

Chapter 2

Affine Algebraic Geometry

2.1 The Algebraic-Geometric Dictionary

The correspondence between algebra and geometry is closest in affine algebraic geometry, where the basic objects are solutions to systems of polynomial equations. For many applications, it suffices to work over the real \mathbb{R} , or the complex numbers \mathbb{C} . Since important applications such as coding theory or symbolic computation require finite fields, \mathbb{F}_q , or the rational numbers, \mathbb{Q} , we shall develop algebraic geometry over an arbitrary field, \mathbb{F} , and keep in mind the important cases of \mathbb{R} and \mathbb{C} . For algebraically closed fields, there is an exact and easily motivated correspondence between algebraic and geometric concepts. When the field is not algebraically closed, this correspondence weakens considerably. When that occurs, we will use the case of algebraically closed fields as our guide and base our definitions on algebra.

Similarly, the strongest and most elegant results in algebraic geometry hold only for algebraically closed fields. We will invoke the hypothesis that \mathbb{F} is algebraically closed to obtain these results, and then discuss what holds for arbitrary fields, particularly the real numbers. Since many important varieties have structures which are independent of the field of definition, we feel this approach is justified—and it keeps our presentation elementary and motivated. Lastly, for the most part it will suffice to let \mathbb{F} be \mathbb{R} or \mathbb{C} ; not only are these the most important cases, but they are also the sources of our geometric intuitions.

Let \mathbb{A}^n denote affine n -space over \mathbb{F} . This is the set of all n -tuples (t_1, \dots, t_n) of elements of \mathbb{F} . The reason for writing \mathbb{A}^n instead of \mathbb{F}^n is to emphasize that we are not doing linear algebra. We may write $\mathbb{A}_{\mathbb{F}}^n$ to emphasize our field. Let t_1, \dots, t_n be variables, which we regard as the coordinate functions on \mathbb{A}^n . Let $\mathbb{F}[t_1, \dots, t_n]$ be the ring of polynomials in these variables t_1, \dots, t_n with coefficients in the field \mathbb{F} . We make the main definition of this chapter.

Definition 2.1 Given polynomials $f_1, \dots, f_s \in \mathbb{F}[t_1, \dots, t_n]$, their set of common zeroes

$$\mathcal{V}(f_1, \dots, f_s) := \{t \in \mathbb{A}^n \mid f_1(t) = \dots = f_s(t) = 0\}$$

is called an *affine variety* in \mathbb{A}^n .

A variety $\mathcal{V}(f)$ defined by a single polynomial equation is called a *hypersurface*. If \mathcal{X} and \mathcal{Y} are varieties with $\mathcal{Y} \subset \mathcal{X}$, then \mathcal{Y} is a *subvariety* of \mathcal{X} .

Example 2.2 Consider the real plane $\mathbb{A}_{\mathbb{R}}^2$. Figure 2.1 shows the three cubic curves $\mathcal{V}(y^2 - x^3)$, $\mathcal{V}(y^2 - x^3 - x^2)$, and $\mathcal{V}(y^2 - x^3 + x)$.

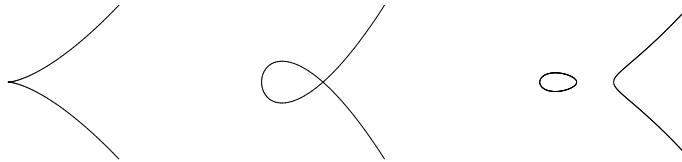


Figure 2.1: Three Cubics

These are, respectively, the cuspidal cubic, the nodal cubic, and a non-singular cubic (elliptic curve). The first two have a singularity at the origin.

Example 2.3 Let $\text{Mat}_{n \times n}$ (or $\text{Mat}_{n \times n}(\mathbb{F})$) be the set of all $n \times n$ matrices with entries in the field \mathbb{F} . Identify $\text{Mat}_{n \times n}$ with the affine space \mathbb{A}^{n^2} , giving it the structure of an affine variety. Set

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

Call SL_n the *special linear group*. We will show that SL_n is smooth, irreducible, and has dimension $n^2 - 1$. (We must first, of course, define those terms.)

Example 2.4 Let $\mathcal{X} = \mathcal{V}(f_1, \dots, f_a) \subset \mathbb{A}^n$ and $\mathcal{Y} = \mathcal{V}(g_1, \dots, g_b) \subset \mathbb{A}^m$ be affine varieties. Here, the polynomials f_i are in $\mathbb{F}[t_1, \dots, t_n]$ and the polynomials g_j are in $\mathbb{F}[s_1, \dots, s_m]$. Then $\mathcal{X} \times \mathcal{Y} \subset \mathbb{A}^{n+m}$ is $\mathcal{V}(f_1, \dots, f_a, g_1, \dots, g_b)$.

We have so far considered affine varieties defined by finitely many polynomials. More generally, given any collection $\mathcal{S} \subset \mathbb{F}[t_1, \dots, t_n]$ of polynomials, define the affine variety

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

Then \mathcal{V} associates affine varieties in \mathbb{A}^n to subsets of polynomials. Observe that \mathcal{V} reverses inclusions so that $\mathcal{S} \subset \mathcal{T}$ implies $\mathcal{V}(\mathcal{T}) \subset \mathcal{V}(\mathcal{S})$.

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

$$\mathcal{I}(\mathcal{Z}) := \{f \in \mathbb{F}[t_1, \dots, t_n] \mid f(z) = 0 \text{ for all } z \in \mathcal{Z}\}.$$

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

Thus we have two inclusion-reversing maps

$$\{\text{Subsets } \mathcal{S} \text{ of } \mathbb{F}[t_1, \dots, t_n]\} \begin{array}{c} \xrightarrow{\mathcal{V}} \\ \xleftarrow{\mathcal{I}} \end{array} \{\text{Subsets } \mathcal{Z} \text{ of } \mathbb{A}^n\} \quad (2.1)$$

which form the basis of the algebraic-geometric dictionary of affine algebraic geometry. We now refine this correspondence.

Lemma 2.5 For any $\mathcal{Z} \subset \mathbb{A}^n$, $\mathcal{I}(\mathcal{Z})$ is an ideal of $\mathbb{F}[t_1, \dots, t_n]$.

Proof: Let $f, g \in \mathcal{I}(\mathcal{Z})$. Since f and g both vanish on \mathcal{Z} , $f + g$ vanishes on \mathcal{Z} , and for any $h \in \mathbb{F}[t_1, \dots, t_n]$, hf vanishes on \mathcal{Z} . Thus both $f + g$ and hf are in $\mathcal{I}(\mathcal{Z})$. \square

Observe that if $\mathcal{S} \subset \mathbb{F}[t_1, \dots, t_n]$ and $g \in \mathbb{F}[t_1, \dots, t_n]$ is in the ideal $\langle \mathcal{S} \rangle$ generated by \mathcal{S} (by this we mean there are $f_1, \dots, f_s \in \mathcal{S}$ and $h_1, \dots, h_s \in \mathbb{F}[t_1, \dots, t_n]$ with

$$g = h_1 f_1 + \dots + h_s f_s),$$

then g vanishes on $\mathcal{V}(\mathcal{S})$. Together with Lemma 2.5, this shows that we lose nothing if we restrict the left hand side of (2.1) to the ideals of $\mathbb{F}[t_1, \dots, t_n]$.

Lemma 2.6 *For any $\mathcal{Z} \subset \mathbb{A}^n$, if $\mathcal{X} = \mathcal{V}(\mathcal{I}(\mathcal{Z}))$ is the variety defined by $\mathcal{I}(\mathcal{Z})$, then $\mathcal{I}(\mathcal{X}) = \mathcal{I}(\mathcal{Z})$.*

Proof: Set $\mathcal{X} = \mathcal{V}(\mathcal{I}(\mathcal{Z}))$. Then $\mathcal{Z} \subset \mathcal{X}$, and \mathcal{X} is the smallest variety containing \mathcal{Z} . If $\mathcal{Z} \subset \mathcal{V}(\mathcal{J})$, then necessarily $\mathcal{J} \subset \mathcal{I}(\mathcal{Z})$. Since $\mathcal{Z} \subset \mathcal{X}$, we then have $\mathcal{I}(\mathcal{Z}) \supset \mathcal{I}(\mathcal{X})$, but we also have $\mathcal{I}(\mathcal{Z}) \subset \mathcal{I}(\mathcal{X})$, and so we conclude that $\mathcal{I}(\mathcal{Z}) = \mathcal{I}(\mathcal{X})$. \square

Thus we also lose nothing if we restrict the right hand side of (2.1) to the subvarieties of \mathbb{A}^n . Our correspondence (2.1) now becomes

$$\{\text{Ideals } \mathcal{I} \text{ of } \mathbb{F}[t_1, \dots, t_n]\} \xrightleftharpoons[\mathcal{I}]{\mathcal{V}} \{\text{Subvarieties } \mathcal{Z} \text{ of } \mathbb{A}^n\} \quad (2.2)$$

This association (more precisely, the map \mathcal{V}) is not one to one. Suppose $n = 1$. When $\mathbb{F} = \mathbb{R}$ we have $\mathcal{V}(1+x^2) = \mathcal{V}(1+x^4) = \emptyset$, but the ideals generated by $1+x^2$ and $1+x^4$ are not equal. While this example is due to \mathbb{R} not being algebraically closed, the map \mathcal{V} is still not one to one when $\mathbb{F} = \mathbb{C}$. To see this, note that $\mathcal{V}(x) = \mathcal{V}(x^2) = \{0\}$.

The map $\mathcal{V} \circ (2.2)$ is one to one when we restrict it to radical ideals. An ideal \mathcal{I} is *radical* if whenever $f^m \in \mathcal{I}$ for some $m \geq 1$, then $f \in \mathcal{I}$. Given an ideal \mathcal{I} of $\mathbb{F}[t_1, \dots, t_n]$, the radical $\sqrt{\mathcal{I}}$ of \mathcal{I} is defined to be

$$\sqrt{\mathcal{I}} := \{f \in \mathbb{F}[t_1, \dots, t_n] \mid f^m \in \mathcal{I} \text{ for some } m \geq 1\}.$$

This is the smallest radical ideal containing \mathcal{I} . The reason for this definition is that if $\mathcal{Z} \subset \mathbb{A}^n$ and f^m vanishes on \mathcal{Z} for some $m \geq 1$, then f vanishes on \mathcal{Z} . We record this fact.

Lemma 2.7 *For $\mathcal{Z} \in \mathbb{A}^n$, $\mathcal{I}(\mathcal{Z})$ is a radical ideal.*

When \mathbb{F} is algebraically closed, the precise nature of the correspondence (2.2) follows from Hilbert's Nullstellensatz (null=zeroes, stelle=places, satz=theorem), one of several fundamental results of Hilbert in the 1890's that helped lay the foundations of algebraic geometry and usher in twentieth century mathematics.

Theorem 2.8 (Nullstellensatz) *Suppose \mathbb{F} is algebraically closed and $\mathcal{I} \subset \mathbb{C}[t_1, \dots, t_n]$ is an ideal. Then $\mathcal{I}(\mathcal{V}(\mathcal{I})) = \sqrt{\mathcal{I}}$.*

We give a proof of this important theorem in Appendix ????. We discuss a real version of the Nullstellensatz in Section 3.1.

