

1 Varieties

The intuitive idea is that a variety is the curve or surface defined by some equations. Differential geometry uses differential functions, algebraic geometry uses polynomials. Much simpler, much stronger results.

The vague idea can be made more precise in various ways.

1.1 Affine algebraic varieties

Let k be a field. An *affine algebraic variety* V is the set of common zeros in k^n of some given polynomials (in n variables) f_1, \dots, f_m .

The choice of the f_i can be fairly arbitrary: the line in k^3 defined by $x - 2 = z - 1 = 0$ is also defined by $x - 2z = x + z - 3 = 0$. So, use the ideal $I = (f_1, \dots, f_m)$ generated by them in $k[x_1, \dots, x_n]$.

The Hilbert Basis Theorem says that every ideal in $k[x_1, \dots, x_n]$ has a finite basis, so that giving V by finitely many equations or giving V by the ideal of all equations is equivalent.

One can go back and forth between varieties and ideals: Given a subset S of k^n , let $I(S)$ be the ideal of all elements of $k[x_1, \dots, x_n]$ that vanish on all points of S . Given a subset F of $k[x_1, \dots, x_n]$, let $V(F)$ be the variety of all points in k^n on which all elements of F vanish.

This is a Galois connection: $I()$ and $V()$ reverse inclusion, and $I(V(I(S))) = I(S)$ and $V(I(V(F))) = V(F)$.

If k is algebraically closed then we have Hilbert's Nullstellensatz that says that if $1 \notin I$ then $V(I) \neq \emptyset$ and that if $J = I(V(I))$ then J is the *radical* of I , the ideal generated by all elements of which some power lies in I .

1.2 Projective space

The n -dimensional projective space \mathbf{P}^n is the set of 1-spaces in k^{n+1} , that is, the set of points coordinatized by $n+1$ coordinates, not all zero, identified when proportional: $(a_0, \dots, a_n) = (\lambda a_0, \dots, \lambda a_n)$ when $\lambda \neq 0$. The open subset of \mathbf{P}^n defined by $X_0 \neq 0$ can be identified with the n -dimensional affine space \mathbf{A}^n , that is, k^n , via $(a_0, \dots, a_n) \mapsto (a_1/a_0, \dots, a_n/a_0)$.

Polynomials (in the $n+1$ coordinates) do not have well-defined values on projective space, since projective coordinates are defined only up to a constant. However, if the polynomial is *homogeneous* (every term has the same degree) then it makes sense to talk about it being zero. Thus, we can define *projective varieties* in projective space using a set of homogeneous polynomials. The corresponding ideals (generated by homogeneous polynomials) are called homogeneous ideals. Of course they also contain inhomogeneous polynomials.

The analog of Hilbert's Nullstellensatz in this setting becomes: Let k be algebraically closed. A homogeneous ideal I defines the empty set if and only if I contains all monomials X_i^N ($0 \leq i \leq n$) for some sufficiently large N .

1.3 Zariski topology

Zariski topology on affine space has as closed sets the affine algebraic varieties.

On projective space one can define Zariski topology by taking as closed sets the projective varieties. Or, equivalently, one can make the sets closed that have a closed intersection with the $n + 1$ affine open sets defined by $X_i \neq 0$.

(Thus, the topology that \mathbf{A}^n inherits from \mathbf{P}^n is its own, and the topology that \mathbf{P}^n inherits from the canonical cover by $n + 1$ copies of \mathbf{A}^n is its own.)

1.4 Quasiprojective varieties

If we want to study affine varieties (closed subsets of affine space) and projective varieties (closed subsets of projective space) simultaneously, a common generalization is needed. A simple-minded one is that of *quasiprojective variety*, by definition the intersection of an open and a closed set in projective space.

Indeed, affine space is an open subset of projective space.

2 Regular maps

A *regular function* (from an affine variety to k) is a polynomial. Let $k[V]$ be the ring of regular functions on V . Polynomials that agree on V differ by a polynomial that vanishes on V , that is, lies in $I(V)$. Thus, $k[V] \simeq k[x_1, \dots, x_n]/I(V)$. The ring $k[V]$ is called the *coordinate ring* of V .

A *regular map* (from affine variety V to affine variety W) is a map of which the coordinate functions are regular. Thus, it looks like $f(a_1, \dots, a_n) = (f_1(a_1, \dots, a_n), \dots, f_m(a_1, \dots, a_n))$, where the f_i are polynomials (such that the images $f(a_1, \dots, a_n)$ satisfy the equations of W).

An *isomorphism* from V to W is a regular map that has a two-sided inverse that also is a regular map.

A regular map $f : V \rightarrow W$ induces a homomorphism (of k -algebras) $f^* : k[W] \rightarrow k[V]$ defined by $f^*(h) = h \circ f$. Conversely, every homomorphism from $k[W]$ to $k[V]$ arises in this way.

The affine varieties V and W are isomorphic if and only if the rings $k[V]$ and $k[W]$ are isomorphic (as k -algebras).

3 Rational maps

A *rational function* (from an irreducible affine variety to k) is an element of the quotient field $k(V)$ of $k[V]$. (If V is irreducible, then $I(V)$ is prime, so $k[V]$ is an integral domain (has no zero divisors), so has a quotient field.) The field $k(V)$ is called the *function field* of V .

