Chapter 1

Affine algebraic geometry

We shall restrict our attention to *affine* algebraic geometry, meaning that the algebraic varieties we consider are precisely the closed subvarieties of affine n-space defined in section one.

1.1 The Zariski topology on $\mathbb{A}^n$

Affine n-space, denoted by $\mathbb{A}^n$, is the vector space k^n. We impose coordinate functions $x_1, \ldots, x_n$ on it and study $\mathbb{A}^n$ through the lens of the polynomial ring $k[x_1, \ldots, x_n]$ viewed as functions $\mathbb{A}^n \to k$.

First we impose topologies on $\mathbb{A}^n$ and k such that the polynomial functions $\mathbb{A}^n \to k$ are continuous. We will require each point on k to be closed, and this forces the fibers $f^{-1}(\lambda)\mathbb{A}^n$ to be closed for each $f \in k[x_1, \ldots, x_n]$ and each $\lambda \in k$. The set $f^{-1}(\lambda) = \{p \mid f(p) = \lambda\}$ is the zero locus of the polynomial $f - \lambda$; since every polynomial can be written in the form $f - \lambda$, the zero locus of every polynomial must be closed. Since a finite union of closed sets is closed, the common zero locus

$$\{p \in k^n \mid f_1(p) = \cdots = f_r(p) = 0\}$$

of every finite collection of polynomials $f_1, \ldots, f_r$ is closed. This is the definition of the Zariski topology on $\mathbb{A}^n$.

And the closed subsets of $\mathbb{A}^n$ are called affine algebraic varieties.

A lot of important geometric objects are affine algebraic varieties. The conic sections are the most ancient examples: the parabola is the zero locus of $y - x^2$, the hyperbolas are the zero loci of equations like $x^2/a^2 - y^2/b^2 - 1$, or more simply $xy - 1$, the circles centered at the origin are the zero loci of the polynomials $x^2 + y^2 - r^2$, and so on. Higher-dimensional spheres and ellipsoids provide further examples. Another example is the union in $\mathbb{R}^4$ of the xy-plane and wz-plane: it is the simultaneous zero locus of xw, xz, yw, and yz (or, more cleverly, of xw, yz, and $xz + yw$). Fermat's last theorem can be restated as asking whether, when $n \geq 3$, the zero locus of the equation $x^n + y^n - z^n$ has any points with rational coordinates other than those in which one of the coordinates is zero. Another family of examples is provided by the $n \times n$ matrices over $\mathbb{R}$ having rank at most some fixed number d; these matrices can be thought of as the points in the n^2-dimensional vector space $M_n(\mathbb{R})$ where all $(d+1) \times (d+1)$ minors vanish, these minors being given by (homogeneous degree $d+1$) polynomials in the variables x_{ij}, where x_{ij} simply takes the ij-entry of the matrix.

We will write $\mathbb{A}^n_k$ for k^n and call it affine n-space over k. For example, $\mathbb{A}^1$ is called the affine line and $\mathbb{A}^2$ is called the affine plane. We will only discuss affine algebraic geometry in this course. Projective algebraic geometry is a much prettier subject.

Definition 1.1 The zero locus of a collection $f_1, \dots, f_r$ of elements in $k[x_1, \dots, x_n]$ is called an affine algebraic variety or a closed subvariety of $\mathbb{A}^n$. We denote it by $V(f_1, \dots, f_r)$. Briefly,

$$V(f_1, \dots, f_r) := \{p \in \mathbb{A}^n_k \mid f_1(p) = \cdots = f_r(p) = 0\}.$$

More generally, if J is any ideal in $k[x_1, \dots, x_n]$ we define

$$V(J) := \{p \in \mathbb{A}^n \mid f(p) = 0 \text{ for all } f \in J\}.$$

◊

It is easy to show that if $J = (f_1, \dots, f_r)$, then $V(J) = V(f_1, \dots, f_r)$. Conversely, since every ideal of the polynomial ring is finitely generated, the subvarieties of $\mathbb{A}^n$ are the zero loci of ideals.

Of course we can define $V(\mathcal{S})$ for any set $\mathcal{S}$ of polynomials. If J denotes the ideal generated by $\mathcal{S}$, then $V(\mathcal{S}) = V(J)$.

Example 1.2 (Plane curves) Let $f \in k[x, y]$ be a non-constant polynomial. We call $C := V(f) \subset \mathbb{A}^2$ a plane curve. If we place no restrictions on the field k, C may not look much like curve at all. For example, when $k = \mathbb{R}$ the curve $x^2 + y^2 + 1 = 0$ is empty. So, let's suppose that k is algebraically closed.

Claim: C is infinite. Proof: First suppose that $f \in k[x]$. Let $\alpha \in k$ be a zero of f. Then $C = \{(\alpha, \beta) \mid \beta \in k\}$. Since k is algebraically closed it is infinite, so C is also infinite. Now suppose that $f \notin k[x]$ and write $f = a_0 + a_1 y + \cdots + a_n y^n$ where each $a_i \in k[x]$, $n \geq 1$, and $a_n \neq 0$. There are infinitely many $\alpha \in k$ such that $a_n(\alpha) \neq 0$. Evaluating all the coefficients at such a point α gives a polynomial $f(\alpha, y) \in k[y]$ of degree $n \geq 1$. Now $f(\alpha, y)$ has a zero so C contains (α, β) for some β. As α varies this provides infinitely many points in C. ◊

Proposition 1.3 *Let I, J, and I_j, $j \in \Lambda$, be ideals in the polynomial ring $A = k[x_1, \dots, x_n]$. Then*

1. *$I \subset J$ implies $V(J) \subset V(I)$;*

2. *$V(0) = \mathbb{A}^n$;*

3. *$V(A) = \phi$;*

4. $\bigcap_{j\in\Lambda} V(I_j) = V(\sum_{j\in\Lambda} I_j)$;

5. $V(I) \cup V(J) = V(IJ) = V(I \cap J)$.

Proof. The first four statements are clear, so we only prove the fifth.

Since $IJ \subset I \cap J$ and $I \cap J$ is contained in both I and J, (1) imples that

$$V(I) \cup V(J) \subset V(I \cap J) \subset V(IJ).$$

On the other hand, if $p \notin V(I) \cup V(J)$, there are functions $f \in I$ and $g \in J$ such that $f(p) \neq 0$ and $g(p) \neq 0$. Hence $(fg)(p) \neq 0$. But $fg \in IJ$, so $p \notin V(IJ)$. Hence $V(IJ) \subset V(I) \cup V(J)$. The equalities in (5) follow. □

Contrast parts (4) and (5) of the proposition. Part (5) extends to finite unions: if Λ is finite, then $\cup_{j\in\Lambda} V(I_j) = V(\prod_{j\in\Lambda} I_j) = V(\cap_{j\in\Lambda} I_j)$. To see that part (5) does not extend to infinite unions, consider the ideals $(x-j)$ in $\mathbb{R}[x]$.

Definition 1.4 The Zariski topology on $\mathbb{A}^n$ is defined by declaring the closed sets to be the subvarieties. ♢

Proposition 1.3 shows that this is a topology. Parts (2) and (3) show that $\mathbb{A}^n$ and the empty set are closed. Part (4) shows that the intersection of a collection of closed sets is closed. Part (5) shows that a finite union of closed sets is closed.

Proposition 1.5 *Let $k = \mathbb{A}^1$ have the Zariski topology.*

1. *The closed subsets of $\mathbb{A}^1$ are its finite subsets and k itself.*

2. *If $f \in k[x_1, \ldots, x_n]$, then $f : \mathbb{A}^n \to k$ is continuous.*

Proof. (1) Of course $k = V(0)$ and $\emptyset = V(1)$ are closed. A non-empty finite subset $\{\alpha_1, \ldots, \alpha_m\}$ of k is the zero locus of the polynomial $(x-\alpha_1)\cdots(x-\alpha_n)$, so is closed. Conversely, if I is an ideal in $k[x]$, then $I = (f)$ for some f, so its zero locus is the finite subset of k consisting of the zeroes of f.

(2) To show f is continuous, we must show that the inverse image of every closed subset of k is closed. The inverse image of k is $\mathbb{A}^n$, which is closed. And $f^{-1}(\phi) = \phi$ is closed. Since the only other closed subsets k are the non-empty finite subsets, it suffices to check that $f^{-1}(\lambda)$ is closed for each $\lambda \in k$. But $f^{-1}(\lambda)$ is precisely the zero locus of $f - \lambda$, and that is closed by definition. □

If X is any subset of $\mathbb{A}^n$, we define

$$I(X) := \{f \in k[x_1, \ldots, x_n] \mid f(p) = 0 \text{ for all } p \in X\}.$$

This is an ideal of $k[x_1, \ldots, x_n]$. It consists of the functions vanishing at all the points of X.

The following basic properties of $I(-)$ are analogues of the properties of $V(-)$ established in Proposition 1.3.

Proposition 1.6 *Let X, Y, and X_j, $j \in \Lambda$, be subsets of $\mathbb{A}^n$. Let $A = k[x_1, \ldots, x_n]$ be the polynomial ring generated by the coordinate functions x_i on $\mathbb{A}^n$. Then*

1. *$X \subset Y$ implies $I(X) \supset I(Y)$;*
2. *$I(\mathbb{A}^n) = 0$;*
3. *$I(\phi) = A$;*
4. *$I(\cap_{j\in\Lambda} X_j) \supset \sum_{j\in\Lambda} I(X_j)$;*
5. *$I(\cup_{j\in\Lambda} X_j) = \cap_{j\in\Lambda} I(X_j)$.*

Proof. Exercise. □

The containment in (4) can not be replaced by an equality: for example, in $\mathbb{A}^2$, if $X_1 = V(x_1)$ and $X_2 = V(x_1^2 - x_2^2)$, then $I(X_1) = (x_1)$ and $I(X_2) = (x_1^2 - x_2^2)$, so $I(X_1) + I(X_2) = (x_1, x_1^2 - x_2^2) = (x_1, x_2^2)$ which is strictly smaller than $(x_1, x_2) = I(\{(0,0)\}) = I(X_1 \cap X_2)$.

The obvious question. To what extent are the maps $V(-)$ and $I(-)$

$$\{\text{ideals in } k[x_1, \ldots, x_n]\} \longleftrightarrow \{\text{subvarieties of } \mathbb{A}^n\} \qquad (1\text{-}1)$$

inverses of one another? It is easy to see that $J \subset I(V(J))$ and $X \subset V(I(X))$, but they are not inverse to each other. There are two reasons they fail to be mutually inverse. Each is important. They can fail to be mutually inverse because the field is not algebraically closed (e.g., over $\mathbb{R}$, $V(x^2+1) = \phi$) and also because $V(f) = V(f^2)$. We now examine this matter in more detail.

Lemma 1.7 *Let X be a subset of $\mathbb{A}^n$. Then*

1. *$V(I(X)) = \bar{X}$, the closure of X;*
2. *if X is closed, then $V(I(X)) = X$.*

Proof. It is clear that (2) follows from (1), so we shall prove (1).

Certainly, $V(I(X))$ contains X and is closed. On the other hand, any closed set containing X is of the form $V(J)$ for some ideal J consisting of functions that vanish on X; that is, $J \subset I(X)$, whence $V(J) \supset V(I(X))$. Thus $V(I(X))$ is the smallest closed set containing X. □

Definition 1.8 Let J be an ideal in a commutative ring R. The radical of J is the ideal

$$\sqrt{J} := \{a \in R \mid a^n \in J \text{ for some } n\}.$$

If $J = \sqrt{J}$ we call J a radical ideal. ◊

Obviously $J \subset \sqrt{J}$. Thus, $\sqrt{J}$ is obtained from J by throwing in all the roots of the elements in J.

A prime ideal $\mathfrak{p}$ is radical because if x^n belongs to $\mathfrak{p}$, so does x.

Lemma 1.9 *If J is an ideal, so is $\sqrt{J}$.*

Proof. It is clear that if $a \in \sqrt{J}$, so is ra for every $r \in R$ because if $a^n \in J$ so is $(ar)^n$. If a and b are in $\sqrt{J}$, so is their sum. To see this, suppose that $a^n, b^m \in J$ and that $n \geq m$. Then

$$(a+b)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i} a^i b^{2n-i},$$

and for every i, either $i \geq n$, or $2n - i \geq n \geq m$, so $a^i b^{2n-i} \in J$, whence $(a+b)^{2n} \in J$. Thus $a + b \in \sqrt{J}$. □

The next lemma and theorem explain the importance of radical ideals in algebraic geometry.

Lemma 1.10 *If J is an ideal in $k[x_1, \dots, x_n]$, then*

$$V(J) = V(\sqrt{J}).$$

Proof. Since $J \subset \sqrt{J}$, $V(\sqrt{J}) \subset V(J)$. On the other hand, if $p \in V(J)$ and $f \in \sqrt{J}$, then $f^d \in J$ for some d, so $0 = f^d(p) = (f(p))^d$. But $f(p)$ is in the field k, so $f(p) = 0$. Hence $p \in V(\sqrt{J})$. □

Theorem 1.11 (Hilbert's Nullstellensatz, strong form) *Let k be an algebraically closed field and set $A = k[x_1, \dots, x_n]$.*

1. *If $J \neq A$ is an ideal, then $V(J) \neq \phi$.*
2. *For any ideal J, $I(V(J)) = \sqrt{J}$.*
3. *there is a bijection*

$$\{\textit{radical ideals in } A\} \longleftrightarrow \{\textit{closed subvarieties of } \mathbb{A}^n\}$$

given by

$$J \mapsto \{p \in \mathbb{A}^n \mid f(p) = 0 \textit{ for all } f \in J\}$$
$$X \mapsto \{f \in A \mid f(p) = 0 \textit{ for all } p \in X\}$$

Proof. (1) This follows from the weak nullstellensatz because J is contained in some maximal ideal, and all functions in that maximal ideal vanish at some point of $\mathbb{A}^n$.

(2) It is clear that $\sqrt{J} \subset I(V(\sqrt{J}))$, and we have seen that $V(\sqrt{J}) = V(J)$, so it remains to show that if f vanishes at all points of $V(J)$, then some power of f is in J. If $f = 0$, there is nothing to do, so suppose that $f \neq 0$.

The proof involves a sneaky trick.

Let y be a new indeterminate and consider the ideal $(J, fy - 1)$ in $A[y]$. Now $V(J, fy-1) \subset k^{n+1}$ and $(\lambda_1, \dots, \lambda_n, \alpha) \in V(J, fy - 1)$ if and only if

$g(\lambda_1, \ldots, \lambda_n) = 0$ for all $g \in J$ and $f(\lambda_1, \ldots, \lambda_n)\alpha = 1$; that is, if and only if $(\lambda_1, \ldots, \lambda_n)$ is in $V(J)$ and $\alpha = f(\lambda_1, \ldots, \lambda_n)^{-1}$. But $f(p) = 0$ for all $p \in V(J)$, so $V(J, fy-1) = \phi$.

Applying (1) to the ideal $(J, fy-1)$ in $A[y]$, it follows that $(J, fy-1) = A[y]$. Hence

$$1 = (fy-1)h_0 + \sum_{i=1}^{m} g_i h_i$$

for some $h_0, \ldots, h_m \in A[y]$ and $g_1, \ldots, g_m \in J$.

Now define $\psi : A[y] \to k(x_1, \ldots, x_n)$ by $\psi|_A = \mathrm{id}_A$ and $\psi(y) = f^{-1}$. The image of ψ is $k[x_1, \ldots, x_n][f^{-1}]$. Every element in it is of the form af^{-d} for some $a \in A$ and $d \geq 0$. Now

$$1 = \psi(1) = \sum_{i=1}^{m} g_i \psi(h_i) = \sum_{i=1}^{m} g_i a_i f^{-d_i},$$

so multiplying through by f^d with $d \geq d_i$ for all i gives $f^d \in J$.

(3) This follows from (2). □

1.2 Closed subvarieties of $\mathbb{A}^n$

From now on we shall work over an algebraically closed base field k.

Let X be a subvariety of $\mathbb{A}^n$. The polynomials in $k[x_1, \ldots, x_n]$ are functions $\mathbb{A}^n \to k$, so their restrictions to X produce functions $X \to k$. The restriction of a polynomial in $I(X)$ is zero, so we are led to the next definition.

Definition 2.1 Suppose that X is an algebraic subvariety of $\mathbb{A}^n$. The ring of regular functions on X, or the coordinate ring of X, is

$$\mathcal{O}(X) := k[x_1, \ldots, x_n]/I(X).$$

◊

The Zariski topology on a variety. The closed subvarieties of $\mathbb{A}^n$ inherit a topology from that on $\mathbb{A}^n$. We declare the closed subsets of X to be the subsets of the form $X \cap Z$ where Z is a closed subset of $\mathbb{A}^n$. Of course, $X \cap Z$ is a closed subset of $\mathbb{A}^n$, so the subsets of X of the form $X \cap Z$ can be characterzed as the closed subsets of $\mathbb{A}^n$ that belong to X. We call this the Zariski topology on X.

Whenever we speak of a subvariety $X \subset \mathbb{A}^n$ as a topological space we mean with respect to the Zariski topology.

The next result shows that the closed subsets of X are the zero loci for the ideals of the ring $\mathcal{O}(X)$.

Proposition 2.2 *Let X be a subvariety of $\mathbb{A}^n$. Then*

1. *$\mathcal{O}(X)$ is a ring of functions $X \to k$,*

2. *the closed subsets of X are those of the form $V(J) := \{p \in X \mid f(p) = 0$ for all $f \in J\}$, where J is an ideal of $\mathcal{O}(X)$;*

3. *the functions $f : X \to k$, $f \in \mathcal{O}(X)$, are continuous if k and X are given their Zariski topologies.*

Proof. (1) Let $C(X,k)$ denote the ring of all k-valued functions on X. We may restrict each $f \in k[x_1,\ldots,x_n]$ to X. This gives a ring homomorphism $\Psi : k[x_1,\ldots,x_n] \to C(X,k)$. The kernel of Ψ is $I(X)$, so the image of Ψ is isomorphic to $k[x_1,\ldots,x_n]/I(X)$.

(2) The ideals of $\mathcal{O}(X) = k[x_1,\ldots,x_n]/I(X)$ are in bijection with the ideals of $k[x_1,\ldots,x_n]$ that contain $I(X)$. If K is an ideal of $k[x_1,\ldots,x_n]$ containing $I(X)$ and $J = K/I(X)$ is the corresponding ideal of $\mathcal{O}(X)$, then $V(K) = V(J)$. Warning: $V(K)$ is defined as the subset of $\mathbb{A}^n$ where all the functions in K vanish, and $V(J)$ is defined to be the subset of X where all the functions in J vanish.

The closed sets of X are by definition the subsets of the form $Z \cap X$ where Z is a closed subset of $\mathbb{A}^n$. But $Z \cap X$ is then a closed subset of $\mathbb{A}^n$, so the closed subsets of X are precisely the closed subsets of $\mathbb{A}^n$ that are contained in X. But these are the subsets of $\mathbb{A}^n$ that are of the form $V(K)$ for some ideal K containing $I(X)$.

(3) This is a special case of Proposition 7.7 below. □

The pair $(X, \mathcal{O}(X))$ is analogous to the pair $(\mathbb{A}^n, k[x_1,\ldots,x_n])$. We have a space and a ring of k-valued functions on it. For each ideal in the ring we have its zero locus, and these form the closed sets for a topology, the Zariski topology, on the space.

The weak and strong forms of Hilbert's Nullstellensatz for $\mathbb{A}^n$ yield the following results for X.

Proposition 2.3 *Let k be an algebraically closed field and X a closed subvariety of $\mathbb{A}^n_k$. Then*

1. *the functions $V(-)$ and $I(-)$ are mutually inverse bijections between the radicaol ideals in $\mathcal{O}(X)$ and the closed subsets of X;*

2. *there is a bijection between the points of X and the maximal ideals in $\mathcal{O}(X)$.*

Proof. Exercise. □

Remarks. 1. Let X be an affine algebraic variety and $f \in \mathcal{O}(X)$. If f is not a unit in $\mathcal{O}(X)$ then the ideal it generates is not equal to $\mathcal{O}(X)$ so is contained in some maximal ideal of $\mathcal{O}(X)$, whence f vanishes at some point of X. In other words, $f \in \mathcal{O}(X)$ is a unit if and only if $f(x) \neq 0$ for all $x \in X$.

2. It is useful to observe that points x and y in X are equal if and only if $f(x) = f(y)$ for all $f \in \mathcal{O}(X)$. To see this suppose that $f(x) = f(y)$ for all f;

then a function vanishes at x if and only if it vanishes at y, so $\mathfrak{m}_x = \mathfrak{m}_y$; it now follows from the bijection between points and ideals that $x = y$.

Lemma 2.4 *Let Z_1 and Z_2 be disjoint closed subsets of an affine algberaic variety X. There exists an $f \in \mathcal{O}(X)$ such that $f(Z_1) = 0$ and $f(Z_2) = 1$.*

Proof. Write $I_j = I(Z_j)$. Then $Z_j = V(I_j)$ because Z_j is closed. Now $V(I_1 + I_2) = V(I_1) \cap V(I_2) = Z_1 \cap Z_2 = \phi$, so $I_1 + I_2 = \mathcal{O}(X)$. Hence we can write $1 = f_1 + f_2$ with $f_j \in I_j$. Thus f_1 is the desired function. □

Finite varieties. If X is any subvariety of $\mathbb{A}^n$ there are generally many functions $X \to k$ that are not regular. (Give an example of a function $\mathbb{A}^1 \to k$ that is not regular.) However, if X is finite $\mathcal{O}(X)$ is exactly the ring of k-valued functions on X.

A single point in $\mathbb{A}^n$ is a closed subvariety, hence any finite subset $X \subset \mathbb{A}^n$ is a closed subvariety. Suppose $X = \{p_1, \dots, p_t\}$. By Lemma 2.4, $\mathcal{O}(X)$ contains the characteristic functions $\chi_i : X \to k$ defined by $\chi_i(p_j) = \delta_{ij}$. It is clear that these functions provide a basis for the ring k^X of all k-valued functions $X \to k$. By definition the only element of $\mathcal{O}(X)$ that is identically zero on X is the zero element, so $\mathcal{O}(X)$ is equal to k^X.

The next proposition is an elementary illustration of how the geometric properties of X are related to the algebraic properties of $\mathcal{O}(X)$.

First we need a result that is useful in a wide variety of situations. It was known to the ancients in the following form: if $m_1, \dots, m_n$ are pairwise relatively prime integers, and $a_1, \dots, a_n$ are any integers, then there is an integer d such that $d \equiv a_i (\text{mod}) m_i$ for all i. This statement appears in the manuscript *Mathematical Treatise in Nine Sections* written by Chin Chiu Shao in 1247 (search on the web if you want to know more).

Lemma 2.5 (The Chinese Remainder Theorem) *Let $I_1, \dots, I_n$ be ideals in a ring R such that $I_i + I_j = R$ for all $i \neq j$. Then there is an isomorphism of rings*

$$\frac{R}{I_1 \cap \cdots \cap I_n} \cong \frac{R}{I_1} \oplus \cdots \oplus \frac{R}{I_n}. \tag{2-2}$$

Proof. We proved this when $n = 2$ on page **??**.

Consider the two ideals $I_1 \cap \cdots \cap I_{n-1}$ and I_n. For each $j = 1, \dots, n-1$, we can write $1 = a_j + b_j$ with $a_j \in I_n$ and $b_j \in I_j$. Then

$$1 = (a_1 + b_1) \cdots (a_{n-1} + b_{n-1}) = a + b_1 b_2 \cdots b_{n-2} b_{n-1},$$

where a is a sum of elements in I_n. Thus $I_n + (I_1 \cap \cdots \cap I_{n-1}) = R$, and we can apply the $n = 2$ case of the result to see that

$$\frac{R}{I_1 \cap \cdots \cap I_n} \cong R/I_1 \cap \cdots \cap I_{n-1} \ \oplus \ R/I_n.$$

Induction completes the proof.

Explictly, the isomorphism in (2-2) is induced by the ring homomorphism $\psi : R \to R/I_1 \oplus \cdots \oplus R/I_n$ defined by

$$\psi(a) = ([a + I_1], \cdots , [a + I_n]).$$

The kernel is obviously $I_1 \cap \cdots \cap I_n$. □

Proposition 2.6 *A closed subvariety $X \subset \mathbb{A}^n$ is finite if and only if $\mathcal{O}(X)$ is a finite dimensional vector space. In particular,* $\dim_k \mathcal{O}(X) = |X|$.

