Chapter 1

Varieties

Outline:

1. Affine varieties and examples.
2. The basics of the algebra-geometry dictionary.
3. Define Zariski topology (Zariski open and closed sets)
4. Primary decomposition and decomposition into components. Combinatorial definition of dimension.
5. Regular functions. Complete the algebraic-geometric dictionary (equivalence of categories). A whisper about schemes.
6. Rational functions.
7. Projective Varieties
8. Do projection and elimination. Use it to define the dimension of a variety. Prove the weak Nullstellensatz.
9. Appendix on Algebra.

1.1 Affine Varieties

The richness of algebraic geometry as a mathematical discipline comes from the interplay of algebra and geometry, as its basic objects are both geometrical and algebraic. The vivid intuition of geometry is expressed with precision via the language of algebra. Symbolic and numeric manipulation of algebraic objects give practical tools for applications.

Let $\mathbb{F}$ be a field, which for us will be either the complex numbers $\mathbb{C}$, the real numbers $\mathbb{R}$, or the rational numbers $\mathbb{Q}$. These different fields have their individual strengths and weaknesses. The complex numbers are *algebraically closed*; every univariate polnomial has a complex root. Algebraic geometry works best when using an algebraically closed field, and most introductory texts restrict themselves to the complex numbers. However, quite often real number answers are needed, particularly 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.

The set of all n-tuples $(a_1, \ldots, a_n)$ of numbers in $\mathbb{F}$ is called *affine n-space* and written $\mathbb{A}^n$ or $\mathbb{A}^n_{\mathbb{F}}$ when we want to indicate our field. We write $\mathbb{A}^n$ rather than $\mathbb{F}^n$ to emphasize that we are not doing linear algebra. Let $x_1, \ldots, x_n$ be variables, which we regard as coordinate functions on $\mathbb{A}^n$ and write $\mathbb{F}[x_1, \ldots, x_n]$ for the ring of polynomials in the variables $x_1, \ldots, x_n$ with coefficients in the field $\mathbb{F}$. We may evaluate a polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ at a point $a \in \mathbb{A}^n$ to get a number $f(a) \in \mathbb{F}$, and so polynomials are also functions on $\mathbb{A}^n$. We make the main definition of this book.

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

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

This is a (affine) *subvariety* of $\mathbb{A}^n$ or simple a *variety*.

If X and Y are varieties with $Y \subset X$, then Y is a *subvariety* of X.

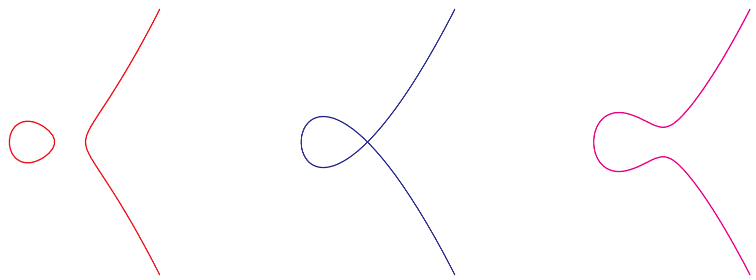
The empty set $\emptyset = \mathcal{V}(1)$ and affine space itself $\mathbb{A}^n = \mathcal{V}(0)$ are varieties. Any linear or affine subspace L of $\mathbb{A}^n$ is a variety. Indeed, L has an equation $Ax = b$, where A is a matrix and b is a vector, and so $L = \mathcal{V}(Ax - b)$ is defined by the linear polynomials which form the rows of $Ax - b$. An important special case of this is when $L = \{a\}$ is a point of $\mathbb{A}^n$. Writing $a = (a_1, \ldots, a_n)$, then L is defined by the equations $x_i - a_i = 0$ for $i = 1, \ldots, n$.

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

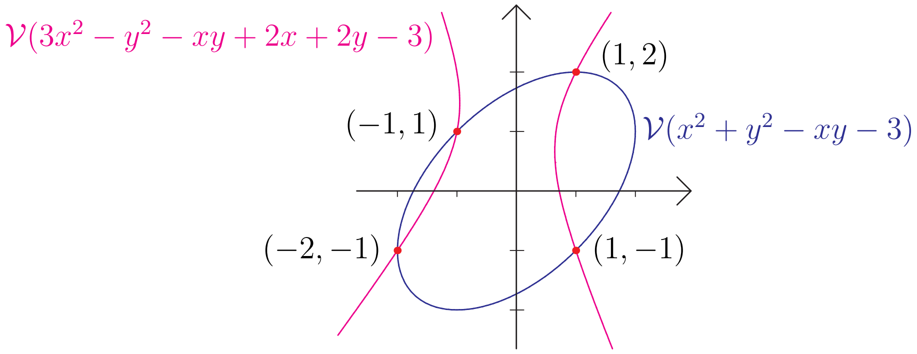
$$f \ := \ \prod_{z \in Z}(x - z)$$

is the monic polynomial with simple zeroes in Z.

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



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



A *quadric* is a variety defined by a single quadratic polynomial. In $\mathbb{A}^2$, these are the plane conics (circles, ellipses, parabolas, and hyperbolas in $\mathbb{R}^2$) and in $\mathbb{R}^3$, these are the spheres, ellipsoids, paraboloids, and hyperboloids. Figure 1.1 shows a hyperbolic paraboloid $\mathcal{V}(xy+z)$ and a hyperboloid of one sheet $\mathcal{V}(x^2-x+y^2+yz)$.

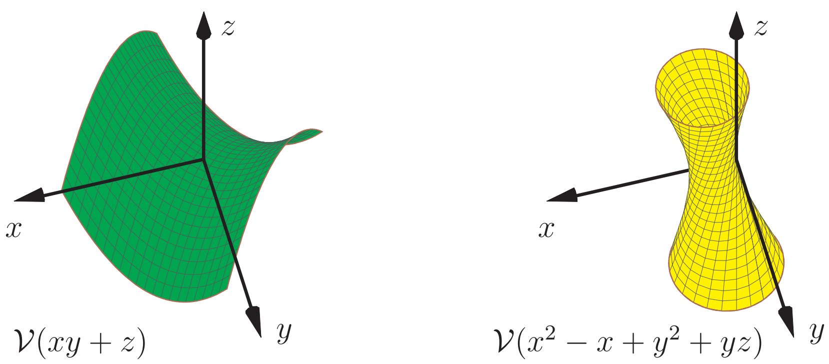


Figure 1.1: Two hyperboloids.

These last three examples, finite subsets of $\mathbb{A}^1$, 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 quadrics of Figure 1.1 meet in the variety $\mathcal{V}(xy+z,\, x^2-x+y^2+yz)$, which is shown on the right in Figure 1.2. 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 $(t^2,-t,t^3)$.