Corollary 2.9 (Algebraic-Geometric Dictionary I) *The maps \mathcal{V} and \mathcal{I} give an inclusion reversing correspondence*

$$\left\{ \begin{array}{l} \text{Radical ideals } \mathcal{I} \\ \text{of } \mathbb{F}[t_1, \dots, t_n] \end{array} \right\} \begin{array}{c} \xrightarrow{\mathcal{V}} \\ \xleftarrow{\mathcal{I}} \end{array} \{ \text{Subvarieties } \mathcal{Z} \text{ of } \mathbb{A}^n \} \quad (2.3)$$

with \mathcal{I} one to one and \mathcal{V} onto, and $\mathcal{V}(\mathcal{I}(\mathcal{Y})) = \mathcal{Y}$. When \mathbb{F} is algebraically closed, the maps \mathcal{I} and \mathcal{V} are inverses, and hence the correspondence is one to one and onto.

Proof: First, we have already observed that \mathcal{V} and \mathcal{I} reverse inclusions. By Definition 2.1, $\mathcal{V}(\mathcal{I})$ is a subvariety of \mathbb{A}^n and by Lemma 2.7, $\mathcal{I}(\mathcal{Z})$ is a radical ideal. When \mathbb{F} is algebraically closed, the Nullstellensatz implies that composition $\mathcal{V} \circ \mathcal{I}$ is the identity, so \mathcal{V} is one to one, for any field. Finally, as $\mathcal{V}(\mathcal{I}) = \mathcal{V}(\sqrt{\mathcal{I}})$, the map \mathcal{V} is onto, when \mathbb{F} is algebraically closed. This proves the corollary. \square

This correspondence will be further refined in Section 2.4 to include maps between varieties. Because of this correspondence, each geometric concept has a corresponding algebraic concept, when \mathbb{F} is algebraically closed. When \mathbb{F} is not algebraically closed, the correspondence is not exact. In that case, we will use algebra (or the situation when \mathbb{F} is algebraically closed) to guide our geometric definitions. This is appropriate, as it is important for us to not only consider the zeroes $\mathcal{V}(\mathcal{I})$ of an ideal $\mathcal{I} \subset \mathbb{F}[t_1, \dots, t_n]$ in $\mathbb{A}_{\mathbb{F}}^n$, but also its super set of zeroes in $\mathbb{A}_{\overline{\mathbb{F}}}^n$, the affine space over $\overline{\mathbb{F}}$, the algebraic closure of \mathbb{F} .

We present an equivalent form of the Nullstellensatz.

Theorem 2.10 (Weak Nullstellensatz) *Suppose \mathbb{F} be algebraically closed. If \mathcal{I} is an ideal of $\mathbb{F}[t_1, \dots, t_n]$ with $\mathcal{V}(\mathcal{I}) = \emptyset$, then $\mathcal{I} = \mathbb{F}[t_1, \dots, t_n]$.*

Thus if $\mathcal{V}(f_1, \dots, f_s) = \emptyset$, by which we mean that there are no common solutions to the system of polynomial equations

$$f_1(t) = f_2(t) = \dots = f_s(t) = 0,$$

then there exist polynomials $g_1, \dots, g_s \in \mathbb{F}[t_1, \dots, t_n]$ such that

$$1 = g_1 f_1 + g_2 f_2 + \dots + g_s f_s.$$

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

Theorem 2.11 (Multivariate Fundamental Theorem of Algebra) *If the ideal generated by polynomials $f_1, \dots, f_s \in \mathbb{F}[t_1, \dots, t_n]$ is not the whole ring $\mathbb{F}[t_1, \dots, t_n]$, then the system of polynomial equations*

$$f_1(t) = f_2(t) = \dots = f_s(t) = 0$$

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

2.2 Generic Properties of Varieties

We saw in Example 2.4 that the product of two affine varieties is again an affine variety. The same is true for intersections and unions.

Theorem 2.12 *The intersection of any collection of affine varieties is again an affine variety. The union of any finite collection of affine varieties is again an affine variety.*

Proof: For the first statement, let $\{\mathcal{I}_\gamma \mid \gamma \in \Gamma\}$ be a collection of ideals in $\mathbb{F}[t_1, \dots, t_n]$. Then we have

$$\bigcap_{\gamma \in \Gamma} \mathcal{V}(\mathcal{I}_\gamma) = \mathcal{V}\left(\bigcup_{\gamma \in \Gamma} \mathcal{I}_\gamma\right).$$

For the second statement, it suffices to consider the union of two affine varieties. Let \mathcal{I}, \mathcal{J} be ideals of $\mathbb{F}[t_1, \dots, t_n]$. Then we have

$$\mathcal{V}(\mathcal{I}) \cup \mathcal{V}(\mathcal{J}) = \mathcal{V}(\{f \cdot g \mid f \in \mathcal{I}, g \in \mathcal{J}\}).$$

□

We introduce the following useful terminology.

Definition 2.13 We call an affine variety a *Zariski closed set*. The complement of a Zariski closed set is a *Zariski open set*. The reason for this terminology is that by Theorem 2.12, affine varieties in \mathbb{A}^n form the closed sets of a topology on \mathbb{A}^n , called the *Zariski topology*.

We emphasize that the purpose of this terminology is to aid our discussion of affine varieties, and not because topology is a prerequisite for algebraic geometry. This Zariski topology is rather strange.

Example 2.14 The Zariski closed subsets of \mathbb{A}^1 are the empty set \emptyset , finite collections of points, and \mathbb{A}^1 itself. Thus the usual separation properties of Hausdorff spaces (any two points are covered by disjoint open sets) fails spectacularly when \mathbb{F} is infinite.

We compare this Zariski topology with the usual (Euclidean) topology on \mathbb{R}^n or \mathbb{C}^n .

Proposition 2.15 *Suppose that \mathbb{F} is one of \mathbb{R} or \mathbb{C} . Then*

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

6. \mathbb{R}^n is Zariski dense in \mathbb{C}^n .

Proof: For statements 1 and 2, a Zariski closed set $\mathcal{V}(\mathcal{I})$ is the intersection of the hypersurfaces $\mathcal{V}(f)$ for $f \in \mathcal{I}$, so it suffices to consider the case of a hypersurface $\mathcal{V}(f)$. But this follows as $f : \mathbb{A}^n \rightarrow \mathbb{F}$ is a continuous function in the Zariski topology and $\mathcal{V}(f) = f^{-1}(0)$.

For the third statement, it suffices to show that a nonempty ball B containing the origin is dense in the Zariski topology. If a polynomial f vanishes on B , then all of its partial derivatives do as well. In particular, as all partial derivatives of f vanish at 0, all coefficients of f vanish, and hence f is identically zero on \mathbb{A}^n . Thus B is dense in the Zariski topology.

For statements 4 and 5, observe that if f is nonconstant, then by 3, the interior of the (Euclidean) closed set $\mathcal{V}(f)$ is empty, hence $\mathcal{V}(f)$ is nowhere dense.

Lastly, if a polynomial vanishes on \mathbb{R}^n , then all of its partial derivatives are zero and so it vanishes on \mathbb{C}^n . \square

Example 2.16 The Zariski topology on a product $\mathcal{X} \times \mathcal{Y}$ of varieties is in general not the product topology. In the product topology on \mathbb{A}^2 , the closed sets are finite unions of the following sets: the empty set, points, lines of the form $\{t\} \times \mathbb{A}^1$ or $\mathbb{A}^1 \times \{t\}$, the whole space \mathbb{A}^2 . On the other hand \mathbb{A}^2 contains a rich collection of 1-dimensional subvarieties (called *curves*), such as the cubic curves of Example 2.2, which are not in that list.

The fourth statement in Proposition 2.15 leads to the very important notions of genericity and of generic sets and properties.

Definition 2.17 A subset $\mathcal{G} \subset \mathbb{A}^n$ is called *generic* if there is a nonempty Zariski open set \mathcal{X} with $\mathcal{X} \subset \mathcal{G}$. A property is generic if the set of points where it holds is a generic set.

When \mathbb{F} is \mathbb{R} or \mathbb{C} , generic sets $\mathcal{G} \subset \mathbb{A}^n$ are dense in the Euclidean topology.

Example 2.18 The generic $n \times n$ matrix is invertible. Set

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

the set of all invertible $n \times n$ matrices, called the *general linear group*. Since GL_n equals $\text{Mat}_{n \times n} - \mathcal{V}(\det)$, it is Zariski open. As GL_n is nonempty (for instance, it contains the $n \times n$ identity matrix I_n), it is a generic set.

Example 2.19 The general univariate polynomial of degree n has n distinct roots. Identify \mathbb{A}^n with the set of univariate polynomials of degree n via

$$(a_1, \dots, a_n) \in \mathbb{A}^n \longmapsto x^n + a_1 x^{n-1} + \dots + a_n \in \mathbb{F}[x]. \quad (2.4)$$

We construct the *discriminant* $\Delta \in \mathbb{F}[a_1, \dots, a_n]$ which vanishes precisely when the polynomial (2.4) has fewer than n distinct complex roots, which shows the general univariate polynomial of degree n has n distinct complex roots.

A polynomial $f \in \mathbb{F}[x]$ of degree n has fewer than n distinct complex roots when it has a double root. In this case, f and its derivative f' have a factor in common. We use linear algebra to detect this. Let S_m be the set of polynomials of degree at most m , a vector space of dimension $m + 1$. Consider the linear map

$$\begin{aligned} \varphi_n : S_{n-1} \times S_{n-2} &\longrightarrow S_{2n-2} \\ (g, h) &\longmapsto f'g + fh \end{aligned}$$

If φ_n is onto, then $1 = f'g + fh$ for some pair (g, h) and so f and f' are relatively prime. Conversely, if f and f' share a common root y in $\overline{\mathbb{F}}$, then every polynomial in the image of φ_n also vanishes at y and so φ_n is not onto. It follows that the *discriminant* polynomial $\Delta := \det \varphi_n$ vanishes precisely when f and f' have a common root. This discriminant is a polynomial of degree $2n - 2$ in the coefficients a_1, \dots, a_n : In the basis of S_m given by the monomials in x , φ_n is a $(2n - 1) \times (2n - 1)$ matrix whose entries are the coefficients of f and f' and the first column has entries the constants $1, n$, and 0 .

For example, if $n = 2$ and $f = x^2 + ax + b$, then

$$\varphi_2 = \begin{bmatrix} 0 & 2 & a \\ 2 & a & 0 \\ 1 & a & b \end{bmatrix} \quad \text{and} \quad \Delta = a^2 - 4b.$$

A complex $n \times n$ matrix is *semisimple* or diagonalizable if \mathbb{C}^n has a basis of eigenvectors for M .

Example 2.20 The generic complex $n \times n$ matrix is semisimple. Let $M \in \text{Mat}_{n \times n}$ and consider the (monic) characteristic polynomial of M .

$$\chi(\lambda) := \det(\lambda I_n - M).$$

If M is not semisimple, then in particular $\chi(\lambda)$ has a double root. The coefficients of $\chi(\lambda)$ are polynomials in the entries of M . Evaluating the discriminant at these coefficients gives a polynomial ψ in the entries of M that vanishes precisely when the characteristic polynomial has a double root.