Proof. ($\Rightarrow$) Suppose that $X = \{p_1, \dots , p_d\}$ are the distinct points of X. Let $\mathfrak{m}_i$ be the maximal ideal of $A = k[x_1, \dots , x_n]$ vanishing at p_i. It is clear that $I(X) = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_d$, so

$$\mathcal{O}(X) = A/\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_d.$$

The map

$$A \to A/\mathfrak{m}_1 \oplus \cdots \oplus A/\mathfrak{m}_d, \quad a \mapsto ([a + \mathfrak{m}_1], \cdots , [a + \mathfrak{m}_d]),$$

is surjective with kernel $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_d$, so

$$\mathcal{O}(X) \cong A/\mathfrak{m}_1 \oplus \cdots \oplus A/\mathfrak{m}_d \cong k \oplus \cdots \oplus k = k^d.$$

Hence $\dim_k \mathcal{O}(X) = d$.

($\Leftarrow$) The Nullstellensatz for X says that the points of X are in bijection with the maximal ideals of $\mathcal{O}(X)$. We must therefore show that a finite dimensional k-algebra has only a finite number of maximal ideals.

Suppose that R is a finite dimensional k-algebra and that $\mathfrak{m}_1, \dots , \mathfrak{m}_d$ are distinct maximal ideals of R. We will show that the intersections

$$\mathfrak{m}_1 \supset \mathfrak{m}_1 \cap \mathfrak{m}_2 \supset \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \mathfrak{m}_3 \supset \cdots \supset \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_d$$

are all distinct from one another. If this were not the case we would have $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \subset \mathfrak{m}_{n+1}$ for some n, whence $\mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_n \subset \mathfrak{m}_{n+1}$. But interpreting this product in the field $R/\mathfrak{m}_{n+1}$, such an inclusion implies that $\mathfrak{m}_i \subset \mathfrak{m}_{n+1}$ for some $i \in \{1, \dots , n\}$. This can't happen since the maximal ideals are distinct. Hence the intersections are distinct as claimed.

Since these ideals are vector subspaces of R, it follows that $\dim_k R \geq d$. Hence the number of distinct maximal ideals of R is at most $\dim_k R$. □

Remark. The Zariski topology on $\mathbb{A}^2$ is *not* the same as the product topology for $\mathbb{A}^1 \times \mathbb{A}^1$. The closed sets for the product topology on $\mathbb{A}^1 \times \mathbb{A}^1$ are $\mathbb{A}^2$ itself, all the finite subsets of $\mathbb{A}^2$, and finite unions of lines that are parallel to one of the axes, and all finite unions of the preceeding sets. In particular, the diagonal Δ is not closed in the product topology; but it is closed in the Zariski topology on $\mathbb{A}^2$ because it is the zero locus of $x - y$.

1.3 Prime ideals

Definition 3.1 An ideal $\mathfrak{p}$ in a commutative ring R is prime if the quotient $R/\mathfrak{p}$ is a domain. ♢

We do not count the zero ring as a domain, so R itself is not a prime ideal.

It is an easy exercise to show that an ideal $\mathfrak{p}$ is prime if and only if it has the property that

$$x \notin \mathfrak{p} \text{ and } y \notin \mathfrak{p} \Rightarrow xy \notin \mathfrak{p}.$$

An induction argument shows that if a prime ideal contains a product $x_1 \cdots x_n$ then it contains one the x_is.

Lemma 3.2 *Let $\mathfrak{p}$ be an ideal of R. The following are equivalent*

1. *$\mathfrak{p}$ is prime;*
2. *a product of ideals IJ is contained in $\mathfrak{p}$ if and only if either I or J is contained in $\mathfrak{p}$.*

Proof. (1) ⇒ (2) Suppose that $\mathfrak{p}$ is a prime ideal. Let I an J be ideals of R. Certainly, if either I or J is contained in $\mathfrak{p}$, so is their product. Conversely, suppose that IJ is contained in $\mathfrak{p}$. We must show that either I or J is contained in $\mathfrak{p}$. If I is not contained in $\mathfrak{p}$, there is an element $x \in I$ that is not in $\mathfrak{p}$. Hence $[x+\mathfrak{p}]$ is a non-zero element of the domain $R/\mathfrak{p}$. If $y \in J$, then $xy \in \mathfrak{p}$, so $[x+\mathfrak{p}][y+\mathfrak{p}] = 0$ in $R/\mathfrak{p}$; hence $[y+\mathfrak{p}] = 0$ and $y \in \mathfrak{p}$. Thus $J \subset \mathfrak{p}$.

(2) ⇒ (1) To show that $\mathfrak{p}$ is prime we must show that $R/\mathfrak{p}$ is a domain. Let $x, y \in R$ and suppose that $[x+\mathfrak{p}]$ and $[y+\mathfrak{p}]$ are non-zero elements of $R/\mathfrak{p}$. Then $x \notin \mathfrak{p}$ and $y \notin \mathfrak{p}$. Thus $\mathfrak{p}$ does not contain either of the principal ideals $I = (x)$ and $J = (y)$; by hypothesis, $\mathfrak{p}$ does not contain there product $IJ = (xy)$. In particular, $xy \notin \mathfrak{p}$. Hence in $R/\mathfrak{p}$,

$$0 \neq [xy+\mathfrak{p}] = [x+\mathfrak{p}][y+\mathfrak{p}].$$

This shows that $R/\mathfrak{p}$ is a domain. □

Lemma 3.3 *Let R be a commutative ring. Then xR is a prime ideal if and only if x is prime.*

Proof. The ideal xR is prime if and only if whenever $ab \in xR$ (i.e., whenever x divides ab) either $a \in xR$ or $b \in xR$ (i.e., x divides either a or b. This is equivalent to the condition that x be prime. □

Certainly every maximal ideal is prime. The only prime ideals in a principal ideal domain are the maximal ideals and the zero ideal.

In the polynomial ring $k[x_1, \dots, x_n]$ one has the following chain of prime ideals

$$0 \subset (x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, \dots, x_n).$$

There are of course many other prime ideals. For example, the principal ideal generated by an irreducible polynomial is prime.

Lemma 3.4 *Let I be an ideal in a commutative ring R. The prime ideals in R/I are exactly those ideals of the form $\mathfrak{p}/I$ where $\mathfrak{p}$ is a prime ideal of R containing I.*

Proof. We make use of the bijection between ideals of R that contain I and ideals of R/I. If $\mathfrak{p}$ is an ideal containing I, then $R/\mathfrak{p} \cong (R/I)/(\mathfrak{p}/I)$ so $\mathfrak{p}$ is a prime ideal of R if and only if $\mathfrak{p}/I$ is a prime ideal of R/I. □

Lemma 3.5 *Intersections of prime ideals are radical.*

Proof. Let $\{\mathfrak{p}_i \mid i \in I\}$ be a collection of prime ideals, and set $J = \cap_{i \in I}\mathfrak{p}_i$. If $f^n \in J$, then $f^n \in \mathfrak{p}_i$ for all i, so $f \in \mathfrak{p}_i$. Hence $f \in J$. □

Proposition 3.6 *If J is an ideal in a noetherian ring and $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ are the minimal primes containing it, then $\sqrt{J} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$.*

Proof. Write $J' = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$. Then J' is radical and $J \subset J'$, so $\sqrt{J} \subset \sqrt{J'} = J'$. By Proposition **??**.3.9, J contains $\mathfrak{p}_1^{i_1} \cdots \mathfrak{p}_n^{i_n}$ for some integers $i_1, \dots, i_n$. Hence $(J')^{i_1+\cdots+i_n} \subset J$, and $J' \subset \sqrt{J}$. □

Proposition 3.6 says that the radical ideals in a commutative noetherian ring are precisely the intersections of finite collections of prime ideals.

Proposition 3.7 *Every ideal in a noetherian ring contains a product of prime ideals.*

Proof. If the set

$$\mathcal{S} := \{\text{ideals of } R \text{ that do not contain a product of prime ideals}\}$$

is not empty it has a maximal member, say I. Now I itself cannot be prime, so contains a product of two strictly larger ideals, say J and K. Since these are strictly larger than I they do not belong to $\mathcal{S}$. Hence each of them contains a product of prime ideals. Now JK, and hence I, contains the product of all those primes. This contradiction implies that $\mathcal{S}$ must be empty. □

As the next result makes clear, Proposition 3.7 is stronger than it first appears. If I is an ideal of R, then the zero ideal in R/I contains a product of primes; however, every prime in R/I is of the form $\bar{\mathfrak{p}} = \mathfrak{p}/I$ where $\mathfrak{p}$ is a prime in R that contains I, so I contains a product of primes, each of which contains I.

Definition 3.8 A prime ideal $\mathfrak{p}$ containing I is called a minimal prime over I if there are no other primes between $\mathfrak{p}$ and I; that is, if $\mathfrak{q}$ is a prime ideal such that $I \subset \mathfrak{q} \subset \mathfrak{p}$, then $\mathfrak{p} = \mathfrak{q}$. ◊

Proposition 3.9 *Let I be an ideal in a noetherian ring R. Then*

1. *there are only finitely many minimal primes over I, say $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$, and*
2. *there are integers $i_1, \ldots, i_n$ such that $\mathfrak{p}_1^{i_1} \cdots \mathfrak{p}_n^{i_n} \subset I$.*

Proof. As just explained, there are prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ containing I such that $\mathfrak{p}_1^{i_1} \cdots \mathfrak{p}_n^{i_n} \subset I$ for some integers $i_1, \ldots, i_n$. If $\mathfrak{p}_i \subset \mathfrak{p}_j$ we can replace each $\mathfrak{p}_j$ appearing in the product by $\mathfrak{p}_i$, so we can assume that $\mathfrak{p}_i \not\subset \mathfrak{p}_j$ if $i \neq j$.

It follows that each $\mathfrak{p}_i$ is minimal over I because if $\mathfrak{q}$ were a prime such that $\mathfrak{p}_i \supset \mathfrak{q} \supset I$, then $\mathfrak{q}$ contains $\mathfrak{p}_1^{i_1} \cdots \mathfrak{p}_n^{i_n}$ so contains some $\mathfrak{p}_j$; but then $\mathfrak{p}_j \subset \mathfrak{p}_i$, so $\mathfrak{p}_i = \mathfrak{q} = \mathfrak{p}_j$. And these are *all* the minimal primes because any prime containing I contains $\mathfrak{p}_1^{i_1} \cdots \mathfrak{p}_n^{i_n}$ so contains some $\mathfrak{p}_j$. □

Corollary 3.10 *Suppose R is a UFD. Let $x \in R$ be a non-zero non-unit, and write $x = p_1^{i_1} \cdots p_n^{i_n}$ as a product of powers of "distinct" irreducibles. Then the minimal primes containing x are $p_1R, \ldots, p_nR$.*

1.4 The spectrum of a ring

Definition 4.1 The spectrum of a commutative ring R is the set of its prime ideals. We denote it by $\operatorname{Spec} R$. ◊

We now impose a topology on $\operatorname{Spec} R$.

Proposition 4.2 *Let R and S be commutative rings.*

1. *The sets*
$$V(I) := \{\mathfrak{p} \in \operatorname{Spec} R \mid I \subset \mathfrak{p}\}$$
as I ranges over all ideals of R are the closed sets for a topology on $\operatorname{Spec} R$.
2. *If $\varphi : R \to S$ is a homomorphism of rings, then the map $\varphi^\sharp : \operatorname{Spec} S \to \operatorname{Spec} R$ defined by*
$$\varphi^\sharp(\mathfrak{p}) = \varphi^{-1}(\mathfrak{p}) := \{r \in R \mid \varphi(r) \in \mathfrak{p}\}$$
is continuous.

Proof. (1) We must show that the subsets of $\operatorname{Spec} R$ of the form $V(I)$ satisfy the axioms to be the closed sets of a topological space.

Since $\emptyset = V(R)$ and $\operatorname{Spec} R = V(0)$, the empty set and $\operatorname{Spec} R$ themselves are closed subsets. Since a prime ideal $\mathfrak{p}$ contains a product IJ of ideals if and only if it contains one of them, $V(I) \cup V(J) = V(IJ)$. Induction shows that a finite union of closed sets is closed. On the other hand the intersection of a collection of closed sets $V(J_i)$ is closed because a prime $\mathfrak{p}$ contains each J_i if and only if it contains the sum of all of them; that is, $\bigcap_i V(J_i) = V(\sum_i J_i)$.

(2) Fix $\mathfrak{q} \in \operatorname{Spec} S$. First, $\varphi^\sharp(\mathfrak{q})$ is a prime ideal of R. It is an ideal because it is the kernel of the composition

$$\begin{tikzcd} R \arrow[r, "\varphi"] & S \arrow[r, "\pi"] & S/\mathfrak{q} \end{tikzcd}$$

where π is the natural map $\pi(s) = [s + \mathfrak{q}]$. And $\varphi^\sharp(\mathfrak{q})$ is prime because

$$R/\varphi^\sharp(\mathfrak{q}) = R/\ker(\pi\varphi) \cong \operatorname{im}\pi\varphi = \pi\varphi(R) \subset S/\mathfrak{q},$$

and a subring of a domain is a domain.

To show that $\varphi^\sharp$ is continuous it suffices to show that the inverse image of a closed set is closed. If I is an ideal of R, let J be the ideal of S generated by $\varphi(I)$. Then

$$\begin{aligned}(\varphi^\sharp)^{-1}(V(I)) &= \{\mathfrak{q} \in \operatorname{Spec} S \mid \varphi^\sharp(\mathfrak{q}) \in V(I)\}\\ &= \{\mathfrak{q} \in \operatorname{Spec} S \mid \varphi^\sharp(\mathfrak{q}) \supset I\}\\ &= \{\mathfrak{q} \in \operatorname{Spec} S \mid \ker(\pi_\mathfrak{q}\varphi) \supset I\}\\ &= \{\mathfrak{q} \in \operatorname{Spec} S \mid \ker(\pi_\mathfrak{q}) \supset \varphi(I)\}\\ &= \{\mathfrak{q} \in \operatorname{Spec} S \mid \mathfrak{q} \supset \varphi(I)\}\\ &= V(J).\end{aligned}$$

Hence $\varphi^\sharp$ is continuous. □

Definition 4.3 Let R be a commutative ring. The Zariski topology on $\operatorname{Spec} R$ is defined by declaring the closed sets to be those subsets of the form

$$V(I) := \{\mathfrak{p} \mid \mathfrak{p} \supset I\}$$

as I ranges over all ideals of R. ♢

Proposition 4.2 says that the rule $R \mapsto \operatorname{Spec} R$ is a contravariant functor from the category of commutative rings to the category of topological spaces.

Lemma 4.4 *The closed points in* $\operatorname{Spec} R$ *are exactly the maximal ideals.*

Proof. If $\mathfrak{m}$ is a maximal ideal of R then $V(\mathfrak{m}) = \{\mathfrak{m}\}$, so $\{\mathfrak{m}\}$ is a closed subspace of $\operatorname{Spec} R$.

On the other hand if $\mathfrak{p}$ is a non-maximal prime ideal in R and $\mathfrak{m}$ is a maximal ideal containing $\mathfrak{p}$, then any closed set $V(I)$ that contains $\mathfrak{p}$ also contains $\mathfrak{m}$; in particular, $\mathfrak{m} \in \overline{\{\mathfrak{p}\}}$. Hence $\{\mathfrak{p}\}$ is not closed. □

We write $\operatorname{Max} R$ for the set of maximal ideals in R.

If X is a closed subvariety of $\mathbb{A}^n$, there is a bijection

$$\begin{aligned}\{\text{points } x \in X\} &\longleftrightarrow \operatorname{Max} \mathcal{O}(X).\\ x &\longleftrightarrow \mathfrak{m}_x := \{\text{functions } f \in \mathcal{O}_X \text{ such that } f(x) = 0\}.\end{aligned}$$

Since $\mathfrak{m}_x$ is the kernel of the evaluation map $\varepsilon_x : \mathcal{O}(X) \to k$, $f \mapsto f(x)$, $\mathfrak{m}_x$ is a maximal ideal.

Let $\operatorname{Max} \mathcal{O}(X) \subset \operatorname{Spec} \mathcal{O}(X)$ have the subspace topology. The next result says that $\operatorname{Max} \mathcal{O}(X)$ is homeomorphic to X.

Proposition 4.5 *If X is a closed subvariety of $\mathbb{A}^n$ the map*

$$\begin{aligned}\Phi : X &\to \operatorname{Spec}\mathcal{O}(X)\\ x &\mapsto \mathfrak{m}_x := \{\textit{functions } f \in \mathcal{O}_X \textit{ such that } f(x)=0\}\end{aligned}$$

is continuous when X and $\operatorname{Spec}\mathcal{O}(X)$ *are given their Zariski topologies.*

Proof. By the Nullstellensatz, if k is algebraically closed Φ is a bijection between the set of maximal ideals in $\mathcal{O}(X)$ and the points of X. To see that Φ is continuous, let I be an ideal in $\mathcal{O}(X)$. Then

$$\Phi^{-1}(V(I)) = \Phi^{-1}(\{\mathfrak{p} \mid \mathfrak{p} \supset I\}) = \{x \in X \mid \mathfrak{m}_x \supset I\} = V(I),$$

which is a closed subset of X. □

Theorem 4.6 *Let $A \subset B$ be rings such that B is a finitely generated A-module. Then the map* $\operatorname{Spec} B \to \operatorname{Spec} A$*, $\mathfrak{p} \mapsto \mathfrak{p} \cap A$, is surjective.*

Proof. [Robson-Small] Let $\mathfrak{q} \in \operatorname{Spec} A$. Choose $\mathfrak{p} \in \operatorname{Spec} B$ maximal such that $A \cap \mathfrak{p} \subset \mathfrak{q}$; we now check that such $\mathfrak{p}$ exists. The set of ideals J in B such that $A \cap J \subset \mathfrak{q}$ is non-empty so, by Zorn's Lemma, there is an ideal $\mathfrak{p}$ in B that is maximal subject to $A \cap \mathfrak{p} \subset \mathfrak{q}$; such $\mathfrak{p}$ is prime because if there were ideals I and J of B strictly larger than $\mathfrak{p}$ such that $IJ \subset \mathfrak{p}$, then

$$(A \cap I)(A \cap J) \subset A \cap IJ \subset A \cap \mathfrak{p} \subset \mathfrak{q}$$

so either $A \cap I \subset \mathfrak{q}$ or $A \cap J \subset \mathfrak{q}$, contradicting the maximality of $\mathfrak{p}$.

It remains to show that $A \cap \mathfrak{p} = \mathfrak{q}$.

We now replace A by $A/A \cap \mathfrak{p}$, $\mathfrak{q}$ by $\mathfrak{q}/A \cap \mathfrak{p}$, and B by $B/\mathfrak{p}$. With these changes $A \subset B$, B is a domain, B is a finitely generated A-module, and $\mathfrak{q} \in \operatorname{Spec} A$ has the property that the only ideal I in B such that $I \cap A \subset \mathfrak{q}$ is $I = 0$. We will show that $\mathfrak{q} = 0$ and this will complete the proof.

Write $B = \sum_{i=1}^{t} Ab_i$ where $b_1 = 1$. We may assume that all b_i are non-zero, so $Ab_i \cong A$ as A-modules. Renumbering the b_is if necessary, we may pick m maximal such that $T = Ab_1 + \cdots + Ab_m$ is a direct sum, and hence a free A-module.

It follows that for all i, $J_i := \operatorname{Ann}_A(b_i + T/T)$ is a non-zero ideal of A. Since A is a domain, the product of the J_is is non-zero, and hence

$$J := \bigcap_{i=1}^{t} J_i$$

is a non-zero ideal of A.

Because $Jb_i \subset T$, it follows that $JB \subset T$, and hence $\mathfrak{q}JB \subset \mathfrak{q}T \subset T$. Now $\mathfrak{q}JB$ is a ideal of B and $\mathfrak{q}JB \cap A \subset \mathfrak{q}T \cap A = \mathfrak{q}$, the last equality being because $T = A \oplus C$ for some A-module C. The inclusion $\mathfrak{q}JB \cap A \subset \mathfrak{q}$ implies that $\mathfrak{q}JB = 0$, whence $\mathfrak{q} = 0$, as required. □

1.5 Irreducible affine varieties

We continue to work over an algebraically closed field k.

Definition 5.1 A topological space X is said to be irreducible if it is not the union of two proper closed subsets. $\Diamond$

Irreduciblity plays a central role in algebraic geometry.

Examples. The unit interval $[0, 1]$ is *not* irreducible with respect to the usual topology because it is the union of the proper closed subsets $[0, \frac{1}{2}] \cup [\frac{1}{2}, 1]$.

The affine line $\mathbb{A}^1$ over an infinite field is irreducible. The union of the two axes in $\mathbb{A}^2$ is not irreducible because it is the union of the individual axes, each of which is closed.

A topological reminder. A subset W of a topological space X is dense in X if $\bar{W} = X$, i.e., its closure is all of X. This is equivalent to the condition that $W \cap U \neq \phi$ for all non-empty open subsets U of X. (Exercise: prove this equivalence).

Lemma 5.2 *Every non-empty open subset of an irreducible topological space is dense.*

Proof. Let X be irreducible and $Z \subsetneq X$ a closed subspace. The equality $X = Z \cup \overline{(X - Z)}$ expresses X as a union of two closed sets so one of them must equal X. Thus $X = \overline{X - Z}$, and $X - Z$ is dense in X. $\square$

We show below that each closed subvariety of $\mathbb{A}^n$ can be written as a union of a finite number of irreducible subvarieties in a unique way; these irreducible subvarieties are called its irreducible components. This is analogous to writing an integer as a product of prime numbers. We have already seen one other extrapolation of this theme, namely the process of expressing an ideal of a Dedekind domain as a product of prime ideals.

Proposition 5.3 *The following conditions on a closed subvariety $X \subset \mathbb{A}^n$ are equivalent:*

1. *X is irreducible;*
2. *$I(X)$ is a prime ideal;*
3. *$\mathcal{O}(X)$ is a domain.*

Proof. Conditions (2) and (3) are equivalent (Definition 3.1).

Let $\mathfrak{p} = I(X)$.

(1) $\Rightarrow$ (2) Suppose that X is irreducible. To show that $\mathfrak{p}$ is prime, suppose that $fg \in \mathfrak{p}$. Then $Y := V(f, \mathfrak{p})$ and $Z := V(g, \mathfrak{p})$ are closed subsets of X. If $p \in X$, then $(fg)(p) = 0$ so p belongs to either Y or Z. Hence $X = Y \cup Z$. By hypothesis, either Y or Z is equal to X. But if $Y = X$, then f vanishes on X so $f \in \mathfrak{p}$. Hence $\mathfrak{p}$ is prime.

(2) ⇒ (1) Now assume $\mathfrak{p}$ is a prime ideal. Suppose Y and Z are closed subsets of X such that $X = Y \cup Z$. To show that X is irreducible we must show that either Y or Z is equal to X. Suppose that $Y \neq X$. The bijection in the strong nullstellensatz ensures that there is a function f that vanishes on Y but not on X. Now let $g \in I(Z)$. Let $p \in X$. Then p is in either Y or Z, so either f or g vanishes at p; hence fg vanishes at p. Hence $fg \in \mathfrak{p}$. But $f \notin \mathfrak{p}$, so $g \in \mathfrak{p}$. It follows that $I(Z) \subset \mathfrak{p}$, whence $Z = V(I(Z)) = V(\mathfrak{p}) = V(I(X)) = X$. □

A topological space X is said to be noetherian if any descending chain of closed subsets

$$X \supset Z_1 \supset Z_2 \supset \cdots$$

eventually stabilizes.

A closed subspace of a noetherian space is obviously noetherian.

Proposition 5.4 *Every affine variety is noetherian.*

Proof. Because the polynomial ring is noetherian, $\mathbb{A}^n$ is noetherian. Hence every closed subvariety $X \subset \mathbb{A}^n$ is noetherian. □

Proposition 5.5 *If X is a noetherian topological space, then there is a unique way of writing $X = X_1 \cup \cdots \cup X_n$ where each X_i is a closed irreducible subspace of X and $X_i \not\subset X_j$ if $i \neq j$.*

Proof. First we show that X is a finite union of irreducible subspaces. Suppose to the contrary that X is not such a union. In particular, X is not irreducible, so we can write $X = Y_1 \cup Z_1$ as a union of proper closed subspaces. If both Y_1 and Z_1 were finite unions of closed irreducible subspaces, X would be too, so one of them, say Z_1, is not such a union. In particular, Z_1 is not irreducible, so we can write $Z_1 = Z_2 \cup Y_2$ as a union of proper closed subspaces, and one of these, say Z_2, is not a finite union of irreducible subspaces.

Repeating this process leads to an infinite descending chain $Z_1 \supset Z_2 \supset \cdots$ of subspaces contradicting the hypothesis that X is noetherian. We therefore conclude that X is a finite union of irreducible subspaces.