The intersection of the hyperboloid $x^2+(y-\frac{3}{2})^2-z^2=\frac{1}{4}$ with the sphere $x^2+y^2+z^2=4$ is a single space curve (drawn on the sphere). If we instead intersect the hyperboloid with the sphere centred at the origin having radius 1.9, then we obtain the space curve on the

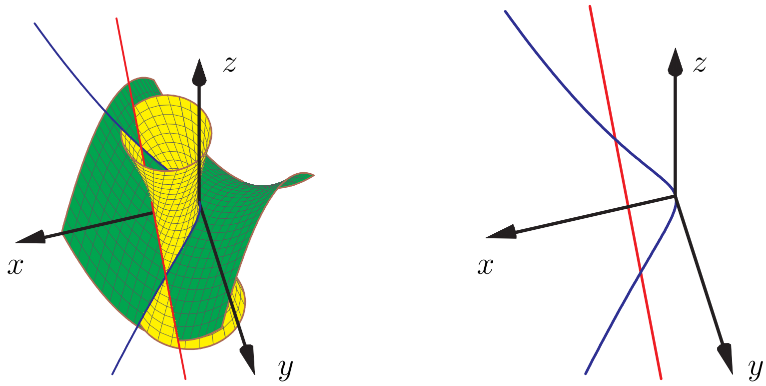
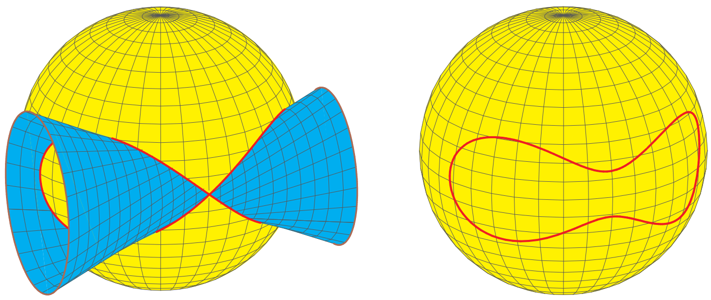


Figure 1.2: Intersection of two quadrics.

right below.



The product $V \times W$ of two varieties V and W is again a variety. Suppose that $V \subset \mathbb{A}^n$ is defined by the polynomials $f_1, \ldots, f_s \in \mathbb{F}[x_1, \ldots, x_n]$ and the variety $W \subset \mathbb{A}^m$ is defined by the polynomials $g_1, \ldots, g_t \in \mathbb{F}[y_1, \ldots, y_m]$. Then $X \times Y \subset \mathbb{A}^n \times \mathbb{A}^m = \mathbb{A}^{n+m}$ is defined by the polynomials $f_1, \ldots, f_s, g_1, \ldots, g_t \in \mathbb{F}[x_1, \ldots, x_n,\, y_1, \ldots, y_m]$.

The set $\mathrm{Mat}_{n\times n}$ or $\mathrm{Mat}_{n\times n}(\mathbb{F})$ of $n \times n$ matrices with entries in $\mathbb{F}$ is identified with the affine space $\mathbb{A}^{n^2}$. The *special linear group* is the set of matrices with determinant 1,

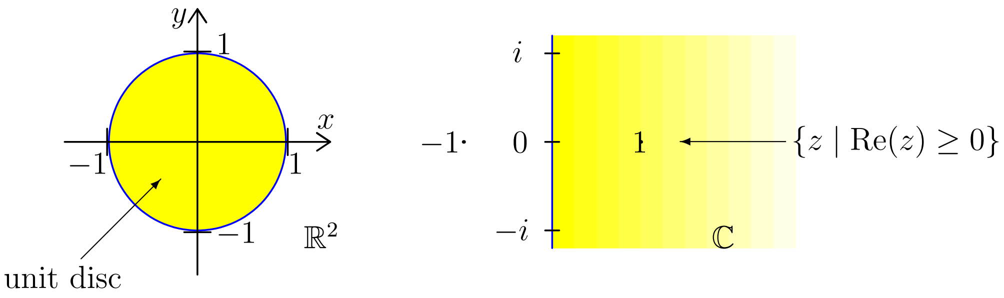
$$SL_n \;:=\; \{M \in \mathrm{Mat}_{n\times n} \mid \det M = 1\} \;=\; \mathcal{V}(\det -1)\,.$$

We will show that SL_n is smooth, irreducible, and has dimension $n^2 - 1$. (We must first, of course, define these notions.)

We also point out some subsets of $\mathbb{A}^n$ which are not varieties. The set $\mathbb{Z}$ of integers is not a variety. The only polynomial vanishing at every integer is the zero polynomial, whose variety is all of $\mathbb{A}^1$. The same is true for any other infinite subset of $\mathbb{A}^1$, for example, the infinite sequence $\{\frac{1}{n} \mid n = 1, 2, \ldots\}$ is not a subvariety of $\mathbb{A}^1$.

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.



Sets like these last two which are defined by inequalities involving real polynomials are called *semi-algebraic*. We will study them later.

1.2 The algebra-geometry dictionary I: ideal-variety correspondence

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

$$\mathcal{V}(S) \;=\; \{a \in \mathbb{A}^n \mid f(a) = 0 \text{ for all } f \in S\}\,.$$

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

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

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

These two inclusion-reversing maps

$$\{\text{Subsets } S \text{ of } \mathbb{F}[x_1,\ldots,x_n]\} \quad \underset{\mathcal{I}}{\overset{\mathcal{V}}{\rightleftarrows}} \quad \{\text{Subsets } Z \text{ of } \mathbb{A}^n\} \tag{1.1}$$

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 $I \subset \mathbb{F}[x_1,\ldots,x_n]$ which is closed under addition and under muntiplication by polynomials in $\mathbb{F}[x_1,\ldots,x_n]$: If $f,g \in I$ then $f+g \in I$ and if we also have $h \in \mathbb{F}[x_1,\ldots,x_n]$, then $hf \in I$. The ideal $\langle S\rangle$ generated by a subset S of $\mathbb{F}[x_1,\ldots,x_n]$ is the smallest ideal containing S. This is the set of all expressions of the form

$$h_1f_1 + \cdots + h_mf_m$$

where $f_1,\ldots,f_m \in S$ and $h_1,\ldots,h_m \in \mathbb{F}[x_1,\ldots,x_n]$. We work with ideals because of f, g, and h are polynomials and $a \in \mathbb{A}^n$ with $f(a) = g(a) = 0$, then $(f+g)(a) = 0$ and $(hf)(a) = 0$. Thus $\mathcal{V}(S) = \mathcal{V}(\langle S\rangle)$, and so we may restrict $\mathcal{V}$ to the ideals of $\mathbb{F}[x_1,\ldots,x_n]$. In fact, we lose nothing if we restrict the left-hand-side of the correspondence (1.1) to the ideals of $\mathbb{F}[x_1,\ldots,x_n]$.

Lemma 1.2.1 *For any subset S of $\mathbb{A}^n$, $\mathcal{I}(S)$ is an ideal of $\mathbb{F}[x_1, \ldots, x_n]$.*

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

When S 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 $\mathcal{I}$ of $\mathbb{F}[x_1, \ldots, x_n]$ is finitely generated.*

We defer the proof of this fundamental result until we discuss Gröbner bases. This result implies many important finiteness properties of algebraic varieties.†

Corollary 1.2.2 *Any variety $Z \subset \mathbb{A}^n$ is the intersection of finitely many hypersurfaces.*

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

Example. The ideal of the cubic space curve C of Figure 1.2 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 $y^3 + z$. These polynomials are not all 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,

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

Lemma 1.2.3 *For any subset Z of $\mathbb{A}^n$, 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 variety 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 is shown in Exercise 6. □

Thus we also lose nothing if we restrict the right-hand-side of the correspondence (1.1) to the subvarieties of $\mathbb{A}^n$. Our correspondence now becomes

$$\{\text{Ideals } I \text{ of } \mathbb{F}[x_1, \ldots, x_n]\} \quad \underset{\mathcal{I}}{\overset{\mathcal{V}}{\rightleftarrows}} \quad \{\text{Subvarieties } X \text{ of } \mathbb{A}^n\} \tag{1.2}$$

This association 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.