Since $\text{Mat}_{n \times n} - \mathcal{V}(\psi)$ consists of matrices with distinct eigenvalues, it is a nonempty Zariski open subset of the set of semisimple matrices. This shows that the semisimple matrices constitute a generic subset of $\text{Mat}_{n \times n}$.

When $n = 2$,

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

and so the polynomial ψ is $(a_{11} + a_{22})^2 - 4(a_{11}a_{22} - a_{12}a_{21})$.

Exercise 2.1 Prove the statement of Example 2.14 about the Zariski topology on \mathbb{A}^1 : A closed set is either the empty set, a finite collection of points, or \mathbb{A}^1 itself.

2.3 Unique Factorization for Varieties

We initially defined an affine variety to be the set of common zeroes of a finite set of polynomials, and then later extended this to the common zeroes of all polynomials in an ideal. Does this added generality give us anything new? In other words, are there any ideals in $\mathbb{F}[t_1, \dots, t_n]$ which are not of the form

$$\langle f_1, \dots, f_s \rangle := \left\{ \sum_{i=1}^s g_i f_i \mid g_1, \dots, g_s \in \mathbb{F}[t_1, \dots, t_n] \right\} ?$$

The answer is that we do not gain anything; all ideals of $\mathbb{F}[t_1, \dots, t_n]$ are finitely generated.

This result, due to Hilbert, implies many important finiteness properties of algebraic varieties. In particular, the existence and effectivity of computational techniques is a consequence of this Hilbert Basis Theorem, which we state below. We give a proof in Section 3.2, where we discuss Gröbner bases, the foundation of many effective algorithms in algebraic geometry.

Theorem 2.21 (Hilbert Basis Theorem) *Every ideal \mathcal{I} of $\mathbb{F}[t_1, \dots, t_n]$ is finitely generated.*

A direct consequence of the Basis Theorem is the following corollary.

Corollary 2.22 *Any affine variety $\mathcal{Z} \subset \mathbb{A}^n$ is an intersection of a finite number of hypersurfaces.*

Proof: Let $f_1, \dots, f_s \in \mathbb{F}[t_1, \dots, t_n]$ generate the ideal $\mathcal{I}(\mathcal{Z})$ of \mathcal{Z} . Then $\mathcal{Z} = \mathcal{V}(f_1) \cap \dots \cap \mathcal{V}(f_s)$. \square

We will establish a basic structure theorem for affine varieties, which is an analog of unique factorization for polynomials. A polynomial $f \in \mathbb{F}[t_1, \dots, t_n]$ is *reducible* if we can write $f = gh$ with neither g nor h a constant; otherwise f is *irreducible*. Given $f \in \mathbb{F}[t_1, \dots, t_n]$, we may write f as a product of irreducible polynomials

$$f = g_1^{l_1} \cdot g_2^{l_2} \cdots g_r^{l_r}, \quad (2.5)$$

where each $l_i > 0$ and each g_i is irreducible and non-constant, and if $i \neq j$, then g_i and g_j are not proportional. A basic property of the polynomial ring $\mathbb{F}[t_1, \dots, t_n]$ is that it is a unique factorization domain; any factorization of f into irreducibles (2.5) is essentially unique. We give a proof in Appendix ????. By this we mean that if we have another such factorization

$$f = h_1^{m_1} \cdot h_2^{m_2} \cdots h_s^{m_s},$$

then $r = s$, and we may reorder the factors so that $l_i = m_i$, and g_i is a scalar multiple of h_i , for each $i = 1, \dots, s$.

This algebraic property has an immediate geometric consequence for hypersurfaces. Suppose a polynomial f is factored into irreducibles (2.5). Then the hypersurface $\mathcal{X} = \mathcal{V}(f)$ is the union of hypersurfaces $\mathcal{X}_i := \mathcal{V}(g_i)$, and this decomposition of \mathcal{X}

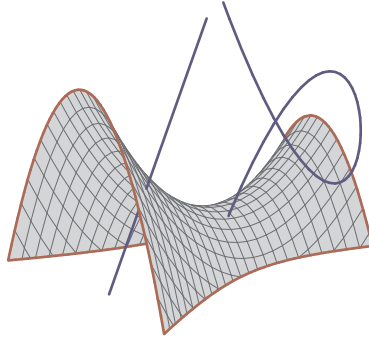
$$\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2 \cup \cdots \cup \mathcal{X}_r$$

into hypersurfaces defined by irreducible polynomials is unique.

We show this decomposition property is shared by general affine varieties, and prove this geometric property.

Definition 2.23 An affine variety \mathcal{X} is *reducible* if there exist proper closed subvarieties $\mathcal{X}_1, \mathcal{X}_2 \subsetneq \mathcal{X}$ with $\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2$. Otherwise \mathcal{X} is *irreducible*.

Example 2.24 We display a reducible variety below. It has 3 components, one is a surface, and the other 2 are curves.



Example 2.25 The special linear group $SL_n = \mathcal{V}(\det - 1)$ is an irreducible variety. If $\det - 1 = fg$ is a nontrivial factorization, then the top homogeneous components of f and g give a nontrivial factorization of the determinant polynomial \det .

We use induction on n to show that the determinant polynomial \det_n for $n \times n$ matrices is irreducible. When $n = 1$, $\det_1 = x_{11}$ is irreducible. Suppose now that \det_{n-1} is irreducible and that we may factor $\det_n = fg$. Since \det_n is linear in the lower right entry x_{nn} of a matrix in $\text{Mat}_{n \times n}$, we may assume that f is the factor of $\det_n = fg$ in which x_{nn} appears. Then f is linear in x_{nn} , so that there are polynomials a and b in which x_{nn} does not appear with $f = x_{nn} \cdot a + b$. We then have

$$\det_n = fg = x_{nn} \cdot ag + bg.$$

Since \det_{n-1} is the coefficient of x_{nn} in \det_n , we have $ag = \det_{n-1}$. Our induction hypothesis is that \det_{n-1} is irreducible, so either $g = 1$, which shows that \det_n is irreducible, or else $a = 1$. If $a = 1$, then $g = \det_{n-1}$ divides \det_n . To see this cannot happen, consider the matrix M whose only non-zero entries are $x_{i,n-i} = 1$. Then $\det_{n-1}(M) = 0$, but $\det_n(M) = (-1)^{\binom{n}{2}} \neq 0$.

Theorem 2.26 A product $\mathcal{X} \times \mathcal{Y}$ of irreducible affine varieties is irreducible.

Proof: Suppose that $\mathcal{X} \times \mathcal{Y} = \mathcal{Z}_1 \cup \mathcal{Z}_2$, with each \mathcal{Z}_i a closed subset of $\mathcal{X} \times \mathcal{Y}$. For each $x \in \mathcal{X}$, the closed set $\{x\} \times \mathcal{Y}$ is isomorphic to \mathcal{Y} , and is therefore irreducible. Since

$$\{x\} \times \mathcal{Y} = ((\{x\} \times \mathcal{Y}) \cap \mathcal{Z}_1) \cup ((\{x\} \times \mathcal{Y}) \cap \mathcal{Z}_2),$$

either $\{x\} \times \mathcal{Y} \subset \mathcal{Z}_1$ or else $\{x\} \times \mathcal{Y} \subset \mathcal{Z}_2$. The subset $\mathcal{X}_1 \subset \mathcal{X}$ consisting of those $x \in \mathcal{X}$ with $\{x\} \times \mathcal{Y} \subset \mathcal{Z}_1$ is a closed subset: We have $\mathcal{X}_1 = \bigcap_{y \in \mathcal{Y}} \mathcal{X}_y$, where \mathcal{X}_y is the collection of points $\{x \in \mathcal{X} \mid x \times y \in \mathcal{Z}_1\}$. Since $\mathcal{X}_y \times \{y\} = (\mathcal{X} \times \{y\}) \cap \mathcal{Z}_1$, \mathcal{X}_y and hence \mathcal{X}_1 is closed. Similarly define the closed subset \mathcal{X}_2 . Since $\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2$ and \mathcal{X} is irreducible, we either have $\mathcal{X} = \mathcal{X}_1$ or $\mathcal{X} = \mathcal{X}_2$. But $\mathcal{X} = \mathcal{X}_i$ implies $\mathcal{X} \times \mathcal{Y} = \mathcal{Z}_i$, which proves $\mathcal{X} \times \mathcal{Y}$ is irreducible. \square

Under the algebraic-geometric dictionary, the geometric property of irreducibility corresponds algebraically to prime ideals. An ideal \mathcal{I} is *prime* if whenever $f_1 \cdot f_2 \in \mathcal{I}$ with $f_1 \notin \mathcal{I}$, then $f_2 \in \mathcal{I}$.

Theorem 2.27 *An affine variety \mathcal{X} is irreducible if and only if the ideal $\mathcal{I}(\mathcal{X})$ of \mathcal{X} is prime.*

This shows that a hypersurface $\mathcal{X} = \mathcal{V}(f)$ is irreducible if and only if f is irreducible.

Proof: Let \mathcal{X} be an affine variety and set $\mathcal{I} := \mathcal{I}(\mathcal{X})$. Suppose \mathcal{X} is irreducible and we have polynomials $f_1, f_2 \notin \mathcal{I}$. Then $\mathcal{X}_1 := \mathcal{X} \cap \mathcal{V}(f_1)$ and $\mathcal{X}_2 := \mathcal{X} \cap \mathcal{V}(f_2)$ are proper Zariski closed subsets of \mathcal{X} so that $\mathcal{X}_1 \cup \mathcal{X}_2 = \mathcal{V}(f_1 f_2)$ is also a proper closed subset of \mathcal{X} , as \mathcal{X} is irreducible. But then $f_1 f_2 \notin \mathcal{I}$, which implies that \mathcal{I} is prime.

