Chapter 1
Varieties: An Introduction

In this chapter, we will look at one of the basic objects of study in algebraic geometry: algebraic varieties defined over an algebraically closed field.

Section 1.1 Curves

We start with a naive definition.

Definition 1.1.1. A curve over a field k is the set of zeros in $k \times k$ of a single polynomial equation in two variables, $f(x, y) = 0$.

Examples. Let $k = \mathbf{R}$ and consider the following curves. (Here we should insert the graphs of the following curves.)

(i) $y = 0$.
(ii) $y^2 = 0$.
(iii) $xy = 1$.
(iv) $x^2 + y^2 = 1$.
(v) $x^2 + y^2 = 0$.
(vi) $x^2 + y^2 = -1$.
(vii) $y^2 = x^3$.
(viii) $y^2 = x^3 + x^2$.
(ix) $y^2 = x^3 - x$.
(x) $x^2 - y^2 = 0$.
(xi) $(y - x)(y - x + 1) = 0$.
(xii) $x^3 + y^3 = 1$.

These examples raise several important questions about the naive definition. For example

(A) Are (i) and (ii) the same or different curves?
(B) Should (v) and (vi) even be called curves at all?
(C) Why are (iii), (ix) and (xi) disconnected?
(D) What's special about (vii), (viii), and (x)?

The questions are of two kinds. The first two questions are metaphysical; they ask if we have the correct definition. The final two questions are analytic; they begin to study the intrinsic geometry of curves.

To elaborate on question (A), consider the families of curves (Pictures again need to be inserted.)

(i) $y = ax$.
(ii) $y^2 = ax$.

Intersect each family of curves with the line $x = 1$. When $a \neq 0$, curves in the first family intersect the line in exactly one point, but curves in the second family intersect in two points. As the parameter $a \mapsto 0$, the limiting curve of the first family is curve (i), and it still intersects in one point. However, the limiting curve in the second family is curve (ii), and the two points of intersection coalesce in the limit. Should the limit curve intersect the line in one point, or in two points "properly counted"?

Regarding question (B), there are two schools of thought (which will be described shortly). In either case, the following theorem shows that the underlying difficulty is that $\mathbf{R}$ is not algebraically closed.

Theorem 1.1.2: *Let k be an algebraically closed field and let $f \in k[x, y]$ be a nonconstant polynomial. Then there are infinitely many solutions to $f(x, y) = 0$.*

Proof: Write $f(x, y) = a_0(y) + a_1(y)x + \cdots + a_n(y)x^n$, with $a_n(y) \neq 0$, as a polynomial of degree n in x with coefficients from $k[y]$. If $n = 0$, then we simply have $f(x, y) = a_0(y)$, a nonconstant polynomial in one variable. Since k is algebraically closed, this polynomial has a root y_0. Then all of the infinitely many pairs (x, y_0) as x ranges over the (infinite) algebraically closed field k provide solutions to $f(x, y) = 0$.

So, suppose $n > 0$. Then $a_n(y) = 0$ has only finitely many solutions. There are infinitely many points y_0 where $a_n(y_0) \neq 0$; at each one of them, we get a polynomial $f(x, y_0)$ of degree n in the single variable x. This polynomial has a solution x_0, yielding infinitely many points (x_0, y_0) where $f(x, y) = 0$. ∎

Remark 1.1.3. The proof also shows that all but finitely many vertical lines hit the curve in exactly n points, properly counted.

The restrictive school of thought says that you can avoid the difficulties posed by examples (v) and (vi) by considering only algebraically closed fields. This seems to be rather narrow-minded, since it foregoes any chance of applying geometric techniques to some interesting problems that arise in number theory. A more open-minded approach is to "fix" the naive definition to make it useful over arbitrary fields. Nevertheless, we will acquiesce (at least temporarily), and work over algebraically closed fields for the remainder of this chapter.

