0 Geometry and Algebra

Algebraic geometry studies zeros of multivariate polynomials. To begin, we introduce the geometric manifestations for the solutions of a system of polynomial equations.

The set $\mathbb{N} := \{0, 1, 2, \dots\}$ of nonnegative integers contains zero. Throughout, $\mathbb{K}$ denotes an arbitrary field. Familiar fields include the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$, the rational numbers $\mathbb{Q}$, and the finite field $\mathbb{F}_p := \mathbb{Z}/\langle p \rangle$ where p is a prime integer.

Unlike $\mathbb{R}$ and $\mathbb{C}$, both $\mathbb{Q}$ and $\mathbb{F}_p$ are computable fields—operations are effectively implemented in computer algebra systems.

0.0 Affine Space

What is the basic ambient space in algebraic geometry?

0.0.0 Definition. A *monomial* is a product of powers of variables with nonnegative integer exponents. Given the variables $x_1, x_2, \dots, x_n$, a monomial has the form $x^u := x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n}$ for some exponent vector $u := (u_1, u_2, \dots, u_n) \in \mathbb{N}^n$. The *total degree* of this monomial is the sum $|u| := u_1 + u_2 + \cdots + u_n$.

The constant $1 := x_1^0 x_2^0 \cdots x_n^0$ is a monomial. It is also the empty product of variables.

A *polynomial* f in the variables $x_1, x_2, \dots, x_n$ with coefficients in the field $\mathbb{K}$ is a finite linear combination of monomials:

$$f := \sum_{u \in \mathbb{N}^n} a_u \, x^u$$

where $a_u \in \mathbb{K}$ and only finitely many *coefficients* a_u are nonzero. The set of all such polynomials is denoted by $S := \mathbb{K}[x_1, x_2, \dots, x_n]$. Both addition and multiplication of polynomials are defined termwise

$$\left(\sum_{u \in \mathbb{N}^n} a_u \, x^u \right) + \left(\sum_{v \in \mathbb{N}^n} b_v \, x^v \right) = \sum_{u \in \mathbb{N}^n} (a_u + b_v) \, x^u$$

$$\left(\sum_{u \in \mathbb{N}^n} a_u \, x^u \right) \left(\sum_{v \in \mathbb{N}^n} b_v \, x^v \right) = \sum_{u \in \mathbb{N}^n} \left(\sum_{v \in \mathbb{N}^n} a_v \, b_{u-v} \right) x^u \, .$$

In the ring S, the additive identity is

$$0_S := \sum_{u \in \mathbb{N}^n} 0 \, x^u$$

and the multiplicative identity is

$$1_S := 1 + \sum_{0 \neq u \in \mathbb{N}^n} 0 \, x^u \, .$$

The coefficient field $\mathbb{K}$ embeds into S by sending $a \in \mathbb{K}$ to $a \, 1 := a$.

Equipped with these operations, one verifies that the *polynomial ring* $S := \mathbb{K}[x_1, x_2, \dots, x_n]$ is a commutative $\mathbb{K}$-algebra.

For a nonzero coefficient a_u, the product $a_u \, x^u$ is a *term* of f. The *total degree* of a nonzero polynomial f in S is the maximum $|u|$ among the nonzero coefficients a_u. A polynomial is *homogeneous* if its nonzero terms all have the same total degree.

When dealing with polynomials in a small number of variables, we usually dispense with subscripts. For example, $\mathbb{K}[w, x, y, z]$ is a polynomial ring in four variables.

0.0.1 Example. The homogeneous polynomial $xyz + 3y^2z - 7wz^2$ in $\mathbb{Q}[w,x,y,z]$ has 3 terms and total degree 3. ◇

0.0.2 Definition. For any nonnegative integer n, the n-dimensional *affine space* over a field $\mathbb{K}$ is the set

$$\mathbb{A}^n = \mathbb{A}^n(\mathbb{K}) := \left\{ (a_1, a_2, \dots, a_n) \;\middle|\; a_i \in \mathbb{K} \text{ for all } 1 \leqslant i \leqslant n \right\}.$$

We use the terminology "affine space" to emphasize the geometry rather than the algebraic properties of the $\mathbb{K}$-vector space $\mathbb{K}^n$. In affine space, the origin has no special role.