†There, outline a proof of the usual (induction on the number of variables) proof in the exercises.

For example, when $\mathbb{F} = \mathbb{Q}$ 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 $\mathbb{F} = \mathbb{R}$ 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) we will sometimes take positivity of polynomials into account.

The problem with the map $\mathcal{V}$ is more fundamental than these examples reveal and occurs even when $\mathbb{F} = \mathbb{C}$. 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

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

In both cases, the lack of injectivity of the map $\mathcal{V}$ boils down to f and f^m having the same set of zeroes, for any positive integer m. In particular, 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 if $f^m \in \mathcal{I}(Z)$, then $f \in \mathcal{I}(Z)$.

We clarify this point with a definition. An ideal $I \subset \mathbb{F}[x_1, \ldots, x_n]$ is *radical* if whenever $f^m \in I$ for some $m \geq 1$, then $f \in I$. The radical $\sqrt{I}$ of an ideal I of $\mathbb{F}[x_1, \ldots, x_n]$ is defined to be

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

This turns out to be an ideal. In fact it is the smallest radical ideal containing I. For example, we just showed that

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

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

Lemma 1.2.4 *For $Z \subset \mathbb{A}^n$, $\mathcal{I}(Z)$ is a radical ideal. If $I \subset \mathbb{F}[x_1, \ldots, x_n]$ is an ideal, then $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$.*

When $\mathbb{F}$ is algebraically closed, the precise nature of the correspondence (1.2) follows from Hilbert's Nullstellensatz (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 a weak form of the Nullstellensatz, which describes the ideals defining the empty set.

†Likely his 1890 paper, maybe the 1893 one.

Theorem 1.2.5 (Weak Nullstellensatz) *If $\mathcal{I}$ is an ideal of $\mathbb{C}[x_1,\ldots,x_n]$ with $\mathcal{V}(\mathcal{I}) = \emptyset$, then $\mathcal{I} = \mathbb{C}[x_1,\ldots,x_n]$.*

Let $a = (a_1,\ldots,a_n) \in \mathbb{A}^n$, which is defined by the linear polynomials $x_i - a_i$. A polynomial f is equal to the constant $f(a)$ modulo the ideal $\mathfrak{m}_a := \langle x_1 - a_1, \ldots, x_n - a_n\rangle$ generated by these polynomials, thus the quotient ring $\mathbb{F}[x_1,\ldots,x_n]/\mathfrak{m}_a$ is isomorphic to the field $\mathbb{F}$ and so $\mathfrak{m}_a$ is a maximal ideal. In the appendix we show that when $\mathbb{F} = \mathbb{C}$ (or any other algebraically closed field), these are the only maximal ideals.

Theorem 1.2.6 *The maximal ideals of $\mathbb{C}[x_1,\ldots,x_n]$ all have the form $\mathfrak{m}_a$ for some $a \in \mathbb{A}^n$.*

Proof of Weak Nullstellensatz. We prove the contrapositive, if $I \subsetneq \mathbb{C}[x_1,\ldots,x_n]$ is a proper ideal, then $\mathcal{V}(I) \neq \emptyset$. There is a maximal ideal $\mathfrak{m}_a$ with $a \in \mathbb{A}^n$ of $\mathbb{C}[x_1,\ldots,x_n]$ which contains I. But then

$$\{a\} \;=\; \mathcal{V}(\mathfrak{m}_a) \;\subset\; \mathcal{V}(I)\,,$$

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

We will later give a second proof that relies on geometric ideas.

The Fundamental Theorem of Algebra states that any nonconstant polynomial $f \in \mathbb{C}[x]$ has a root (a solution to $f(x) = 0$). We recast the weak Nullstellensatz as the multivariate fundamental thoerem of algebra.

Theorem 1.2.7 (Multivariate Fundamental Theorem of Algebra) *If the ideal generated by polynomials $f_1,\ldots,f_m \in \mathbb{C}[x_1,\ldots,x_n]$ is not the whole ring $\mathbb{C}[x_1,\ldots,x_n]$, then the system of polynomial equations*

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

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

We now deduce the full Nullstellensatz, which we will use to complete the characterization (1.2).

Theorem 1.2.8 (Nullstellensatz) *If $I \subset \mathbb{C}[x_1,\ldots,x_n]$ 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. Suppose that we have a polynomial $f \in \mathcal{I}(\mathcal{V}(I))$. Introduce a new variable t. Then the variety $\mathcal{V}(tf-1, I) \subset \mathbb{A}^{n+1}$ defined by I and $tf-1$ is empty. Indeed, if $(a_1,\ldots,a_n,b)$ were a point of this variety, then $(a_1,\ldots,a_n)$ would be a point of $\mathcal{V}(I)$. But then $f(a_1,\ldots,a_n) = 0$, and so the polynomial $tf-1$ evaluates to 1 at the point $(a_1,\ldots,a_n,b)$.

By the weak Nullstellensatz, $\langle tf-1, I\rangle = \mathbb{C}[x_1,\ldots,x_n,\, t]$. In particular, $1 \in \langle tf-1, I\rangle$, and so there exist polynomials $f_1,\ldots,f_m \in \mathcal{I}$ and $g, g_1,\ldots,g_m \in \mathbb{C}[x_1,\ldots,x_n,\, t]$ such that

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

If we apply the substitution $t = \frac{1}{f}$, then the first term with the factor $tf-1$ vanishes and each polynomial $g_i(x,t)$ becomes a rational function in $x_1,\ldots,x_n$ 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 $G_1,\ldots,G_m \in \mathbb{C}[x_1,\ldots,x_n]$. But this shows that $f \in \sqrt{\mathcal{I}}$, and completes the proof of the Nullstellensatz. ☐

Corollary 1.2.9 (Algebraic-Geometric Dictionary I) *The maps $\mathcal{V}$ and $\mathcal{I}$ give an inclusion reversing correspondence*

$$\left\{\begin{matrix}\textit{Radical ideals } \mathcal{I}\\ \textit{of } \mathbb{F}[x_1,\ldots,x_n]\end{matrix}\right\} \;\underset{\mathcal{I}}{\overset{\mathcal{V}}{\rightleftarrows}}\; \{\textit{Subvarieties } X \textit{ of } \mathbb{A}^n\} \tag{1.3}$$

with $\mathcal{V}(\mathcal{I}(X)) = X$. When $\mathbb{F} = \mathbb{C}$, 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 $\mathbb{A}^n$. In Lemma 1.2.3 we showed that $X = \mathcal{V}(\mathcal{I}(X))$. Thus $\mathcal{V}$ is onto and $\mathcal{I}$ is one-to-one.