It remains to prove the uniqueness. Suppose that $X = X_1 \cup \cdots \cup X_n = Y_1 \cup \cdots \cup Y_m$ where each X_i and each Y_s is irreducible and $X_i \not\subset X_j$ if $i \neq j$ and $Y_s \not\subset Y_t$ if $s \neq t$. Then the irreducible space $X_i = (X_i \cap Y_1) \cup \cdots \cup (X_i \cap Y_m)$ is a union of closed subspaces so must equal one of them, whence $X_i \subset SY_s$ for some s. Likewise each Y_s is contained in some X_j. But then $X_i \subset Y_s \subset X_j$, so $X_i = Y_s$. It follows that $m = n$ and $\{X_1, \ldots, X_n\} = \{Y_1, \ldots, Y_m\}$. □

Definition 5.6 The closed subspaces $X_1, \ldots, X_n$ appearing in Proposition 5.5 are called the irreducible components of X. ♢

Theorem 5.7 *The irreducible components of an affine algebraic variety X are $V(\mathfrak{p}_1), \ldots, V(\mathfrak{p}_n)$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are the minimal primes over $I(X)$.*

Proof. We can view X as a closed subvariety of some affine space $\mathbb{A}^m$. Let $I(X)$ be the ideal of functions vanishing on X. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the distinct minimal primes over X. Since $I(X)$ is radical, $I(X) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$, whence

$$X = V(\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n) = V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_n).$$

Now $X_i := V(\mathfrak{p}_i)$ is a closed irreducible subvariety of X, and because $\mathfrak{p}_j \not\subset \mathfrak{p}_i$ when $i \neq j$, $X_i \not\subset X_j$ when $i \neq j$. □

The minimal primes over a principal ideal fR in a UFD R are $p_1R, \ldots, p_nR$ where $p_1, \ldots, p_n$ are the distinct irreducible divisors of f. Hence the irreducible components of $V(f)$ are $V(p_1), \ldots, V(p_n)$. Expressing a variety as the union of its irreducible components is the geometric analog of expressing an element as a product of powers of irreducibles.

Theorem 5.7 suggests that we can examine an algebraic variety by studying one irreducible component at a time. This is why, in algebraic geometry texts, you will often see the hypothesis that the variety under consideration is irreducible. Of course, questions such as *how do the irreducible components intersect one another* cannot be studied one component at a time.

Lemma 5.8 *Let X be a subspace of a topological space Y. Then every irreducible component of X is contained in an irreducible component of Y.*

Proof. Let Z be an irreducible component of X. Write $Y = \cup_{i \in I} Y_i$ where the Y_is are the distinct irreducible components of Y. Then $Z = \cup_{i \in I}(Z \cap Y_i)$ expresses Z as a union of closed subspaces. But Z is irreducible so some $Z \cap Y_i$ is equal to Z; i.e., $Z \subset Y_i$ for some i. □

Lemma 5.9 *Let $f : X \to Y$ be a continuous map between topological spaces. Then*

1. *if X is irreducible so is $f(X)$;*
2. *if Z is an irreducible component of X, then $f(Z)$ is contained in an irreducible component of Y.*

Proof. (1) We can, and do, replace Y by $f(X)$ and $f(X)$ is given the subspace topology. If $f(X) = W_1 \cup W_2$ with each W_i closed in $f(X)$, then $X = f^{-1}(f(X)) = f^{-1}(W_1) \cup f^{-1}(W_2)$ so $X = f^{-1}(W_i)$ for some i. Thus $f(X) \subset W_i$. Hence $f(X)$ is irreducible.

(2) Let Z be an irreducible component of X. By (1), $f(Z)$ is an irreducible subspace of Y so, by Lemma 5.8, $f(Z)$ is contained in an irreducible component of Y. □

Connected components and idempotents. A topological space X is connected if the only way in which it can be written as a disjoint union of closed subsets $X = X_1 \sqcup X_2$ is if one of those sets is equal to X and the other is empty. There is a unique way of writing X as a disjoint union of connected subspaces, and those subspaces are called the connected components of X.

An affine algebraic variety has only finitely many connected components because it is noetherian.

An irreducible variety is connected, but the converse is not true: for example, the union of the axes $V(xy) \subset \mathbb{A}^2$ is conncted but not irreducible. Hence the decomposition of a variety into its connected components is a coarser decomposition than that into its irreducible components.

Suppose a variety X is not connected and write $X = X_1 \sqcup X_2$ with $X_1 \neq \phi$ and $X_2 \neq \phi$. Write $I_j = I(X_j)$. Then $I_1 \cap I_2 = 0$ because $X_1 \cup X_2 = X$, and $I_1 + I_2 = R$ because $X_1 \cap X_2 = \phi$. In other words, we have a direct sum decomposition $\mathcal{O}(X) = I_1 \oplus I_2$. Conversely, if $\mathcal{O}(X) = I \oplus J$ is a decomposition as a direct sum of two non-zero ideals, there is a non-trivial decomposition $X = V(I) \sqcup V(J)$.

If $\mathcal{O}(X) = I_1 \oplus I_2$ there is a unique way of writing $1 = e_1 + e_2$ with $e_j \in I_j$. It is clear that e_1 and e_2 are orthogonal idempotents, i.e., $e_j^2 = e_j$ and $e_1e_2 = e_2e_1 = 0$. Notice that e_1 is the function that is identically 1 on X_2 and zero on X_1.

More generally, a decomposition $X = X_1 \sqcup \cdots \sqcup X_n$ into connected components corresponds to a decomposition $1 = e_1 + \cdots + e_n$ of 1 as a sum of pairwise orthogonal idempotents.

1.6 Plane Curves

The simplest algebraic varieties after those consisting of a finite set of points are the plane curves. These have been of central importance in mathematics since ancient times. Earlier we defined a plane curve as $V(f)$ where $f \in k[x, y]$ is a non-constant polynomial (see Example 1.2) and showed that a plane curve has infinitely many points when k is algebraically closed. In this section we will show that the intersection of two distinct irreducible curves is a finite set.

We continue to work over an algebraically closed field k.

Lemma 6.1 *Let R be a UFD and $0 \neq f, g \in R[X]$. Then f and g have a common factor of degree ≥ 1 if and only if $af = bg$ for some non-zero $a, b \in R[x]$ such that $\deg a < \deg g$ (equivalently $\deg b < \deg f$).*

Proof. ($\Rightarrow$) If $f = bc$ and $g = ac$ where c is a common factor of degree ≥ 1, the $af = bg$ and $\deg a < \deg g$.

($\Leftarrow$) Suppose such a and b exist. Because $R[X]$ is a UFD we can cancel any common factors of a and b, so we will assume that a and b have no common factor. Since $R[X]$ is a UFD and $a|bg$ it follows that $a|g$. Thus $g = ac$ and $\deg c > 0$ since $\deg a < \deg g$. Now $af = bg = bac$ implies $f = bc$ so c is a common factor. □

Definition 6.2 Let R be a domain. The resultant, $R(f, g)$, of polynomials

$$f = a_0X^m + \ldots + a_{m-1}X + a_m$$
$$g = b_0X^n + \ldots + b_{n-1}X + b_n$$

in $R[X]$ of degrees m and n is the determinant of the $(m+n)\times(m+n)$ matrix

$$\begin{pmatrix}
a_0 & a_1 & \dots & a_m & 0 & \dots & & & & 0\\
0 & a_0 & a_1 & \dots & a_m & 0 & \dots & & & 0\\
\vdots & & & & & & & & & \vdots\\
b_0 & b_1 & \dots & b_{n-1} & b_n & 0 & \dots & & & 0\\
0 & b_0 & b_1 & \dots & b_{n-1} & b_n & 0 & \dots & & 0\\
\vdots & & & & & & & & & \vdots\\
0 & \dots & & & 0 & b_0 & b_1 & \dots & b_{n-1} & b_n
\end{pmatrix}$$

where there are n rows of the a's and m rows of the b's. ♢

Lemma 6.3 *Let R be a UFD and $0 \neq f, g \in R[X]$. Then f and g have a common factor of degree ≥ 1 if and only if $R(f,g) = 0$.*

Proof. By Lemma 6.1 it suffices to show that $R(f,g) = 0$ if and only if $af = bg$ for some $0 \neq a, b \in R[X]$ such that $\deg a < \deg g$ and $\deg b < \deg f$. It imposes no additional restriction to require that $\deg a = \deg g - 1$ and $\deg b = \deg f - 1$. There exist such polynomials

$$a = \sum_{i=0}^{n-1} c_i X^{n-1-i} \quad \text{and} \quad b = -\sum_{j=0}^{m-1} d_j X^{m-1-j}$$

if and only if

$$(c_0X^{n-1} + c_1X^{n-2} + \cdots + c_{n-2}X + c_{n-1})(a_0X^m + \cdots + a_{m-1}X + a_m) \qquad + \\ (d_0X^{m-1} + d_1X^{m-2} + \cdots + d_{m-2}X + d_{m-1})(b_0X^n + \cdots + b_{n-1}X + b_n) \;= 0.$$

Thus f and g have a common factor if and only if there is a solution to the matrix equation

$$\begin{pmatrix}
a_0 & a_1 & \dots & a_m & 0 & \dots & & & & 0\\
0 & a_0 & a_1 & \dots & a_m & 0 & \dots & & & 0\\
\vdots & & & & & & & & & \vdots\\
b_0 & b_1 & \dots & b_{n-1} & b_n & 0 & \dots & & & 0\\
0 & b_0 & b_1 & \dots & b_{n-1} & b_n & 0 & \dots & & 0\\
\vdots & & & & & & & & & \vdots\\
0 & \dots & & & 0 & b_0 & b_1 & \dots & b_{n-1} & b_n
\end{pmatrix}
\begin{pmatrix}
c_{n-1}\\ c_{n-2}\\ \vdots\\ c_0\\ d_{m-1}\\ \vdots\\ d_0
\end{pmatrix} = 0;$$

i.e., if and only if $R(f,g) = 0$. □

Proposition 6.4 *Let $f, g \in R[X]$. Then $R(f,g) = cf + dg$ for some $c, d \in R[X]$ with $\deg c = \deg g - 1$ and $\deg d = \deg f - 1$. In particular, $R(f,g)$ belongs to the ideal (f,g).*

Proof. For each $i = 1, \ldots, m+n$ multiply the i^{th} column of the matrix whose determinant is $R(f,g)$ by X^{m+n-i} and add it to the last column. This leaves all columns unchanged except the last which is now the transpose of

$$\begin{pmatrix} X^{n-1}f & X^{n-2}f & \ldots & Xf & f & X^{m-1}g & X^{m-2}g & \ldots & Xg & g \end{pmatrix}.$$

The determinant of this new matrix is the same as the determinant of the original one, namely $R(f,g)$. But computing the determinant by expanding this new matrix down the last column shows that $R(f,g) = cf + dg$. □

Corollary 6.5 *Let $f, g \in k[x,y]$ be polynomials of positive degree having no common factor. Then $V(f,g)$ is finite.*

Proof. Let I be the ideal of $k[x,y]$ generated by f and g.

First view f and g as polynomials in $R[x]$ where $R = k[y]$. Because f and g have no common factor $R(f,g) \neq 0$. But $R(f,g) \in k[y]$ and is also in I by Proposition 6.4. Hence $I \cap k[y] \neq 0$. Similarly, $I \cap k[x] \neq 0$.

Let $0 \neq a \in I \cap k[y]$ and $0 \neq b \in I \cap k[x]$. Then $V(f,g) \subset V(a,b) = V(a) \cap V(b)$. But $V(a)$ is a finite union of horizontal lines $\{\lambda\} \times \mathbb{A}^1$ where λ runs over the zeroes of $a \in k[y]$. Similarly, $V(b)$ is a finite union of vertical lines, so $V(a) \cap V(b)$ is finite. It follows that $V(f,g)$ is finite. □

Corollary 6.6 *Let k be an algebraically closed field, and let $f, g \in k[x]$ be polynomials of degree m and n respectively. Then f and g have a common zero if and only if $R(f,g) = 0$.*

Proof. If they have a common zero, say $\lambda \in k$ then they have the common factor $(x - \lambda)$, so $R(f,g) = 0$. Conversely, if $R(f,g) = 0$ then they have a common factor, and hence a common factor of degree 1, say $x - \lambda$, since k is algebraically closed. Thus $f(\lambda) = g(\lambda) = 0$. □

The next result gives a more concrete interpretation of the resultant $R(f,g)$: it is the determinant of a map which is rather naturally defined in terms of f and g. Before we state the result, recall that if R is a commutative ring, N a free R-module, and $\varphi : N \to N$ a R-module map, then a choice of basis for N allows us to express φ as a matrix with respect to that basis, and the determinant of that matrix may be defined in the usual way. Since the determinant is independent of the choice of basis, we may speak of the determinant of φ, $\det(\varphi)$, as a well-defined element of R.

Theorem 6.7 *Let R be a domain and suppose that $f = \sum_{i=0}^{m} a_i X^{m-i}$ and $g = \sum_{i=0}^{n} b_i X^{n-i}$ are polynomials in $R[X]$ such that a_0 and b_0 are units in R. Then $R[X]/(f)$ is a free R-module of rank m, and if $\varphi : R[X]/(f) \to R[X]/(f)$ is defined by $\varphi(a) = ga$, then*

$$\mathit{det}(\varphi) = cR(f,g)$$

for some unit $c \in R$.

Proof. The proof is given in several steps, and is finally completed by combining steps (2) and (7). For each $j \geq 1$ define $V_j = R \oplus RX \oplus \ldots \oplus RX^{j-1}$.

<u>Step 1</u> *Claim:* $R[X] = (f) \oplus V_m$. *Proof:* Since $deg(f) = m$, $(f) \cap V_m = 0$. The R-module $(f) + V_m$ contains $1, X, \ldots, X^{m-1}$ and also X^m since a_0 is a unit. Therefore, if $X^j = fa + b$ with $b \in V_m$ then $X^{j+1} = faX + bX$ is also in $(f) + V_m$. The result follows by induction on j.

<u>Step 2</u> It follows that the natural map $\gamma : V_m \to R[X] \to R[X]/(f)$ is a R-module isomorphism. Define $\psi : V_m \to V_m$ by $\psi = \gamma^{-1}\varphi\gamma$. Then $\det(\psi) = \det(\varphi)$.

<u>Step 3</u> *Claim:* if $w \in V_m$, then there is a unique $v \in V_n$ such that $fv + gw \in V_m$. *Proof:* Since $R[X] = (f) \oplus V_m$, and since $R[X]$ is a domain, there is a unique $v \in R[X]$ such that $fv + gw \in V_m$. Now $deg(fv) \leq \max\{deg(gw), m-1\} \leq m+n-1$, so $deg(v) \leq n-1$ as required.

<u>Step 4</u> For each $w \in V_m$ define $\theta(w) = X^m v$ where $v \in V_n$ has the property $fv + gw \in V_m$. The uniqueness of v ensures that we obtain a well-defined map $\theta : V_m \to X^m V_n$. It is routine to check that θ is a R-module homomorphism.

<u>Step 5</u> *Claim:* $R(f,g) = \det(\rho)$ where $\rho : V_{m+n} = X^m V_n \oplus V_m \to V_{m+n}$ is defined by $\rho(X^m v + w) = fv + gw$ for $v \in V_n$, $w \in V_m$. *Proof*: Consider the matrix representation of ρ with respect to the ordered basis $X^{m+n-1}, X^{m+n-2}, \ldots, X, 1$ for the free R-module V_{m+n}. We have

$$\begin{aligned}
\rho(X^{m+n-1}) &= fX^{n-1} = a_0X^{m+n-1} + a_1X^{m+n-2} + \ldots + a_mX^{n-1} \\
\rho(X^{m+n-2}) &= fX^{n-2} = a_0X^{m+n-2} + a_1X^{m+n-3} + \ldots + a_mX^{n-2} \\
&\vdots \\
\rho(X^m) &= f = a_0X^m + \ldots + a_m \\
\rho(X^{m-1}) &= gX^{m-1} = b_0X^{m+n-1} + b_1X^{m+n-2} + \ldots + b_nX^{m-1} \\
&\vdots \\
\rho(1) &= g = b_0X^{n-1} + \ldots + b_n
\end{aligned}$$

Thus the matrix representing ρ is

$$\begin{pmatrix}
a_0 & 0 & \ldots & 0 & b_0 & 0 & \ldots & 0 \\
0 & a_0 & \ldots & 0 & b_1 & b_0 & \ldots & 0 \\
\vdots & & & \vdots & \vdots & \vdots & & \vdots \\
a_m & a_{m-1} & \ldots & & & & \ldots & 0 \\
0 & a_m & \ldots & & & & \ldots & 0 \\
\vdots & & & \vdots & \vdots & \vdots & & \vdots \\
0 & 0 & \ldots & a_0 & b_{n-1} & & \ldots & \\
0 & 0 & \ldots & a_1 & b_n & b_{n-1} & \ldots & \\
0 & 0 & \ldots & a_2 & 0 & b_n & \ldots & \\
\vdots & & & \vdots & \vdots & \vdots & & \vdots \\
0 & 0 & \ldots & a_m & 0 & 0 & \ldots & b_n
\end{pmatrix}$$

which is the transpose of the matrix whose determinant is $R(f,g)$. Hence $\det(\rho) = R(f,g)$.

Step 6 *Claim:* $\psi = \rho(\theta+1)$ on V_m. *Proof:* Let $w \in V_m$. Then
$\gamma\rho(\theta+1)(w) = \gamma\rho(\theta(w)+w) = \gamma(fX^{-m}\theta(w)+gw) = \gamma(gw) = g\gamma(w) = \varphi\gamma(w)$
whence $\gamma\rho(\theta+1) = \varphi\gamma$. The claim follows since $\psi = \gamma^{-1}\varphi\gamma$.

Step 7 *Claim:* There is a unit $c \in R$ such that $\det(\rho) = c\det(\psi)$. *Proof:* If $u \in X^mV_n$ and $w \in V_m$, we will write the element $u+w \in V_{m+n} = X^mV_n \oplus V_m$ as a column vector $\binom{u}{w}$. We will also represent a R-module map $V_{m+n} \to V_{m+n}$ as a blocked matrix accordingly. For example, $\rho = \begin{pmatrix}\rho_{11} & \rho_{12}\\ \rho_{21} & \rho_{22}\end{pmatrix}$ where $\rho_{11} : X^mV_n \to X^mV_n$, $\rho_{12} : V_m \to X^mV_n$ etc. In particular

$$\begin{pmatrix}\rho_{11} & 0\\ \rho_{21} & \mathrm{Id}_{V_m}\end{pmatrix}\begin{pmatrix}u\\ w\end{pmatrix} = \begin{pmatrix}\rho_{11}(u)\\ \rho_{21}(u)+w\end{pmatrix} = \rho_{11}(u)+\rho_{21}(u)+w = \rho(u)+w.$$

Thus

$$\begin{aligned}\begin{pmatrix}\rho_{11} & 0\\ \rho_{21} & \mathrm{Id}_{V_m}\end{pmatrix}\begin{pmatrix}\mathrm{Id}_{X^mV_n} & -\theta\\ 0 & \psi\end{pmatrix}\begin{pmatrix}u\\ w\end{pmatrix} &= \begin{pmatrix}\rho_{11} & 0\\ \rho_{21} & \mathrm{Id}_{V_m}\end{pmatrix}\begin{pmatrix}u-\theta(w)\\ \psi(w)\end{pmatrix}\\ &= \rho(u-\theta(w))+\psi(w)\\ &= \rho(u)+\rho(w).\end{aligned}$$

Thus

$$\begin{pmatrix}\rho_{11} & 0\\ \rho_{21} & 1\end{pmatrix}\begin{pmatrix}1 & -\theta\\ 0 & \psi\end{pmatrix} = \rho,$$

from which it follows that $\det(\rho) = \det(\rho_{11})\det(\psi)$.

It remains to show that ρ_{11} is invertible, and hence that $\det(\rho_{11})$ is a unit in R. By definition, if $v \in V_n$ then $\rho_{11}(X^mv)$ is the component of $\rho(X^mv) = fv$ in X^mV_n. Since $fV_n \cap V_m = 0$, ρ_{11} is injective. On the other hand, ρ_{11} is a R-module map, so it is enough to show that $X^m, X^{m+1}, \dots, X^{m+n-1}$ are in the image of ρ_{11}. Now $\rho_{11}(X^m)$ is the component of f in X^mV_n, namely a_0X^m. Since a_0 is a unit, $X^m \in \mathrm{Im}(\rho_{11})$. Now $\rho_{11}(X^{m+1}) = a_0X^{m+1} + a_1X^m$, and since $X^m \in \mathrm{Im}(\rho_{11})$ we have $X^{m+1} \in \mathrm{Im}(\rho_{11})$. Continuing inductively yields the result. □

1.7 Morphisms between affine varieties

Algebraic geometry is the study of algebraic varieties *and* the maps between them.

Our next job is to specify the class of maps we allow between two affine algebraic varieties; i.e., what maps $\psi : X \to Y$ should we allow between closed subvarieties $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$? We will eventually call the allowable maps between two varieties morphisms, so the question is, what are the morphisms $\psi : X \to Y$ between two affine algebraic varieties?

The answer appears in Definition 7.1 below, but let's take our time getting there and see why that definition is reasonable.

We start with the case $\mathbb{A}^n \to \mathbb{A}^1 = k$. It is reasonable to allow the coordinate functions $x_i : \mathbb{A}^n \to k$ to be morphisms, and then agree that sums and products of such functions should also be morphisms. We therefore allow all polynomial maps $f : \mathbb{A}^n \to k$, $f \in k[x_1, \dots, x_n]$, to be morphisms and, since this is *algebraic* geometry, allow no other maps $\mathbb{A}^n \to k$ to be morphisms.

Returning to X, we allow the inclusion map $X \to \mathbb{A}^n$ to be a morphism. A composition of morphisms should be a morphism, because we want a *category* of algebraic varieties, so the composition of the inclusion $X \to \mathbb{A}^n$ with a polynomial map $f : \mathbb{A}^n \to k$ is a morphism. That is, if $f \in k[x_1, \dots, x_n]$ its restriction $f|_X$ is a morphism $X \to k$. The collection of such restriction maps is a subset of the ring of *all* k-valued functions on X. Since the sum and product of two such restrictions is the restriction of the sum and product respectively, the restrictions $f|_X$ form a subring of the ring of all functions $X \to k$. The rule $f \mapsto f|_X$ is a homomorphism from $k[x_1, \dots, x_n]$ onto this subring, so the subring is isomorphic to the quotient of $k[x_1, \dots, x_n]$ by the kernel. However, $f|_X$ is zero if and only if $f \in I(X)$ so the ring of all functions $f|_X$, $f \in k[x_1, \dots, x_n]$, is isomorphic to $k[x_1, \dots, x_n]/I(X)$.

The morphisms $X \to k$ are exactly the functions in $\mathcal{O}(X)$.

Let's return to the question of what maps $\psi : X \to Y$ we should allow as morphisms. Now Y is a subvariety of $\mathbb{A}^m$ and we have agreed that the inclusion $Y \to \mathbb{A}^m$ should be a morphism so, if ψ is a morphism, the composition

$$X \xrightarrow{\psi} Y \longrightarrow \mathbb{A}^m \tag{7-3}$$

should be a morphism $X \to \mathbb{A}^m$. We now make the reasonable requirement that ψ is a morphism if and only if the composition (7-3) is a morphism $X \to \mathbb{A}^m$. In other words, the morphisms $X \to Y$ are the morphisms $X \to \mathbb{A}^m$ whose images belong to Y.

We therefore ask, what maps $\psi : X \to \mathbb{A}^m$ should we allow to be morphisms? Choosing coordinate functions $x_1, \dots, x_m$ on $\mathbb{A}^m$, ψ can be written as

$$\psi(p) = (\psi_1(p), \cdots, \psi_m(p)) = (x_1(\psi(p)), \dots, x_m(\psi(p))), \qquad p \in X. \tag{7-4}$$

Each $\psi_i = x_i \circ \psi$ is a map $X \to k$. We have agreed that the coordinate functions $x_i : \mathbb{A}^m \to k$ are morphisms, so the compositions $x_i \circ \psi = \psi_i$ should be morphisms $X \to k$; that is, each ψ_i should belong to $\mathcal{O}(X)$. We now declare that $\psi : X \to \mathbb{A}^m$ is a morphism if and only if each ψ_i in (7-4) is a morphism $X \to k$. That is, each ψ_i must be given by a polynomial.

Definition 7.1 Let $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ be closed subvarieties. A map $\psi : X \to Y$ is a morphism, or regular map, or polynomial map, if there are polynomials $\psi_1, \dots, \psi_m \in k[x_1, \dots, x_n]$ such that

$$\psi(p) = (\psi_1(p), \cdots, \psi_m(p))$$

for all $p \in X$. ◊

For example, the map $\lambda \mapsto (\lambda^2, \lambda^3)$ is a morphism $\mathbb{A}^1 \to \mathbb{A}^2$. Its image is the curve $x^3 - y^2$. Similarly, the map $\mathbb{A}^1 \to \mathbb{A}^2$ given by $\lambda \mapsto (\lambda^2 - 1, \lambda(\lambda^2 - 1))$ is a morphism onto the curve $y^2 = x^2(x+1)$.