Elements in the polynomial ring $S := \mathbb{K}[x_1, x_2, \dots, x_n]$ are regarded as functions on the affine space $\mathbb{A}^n$. Is the zero polynomial the same as the zero function?

0.0.3 Proposition. *Let $\mathbb{K}$ be an infinite field and let n be a nonnegative integer. A polynomial f in $S := \mathbb{K}[x_1, x_2, \dots, x_n]$ is zero if and only if the function $f \colon \mathbb{A}^n \to \mathbb{K}$, defined by evaluation, is zero.*

Proof. Since its evaluation at any point is zero, the zero polynomial gives a zero function. For the converse, we must show that f is the zero polynomial when $f(a_1, a_2, \dots, a_n) = 0$ for all $(a_1, a_2, \dots, a_n) \in \mathbb{A}^n$. We proceed by induction on n.

The case $n = 0$ is trivial. When $n = 1$, a nonzero polynomial in $\mathbb{K}[x]$ of degree m has at most m distinct roots. By assumption, we have $f(a) = 0$ for all $a \in \mathbb{K}$. Since $\mathbb{K}$ is infinite, this means f has infinitely many roots which implies that f is the zero polynomial.

Assume the claim holds for $n-1$ and let f be a polynomial in $\mathbb{K}[x_1, x_2, \dots, x_n]$ that vanishes at all points in $\mathbb{A}^n$. Express f in the form $f = \sum_{i \in \mathbb{N}} g_i \, x_n^i$ where $g_i \in \mathbb{K}[x_1, x_2, \dots, x_{n-1}]$. Fixing a point $(a_1, a_2, \dots, a_{n-1})$ in $\mathbb{A}^{n-1}$, the partial evaluation $f(a_1, a_2, \dots, a_{n-1}, x_n)$ lies in $\mathbb{K}[x_n]$. By hypothesis, the polynomial $f(a_1, a_2, \dots, a_{n-1}, x_n)$ vanishes when $x_n = a_n$ for any a_n in $\mathbb{K}$. The base case of the induction establishes that $f(a_1, a_2 \dots, a_{n-1}, x_n)$ is the zero polynomial, whence $g_i(a_1, a_2, \dots, a_{n-1}) = 0$ for all $i \in \mathbb{N}$. Since $(a_1, a_2, \dots, a_{n-1})$ in $\mathbb{A}^{n-1}$ is an arbitrary point, the induction hypothesis guarantees that each g_i is the zero polynomial, so we have $f = 0$. □

0.0.4 Corollary. *Let $\mathbb{K}$ be an infinite field and let n be a nonnegative integer. Consider two polynomials f and g in $S := \mathbb{K}[x_1, x_2, \dots, x_n]$. We have the equality $f = g$ if and only if the functions $f \colon \mathbb{A}^n \to \mathbb{K}$ and $g \colon \mathbb{A}^n \to \mathbb{K}$, defined by evaluation, are equal.*

Proof. Apply Proposition 0.0.3 to the difference $f - g$. □

0.1 Affine Subvarieties

What are the basic geometry objects in algebraic geometry?

0.1.0 Definition. An *affine subvariety* is the set of the common zeroes for a collection of polynomials. For any field $\mathbb{K}$ and any nonnegative

This definition is extrinsic; it depends on the choice of an ambient space.

integers m and n, the affine subvariety defined by the polynomials $f_1, f_2, \dots, f_m$ in the ring $S := \mathbb{K}[x_1, x_2, \dots, x_n]$ is

$$\mathrm{V}(f_1, f_2, \dots, f_m) := \left\{ (a_1, a_2, \dots, a_n) \in \mathbb{A}^n \;\middle|\; f_i(a_1, a_2, \dots, a_n) = 0 \text{ for all } 1 \leqslant i \leqslant m \right\}.$$

We illustrate this fundamental concept with several examples.

