University Press, 2006, Translated from French original by Eric Feron.
5. B. Buchberger, *Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems*, Aequationes Math. **4** (1970), 374–383.
6. ———, *An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal*, J. Symbolic Comput. **41** (2006), no. 3-4, 475–511.
7. François Budan de Boislaurent, *Nouvelle méthode pour la résolution des équations numériques d'un degré quelconque*, Courcier, 1807.
8. D. Cox, J. Little, and D.l O'Shea, *Ideals, varieties, and algorithms*, third ed., Undergraduate Texts in Mathematics, Springer, New York, 2007.
9. D.A. Cox, *Stickelberger and the eigenvalue theorem*, `arXiv.org/2007:12573`, 2020.
10. D.A. Cox, J. Little, and D. O'Shea, *Using algebraic geometry*, second ed., Graduate Texts in Mathematics, vol. 185, Springer, New York, 2005.
11. Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann, Singular *4-1-2 — A computer algebra system for polynomial computations*, `http://www.singular.uni-kl.de`, 2019.
12. R. Descartes, *La géométrie*, 1637.
13. A. Dickenstein and I. Z. Emiris (eds.), *Solving polynomial equations*, Algorithms and Computation in Mathematics, vol. 14, Springer-Verlag, Berlin, 2005.
14. D. Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995, With a view toward algebraic geometry.
15. G. Ewald, *Combinatorial convexity and algebraic geometry*, Graduate Texts in Mathematics, vol. 168, Springer-Verlag, New York, 1996.
16. J.-C. Faugère, *FGb*, See `http://fgbrs.lip6.fr/jcf/Software/FGb/index.html`.
17. J. C. Faugère, P. Gianni, D. Lazard, and T. Mora, *Efficient computation of zero-dimensional Gröbner bases by change of ordering*, J. Symbolic Comput. **16** (1993), no. 4, 329–344.
18. Joseph Fourier, *Sur l'usage du théorème de Descartes dans la recherche des limites des racines*, Bulletin des Sciences (1820), 156–165.
19. D. R. Grayson and M. E. Stillman, *Macaulay2, a software system for research in algebraic geometry*, Available at `http://www.math.uiuc.edu/Macaulay2/`.
20. J. Harris, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 133, Springer-Verlag, New York, 1992, A first course.
21. R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.
22. H. Hironaka, *Resolution of singularities of an algebraic variety over a field of characteristic zero*, Ann. Math. **79** (1964), 109–326.

23. A. Holme, *A royal road to algebraic geometry*, Springer, Heidelberg, 2012.
24. K. Hulek, *Elementary algebraic geometry*, Student Mathematical Library, vol. 20, American Mathematical Society, Providence, RI, 2003, Translated from the 2000 German original by Helena Verrill.
25. János Kollár, *Sharp effective nullstellensatz*, J. Amer. Math. Soc. **1** (1988), no. 4, 963–975.
26. T. Y. Li, T. Sauer, and J. A. Yorke, *The cheater's homotopy: an efficient procedure for solving systems of polynomial equations*, SIAM J. Numer. Anal. **26** (1989), no. 5, 1241–1251.
27. F.S. Macaulay, *Some properties of enumeration in the theory of modular systems*, Proc. London Math. Soc. **26** (1927), 531–555.
28. D. Perrin, *Algebraic geometry*, Universitext, Springer-Verlag London Ltd., London, 2008, Translated from the 1995 French original by Catriona Maclean.
29. R. Schneider, *Convex bodies: The Brunn-Minkowski theory*, Encyclopedia of Mathematics and its Applications, vol. 44, Cambridge University Press, Cambridge, 1993.
30. I. R. Shafarevich, *Basic algebraic geometry. 1*, second ed., Springer-Verlag, Berlin, 1994, Varieties in projective space, Translated from the 1988 Russian edition and with notes by Miles Reid.
31. K. E. Smith, L. Kahanpää, P. Kekäläinen, and W. Traves, *An invitation to algebraic geometry*, Universitext, Springer-Verlag, New York, 2000.
32. Jacques Charles François Sturm, *Mémoire sur la résolution des équations numériques*, Bulletin des Sciences de Férussac **11** (1829), 419–425.
33. B. Sturmfels, *Solving systems of polynomial equations*, CBMS Regional Conference Series in Mathematics, vol. 97, Conference Board of the Mathematical Sciences, Washington, DC, 2002.
34. Thorsten Theobald, *Real algebraic geometry and optimization*, Graduate Studies in Mathematics, vol. 241, American Mathematical Society, Providence, RI, [2024] ©2024.
35. Oscar Zariski, *A new proof of Hilbert's Nullstellensatz*, Bull. Amer. Math. Soc. **53** (1947), 362–368.
36. G. M. Ziegler, *Lectures on polytopes*, Springer-Verlag, New York, 1995.