Now suppose that $\mathbb{F} = \mathbb{C}$. 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. In particular, this shows that $\mathcal{I}$ and $\mathcal{V}$ are inverse bijections. ☐

Corollary 1.2.9 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

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

Lemma 1.2.10 *Let I, J be ideals in $\mathbb{F}[x_1,\ldots,x_n]$ and set $X := \mathcal{V}(I)$ and $Y = \mathcal{V}(J)$ to be their corresponding varieties. Then*

1. $\mathcal{V}(I+J) = X \cap Y$,
2. $\mathcal{I}(X\cap Y) = \sqrt{I+J}$,
3. $\mathcal{V}(I\cdot J) = \mathcal{V}(I\cap J) = X\cup Y$, *and*

4. $\mathcal{I}(X \cup Y) = \sqrt{I \cap J} = \sqrt{I \cdot J}$.

Example. It can happen that $I \cdot J \neq I \cap J$. For example, if $I = \langle xy - x^3 \rangle$ and $J = \langle y^2 - x^2y \rangle$, then $I \cdot J = \langle xy(y - x^2)^2 \rangle$, while $I \cap J = \langle xy(y - x^2) \rangle$.

This correspondence will be further refined in Section 1.5 to include maps between varieties. Because of this correspondence, each geometric concept has a corresponding algebraic concept, when $\mathbb{F} = \mathbb{C}$ is algebraically closed. When $\mathbb{F}$ is not algebraically closed, this correspondence is not exact. In that case we will often use algebra to guide our geometric definitions.

Exercises for Section 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 in $\mathcal{I}(S)$.)

2. Verify the claim in the text that smallest ideal containing a set $S \subset \mathbb{F}[x_1, \ldots, x_n]$ of polynomials 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 $h_1, \ldots, h_m \in \mathbb{F}[x_1, \ldots, x_n]$.

3. Prove that in $\mathbb{A}^2$, we have $\mathcal{V}(y - x^2) = \mathcal{V}(y^3 - y^2x^2, x^2y - x^4)$.

4. Express the cubic space curve C with parametrization (t, t^2, t^3) in each of the following ways.
   (a) The intersection of a quadric and a cubic hypersurface.
   (b) The intersection of two quadrics.
   (c) The intersection of three quadrics.

5. Let $\mathcal{I}$ be an ideal of $\mathbb{C}[x_1, \ldots, x_n]$. Show that
$$\sqrt{\mathcal{I}} \ := \ \{f \in \mathbb{F}[x_1, \ldots, x_n] \mid f^m \in \mathcal{I} \text{ for some } m \geq 1\}$$
is an ideal, is radical, and is the smallest radical ideal containing $\mathcal{I}$.

6. If $Y \subsetneq X$ are varieties, show that $\mathcal{I}(X) \subsetneq \mathcal{I}(Y)$.

7. Suppose that I and J are radical ideals. Show that $I \cap J$ is also a radical ideal.

8. Give radical ideals I and J for which $I + J$ is not radical.

9. Given ideals I and J show that $\{f \cdot g \mid f \in I \text{ and } g \in J\}$ is an ideal.

1.3 Generic properties of varieties

A useful feature in algebraic geometry is that many properties 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. We develop the terminology 'generic' and 'Zariski open' to describe this situation.

A starting point is that intersections and unions of affine varieties behave well.

Theorem 1.3.1 *The intersection of any collection of affine varieties is an affine variety. The union of any finite collection of affine varieties is an affine variety.*

Proof. For the first statement, let $\{I_t \mid t \in T\}$ be a collection of ideals in $\mathbb{F}[x_1, \ldots, x_n]$. Then 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 but that case is Lemma 1.2.10 (3). □

Theorem 1.3.1 shows that affine varieties have the same properties as the closed sets of a topology on $\mathbb{A}^n$. This was observed by Oscar Zariski.

Definition. We call an affine variety a *Zariski closed set*. The complement of a Zariski closed set is a *Zariski open set*. The *Zariski topology* on $\mathbb{A}^n$ is the topology whose closed sets are the affine varieties in $\mathbb{A}^n$. The *Zariski closure* of a subset $Z \subset \mathbb{A}^n$ is the smallest variety containing Z, which is $\mathcal{V}(\mathcal{I}(Z))$, by Lemma 1.2.3. Any subvariety X of $\mathbb{A}^n$ inherits its Zariski topology from $\mathbb{A}^n$, the closed subsets are simply the subvarieties of X. A subset $Z \subset X$ of a variety X is *Zariski dense* in X if its closure is X.

We emphasize that the purpose of this terminology is to aid our discussion of varieties, and not because we will use notions from topology in any essential way. This Zariski topology is behaves quite differently from the usual *Euclidean* topology on $\mathbb{R}^n$ or $\mathbb{C}^n$ with which we are familiar. A topology on a space may be defined by giving a collection of basic open sets which generate the topology—any open set is a union or a finite intersection of basic open sets. In the Euclidean topology, the basic open sets are balls. The *ball* with radius $\epsilon > 0$ centered at $z \in \mathbb{A}^n$is

$$B(z, \epsilon) \;:=\; \{a \in \mathbb{A}^n \mid \sum |a_i - z_i|^2 \;<\; \epsilon\}\,.$$

In the Zariski topology, the basic open sets are complements of hypersurfaces, called principal open sets.† Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ and set

$$U_f \;:=\; \{a \in \mathbb{A}^n \mid f(a) \neq 0\}\,.$$

†Is this the terminology you want?

In both these topologies the open sets are unions of basic open sets—we do not need intersections to generate the topology.

We give two examples to illustrate the Zariski topology.

Example. The Zariski closed subsets of $\mathbb{A}^1$ are the empty set, finite collections of points, and $\mathbb{A}^1$ itself. Thus when $\mathbb{F}$ is infinite the usual separation property of Hausdorff spaces (any two points are covered by two disjoint open sets) fails spectacularly as any two nonempty open sets meet.

Example. The Zariski topology on a product $X \times Y$ of affine varieties X and Y is in general not the product topology. In the product topology on $\mathbb{A}^2$, the closed sets are finite unions of sets of the following form: the empty set, points, vertical and horizontal lines of the form $\{a\} \times \mathbb{A}^1$ and $\mathbb{A}^1 \times \{a\}$, and the whole space $\mathbb{A}^2$. On the other hand, $\mathbb{A}^2$ contains a rich collection of 1-dimensional subvarieties (called *plane curves*), such as the cubic plane curves of Section 1.1.

We compare the Zariski topology with the Euclidean topology.

Theorem 1.3.2 *Suppose that $\mathbb{F}$ is one of $\mathbb{R}$ or $\mathbb{C}$. Then*

1. *A Zariski closed set is closed in the Euclidean topology on $\mathbb{A}^n$.*
2. *A Zariski open set is open in the Euclidean topology on $\mathbb{A}^n$.*
3. *A nonempty Euclidean open set is Zariski dense.*
4. *$\mathbb{R}^n$ is Zariski dense in $\mathbb{C}^n$.*
5. *A Zariski closed set is nowhere dense in the Euclidean topology on $\mathbb{A}^n$.*
6. *A nonempty Zariski open set is dense in the the Euclidean topology on $\mathbb{A}^n$.*

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 consider the case of a hypersurface $\mathcal{V}(f)$. But then Statement 1 (and hence also 2) follows as the polynomial function $f\colon \mathbb{A}^n \to \mathbb{F}$ is continuous in the Euclidean topology, and $\mathcal{V}(f) = f^{-1}(0)$.