0.1.1 Examples.

- Both $\mathbb{A}^n = \mathrm{V}(0)$ and $\varnothing = \mathrm{V}(1)$ are affine subvarieties.
- The singleton $\{(a_1, a_2 \dots, a_n)\}$ is $\mathrm{V}(x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$.
- Any individual affine subvariety is determined by more than one collection of polynomials. For instance, we have

$$\begin{aligned} \big\{(1,1),(2,3)\big\} &= \mathrm{V}(2x - y - 1, x^2 - 3x + 2) \\ &= \mathrm{V}(2x - y - 1, y^2 - 4y + 3)\,. \end{aligned}$$

- The z-axis in $\mathbb{A}^3$ is $\mathrm{V}(x, y)$. Moreover, any coordinate subspace is an affine subvariety defined by a subset of the variables.
- The zero set of a single polynomial is a *hypersurface*.
- The zero set of a linear (degree-one) polynomial is a *hyperplane*. For any a, b, c, d in $\mathbb{K}$, the line defined by $a\,x + b\,y = c$ in $\mathbb{A}^2$ and the plane defined by $a\,x + b\,y + c\,z = d$ in $\mathbb{A}^3$ are hyperplanes.
- A *linear subspace* is the common zeroes of linear polynomials.
- The set of all $(n \times n)$-matrices can be identified with $\mathbb{A}^{n^2}$. The subset $\mathrm{SL}(n, \mathbb{K})$ of matrices having determinant 1 forms an affine subvariety. It is the hypersurface determined by the polynomial

$$\det\left(\begin{bmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,n} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n,1} & x_{n,2} & \cdots & x_{n,n} \end{bmatrix} \right) - 1\,.$$

- A *determinantal variety* is an affine subvariety in $\mathbb{A}^{mn}$ formed by $(m \times n)$-matrices of rank at most r. When $r \geqslant \min(m, n)$, this variety is $\mathbb{A}^{mn}$. For any $r < \min(m, n)$, the rank of a matrix is at most r if and only if its $(r+1) \times (r+1)$ subdeterminants vanish. Because the subdeterminants are polynomials, the set of matrices of rank at most r do determine an affine subvariety. $\diamond$

0.1.2 Examples (Counterexamples)**.**

- Since a nonzero polynomial has finitely many roots, neither $\mathbb{N}$ nor $\mathbb{Z}$ are affine subvarieties in $\mathbb{A}^1(\mathbb{C})$.
- Since polynomials are holomorphic functions, a closed ball with positive radius in $\mathbb{A}^n(\mathbb{C})$ is not an affine subvariety. $\diamond$

In complex analysis, the identity theorem establishes that two entire functions that agree on a subset with an accumulation point are equal.

Affine subvarieties are compatible with finite unions and arbitrary intersections.

0.1.3 Lemma. *The union of two affine subvarieties is an affine subvariety. The intersection of any family of affine subvarieties is an affine subvariety.*

Proof. First, for any $X := \mathrm{V}(f_1, f_2, \dots, f_\ell)$ and $Y := \mathrm{V}(g_1, g_2, \dots, g_m)$ in $\mathbb{A}^n$, we show that $X \cup Y = \mathrm{V}(f_i\, g_j \mid 1 \leqslant i \leqslant \ell \text{ and } 1 \leqslant j \leqslant m)$ by proving containment in both directions.

$\subseteq$: Given a point a in $X \cup Y$, it follows that either $a \in X$ or $a \in Y$, so a is a zero of each product $f_i\, g_j$.

$\supseteq$: Suppose that $a \in \mathrm{V}(f_i\, g_j)$ and $a \not\in X$. Hence, there exists an index i such that $f_i(a) \neq 0$. For any index j, the polynomial $f_i\, g_j$ vanishes at a, so $g_j(a) = 0$ and $a \in Y$.