However, the inverse of the bijective map $\lambda \to (\lambda^2, \lambda^3)$ is *not* a morphism from $V(x^3 - y^2)$ to $\mathbb{A}^1$ (see Example 7.6).

Observe that the definition of a morphism is compatible with our earlier remarks. For example, the morphisms $X \to k$ are exactly the regular functions.

It is clear that the identity map $\mathrm{id}_X : X \to X$ is a morphism. It is easy to show that a composition of morphisms is a morphism. We may therefore speak of the category of affine algebraic varieties. The objects are the closed subvarieties of the affine spaces $\mathbb{A}^n$ and the morphisms are the maps defined in Definition 7.1.

Theorem 7.2 *Let $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ be closed subvarieties.*

1. *A morphism $\psi : X \to Y$ induces a ring homomorphism $\psi^* : \mathcal{O}(Y) \to \mathcal{O}(X)$ defined by composition of functions: that is, $\psi^*(f) = f \circ \psi$.*
2. *Every k-algebra homomorphism $\mathcal{O}(Y) \to \mathcal{O}(X)$ is of the form ψ^* for a unique morphism $\psi : X \to Y$.*
3. *If $\psi : X \to Y$ and $\varphi : Y \to Z$ are morphisms, then $(\varphi \circ \psi)^* = \psi^* \circ \varphi^*$.*
4. *The category of affine algebraic varieties is equivalent to the opposite of the category of finitely generated commutative k-algebras.*

Proof. (1) Every $f \in \mathcal{O}(Y)$ is a morphism $f : Y \to k$. Since a composition of morphisms is a morphism, $f \circ \psi$ belongs to $\mathcal{O}(X)$. It is clear that ψ^* is a ring homomorphism, and even a k-algebra homomorphism.

(2) Let $\varphi : \mathcal{O}(Y) \to \mathcal{O}(X)$ be a homomorphism of k-algebras. Write $\mathcal{O}(Y) = k[y_1, \dots, y_m]/I(Y)$ and $\mathcal{O}(X) = k[x_1, \dots, x_n]/I(X)$. It is helpful to think of φ as a homomorphism $k[y_1, \dots, y_m] \to \mathcal{O}(X)$ that vanishes on $I(Y)$.

Define $\psi_i = \varphi(y_i)$ and $\psi : X \to \mathbb{A}^m$ by

$$\psi(p) = (\psi_1(p), \dots, \psi_m(p)).$$

Now $\psi(p)$ belongs to Y because if $g \in I(Y)$, then

$$g(\psi(p)) = g((\psi_1(p), \dots, \psi_m(p)) = g(\psi_1, \dots, \psi_m)(p)$$

where $g(\psi_1, \dots, \psi_m)$ means substitute the polynomial ψ_i for y_i in $g(y_1, \dots, y_m)$. Hence

$$g(\psi_1, \dots, \psi_m) = g(\varphi(y_1), \dots, \varphi(y_m)) = \varphi(g) = 0$$

where the last equality is because φ vanishes on $I(Y)$. □

Two objects in a category are isomorphic if there are morphisms between them such that each of the two compositions of the maps is the identity. In particular, two varieties X and Y are isomorphic if and only if there are morphisms $\psi : X \to Y$ and $\varphi : Y \to X$ such that $\psi \circ \varphi = \mathrm{id}_Y$ and $\varphi \circ \psi = \mathrm{id}_X$.

Because of the equivalence of categories, we can rephrase this.

Proposition 7.3 *Two affine varieties X and Y are isomorphic if and only if the k-algebras $\mathcal{O}(X)$ and $\mathcal{O}(Y)$ are isomorphic.*

Corollary 7.4 *If X and Y are finite affine varieties, then $X \cong Y$ if and only if $|X| = |Y|$.*

Proof. ($\Rightarrow$) This is obvious.

($\Leftarrow$) By the remarks after Lemma 2.4, $\mathcal{O}(X)$ is equal to the ring of all functions $X \to k$. This ring obviously depends only on the cardinality of X. Hence the result. □

Remark. If X and Y are finite varieties then any set map $X \to Y$ is a morphism (because any map $X \to k$ is a regular function). Suppose that G is a finite group. Then we can view G as an affine variety, and the mutiplication map $G \times G \to G$ and the inversion $G \to G$, $g \mapsto g^1$, are morphisms. In this way G becomes an algebraic group (see later).

Example 7.5 Let $f(x) \in k[x]$ be any non-zero polynomial. Then the curve $y = f(x)$ is isomorphic to the affine line via the morphism $t \mapsto (t, f(t))$ and its inverse $(x, y) \mapsto x$. Equivalently, the k-algebra homomorphism $\phi : k[x, y] \to k[x]$ given by $\phi(x) = x$ and $\phi(y) = f(x)$ is surjective and has kernel $(y - f(x))$. ♢

Example 7.6 Not every continuous map between affine varieties is a morphism.

1. Recall that the closed subsets of $\mathbb{A}^1$ are just the finite subsets and $\mathbb{A}^1$ itself. It follows that every bijective set map $\mathbb{A}^1 \to \mathbb{A}^1$ is continuous in the Zariski topology. No doubt you can think of lots of bijective maps $\mathbb{C} \to \mathbb{C}$ that are not given by polynomial maps.

2. The map $\psi^{-1} : X \to \mathbb{A}^1$ that is the inverse of the morphism $\lambda \mapsto (\lambda^2, \lambda^3)$ to the cusp $X = V(y^2 - x^3)$, is bijective, hence continuous. But ψ^{-1} is not given by the restriction of a polynomial map $\mathbb{A}^2 \to k$ so is not a morphism. To verify this last claim, suppose to the contrary that ψ^{-1} is given by a polynomial $f \in k[x, y]$; i.e., $f|_C = \psi^{-1}$. In particular, if $\lambda \neq 0$, then $f(\lambda^2, \lambda^3) = \psi^{-1}(\lambda^2, \lambda^3) = \lambda$; in other words, $\lambda^3 f(\lambda^2, \lambda^3) = \lambda^2$. Hence $yf - x$ vanishes at (λ^2, λ^3).

Now $V(yf - x)$ is closed in $\mathbb{A}^2$ and contains $C \backslash \{0\}$, so contains C. Since $yf - x$ vanishes on C it is a multiple of $y^2 - x^3$. Passing to $k[x, y]/(y^2 - x^3)$ which is isomorphic to $k[t^2, t^3]$, this gives $t^3 \bar{f} = t^2$. That is not possible!

3. The Frobenius morphism. If $\operatorname{char} k = p$, the map $f \mapsto f^p$ from $k[x_1, \dots, x_n]$ to itself is a ring homomorphism. The corresponding morphism $\mathrm{Fr} : \mathbb{A}^n \to \mathbb{A}^n$, $(a_1, \dots, a_n) \to (a_1^p, \dots, a_n^p)$ is called the Frobenius morphism. It is bijective, hence a homeomorphism, but its inverse is not a morphism. ♢

Exercise. Let $f : X \to Y$ be a morphism. If X' is an irreducible component of X show that $f(X')$ is contained in one of the irreducible components of Y.

Proposition 7.7 *Let $f : X \to Y$ be a morphism between affine varieties and write $\phi : \mathcal{O}(Y) \to \mathcal{O}(X)$ for the corresponding ring homomorphism. Then*

1. *if $Z \subset Y$ is closed, then $f^{-1}(Z) = V(\phi(I(Z)))$;*

2. f is continuous,

3. if $W \subset X$ is closed, then $I(f(W)) = \phi^{-1}(I(W)) = I(\overline{f(W)})$;

4. $\ker \phi = I(f(X))$ and $\overline{f(X)} = V(\ker \phi)$;

5. ϕ is injective if and only if $f(X)$ is dense in Y;

6. the fibers $X_y := f^{-1}(y)$ are closed subvarieties of X;

7. $\mathfrak{m}_{f(x)} = \phi^{-1}(\mathfrak{m}_x)$.

Proof. (1) Let $J = I(Z)$. Then

$$\begin{aligned} f^{-1}(Z) &= \{x \in X \mid f(x) \in Z\} \\ &= \{x \in X \mid g(f(x)) = 0 \text{ for all } g \in J\} \\ &= \{x \in X \mid \phi(g)(x) = 0 \text{ for all } g \in J\} \\ &= V(\phi(J)). \end{aligned}$$

(2) Part (1) shows that the inverse image of a closed set is closed, so f is continuous.

(3) We have

$$\begin{aligned} I(f(W)) &= \{g \in \mathcal{O}(Y) \mid g(f(W)) = 0\} \\ &= \{g \in \mathcal{O}(Y) \mid \phi(g)(W) = 0\} \\ &= \{g \in \mathcal{O}(Y) \mid \phi(g) \in I(W)\} \\ &= \phi^{-1}(I(W)). \end{aligned}$$

(4) Applying (3) with $W = X$ gives

$$\ker \phi = \phi^{-1}(0) = \phi^{-1}(I(X)) = I(f(X)).$$

By Lemma 1.7, $\overline{f(X)} = V(I(f(X)) = V(\ker \phi)$.

(5) This follows from (4).

(6) and (7) are special cases of (1) and (3) respectively. □

A morphism $f : X \to Y$ need not send closed sets to closed sets. For example, the projection of the hyperbola $xy = 1$ onto the x-axis is a morphism and the image of the hyperbola is $\mathbb{A}^1 - \{0\}$.

Lemma 7.8 *If $f : X \to Y$ is a continuous map between topological spaces and X is irreducible, then both $f(X)$ and $\overline{f(X)}$ are irreducible (when given the subspace topology).*

Proof. Suppose $f(X) = Z \cup W$ where Z and W are closed subspaces of $f(X)$. Then $X = f^{-1}(Z) \cup f^{-1}(W)$ expresses X as a union of closed subspaces so one of them equals X, say $X = f^{-1}(Z)$. Then $f(X) = Z$, so $f(X)$ is irreducible.

We will now show that if U is any subspace of Y that is irreducible (with the induced subspace topology), then $\overline{U}$ is irreducible. The Lemma will follow when we apply this to $U = f(X)$.

If $\overline{U} = Z \cup W$, then $U = (U \cap Z) \cup (U \cap W)$ expresses U as a union of closed subspaces of itself; hence U is equal to either $U \cap Z$ or $U \cap W$, and either $U \subset Z$ or $U \subset W$, whence $\overline{U}$ is contained in either Z or W, and so equal to either Z or W. Hence $\overline{U}$ is irreducible. □

Dominant morphisms. When considering a continuous map $f : X \to Y$ between topological spaces one can frequently replace Y by $f(X)$ and consider instead the surjective map $f : X \to f(X)$. We can't quite do this when considering morphisms between varieties because $f(X)$ need not be an affine variety—the problem is that $f(X)$ need not be a *closed* subspace of Y. However, we can replace Y by $\overline{f(X)}$ and then consider the morphism $f : X \to \overline{f(X)}$ between varieties.

Definition 7.9 A morphism $f : X \to Y$ is dominant if $\overline{f(X)} = Y$, i.e., if the image of f is dense in Y. ♢

Part (5) of Proposition 7.7 says that $f : X \to Y$ is dominant if and only if the corresponding k-agebra homomorphism $\phi : \mathcal{O}(Y) \to \mathcal{O}(X)$ is injective. The hypothesis that a morphism is dominant is the geometric analogue of the hypothesis that a ring homomorphism is injective; or, it is the geometric analogue of *"subalgebra"*.

Part (2) of Lemma 7.8 allows us to restrict our attention to morphisms between *irreducible* algebraic varieties.

The next example further reinforces the idea that dominance rather than surjectivity is the key notion for morphisms.

Example 7.10 There exists a surjective morphism $f : X \to Y$ in which Y is irreducible but $f|_Z : Z \to Y$ is not surjective for any irreducible component Z of X.

Take $X = V(x(xy-1)) \subset \mathbb{A}^2$; then $X = L \cup C$ where L is the y-axis and C is the hyperbola $y = x^{-1}$, and these are the two irreducible components of X. Now let $Y = \mathbb{A}^1$ be the x-axis and $f : X \to Y$ the projection onto the x-axis; i.e., $f(x,y) = x$. Then Y is irreducible and f is surjective, but $f(L) = \{0\}$ and $f(C) = Y - \{0\}$, so neither $f|_L$ nor $f|_C$ is surjective. ♢

The function field of an irreducible variety. Let X be an irreducible affine variety over k. Then $\mathcal{O}(X)$ is a domain. We usually write $k(X)$ for the field of fractions of $\mathcal{O}(X)$ and call it the function field or the field of rational functions on X.

Let $f : X \to Y$ be a dominant morphism between irreducible varieties. Then $\mathcal{O}(X)$ is a domain and, since the homomorphism $\phi : \mathcal{O}(Y) \to \mathcal{O}(X)$ is injective, there is a commutative diagram of inclusions

$$\begin{tikzcd}\mathcal{O}(Y) \arrow[r] \arrow[d] & k(Y) \arrow[d] \\ \mathcal{O}(X) \arrow[r] & k(X).\end{tikzcd}$$

We therefore view $k(Y)$ and a subfield of $k(X)$.

Let X be an irreducible algebraic variety and $f \in k(X)$. Write $f = g/h$ where $g, h \in \mathcal{O}(X)$. We can evaluate f at those points $x \in X$ such that $h(x) \neq 0$. We usually write

$$X_h := \{x \in X \mid h(x) \neq 0\}.$$

This is an open subset of X because the zero locus of h is closed. Also, if h is not zero X_h is a non-empty (see Remark 1 after Proposition 2.2) open subset of X and hence dense. Thus f is defined on a dense open subset of X.

For example, the rational function $f = x/z = z/y$ on the surface $xy = z^2$ is defined at all points except $(0, 0, 0)$.

A finite intersection of dense open sets is dense and open so if we are given a finite number of non-zero regular functions on an irreducible X the locus where none of them vanishes is dense and open. Notice that an intersection of two dense subsets may be empty: for example the even (resp., odd) integers form a dense subset of $\mathbb{C}$ in the Zariski topology, but their intersection is empty.

Final examples. Consider an affine algebraic variety X. By Lemma 2.4, there are enough functions in $\mathcal{O}(X)$ to distinguish the points, and more generally disjoint closed subsets, of X. However, if x and y are different points of X the functions in $k + \mathfrak{m}_x\mathfrak{m}_y \subset \mathcal{O}(X)$ no longer distinguish x and y: if $f \in k + \mathfrak{m}_x\mathfrak{m}_y$, then $f(x) = f(y)$. Now $k + \mathfrak{m}_x\mathfrak{m}_y$ is a finitely generated k-subalgebra of $\mathcal{O}(X)$ so is the coordinate ring of some affine algebraic variety Y and the inclusion $\mathcal{O}(Y) \to \mathcal{O}(X)$ corresponds to a morphism $\pi : X \to Y$ with the property that $\pi(x) = \pi(y)$.

This is one crude way of constructing new varieties from old: by identifying points.

Another simle example of this is to consider the subring $k[x^2]$ of $k[x] = \mathcal{O}(\mathbb{A}^1)$. Functions in $k[x^2]$ take the same value at the points $p, -p \in \mathbb{A}^1$. Thus $k[x^2]$ is the coordinate ring of $\mathbb{A}^1/\sim$ where $\sim$ is the equivalence relation $p \sim -p$ on $\mathbb{A}^1$. Of course, $\mathbb{A}^1/\sim$ is still an affine line, but it is a *different* affine line than the original one.

One might be more ambitious and try to collapse a curve on a surface X to a single point. For example, if $R = k[x, y]$, then a function in $k + xR$ takes the same value at all points of the y-axis $V(x)$. However, $k + xR$ is not a finitely generated k-algebra (because it is not noetherian–why?) so is not the coordinate ring of an affine algebraic variety. However, the subalgebra $k[x, xy]$ of $k[x, y]$ is finitely generated and, because $k[x, xy] \subset k + xR$, a function in it takes the same value at all points $(0, *) \in \mathbb{A}^2$. Precisely, $k[x, xy]$ is also a polynomial ring in two variables so the inclusion $k[x, xy] \to k[x, y]$ corresponds to a morphism $\pi : \mathbb{A}^2 \to \mathbb{A}^2$ that sends the y-axis to the origin but is bijective elsewhere.

This example is also important because it shows that the fibers of a morphism can have different dimensions.

The other reason this example is important is because it is the simplest (partial) example of blowing up a point on a surface. From the point of view of the target X this map $\pi : \tilde{X} = \mathbb{A}^2 \to X = \mathbb{A}^2$ has replaced the single point $(0, 0) \in X$ by an affine line—we say we have blown up the origin.

Actually, blowing up a point on a surface really involves replacing the point by a *projective line* $\mathbb{P}^1$. Over $k = \mathbb{C}$, the projective line is the Riemann sphere $\mathbb{CP}^1$ so the point has been replaced by a sphere. Think of putting a straw into the point and puffing, thus producing a bubble, the sphere $\mathbb{CP}^1$.

Returning to the idea of passing from $\mathcal{O}(X)$ to $k+\mathfrak{m}_x\mathfrak{m}_y$, one could consider instead $k+\mathfrak{m}_x^2$. This is also a finitely generated k-algebra so is of the form $\mathcal{O}(Y)$ and the inclusion $\mathcal{O}(Y) \subset \mathcal{O}(X)$ corresponds to a map $\pi : X \to Y$. It is not hard to show that π is bijective (show that the map $\mathfrak{m} \mapsto \mathfrak{m} \cap \mathcal{O}(Y)$ is a bijection between the maximal ideals in $\mathcal{O}(X)$ and $\mathcal{O}(Y)$). However, $\pi : X \to Y$ is not an isomorphism because one has lost some first order data. For example, look at the case of $X = \mathbb{A}^1$ and the subring $k[t^2, t^3] \subset k[t]$. The map $\pi : X \to Y$ produces a singularity at the origin.. For example, look at the case of $X = \mathbb{A}^1$ and the subring $k[t^2, t^3] \subset k[t]$. The map $\pi : X \to Y$ produces a singularity at the origin.

1.8 Open subsets of an affine variety

We showed in section 1.2 that the topology on a closed subvariety $X \subset \mathbb{A}^n$ inherited from the Zariski topology on $\mathbb{A}^n$ may be described intrinsically in terms of $\mathcal{O}(X)$. Namely, the closed subsets of X are the

$$V(I) := \{x \in X \mid f(x) = 0 \text{ for all } f \in \mathcal{O}(X)\}.$$

The simplest such sets are those of the form $V(f)$, the zero loci of a single equation $f \in \mathcal{O}(X)$. Their open complements

$$X_f := \{x \in X \mid f(x) \neq 0\}$$

are called basic open sets. They play a particularly important role. Notice that $X_f \cap X_g = X_{fg}$.

If $Z \subset X$ is any closed set, say $Z = \{x \mid f_1(x) = \cdots = f_r(x) = 0\}$, then

$$X - Z = X_{f_1} \cup X_{f_2} \cup \cdots \cup X_{f_r},$$

so every open set is a finite union of basic open sets. In other words, the basic open sets provide a basis for the Zariski topology on X.

Proposition 8.1 *The open set X_f may be given the structure of an affine algebraic variety in such a way that the inclusion $X_f \to X$ is a morphism.*

Proof. Let $I = I(X)$ be the ideal of X, $x_1, \ldots, x_n$ a set of coordinate functions on $\mathbb{A}^n$, and let x_{n+1} be a new variable.. There is bijection

$$\begin{aligned} X_f &\longleftrightarrow V(I, fx_{n+1} - 1) \subset \mathbb{A}^{n+1} \\ p &\longleftrightarrow (p, f(p)^{-1}) \in \mathbb{A}^n \times \mathbb{A}^1 \end{aligned}$$

so we will identify X_f with the closed subvariety $V(I, fx_{n+1}-1)$ of $\mathbb{A}^{n+1}$. Doing this we find

$$\mathcal{O}(X_f) = \frac{\mathcal{O}(X)[x_{n+1}]}{(fx_{n+1} - 1)} = \mathcal{O}(X)[f^{-1}].$$

The projection map $\pi : \mathbb{A}^{n+1} \to \mathbb{A}^n$ onto the first n coordinates yields a commutative diagram

$$\begin{tikzcd} V(I, fx_{n+1} - 1) \arrow[r] \arrow[d, "i"'] & \mathbb{A}^{n+1} \arrow[d, "\pi"] \\ X = V(I) \arrow[r] & \mathbb{A}^n \end{tikzcd}$$

when restrictied to the indicated closed subvarieties. It is easy to see that i is a bijection onto X_f and is therefore a homeomorphism. The corresponding commutative diagram of k-algebra homomorphisms is

$$\begin{tikzcd} \mathcal{O}(X)[f^{-1}] & k[x_1, \ldots, x_n, x_{n+1}] \arrow[l] \\ \mathcal{O}(X) \arrow[u] & k[x_1, \ldots, x_n]. \arrow[l] \arrow[u] \end{tikzcd}$$

This completes the proof. □

Remark. Not every open subset of X can be given the structure of an algebraic variety. For example, $U = \mathbb{C}^2 - \{0\}$ can not be given the structure of an algebraic variety in such a way that the inclusion $U \to \mathbb{C}^2$ is a morphism. This is essentially because any regular function $f : U \to \mathbb{C}$ would be regular on $\mathbb{C} - \{\text{either axis}\}$ so would belong to $\mathbb{C}[x, y][x^{-1}] \cap \mathbb{C}[x, y][y^{-1}]$ which is equal to $\mathbb{C}[x, y]$. Thus the map $\mathcal{O}(\mathbb{C}^2) \to \mathcal{O}(U)$ is an isomorphism, but this is absurd because of the Nullstellensatz—it would say that the natural map $U \to \mathbb{C}^2$ is a bijection.

Of course, $\mathbb{C}^2 - \{0\}$ is not a pathological object so algebraic geometry must be adapted to accomodate it. This has been done long ago. What one does is this. Rather than having a single ring of functions on $\mathbb{C}^2 - \{0\}$, one has a sheaf of functions on $\mathbb{C}^2 - \{0\}$; that is, for every open subset U of $\mathbb{C}^2 - \{0\}$ one has a ring $\mathcal{O}(U)$ of $\mathbb{C}$-valued functions, and there are some obvious compatibilities between these rings that correspond to inclusions $U_1 \subset U_2$ and so on. The jargon is that $\mathbb{C}^2 - \{0\}$ is a *quasi-affine* algebraic variety.

More generally, if X is an irreducible affine algebraic variety and Z is a closed subvariety such that $\dim Z \leq \dim X - 2$, then $X - Z$ can not be given the structure of an affine algebraic variety.

Exercise. Let $f : X \to Y$ be a morphism between two affine algebraic varieties and let $\phi : \mathcal{O}(Y) \to \mathcal{O}(X)$ be the corresponding k-algebra homomorphism. If $g \in \mathcal{O}(Y)$, then $f^{-1}(Y_g) = X_{\phi(g)}$.

Birational Geometry. One of the long-standing themes in algebraic geometry is *birational* geometry. Two irreducible varieties X and Y are birational or birationally equivalent if $k(X) \cong k(Y)$. A central problem in algebraic geometry is to find, for a given variety X a nice variety Y that is birational to X. Of course one wants Y to be "nicer" than X in some way. For example, one might ask that Y be smooth. Of course, one can always do that because X has a dense open subset that is smooth, so one asks also that there be a surjective morphism $f : Y \to X$ with Y smooth and f an isomorphism on a dense open set. Hironaka won the Fields Medal for proving that this is possible in characteristic zero. You will win the Fields medal if you can prove the result in positive charateristic.

The close relationship between a pair of birationally equivalent varieties is exhibited by the following observation.

Proposition 8.2 *Two irreducible varieties are birational if and only if they possess isomorphic dense open subvarieties.*

Proof. Let X and Y be the irreducible varieties in question.

($\Rightarrow$) This is more straightforward than the proof suggests—the difficulty lies in finding the domains of definition of the appropriate morphisms.