We show that any ball $B(z, \epsilon)$ is Zariski dense. If a polynomial f vanishes identically on $B(z, \epsilon)$, then all of its partial derivaties do as well. This implies that its Taylor series expansion at z is identically zero. But then f is the zero polynomial. This shows that $\mathcal{I}(B) = \{0\}$, and so $\mathcal{V}(\mathcal{I}(B)) = \mathbb{A}^n$, that is, B is dense in the Zariski topology on $\mathbb{A}^n$.

For statement 4, we use 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 $\mathcal{V}(\mathcal{I}(\mathbb{R}^n)) = \mathbb{C}^n$.

For statements 5 and 6, observe that if f is nonconstant, then the interior of the (Euclidean) closed set $\mathcal{V}(f)$ is empty and so $\mathcal{V}(f)$ is nowhere dense. A subvariety is an intersection of nowhere dense hypersurfaces, so varieties are nowhere dense. The complement of a nowhere dense set is dense, so Zariski open sets are dense in $\mathbb{A}^n$. ☐

The last statement of Theorem 1.3.2 leads to the important notions of genericity and generic sets and properties.

Definition. Let X be a variety. A subset $Y \subset X$ is called *generic* if it contains a Zariski dense open subset of 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.

This notion of general depends on the context, and so care must be exercised in its use. For example, the general quadratic polynomial $ax^2 + bx + c$ 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 $b^2 - 4ac = 0$. 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, we will see that this is a very useful concept.

When $\mathbb{F}$ is $\mathbb{R}$ or $\mathbb{C}$, generic sets are dense in the Euclidean topology, by Theorem 1.3.2(6). Thus generic properties hold almost everywhere, in the standard sense.

Example. The generic $n \times n$ matrix is invertible, as it is a nonempty principal open subset of $\mathrm{Mat}_{n\times n} = \mathbb{A}^{n\times n}$. It is the complement of the variety $\mathcal{V}(\det)$ of singular matrices. Define the *general linear group GL_n* to be the set of all invertible matrices,

$$GL_n \ := \ \{M \in \mathrm{Mat}_{n\times n} \mid \det(M) \neq 0\} \ = \ U_{\det}\,.$$

Example. The general univariate polynomial of degree n has n distinct complex roots. Identify $\mathbb{A}^n$ with the set of univariate polynomials of degree n via

$$(a_1, \ldots, a_n) \ \in \ \mathbb{A}^n \ \longmapsto \ x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \ \in \ \mathbb{F}[x]\,. \qquad (1.4)$$

The classical discriminant $\Delta \in \mathbb{F}[a_1, \ldots, a_n]$ is a polynomial of degree $2n - 1$ which vanishes precisely when the polynomial (1.4) has a repeated factor. This identifies the set of polynomials with n distinct complex roots as the set U_Δ. The discriminant of a quadric $x^2 + bx + c$ is $b^2 - 4c$.

Example. The generic complex $n \times n$ matrix is semisimple (diagonalizable). Let $M \in \mathrm{Mat}_{n\times n}$ and consider the (monic) characteristic polynomial of M

$$\chi(x) \ := \ \det(xI_n - M)\,.$$

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. 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.

We see that the set of matrices with distinct eigenvalues equals the basic open set U_ψ, which is nonempty. Thus the set of semisimple matrices contains an open dense subset of $\mathrm{Mat}_{n\times n}$ set and is therefore generic.

When $n = 2$,

$$\det\left(xI_2 \;-\; \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}\right) \;=\; t^2 - t(a_{11} + a_{22}) + a_{11}a_{22} - a_{12}a_{21}\,,$$

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 1.3.3 *A set $X \subset \mathbb{A}^n$ is generic if and only if there is a nonconstant polynomial that vanishes on its complement.*

Exercises

1. Look up the definition of a topology in a text book and verify the claim that the collection of affine subvarieties of $\mathbb{A}^n$ form the closed sets in a topology on $\mathbb{A}^n$.

2. Prove that a closed set in the Zariski topology on $\mathbb{A}^1$ is either the empty set, a finite collection of points, or $\mathbb{A}^1$ itself.

3. Let $n \leq m$. Prove that a generic $n \times m$ matrix has rank n.

4. Prove that the generic triple of points in $\mathbb{A}^2$ are the vertices of a triangle.

1.4 Unique factorization for varieties

We establish a basic structure theorem for affine varieties which is an analog of unique factorization for polynomials. A polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ is *reducible* if we may factor f notrivially, that is, if $f = gh$ with neither g nor h a constant polynomial. Otherwise f is *irreducible*. Any polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ may be factored

$$f \;=\; g_1^{\alpha_1} g_2^{\alpha_2} \cdots g_m^{\alpha_m} \tag{1.5}$$

where the exponents α_i 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. This factorization is essentially unique as any other such factorization is obtained from this by permuting the factors and possibly multiplying each polynomial g_i by a constant. The polynomials g_j are *irreducible factors* of f.

This algebraic property has a consequence for the geometry of hypersurfaces. Suppose that a polynomial f is factored into irreducibles (1.5). Then the hypersurface $X = \mathcal{V}(f)$ is the union of hypersurfaces $X_i := \mathcal{V}(g_i)$, and this decomposition

$$X \;=\; X_1 \cup X_2 \cup \cdots \cup X_m$$

of X into hypersurfaces X_i defined by irreducible polynomials is unique.

This decomposition property is shared by general affine varieties.

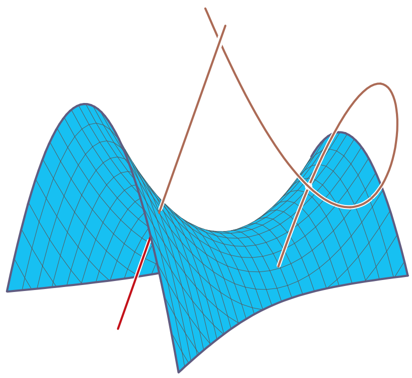
Definition. An affine variety X is *reducible* if it is the union $X = Y \cup Z$ of proper closed subvarieties $Y, Z \subsetneq X$. Otherwise X is *irreducible*. In particular, if an irreducible variety is written as a union of subvarieties $X = Y \cup Z$, then either $X = Y$ or $X = Z$.

Example. Figure 1.2 shows that the variety $\mathcal{V}(xy + z,\, x^2 - x + y^2 + yz)$ 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 see that $y + z = 0$ and these equations define the line in Figure 1.2. When $x = y^2$, we get $z = y^3$, and these equations define the cubic curve parametrized by (t^2, t, t^3).

Here is another reducible variety. It has three components, one is a surface and the other two are curves.



Theorem 1.4.1 *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

$$\begin{aligned} X_1 &= \{x \in X \mid \{x\} \times Y \subset Z_1\}\,, \quad \text{and} \\ X_2 &= \{x \in X \mid \{x\} \times Y \subset Z_2\}\,, \end{aligned}$$

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 $X \times Y = Z_1$.