Next, consider a family $\mathrm{V}(f_{\beta,1}, f_{\beta,2}, \dots, f_{\beta,m_\beta})$ of affine subvarieties in $\mathbb{A}^n$, where $\beta \in \mathcal{B}$ and $\mathcal{B}$ is an arbitrary index set. It follows that

$$\begin{aligned}
&\mathrm{V}\Big(\textstyle\bigcup_{\beta \in \mathcal{B}} \{f_{\beta,1}, f_{\beta,2}, \dots, f_{\beta,m_\beta}\}\Big) \\
&= \Big\{a \in \mathbb{A}^n \;\Big|\; f(a) = 0 \text{ for all } f \in \textstyle\bigcup_{\beta \in \mathcal{B}} \{f_{\beta,1}, f_{\beta,2}, \dots, f_{\beta,m_\beta}\}\Big\} \\
&= \textstyle\bigcap_{\beta \in \mathcal{B}} \{a \in \mathbb{A}^n \mid f(a) = 0 \text{ for all } f \in \{f_{\beta,1}, f_{\beta,2}, \dots, f_{\beta,m_\beta}\}\} \\
&= \textstyle\bigcap_{\beta \in \mathcal{B}} \mathrm{V}(f_{\beta,1}, f_{\beta,2}, \dots, f_{\beta,m_\beta}) \,.
\end{aligned}$$ □

0.1.4 Example. The *twisted cubic curve* in $\mathbb{A}^3$ is the intersection of two hypersurfaces: $\mathrm{V}(x^2 - y, x^3 - z) = \mathrm{V}(x^2 - y) \cap \mathrm{V}(x^2 - z)$. The union of the yz-plane and the x-axis in $\mathbb{A}^3$ is $\mathrm{V}(xy, xz) = \mathrm{V}(x) \cup \mathrm{V}(y, z)$ ◇

0.1.5 Definition. The first part of Example 0.1.1 and Lemma 0.1.3 prove that affine subvarieties in $\mathbb{A}^n$ satisfy the axioms for closed sets in a topological space, called the *Zariski topology*. Each Zariski open set is the complement of an affine subvariety.

This topology is named after Oscar Zariski (1899–1986), who championed the use of modern algebra in algebraic geometry.

We can describe the Zariski topology on complex affine line $\mathbb{A}^1(\mathbb{C})$.

0.1.6 Example. Every ideal in the univariate polynomial ring $\mathbb{C}[x]$ is principal, so every affine variety is a hypersurface. Since the field $\mathbb{C}$ is algebraically closed, every nonzero polynomial f in $\mathbb{C}[x]$ factors as $a_0(x - a_1)(x - a_2)\cdots(x - a_d)$ for some nonnegative integer d and some complex numbers $a_0, a_1, \dots, a_d$. It follows that $\mathrm{V}(f) = \{a_1, a_2, \dots, a_d\}$. Thus, the affine varieties in $\mathbb{A}^1(\mathbb{C})$ are the finite subsets (including the empty set) and the whole space. The open sets in $\mathbb{A}^1(\mathbb{C})$ are the empty set and the complements of finite subsets. In particular, the Zariski topology is coarser than the Euclidean topology and the Zariski topology is not Hausdorff. ◇

The structure of an affine subvariety depends on the base field. The set of rational numbers $\mathbb{Q}$ is an affine variety in $\mathbb{A}^1(\mathbb{Q})$, but not when it is viewed as a subset of $\mathbb{A}^1(\mathbb{R})$ or $\mathbb{A}^1(\mathbb{C})$.

0.1.7 Definition. A topological space is *irreducible* if it is not the union of two proper closed subsets.

The empty set is not irreducible.

0.1.8 Example. The affine line $\mathbb{A}^1(\mathbb{C})$ is irreducible because its only proper closed subsets are finite, yet it is infinite. ◇

0.2 Parametrization

How can we describe the points in an affine subvariety?