Definition 1.1.4. As a set, affine n-space over a field k is defined to be the Cartesian product

$$\mathbf{A}_k^n = k \times k \times \cdots \times k$$

of k with itself n times.

Definition 1.1.5. Let k be algebraically closed. An *affine algebraic set* over k is the set of common zeros in $\mathbf{A}_k^n$ of some set of polynomials $S \subset k[x_1, \ldots, x_n]$. Given such a set S, its algebraic set of zeros will be denoted $Z(S)$.

Remark 1.1.6. If I is the ideal generated by S, then it is easy to see that $Z(I) = Z(S)$.

Definition 1.1.7. The *Zariski topology* on $\mathbf{A}^n$ is defined by taking the closed sets to be the algebraic sets. The Zariski toplogy on an algebraic set is defined as the topology induced from its embedding in $\mathbf{A}^n$.

Remark 1.1.8. The algebraic sets really do form the closed sets of a topology, but it does not fully reflect the structure of affine space. For instance, the topological space $\mathbf{A}^2$ is not the same thing as the space $\mathbf{A}^1 \times \mathbf{A}^1$ with the product topology.

Section 1.2 Hilbert's Theorems

The previous section contained a defintion of an algebraic set as the locus defined by an ideal. The first result of this section is a crucial finiteness result.

Theorem 1.2.1: *(Hilbert's Basis Theorem) If k is a field, then every ideal in the polynomial ring $k[x_1, \ldots, x_n]$ is finitely generated.*

Proof: The proof will proceed by induction on the number of variables. Since we know that $k[x_1]$ is a Euclidean domain, hence a principal ideal domain, we know the result with only one variable. (In this case, each ideal is generated by just one element.) The induction step is made more managable by introducing the following definition. (Notice that the definition contains within itself the statement of a proposition, that its two parts are equivalent. This proposition is left as an exercise.) ∎

Definition 1.2.2. A commutative ring R with 1 is called *noetherian* if one of the following equivalent conditions holds.

(a) Every ideal in R is finitely generated.
(b) Every ascending chain of ideals in R terminates.

Now the Hilbert Basis Theorem will follow from the following more general result.

Theorem 1.2.3: *If R is a noetherian ring, then so is the polynomial ring $R[x]$.*

Proof: We will actually prove the contrapositive. So, assume that $R[x]$ is not noetherian. Let I be an ideal in R that is not finitely generated. Choose an element $f_1 \in I$ of minimal positive degree. Inductively, we can choose elements $f_{k+1} \in I \backslash (f_1, \ldots, f_k)$ that have minimal positive degree. Let n_k denote the degree of f_k, and let a_k denote its leading coefficient. Observe first that

$$n_1 \leq n_2 \leq n_3 \leq \cdots.$$

Now consider the chain of ideals

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \cdots$$

contained in R. This chain of ideals cannot be stationary. For, suppose that $(a_1, \ldots, a_k) = (a_1, \ldots, a_k, a_{k+1})$. Then we can write

$$a_{k+1} = \sum_{i=1}^{k} b_i a_i$$

for some $b_i \in R$. Now consider the polynomial

$$g = f_{k+1} - \sum_{i=1}^{k} b_i x^{n_{k+1} - n_i} f_i.$$

By the construction of the sequence of f_i's, we know that $g \in I \backslash (f_1, \ldots, f_k)$. However, we have constructed g in a way that kills off the leading coefficient, leaving a polynomial of degree smaller than the degree of f_{k+1}. This is a contradiction. So, we have shown that if $R[x]$ is not noetherian, then R is not noetherian. The theorem follows. ∎

Definition 1.2.4. Let X be any subset of $\mathbf{A}^n$. Define its associated ideal in the polynomial ring to be

$$I(X) = \{f \in k[x_1, \ldots, x_n] : f(x) = 0 \ \forall x \in X\}.$$

Lemma 1.2.5:

(a) For ideals $I \subset J$, we have $Z(I) \supset Z(J)$.
(b) For algebraic sets $X \subset Y$, we have $I(X) \supset I(Y)$.
(c) For any subset X of $\mathbf{A}^n$, we have $Z(I(X)) = \bar{X}$, the closure in the Zariski topology.