We will show that X_1 is a subvariety of X. 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. An identical argument for X_2 completes the proof. □

The geometric notion of an irreducible variety corresponds to the algebraic notion of a prime ideal. An ideal $I \subset \mathbb{F}[x_1, \ldots, x_n]$ 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 1.4.2 *An affine variety X is irredicuble if and only if its ideal $\mathcal{I}(X)$ is prime.*

Proof. Let X be an affine variety and set $I := \mathcal{I}(X)$. First suppose that X is irreducible. Let $f, g \notin I$. Then neither f nor g vanishes identically on X. Thus $Y := X \cap \mathcal{V}(f)$ and $Z := X \cap \mathcal{V}(z)$ 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 $fg \notin I$.

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 $f \in \mathcal{I}(Y) - \mathcal{I}(X)$, a polynomial which vanishes on Y but not on X. Similarly, let $g \in \mathcal{I}(Z) - \mathcal{I}(X)$ be a polynomial which vanishes on Z but not on X. Since $X = Y \cup Z$, fg vanishes on X and therfore lies in $\mathcal{I}(X)$. This shows that I is not prime. □

We have seen examples of varieties with one, two, and three irreducible components. Taking products of distinct irreducible polynomials (or dually unions of distinct hypersurfaces), gives varieties having any finite number of irreducible components. This is all can occur as Hilbert's Basis Theorem implies that a variety is a union of finitely many irreducible varieties.

Lemma 1.4.3 *Any affine variety is a finite union of irreducible 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 are reducible, and continue this process, stopping only when all subvarieties obtained are irreducible. *A priori*, this process could continue indefinitely. We argue 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 one properly contained in the previous one,

$$X \supsetneq X_1 \supsetneq X_2 \supsetneq \cdots .$$

Their ideals form an infinite increasing chain of ideals in $\mathbb{F}[x_1, \ldots, x_n]$,

$$\mathcal{I}(X) \subsetneq \mathcal{I}(X_1) \subsetneq \mathcal{I}(X_2) \subsetneq \cdots .$$

The union I of these ideals is again an ideal. Note that no ideal $I(X_m)$ is equal to I. 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. □

A consequence of this proof is that any decreasing chain of subvarieties of a given variety must have finite length. There is however a bound for the length of the longest decreasing chain of irreducible subvarieties.

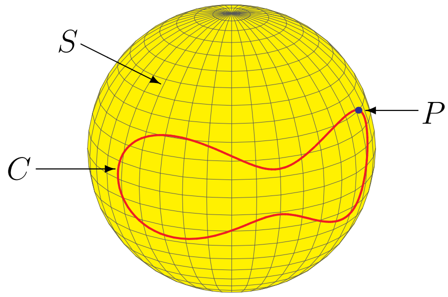
Combinatorial Definition of Dimension. The *dimension* of an irreducible variety X is given by the length of the longest decreasing chain of irreducible subvarieties of X. If

$$X \subset X_0 \supsetneq X_1 \supsetneq X_2 \supsetneq \cdots \supsetneq X_m \supsetneq \emptyset ,$$

is such a chain of maximal length, then X has dimension m.

Since maximal ideals of $\mathbb{C}[x_1, \ldots, x_n]$ necessarily have the form $\mathfrak{m}_a$, we see that X_m must be a point when $\mathbb{F} = \mathbb{C}$. The only problem with this definition is that we cannot yet show that it is well-founded, as we do not yet know that there is a bound on the length of such a chain. Later we shall prove that this definition is correct by relating it to other notions of dimension.

Example. The sphere S has dimenion at least two, as we have the chain of subvarieties $S \supsetneq C \supsetneq P$ as shown below.



It is quite challenging to show that any maximal chain of irreducble subvarieties of the sphere has length 2 with the tools that we have developed.

By Lemma 1.4.3, an affine variety X may be written as a finite union

$$X \;=\; X_1 \,\cup\, X_2 \,\cup\, \cdots \,\cup\, X_m$$

of irreducible subvarieties. We may assume that this is irredundant in that if $i \neq j$ then X_i is not a subvariety of 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 prove that this decomposition is unique, which is the main result of this section and a basic structural result about varieties.

Theorem 1.4.4 (Unique Decomposition of Varieites) *An affine variety X has a unique irredundant decomposition as a finite union of irreducible subvarieties*

$$X \;=\; X_1 \,\cup\, X_2 \,\cup\, \cdots \,\cup\, X_m\,.$$

We call these distinguished subvarieties X_i the *irreducible components* of X.

Proof. Suppose that we have another irredundant decomposition into irreducible subvarieties,

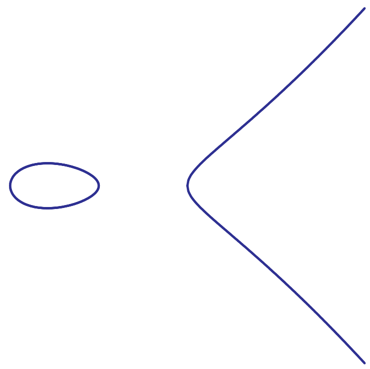
$$X \;=\; Y_1 \,\cup\, Y_2 \,\cup\, \cdots \,\cup\, Y_n\,,$$

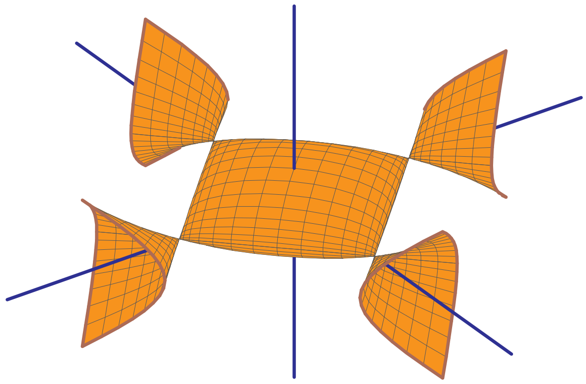
where each Y_i is irreducible. Then

$$X_i \;=\; (X_i \cap Y_1) \,\cup\, (X_i \cap Y_2) \,\cup\, \cdots \,\cup\, (X_i \cap Y_n)\,.$$

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 $Y_j \subset X_k$. Since this implies that $X_i \subset X_k$, we have $i = k$, 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. □

When $\mathbb{F} = \mathbb{C}$, we will show that an irreducible variety is connected in the ususal 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 irreducible cubic plane curve $\mathcal{V}(y^2 - x^3 + x)$ in $\mathbb{A}^2_{\mathbb{R}}$ and the surface $\mathcal{V}((x^2-y^2)^2 - 2x^2 - 2y^2 - 16z^2 + 1)$ in $\mathbb{A}^3_{\mathbb{R}}$.





Both are irreducible hypersurfaces. The first has two connected components in the Euclidean topology, while in the second, the five components of singular points meet at the four singular points.

Exercises

1. Show that the ideal of a hypersurface $\mathcal{V}(f)$ is generated by the *squarefree* part of f, which is the product of the irreducible factors of f, all with exponent 1.
2. For every positive integer n, give a decreasing chain of subvarieties of $\mathbb{A}^1$ of length $n{+}1$.
3. Prove that the dimension of a point is 0 and the dimension of $\mathbb{A}^1$ is 1.
4. Prove that the dimension of an irreducible plane curve is 1 and use this to show that the dimension of $\mathbb{A}^2$ is 2.
5. Write the ideal $\langle x^3 - x, x^2 - y\rangle$ as the intersection of two prime ideals. Decribe the correponding geometry.

[†]When and where will we show this?