0.2.0 Example. Consider the line $\mathrm{V}(x+y+z-1, x+2y-z-3)$ in $\mathbb{A}^3$ given as the intersection of two planes. The points in this linear subspace may also be described algebraically. Since we have

The row reduction algorithm allows one to parametrize linear subspaces.

$$\left\{\begin{aligned} x + y + z &= 1 \\ x + 2y - z &= 3 \end{aligned}\right\} \Leftrightarrow \left\{\begin{aligned} x \phantom{{}-2y} + 3z &= -1 \\ y - 2z &= 2 \end{aligned}\right\},$$

all the points on the line are given, for some $t \in \mathbb{K}$, by $x = -1 - 3t$, $y = 2 + 2t$, and $z = t$. This is a parametrization of the line. $\diamond$

0.2.1 Definition. A *rational function* in the variables $t_1, t_2, \dots, t_m$ with coefficients in $\mathbb{K}$ is a quotient f/g where f and g are polynomials in $\mathbb{K}[t_1, t_2, \dots, t_m]$, and g is nonzero. Two rational functions f_1/g_1 and f_2/g_2 are equal if $f_1\,g_2 = f_2\,g_1$ in $\mathbb{K}[t_1, t_2, \dots, t_m]$. The set of all rational functions in variables $t_1, t_2, \dots, t_m$ with coefficients in $\mathbb{K}$ is denoted by $\mathbb{K}(t_1, t_2, \dots, t_m)$; it is the fraction field of the polynomial ring $\mathbb{K}[t_1, t_2, \dots, t_m]$.

0.2.2 Example. Consider $X = \mathrm{V}(x^2 + y^2 - 1) \subset \mathbb{A}^2(\mathbb{R})$. A common way to parametrize the unit circle involves the trigonometric functions $x = \cos(t)$ and $y = \sin(t)$. However, there is also an algebraic way. Since $\lim\limits_{t \to \pm\infty} (1 - t^2)/(1 + t^2) = -1$, $\lim\limits_{t \to \pm\infty} 2t/(1 + t^2) = 0$, and

$$\left(\frac{1 - t^2}{1 + t^2}\right)^2 + \left(\frac{2t}{1 + t^2}\right)^2 = \frac{1 - 2t^2 + t^4 + 4t^2}{(1 + t^2)^2} = \frac{(1 + t^2)^2}{(1 + t^2)^2} = 1$$

we see that $X \setminus \{(-1, 0)\} = \left\{ \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) \;\middle|\; t \in \mathbb{A}^1(\mathbb{R}) \right\}$. $\diamond$

0.2.3 Definition. The *rational map* $\rho \colon \mathbb{A}^m \dashrightarrow \mathbb{A}^n$ is determined by an assignment $(t_1, t_2, \dots, t_m) \mapsto (\rho_1, \rho_2, \dots, \rho_n)$ where ρ_j, for any index j, is a rational function in $\mathbb{K}(t_1, t_2, \dots, t_m)$. We use the dashed arrow because a rational map need not give a well-defined function from $\mathbb{A}^m$ to $\mathbb{A}^n$. When $\rho_j = f_j/g_j$ for some relatively prime polynomials f_j and g_j in $\mathbb{K}[t_1, t_2, \dots, t_m]$, the rational map ρ is not well-defined at the points where any of the $g_j = 0$. Nevertheless, over the Zariski open subset $U := \mathbb{A}^m \setminus \mathrm{V}(g_1, g_2, \dots, g_n)$, we get a function $\rho \colon U \to \mathbb{A}^n$.

Can the image of a rational map be described by polynomials?

0.2.4 Definition. Let W be a subset of $\mathbb{A}^n$. The *Zariski closure* of W, denoted $\overline{W}$, is the smallest affine subvariety in $\mathbb{A}^n$ containing W. Thus, $\overline{W}$ is the intersection of all the closed subsets containing W.

0.2.5 Problem (Implicitization). For any subset $W \subseteq \mathbb{A}^m$ and any rational map $\rho \colon \mathbb{A}^m \dashrightarrow \mathbb{A}^n$, find polynomials $f_1, f_2 \dots, f_\ell$ in $\mathbb{K}[x_1, x_2, \dots, x_n]$ such that $\overline{\rho(W)} = \mathrm{V}(f_1, f_2, \dots, f_\ell)$.