Proof: Obvious. ∎

Theorem 1.2.6: *(Weak Nullstellensatz) Let k be an algebraically closed field. Let $I \subset k[x_1, \ldots, x_n]$ be a proper ideal. Then $Z(I)$ is a nonempty algebraic set in $\mathbf{A}^n$.*

Proof: By the previous lemma, it suffices to prove this when I is a maximal ideal. Let $L = k[x_1, \ldots, x_n]/I$ be the quotient field. If $L = k$, then we're done. To see this, write $a_i \in k$ for the image $a_i \equiv x_i \bmod I$. Thus, each polynomial $x_i - a_i \in I$ and

$$(x_1 - a_1, \ldots, x_n - a_n) \subset I.$$

Since the former ideal is maximal, this containment is an equality, and it is easy to see that $Z(I) = \{(a_1, \ldots, a_n)\}$.

It now suffices to prove the following proposition.

Proposition 1.2.7: *Let k be a field, and let L be an extension field of k that is finitely generated as a k-algebra. Then L is an algebraic extension of k.*

Proof: We can write $L = k[a_1, \ldots, a_n]$. If $n = 1$, then either a_1 is an algebraic element or $L \approx k[a_1]$ is not a field. So, by induction, we may assume that $L = k(a_1)[a_2, \ldots, a_n]$ is an algebraic extension of the field $k(a_1)$. We may also assume that a_1 is transcendental over k (otherwise, we are done).

For all $2 \leq i \leq n$, we have an equation

$$a_i^{n_i} + b_{i,1} a_i^{n_i - 1} + \cdots + b_{i,n_i} = 0,$$

with coefficients $b_{i,j} \in k(a_1)$. We can choose an element $b \in k(a_1)$ large enough to clear all the denominators of the $b_{i,j}$, so that

$$(ba_i)^{n_i} + bb_{i,1}(ba_i)^{n_i - 1} + \cdots + b^{n_i} b_{i,n_i} = 0.$$

In particular, L is an integral extension of $k(a_1)$. (In other words, it is generated by the *integral elements* $ba_2, \ldots, ba_n$.) In particular, given any element $z \in L$, there exists a non-negative integer N such that $b^N z$ is integral over $k[a_1]$. To see this, one needs a series of lemmas.

Lemma 1.2.8: *If s is an integral element over a ring R, then $R[s]$ is finitely generated as an R-module.*

Proof: Obvious. ∎

Lemma 1.2.9: *Let $R \subset S$ be an extension of commutative rings with 1. If S is finitely generated as an R-module, then every element $s \in S$ is integral over R.*

Proof: Let $t_1, \ldots, t_m$ be module generators. Write each product

$$st_i = \sum_{j=1}^{m} r_{ij} t_j,$$

with coefficients $r_{ij} \in R$. Rewriting this with Kronecker deltas yields

$$\sum_{j=1}^{m} (\delta_{ij} s - r_{ij}) w_j = 0$$

for all $i = 1, \ldots, m$. Looking at this equation in an appropriate vector space over the field of fractions of S, one gets a nontrivial solution to a certain matrix equation. Therefore, one has

$$0 = det(\delta_{ij} s - r_{ij}) = s^m + (\text{terms of lower degree}),$$

a monic equation satisfied by s with coefficients in R. ∎

Lemma 1.2.10: *The $R \subset S$ be an inclusion of commutative rings with 1. Then the set of elements of S that are integral over R forms a subring of S.*

Proof: Let a, $b \in S$ be integral elements. Since b is certainly integral over $R[a]$, we have that $R[a]/R$ and $R[a,b]/R[a]$ are finitely generated modules. Thus, $R[a,b]$ is a finitely generated R-module. Thus, the elements $a+b$ and $ab \in R[a,b]$ are integral over R, and the result follows. ■

Returning to the proof of the proposition, we see that any $z \in L$ can be written as a polynomial in $a_2, \ldots, a_n$; multiplying by a large power of b writes it as a combination of things that are known to be integral over the polynomial ring $k[a_i]$, and it follows that $b^N z$ is also integral.