Suppose $\phi : k(Y) \to k(X)$ is an isomorphism. Write $\mathcal{O}(Y) = k[y_1, \dots, y_m]$ and $\phi(y_i) = a_i b_i^{-1}$ where $a_i, b_i \in \mathcal{O}(X)$. If we set $b = \prod b_i$, then

$$\phi(\mathcal{O}(Y)) \subset \mathcal{O}(X)[b^{-1}].$$

In other words, if $X' = X_b$, the restriction of ϕ to $\mathcal{O}(Y)$ corresponds to a morphism

$$f : X' \to Y.$$

Similarly, there is a non-empty open subset $Y' \subset Y$ such that restriction of ϕ^{-1} to $\mathcal{O}(X)$ corresponds to a morphism

$$g : Y' \to X.$$

Define

$$X_0 := f^{-1}g^{-1}(X') \subset X' \qquad \text{and} \qquad Y_0 := g^{-1}f^{-1}(Y') \subset Y'.$$

Because f is the morphism corresponding to an injective homomorphism $\mathcal{O}(Y) \to \mathcal{O}(X')$, $f(X')$ is dense in Y; thus $Y' \cap f(X') \neq \phi$ and $f^{-1}(Y') \neq \phi$; repeating this argument we see that $g^{-1}f^{-1}(Y') \neq \phi$ also. Thus X_0 and Y_0 are non-empty open subvarieties of X and Y.

We now show that $f(X_0) \subset Y_0$ and $g(Y_0) \subset X_0$. We will prove the first of these inclusions; the same argument with the roles of X and Y reversed will then establish the second inclusion.

By definition, $f(X_0) \subset g^{-1}(X')$. Let $y \in g^{-1}(X')$. Then $y \in Y'$ and $fg(y) \in f(X')$. Because f and g are the morphisms corresponding to (restrictions of) ϕ and ϕ^{-1}, $fg(y) = y$. Thus $y \in g^{-1}f^{-1}(y) \subset g^{-1}f^{-1}(Y') = Y_0$. Hence $f(X_0) \subset g^{-1}(X') \subset Y_0$. Similarly, $g(Y_0) \subset X_0$.

Now consider f and g as morphisms between X_0 and Y_0. Because these two morphisms correspond to (restrictions of) ϕ and ϕ^{-1} it follows that $fg = \mathrm{id}_{Y_0}$ and $gf = \mathrm{id}_{X_0}$.

($\Leftarrow$) Let $X_0 \subset X$ and $Y_0 \subset Y$ be non-empty open subsets and $f : X_0 \to Y_0$ an isomorphism. Then f induces an isomorphism $\mathcal{O}(Y_0) \to \mathcal{O}(X_0)$ and extends to an isomorphism $k(Y_0) \to k(X_0)$ between the fields of fractions. But the inclusions $X_0 \to X$ and $Y_0 \to Y$ also induce morphisms $\mathcal{O}(X) \to \mathcal{O}(X_0)$ and $\mathcal{O}(Y) \to \mathcal{O}(Y_0)$ that extend to isomorphisms $k(X) \to k(X_0)$ and $k(Y) \to k(Y_0)$. All this can be expressed in the commutative diagram

$$\begin{tikzcd}
\mathcal{O}(Y) \arrow[r] \arrow[d] & \mathcal{O}(X) \arrow[d] \\
\mathcal{O}(Y_0) \arrow[r] \arrow[d] & \mathcal{O}(X_0) \arrow[d] \\
k(Y) = k(Y_0) \arrow[r] & k(X_0) = k(X).
\end{tikzcd}$$

This is long-winded. The point is simply that X is birational to every non-empty open subvariety of itself. □

In other words, birational varieties are almost isomorphic.

Theorem 8.3 *Let X be an irreducible affine algebraic variety. Then X is birational to a hypersurface.*

Proof. (Characteristic zero.) Write $K = k(X)$. We must show there is a hypersurface Y such that $k(Y) \cong K$.

Noether normalization provides a polynomial subalgebra $S = k[x_1, \ldots, x_d]$ over which $\mathcal{O}(X)$ is integral. Now K is a finite extension of $F = \operatorname{Fract} S$ so the Primitive Element Theorem tells us there is a single $a \in K$ such that $K = F(a)$. In other words, $K \cong F[T]/(f)$ where f is the minimal polynomial of a. We can replace f by any non-zero scalar multiple of itself so we can, and will, assume that the coefficients of f belong to S.

Define $Y \subset \mathbb{A}^{d+1}$ to be the zero locus of the polynomial $f \in S[T] = k[x_1, \ldots, x_d, T]$. Thus Y is a hypersurface and there is a surjective map $S[T] \to S[a]$, $T \mapsto a$, whose kernel is (f) because f is the minimal polynomial of a over F. Thus $\mathcal{O}(Y) \cong S[a]$ and $k(Y) = \operatorname{Fract} \mathcal{O}(Y) \cong \operatorname{Fract} S[a] = F(a) = K$. □

A further advantage of the birational perspective is that the study of fields is a branch of algebraic geometry. Given a finitely generated field $K = k(x_1, \ldots, x_n)$, there are many varieties having K as their function field. The geometric properties of those varieties gives insight into the field K.

For example, let K be a finite extension of $\mathbb{C}(x)$, the function field in one variable. There is a unique smooth projective curve X having K as its function field. Not only is X an algebraic variety but it is also a compact Riemann surface, and as such we can speak of its topological genus, the number of "holes" in it. The genus of X is then an invariant of the field K. The only smooth projective curve of genus zero is the projective line $\mathbb{P}^1$, or $\mathbb{CP}^1$ if you prefer to think of it as the Riemann sphere. Its function field is $\mathbb{C}(x)$. The affine line $\mathbb{A}^1_{\mathbb{C}}$ is a dense open subvariety of $\mathbb{P}^1$.

The fields of genus one are of the form $\mathbb{C}(X)$ where $X \subset \mathbb{C}^2$ is the zero locus of a curve of the form $y^2 = x(x-1)(x-\lambda)$ where $\lambda \neq 0, 1$. This is an open subset of the plane projective curve $Y^2Z = X(X-Z)(X-\lambda Z)$.

1.9 Some algebra

Lemma 9.1 *Let I be a finitely generated ideal in a domain R. If $I \neq 0$ and $I \neq R$, then $I \neq I^2$.*

Proof. Suppose $I^2 = I = x_1R + \cdots + x_nR$. Then there are elements $a_{ij} \in I$ such that

$$x_i = x_1a_{i1} + \cdots + x_na_{in}$$

for all $i = 1, \ldots, n$. We can arrange this as a matrix equation

$$(x_1 \cdots x_n)M = 0$$

where M is the $n \times n$ matrix with entries

$$M_{ij} = \begin{cases} a_{ii} - 1 & \text{if } i = j \\ a_{ij} & \text{if } i \neq j. \end{cases}$$

Notice that every non-diagonal element of M belongs to I and the product of the diagonal elements is of the form $(-1)^n + b$ with $b \in I$. It follows that $\det M = (-1)^n + c$ with $c \in I$. However $\underline{x}M = 0$ so $\det M = 0$. Hence $1 \in I$. □

Theorem 9.2 (Krull's Intersection Theorem) *Let I be an ideal in a commutative noetherian ring R. If $b \in \cap_{n=1}^{\infty} I^n$, then $b \in bI$. If $I \neq R$ and R is either a domain or local, then $\cap_{n=1}^{\infty} I^n = 0$.*

Proof. We may write $I = a_1R + \cdots + a_tR$. Since $b \in I^n$ there is a homogeneous polynomial $P_n(X_1, \ldots, X_t) \in R[X_1, \ldots, X_t]$ of degree n such that $b = P_n(a_1, \ldots, a_t)$. Since $R[X_1, \ldots, X_t]$ is noetherian there is an integer n such that P_{n+1} is in the ideal generated by $P_1, \ldots, P_n$, say $P_{n+1} = Q_1P_1 + \cdots + Q_nP_n$

and each Q_i is homomogeneous of degree ≥ 1. Hence

$$\begin{aligned} b &= P_{n+1}(a_1, \ldots, a_t) \\ &= \sum_{i=1}^{n} Q_i(a_1, \ldots, a_t) P_i(a_1, \ldots, a_t) \\ &= b \sum_{i=1}^{n} Q_i(a_1, \ldots, a_t) \in bI. \end{aligned}$$

Now suppose $I \neq R$. If R is a domain, then $\cap_{n=1}^{\infty} I^n = 0$ because $b = bx$ with $x \in I$ implies $b = 0$. If R is local, then $b = bx$ implies $b(1-x) = 0$ but $1 - x$ is a unit so $b = 0$. □

The next result is already part of Theorem 4.6 but we state it again here because it is the key to the results on finite morphisms that appear in the next section. Also the proof we give now is the one usually appearing in commutative algebra texts.

Proposition 9.3 *Let R be a subring of S and suppose that S is a finitely generated R-module. If $\mathfrak{m}$ is a maximal ideal of R, then there is a maximal ideal $\mathfrak{n}$ of S such that $\mathfrak{n} \cap R = \mathfrak{m}$.*

Proof. We can write $S = \sum_{j=1}^{n} R s_j$ with $s_1 = 1$.

First we show that $S \neq S\mathfrak{m}$. Suppose to the contrary that $S = S\mathfrak{m}$. Then $S = \sum s_j R\mathfrak{m} = \sum s_j \mathfrak{m}$. For each $i = 1, \ldots, n$, we may write $s_i = \sum_j r_{ij} s_j$ for suitable $r_{ij} \in \mathfrak{m}$. In other words, $\sum_{j=1}^{n} (\delta_{ij} - r_{ij}) s_j = 0$. Let M be the $n \times n$ matrix with ij^{th} entry $\delta_{ij} - r_{ij}$, set $\Delta = \det M$ and write $\underline{s}$ for the column vector $(s_1, \ldots, s_n)^{\mathsf{T}}$. Thus $M\underline{s} = 0$, and

$$0 = (M^{\text{adj}}) M \underline{s} = \Delta \underline{s}$$

where M^{adj} is the adjoint matrix. Hence $\Delta s_i = 0$ for all i; in particular, $0 = \Delta s_1 = \Delta = \det(\delta_{ij} - r_{ij})$. Writing out this determinant explicitly we see that $1 \in \mathfrak{m}$. This is a contradiction, so we conclude that $S \neq S\mathfrak{m}$.

Since $S\mathfrak{m}$ is a proper ideal of S it is contained in a maximal ideal, say $\mathfrak{n}$. Then $\mathfrak{n} \cap R \supset \mathfrak{m}$, and $1 \notin \mathfrak{n}$, so $\mathfrak{n} \cap R = \mathfrak{m}$ because $\mathfrak{m}$ is maximal. □

1.10 Finite morphisms

Definition 10.1 A morphism $f : X \to Y$ between affine varieties X and Y is finite if $\mathcal{O}(X)$ is a finitely generated $\mathcal{O}(Y)$-module via the induced k-algebra homomorphism $\phi : \mathcal{O}(Y) \to \mathcal{O}(X)$.

The degree of a finite surjective morphism $f : X \to Y$ between *irreducible* varieties is $[k(X) : k(Y)] = \dim_{k(Y)} k(X)$, the degree of the field extension. ◊

Remarks. The k-algebra homomorphism $\phi : \mathcal{O}(Y) \to \mathcal{O}(X)$ corresponding to a finite surjective morphism $f : X \to Y$ is injective by Proposition 7.7 so, when X and Y are irreducible, it induces an injective map $k(Y) \to k(X)$. Hence the definition of degree makes sense.

Theorem 10.2 *Let $f : X \to Y$ be a finite dominant morphism. Suppose that $\mathcal{O}(X)$ is generated by $\le t$ elements as an $\mathcal{O}(Y)$-module. Then*

1. *$|f^{-1}(y)| \le t$ for all $y \in Y$;*
2. *f is surjective;*
3. *f sends closed sets to closed sets.*

Proof. The hypothesis that f is dominant says that the corresponding k-algebra homomorphism $\phi : \mathcal{O}(Y) \to \mathcal{O}(X)$ is injective, so we will simply view $\mathcal{O}(Y)$ as a subalgebra of $\mathcal{O}(X)$.

(1) Let $\mathfrak{m}$ be the maximal ideal of $\mathcal{O}(Y)$ vanishing at y. Then $f^{-1}(y) = V(\phi(\mathfrak{m}))$. The morphism $f^{-1}(y) \to \{y\}$ induces a commutative diagram

$$\begin{tikzcd}
\mathcal{O}(Y) \arrow[r, "\phi"] \arrow[d] & \mathcal{O}(X) \arrow[d] \\
\frac{\mathcal{O}(Y)}{\mathfrak{m}} = \mathcal{O}(\{y\}) \arrow[r] & \mathcal{O}(f^{-1}(y)) = \frac{\mathcal{O}(X)}{\sqrt{\phi(\mathfrak{m})\mathcal{O}(X)}}.
\end{tikzcd}$$

of k-algebra homomorphisms. Therefore $\mathcal{O}(f^{-1}(y)$ is generated by $\le t$ elements as a module over $\mathcal{O}(\{y\}) \cong k$, i.e., $\mathcal{O}(f^{-1}(y))$ is a k-vector space of dimension $\le t$. It now follows from Proposition 2.6 that $f^{-1}(y)$ is finite with cardinality $\le t$.

(2) This is an immediate consequence of Proposition 9.3 because of the bijection between points and maximal ideals.

(3) Let $W \subset X$ be closed. It suffices to show that $f(W) = \overline{f(W)}$. The restriction $f|_W : W \to \overline{f(W)}$ is a morphism of varieties. The corresponding k-algebra homomorphism fits into the commutative diagram

$$\begin{tikzcd}
\mathcal{O}(Y) \arrow[r, "\phi"] \arrow[d] & \mathcal{O}(X) \arrow[d] \\
\frac{\mathcal{O}(Y)}{I(f(W)} = \mathcal{O}(\overline{f(W)}) \arrow[r] & = \frac{\mathcal{O}(X)}{I(W)} = \mathcal{O}(W).
\end{tikzcd}$$

The bottom map is injective because $I(f(W)) = \phi^{-1}(I(W))$. Hence by (1) applied to $f|_W$, $f|_W$ is a surjective morphism $W \to \overline{f(W)}$. □

For example, the inclusion $k[x^2] \to k[x]$ makes $k[x]$ a finitely generated $k[x^2]$-module, generated by 1 and x for example, so the corresponding morphism $\psi : \mathbb{A}^1 \to \mathbb{A}^1$ is surjective with finite fibers. Explicitly, if $\lambda \in \mathbb{A}^1$, then

$$\psi^{-1}(\lambda) = \begin{cases} 0 & \text{if } \lambda = 0 \\ \pm\sqrt{\lambda} & \text{if } \lambda \neq 0 \end{cases}.$$

Let Q be the surface over $\mathbb{C}$ cut out by $xy = z^2$ in $\mathbb{A}^3$. Write $u = \frac{1}{2}(x+y)$ and $u = \frac{1}{2i}(x-y)$. Then $x = u+iv$ and $y = u-iv$ so the equation $xy = z^2$ becomes $u^2+v^2 = z^2$. This makes it easier to picture the real surface as the doubly infinite icecream cone with vertex at the origin. The map $\psi : k[x,y,z]/(xy-z^2) \to k[s,t]$ defined by $x \mapsto s^2$, $y \mapsto t^2$, and $z \mapsto st$, makes $k[s,t]$ a finitely generated $\mathcal{O}(Q)$-module, generated by $1, s, t$ for example. The map $\psi : \mathbb{A}^2 \to Q$, $(s,t) \mapsto (s^2, t^2, st)$ is therefore surjective with finite fibers. What are the cardinalities of the fibers?

Example 10.3 Let $f : \mathbb{A}^2 = X \to \mathbb{A}^2 = Y$ be the morphism defined by $f(x,y) = (xy, y)$. The corresponding k-algebra homomorphism $\phi : \mathcal{O}(Y) = k[s,t] \to \mathcal{O}(X) = k[x,y]$ is given by $\phi(s) = xy$ and $\phi(t) = y$. It is better to think of ϕ as the inclusion $k[xy,y] \to k[x,y]$. The image of ϕ is $\{(\alpha,\beta) \mid \beta \neq 0\} \cup \{(0,0)\}$. It is clear that $\overline{f(X)} = Y$. Notice that $f^{-1}((0,0)) = (*,0)$ but for every other point $p = (\alpha,\beta) \in f(X)$, $f^{-1}(p) = (\alpha\beta^{-1},\beta)$ is a singleton. In particular, we see that one of the fibers is a line and all other fibers are singletons. Notice too that it now follows that $k[x,y]$ is not a finitely generated module over $k[xy,y]$. $\Diamond$

The upper bound on the cardinality of the fibers in Theorem 10.2 is far from the best possible result. We will now prove the definitive result: the cardinality of the fibers is at most $\deg f$.

First we show that $\deg f$ is no more than the number of generators for $\mathcal{O}(X)$ as a $\mathcal{O}(Y)$-module.

Lemma 10.4 *Let S be a domain with field of fractions L. Let R be a subring of S and consider $K = \operatorname{Fract} R$ as a subfield of L. If S is generated by t elements as an R-module, then $\dim_K L \leq t$ and S contains a K-basis for L.*

Proof. Suppose $S = Rs_1 + \cdots + Rs_t$. Then $Ks_1 + \cdots + Ks_t$ is a subring of L because

$$s_i s_j \in \sum_{k=1}^{t} Rs_k \subset \sum_{k=1}^{t} Ks_k.$$

Now $Ks_1 + \cdots + Ks_t$ is a domain and a finite dimensional K-vector space so is a field. But this field contains S so must equal L. It follows that $L = Ks_1 + \cdots + Ks_t$, and the result follows because some subset of $\{s_1, \ldots, s_n\}$ must provide a basis for L over K. $\square$

Exercise. In the situation of Lemma 10.4 show that a subset of L is linearly independent over K if and only if it is linearly independent over R.

Theorem 10.5 *Let $f : X \to Y$ be a finite dominant morphism between irreducible varieties. Then the fibers of f have cardinality at most the degree of f and some fiber has that cardinality.*

Proof. In order to lighten the notation we will write $R = \mathcal{O}(Y) \subset S = \mathcal{O}(X)$, $K = k(Y) \subset L = k(X)$, and $n = \deg f = [L : K]$. There are inclusions

$$\begin{tikzcd}
Y & R \arrow[r] \arrow[d] & K \arrow[d] \\
X \arrow[u, "f"] & S \arrow[r] & L.
\end{tikzcd}$$

By Lemma 10.4,

$$L = Kf_1 \oplus \cdots \oplus Kf_n$$

for some $f_1, \ldots, f_n \in S$. Without loss of generality we may assume that $f_1 = 1$, so

$$R \subset Rf_1 \oplus \cdots \oplus Rf_n \subset S.$$

Consider the finitely generated R-module

$$M = S/(Rf_1 \oplus \cdots Rf_n).$$

Let $s \in S$ and write $\bar{s}$ for its image in M. Since $s = a_1 f_1 + \cdots + a_n f_n$ for some $a_i \in K$, there is a non-zero $x \in R$ such that $xs \in Rf_1 + \cdots + Rf_n$. Hence $\mathrm{Ann}(\bar{s}) \neq 0$. Now M is a finitely generated R-module, say $M = Rm_1 + \cdots + Rm_t$, so $\mathrm{Ann} M = \cap_{i=1}^{t} \mathrm{Ann}(m_i)$ and this is non-zero because a finite intersection of non-zero ideals in a domain is non-zero (look at their product!).

Write $J = \mathrm{Ann} M$. Then $Y - V(J)$ is non-empty and open, hence dense. Pick $y \in Y - V(J)$ and let $\mathfrak{m}_y$ be the maximal ideal of R vanishing at y. Then $J + \mathfrak{m}_y = R$. But

$$\frac{S}{\mathfrak{m}_y S + Rf_1 + \cdots + Rf_n}$$

is annihilated by $\mathfrak{m}_y + J$ so must be zero. In other words, as an R-module, and thus as an $R/\mathfrak{m}_y$-module, $S/\mathfrak{m}_y S$ is generated by the images of $f_1, \ldots, f_n$. Thus

$$\dim_k \frac{S}{\mathfrak{m}_y S} \leq n = \deg f.$$

Hence, as in the proof of Theorem 10.2, $|f^{-1}(y)| \leq n$.

It remains to prove that this bound is obtained. □

Noether normalization again. Let X be a closed subvariety of $\mathbb{A}^n$. The coordinate ring $\mathcal{O}(X)$ is a finitely generated k-algebra, so Noether normalization says that $\mathcal{O}(X)$ contains a polynomial ring $k[y_1, \ldots, y_m]$ such that $\mathcal{O}(X)$ is integral, and hence a finitely generated module, over $k[y_1, \ldots, y_m]$. The inclusion $k[y_1, \ldots, y_m] \to \mathcal{O}(X)$ is a homomorphism of k-algebras, so corresponds to a morphism $\psi : X \to \mathbb{A}^m$. By Corollary **??**, ψ is surjective with finite fibers.

Let's reconsider the example, $k[t+t^{-1}] \subset k[t, t^{-1}]$. Now, $k[t, t^{-1}] \cong k[x, y]/(xy-1)$, so $k[t, t^{-1}]$ is isomorphic to the hyperbola $xy = 1$; let's write X for this hyperbola. Since $k[t + t^{-1}]$ is the polynomial ring in one variable, it is the coordinate ring of the affine line. Hence the inclusion $k[t + t^{-1}] \to k[t, t^{-1}]$

corresponds to a morphism $X \to \mathbb{A}^1$. That morphism is given by $(x,y) \mapsto x+y$, or $(x,x^{-1}) \mapsto x+x^{-1}$. The surjectivity says that for every $\alpha \in k = \mathbb{A}^1$, there is a point $(x,x^{-1}) \in X$ such that $x+x^{-1} = \alpha$; this is nothing more than the statement that because k is algebraically closed the equation $x^2+1 = \alpha x$ has a solution in k. Because $k[t,t^{-1}]$ is generated by two elements as a $k[t+t^{-1}]$-module, there are at most two points in each fiber $\psi^{-1}(\alpha)$.

Contrast this with the inclusion $k[t] \subset k[t,t^{-1}]$. The associated morphism $X \to \mathbb{A}^1$ is given by $(x,x^{-1}) \mapsto x$. This morphism is not surjective (0 is not in the image). This tells us at once that $k[t,t^{-1}]$ is not a finitely generated $k[t]$-module.

Example 10.6 Let $R = k[t]$ and $S = k[x,y]$ be the polynomial rings in one and two variables respectively. If $\phi : k[t] \to k[x,y]$ is any k-algebra homomorphism, then $k[x,y]$ is not a finitely generated $k[t]$-module.

Proof: If $\ker\phi \neq 0$, then $\operatorname{im}\phi$ has finite dimension so the infinite dimensional vector space $k[x,y]$ cannot be a finitely generated $k[t]$-module.

Now suppose ϕ is injective. The corresponding morphism $f : \mathbb{A}^2 \to \mathbb{A}^1$ is the map $p \mapsto \phi(t)(p)$ so $f^{-1}(0)$ is the zero locus of the polynomial $\phi(t)$. By Theorem 10.2 $f^{-1}(0)$ is finite; but Example 1.2 shows this can only happen if $\phi(t)$ is a constant; but in that case ϕ is not injective. We conclude that there is no map ϕ making $k[x,y]$ a finitely generated $k[t]$-module. ♢

1.11 Finite group actions

Let $G \subset \operatorname{Aut} X$ be a finite group of automorphisms acting on a variety X. Let's write $X/\!\sim$ for the set of orbits for the moment. One of the most important constructions in algebraic geometry is the imposition of an algebraic variety structure on $X/\!\sim$.

The strategy we employ to do this is not one you have met before. So far we have defined and/or constructed all varieties as explicit subvarieties of particular affine spaces. In contrast, we will first define a particular subring $\mathcal{O}(X)^G \subset \mathcal{O}(X)$, then show there is a variety having $\mathcal{O}(X)^G$ as its coordinate ring, then introduce the notation X/G for that variety. We do *not* know what X/G is at this stage—all we know is its coordinate ring. The inclusion $\mathcal{O}(X)^G \to \mathcal{O}(X)$ corresponds to a morphism $\pi : X \to X/G$ as in Theorem 7.2 and we will use the algebraic properties of this inclusion to show that π is surjective and $\pi(x) = \pi(y)$ if and only if $Gx = Gy$. In other words, the points of X/G are in bijection with the orbits and the fibers of the map $\pi : X \to X/G$ are exactly the orbits. Thus, there is a bijection between $X/\!\sim$ and X/G with the property that the diagram

$$\begin{tikzcd}
& X \arrow[dl] \arrow[dr, "\pi"] & \\
X/\!\sim \arrow[rr, leftrightarrow, "\text{1-1}"] & & X/G
\end{tikzcd}$$

commutes.