0.2.6 Example. Consider the polynomial map $\rho\colon \mathbb{A}^2 \to \mathbb{A}^3$ defined by $(s,t) \mapsto (s+t, s-t, s+2t)$. It follows that

$$\left\{\begin{aligned} x &= s+t \\ y &= s-t \\ z &= s+2t \end{aligned}\right\} \Leftrightarrow \left\{\begin{aligned} s+t-x &= 0 \\ s-t-y &= 0 \\ s+2t-z &= 0 \end{aligned}\right\}$$

$$\Leftrightarrow \left\{\begin{aligned} s+t-x &= 0 \\ -2t+x-y &= 0 \\ t+x-z &= 0 \end{aligned}\right\} \Leftrightarrow \left\{\begin{aligned} s+t-x &= 0 \\ t+x-z &= 0 \\ 3x-y-2z &= 0 \end{aligned}\right\}$$

Hence, the image is the hyperplane $\mathrm{V}(3x-y-2z) \subset \mathbb{A}^3$. ◇

0.2.7 Example. For any nonnegative integer n, let $\rho\colon \mathbb{A}^2 \to \mathbb{A}^n$ be the polynomial map defined by $t \mapsto (t, t^2, \dots, t^n)$. The quadratic equations $x_i\, x_j = x_k\, x_\ell$, for all $i+j = k+\ell$, vanish on the image. Are there more polynomial equations that vanish on the image? ◇

In this course, we will see that the implicitization problem has an algorithmic solution. However, the converse is much harder.

0.2.8 Definition. A *rational parametrization* of an affine subvariety X in $\mathbb{A}^n$ is a rational map $\rho\colon \mathbb{A}^m \dashrightarrow \mathbb{A}^n$ such that X is the Zariski closure of the image of ρ. An affine subvariety X is *unirational* if it admits a rational parametrization.

0.2.9 Example. The unit circle is, by Example 0.2.2, unirational. ◇

0.2.10 Example. The affine subvariety $\mathrm{V}(x^2+y^2+z^2-1) \subset \mathbb{A}^3$ is unirational with a polynomial parametrization given by

$$(t_0, t_1) \mapsto \left(\frac{2\,t_0}{t_0^2+t+1^1+1}, \frac{2\,t_1}{t_0^2+t_1^1+1}, \frac{t_0^2+t_1^2-1}{t_0^2+t_1^2+1} \right) . \qquad ◇$$

0.2.11 Example. The Fermat hypersurface $\mathrm{V}(w^3+x^3+y^3+z^3) \subset \mathbb{A}^4$ is unirational with a parametrization given by

$$\begin{pmatrix} t_0 \\ t_1 \\ t_2 \end{pmatrix} \mapsto \begin{pmatrix} -(t_0+t_1)t_2^2 + (t_1^2+2t_0^2)t_2 - t_1^3 + t_0t_1^2 - 2t_0^2t_1 - t_0^3 \\ t_2^3 - (t_0+t_1)t_2^2 + (t_1^2+2t_0^2)t_2^3 + t_0t_1^2 - 2t_0^2t_1 + t_0^3 \\ -t_2^3 + (t_0+t_1)t_2^2 - (t_1^2+2t_0^2)t_2 + 2t_0t_1^2 - t_0^2t_1 + 2t_0^3 \\ (t_1-2t_0)t_2^2 + (t_1^2-t_0^2)t_2 + t_1^3 - t_0t_1^2 + 2t_0^2t_1 - 2t_1^3 \end{pmatrix} . \qquad ◇$$

0.2.12 Remark. For a general low-degree hypersurface, there are no techniques for disproving unrationality. However, unirationality has been established only when $\deg(f) = 2$ and $n \geqslant 2$, $\deg(f) = 3$ and $n \geqslant 3$, or $n \gg \deg(f)$. For a fixed degree greater than 3, there are many values of n for which unirationality is an open problem. In contrast, a general degree d hypersurface in $\mathbb{A}^n(\mathbb{C})$ does not admit a rational parametrization whenever $d > n$. For instance, the quartic hypersurface $\mathrm{V}(x^4+y^4+z^4-1)$ in $\mathbb{A}^3$ lacks one.