Suppose now that \mathcal{X} is reducible with $\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2$ where \mathcal{X}_1 and \mathcal{X}_2 are proper closed subvarieties of \mathcal{X} . Then there exist polynomials f_1, f_2 with f_i vanishing on \mathcal{X}_i , but not on all of \mathcal{X} , for $i = 1, 2$. That is, $f_1, f_2 \notin \mathcal{I}$. Since $\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2$, the polynomial $f_1 f_2$ vanishes on \mathcal{X} and so is in \mathcal{I} . Thus \mathcal{I} is not prime. \square

Theorem 2.28 *Any affine variety is a finite union of irreducible subvarieties.*

Proof: Suppose the theorem fails for an affine variety $\mathcal{X} \subset \mathbb{A}^n$. Then \mathcal{X} is reducible, and we may write $\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}'_1$ with both \mathcal{X}_1 and \mathcal{X}'_1 proper subvarieties of \mathcal{X} . If the theorem held for both \mathcal{X}_1 and \mathcal{X}'_1 , then it would hold for \mathcal{X} . Thus it must fail for one, say \mathcal{X}_1 . But then \mathcal{X}_1 is reducible, and has a proper subvariety \mathcal{X}_2 for which the theorem fails. Continuing in this fashion, we find an infinite descending chain of subvarieties of \mathcal{X}

$$\mathcal{X} \supsetneq \mathcal{X}_1 \supsetneq \mathcal{X}_2 \supsetneq \cdots .$$

If we consider the ideals of these varieties, we obtain an infinite increasing chain of ideals in $\mathbb{F}[t_1, \dots, t_n]$

$$\mathcal{I}(\mathcal{X}) \subsetneq \mathcal{I}(\mathcal{X}_1) \subsetneq \mathcal{I}(\mathcal{X}_2) \subsetneq \cdots .$$

The union \mathcal{I} of these ideals is an ideal. By the Hilbert Basis Theorem 2.21, \mathcal{I} is finitely generated, thus there is some integer N so that $\mathcal{I}(\mathcal{X}_N)$ contains these generators, and so $\mathcal{I} = \mathcal{I}(\mathcal{X}_N)$, which is a contradiction. \square

If we write an affine variety $\mathcal{X} = \cup_i \mathcal{X}_i$ as a finite union of irreducible subvarieties \mathcal{X}_i , and we have $\mathcal{X}_i \subset \mathcal{X}_j$ for some $i \neq j$, then we may delete \mathcal{X}_i from this union. Continuing in this fashion, we arrive at a decomposition $\mathcal{X} = \cup_i \mathcal{X}_i$ where if $i \neq j$, then $\mathcal{X}_i \not\subset \mathcal{X}_j$. This decomposition is unique: If $\mathcal{X} = \cup_j \mathcal{Y}_j$, then as $\mathcal{X}_i = \cup_j (\mathcal{Y}_j \cap \mathcal{X}_i)$ and \mathcal{X}_i is irreducible, we must have $\mathcal{X}_i \subset \mathcal{Y}_j$ for some j . Applying the same reasoning to \mathcal{Y}_j gives $\mathcal{Y}_j \subset \mathcal{X}_k$, for some k . But then $\mathcal{X}_i \subset \mathcal{X}_k$ and so $i = k$ and $\mathcal{X}_i = \mathcal{Y}_j$. We call these subvarieties \mathcal{X}_i the *irreducible components* of \mathcal{X} . We summarize these facts in the following basic structure theorem for varieties.

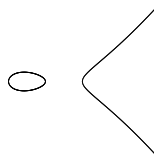
Corollary 2.29 (Unique Decomposition of Varieties) *An affine variety \mathcal{X} has a unique decomposition as a finite union of irreducible subvarieties*

$$\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2 \cup \cdots \cup \mathcal{X}_s.$$

When \mathbb{F} is algebraically closed, we have the following result comparing the algebraic and usual Euclidean notions of connected components. **Cite Something?**

Proposition 2.30 *An irreducible complex affine variety is connected in the Euclidean topology.*

Example 2.31 Irreducible real algebraic varieties need not have this property. Consider the irreducible cubic plane curve $\mathcal{V}(y^2 - x^3 + x)$ in $\mathbb{A}_{\mathbb{R}}^2$:



This has 2 (Euclidean) connected components, even though it is irreducible as an algebraic variety.

2.4 Regular and Rational Functions

The algebraic-geometric dictionary of Section 2.1 is strengthened significantly when we include regular algebraic maps between affine varieties and corresponding homomorphisms between rings of regular functions. In addition to regular functions and maps, algebraic geometry also uses rational maps between varieties which are not defined at all points of a variety. Working with functions and maps not defined at every point is a special feature of algebraic geometry that sets it apart from other branches of geometry.

Suppose \mathbb{F} is algebraically closed. Then a *regular function* $f : \mathcal{X} \rightarrow \mathbb{F}$ on an affine variety $X \subset \mathbb{A}^n$ is given by restricting a polynomial function $F \in \mathbb{F}[t_1, \dots, t_n]$ to X . Since we may add and multiply regular functions, the set of all regular functions on a variety \mathcal{X} forms a ring $\mathbb{F}[\mathcal{X}]$ called the *coordinate ring* of \mathcal{X} or *ring of regular functions* on \mathcal{X} . The surjective ring homomorphism

$$\mathbb{F}[t_1, \dots, t_n] \twoheadrightarrow \mathbb{F}[\mathcal{X}] \tag{2.6}$$

given by restricting polynomials to \mathcal{X} has kernel those polynomials that vanish on \mathcal{X} , that is $\mathcal{I}(\mathcal{X})$. Thus we see that

$$\mathbb{F}[\mathcal{X}] \simeq \mathbb{F}[t_1, \dots, t_n]/\mathcal{I}(\mathcal{X}). \quad (2.7)$$

When \mathbb{F} is not algebraically closed, suppose that the variety $\mathcal{X} = \mathcal{V}(\mathcal{I})$, where \mathcal{I} is radical. Then we define the coordinate ring $\mathbb{F}[\mathcal{X}]$ of \mathcal{X} to be the ring $\mathbb{F}[t_1, \dots, t_n]/\mathcal{I}$. This is consistent with our desire to have definitions that are stable when we pass to the algebraic closure of our ground field.

Suppose $\mathcal{X} \subset \mathbb{A}^n$ and $\mathcal{Y} \subset \mathbb{A}^m$ are varieties respectively defined by radical ideals \mathcal{I} and \mathcal{J} , and we form their product $\mathcal{X} \times \mathcal{Y} \subset \mathbb{A}^{n+m}$ as in Example 2.4. Since $\mathcal{X} \times \mathcal{Y}$ is defined by the ideal $\mathcal{I} + \mathcal{J}$, we see that $\mathbb{F}[\mathcal{X} \times \mathcal{Y}] = \mathbb{F}[\mathcal{X}] \otimes_{\mathbb{F}} \mathbb{F}[\mathcal{Y}]$, the tensor product of the coordinate rings.

By (2.6), the coordinate ring $\mathbb{F}[\mathcal{X}]$ is a finitely generated \mathbb{F} -algebra. Since $\mathcal{I}(\mathcal{X})$ is radical, if $0 \neq f \in \mathbb{F}[\mathcal{X}]$, then $f^m \neq 0$ for every integer $m \geq 0$. We call such an algebra with no nilpotent elements *reduced*. When \mathbb{F} is algebraically closed, these two properties characterize coordinate rings of affine varieties.

Theorem 2.32 *Suppose \mathbb{F} is algebraically closed. Then a \mathbb{F} -algebra R is the coordinate ring of an affine variety if and only if R is finitely generated and reduced.*

Proof: Suppose that R is a reduced \mathbb{F} -algebra with generators f_1, \dots, f_n . Consider the surjective ring homomorphism

$$\varphi : \mathbb{F}[t_1, \dots, t_n] \longrightarrow R$$

given by $t_i \mapsto f_i$. Let $\mathcal{I} \subset \mathbb{F}[t_1, \dots, t_n]$ be the kernel of φ . Since R is reduced, \mathcal{I} is a radical ideal.

When \mathbb{F} is algebraically closed, the algebraic-geometric dictionary of Corollary 2.9 shows that $\mathcal{I} = \mathcal{I}(\mathcal{V}(\mathcal{I}))$, and so $R \simeq \mathbb{F}[t_1, \dots, t_n]/\mathcal{I} = \mathbb{F}[\mathcal{V}(\mathcal{I})]$. \square

Note that a different choice of generators g_1, \dots, g_m for R in this proof will give a different affine variety with coordinate ring R . One goal of this section is to understand this apparent ambiguity.

Among the coordinate rings $\mathbb{F}[\mathcal{X}]$ of affine varieties are the polynomial algebras $\mathbb{F}[t_1, \dots, t_n] = \mathbb{F}[\mathbb{A}^n]$. Many properties of polynomial algebras, including the algebraic-geometric dictionary (Corollary 2.9) and the Hilbert Theorems (Theorems 2.8 and 2.21) hold for coordinate rings $\mathbb{F}[\mathcal{X}]$. We briefly describe that here.

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

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

is a subvariety of \mathcal{X} . To see this, let $F_1, \dots, F_s \in \mathbb{F}[t_1, \dots, t_n]$ be polynomials representing f_1, \dots, f_s . Then

$$\mathcal{V}(f_1, \dots, f_s) = \mathcal{X} \cap \mathcal{V}(F_1, \dots, F_s).$$

As in Section 2.1, we extend this notion and define $\mathcal{V}(\mathcal{I})$ for an ideal \mathcal{I} of $\mathbb{F}[\mathcal{X}]$. Similarly, if $\mathcal{Z} \subset \mathcal{X}$, then $\mathcal{I}(\mathcal{X}) \subset \mathcal{I}(\mathcal{Z})$ in $\mathbb{F}[t_1, \dots, t_n]$ and so $\mathcal{I}(\mathcal{Z})/\mathcal{I}(\mathcal{X})$ is an ideal of $\mathbb{F}[\mathcal{X}] = \mathbb{F}[\mathbb{A}^n]/\mathcal{I}(\mathcal{X})$.

Both Hilbert's Nullstellensatz and Hilbert's Basis Theorem have analogs for affine varieties \mathcal{X} and their coordinate rings $\mathbb{F}[\mathcal{X}]$. These are consequences of the original Hilbert Theorems which follow from the surjection $\mathbb{F}[\mathbb{A}^n] \rightarrow \mathbb{F}[\mathcal{X}]$ and the corresponding inclusion $\mathcal{X} \subset \mathbb{A}^n$.

Theorem 2.33 (Hilbert Theorems for $\mathbb{F}[\mathcal{X}]$) *Let \mathcal{X} be an affine variety. Then*

1. *Any ideal of $\mathbb{F}[\mathcal{X}]$ is finitely generated.*
2. *If $\mathcal{Z} \subset \mathcal{X}$, then $\mathcal{I}(\mathcal{Z}) \subset \mathbb{F}[\mathcal{X}]$ is a radical ideal.*
3. *Suppose \mathbb{F} is algebraically closed. An ideal \mathcal{I} of $\mathbb{F}[\mathcal{X}]$ defines the empty set if and only if $\mathcal{I} = \mathbb{F}[\mathcal{X}]$.*

We obtain a version of the algebraic-geometric dictionary between subvarieties of \mathcal{X} and radical ideals of $\mathbb{F}[\mathcal{X}]$ in the same fashion as the original algebraic-geometric dictionary of Corollary 2.9.

Theorem 2.34 *Let \mathcal{X} be an affine variety. Then the maps \mathcal{V} and \mathcal{I} give an inclusion reversing correspondence*

$$\left\{ \begin{array}{l} \text{Radical ideals} \\ \mathcal{I} \text{ of } \mathbb{F}[\mathcal{X}] \end{array} \right\} \begin{array}{c} \xrightarrow{\mathcal{V}} \\ \xleftarrow{\mathcal{I}} \end{array} \{ \text{Subvarieties } \mathcal{Y} \text{ of } \mathcal{X} \} \quad (2.8)$$

with \mathcal{I} one to one and \mathcal{V} onto, and $\mathcal{V}(\mathcal{I}(\mathcal{Y})) = \mathcal{Y}$. When \mathbb{F} is algebraically closed, the maps \mathcal{I} and \mathcal{V} are inverses, and hence bijections.

Definition 2.35 A list $f_1, \dots, f_m \in \mathbb{F}[\mathcal{X}]$ of regular functions on an affine variety \mathcal{X} gives a *regular map*

$$\begin{aligned} \varphi : \mathcal{X} &\longrightarrow \mathbb{A}^m \\ x &\longmapsto (f_1(x), \dots, f_m(x)). \end{aligned}$$

Regular maps between affine varieties are continuous in the Zariski topology.