The rational function ϕ is *regular* at $x \in V$ when $\phi = f/g$ where f, g are regular functions with $g(x) \neq 0$. Now $\phi(x) = f(x)/g(x)$ is independent of the choice of f, g .

A *rational map* (from affine variety V to affine variety W) is a map of which the coordinate functions are rational.

A birational isomorphism from V to W is a rational map that has a two-sided inverse that also is a rational map.

The affine varieties V and W are birationally isomorphic if and only if the function fields $k(V)$ and $k(W)$ are isomorphic.

4 Examples

- (i) Let $V = k^n$. Then $I(V) = 0$ and $k[V] = k[x_1, \dots, x_n]$, $k(V) = k(x_1, \dots, x_n)$.
- (ii) Let $V = I(xy - 1)$. Then $k[V] = k[x, x^{-1}]$ and $k(V) = k(x)$. Thus, the line and the hyperbola are not isomorphic, but are birationally isomorphic. Rational maps are $(x, y) \mapsto x$ with inverse $x \mapsto (x, x^{-1})$.
- (iii) Let k have characteristic p . Then $f(a_1, \dots, a_n) = (a_1^p, \dots, a_n^p)$ is a regular map from V to itself. It is known as the Frobenius map.
- (iv) The domain of a rational function ϕ is an open set.
- (v) Let $V = I(y^2 - x^3)$. Then the map $(t) \mapsto (t^2, t^3)$ from k to V is regular. Its inverse $(x, y) \mapsto y/x$ is rational but is not defined at $(0,0)$. (For: if $y/x = f/g$, and $g(0,0) \neq 0$, then $xf = yg$ in $k[V]$, impossible.) This is a birational isomorphism between k and V .
- (vi) Let k be algebraically closed. Then the only rational functions that are everywhere regular are the regular functions.
- (Indeed: suppose $\phi = f_x/g_x$ for certain polynomials f_x, g_x where $g_x(x) \neq 0$. The ideal $I = I(g_x|x)$ has $V(I) = \emptyset$ so by the Nullstellensatz $1 = \sum u_i g_{x_i}$ for certain $u_i \in k[V]$, and hence $\phi = \sum u_i f_{x_i} \in k[V]$.)
- (vii) Consider the equation $y^2 = ax^4 + bx^3 + cx^2 + dx + e$. Use a transformation $x \rightarrow x - \alpha$ (where α is a root of the polynomial on the right-hand side) to get the shape $y^2 = ax^4 + bx^3 + cx^2 + dx$. Now divide by x^4 and put $u = 1/x$ and $v = y/x^2$. We get $v^2 = du^3 + cu^2 + bu + a$ and have reduced a fourth degree equation to a cubic. The corresponding curves are birationally isomorphic.
- (viii) If a rational function $\phi : V \rightarrow W$ is zero on a nonempty open subset U of V , then everywhere. (Since V is irreducible and the union of the closed subsets $V \setminus U$ and $\phi^{-1}(0)$.)
- (ix) If the image of a rational function $\phi : V \rightarrow W$ is dense in W (that is, if the closure of the image is all of W), then the kernel of ϕ^* consists of the zero function only, so ϕ^* provides an embedding of $k(W)$ into $k(V)$.

5 Hypersurfaces

Let k be algebraically closed. Every irreducible closed set V is birationally isomorphic to a hypersurface (that is, a variety defined by a single polynomial).

Indeed, look at the field $K = k(V)$. It is finitely generated over k , so can be obtained by first adjoining d elements t_i that are transcendental over what was obtained thus far, and then making an algebraic extension. Now a finite separable algebraic extension is generated by a single element, so if K is separable over $k(t_1, \dots, t_d)$ then $K = k(t_1, \dots, t_d, c)$ for some c , and the minimum polynomial of c gives the single polynomial sought. Remains to check separability.

(Reminder: an element α is called *inseparable* over a field k when it is algebraic but a multiple root of its minimum polynomial $g(x)$. But if α is a multiple root of $g(x)$, then it is also a root of $g'(x)$, which has lower degree. This can happen only if $g'(x) = 0$, that is, the field k has characteristic p , and g only contains terms x^e where e is a multiple of p .)

If t_{d+1} is inseparable over $k(t_1, \dots, t_d)$, we find a polynomial $f \in k[x_1, \dots, x_{d+1}]$ with $f(t_1, \dots, t_{d+1}) = 0$ (the minimum polynomial of t_{d+1} , found in $k(t_1, \dots, t_d)[x]$, multiplied by a constant so as to get into $k[t_1, \dots, t_d, x]$, then with t_i viewed as

variables) that has zero derivative w.r.t. x_{d+1} . It cannot have zero derivative w.r.t. all variables, otherwise f would be a p -th power (this uses that k is closed for taking p -th roots). But if the derivative w.r.t. x_j is nonzero, interchange t_j and t_{d+1} . Now repeatedly use the theorem on the single generating element in $k(t_1, \dots, t_{d+2})$ over $k(t_1, \dots, t_d)$ to reduce the number of generators until it has become $d + 1$.

The version of the theorem on the single generating element that we used is: Let K, L be fields, $L = K(\alpha, \beta)$ where α is separable over K and β algebraic over $K(\alpha)$. Then $L = K(\gamma)$ for some γ .