Now suppose $f \in k[a_1]$ is any polynomial that is relatively prime to b. Then $1/f \in L$, but none of the elements b^N/f can possibly be integral over $k[a_1]$. This is a contradiction; therefore, a_1 could not have been transcendental, and the proposition (and the Weak Nullstellensatz) follows. ■

The previous theorem shows that every proper ideal cuts out a nonempty algebraic set. The next theorem will characterize the ideals associated to algebraic sets.

Definition 1.2.11. Let I be an ideal in a ring R. The radical of I is defined as

$$Rad(I) = \{f \in R : \exists N > 0, f^N \in I\}.$$

Remark 1.2.12. The radical $Rad(I)$ is always an ideal. Any ideal that satisfies $I = Rad(I)$ is called a *radical ideal* . If X is any subset of $\mathbf{A}^n$, then $I(X)$ is a radical ideal.

Theorem 1.2.13: *(Hilbert's Nullstellensatz) Let k be an algebraically closed field. Let $J \subset k[x_1, \ldots, x_n]$ be any ideal. Then*

$$I(Z(J)) = Rad(J).$$

Proof: Since $I(X)$ is always radical and $J \subset I(Z(J))$, the inclusion $Rad(J) \subset I(Z(J))$ is trivial. So, let $g \in I(Z(J))$ Now use Hilbert's Basis Theorem to choose generators $f_1, \ldots, f_s$ of J. Consider the auxiliary ideal

$$J' = (f_1, \ldots, f_s, gx_{n+1} - 1) \subset k[x_1, \ldots, x_{n+1}].$$

Since $g = 0$ whenever all $f_i = 0$, we see that $Z(J') = \emptyset$. By the Weak Nullstellensatz, $J' = k[x_1, \ldots, x_{n+1}]$. Thus, there is a relation

$$1 = (\sum_1^s a_i f_i) + b(gx_{n+1} - 1)$$

for some $b, a_i \in k[x_1, \ldots, x_{n+1}]$. Substitute $y = 1/x_{n+1}$ in this equation and clear denominators to get

$$y^m = \sum a_i' f_i + b'(g - y)$$

with coefficients now living in $k[x_1, \ldots, x_n, y]$. Now specialize by setting $y = g$ to obtain

$$g^m = \sum a_i'' f_i \in J \subset k[x_1, \ldots, x_n].$$

Thus, $g \in Rad(J)$ and the theorem is proved. ■

Corollary 1.2.14: *Two algebraic sets $X_1, X_2 \in \mathbf{A}^n$ are equal if and only if $I(X_1) = I(X_2)$.*

Corollary 1.2.15: *There is a natural one-to-one inclusion-reversing correspondence between algebraic sets in $\mathbf{A}^n$ and radical ideals in $k[x_1, \ldots, x_n]$. Under this correspondence, points are associated with maximal ideals.*

Definition 1.2.16. Let X be an algebraic set in $\mathbf{A}^n$. Define the ring of *regular functions* on X to be

$$A(X) = k[x_1, \ldots, x_n]/I(X).$$

Remark 1.2.17. The elements of $A(X)$ can be interpreted as functions on X with values in k. To, see this, note that $A(\mathbf{A}^n) = k[x_1, \ldots, x_n]$ is the full polynomial ring. Clearly, we can view a polynomial in n variables as a well defined function on the set of n-tuples from k. When X is an algebraic set, we can restrict any polynomial function on affine n-space to a function on X. Two polynomials restrict to the same function on X if and only if their difference lives in the ideal $I(X)$.