If $g(t_1, \dots, t_m) \in \mathbb{F}[\mathbb{A}^m]$ is a polynomial, then $\varphi^*g(x) := g(f_1(x), \dots, f_m(x))$ defines a regular function φ^*g , equivalently, $\varphi^*g := g(f_1, \dots, f_m) \in \mathbb{F}[\mathcal{X}]$. This pullback $\varphi^* : \mathbb{F}[\mathbb{A}^m] \rightarrow \mathbb{F}[\mathcal{X}]$ is a ring homomorphism and when \mathbb{F} is algebraically closed, its kernel consists of those polynomials $g \in \mathbb{F}[\mathbb{A}^m]$ which vanish on $\varphi(\mathcal{X})$. In this way, we say that $\varphi(\mathcal{X})$ is a subset of an affine variety Y if and only if $\varphi^*(\mathcal{I}(Y)) = 0$ in $\mathbb{F}[\mathcal{X}]$. When \mathbb{F} is algebraically closed, this characterizes the affine varieties Y with $\varphi(\mathcal{X}) \subset Y$, and when \mathbb{F} is not algebraically closed, it provides an adequate notion that is stable under extension to the algebraic closure. Thus if $\varphi : \mathcal{X} \rightarrow \mathcal{Y}$ with \mathcal{Y} an affine variety, then the ring homomorphism φ^* factors through the coordinate ring $\mathbb{F}[\mathcal{Y}] = \mathbb{F}[\mathbb{A}^m]/\mathcal{I}(\mathcal{Y})$ of \mathcal{Y} .

Conversely, let $\psi : \mathbb{F}[\mathcal{Y}] \rightarrow \mathbb{F}[\mathcal{X}]$ be a ring homomorphism between the coordinate rings of affine varieties $Y \subset \mathbb{A}^m$ and $\mathcal{X} \subset \mathbb{A}^n$. Let t_1, \dots, t_m be the images in $\mathbb{F}[\mathcal{Y}]$ of the coordinate functions on \mathbb{A}^m and for $i = 1, \dots, m$, set $f_i := \psi(t_i)$. Then $f_1, \dots, f_m \in \mathbb{F}[\mathcal{X}]$ defines a regular map $\varphi : \mathcal{X} \rightarrow \mathcal{Y} \subset \mathbb{A}^m$ such that $\varphi^* = \psi$.

Example 2.36 Matrix multiplication is a regular map. If (x_{ij}) and (y_{kl}) are the coordinates of $\text{Mat}_{n \times m}$ and $\text{Mat}_{m \times p}$, respectively, then the multiplication map $\mu : \text{Mat}_{n \times m} \times \text{Mat}_{m \times p} \rightarrow \text{Mat}_{n \times p}$ is defined by the np regular functions

$$f_{il} := x_{i1}y_{1l} + x_{i2}y_{2l} + \cdots + x_{im}y_{ml}.$$

Definition 2.37 A regular map $\varphi : \mathcal{X} \rightarrow \mathcal{Y}$ of affine varieties is an *isomorphism* if φ has an inverse which is also a regular map.

By the correspondence between maps of affine varieties and homomorphisms of their coordinate rings, we can see that $\varphi : \mathcal{X} \rightarrow \mathcal{Y}$ is an isomorphism if and only if $\varphi^* : \mathbb{F}[\mathcal{Y}] \rightarrow \mathbb{F}[\mathcal{X}]$ is a ring isomorphism.

Example 2.38 The map $t \mapsto (t, t^2)$ from \mathbb{A}^1 to the parabola $\mathcal{V}(y - x^2)$ is an isomorphism as it has inverse $(x, y) \mapsto x$. On the other hand, the bijection $\varphi : t \mapsto (t^2, t^3)$ from \mathbb{A}^1 to the cuspidal cubic $(y^2 - x^3)$ is not an isomorphism as the image of φ^* in $\mathbb{F}[t]$ consists of those polynomials f without a linear term, that is $f'(0) = 0$.

We refine the algebraic-geometric dictionary. A map between mathematical structures which takes maps to maps, but reverses directions of arrows is called a *contravariant functor* [19].

Theorem 2.39 (Algebraic-Geometric Dictionary II) *The association $\mathcal{X} \mapsto \mathbb{F}[\mathcal{X}]$ of an affine variety \mathcal{X} its coordinate ring $\mathbb{F}[\mathcal{X}]$ is a contravariant functor*

$$\{\text{Affine algebraic varieties}\} \xrightarrow{\mathbb{F}[\cdot]} \left\{ \begin{array}{l} \text{Finitely generated} \\ \text{reduced } \mathbb{F}\text{-algebras} \end{array} \right\} \quad (2.9)$$

When \mathbb{F} is algebraically closed, there is an inverse map Spec such that if R is a finitely generated reduced \mathbb{F} -algebra, then $R \simeq \mathbb{C}[\text{Spec}(R)]$, and if $\mathcal{X} \in \mathbb{A}^n$ is an affine variety, then $\mathcal{X} \simeq \text{Spec}(\mathbb{F}[\mathcal{X}])$.

We remark on this map Spec . Given a finitely generated reduced \mathbb{C} -algebra $R = \mathbb{F}[t_1, \dots, t_n]/\mathcal{I}$, let $\text{Spec}(R) = \mathcal{V}(\mathcal{I}) \subset \mathbb{A}_{\mathbb{F}}^n$. Even though this map depends upon the choice of algebraic generators t_1, \dots, t_n for R , any two such choices are canonically isomorphic. Theorem 2.39 is the strongest statement about the equivalence of algebraic and geometrical concepts.

We use the notion of isomorphism to introduce the important construction of a principal affine open set.

Definition 2.40 Let $\mathcal{X} \subset \mathbb{A}^n$ be an affine variety and let $f \in \mathbb{F}[\mathcal{X}]$ be a non-zero regular function. Define the *principal (affine) open set* \mathcal{X}_f by

$$\mathcal{X}_f := \{x \in X \mid f(x) \neq 0\}.$$

Let $F \in \mathbb{F}[\mathbb{A}^n]$ be a polynomial representative of $f \in \mathbb{F}[\mathcal{X}]$. Consider the affine variety in \mathbb{A}^{n+1}

$$\mathcal{U} := \mathcal{V}(F_1, \dots, F_s, Ft_{n+1} - 1), \quad (2.10)$$

where F_1, \dots, F_s generate the ideal of \mathcal{X} and t_{n+1} is the last coordinate function on \mathbb{A}^{n+1} . The projection $\mathbb{A}^{n+1} \rightarrow \mathbb{A}^n$ on to the first n coordinates maps U bijectively to \mathcal{X}_f , with inverse given by $x \mapsto (x, 1/f(x))$. Identifying \mathcal{X}_f with \mathcal{U} gives \mathcal{X}_f the structure of an affine variety with coordinate ring

$$\mathbb{F}[\mathcal{X}_f] = \mathbb{F}[\mathcal{X}][t_{n+1}]/\langle t_{n+1}f - 1 \rangle = \mathbb{F}[\mathcal{X}][1/f].$$

Example 2.41 Set $\mathbb{F}^\times := \mathbb{A}^1 - \{0\}$. If x is the coordinate function on \mathbb{A}^1 , then \mathbb{F}^\times is \mathbb{A}_x^1 , and the variety \mathcal{U} in (2.10) is the hyperbola $\mathcal{V}(xy - 1)$.

Example 2.42 The general linear group GL_n from Example 2.18 is the principal open subset of $\text{Mat}_{n \times n}$ defined by the non-vanishing of the determinant polynomial \det . By Definition 2.40, GL_n is an affine variety. Since the inverse of a matrix is given by its adjoint matrix divided by its determinant, and the entries of the adjoint matrix are polynomial functions of the entries of the original matrix, we see that the inverse map

$$M \mapsto M^{-1}$$

is a regular map on GL_n .

Definition 2.43 A *linear algebraic group* G is a subvariety of GL_n for some n which is closed under matrix multiplication and matrix inverse. More abstractly, an *algebraic group* is an algebraic variety whose multiplication and inverse maps are regular.

These two notions are related by a Theorem of Chevalley¹.

Theorem 2.44 *Every affine algebraic group is a linear algebraic group.*

Example 2.45 Both the general linear group and the special linear group $SL_n := \mathcal{V}(\det - 1) \subset \text{Mat}_{n \times n}$ are linear algebraic groups.

Let g^T be the transpose of a matrix $g \in \text{Mat}_{n \times n}$. Then for $M \in \text{Mat}_{n \times n}$,

$$G_M := \{g \in SL_n \mid gMg^T = M\}$$

is a linear algebraic group, as the condition $gMg^T = M$ is n^2 polynomial equations in the entries of g , and G_M is closed under matrix multiplication and matrix inversion.

When M is skew-symmetric and invertible, G_M is a *symplectic group*. In this case, n is necessarily even. If we let J_n denote the $n \times n$ matrix with ones on its anti-diagonal, then the matrix

$$\begin{bmatrix} 0 & J_n \\ -J_n & 0 \end{bmatrix}$$

is conjugate to every other invertible skew-symmetric matrix in $\text{Mat}_{2n \times 2n}$. We assume M is this matrix and write Sp_{2n} for the symplectic group.

When M is symmetric and invertible, G_M is a *special orthogonal group* $SO_n\mathbb{C}$. When K is algebraically closed, all invertible symmetric matrices are conjugate, and we may assume $M = J_n$. For general fields, there may be many different forms of the special orthogonal group. For instance, when $\mathbb{F} = \mathbb{R}$, let k and l be,

¹Is this Chevalley's?

respectively, the number of positive and negative eigenvalues of M (these are conjugation invariants of M). Then we obtain the group $SO_{k,l}\mathbb{R}$. We have $SO_{k,l}\mathbb{R} \simeq SO_{l,k}\mathbb{R}$.

Consider the two extreme cases. When $l = 0$, we may take $M = I_n$, and when $|k - l| \leq 1$, we take $M = J_n$. We will write $SO_{2n}\mathbb{F}$ and $SO_{2n+1}\mathbb{F}$ for the special orthogonal groups defined for $M = J_{2n}$ and $M = J_{2n+1}$.

When $\mathbb{F} = \mathbb{R}$, this differs from the standard convention that the real special orthogonal group is $SO_{n,0}\mathbb{R}$, which is compact in the Euclidean topology. Our reason for this deviation is that we want $SO_n\mathbb{R}$ to share more properties with $SO_n\mathbb{C}$. Our group $SO_n\mathbb{R}$ is often called the *split form* of the special linear group.

When $n = 2$, consider the two different real groups:

$$\begin{aligned} SO_{2,0}\mathbb{R} &:= \left\{ \left[\begin{array}{cc} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{array} \right] \mid \theta \in S^1 \right\} \\ SO_{1,1}\mathbb{R} &:= \left\{ \left[\begin{array}{cc} a & 0 \\ 0 & a^{-1} \end{array} \right] \mid a \in \mathbb{R}^\times \right\} \end{aligned}$$

Note that in the Euclidean topology $SO_{2,0}\mathbb{R}$ is compact, while $SO_{1,1}\mathbb{R}$ is not. The complex group $SO_2\mathbb{C}$ is also not compact in the Euclidean topology.