In order to explain why $\mathcal{O}(X)^G$ (defined below) is a good candidate for the coordinate ring of $X/\sim$ let's forget algebraic geometry for a moment and just think of G as a group acting on a set X and write $X/\sim$ for the set of orbits. Write $R(X)$ and $R(X/\sim)$ for the rings of k-valued functions on X and $X/\sim$ respectively. Every function $f : X/\sim \to k$ induces a function $\bar{f} : X \to k$, $x \mapsto f(Gx)$. The map $f \mapsto \bar{f}$ is obviously injective, so we can think of $R(X/\sim)$ as a subring of $R(X)$. What subring is it? The crucial point is this:

> *if $f \in R(X/\sim)$, then as a function on X it takes the same value at x and gx for every $x \in X$ and $g \in G$ because $f(x)$ is really $f(Gx)$ and, likewise, $f(gx)$ is really $f(Ggx)$ BUT $Gx = Ggx$ so $f(x) = f(gx)$.*

Just as any map $\pi : X \to Y$ between two sets induces a ring homomorphism $R(Y) \to R(X)$, $f \mapsto f\pi$, each $g \in G$ induces a map $R(X) \to R(X)$, $f \mapsto f \circ g$. I prefer to write $f \circ g$ as f^g because the roles of f and g are very different: $f : X \to k$ but I now want to think of g as giving an automorphism $f \mapsto f^g = f \circ g$ of $R(X)$. In this situation we define

$$R^G := \{f \in R \mid f^g = f \text{ for all } g \in G\}.$$

Notice that R^G consists of the k-valued functions on X that are constant along each orbit. The previous paragraph shown that the subring $R(X/G)$ of $R(X)$ belongs to $R(X)^G$.

If $f \in R(X)$ is constant along orbits then we may also view f as a function $X/G \to k$ because the map $Gx \mapsto f(x)$ is unambiguous. We have therefore shown that $R(X/G)$ is equal to R^G.

If a group G acts as automorphisms of a ring R the subring of invariants is

$$R^G := \{r \in R \mid r^g = r \text{ for all } g \in G\}.$$

This is a ring because 0 and 1 are invariants, and products, sums, and differences, of invariants are again invariants. Usually R is a k-algebra and G acts as k-linear transformations, in which case R^G is a k-algebra.

Theorem 11.1 (Hilbert-Noether) *Let k be a field and R a finitely generated commutative k-algebra. Let G be a finite group acting as automorphisms of R. Then*

1. *R^G is a finitely generated k-algebra, and*

2. *R is a finitely generated R^G-module.*

Proof. An element $r \in R$ is a zero of the monic polynomial

$$f(x) := \prod_{\sigma \in G} (x - r^\sigma) \in R[x].$$

The action of G on R extends to an action of G on $R[x]$ by declaring that $x^\sigma = x$ for all $\sigma \in G$. The action of G on $f(x)$ permutes its factors, so $f(x) \in R^G[x]$. Thus r is integral over R^G.

Write $R = k[r_1, \ldots, r_n]$ and let $f_i \in R^G[x]$ be a monic polynomial satisfied by r_i. The subalgebra $S \subset R^G$ generated by the coefficients appearing in the f_is is a finitely generated k-algebra and hence noetherian. Because its generators are integral over S, R is integral over S. Because R is finitely generated as an S-algebra it is a noetherian S-module. Therefore R^G is a noetherian S-module, hence a finitely generated k-algebra, a noetherian ring, and R is a finitely generated R^G-module. □

Proposition 11.2 *Let R be a domain and K its field of fractions. Let G be a finite group acting as automorphisms of R. Then*

1. *K^G is the field of fractions of R^G;*
2. *K is generated by R and K^G;*
3. *if the map $G \to \operatorname{Aut} R$ is injective, then K is a Galois extension of K^G with Galois group G.*

Proof. (1) Certainly K^G is a subfield of K. A non-zero element a in K^G can be written as bc^{-1} with $b, c \in R$. But $d := \prod_{\sigma \in G} c^\sigma$ belongs to R^G and $a = (bc^{-1}d)d^{-1}$; but $bc^{-1}d \in R$ and is also G-invariant because it is equal to ad, so $a \in \operatorname{Fract} R^G$.

(2) Let T be the subring of K generated by R and K^G. Now K is integral over K^G because $q \in K$ satisfies the monic polynomial $\prod_{\sigma \in G}(x - q^\sigma) \in K^G[x]$. Hence T is integral over K^G. But an integral extension of a field is a field, so T is a field. But $R \subset T$ so $K \subset T$ too; thus $K = T$ as required.

(3) The hypothesis implies that the induced map $G \to \operatorname{Aut} K$ is injective, so we will consider G as a subgroup of $\operatorname{Aut} K$. By a theorem of E. Artin, $[K : K^G] = |G|$. Certainly, $G \subset \operatorname{Aut}(K/K^G)$; also, the subfield of K fixed by $\operatorname{Aut}(K/K^G)$ is exactly K^G, so another application of Artin's theorem tells us that $[K : K^G] = |\operatorname{Aut}(K/K^G)|$, so we must have $G = \operatorname{Aut}(K/K^G)$. Hence K/K^G is a Galois extension. □

A more formal way of stating part (2) is to say that the multiplication map $R \otimes_{R^G} K^G \to K$ is an isomorphism.

Definition 11.3 Let G be a finite group of automorphisms acting on an irreducible affine algebraic variety X. We define the quotient variety X/G to be the variety whose ring of regular functions is $\mathcal{O}(X)^G$, i.e.,

$$\mathcal{O}(X/G) := \mathcal{O}(X)^G.$$

We call the morphism

$$\pi : X \to X/G$$

corresponding to the inclusion $\mathcal{O}(X)^G \to \mathcal{O}(X)$ the quotient map. ◊

Remarks. 1. We defined an affine variety as a Zariski-closed subset of $\mathbb{A}^n$. But in this definition we are *not* defining X/G as a particular closed subset of any particular $\mathbb{A}^n$. What happens is this: we know $\mathcal{O}(X)^G$ is finitely generated so there is a *surjective* map $k[x_1, \ldots, x_n] \to \mathcal{O}(X)^G$ for some large integer n, and this map will have a kernel I and $V(I) \subset \mathbb{A}^n$ is an affine variety whose coordinate ring is isomorphic to $\mathcal{O}(X)^G$. But another person may pick a completely different set of generators for $\mathcal{O}(X)^G$ and so be led to a different $V(I') \subset \mathbb{A}^{n'}$ whose coordinate ring is isomorphic to $\mathcal{O}(X)^G$. Thus, X/G is really only defined up to isomorphism!

2. Recall the discussion on page 28: although a subalgebra R of $\mathcal{O}(X)$ is a ring of functions on X there may not be sufficiently many functions in R to distinguish all the points of X, and that the closed points of $\operatorname{Spec} R$ are obtained by collapsing together the points of X that R fails to distinguish. This idea applies to $\mathcal{O}(X)^G$. Functions in $\mathcal{O}(X)^G$ cannot distinguish between two points belonging to the same orbit so X/G is obtained from X by crushing each orbit to a single point.

Theorem 11.4 *Let $G \subset \operatorname{Aut} X$ be a finite group acting on an affine algebraic variety X. The quotient morphism $\pi : X \to X/G$ is surjective and its fibers are exactly the orbits. If X is irreducible, then $\mathcal{O}(X)$ is integral over $\mathcal{O}(X/G)$ and* $\deg \pi = |G|$.

Proof. By Theorem 11.1, $\mathcal{O}(X)$ is integral over $\mathcal{O}(X)^G$ so π is surjective by Theorem 10.2.

By the Remark after Proposition 2.2, to show that $\pi(x) = \pi(gx)$ it suffices to show that $f(\pi(x)) = f(\pi(gx))$ for all $f \in \mathcal{O}(X)^G$. However, $f \circ \pi$ is really just f since we are identifying $\mathcal{O}(X/G)$ with $\mathcal{O}(X)^G \subset \mathcal{O}(X)$.

Now suppose $x, y \in X$ have distinct orbits. Then Gy and Gx are distinct closed sets so there is a function $f \in \mathcal{O}(X)$ such that $f(gx) = 1$ and $f(gy) = 0$ for all $g \in G$. The function $F := \prod_{g \in G} f^g$ is certainly in $\mathcal{O}(X)^G$, and $F(x) = 1$ and $F(y) = 0$. Hence $\pi(x) \neq \pi(y)$.

The previous two paragraphs show that the fibers of π are exactly the orbits of G. □

Finally, we show that X/G, or rather the pair consisting of X/G and the quotient map $\pi : X \to X/G$, has an appropriate universal property.

Proposition 11.5 *Let G be a finite group acting on an affine algebraic variety X and suppose that $\rho : X \to Y$ is a morphism that is constant on each G-orbit. Then there is a unique morphism $\delta : X/G \to Y$ such that $\rho = \delta\pi$.*

Proof. Let $\psi : \mathcal{O}(Y) \to \mathcal{O}(X)$ be the k-algebra homomorphism corresponding to ρ. The hypothesis that ψ is constant on each orbit means that if $g \in G$, then $\rho = \rho \circ g$. Hence if $f \in \mathcal{O}(Y)$, then $\psi(f)^g = (f \circ \rho)^g = f \circ \rho \circ g = f \circ \rho = \psi(f)$. In other words $\psi(f) \in \mathcal{O}(X)^G$, so we get a factorization $\psi = \phi\theta$ where $\phi : \mathcal{O}(X)^G \to \mathcal{O}(X)$ is the inclusion and $\theta : \mathcal{O}(Y) \to \mathcal{O}(X)^G$ is just ψ viewed as a map to $\mathcal{O}(X)^G$. Hence, if $\delta : X/G \to Y$ is the morphism corresponding to θ, the equality $\psi = \phi\theta$ gives $\rho = \delta\pi$. □

Some precision. We adopt the convention that G acts from the *left* on geometric objects such as topological spaces, varieties, and manifolds. Thus if X is a geometric object on which G acts, then $g.(h.x) = (gh).x$ for all $g, h \in G$ and $x \in X$.

If R is a ring of functions on X, there are two induced actions of G on R. We can either define $g.f$ by $(g.f)(x) = f(g^{-1}x)$ or $(g.f)(x) = f(g.x)$. The first option leads to a *left* action of G on the ring of functions and the second leads to a *right* action of G on the ring of functions.

We prefer the second alternative and the notation f^g for the function defined by

$$f^g(x) := f(gx).$$

Thus $f^{gh} = (f^g)^h$.

The notation f^g is compatible with notation you already use! Let u be a unit in a ring R. The notation u^n, $n \in \mathbb{Z}$, can be thought of as indicating an action of $\mathbb{Z}$ on the set of powers of u. Or, if you prefer, the notation r^n can be thought of as indicating the action of the semigroup $\mathbb{N}$ on R.

1.12 Basic constructions

To illustrate the ideas in the preceeding sections we now turn to some examples and applications.

The product of two varieties. If $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ are closed subvarieties, then $X \times Y$ is a closed subvariety of $\mathbb{A}^{n+m} = \mathbb{A}^n \times \mathbb{A}^m$. To see this, suppose that $I(X) = (a_1, \dots, a_s) \subset k[x_1, \dots, x_n]$ and $I(Y) = (b_1, \dots, b_t) \subset k[y_1, \dots, y_n]$. Then $X \times Y$ is the zero locus of the ideal in $k[x_1, \dots, x_m, y_1, \dots, y_n]$ generated by $a_1, \dots, a_s, b_1, \dots, b_t$.

Even before one knows that $X \times Y$ is a closed subvariety there are some obvious functions $X \times Y \to k$. If $f \in \mathcal{O}(X)$ and $g \in \mathcal{O}(Y)$ we define the function

$$f \otimes g : X \times Y \to k$$

by

$$(p, q) \mapsto f(p)g(q), \qquad (p, q) \in X \times Y.$$

Using the $+$ in k we can add such functions to obtain k-valued functions

$$f_1 \otimes g_1 + \cdots + f_t \otimes g_t$$

on $X \times Y$. Every regular function on $X \times Y$ is of this form. All this is quite tautological. The ring of regular functions on $\mathbb{A}^1 \times \mathbb{A}^1$ is $k[x, y]$ where x is the coordinate function on the first $\mathbb{A}^1$ and y is the coordinate function on the second $\mathbb{A}^1$, and every regular function is of the form

$$\sum_{i,j} \alpha_{ij} x^i y^j = \sum_{i,j} \alpha_{ij} x^i \otimes y^j.$$

In fact

$$\mathcal{O}(X \times Y) \cong \mathcal{O}(X) \otimes \mathcal{O}(Y).$$

Corresponding to the obvious k-algebra homomorphisms $\mathcal{O}(X) \to \mathcal{O}(X) \otimes_k \mathcal{O}(Y)$ and $\mathcal{O}(Y) \to \mathcal{O}(X) \otimes_k \mathcal{O}(Y)$ are the projection morphisms $\pi_1 : X \times Y \to X$ and $\pi_2 : X \times Y \to Y$. Let $f : Z \to X$ and $g : Z \to Y$ be morphisms. Then there is a morphism $(f, g) : Z \to X \times Y$ defined by $(f, g)(z) := (f(z), g(z))$. Check that $f = \pi_1 \circ (f, g)$ and $g = \pi_2 \circ (f, g)$.

Exercises. 1. Suppose that $h : Z \to W$, $f' : W \to X$, and $g' : W \to Y$ are morphisms such that $f'h = f$ and $g'h = g$. Show there is a unique morphism $\psi : X \times Y \to W$ such that $h = \psi \circ (f, g)$.

2. Suppose that k is algebraically closed. If I and J are radical (resp., prime) ideals in $A = k[x_1, \ldots, x_n]$ and in $B = k[y_1, \ldots, y_m]$, show that the zero ideal in $A/I \otimes_k A/J$ is is radical (rep., prime).

3. Show that the hypothesis on k in the previous example is essential by showing that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \oplus \mathbb{C}$ and that if $K = \mathbb{F}_p(x)$ and $k = \mathbb{F}_p(x^p) \subset K$, then $x \otimes 1 - 1 \otimes x \in K \otimes_k K$ is nilpotent.

The diagonal. Let X be an affine algebraic variety. The diagonal,

$$\Delta := \{(x, x) \mid x \in X\} \subset X \times X\},$$

is a closed subvariety of X because it is the common zero locus of the elements $1 \otimes f - f \otimes 1 \in \mathcal{O}(X \times X) = \mathcal{O}(X) \otimes_k \mathcal{O}(X)$ as f runs over all elements of $\mathcal{O}(X)$.

The locus where $f = g$. Let $f, g : X \to Y$ be morphisms. The locus where f and g agree, namely

$$\{x \in X \mid f(x) = g(x)\} \subset X$$

is closed because it is $(f, g)^{-1}(\Delta_Y)$.

The graph of a morphism. The graph of a morphism $f : X \to Y$ is

$$\Gamma_f := \{(x, f(x)) \mid x \in X\} \subset X \times Y\}$$

and it is a closed subvariety of $X \times Y$ because the diagonal $\Delta \subset Y \times Y$ is closed and $\Gamma_f = (f, \mathrm{id}_Y)^{-1}(\Delta)$. The ideal in $\mathcal{O}(X \times Y) = \mathcal{O}(X) \otimes_k \mathcal{O}(Y)$ defining Γ_f is generated by elements of the form

$$1 \otimes g - \phi(g) \otimes 1$$

where $g \in \mathcal{O}(Y)$ and $\phi : \mathcal{O}(Y) \to \mathcal{O}(X)$ is the k-algebra homomorphism corresponding to $f : X \to Y$.

Some varieties associated to the action of a finite group. Let G be a finite group acting on an affine algebraic variety X. For each $g \in G$ we define

$$X^g := \{x \in X \mid gx = x\}$$

for each $g \in G$. Since X^g is the locus where the morphisms $\mathrm{id}_X : X \to X$ and $g : X \to X$ agree it is a closed subvariety of X. More generally, if S is any subset of G, then

$$X^S := \bigcap_{g \in S} X^g$$

is closed. For example, if H is a subgroup of G, then

$$X^H = \{x \in X \mid H \subset \mathrm{Stab}_G(x)\}$$

is closed. Therefore, for each integer n, the set

$$X_n := \{x \in X \mid |Gx| \leq n\}$$

is closed because it is the union of the X^Hs as H runs over all those subgroups of G such that $|G : H| \leq n$. Hence we get an ascending chain

$$X^G = X_1 \subset \cdots \subset X_{|G|} = X$$

of closed subvarieties. If $\pi : X \to X/G$ is the quotient morphism, then $\pi(X_n)$ is closed and

$$\pi(X_n) = \{\bar{x} \in X/G \mid |\pi^{-1}(\bar{x})| \leq n\}.$$

It is a general result that if $f : X \to Y$ is a finite morphism the sets $\{y \in Y \mid |f^{-1}(y)| \leq n\}$ are closed. The way in which this is proved is important because it illustrates a rather general idea: we translate the question into a question about the number of zeroes of a polynomial in $k[t]$. That is, we obtain a variety of degree d polynomials and show that the subset consisting of thse polynomials having $\leq n$ distinct zeroes is closed.

1.13 Examples

In this section we establish some results having the general form:

> *almost every point on a variety X has property P*

where the property P depends on the matter being considered. First we make the phrase "almost all" precise.

Definition 13.1 If the set of points on a variety X having property P is dense and open we will say almost all points on X have property P. ♢

Proposition 13.2 *Almost all monic polynomials of degree d in one variable over an algebraically closed field have d distinct zeroes.*

Proof. First we give the set of degree d monic polynomials $f \in k[t]$ the structure of an algebraic variety. Such a polynomial can be written uniquely as

$$f(t) = t^d + a_1 t^{d-1} + \cdots + a_{d-1} t + a_d,$$

so we can view f as the point

$$f = (a_1, \dots, a_d) \in \mathbb{A}^d = Y.$$

There are coordinate functions $y_1, \dots, y_d$ defined by $y_i(f) = a_i$, the coefficient of t^{d-i}. We now define a morphism

$$\begin{aligned} \pi : X = \mathbb{A}^d &\longrightarrow Y = \mathbb{A}^d \\ \pi(\alpha_1, \dots, \alpha_d) &= (t-\alpha_1)(t-\alpha_2)\cdots(t-\alpha_d) \\ &= \sum_{i=0}^{d} (-1)^i s_i(\alpha_1, \dots, \alpha_d) t^{d-i} \end{aligned}$$

where $s_i(\alpha_1, \dots, \alpha_d)$ is the i^{th} symmetric function

$$\begin{aligned} s_0(\alpha_1, \dots, \alpha_d) &= 1 \\ s_1(\alpha_1, \dots, \alpha_d) &= \alpha_1 + \cdots + \alpha_d \\ s_2(\alpha_1, \dots, \alpha_d) &= \sum_{i,j=1}^{n} \alpha_i \alpha_j \\ &\text{et cetera.} \end{aligned}$$

Notice that $\pi^{-1}(f)$ is the set of zeroes of f counted with multiplicity. The k-algebra homomorphism $\phi : k[y_1, \dots, y_d] \to k[x_1, \dots, x_d]$ corresponding to π is

$$\phi(y_n) = \sum_{i_1, \dots, i_n = 1}^{d} (-1)^n x_{i_1} \cdots x_{i_n}.$$

Since ϕ is injective we view $\mathcal{O}(Y)$ as the subalgebra

$$\mathcal{O}(Y) = k[s_1, \dots, s_d] \subset k[x_1, \dots, x_d] = \mathcal{O}(X).$$

Now $\mathcal{O}(X)$ is integral over $\mathcal{O}(Y)$ because each x_i is a zero of the monic polynomial

$$(t - x_1)(t - x_2)\cdots(t - x_d) \in \mathcal{O}(Y)[t].$$

By Theorem 10.2, π is surjective, has finite fibers, and

$$\{f \mid f \text{ has a multiple zero}\} = \pi(\Delta)$$

is closed because

$$\Delta := V\Bigg(\prod_{1 \le i < j \le d} (x_i - x_j) \Bigg) \subset \mathbb{A}^d$$

is closed. Thus the set of monic polynomials having d distinct zeroes is the dense open set $Y - \pi(\Delta)$. □

The morphism π in the previous proof is the quotient morphism $\pi : \mathbb{A}^d \to \mathbb{A}^d/S_d$ for the action of the symmetric group S_d on $\mathbb{A}^d$.

Remark. It is probably better to prove the following result. Let $Y = k[t]_{\le d} \cong \mathbb{A}^{d+1}$ denote the set of polynomials of degree $\le d$. Then

$$Y_i := \{f \in Y \mid f \text{ has } \le i \text{ distinct zeroes}\} \tag{13-5}$$

is a closed subvariety of Y. Hence there is a chain of closed subspaces

$$Y_0 \subset Y_1 \subset \cdots \subset Y_d = k[t]_{\le d}.$$

In particular, $Y - Y_{d-1}$, which is the set of degree d polynomials having d distinct zeroes, is open. If k is algebraically closed it is infinite so there *is* a degree d polynomial having d distinct zeroes, whence $Y - Y_{d-1}$ is dense an open.

Question. Can you show that almost all polynomials in $\mathbb{Q}[t]$ of degree $\le n$ $(n \ge 2)$ are irreducible?

Proposition 13.3 *Let $X \subset \mathbb{A}^n$ be the zero locus of an irreducible polynomial $f \in k[x_1, \ldots, x_n]$ of degree d. Let $p \in \mathbb{A}^n$. Then almost every line through p meets X at d distinct points.*

Proof. First we give the set of lines in $\mathbb{A}^n$ passing through p the structure of an affine algebraic variety. For each $0 \ne q \in k^n$, let

$$L_q := \{p + \lambda q \mid \lambda \in k\}$$

be the line through p in the direction of q. Every line through p is of the form L_q. We will write $X = k^n - \{0\}$ and consider this as the set of lines through p. (Of course, this is not a variety, at least as we have defined a variety, because it is not a closed subspace of k^n...however, this can be fixed by enlarging our category from affine varieties to quasi-affine varieties defined as the open subspaces of affine varieties.) There is another reasonable objection: if $0 \ne \mu \in k$, then $L_{\mu q} = L_q$, so the rule $q \mapsto L_q$ is not a bijection between the points of X and the lines through p. This objection is met by passing to projective varieties, the most basic example of which is $\mathbb{P}^{n-1}$ the set of lines through the origin in k^n, and taking $X = \mathbb{P}^{n-1}$. But we won't do this here, we will just work with X acknowledging the shortcomings of using X to parametrize the lines through p.

The basic observation is that

$$L_q \cap X = \{p + \lambda q \mid f(p + \lambda q) = 0\}$$

so $L_q \cap X$ will consist of d distinct points if and only if the polynomial $f(p+tq) \in k[t]$ has d distinct zeroes.

Now $f(p + tq)$ is a polynomial in t of degee $\le d$, and the coefficient of t^j is a polynomial function in the coordinates of q, so the rule $q \mapsto f(p + tq)$ is a morphism

$$\pi : k^n \to Y = k[t]_{\le d}.$$

Let $Y_i \subset Y$ be the closed set defined in (13-5) and set $Z_i := \pi^{-1}(Y_i)$. Hence k^n has a stratification by closed subsets

$$Z_0 \subset Z_1 \subset \cdots \subset Z_d = k^n$$

where

$$Z_i = \{q \in k^n \mid |L_q \cap X| \leq i\}.$$

In particular, $k^n - Z_{d-1}$ is open. We want to show it is non-empty.

Write $f = g + h$ where

$$g = \sum_{i_1 + \cdots i_n = d} \alpha_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$$

is homogeneous of degree d and $\deg h \leq d-1$. The coefficient of t^d in $f(p+tq)$ is $g(q)$ so $\{q \in k^n \mid g(q) \neq 0\}$ is non-empty and open. Another way of saying this is that if $U \subset k[t]_{\leq d}$ is the set of degree d polynomials, then $\pi^{-1}(U) \neq \phi$. However, U is a dense open subset of $k[t]_{\leq d}$ (it is the complement to a hyperplane), so $\pi^{-1}(U)$ is a non-empty open subset of k^n, hence dense.

We know that the subset of U consisting of those polynomials have d distinct zeroes is non-empty and dense. □

To think about. The case of a curve is already interesting: if $C \subset k^2$ is a curve cut out by an irreducible $f \in k[x,y]$ of degree d, then almost every line in k^2 meets C at d distinct points.

Can you show that almost every degree m curve meets C at exactly md distinct points? Try to use the fact that such a curve D degenerates into m distinct lines and such a degenerate D meets C at md distinct points.

Motivate Bézout.

Proposition 13.4 *Let f be an irreducible polynomial in $k[x,y]$. Then $k[x,y]/(f)$ is integral over $k[t]$ for almost all $t \in kx + ky + k$.*

Proposition 13.5 *Let $k[x,y]_d$ be the space of homogeneous degree d polynomials. Then almost every $f \in k[x,y]_d$ is not of the form u^d for any $u \in kx + ky$.*

Lemma 13.6 *Almost all $n \times n$ matrices are diagonalizable.*

Proof. Define

$$f : M_n(k) \to Y := \{\text{monic polynomials in } k[t] \text{ of degree } n\}$$

by

$$f(A) = \det(tI - A).$$

This is a morphism because the coefficient of t^i in $f(A)$ is a polynomial function of the entries in the matrix A. By ???, the set

$$Y^o := \{\text{polynomials in } Y \text{ having } n \text{ distinct zeroes}\}$$

is a non-empty open subset. Hence $f^{-1}(Y^o)$ is a non-empty open subset of $M_n(k)$. However, every element of $f^{-1}(Y^o)$ has n distinct eigenvalues so is diagonalizable. Hence the set of diagonalizable matrices contains a non-empty open open subset of $M_n(k)$. □

Questions. 1. Is the set of diagonalizable matrices open?