1.5 The algebra-geometry dictionary II

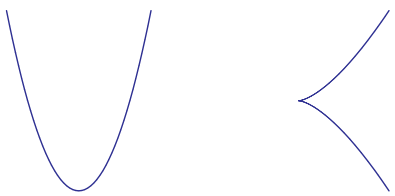
The algebra-geometry dictionary of Section 1.2 is strengthened when we include regular maps between varieties and the corresponding homomorphisms between rings of regular functions.

Let $X \subset \mathbb{A}^n$ be an affine variety. Any polynomial function $f \in \mathbb{F}[x_1, \ldots, x_n]$ restricts to give a *regular function* on X, $f\colon X \to \mathbb{F}$. We may add and multiply regular functions, and the set of all regular functions on X forms a ring, $\mathbb{F}[X]$, called the *coordinate ring* of the affine variety X or the ring of regular functions on X. The coordinate ring of an affine variety X is a basic invariant of X, which is, in fact equivalent to X itself.

The restriction of polynomial functions on $\mathbb{A}^n$ to regular functions on X defines a surjective ring homomorphism $\mathbb{F}[x_1, \ldots, x_n] \twoheadrightarrow \mathbb{F}[X]$. The kernel of this restriction homomorphism is the set of polynomials which 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 and isomorphism between $\mathbb{F}[X]$ and the quotient ring $\mathbb{F}[x_1, \ldots, x_n]/\mathcal{I}(X)$.

Example. The coordinate ring of the parabola $y = x^2$ is $\mathbb{F}[x, y]/\langle y - x^2\rangle$, which is isomorphic to $\mathbb{F}[x]$, the coordinate ring of $\mathbb{A}^1$. To see thia, observe that substituting x^2 for y rewrites and polynomial $f(x, y)$ as a polynomial $g(x)$ in x alone, and $y - x^2$ divides the difference $f(x, y) - g(x)$.

On the other hand, the coordinate ring of the semicubical parabola $y^2 = x^3$ is $\mathbb{F}[x, y]/\langle y^2 - x^3\rangle$. This ring is not isomorphic to the previous ring. For example, the element $y^2 = x^3$ has two factorizations into irreducible elements, while polynomials $\mathbb{F}[x]$ in one variable always factor uniquely



Parabola Semicubical Parabola

This quotient ring $\mathbb{F}[x_1, \ldots, x_n]/\mathcal{I}(X)$ is finitely generated by the images of the variables x_i. Since $\mathcal{I}(X)$ is radical, the quotient ring has no nilpotent elements (elements f such that $f^m = 0$ for some m) and is therefore reduced. When $\mathbb{F}$ is algebraically closed, these two properties characterize coordinate rings of algebraic varieties.

Theorem 1.5.1 *Suppose that $\mathbb{F}$ is algebraically closed. Then an $\mathbb{F}$ 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 $\mathbb{F}$ algebra R is the coordinate ring of an affine variety. Suppose that the reduced $\mathbb{F}$ algebra R has generators $r_1, \ldots, r_n$. Then there is a surjective ring homomorphism

$$\varphi \;:\; \mathbb{F}[x_1, \ldots, x_n] \longrightarrow\!\!\!\!\rightarrow \; R$$

given by $x_i \mapsto r_i$. Let $I \subset \mathbb{F}[x_1, \ldots, x_n]$ be the kernel of φ. This identifies R with $\mathbb{F}[x_1, \ldots, x_n]/I$. Since R is reduced, we see that I is radical.

When $\mathbb{F}$ is algebraically closed, the algebra-geometry dictionary of Corollary 1.2.9 shows that $I = \mathcal{I}(\mathcal{V}(I))$ and so $R \simeq \mathbb{F}[x_1, \ldots, x_n]/I \simeq \mathbb{F}[\mathcal{V}(I)]$. □

A different choice $s_1, \ldots, s_m$ of generators for R in this proof will give a different affine variety with coordinate ring R. One goal of this section is to understand this apparent ambiguity.

Example. Consider the finitely generated $\mathbb{F}$ algebra $R := \mathbb{F}[t]$. Chosing the generator t realizes R as $\mathbb{F}[\mathbb{A}^1]$. We could, however choose as generators $x := t + 1$ and $y := t^2 + 3t$. Since $y = x^2 + x - 2$, this also realizes R as $\mathbb{F}[x, y]/\langle y - x^2 - x + 2\rangle$, which is the coordinate ring of a parabola.

Among the coordinate rings $\mathbb{F}[X]$ of affine varieties are the polynomial algebras $\mathbb{F}[\mathbb{A}^n] = \mathbb{F}[x_1, \ldots, x_n]$. Many properties of polynomial algebras, including the algebra-geometry of Corollary 1.2.9 and the Hilbert Theorems hold for these coordinate ring $\mathbb{F}[X]$.

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

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

is a subvariety of X. Indeed, let $F_1, \ldots, F_m \in \mathbb{F}[x_1, \ldots, x_n]$ be polynomials which restrict to $f_1, \ldots, f_m$. Then

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

As in Section 1.2, we may extend this notation and define $\mathcal{V}(I)$ for an ideal I of $\mathbb{F}[X]$. 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 $\mathbb{F}[X] = \mathbb{F}[\mathbb{A}^n]/\mathcal{I}(X)$ of X. Write $\mathcal{I}(Y) \subset \mathbb{F}[X]$ for the ideal of Y in $\mathbb{F}[X]$.

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

Theorem 1.5.2 (Hilbert Theorems for $\mathbb{F}[X]$) *Let X be an affine variety. Then*

1. *Any ideal of $\mathbb{F}[X]$ is finitely generated.*

2. *If Y is a subvariety of X then $\mathcal{I}(Y) \subset \mathbb{F}[X]$ is a radical ideal. The subvariety Y is irreducible if and only if $I(Y)$ is a prime ideal.*

3. *Suppose that $\mathbb{F}$ is algebraically closed. An ideal I of $\mathbb{F}[X]$ defines the empty set if and only if $I = \mathbb{F}[X]$.*

In the same way 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 $\mathbb{F}[X]$. The proofs are the same, so we leave them to the reader. For this, you will need to recall that ideals J of a quotient ring R/I all have the form K/I, where K is an ideal of R which contains I.

Theorem 1.5.3 *Let X be an affine variety. Then the maps $\mathcal{V}$ and $\mathcal{I}$ give an inclusion reversing correspondence*

$$\{Radical\ ideals\ \mathcal{I}\ of\ \mathbb{F}[X]\} \quad \underset{\mathcal{I}}{\overset{\mathcal{V}}{\rightleftarrows}} \quad \{Subvarieties\ Y\ of\ X\} \tag{1.6}$$

with $\mathcal{I}$ injective and $\mathcal{V}$ surjective. When $\mathbb{F} = \mathbb{C}$, the maps $\mathcal{V}$ and $\mathcal{I}$ are inverses, and this correspondence is a bijection.

In algebraic geometry, we do not just study varieties, but also the maps between them.

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

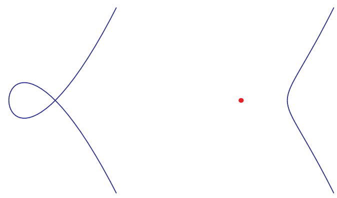
$$\begin{array}{rccl} \varphi\ : & X & \longrightarrow & \mathbb{A}^m \\ & x & \longmapsto & (f_1(x), f_2(x), \ldots, f_m(x))\,, \end{array}$$

which we call a *regular map*.