Let G be one of the groups $GL_n\mathbb{F}$, $SL_{n+1}\mathbb{F}$, $SO_{2n+1}\mathbb{F}$, $Sp_{2n}\mathbb{F}$, or $SO_{2n}\mathbb{F}$ defined here, considered as a subgroup of the obvious general linear group. Then the set of diagonal matrices in G is *maximal torus* T of G , and any subgroup of the form gTg^{-1} conjugate to T is also a maximal torus of G . Any maximal torus of these groups is isomorphic to $(\mathbb{F}^\times)^n$. The upper triangular matrices B (or B_+) in G form a *Borel subgroup* of G , and any subgroup conjugate to B is also a Borel subgroup. The lower triangular matrices in G form the Borel subgroup B_- opposite to B_+ . Those upper triangular matrices U with 1's on their diagonal form a *unipotent subgroup* of G .

Suppose \mathcal{X} is any irreducible affine variety. By Theorem 2.27, its ideal $\mathcal{I}(\mathcal{X})$ is prime, so its coordinate ring $\mathbb{F}[\mathcal{X}]$ has no zero divisors ($0 \neq f, g \in \mathbb{F}[\mathcal{X}]$ with $fg = 0$). A ring without divisors of zero is called an *integral domain*. In exact analogy with the construction of the rational numbers \mathbb{Q} as quotients of integers \mathbb{Z} , we form the *function field* $\mathbb{F}(\mathcal{X})$ of \mathcal{X} as the quotients of regular functions in $\mathbb{F}[\mathcal{X}]$. Formally, $\mathbb{F}(\mathcal{X})$ is the collection of all quotients f/g with $f, g \in \mathbb{F}[\mathcal{X}]$ and $g \neq 0$, where we identify

$$\frac{f_1}{g_1} = \frac{f_2}{g_2} \iff f_1g_2 - f_2g_1 = 0 \text{ in } \mathbb{F}[\mathcal{X}].$$

Example 2.46 The function field of affine space \mathbb{A}^n is the collection of quotients of polynomials P/Q with $P, Q \in \mathbb{F}[t_1, \dots, t_n]$. This field $\mathbb{F}(t_1, \dots, t_n)$ is called the *field of rational functions* in the variables t_1, \dots, t_n .

Given an irreducible affine variety $\mathcal{X} \subset \mathbb{A}^n$, we may also express $\mathbb{F}(\mathcal{X})$ as the collection of quotients f/g of polynomials $f, g \in \mathbb{F}[\mathbb{A}^n]$ with $g \notin \mathcal{I}(\mathcal{X})$, where we identify

$$\frac{f_1}{g_1} = \frac{f_2}{g_2} \iff f_1g_2 - f_2g_1 \in \mathcal{I}(\mathcal{X}).$$

Rational functions on an affine variety \mathcal{X} do not in general have unique representatives as quotients of polynomials or even regular functions.

Example 2.47 Let $\mathcal{X} := \mathcal{V}(x^2 + y^2 + 2y) \subset \mathbb{A}^2$ be the circle of radius 1 and center at $(0, -1)$. In $\mathbb{F}(\mathcal{X})$ we have

$$-\frac{x}{y} = \frac{y^2 + 2y}{x}.$$

A point $x \in \mathcal{X}$ is a *regular point* of a rational function $\varphi \in \mathbb{F}(\mathcal{X})$ if φ has a representative f/g with $f, g \in \mathbb{F}[\mathcal{X}]$ and $g(x) \neq 0$. From this we see that all points of the neighborhood \mathcal{X}_g of x in \mathcal{X} are regular points of φ . Thus the set of regular points of φ , which we call the *domain of regularity* of φ , is a nonempty Zariski open subset of \mathcal{X} .

When $x \in \mathcal{X}$ is a regular point of a rational function $\varphi \in \mathbb{F}(\mathcal{X})$, we set $\varphi(x) := f(x)/g(x) \in \mathbb{F}$, where φ has representative f/g with $g(x) \neq 0$. The value of $\varphi(x)$ does not depend upon the choice of representative f/g of φ . In this way, φ gives a function from a dense subset of \mathcal{X} (its domain of regularity) to \mathbb{F} . We write this as

$$\varphi : \mathcal{X} \dashrightarrow \mathbb{F}$$

with the dashed arrow indicating that φ is not necessarily defined at all points of \mathcal{X} .

The rational function φ of Example 2.47 has domain of regularity $\mathcal{X} - \{(0, 1)\}$. Here $\varphi : \mathcal{X} \dashrightarrow \mathbb{F}$ is stereographic projection of the circle onto the line $y = -1$ from the point $(0, 0)$. (See Figure 4.1.)

Example 2.48 Let $\mathcal{X} = \mathbb{A}_{\mathbb{R}}^1$ and $\varphi = 1/(1 + x^2) \in \mathbb{R}(\mathcal{X})$. Then every point of \mathcal{X} is a regular point of φ . The existence of rational functions which are regular at every point, but are not elements of the coordinate ring is a special feature of real algebraic geometry. Observe that φ is not regular at the points $\pm\sqrt{-1} \in \mathbb{A}_{\mathbb{C}}^1$.

Theorem 2.49 *When \mathbb{F} is algebraically closed, a rational function that is regular at all points of an irreducible affine variety \mathcal{X} is a regular function in $\mathbb{C}[\mathcal{X}]$.*

Proof: For each point $x \in \mathcal{X}$, there are regular functions $f_x, g_x \in \mathbb{F}[\mathcal{X}]$ with $\varphi = f_x/g_x$ and $g_x(x) \neq 0$. Let \mathcal{I} be the ideal generated by the regular functions g_x for $x \in \mathcal{X}$. Then $\mathcal{V}(\mathcal{I}) = \emptyset$, as φ is regular at all points of \mathcal{X} .

If we let g_1, \dots, g_s be generators of \mathcal{I} and let f_1, \dots, f_s be regular functions such that $\varphi = f_i/g_i$ for each i . Then by the Weak Nullstellensatz for \mathcal{X} (Theorem 2.33(3)), there are regular functions $h_1, \dots, h_s \in \mathbb{C}[\mathcal{X}]$ such that

$$1 = h_1g_1 + \dots + h_s g_s.$$

multiplying this equation by φ , we obtain

$$\varphi = h_1f_1 + \dots + h_s f_s,$$

which proves the theorem. □

A list f_1, \dots, f_m of rational functions gives a *rational map*

$$\begin{aligned} \varphi : \mathcal{X} &\dashrightarrow \mathbb{A}^m, \\ x &\longmapsto (f_1(x), \dots, f_m(x)). \end{aligned}$$

This rational map φ is only defined on the intersection \mathcal{U} of the domains of regularity of each of the f_i . We call \mathcal{U} the *domain of φ* and write $\varphi(\mathcal{X})$ for $\varphi(\mathcal{U})$.

Let \mathcal{X} be an irreducible affine variety. Since $\mathbb{F}[\mathcal{X}] \subset \mathbb{F}(\mathcal{X})$, any regular map is also a rational map. As with regular maps, a rational map $\varphi : \mathcal{X} \dashrightarrow \mathbb{A}^m$ given by functions $f_1, \dots, f_m \in \mathbb{F}(\mathcal{X})$ defines a homomorphism $\varphi^* : \mathbb{F}[\mathbb{A}^m] \rightarrow \mathbb{F}(\mathcal{X})$ by $\varphi^*(g) = g(f_1, \dots, f_m)$. If \mathcal{Y} is an affine subvariety of \mathbb{A}^m , then $\varphi(\mathcal{X}) \subset \mathcal{Y}$ if and only if $\varphi(\mathcal{I}(\mathcal{Y})) = 0$. In particular, the kernel \mathcal{J} of the map $\varphi^* : \mathbb{F}[\mathbb{A}^m] \rightarrow \mathbb{F}(\mathcal{X})$ defines the smallest subvariety $Y = \mathcal{V}(\mathcal{J})$ containing $\varphi(\mathcal{X})$, that is, the Zariski closure of $\varphi(\mathcal{X})$. Since $\mathbb{F}(\mathcal{X})$ is a field, this kernel is a prime ideal, and so \mathcal{Y} is irreducible.

When $\varphi : \mathcal{X} \dashrightarrow \mathcal{Y}$ is a rational map with $\varphi(\mathcal{X})$ dense in \mathcal{Y} , then we say that φ is *dominant*. A dominant rational map $\varphi : \mathcal{X} \dashrightarrow \mathcal{Y}$ induces an embedding $\varphi^* : \mathbb{F}[\mathcal{Y}] \hookrightarrow \mathbb{F}(\mathcal{X})$. Since \mathcal{Y} is irreducible, this map extends to a map of function fields $\varphi^* : \mathbb{F}(\mathcal{Y}) \rightarrow \mathbb{F}(\mathcal{X})$. Conversely, given a map $\psi : \mathbb{F}(\mathcal{Y}) \rightarrow \mathbb{F}(\mathcal{X})$ of function fields, with $\mathcal{Y} \subset \mathbb{A}^m$, we obtain a dominant rational map $\varphi : \mathcal{X} \dashrightarrow \mathcal{Y}$ given by the rational functions $\psi(t_1), \dots, \psi(t_m) \in \mathbb{F}(\mathcal{X})$ where t_1, \dots, t_m are the coordinate functions on $\mathcal{Y} \subset \mathbb{A}^m$.

Suppose we have two rational maps $\varphi : \mathcal{X} \dashrightarrow \mathcal{Y}$ and $\psi : \mathcal{Y} \dashrightarrow \mathcal{Z}$ with φ dominant. Then $\varphi(\mathcal{X})$ intersects the set of regular points of ψ , and so we may compose these maps $\psi \circ \varphi : \mathcal{X} \dashrightarrow \mathcal{Z}$. Two irreducible affine varieties \mathcal{X} and \mathcal{Y} are *birationally equivalent* if there is a rational map $\varphi : \mathcal{X} \dashrightarrow \mathcal{Y}$ with a rational inverse $\psi : \mathcal{Y} \dashrightarrow \mathcal{X}$. By this we mean that the compositions $\varphi \circ \psi$ and $\psi \circ \varphi$ are the identity maps on their respective domains. Equivalently, \mathcal{X} and \mathcal{Y} are birationally equivalent if and only if their function fields are isomorphic, if and only if they have isomorphic open subsets.

Exercise 2.2 Show that if two varieties \mathcal{X} and \mathcal{Y} are isomorphic, then they are homeomorphic as topological spaces. Show that the converse does not hold.

Exercise 2.3 Prove the Hilbert Theorems (Theorem 2.33) for an affine variety \mathcal{X} .

Exercise 2.4 Prove that a regular map $\varphi : \mathcal{X} \rightarrow \mathcal{Y}$ between affine varieties \mathcal{X} and \mathcal{Y} is continuous in the Zariski topology.

Exercise 2.5 Show that the bijection $\varphi : t \mapsto (t^2, t^3)$ from \mathbb{A}^1 to the cuspidal cubic $(y^2 - x^3)$ is not an isomorphism of affine varieties.

Exercise 2.6 Let $M \in \text{Mat}_{n \times n}$. Prove that the subvariety $G_M \subset \text{Mat}_{n \times n}$ defined by

$$G_M := \{g \in SL_n \mid gMg^T = M\}$$

is a linear algebraic group.

Exercise 2.7 Let $M \in \text{Mat}_{2n \times 2n} \mathbb{F}$ be a skew symmetric matrix. Show that M is conjugate to the matrix

$$\begin{bmatrix} 0 & J_n \\ -J_n & 0 \end{bmatrix}$$

where J_n is the $n \times n$ matrix with ones on its anti-diagonal.