Notice that the assignment $X \mapsto A(X)$ shows that X determines $A(X)$ uniquely. However, unlike the ideal $I(X)$, the ring $A(X)$ does not directly determine X as a closed subset of $\mathbf{A}^n$. The problem, of course, is that there is no canonical way to recover the generators of the polynomial ring from the quotient ring. If you choose two different sets of generators for $A(X)$, you get two distinct algebraic sets, possibly embedded in different affine spaces, with the same coordinate ring.

We can already see, however, that $A(X)$ has the potential to recover X in a more abstract form. For example, the points of X are in one-to-one correspondence with the maximal ideals of $k[x_1, \ldots, x_n]$ that contain $I(X)$; by the usual yoga of the isomorphism theorems, these are, in turn, in one-to-one correspondence with the maximal ideals of $A(X)$.

Section 1.3 Morphisms

Definition 1.3.1. Let $X \subset \mathbf{A}^n$ and $Y \subset \mathbf{A}^m$ be algebraic sets. A *regular mapping* $\varphi : X \to Y$, also called a *morphism* , is defined to be any function on the underlying sets that can be represented by polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ such that

$$\varphi(x) = (f_1(x), \ldots, f_m(x))$$

and

$$g(f_1(x), \ldots, f_m(x)) = 0$$

whenever $x \in X$ and $g \in I(Y)$.

Definition 1.3.2. The set of all morphisms from X to Y will be denoted $Mor(X, Y)$.

Lemma 1.3.3: *Let $X \subset \mathbf{A}^n$ be an algebraic set. Then*

$$Mor(X, \mathbf{A}^1) \approx k[x_1, \ldots, x_n]/I(X) = A(X).$$

Proof: By definition, a morphism $\varphi : X \to \mathbf{A}^1$ is given by one polynomial in n variables. Two polynomials represent the same function on the underlying set of X if and only if their difference lies in the ideal $I(X)$. The result follows. ∎

Remark 1.3.4. Suppose $\varphi : X \to Y$ is a morphism of algebraic sets. Then φ induces a ring homorphism

$$\varphi^{\#} : A(Y) \to A(X)$$

defined by

$$\varphi^{\#}(f) = f \circ \varphi.$$

In this way, we can view A as a *contravariant functor* from the category ALGSET $/k$ (whose objects are all algebraic sets with the definition of morphism just presented) taking values in the category k-ALG (whose objects are all commutative k-algebras with the evident definition of morphism).

Proposition 1.3.5: $Mor(X, Y) \approx Hom_{k-Alg}(A(Y), A(X))$.

Proof: As above, one can associate to any morphism φ of algebraic sets the k-algebra homomorphism $\varphi^{\#}$. On the other hand, suppose $f : A(Y) \to A(X)$ is a homomorphism of k-algebras. Write

$$A(Y) = k[y_1, \ldots, y_m]/I(Y)$$

and

$$A(X) = k[x_1, \ldots, x_n]/I(X).$$

Define $s_i = f(y_i) \in A(X)$, and choose an arbitrary lifting $s'_i \in k[x_1, \ldots, x_n]$. Then there is a morphism

$$s = (s'_1, \ldots, s'_m) : X \to Y$$

that is independent of the choice of lifting, and clearly satisfies $s^{\#} = f$. ∎

Corollary 1.3.6: *The functor* $A : \mathcal{ALGSET}/k \to k-\mathcal{ALG}$ *is a fully faithful embedding of categories. Moreover, the image of this functor allows us to identify algebraic sets with finitely generated k-algebras that contain no nilpotent elements.*

Remark 1.3.7. As we noted earlier, the algebra $A(X)$ does not have enough information to allow us to recover X as a particular subset of a particular affine space $\mathbf{A}^n$. Nevertheless, this result says that we can recover X up to isomorphism of algebraic sets. That means that any *intrinsic* geometric properties of X can be discovered by studying the algebra $A(X)$; only the *extrinsic* properties that depend on the particular embedding are lost.