2. You can almost think of the last result as saying that almost all n-dimensional $k[t]$-modules are semisimple. Explain.

3. Can you formalize and prove the statement that almost all n-dimensional $k[t]$-modules are semisimple?

Nilpotent matrices. At the other extreme from the diagonalizable matrices are the nilpotent ones. We write $\mathcal{N}$ for the set of nilpotent $n \times n$ matrices. This is a closed subvariety of $M_n(k)$ because A is nilpotent if and only if $A^n = 0$ and this can be expressed as a polynomial condition on the entries of A.

Exercise. Write out the defining equations of the variety of nilpotent 2×2 matrices. Compare the variety of nilpotent 2×2 matrices to the subvariety of $M_2(k)$ cut out by the conditions

$$\text{trace} = \text{determinant} = 0.$$

When we studied Jordan normal form we observed that the conjugacy classes of nilpotent $n \times n$ matrices are in natural bijection with the set of partitions of n. Let's write X_π for the conjugacy class correponding to the partition π.

Here are some natural questions. You might find it helpful to consider the Young diagram associated to a partition. It might also be helpful to consider the conjugacy class in the symmetric group corresponding to each partition.

A conjugacy class of nilpotent matrices is not necessarily closed. Show that its closure is a union of conjugacy classes.

Find conditions on partitions π and σ such that $X_\sigma \subset \overline{X}_\pi$.

When is $\overline{X}_\pi \cap \overline{X}_\sigma \neq \phi$?

What is $\dim \overline{X}_\pi$?

You can explore these questions is some detail for $n = 4$ and perhaps on that basis make some conjectures about the answers to these questions.

1.14 Tangent spaces

Fix a point p on an affine variety $X \subset \mathbb{A}^n$. A line in $\mathbb{A}^n$ through p is of the form

$$L_q = \{p + \lambda q \mid \lambda \in k\}$$

where $0 \neq q \in k^n$ is a fixed point giving the "direction" of L. Different choices of q give different lines through p.

Suppose that $I(X) = (f_1, \dots, f_m)$. Fix $p \in X$ and $0 \neq q \in k^n$. Introduce a new variable t and consider the polynomials $f_j(p + tq)$ in $k[t]$.

Lemma 14.1 *Retain the above notation and set*

$$f(t) := \gcd\{f_j(p + tq) \mid j = 1, \dots, m\}.$$

Then

$$L_q \cap X = \{p + \lambda q \mid \lambda \in k,\ f(\lambda) = 0\}.$$

Proof. Suppose $x \in L_q \cap X$. Then $x = p + \lambda q$ for some $\lambda \in k$ and $f_1(x) = \cdots = f_m(x) = 0$. Hence λ is a zero of each $f_j(p+tq) \in k[t]$. Equivalently, $t - \lambda$ divides each $f_j(p+tq)$, so divides $f(t)$, whence $f(\lambda) = 0$.

Conversely, suppose $f(\lambda) = 0$. Then $t - \lambda$ divides $f(t)$ and hence each $f_j(p+tq)$. In other words, $f_j(p + \lambda q) = 0$ for all j so $x = p + \lambda q \in X$. But x is also on the line L_q so $x \in L_q \cap X$. □

In other words there is a bijection

$$\{\text{the points of } L_q \cap X\} \longleftrightarrow \{\text{the zeroes of } f(t)\}.$$

In particular $p \in L_q \cap X$ corresponds to $t = 0$.

Definition 14.2 The intersection multiplicity of X and L_q at p is the multiplicity of the root $t = 0$ in the polynomial $f(t)$. We say that L_q is tangent to X at p if the intersecion multiplicity of L_q and X at p is > 1. The tangent space to X at p is

$$T_pX := \{q \in k^n \mid L_q = \{p + tq \mid \lambda \in k\} \text{ is tangent to } X \text{ at } p\} \cup \{0\}.$$

♢

We must show that the intersection multiplicity, and hence T_pX, is well-defined.

Lemma 14.3 *The intersection multiplicity of X and L_q at p does not depend on the choice of generators for $I(X)$.*

Proof. Retain the previous notation, and suppose that $I(X) = (g_1, \ldots, g_r)$ also. Set $g(t) := \gcd\{g_i(p+tq) \mid i = 1, \ldots, r\}$. Since $g_1 = a_1 f_1 + \cdots + a_m f_m$,

$$g_1(p+tq) = a_1(p+tq)f_1(p+tq) + \cdots + a_m(p+tq)f_m(p+tq).$$

Hence $f(t)$ divides $g_1(p+tq)$; likewise, $f(t)$ divides every $g_i(p+tq)$ so divides $g(t)$. Similarly $g(t)$ divides $f(t)$ so $f(t) = g(t)$ up to a unit multiple. □

Next we describe T_pX directly in terms of the defining equations for X.

The Jacobian matrix. The partial derivatives

$$\frac{\partial}{\partial x_j} : k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n]$$

make complete sense. The Taylor expansion of a polynomial $g \in k[x_1, \ldots, x_n]$ around a point $p = (\alpha_1, \ldots, \alpha_n) \in \mathbb{A}^n$ is

$$g = g(p) + \sum_{i=1}^{n} \frac{\partial g}{\partial x_i}(p)(x_i - \alpha_i) + \frac{1}{2!}\sum_{i,j=1}^{n} \frac{\partial^2 g}{\partial x_i \partial x_j}(p)(x_i - \alpha_i)(x_j - \alpha_j) + \cdots .$$

Now let $p \in X$ and $q = (\beta_1, \ldots, \beta_n) \in k^n$. Writing $I(X) = (f_1, \ldots, f_m)$ as before, since $f_r(p) = 0$, we have

$$f_r(p+tq) = \sum_{i=1}^{n} \frac{\partial f_r}{\partial x_i}(p)(t\beta_i) + \frac{1}{2!}\sum_{i,j=1}^{n} \frac{\partial^2 f_r}{\partial x_i \partial x_j}(p)(t\beta_i)(t\beta_j) + \cdots . \qquad (14\text{-}6)$$

It follows that

$$\begin{aligned} L_q \text{ is tangent to } X \text{ at } p &\iff t^2 \text{ divides } f_r(p+tq) \text{ for all } 1 \le r \le m \\ &\iff \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(p)\beta_i = 0 \text{ for all } 1 \le r \le m. \end{aligned}$$

Definition 14.4 The Jacobian matrix for X with respect to the generators $f_1, \ldots, f_m$ for $I(X)$ is the $m \times n$ matrix with entries in $k[x_1, \ldots, x_n]$ whose ij^{th} entry is $\frac{\partial f_i}{\partial x_j}$. The Jacobian matrix at p is the matrix $J_p \in M_{m\times n}(k)$ obtained by evaluating the entries of J at p, i.e.,

$$J_p := \left(\frac{\partial f_i}{\partial x_j}(p)\right).$$

◊

We think of the Jacobian as a linear map $J_p : k^n \to k^m$,

$$J_p \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{n} \frac{\partial f_1}{\partial x_j}(p)\beta_j \\ \vdots \\ \sum_{j=1}^{n} \frac{\partial f_m}{\partial x_j}(p)\beta_j \end{pmatrix}.$$

Therefore

$$\begin{aligned} q = (\beta_1, \ldots, \beta_n) \in T_pX &\iff \sum_{j=1}^{n} \frac{\partial f_i}{\partial x_j}(p)\beta_j = 0 \text{ for all } i \\ &\iff J_p q = 0. \end{aligned}$$

We have proved the next result.

Theorem 14.5 *Let $X \subset \mathbb{A}^n$ be a closed subvariety and $p \in X$. Then*

$$T_pX = \ker\bigl(J_p : k^n \to k^m\bigr).$$

In particular, T_pX is a linear subspace of k^n of dimension $n - \operatorname{rank} J_p$.

A standard observation. Let V be a finite dimensional k-vector space. If D is a subspace of $V^* = \operatorname{Hom}_k(V, k)$ we define $D^\perp := \{v \in V \mid \delta(v) = 0 \text{ for all } \delta \in D\}$. The inclusion $D \to V^*$ dualizes to give a surjective map $V \to D^*$ whose kernel is $D^\perp$. Hence $V/D^\perp \cong D^*$.

Theorem 14.6 *Let $X \subset \mathbb{A}^n$ be a closed subvariety, $p \in X$, and $\mathfrak{m}_p$ the corresponding maximal ideal in $\mathcal{O}(X)$. There is a vector space isomorphism*

$$d_p : \mathfrak{m}_p/\mathfrak{m}_p^2 \to (T_pX)^*.$$

Proof. Let $x_1, \dots, x_n$ be coordinate functions on $\mathbb{A}^n$, set $p = (\alpha_1, \dots, \alpha_n)$, and write $\mathfrak{n} = (x_1 - \alpha_1, \dots, x_n - \alpha_n)$ for the corresponding maximal ideal in the polynomial ring $k[x_1, \dots, x_n]$. Then $\mathfrak{m}_p = \mathfrak{n}/I(X)$ and $\mathfrak{m}_p/\mathfrak{m}_p^2 \cong \mathfrak{n}/\mathfrak{n}^2 + I(X)$.

We now view $x_1, \dots, x_n$ as a basis for $(k^n)^* = \operatorname{Hom}_k(k^n, k)$. Define $\psi : \mathfrak{n} \to (k^n)^*$ by

$$\psi(f) := \sum_{i=1}^n \frac{\partial f}{\partial x_i}(p)x_i.$$

Since $\psi(x_i - \alpha_i) = x_i$, ψ is surjective. Since $\dim_k(\mathfrak{n}/\mathfrak{n}^2) = n$ and $\psi(\mathfrak{n}^2) = 0$ there is an isomorphism

$$\psi : \mathfrak{n}/\mathfrak{n}^2 \longrightarrow (k^n)^*.$$

If $q = (\lambda_1, \dots, \lambda_n) \in k^n$,

$$\psi(f)(q) = \sum_{i=1}^n \frac{\partial f}{\partial x_i}(p)\lambda_i = J_p(q),$$

so Theorem 14.5 may be restated as

$$\begin{aligned} T_pX &= \ker(J_p : k^n \to k^m) \\ &= \{q = (\lambda_1, \dots, \lambda_n) \in k^n \mid \psi(f)(q) = 0 \text{ for all } f \in I(X)\} \\ &= \psi(I(X))^\perp. \end{aligned}$$

If we identify $(k^n)^*$ with $\mathfrak{n}/\mathfrak{n}^2$ via ψ this can be restated as

$$T_pX = \left(\frac{\mathfrak{n}^2 + I(X)}{\mathfrak{n}^2}\right)^\perp \subset \left(\frac{\mathfrak{n}}{\mathfrak{n}^2}\right)^* = k^n.$$

The observation just before this theorem now tells us that

$$(T_pX)^* \cong \frac{\mathfrak{n}/\mathfrak{n}^2}{I(X) + \mathfrak{n}^2/\mathfrak{n}^2} \cong \frac{\mathfrak{n}}{\mathfrak{n}^2 + I(X)} \cong \frac{\mathfrak{m}_p}{\mathfrak{m}_p^2}.$$

Explicitly, this isomorphism

$$d_p : \frac{\mathfrak{m}_p}{\mathfrak{m}_p^2} \longrightarrow (T_pX)^*$$

is given by

$$f \mapsto d_pf := \sum_{i=1}^n \frac{\partial f}{\partial x_i}(p)x_i$$

for $f \in \mathfrak{m}_p$. □

Our definition of tangent space agrees with that in differential geometry. Of course, we are working over an arbitrary field so it is only over the reals and complexes that we can make such a comparison. Also, we must be aware that not every algebraic variety over $\mathbb{R}$ or $\mathbb{C}$ is actually a manifold. However, if X is an affine variety over $\mathbb{R}$ or $\mathbb{C}$, and $p \in X$ is a point around which X is a smooth real (or complex) manifold, then our definition of T_pX coincides with the differential geometers tangent space.

We will use this to define what we mean by a smooth point of X.

Proposition 14.7 *Consider morphisms*

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

between affine algebraic varieties, and points $x \in X$, $y = f(x)$, and $z = g(y)$. Then

1. *there are induced linear maps*

$$T_xX \xrightarrow{d_xf} T_yY \xrightarrow{d_yg} T_zZ$$

called the differentials of f at x, etc., and

2. $d_x(g \circ f) = (d_yg) \circ (d_xf)$*;*
3. $d_x(\mathrm{id}_X) = \mathrm{id}_{T_xX}$*;*
4. *if f is an isomorphism, then $d_xf : T_xX \to T_{f(x)}Y$ is an isomorphism.*

We take the point of view of the differential geometers: the tangent space at a point p of a manifold M is a linear approximation to M near p. We make use of this idea by using the tangent space to define the dimension of the variety. (This has no parallel in differential geometry—there one defines the dimension of M first and then proves that the dimension of the tangent space at a point is equal to the dimension of M.) However, this needs some care since the dimension of the tangent space T_pX can vary as p varies.

Theorem 14.8 *Let X be an irreducible affine algebraic variety.*

1. *There is a unique integer d such that $\dim_k T_pX = d$ for almost all $p \in X$ and $\dim_k T_xX > d$ for all other points $x \in X$.*
2. *For every integer n, the set of points x such that $\dim_k T_xX \geq n$ is closed.*

Proof. Suppose that X is a closed subvariety of $\mathbb{A}^n$. Let J be the Jacobian matrix for X with respect to a set of generators for $I(X)$. For each integer r, the subset

$$X_r := \{x \in X \mid \dim T_xX \geq r\}$$

is equal to

$$\{x \in X \mid \operatorname{rank} J_x \leq n - r\}.$$

This is a closed subset of X in the Zariski topology because it is the zero locus of the set of all $(n-r+1)\times(n-r+1)$ minors of J. Hence we have an ascending chain of closed subvarieties

$$X_n \subset X_{n-1} \subset \cdots \subset X.$$

Let d be the largest integer such that $X_d = X$. Then X_{d+1} is a proper closed subvariety of X. □

Definition 14.9 Let X be an irreducible affine algebraic variety, and let d be the integer in Theorem 14.8. We say that p is a smooth point of X if $\dim T_pX = d$, and singular otherwise. We write $\operatorname{Sing} X$ for the singular locus X, i.e., for the set of singular points. If $\operatorname{Sing} X = \phi$ we say X is a smooth or non-singular variety. Otherwise we say X is singular. ♢

Synonyms. A smooth point is also called a simple, or regular, or non-singular point of X.

Theorem 14.8 says that the smooth points form a non-empty open (hence dense) subset of X, and $\operatorname{Sing} X$ is a closed subvariety of X.

Example 14.10 Determine all singular points of the cubic surface cut out by

$$f = xyz - x^2 - y^2 - z^2 + 4.$$

The partial derivatives are $yz - 2x$, $xz - 2y$, $xy - 2z$, so the singular points of X are those where all three vanish. These are $(a, b, \frac{1}{2}ab)$ where $a, b \in \{\pm 2\}$. ♢

Definition 14.11 The dimension of an irreducible affine algebraic variety X is the number d appearing in Theorem 14.8. That is, $\dim X$ is the smallest number d such that $\dim T_pX = d$ for some $p \in X$. Equivalently, $\dim X$ is the unique integer d such that $\dim T_pX = d$ for all p belonging to some dense open subset of X.

The dimension of an arbitrary affine algebraic variety is the maximum of the dimensions of its irreducible components. ♢

Remark. The dimension of $\mathbb{A}^n$ is n because if $\mathfrak{m}$ is a maximal ideal in $k[x_1, \ldots, x_n]$ we can pick coordinates so $\mathfrak{m} = (x_1, \ldots, x_n)$, and then it is clear that $\{\bar{x}_1, \ldots, \bar{x}_n)$ is a basis for $\mathfrak{m}/\mathfrak{m}^2$.

Proposition 14.12 *The dimension of a hypersurface in $\mathbb{A}^n$ is $n-1$.*

Proof. Let $X = V(f)$ be the zero locus of an irreducible f in the polynomial ring $k[x_1, \ldots, x_n]$.

Suppose the result fails for X. Because $X \subset \mathbb{A}^n$, $\dim T_pX \le n$ for all $p \in X$ so it would follow that $\dim T_pX = n$ for all $p \in X$. Hence $\operatorname{rank} J_p = 0$ for all $p \in X$, where J_p is the Jacobian matrix.

$$J_p = \left(\frac{\partial f}{\partial x_1}(p), \cdots, \frac{\partial f}{\partial x_n}(p)\right).$$

In other words, $V(f) \subset V(I)$ where I is the ideal in the polynomial ring generated by all $\partial f/\partial x_i$. It then follows that $\sqrt{I} \subset \sqrt{(f)}$. However, f is irreducible so (f) is a prime ideal and hence radical, so $\sqrt{I} \subset (f)$. In particular, $I \subset (f)$ so every $\partial f/\partial x_i$ is a multiple of f. However, the x_i-degree of $\partial f/\partial x_i$ is strictly smaller than the x_i-degree of f, so this can only happen if $\partial f/\partial x_i = 0$.

In characteristic zero, if $\partial f/\partial x_i = 0$ for all i, then f is constant which contradicts the hypothesis that f is irreducible. Thus the proposition holds in characteristic zero.

Now suppose char $k = p$. Because $\partial f/\partial x_1 = 0$, f belongs to $k[x_1^p, x_2, \dots, x_n]$. Because all partials vanish $f \in k[x_1^p, \dots, x_n^p]$. But every element in this subring is a p^{th} power of an element in $k[x_1, \dots, x_n]$ so f would not be irreducible. □

Proposition 14.13 *Let X be an irreducible affine algebraic variety, $f \in \mathcal{O}(X)$, and p a point in $X_f := \{x \in X \mid f(x) \neq 0\}$. Then the natural map $T_pX_f \to T_pX$ is an isomorphism.*

Proof. Write $R = \mathcal{O}(X)$ and $R_f := R[f^{-1}]$. Then X_f is an affine algebraic variety with $\mathcal{O}(X_f) = R[f^{-1}] \cong R[T]/(Tf-1)$.

Let $\mathfrak{m}$ and $\mathfrak{n}$ be the maximal ideals in R and R_f vanishing at p. After Theorem 14.6, it suffices to show that the composition

$$\mathfrak{m} \to \mathfrak{n} \to \mathfrak{n}/\mathfrak{n}^2$$

is surjective and has kernel equal to $\mathfrak{m}^2$. In other words, we must show that $\mathfrak{n} = \mathfrak{n}^2 + \mathfrak{m}$ and $\mathfrak{n}^2 \cap R = \mathfrak{m}^2$.

First notice that $\mathfrak{n} = \mathfrak{m}R_f$ because if $b \in R$ and bf^{-n} vanishes at p, then $0 = b(p)f(p)^{-n}$, so $b(p) = 0$, whence $b \in \mathfrak{m}$ and $bf^{-n} \in \mathfrak{m}R_f$.

To see that $\mathfrak{n} = \mathfrak{m} + \mathfrak{n}^2$, consider a typical element $bf^{-n} \in \mathfrak{n}$ where $b \in \mathfrak{m}$. Then $1 - f(p)^{-n}f^n \in \mathfrak{m}$, so $b(1 - f(p)^{-n}f^n)f^{-n} \in \mathfrak{n}^2$. Thus

$$bf^{-n} = b(1 - f(p)^{-n}f^n)f^{-n} + f(p)^{-n}b \in \mathfrak{n}^2 + \mathfrak{m}.$$

Hence $\mathfrak{n} = \mathfrak{n}^2 + \mathfrak{m}$.

Now $R \cap \mathfrak{n}^2 = R \cap (\mathfrak{m}R_f)^2 = R \cap \mathfrak{m}^2R_f$, but this is equal to $\mathfrak{m}^2$. (Indeed, we have shown before that $R \cap IR_f = I$ for every ideal I in R). □

Corollary 14.14 *Let X be an irreducible affine algebraic variety and $0 \neq f \in \mathcal{O}(X)$. Then $\dim X = \dim X_f$.*

Proof. Write $d = \dim X$ and $d' = \dim X_f$. Then

$$U := \{p \in X \mid \dim T_pX = d\}$$

is a dense open subset of X, and $U' := \{p \in X_f \mid \dim T_pX_f = d'\}$ is a dense open subset of X_f. But X_f is a dense open subset of X, so U' is a dense open subset of X; thus $U \cap U' \neq \phi$. Let $p \in U \cap U'$; but $T_pX \cong T_pX_f$, so $d = d'$. □

The next result shows that the dimension of an irreduucible variety depends only on its function field.

Corollary 14.15 *Let X and Y be birationally equivalent irreducible affine algebraic varieties. Then* $\dim X = \dim Y$.

Proof. By Proposition 8.2, there are non-empty open subsets X_f and Y_g such that $X_f \cong Y_g$. The result now follows from Corollary 14.14. □

Theorem 14.16 *Let X be an irreducible affine algebraic variety. If $\mathcal{O}(X)$ is integral over a polynomial ring $k[t_1, \dots, t_d]$, then $d = \dim X$.*

Proof. By Noether normalization, there is a subring $k[x_1, \dots, x_d] \subset \mathcal{O}(X)$ over which $\mathcal{O}(X)$ is integral. For a suitably large n there is a surjective map

$$\phi : k[X_1, \dots, X_n] \to \mathcal{O}(X)$$

such that $\phi(X_i) = x_i$ for $1 \le i \le d$. The kernel of ϕ is $I(X) = (f_1, \dots, f_m)$.

Thus $I(X) \cap k[X_1, \dots, X_d] = 0$ and, because $\mathcal{O}(X)$ is integral over $k[x_1, \dots, x_d]$, for each $r > d$ there is a non-zero

$$g_r \in I(X) \cap k[X_1, \dots, X_d][X_r].$$

that is monic as a polynomial in X_r and of minimal degree subject to this.

Define the $(n-d) \times n$ matrix

$$A := \left(\frac{\partial g_r}{\partial X_j} \right)_{\substack{d+1 \le r \le n \\ 1 \le j \le n}}.$$

The $(n-d) \times (n-d)$ submatrix in the bottom right corner

$$A' := \left(\frac{\partial g_r}{\partial X_j} \right)_{d+1 \le r, j \le n}$$

is a diagonal matrix because $g_r \in k[X_1, \dots, X_d, X_r]$. But g_r was chosen to be of minimal degree in X_r so

$$\frac{\partial g_r}{\partial X_r} \notin I(X).$$

Therefore

$$U_r := \left\{ p \in X \;\middle|\; \frac{\partial g_r}{\partial X_r}(p) \ne 0 \right\}$$

is a non-empty open, hence dense, subset of X. Thus

$$U := U_{d+1} \cap \cdots \cap U_n$$

is a dense open subset of X. If $p \in U$, then the diagonal entries of A'_p are non-zero so

$$\operatorname{rank} A_p = n - d$$

for all $p \in U$.

Because each g_r is in $I(X)$, we can write $g_r = \sum_{i=1}^{d} b_{ri} f_i$ for some $(n-d) \times m$ matrix (b_{ri}). Differentiating this with respect to X_j and evaluating at $p \in X$ we get $A_p = B_p J_p$ where J_p is the Jacobian matrix at p. Hence $\operatorname{rank} A_p \leq \operatorname{rank} J_p = n - \dim T_pX$ and $\dim T_pX \leq n - \operatorname{rank} A_p$ for all $p \in X$. In particular, $\dim T_pX \leq d$ for all $p \in U$.

It remains to show that $\dim T_pX = d$ for some $p \in U$. Once that is done we will □

1.15 Derivations and differentials

Definition 15.1 A k-linear derivation on a commutative k-algebra R is a k-linear map $\delta : R \to R$ that satisfies the Leibniz identity:

$$\delta(ab) = \delta(a)b + a\delta(b)$$

for all $a, b \in R$. The set of all such maps is denoted by $\operatorname{Der}_k R$.

If M is an R-module an M-valued derivation on R is a k-linear map $\delta : R \to M$ such that

$$\delta(ab) = a\delta(b) + b\delta(a) \tag{15-7}$$

for all $a, b \in R$. We write $\operatorname{Der}_k(R, M)$ or just $\operatorname{Der}(R, M)$ for all such maps. ♢

Notice that $\delta(1) = 0$ because $\delta(1) = \delta(1 \times 1) = \delta(1) + \delta(1)$. The k-linearity of δ then implies that $\delta(a) = 0$ for all $a \in k$.