Exercise 2.8 Show that irreducible affine varieties \mathcal{X} and \mathcal{Y} are birationally equivalent if and only if they have isomorphic open sets.

2.5 Smooth and Singular Points, Dimension

Some of the algebraic varieties we have seen, particularly in Examples 2.2 and 2.24, have singularities—points which do not have a neighborhood that is a manifold. We develop the tools and language to treat this common phenomenon in algebraic geometry.

Given a polynomial $f \in \mathbb{F}[t_1, \dots, t_n]$ and a point $x = (x_1, \dots, x_n) \in \mathbb{A}^n$, we can make a linear change of variables and write f as a polynomial in new variables $\xi := t - x$. This gives the Taylor expansion of f at the point x :

$$f = f(x) + \sum_{i=1}^n \frac{\partial f}{\partial t_i} (t_i - x_i) + \cdots ,$$

where the remaining terms are homogeneous with degree greater than 1 in the differences $\xi_i = (t_i - x_i)$. When the characteristic of \mathbb{F} is zero, this is the usual Taylor expansion of multivariate calculus where the coefficient of the monomial $\xi^{\mathbf{i}} = \xi_1^{i_1} \xi_2^{i_2} \cdots \xi_n^{i_n}$ is the mixed partial derivative of f :

$$\frac{1}{i_1! i_2! \cdots i_n!} \left(\frac{\partial}{\partial t_1} \right)^{i_1} \left(\frac{\partial}{\partial t_2} \right)^{i_2} \cdots \left(\frac{\partial}{\partial t_n} \right)^{i_n} f .$$

If we use ξ as coordinates for \mathbb{F}^n , then the linear term in the Taylor expansion is a linear map $d_x f: \mathbb{F}^n \rightarrow \mathbb{F}$ called the *differential* of f at the point x .

Definition 2.50 Let $\mathcal{X} \subset \mathbb{A}^n$ be a subvariety with $\mathcal{I} = \mathcal{I}(\mathcal{X})$. The (*Zariski*) *tangent space* $T_x \mathcal{X}$ to \mathcal{X} at a point $x \in X$ is the joint kernel of the linear maps $\{d_x f \mid f \in \mathcal{I}\}$. Since we have

$$\begin{aligned} d_x(f + g) &= d_x f + d_x g & \text{and} \\ d_x(fg) &= f(x)d_x g + g(x)d_x f , \end{aligned}$$

only a finite generating set for the ideal \mathcal{I} is needed to define $T_x \mathcal{X}$ at all points $x \in \mathcal{X}$.

Example 2.51 Consider the polynomials $f = y^2 - x^3$, $g = y^2 - x^3 - x^2$, and $h = y^2 - x^3 + x$ which define (respectively) the cuspidal cubic, nodal cubic, and elliptic curve of Example 2.2. Their differentials are

$$\begin{aligned} d_{(x,y)} f &= \langle -3x^2, 2y \rangle , \\ d_{(x,y)} g &= \langle -3x^2 - 2x, 2y \rangle , & \text{and} \\ d_{(x,y)} h &= \langle -3x^2 + 1, 2y \rangle . \end{aligned}$$

We see that $d_{(x,y)} f$ vanishes only at the origin, which is on the cuspidal cubic. Similarly, $d_{(x,y)} g$ vanishes at the origin and at the point $(-2/3, 0)$, and of these only the origin is on the nodal cubic. Thus the tangent spaces of both the cuspidal and nodal cubics have dimension 1 at all points except at the origin, where they have dimension 2. The elliptic curve in contrast has all of its tangent spaces one-dimensional, as $d_{(x,y)} h$ vanishes only at the points $(\pm 1/\sqrt{3}, 0)$, which are not on the elliptic curve.

Example 2.52 The special linear group SL_n has all of its Zariski tangent spaces isomorphic to \mathbb{F}^{n^2-1} . Indeed, $SL_n = \mathcal{V}(\det - 1)$, and the partial derivative

$$\frac{\partial \det}{\partial x_{i,j}}$$

is the cofactor of $x_{i,j}$ ($(-1)^{i+j}$ times the determinant of the $(n-1) \times (n-1)$ matrix obtained by deleting the i th row and j th column). Thus $d_x \det = 0$ only when all such cofactors vanish, but the vanishing of all cofactors implies that $\det = 0$, which does not occur at any point of SL_n .

Theorem 2.53 *Let \mathcal{X} be an affine variety. Then there exists a (non-empty) open subset of \mathcal{X} consisting of the points of \mathcal{X} whose tangent space has minimal dimension.*

Proof: Let f_1, \dots, f_s be generators of $\mathcal{I}(\mathcal{X})$. Let $M \in \text{Mat}_{s \times n}(\mathbb{F}[\mathbb{A}^n])$ be the matrix whose entry in row i and column j is $\partial f_i / \partial t_j$, which is a polynomial in $\mathbb{F}[\mathbb{A}^n]$. Then, for $\xi \in \mathbb{F}^n$ and $x \in \mathbb{A}^n$, $M(x)\xi$ is the s -tuple of the differentials of f_1, \dots, f_s . Thus when $x \in \mathcal{X}$, the Zariski tangent space $T_x \mathcal{X}$ is the kernel of the matrix $(M(x))$.

For each number $l = 1, 2, \dots, \min\{s, n\}$, define the *degeneracy locus* $\Delta_l \subset \mathbb{A}^n$ to be the variety defined by the collection of all $l \times l$ minors of the matrix M , and set $\Delta_l := \mathbb{A}^n$ if l is greater than $\min\{s, n\}$. Then we have

$$\Delta_1 \subset \Delta_2 \subset \dots \subset \Delta_{\min\{s, n\}} \subset \mathbb{A}^n = \Delta_{1+\min\{s, n\}}.$$

On the set $\Delta_{i+1} - \Delta_i$, the matrix $M(x)$ has constant rank i . Thus if $x \in \Delta_{i+1} - \Delta_i$, the kernel of $M(x)$ has dimension $n - i$. Let i be the minimal index with $X \subset \Delta_{i+1}$. Then $X - \Delta_i = \{x \in X \mid \dim T_x \mathcal{X} = n - i\}$ is open in \mathcal{X} , and $n - i$ is the minimum dimension of a tangent space to \mathcal{X} . \square

A subset $X \subset \mathbb{A}^n$ is *locally closed* if \mathcal{X} is a Zariski open subset of the closure \overline{X} of \mathcal{X} in \mathbb{A}^n . In the proof of Theorem 2.53, we showed the following.

Theorem 2.54 *Let \mathcal{X} be an affine variety. For each number k , the set of points $x \in X$ such that $\dim_{\mathbb{F}} T_x \mathcal{X} = k$ is locally closed.*

Definition 2.55 A point x of a variety \mathcal{X} is *smooth* if it has an open neighborhood $\mathcal{U} \subset \mathcal{X}$ such that $\dim_{\mathbb{F}} T_y \mathcal{X}$ is minimized on \mathcal{U} when $y = x$. Points of \mathcal{X} where $\dim_{\mathbb{F}} T_x \mathcal{X}$ is not locally minimal are called *singular*. Let \mathcal{X}'_{sm} be the open subset of \mathcal{X} consisting of its smooth points and X'_{sing} be its closed subset of singular points. Thus the cuspidal and nodal cubics are singular only at the origin, while the elliptic curve and special linear group SL_n are smooth varieties.

We make the definition of tangent spaces intrinsic so that it becomes functorial under maps of algebraic varieties. To that end, let \mathcal{X} be an affine variety and $I = \mathcal{I}(\mathcal{X})$. Let $x \in \mathcal{X}$ and consider a regular function $f \in \mathbb{F}[\mathcal{X}]$. If we define $d_x f = d_x F$, where $F \in \mathbb{F}[\mathbb{A}^n]$ is any polynomial representing f , then $d_x f$ is only defined modulo the subspace $\{d_x G \mid G \in I\}$ of differentials of polynomials in the ideal of \mathcal{X} . Thus $d_x f$

is a well-defined linear map on the common kernel of the differentials $\{d_x G \mid G \in I\}$, in other words, $d_x f$ is a linear map on the tangent space $T_x \mathcal{X}$ to \mathcal{X} at x .

Thus we have a linear map $d_x: \mathbb{F}[\mathcal{X}] \rightarrow T_x \mathcal{X}^*$, the space of linear maps on $T_x \mathcal{X}$. Since $d_x \alpha = 0$ for $\alpha \in \mathbb{F}$ a constant, $d_x f = d_x(f - f(x))$, and so it suffices to consider the restriction of d_x to the *maximal ideal* of functions vanishing at x , $\mathfrak{m}_{\mathcal{X},x}$ or \mathfrak{m}_x to be $\{f \in \mathbb{F}[\mathcal{X}] \mid f(x) = 0\}$. Observe that the inclusion $\mathcal{X} \subset \mathbb{A}^n$ induces the restriction $\mathfrak{m}_{\mathbb{A}^n,x} \rightarrow \mathfrak{m}_{\mathcal{X},x}$.

Theorem 2.56 *The map d_x defines an isomorphism of the vector spaces $\mathfrak{m}_x/\mathfrak{m}_x^2$ and $T_x \mathcal{X}^*$.*

Proof: To see that d_x is surjective, observe that the differential of any linear map is that linear map. Since $T_x \mathcal{X}$ is a linear subspace of \mathbb{F}^n , the restriction of linear maps on \mathbb{F}^n to $T_x \mathcal{X}$ gives all linear maps on $T_x \mathcal{X}$. But this restriction factors through the composition of the quotient map $\mathbb{F}[\mathbb{A}^n] \rightarrow \mathbb{F}[\mathcal{X}]$ with the differential d_x .

Suppose now that $f \in \mathfrak{m}_x$ satisfies $d_x f = 0$. Let F be any polynomial representative of f . Since the linear map $d_x F$ vanishes on $T_x \mathcal{X}$ it equals $d_x G$ for some $G \in I$. If we set $H = F - G$, then $d_x H = 0$ as a linear map on \mathbb{A}^n , and so the Taylor expansion of H has no constant or linear terms. But this says that $H \in \mathfrak{m}_{\mathbb{A}^n,x}^2$, the square of the maximal ideal of x in $\mathbb{F}[\mathbb{A}^n]$. Since H is another polynomial representative of f , we conclude that $f \in \mathfrak{m}_x^2$ in $\mathbb{F}[\mathcal{X}]$. \square

Henceforth, we will define the tangent space $T_x \mathcal{X}$ at a point x of an algebraic variety \mathcal{X} to be $(\mathfrak{m}_x/\mathfrak{m}_x^2)^*$, where \mathfrak{m}_x is the maximal ideal in the coordinate ring of \mathcal{X} of functions vanishing at x . This intrinsic definition is functorial: A map $\varphi: \mathcal{X} \rightarrow \mathcal{Y}$ induces maps $d_x \varphi: T_x \mathcal{X} \rightarrow T_{\varphi(x)} \mathcal{Y}$ and if we have $\psi: \mathcal{Y} \rightarrow \mathcal{Z}$ as well, then the composite map $T_x \mathcal{X} \rightarrow T_{\varphi(x)} \mathcal{Y} \rightarrow T_{\psi(\varphi(x))} \mathcal{Z}$ is the composition of $d_x \varphi$ and $d_{\psi(\varphi(x))} \psi$.