Definition 1.3.8. Let k be an algebraically closed field. Let $J \subset k[x_1, \ldots, x_n]$ be any ideal. The *structured algebraic set* defined by J is the pair $(Z(J), R(J))$ consisting of the algebraic set $Z(J)$ together with the coordinate ring $R(J) = k[x_1, \ldots, x_n]/J$.

By abuse of notation, if $X = (Z(J), R(J))$ is the structured algebraic set associated to the ideal J, we will write $A(X) = R(J)$. When X is any (unstructured) algebraic set, unless otherwise specified, it can be identified in a natural way with the canonical structured algebraic set defined by its ideal $I(X)$. With this convention, $A(X)$ has the same meaning that it had previously. Finally, we can define

$$Mor(X, Y) = Hom_k(A(Y), A(X))$$

for any pair of structured algebraic sets. It follows easily from the definitions that there is a fully faithful contravariant functor

$$A : \mathcal{STRALGSETS}/k \to k - \mathcal{ALG}$$

that identifies the category of structured algebraic sets with the category of finitely generated k-algebras. In particular, one has the following result.

Corollary 1.3.9: *Two (structured) algebraic sets are isomorphic if and only if their coordinate rings are isomorphic.*

Remark 1.3.10. One advantage of viewing all algebraic sets as structured algebraic sets is that the definition is coordinate-free, and all the geometric information can be extracted from the coordinate ring itself.

Theorem 1.3.11: *Let $X \subset \mathbf{A}^n$ and $Y \subset \mathbf{A}^m$ be structured algebraic sets. Then their product exists in the category of structured algebraic sets over k.*

Proof: Using the contravariant functor A to transfer the problem into the category of finitely generated k-algebras, we can try to construct a coproduct. It is straightforward to check that the tensor product is such a coproduct. Thus, the product $X \times Y$ of the structured algebraic sets is determined up to isomorphism by the formula

$$A(X \times Y) = A(X) \otimes_k A(Y).$$

■

Example. In particular, we see that $\mathbf{A}^n \times \mathbf{A}^m = \mathbf{A}^{n+m}$ in the category of structured algebraic sets.

Definition 1.3.12. Let $X, Y \subset \mathbf{A}^n$ be structured algebraic sets. Define $X \cap Y$ to be the pullback in the category of structured algebraic sets of the diagram

$$\begin{array}{ccc} & & Y \\ & & \downarrow \\ X & \rightarrow & \mathbf{A}^n \end{array}$$

Lemma 1.3.13: *Let $X, Y \subset \mathbf{A}^n$ be structured algebraic sets. Then $X \cap Y$ exists, and*

$$I(X \cap Y) = (I(X) \cup I(Y)).$$

Proof: We again use the functor A to transport this problem into the category of finitely generated k-algebras, where one needs to complete the pushout diagram

$$\begin{array}{ccc} k[x_1, \ldots, x_n] & \rightarrow & k[x_1, \ldots, x_n]/I(X) \\ \downarrow & & \\ k[x_1, \ldots, x_n]/I(Y) & & \end{array}$$

It is easy to check that $k[x_1, \ldots, x_n]/(I(X) \cup I(Y))$ satisfies the necessary universal property.

■

Example. We need to work in the category of *structured* algebraic sets for this definition to be truly useful. Consider, for example, the intersection in $\mathbf{A}^2$ of the parabola X defined by $y = x^2$ with the line Y defined by $y = 0$. The intersection satisfies

$$I(X \cap Y) = (y - x^2, y) = (y, x^2),$$

so the coordinate ring is

$$A(X \cap Y) = k[x, y]/(y, x^2) \approx k[x]/(x^2).$$

In particular, the intersection of algebraic sets can turn out to be a structured algebraic set; in the present case, this structured algebraic set conatins the extra geometric information that the two curves are tangent at the point of intersection.