Lemma 15.2 $\operatorname{Der}(R, M)$ *is an R-module and* $\operatorname{Der} R$ *is a Lie algebra with resepct to the bracket*

$$[\delta, \eta] := \delta \circ \eta - \eta \circ \delta.$$

Proof. It is obvious that $r\delta$ is a derivation if δ is. It is also straightforward to check that $[\delta, \eta]$ is again a derivation. □

Perhaps you have already met a definition of the tangent space to a point on a manifold. The next proposition might match up with that definition. It says that T_pX is isomorphic to the space of all k-linear maps $\delta : \mathcal{O}(X) \to k$ such that

$$\delta(fg) = f(p)\delta(g) + \delta(f)g(p)$$

for all regular functions $f, g : X \to k$. To see that this statement is equivalent to the proposition simply observe that, as an $\mathcal{O}(X)$-module, $\mathcal{O}(X)/\mathfrak{m}_p$ is isomorphic to k with the action of $f \in \mathcal{O}(X)$ on $\alpha \in k$ given by $f.\alpha = f(p)\alpha$.

Proposition 15.3 *Let p be a point on an affine algebraic variety X over k. Write $R = \mathcal{O}(X)$ and $\mathfrak{m}$ for the maximal ideal at p. Then*

$$T_pX \cong \operatorname{Der}(R, R/\mathfrak{m}).$$

Proof. We have already shown there is an isomorphism

$$T_pX \cong \left(\frac{\mathfrak{m}}{\mathfrak{m}^2}\right)^2.$$

We will now show that the map

$$\Phi : \operatorname{Der}(R, R/\mathfrak{m}) \to \left(\frac{\mathfrak{m}}{\mathfrak{m}^2}\right)^*$$

defined by $\Phi(\delta)(\bar{f}) := \delta(f)(p)$ for $\bar{f} \in \mathfrak{m}/\mathfrak{m}^2$ is an isomorphism. In the definition of $\Phi(\delta)$, $f \in \mathfrak{m}$ is any preimage of $\bar{f}$. The definition makes sense because $\delta(\mathfrak{m}^2) = 0$. Thus Φ is a well-defined k-linear map and we must show it has an inverse.

Define

$$\Psi : \left(\frac{\mathfrak{m}}{\mathfrak{m}^2}\right)^* \longrightarrow \operatorname{Der}(R, R/\mathfrak{m})$$

by

$$\Psi(\lambda)(f) = \lambda(\overline{f - f(p)})$$

where $\overline{f - f(p)}$ denotes the image of $f - f(p)$ in $\mathfrak{m}/\mathfrak{m}^2$, which makes sense because $f - f(p) \in \mathfrak{m}$. To see that $\Psi(\lambda)$ really belongs to $\operatorname{Der}(R, R/\mathfrak{m})$ notice first that

$$(f - f(p))(g - g(p)) \in \mathfrak{m}^2$$

so

$$\overline{fg - f(p)g(p)} = f(p)\overline{(g - g(p))} + g(p)\overline{(f - f(p))};$$

hence

$$\begin{aligned} \Psi(\lambda)(fg) &= \lambda(\overline{fg - f(p)g(p)}) \\ &= f(p)\lambda(\overline{g - g(p)}) + g(p)\lambda\overline{f - f(p)}) \\ &= f(p)\Psi(\lambda)(g) + g(p)\Psi(\lambda)(f). \end{aligned}$$

Thus $\Psi(\lambda)$ is an $R/\mathfrak{m}$-valued derivation on R.

It is now a routine matter to check that Ψ and Φ are mutually inverse. □

Fix a commutative ring R. The rule

$$M \mapsto \operatorname{Der}(R, M)$$

is a functor from the category of R-modules to itself because if $\delta : R \to M$ is a derivation and $f : M \to N$ an R-module homomorphism then $f \circ \delta : R \to N$ is a derivation. We ask, as always, *is this functor representable*, i.e., is there an R-module Ω such that

$$\operatorname{Der}(R, M) \cong \operatorname{Hom}_R(\Omega, M)$$

for all R-modules M? There is.

Proposition 15.4 *Let k be any commutative ring and R any commutative k-algebra. There is an R-module $\Omega_{R/k}$ and a k-linear derivation*

$$d : R \to \Omega_{R/k}$$

such that if $\delta : R \to M$ is any k-linear derivation, there is a unique R-module homomorphism $f : \Omega_{R/k} \to M$ such that $\delta = f \circ d$.

Definition 15.5 In the context of Proposition 15.4, the pair $(\Omega_{R/k}, d)$ is called the module of relative differentials. ♢

Suppose that $f : R \to S$ is a k-algebra homomorphism. Then every S-module is an R-module in a natural way, and a derivation $\delta : S \to M$ can be composed with f to provide a derivation $\delta \circ f : R \to M$. In particular, $d_{S/k} \circ f : R \to \Omega_{S/k}$ is a derivation so there is a unique R-module homomorphism $\rho : \Omega_{R/k} \to \Omega_{S/k}$ such that $d_{S/k} \circ f = \rho \circ d_{R/k}$.

The map $f : R \to S$ also allows us to view S as an R-algebra so there is a module $\Omega_{S/R}$ of relative differentials and a universal derivation $d_{S/R} : S \to \Omega_{S/R}$. There is therefore an S-module homomorphism $\eta : \Omega_{S/k} \to \Omega_{S/R}$ such that $d_{S/R} = \eta \circ d_{S/R}$.

Putting all this together, we have the following result.

Proposition 15.6 *There is an exact sequence*

$$\Omega_{R/k} \longrightarrow \Omega_{S/k} \longrightarrow \Omega_{S/R} \longrightarrow 0.$$

Proof. □

1.16 A first glimpse of schemes

Schemes are geometric objects that are somewhat more general than algebraic varieties.

A blunt definition: *the category of affine schemes is the opposite of the category of commutative rings.*

If k is any commutative ring *the category of affine k-schemes, or affine schemes over k, is the opposite of the category of commutative k-algebras.*

We saw earlier that the category of affine algebraic varieties over an algebraically closed field k is equivalent to the opposite of the category of finitely generated commutative k-algebras having no nilpotent elements. Thus every algebraic variety over k can be viewed as an affine k-scheme.

There are many ideas, or ways of thinking, that lead naturally from varieties to schemes. Natural questions about varieties suggest we need more general objects than varieties.

As a simple example consider the fact that a degree d polynomial $f(x)$ over an algebraically closed field has exactly d zeroes when counted with multiplicity. Geometrically, this says that the curve $y = f(x)$ meets the x-axis d times if we count the points of intersection with appropriate multiplicity.

Lots to say... $\operatorname{Spec} k[\varepsilon]$ and $T_pX =$ morphisms $\operatorname{Spec} k[\varepsilon] \to X$ centered at p... non-separated schemes (and reln to eg quotient for $\xi.(x,y) = (\xi x, \xi^{-1}y)$)... projective spaces and sheaf of regular fns....

1.17 Algebraic group actions

Definition 17.1 An affine algebraic group is an affine algebraic variety G that has the structure of a group and is such that the multiplication map $G \times G \to G$ and the inversion map $G \to G$, $g \mapsto g^{-1}$, are both morphisms. $\lozenge$

For example, the additive group $(k, +)$ is an algebraic group. It is usually denoted by $\mathbb{G}_a$. Its coordinate ring is $\mathcal{O}(\mathbb{G}_a) = k[x]$. The inversion map is the morphism $g \mapsto -g$ and this corresponds to the k-algebra automorphism $x \mapsto -x$. The muliplication map $\mathbb{G}_a \times \mathbb{G}_a$ is the addition map $(x, y) \mapsto x + y$. Now, $\mathcal{O}(\mathbb{G}_a \times \mathbb{G}_a) \cong \mathcal{O}(\mathbb{G}_a) \otimes_k \mathcal{O}(\mathbb{G}_a) \cong k[x] \otimes k[y] = k[x, y]$, and the k-algebra homomorphism $k[x] \to k[x, y]$ corresponding to the binary operation of addition is $x \mapsto x + y$.

$\mathrm{GL}_n(k)$ **as an affine algebraic variety.** The general linear group $\mathrm{GL}_n(k)$, the group of invertible $n \times n$ matrices with entries in k, is an algebraic group. To see this we must first impose the structure of an algebraic variety on it. Since $\mathrm{GL}_n(k)$ is the subset of $M_n(k)$ where $\det \neq 0$ it is an *open* subspace of $M_n(k)$. However, the natural projection $M_n(k) \times \mathbb{A}^1 \to M_n(k)$ sends the closed subvariety

$$X := \{(A, \lambda) \mid \lambda \det A = 1\}$$

bijectively to $\mathrm{GL}_n(k)$. The coordinate ring of this closed subvariety is

$$k[x_{ij}, t]/(t \det -1) \cong k[x_{ij}][\det^{-1}].$$

We therefore consider $\mathrm{GL}_n(k)$ as an affine algebraic variety and take the above ring as its ring of regular functions. The multpilication map $(g, h) \mapsto gh$ corresponds to the k-algebra homomorphism $x_{ij} \mapsto \sum_{r=1}^n x_{ir} \otimes x_{rj}$.

Actions of algebraic groups. Let G be an affine algebraic group and X an affine algebraic variety. We are often interested in actions with the property that the action map $G \times X \to X$ is a morphism of algebraic varieties.

If G is finite so are its orbits, so every orbit is a closed subvariety of X. When G is not finite this is no longer true. For example, consider the two actions of $G = \mathbb{C}^* = \mathrm{GL}_1(\mathbb{C})$ on $\mathbb{C}^2$ given by

1. $\xi.(\alpha, \beta) = (\xi\alpha, \xi\beta)$ for $\xi \in \mathbb{C}^*$ and $(\alpha, \beta) \in \mathbb{C}^2$, and
2. $\xi.(\alpha, \beta) = (\xi\alpha, \xi^{-1}\beta)$ for $\xi \in \mathbb{C}^*$ and $(\alpha, \beta) \in \mathbb{C}^2$.

The orbits are as follows:

1. $\{(0, 0)\}$, and the lines through the origin (less the origin); the only closed orbit is $\{(0, 0)\}$, and the origin is in the closure of every orbit.

2. $\{(0,0)\}$, the x- and y-axes less the origin, and the hyperbolas $xy = \lambda$, $0 \neq \lambda \in k$; the closed orbits consist of the origin and the hyperbolas; the origin is in the closure of each of the two non-closed orbits (the x- and y-axes).

The fact that there are non-closed orbits means that the method we used for finite groups (i.e., the imposition of an algebraic variety structure on the orbit space) will fail for infinite groups. Although the ring of G-invariant functions $\mathcal{O}(X)^G$ still consists of functions that are constant on orbits, these functions are actually constant on *closures of orbits* (because $f^{-1}(\lambda)$ is closed!). A further problem is that $\mathcal{O}(X)^G$ need not be a finitely generated algebra; even if it is the points of the affine variety having $\mathcal{O}(X)^G$ as its coordinate ring are in natural bijection with the closed orbits.

For example, consider Example (1) above. The action of $\mathbb{C}^*$ on $\mathbb{C}[x,y] = \mathcal{O}(\mathbb{C}^2)$ is given by $\xi.x = \xi x$ and $\xi.y = \xi y$, so $\mathbb{C}[x,y]^G = \mathbb{C}$, the constant functions. And $\mathbb{C}$ is the coordinate ring of the variety with one point. That point corresponding to the closed orbit $\{(0,0)\}$.

In Example (2) above the induced action of $G = \mathbb{C}^*$ on $\mathbb{C}[x,y]$ is given by $\xi.x = \xi x$ and $\xi.y = \xi^{-1}y$, so $\mathbb{C}[x,y]^G = \mathbb{C}[x,y]$ which is the coordinate ring of the affine line; and the affine line is in natural bijection with the closed orbits.

When $\mathcal{O}(X)^G$ is finitely generated it is usual to write $X/\!\!/G$ for the affine algebraic variety whose coordinate ring is $\mathcal{O}(X)^G$. The inclusion $\mathcal{O}(X)^G \to \mathcal{O}(X)$ then corresponds to a morphism $\pi : X \to X/\!\!/G$ with the property that

1. each fiber of π is a union of orbits;
2. orbits Gx and Gx' belong to the same fiber if and only if $\overline{Gx} \cap \overline{Gx'} \neq \phi$;
3. each fiber contains a unique closed orbit.

Obviously $X/\!\!/G$ is a rather crude approximation of the orbit space so one proceeds as follows. One takes various "good" open subvarieties X_0 of X that are stable under the action of G and have the property that the orbits of G on X_0 are closed (as subsets of X_0), and then one imposes on X_0/G, the set of G-orbits on X_0, the structure of an algberaic variety.

This is the subject of Geometric Invariant Theory.

Returning to Example (1), consider $\mathbb{C}^2 - \{0\}$. This set is G-stable and the orbits on it are closed. The quotient $\mathbb{C}^2 - \{0\}/\mathbb{C}^*$ is the projective line $\mathbb{P}^1$.

Now consider Example (2)....affine line with a double point, a non-separated scheme.

Conjugacy classes. The conjugacy classes of $n\times n$ complex matrices are the orbits for the conjugation action of $\mathrm{GL}(n,\mathbb{C})$ on $M_n(\mathbb{C})$. Functions on matrices that depend only on the conjugacy class of a matrix are of great importance—the trace and determinant are such functions. the functions that are constant on conjugacy classes are those in the ring of invariants $\mathcal{O}(M_n(\mathbb{C}))^{\mathrm{GL}(n,\mathbb{C})}$.

Is this a finitely generated $\mathbb{C}$-algebra and, if so, what are its generators?

It turns out that the closures of the conjugacy classes are in bijection with the diagonal matrices. Equivalently, the closure of each orbit contains a unique dense orbit and that orbit is the conjugacy class of a unique diagonal matrix.

Notice that the trace and determinant of a matrix are (up to a sign) coefficients of the characteristic polynomial of that matrix. That is,

$$\det(tI - A) = t^n - (a_{11} + \cdots + a_{nn})t^{n-1} + \cdots + (-1)^{n-1} \det A.$$

We know that conjugate matrices have the same minimal polynomial so *every* coefficient of the characteristic polynomial is constant on conjugacy classes so belongs to $\mathcal{O}(M_n(\mathbb{C}))^{\mathrm{GL}(n,\mathbb{C})}$. It is an important result that these generate the invariant ring.

There are n of these, and they are algebraically independent so $\mathcal{O}(M_n(\mathbb{C}))^{\mathrm{GL}(n,\mathbb{C})}$ is isomorphic to the polynomial ring in n variables.

There is another way to obtain generators for $\mathcal{O}(M_n(\mathbb{C}))^{\mathrm{GL}(n,\mathbb{C})}$. If x_{ij} is the coordinate function on $M_n(\mathbb{C})$ that takes the ij-entry of a matrix, then the trace function is $x_{11} + \cdots + x_{nn}$. Now consider the morphism $M_n(\mathbb{C}) \to M_n(\mathbb{C})$, $A \mapsto A^r$. Composing this with the trace function gives a function that is constant on conjugacy classes.

Let's compute this function when $r = 2$. Let $A = (a_{ij})$. Then the diagonal entries of A^2 are

$$\sum_{i=1}^n a_{1i}a_{i1}, \ \sum_{i=1}^n a_{2i}a_{i2}, \ \cdots \sum_{i=1}^n a_{ni}a_{in},$$

so

$$\mathrm{Tr}(A^2) = \sum_{j=1}^n \sum_{i=1}^n a_{ji}a_{ij}.$$

Hence the function is

$$\sum_{j=1}^n \sum_{i=1}^n x_{ji}x_{ij}.$$

Similarly, for $r = 3$ we have the function

$$\sum_{i,j,k=1}^n x_{ij}x_{jk}x_{ki}.$$

These functions also provide a set of generators for $\mathcal{O}(M_n(\mathbb{C}))^{\mathrm{GL}(n,\mathbb{C})}$.

Look at the simple case of a 2×2 generic matrix X. Its characteristic polynomial is

$$t^2 - (\mathrm{Tr}\, X)t + \det X.$$

The Cayley-Hamilton Theorem tells us that a matrix satisfies its minimal polynomial, so

$$X^2 - (\mathrm{Tr}\, X)X + \det X = 0 \tag{17-8}$$

where the last term is really $(\det X)I$. Now take the trace of the matrices in (17-8) to get

$$\mathrm{Tr}(X^2) - (\mathrm{Tr}\, X)^2 + 2 \det X = 0.$$

This shows that $\mathbb{C}[\mathrm{Tr}\, X, \det X] = \mathbb{C}[\mathrm{Tr}\, X, \mathrm{Tr}(X^2)]$.

1.18 Dimension

There are several ways of defining the dimension of an algebraic variety all of which lead to the same number.

Let's list some of the properties we want a dimension function to have. We want it to agree with our primitive notions of dimension: a point has dimension zero, a curve (or line) has dimension one, a surface has dimension two, etc. We want the dimension of $\mathbb{A}^n$ to be n. If $X \subset Y$ we want the dimension of Y to be at least as big as that of X. We want the dimension of X to be the maximum of the dimension of its irreducible components. If $f : X \to Y$ is a surjective map with finite fibers then X and Y should have the same dimension. We would like to have $\dim X \times Y = \dim X + \dim Y$. If $f : X \to Y$ is a dominant morphism we might expect that $\dim f^{-1}(y) = \dim X - \dim Y$ for almost all $y \in Y$. Perhaps we want a variety of dimension n to have infinitely many subvarieties of dimension $n-1$.

Definition 18.1 The dimension of a topological space X is the largest n for which there is a chain of closed irreducible subspaces

$$\phi \neq X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n.$$

The dimension of the empty set is $-\infty$. ◊

This definition of dimension is not suited to all topological spaces.

It is easy to see that a point has dimension zero, and that $\mathbb{A}^n$ has dimension at least n because of the chain

$$V(x_1, \ldots, x_n) \subset V(x_1, \ldots, x_{n-1}) \subset \cdots \subset V(x_1) \subset V(0).$$

It is quite a bit harder to show that $\dim \mathbb{A}^n \leq n$.

Lemma 18.2 *Let X be a topological space.*

1. *If Z is a closed subspace of X, then* $\dim Z \leq \dim X$.
2. $\dim X$ *is the maximum of the dimension of its irreducible components.*
3. *If X is irreducible, then* $\dim Z \leq \dim X - 1$ *for all closed subspaces* $Z \subsetneq X$.
4. *If $X = X_1 \cup \ldots \cup X_t$ expresses X as a union of closed subspaces, then* $\dim X = \max\{\dim X_i\}$.

Proof. (1) A closed irreducible subspace of Z is a closed irreducible subspace of X, so a chain $\phi \neq Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n$ of Z is also a chain of closed irreducible subspaces of X.

(2) The definition of $\dim X$ implies that X has a closed irreducible subvariety X' such that $\dim X = \dim X'$. Since X' is an irreducible component of itself it is contained in some irreducible component of X, say X_1, by Lemma 5.8. Now (1) gives the inequalities in $\dim X = \dim X' \leq \dim X_1 \leq \dim X$, so $\dim X_1 =$

$\dim X$. By (1) $\dim X$ is at least as big as the dimension of all its irreducible components.

(3) This follows at once from the definition.

(4) Let X' be an irreducible component of X such that $\dim X' = \dim X$. Then $X' = (X' \cap X_1) \cup \cdots \cup (X' \cap X_n)$ so $X' = X' \cap X_i$ for some X. Thus $X' \subset X_i$ for some i and $\dim X = \dim X' \leq \dim X_i \leq \dim X$. □

We now reformulate this notion of dimension for $\operatorname{Spec} R$ with the Zariski topology directly in terms of prime ideals.

Definition 18.3 The Krull dimension of a ring R is the largest integer n such that there is a chain $\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ of distinct prime ideals of R. ♢

If X is an affine algebraic variety it is clear that $\dim X = \operatorname{Kdim} \mathcal{O}(X)$.

Proposition 18.4 *Let $R \subset S$ be rings such that S is a finitely generated R-module. Then* $\operatorname{Kdim} R = \operatorname{Kdim} S$.

Proof. Let

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

be a chain of primes in R. By Theorem 4.6, there is a prime $\mathfrak{q}_0$ in S such that $\mathfrak{p}_0 = R \cap \mathfrak{q}_0$. Applying Theorem 4.6 to the prime $\mathfrak{p}_1/fp_0$ in $R/fp_0 \subset S/\mathfrak{q}_0$, there is a prime $\mathfrak{q}_1$ in S that contains $\mathfrak{q}_0$ such that $\mathfrak{p}_1 = R \cap \mathfrak{q}_1$. Continuing in this way, there is a chain of primes

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_n$$

in S such that $\mathfrak{p}_i = R \cap \mathfrak{q}_i$ for all i. Hence $\operatorname{Kdim} S \geq \operatorname{Kdim} R$.

Now suppose that $\mathfrak{q}' \subsetneq \mathfrak{q}$ are distinct primes in S. Then there is an inclusion $\mathfrak{p}' := R \cap \mathfrak{q}' \subset \mathfrak{p} := R \cap \mathfrak{q}$ of primes in R. If we can show that $\mathfrak{p} \neq \mathfrak{p}'$ it will follow that $\operatorname{Kdim} R \geq \operatorname{Kdim} S$.

Suppose that $\mathfrak{p} = \mathfrak{p}'$. Replace S by $S/\mathfrak{q}'$ and R by $R/\mathfrak{q}' \cap R$. With this new notation we are in the following situation: S is a domain, $R \subset S$, S is a finitely generated R-module, and $\mathfrak{q}$ is a non-zero prime in S. We will now show that $\mathfrak{q} \cap R \neq 0$.

We work inside the field $\operatorname{Fract} S$. This contains $K := \operatorname{Fract} R$. Notice that

$$T := \{sr^{-1} \mid s \in S, 0 \neq r \in R\}$$

is a subring of $\operatorname{Fract} S$ that contains K and S. Since S is a finitely generated R-module T is a finitely generated K-module, i.e., T is a domain and is a finite dimensional K-vector space. It is therefore a field. Hence if $0 \neq f \in S$, then T contains f^{-1}, i.e., $f^{-1} = sr^{-1}$ for some $r \in R$ and $s \in S$. Hence $0 \neq r = fs$, and we conclude that $R \cap fS \neq 0$. In particular, $\mathfrak{q} \cap R \neq 0$. □

Theorem 18.5 *If $f : X \to Y$ is a dominant morphism, then* $\dim X \geq \dim Y$.

Proof. Claim: If the theorem is true when X is irreducible, it is true for all X. Proof: Write $X = X_1 \cup \ldots \cup X_t$ as the union of its irreducible components. By applying the theorem to $f|_{X_i} : X_i \to \overline{f(X_i)}$, we have $\dim X_i \geq \dim \overline{f(X_i)}$. However,

$$Y = \overline{f(X)} = \overline{f(X_1) \cup \cdots \cup f(X_t)} = \overline{f(X_1)} \cup \cdots \cup \overline{f(X_t)}$$

so $\dim Y = \dim \overline{f(X_i)}$ for some i by part (4) of Lemma 18.2.

We now assume X is irreducible.

We will prove the theorem by induction on $n = \dim Y$. If $n = 0$ then X is non-empty so $\dim X \geq 0$. Let $\dim Y = n > 0$ and suppose the result is true for varieties of dimension $\leq n - 1$.

Let $Y_{n-1} \subset Y$ be a closed irreducible subvariety of dimension $n-1$. Then $f^{-1}(Y_{n-1})$ is a closed subvariety of X. If $f^{-1}(Y_{n-1}) = X$, then $f(X) \subset Y_{n-1}$ contradicting the hypothesis that $\overline{f(X)} = Y$. Hence $f^{-1}(Y_{n-1}) \neq X$. Since X is irreducible, part (3) of Lemma 18.2 gives $\dim X > \dim f^{-1}(Y_{n-1})$; but $\dim f^{-1}(Y_{n-1}) \geq n - 1$ by applying the induction hypothesis to $f^{-1}(Y_{n-1}) \to Y_{n-1}$.

Not complete □

When X is irreducible we may define $\dim X := \operatorname{trdeg}_k k(X)$, the transcendence degree of $k(X)$, i.e., the maximal d such that $k(X)$ contains algebraically independent elements $x_1, \ldots, x_n$.

Theorem 18.6 *Let X be an irreducible affine variety. Then $\dim X$ is the unique integer d such that $\mathcal{O}(X)$ is integral over a polynomial subring $k[t_1, \ldots, t_d]$.*

Proof. We want to show that the integer d is unique, so suppose that $\mathcal{O}(X)$ is integral over the polynomial subrings $k[t_1, \ldots, t_d]$ and $k[x_1, \ldots, x_n]$. Then there are surjective morphisms $f : X \to \mathbb{A}^d$ and $g : X \to \mathbb{A}^n$. □

1.19 Localization

1.20 Local Rings

Nakayama's Lemma

Completion.

Hensel's Lemma

Henselization.