Example. The elements $t^2, t, t^3 \in \mathbb{F}[t] = \mathbb{F}[\mathbb{A}^1]$ define the map $\mathbb{A}^1 \to \mathbb{A}^3$ with image the cubic curve of Figure 1.1.

The elements t^2, t^3 of $\mathbb{F}[\mathbb{A}^1]$ define a map $\mathbb{A}^1 \to \mathbb{A}^2$ whose image is the cuspidal cubic that we saw earlier.

Let $x = t^2 - 1$ and $y = t^3 - t$, which are elements of $\mathbb{F}[t] = \mathbb{F}[\mathbb{A}^1]$. These define a map $\mathbb{A}^1 \to \mathbb{A}^2$ whose image is the 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 $\mathbb{A}^1 \to \mathbb{A}^2$ whose image is the curve on the right below.



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

Suppose that X is an affine variety and we have a regular map $\varphi\colon X \to \mathbb{A}^m$ given by regular functions $f_1, \ldots, f_m \in \mathbb{F}[X]$. A polynomial $g \in \mathbb{F}[x_1, \ldots, x_m] \in \mathbb{F}[A^m]$ *pulls back along φ* to give the regular function $\varphi^* g$, which is defined by

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

This is an element of the coordinate ring $\mathbb{F}[X]$ of X. This is the usual pull back of a function, for $x \in X$,

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

The resulting map $\varphi^*\colon \mathbb{F}[\mathbb{A}^m] \to \mathbb{F}[X]$ is a homomorphism of $\mathbb{F}$ algebras. Conversely, given a homomorphism $\psi\colon \mathbb{F}[x_1, \ldots, x_m] \to \mathbb{F}[X]$ of $\mathbb{F}$ algebras, if we set $f_i := \psi(x_i)$, then $f_1, \ldots, f_m \in \mathbb{F}[X]$ define a regular map φ with $\varphi^* = \psi$.

We have just shown the following basic fact.

Lemma 1.5.4 *The association $\varphi \mapsto \varphi^*$ defines a bijection*

$$\left\{\begin{matrix}\textit{regular maps}\\ \varphi\colon X \to \mathbb{A}^m\end{matrix}\right\} \quad\longleftrightarrow\quad \left\{\begin{matrix}\textit{ring homomorphisms}\\ \psi\colon \mathbb{F}[\mathbb{A}^m] \to \mathbb{F}[X]\end{matrix}\right\}$$

In the examples that we gave, the image $\varphi(X)$ of X under φ was contained in a subvariety. This is always the case.

Lemma 1.5.5 *Let X be an affine variety, $\varphi\colon X \to \mathbb{A}^m$ a regular map, and $Y \subset \mathbb{A}^m$ a subvariety. Then $\varphi(X) \subset Y$ if and only if $\mathcal{I}(Y) \subset \ker\varphi^*$.*

Proof. Suppose that $\varphi(X) \subset Y$. If $f \in \mathcal{I}(Y)$ then f vanishes on Y and hence on $\varphi(X)$. But then $\varphi^* f$ is the zero function. Thus $\mathcal{I}(Y) \subset \ker\varphi^*$.

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 $0 = \varphi^* f(x) = f(\varphi(x))$. Since this is true for every $f \in \mathcal{I}(Y)$, we conclude that $\varphi(x) \in Y$. Since this is true for every $x \in X$, we conclude that $\varphi(X) \subset Y$. □

Corollary 1.5.6 *Let X be an affine variety, $\varphi\colon X \to \mathbb{A}^m$ a regular map, and $Y \subset \mathbb{A}^m$ a subvariety. Then*

(1) $\ker\varphi^*$ *is a radical ideal.*

(2) *If X is irreducible, then* $\ker\varphi^*$ *is a prime ideal.*

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

(4) *If $\varphi\colon X \to Y$, then $\varphi^*\colon \mathbb{F}[Y] \to \mathbb{F}[X]$.*

Proof. For (1), suppose that $f^m \in \ker\varphi^*$, so that $0 = \varphi^*(f^m) = (\varphi(f))^m$. Since $\mathbb{F}[X]$ has no nilpotent elements, we conclude that $\varphi(f) = 0$ and so $f \in \ker\varphi^*$.[†]

For (2), suppose that $f\cdot g \in \ker\varphi^*$ with $g \notin \ker\varphi^*$. Then $0 = \varphi^*(f\cdot g) = \varphi^*(f)\cdot\varphi^*(g)$ in $\mathbb{F}[X]$, but $0 \neq \varphi^*(g)$. Since $\mathbb{F}[X]$ is a domain, we must have $0 = \varphi^*(f)$ and so $f \in \ker\varphi^*$, which shows that $\ker\varphi^*$ is a prime ideal.

[†]Mabe we should do these in the Appendix and just quote them from there.

Suppose that Y is an affine variety containing $\varphi(X)$. By Lemma 1.5.5 $\mathcal{I}(Y) \subset \ker \varphi^*$ and so $\mathcal{V}(\ker \varphi^*) \subset Y$. Statement (3) follows as we also have $X \subset \mathcal{V}(\ker \varphi^*)$.

For (4), we have $\mathcal{I}(Y) \subset \ker \varphi^*$ and so the map $\varphi^* \colon \mathbb{F}[\mathbb{A}^1] \to \mathbb{F}[X]$ factors through the quotient map $\mathbb{F}[\mathbb{A}^1] \twoheadrightarrow \mathbb{F}[\mathbb{A}^1]/\mathcal{I}(Y)$. reword this better! Maybe do this last one in the text? □

Thus we may refine the correspondence of Lemma 1.5.4. Let X and Y be affine varieties. Then $\varphi \mapsto \varphi^*$ gives a bijective correspondence

$$\left\{\begin{array}{l}\text{regular}\\ \text{maps}\\ \varphi\colon X \to Y\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{ring homomorphisms}\\ \psi\colon \mathbb{F}[Y] \to \mathbb{F}[X]\end{array}\right\}$$

This map $X \mapsto \mathbb{F}[X]$ from affine varieties to finitely generated $\mathbb{F}$ algebras without nilpotents not only maps objects to objects, but is an isomorphism on maps between objects. In mathematics, such an association is called a *contravariant equivalence of categories*.

The prototypical example of this comes from linear algebra. To a finite-dimensional vector space V, we may associate its dual space V^*. Given a linear transformation $L\colon V \to W$, its adjoint is a map $L^*\colon W^* \to V^*$. Since $(V^*)^* = V$ and $(L^*)^* = L$, this association is a bijection on the objects (finite-dimensional vector spaces) and a bijection on linear maps linear maps from V to W.

Need to discuss more about the equivalence of categories, and then make a whisper about schemes.

1. Give a proof of Theorem 1.5.2.

2. Show that a regular map $\varphi\colon X \to Y$ is continuous in the Zariski topology.

1.6 Rational functions

1.7 Smooth and singular points

1.8 Projective varieties

Notes

At the end of chapters, we should have a section on notes which describes some of the history, etc. In this chapter, we need only discuss some other sources for Algebraic Geometry and maybe Hilbert's breakthroughs.