Proposition 1.3.14: *Let $X \subset \mathbf{A}^n$ and $Y \subset \mathbf{A}^m$ be structured algebraic sets. Then $X \times Y$ can be canonically identified with the structured algebraic set*

$$(X \times \mathbf{A}^m) \cap (\mathbf{A}^n \times Y),$$

where the intersection is computed inside $\mathbf{A}^n \times \mathbf{A}^m = \mathbf{A}^{n+m}$.

Proof: The natural inclusions

$$I(X) \subset k[x_1, \dots, x_n] \subset k[x_1, \dots, x_n, y_1, \dots, y_m]$$

and

$$I(Y) \subset k[y_1, \dots, y_m] \subset k[x_1, \dots, x_n, y_1, \dots, y_m]$$

clearly allow us to identify the images with

$$I_1(X) = I(X \times \mathbf{A}^m) \text{and } I_2(Y) = I(\mathbf{A}^n \times Y).$$

By the previous lemma, we have

$$I((X \times \mathbf{A}^m) \cap (\mathbf{A}^n \times Y)) = (I_1(X) \cup I_2(Y)).$$

Now one can verify that multiplication defines an isomorphism

$$A(X) \otimes_k A(Y) \to k[x_1, \dots, x_n, y_1, \dots, y_m]/(I_1(X) \cup I_2(Y)),$$

by the "formula"

$$f(x) \otimes g(y) \to f(x, 0)g(0, y).$$

■

Examples.

(i) Let $*$ denote the algebraic set consisting of a single point. Then $A(*) = k$ and $*$ is a final object in the category of structured algebraic sets. In other words, given any structured algebraic set X, there is always a unique morphism $X \to *$ corresponding to the structure map $k \to A(X)$ that includes k as the ring of constant functions on X. More precisely, one has

$$Mor(X, *) = Hom_k(k, A(X)),$$

and it is the set of k-homomorphism that can easily be seen to consist of exactly one element.

(ii) Consider again the one point algebraic set $*$. We have seen that $Mor(X, *)$ always contains exactly one element. What is the set $Mor(*, X)$? Turning the question into one about algebras, we are asking about the set of k-algebra homomorphisms $Hom_k(A(X), k)$. Since these must preserve the k-structure, and k is a field, such homomorphisms are necessarily onto. Each surjective homomorphism to the field k corresponds to a maximal ideal in $A(X)$ (obtained as the kernel). So, using the Weak Nullstellensatz, one has

$$Mor(*, X) = \{\text{maximal ideals in } A(X)\} = \{\text{points in } X\} = X(k).$$

(iii) Let X be the (disjoint) union of two points, viewed as an algebraic set over k. Then

$$A(X) = k \times k.$$

To see this, notice that we can take

$$A(X) = k[x]/(x^2 - x) \approx k[x]/(x) \oplus k[x]/(x-1).$$

More generally, if X and Y are structured algebraic sets, then their disjoint union satisfies $A(X \coprod Y) = A(X) \times A(Y)$. In other words, A takes disjoint unions into Cartesian products of algebras.

(iv) Let X be a structured algebraic set, and consider the diagonal map

$$\Delta : X \to X \times X.$$

This is actually a morphism of structured algebraic sets; it corresponds to the algebra homomorphism $A(X) \otimes A(X) \to A(X)$ by multiplication.

(v) Let X be the affine plane curve defined by the equation $y^2 = x^3 + x^2$. So, $A(X) = k[x,y]/(y^2 - x^3 - x^2)$. We can define a morphism from $\mathbf{A}^1 \to X$ as follows. Let $y = mx$ be a general line through the origin. This line intersects X at the points where

$$x^3 + x^2(1 - m^2) = 0.$$

Ignoring the obvious point at the origin, we get an additional point

$$x = m^2 - 1, y = m^3 - m.$$

These equations define an algebra homomorphism

$$k[x,y]/(y^2 - x^3 - x) \to k[m],$$

since one can easily check that

$$(m^3 - m)^2 - (m^2 - 1)^3 - (m^2 - 1)^2 = 0.$$

(vi) Let H be the hyperbola defined by the equation $xy = 1$. So, the coordinate ring of H is $A(H) = k[x,y]/(xy - 1) \approx k[x, x^{-1}]$. Now let X be any structured algebraic set. Then