To see this, let $\varphi: \mathcal{X} \rightarrow \mathcal{Y} \subset \mathbb{A}^m$ be a map of affine varieties given by the functions $f_1, \dots, f_m \in k[\mathcal{X}]$. Then the map $\varphi^*: k[\mathcal{Y}] \rightarrow k[\mathcal{X}]$ is given by $g \mapsto g(f_1, \dots, f_m)$. Let $x \in \mathcal{X}$ and $g \in \mathfrak{m}_{\varphi(x)}$. Then $\varphi^* g(x) = g(\varphi(x)) = 0$, and so we see that $\varphi^*: \mathfrak{m}_{\varphi(x)} \rightarrow \mathfrak{m}_x$, and also $\varphi^*: \mathfrak{m}_{\varphi(x)}^2 \rightarrow \mathfrak{m}_x^2$. Thus the map

$$\mathfrak{m}_{\varphi(x)} \longrightarrow \mathfrak{m}_x \longrightarrow \mathfrak{m}_x/\mathfrak{m}_x^2$$

factors through the quotient $\mathfrak{m}_{\varphi(x)}/\mathfrak{m}_{\varphi(x)}^2$. Dualizing, we obtain the map $d_x \varphi: T_x \mathcal{X} \rightarrow T_{\varphi(x)} \mathcal{Y}$. The functoriality of $d_x \varphi$ follows from the functoriality of the maps φ^* .

This functoriality has an immediate consequence: If $\varphi: \mathcal{X} \simeq \mathcal{Y}$ is an isomorphism, then $d_x \varphi$ is an isomorphism for every $x \in \mathcal{X}$. In particular, we have the following.

Theorem 2.57 *Algebraic groups are smooth.*

Proof: Let G be an algebraic group and $g \in G$. Left multiplication by g , $\lambda_g: G \rightarrow G$, which is the map $h \mapsto gh$, is an isomorphism of the variety G . Thus we have

$$d_e \lambda_g: T_e G \xrightarrow{\sim} T_g G.$$

Sine all tangent spaces of G are isomorphic, G is smooth. \square

We generalize this Theorem to group actions on varieties. Let G be an algebraic group and \mathcal{X} a variety. A (left) action of G on \mathcal{X} is a map $\varphi: G \times \mathcal{X} \rightarrow \mathcal{X}$ which we write as $(g, x) \mapsto g.x$, and which satisfies $e.x = x$ and $h.(g.x) = hg.x$ for all $g, h \in G$ and $x \in \mathcal{X}$. The map $x \mapsto g.x$ is written $\varphi_g: \mathcal{X} \rightarrow \mathcal{X}$ and we have that φ_e is the identity map on \mathcal{X} and $\varphi_h(\varphi_g) = \varphi_{hg}$. Since $\varphi_{g^{-1}}(\varphi_g) = \varphi_e$, each map φ_g is an isomorphism of \mathcal{X} . An *orbit* of G is the set $G.x$ of all translates of a single point $x \in \mathcal{X}$.

Theorem 2.58 (Equisingularity of orbits) *Let \mathcal{X} be an affine variety equipped with the action of an algebraic group G . The tangent spaces at any two points of a G -orbit are isomorphic. Furthermore, each orbit of G in \mathcal{X} is a smooth, locally closed subset of \mathcal{X} whose boundary is a union of orbits of strictly smaller dimension. In particular, minimal orbits are closed.*

Proof: Let $x \in \mathcal{X}$, then since $d_x\varphi_g T_x\mathcal{X} \simeq T_{g.x}\mathcal{X}$, we see that the any two points of a G -orbit are isomorphic. Let $Y = G.x$, the orbit of x in \mathcal{X} . Since \mathcal{Y} is dense in $\overline{\mathcal{Y}}$, it meets the open subset $(\overline{\mathcal{Y}})_{sm}$ of smooth points of \mathcal{Y} . Since all tangent spaces $T_y\mathcal{Y}$ have the same dimension, from which it follows that all points of \mathcal{Y} are smooth points in $\overline{\mathcal{Y}}$.

We have that \mathcal{Y} is the image of the map $G \rightarrow \overline{\mathcal{Y}}$ given by $g \mapsto g.y$, and so \mathcal{Y} is constructible.² Let \mathcal{U} be an open subset of $\overline{\mathcal{Y}}$ contained in \mathcal{Y} . Since $G\mathcal{U} = \mathcal{Y}$, we see that \mathcal{Y} is a union of open subsets, and so is open in $\overline{\mathcal{Y}}$ and thus locally closed.

Finally, \mathcal{Y} , and hence $\overline{\mathcal{Y}}$ are G -stable, and so $\overline{\mathcal{Y}} - \mathcal{Y}$ is closed and G -stable, and has lower dimension than \mathcal{Y} , as \mathcal{Y} is dense in $\overline{\mathcal{Y}}$. Thus it is a union of G -orbits. \square

Example 2.59 We illustrate this Theorem. Consider the following group action of the multiplicative group \mathbb{F}^\times of a field on \mathbb{A}^2 given by $t.(x, y) = (t^2x, t^3y)$. The orbits of this action are the origin, $(0, 0)$, each coordinate axis with the origin removed, and the cuspidal cubics $\mathcal{V}(a^3y^2 - b^2x^3)$ with the origin removed. This last type of orbit consists of the smooth points of the cubic.

We use this work to define the dimension of an affine variety.

Definition 2.60 If \mathcal{X} is irreducible, then the *dimension* of \mathcal{X} is the dimension of the Zariski tangent space $T_x\mathcal{X}$ at any smooth point x of \mathcal{X} . If \mathcal{X} is reducible then the dimension of \mathcal{X} is the maximum dimension of its irreducible components.

Example 2.61 The dimension of \mathbb{A}^n is n . The dimension of the cubic curves of Examples 2.2 and 2.51 are 1. The dimension of the special linear group SL_n is $n^2 - 1$.

We call an algebraic variety, all of whose components have dimension 1 a *curve*. A *surface* is an algebraic variety where each component has dimension 2.

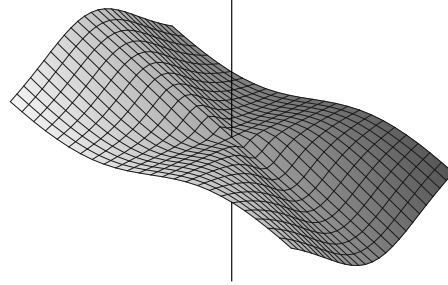
Remark 2.62 When \mathbb{F} is the real or complex numbers, and \mathcal{X} is an affine variety, then the smooth points of \mathcal{X} are precisely those points where \mathcal{X} is a manifold. Furthermore, when \mathcal{X} is smooth at a point x , the Zariski tangent space coincides with the usual tangent space of \mathcal{X} at x , as given in differential geometry. As a consequence, when \mathcal{X} is irreducible the dimension of \mathcal{X}_{sm} as a manifold agrees with its dimension as an algebraic variety.

²Define constructible sets somewhere!

We have the following facts concerning the locus of smooth and singular points on a real or complex variety

Proposition 2.63 *The set of smooth points of an irreducible complex affine subvariety \mathcal{X} of dimension d whose complex local dimension in the Euclidean topology is d is dense in the Euclidean topology.*

Example 2.64 Irreducible real algebraic varieties need not have this property. The Cartan umbrella $\mathcal{V}(z(x^2 + y^2) - x^3)$:



is a connected irreducible surface in $\mathbb{A}_{\mathbb{R}}^3$ where the local dimension of its smooth points is either 1 (along the z axis) or 2 (along the ‘canopy’ of the umbrella).

There are a number of equivalent definitions of dimension. One particularly algebraic definition is the following:

$$\dim \mathcal{X} := \max\{f_1, \dots, f_n \in \mathbb{F}[\mathcal{X}] \mid f_1, \dots, f_n \text{ are algebraically independent}\}.$$

When \mathcal{X} is irreducible, this is the transcendence degree of the function field $\mathbb{F}(\mathcal{X})$ of \mathcal{X} . The equivalence of this definition with our first definition is proven in ??????

Theorem 2.65 *Suppose \mathcal{Y} is a closed subset of \mathcal{X} . Then $\dim \mathcal{Y} \leq \dim \mathcal{X}$. If \mathcal{X} is irreducible and $\dim \mathcal{Y} = \dim \mathcal{X}$, then $\mathcal{Y} = \mathcal{X}$.*

Proof: For the first statement, suppose $\dim \mathcal{X} = n$. Given $n + 1$ functions in $\mathbb{F}[\mathcal{Y}]$, lift them to $\mathbb{F}[\mathcal{X}]$. Then they are algebraically dependent, and this dependence drops to $\mathbb{F}[\mathcal{Y}]$.

For the second statement, suppose $\dim \mathcal{X} = \dim \mathcal{Y} = n$. Let $f_1, \dots, f_n \in \mathbb{F}[\mathcal{Y}]$ be algebraically independent. Then any lifts to $\mathbb{F}[\mathcal{X}]$, also denoted f_1, \dots, f_n , are also independent. For $t \in \mathbb{F}[\mathcal{X}]$, there is a polynomial $a(X, T) \in \mathbb{F}[X_1, \dots, X_n][T]$ such that $a(f, t) = 0$ in $\mathbb{F}[\mathcal{X}]$, and so

$$a(f, t) = a_0(f_1, \dots, f_n)t^l + \dots + a_l(f_1, \dots, f_n) = 0. \quad (2.11)$$

Suppose further that we have chosen the polynomial $a(X, T)$ to be irreducible with this property (which we may do as $\mathbb{F}[\mathcal{X}]$ is a domain).

Suppose t vanishes on \mathcal{Y} . Since (2.11) holds on \mathcal{Y} , we have that $a_l(f_1, \dots, f_n) = 0$ in $\mathbb{F}[\mathcal{Y}]$. Since f_1, \dots, f_n are algebraically independent, we see that $a_l(X) = 0$ as a polynomial, which contradicts the irreducibility of $a(X, T)$. \square

The second statement can be strengthened as follows:

Theorem 2.66 *If \mathcal{X} is irreducible and has dimension n , and $f \in \mathbb{F}[\mathcal{X}]$ is non-zero, then every irreducible component of $\mathcal{V}(f)$ has dimension $n - 1$.*

We give a proof later, when we do Noether Normalization.

A consequence of this is the combinatorial definition of dimension. The dimension of a variety \mathcal{X} is the largest number n for which there exists a chain of irreducible subvarieties of \mathcal{X} .

$$\mathcal{X}_0 \subsetneq \mathcal{X}_1 \subsetneq \mathcal{X}_2 \subsetneq \cdots \subsetneq \mathcal{X}_n \subset \mathcal{X},$$

Exercise 2.9 Let \mathcal{X} be an affine variety. Show that $\mathfrak{m}_{\mathcal{X},x} = \{f \in \mathbb{F}[\mathcal{X}] \mid f(x) = 0\}$ is a maximal ideal of the coordinate ring of \mathcal{X} .

Exercise 2.10 Give another proof that \mathbb{A}^1 and the cuspidal cubic are not isomorphic using their tangent spaces.