$$Mor(X, H) = Hom_k(k[x, x^{-1}], A(X)) = A(X)^*,$$

the set of invertible elements in the ring $A(X)$. It is interesting to note that, in this case, the set of morphisms always forms an abelian group. One interpretation of this remark is that there is a functor

$$Mor(-, H) : \mathcal{STRALGSET} \to \mathcal{AB}.$$

Another interpretation says that H is a group-object in the category of structured algebraic sets. Concretely, there are morphisms

$$\begin{aligned} \mu : H \times H \to H \qquad & \mu^\#(x) = x \otimes x \\ \varepsilon : * \to H \qquad & \varepsilon^\#(x) = 1 \\ \iota : H \to H \qquad & \iota^\#(x) = x^{-1}. \end{aligned}$$

The first morphism is multiplication, the second is the inclusion of the identity element, and the third identifies inverses. These maps satisfy

$$\begin{aligned} \text{associativity:} &\quad \mu \circ (\mu \times 1) = \mu \circ (1 \times \mu) \\ \text{existence of identity:} &\quad \mu(\varepsilon \times 1) = 1 \\ \text{existence of inverse:} &\quad \mu(\iota, 1) = \varepsilon\pi. \end{aligned}$$

(vii) Let T be the structured algebraic set with coordinate ring

$$A(T) = k[x]/(x^2) = k[\varepsilon].$$

How should one interpret the set $Mor(T, X)$? By definition, every such morphism corresponds to an algebra homomorphism $f : A(X) \to k[\varepsilon]$. By composing with the canonical surjection $k[\varepsilon] \to k$ (which takes ε to 0), one obtains a well-defined point $x \in X$, corresponding to the maximal ideal M that is the kernel of the composite. Now we can decompose the set $Mor(T, X)$ into subsets

$$Mor(T, X; x) = \{\varphi : T \to X | \varphi(*) = x\}.$$

We now observe that $f(M) \subset (\varepsilon)$ and $f(M^2) \subset (\varepsilon^2) = 0$. Therefore,

$$Mor(T, X; x) = Hom_{k-VS}(M/M^2, k).$$

In a natural sense, this set of vector space homomorphism can be thought of as the tangent space to X at the point x. For example, let H be the hyperbola considered earlier, and look at the set $Mor(T, H; (1, 1))$. Any such morphism is given by

$$f(x) = 1 + \lambda\varepsilon \text{and } f(y) = 1 + \mu\varepsilon.$$

Moreover, since $xy = 1$, we have

$$0 = (1 + \lambda\varepsilon)(1 + \mu\varepsilon) - 1 = (\lambda + \mu)\varepsilon.$$

Therefore, $\mu = -\lambda$ and the points $x = 1 + \lambda\varepsilon$, $y = 1 - \lambda\varepsilon$ all lie along the line $x + y = 2$, the usual tangent line to the hyperbola at that point.

Section 1.4 Irreducibility

Definition 1.4.1. A topological space is called *reducible* if it can be written as the union of two proper nonempty closed subsets. A space that is not reducible is called *irreducible* .

Remark 1.4.2. If X is an irreducible topological space, then every nonempty open subset is both irreducible and dense. Moreover, any two nonempty open subsets of an irreducible topological space have a nonempty intersection. The closure of an irreducible subset of a topological space is also irreducible.

Proposition 1.4.3: *An algebraic set X is irreducible if and only if the ideal $I(X)$ is prime.*

Proof: If $I(X)$ is not prime, then there exist polynomials f, $g \notin I(X)$ with product $fg \in I(X)$. So, we can write

$$X = (X \cap Z(f)) \cup (X \cap Z(g))$$

as a nontrivial decomposition of X.

Conversely, suppose $X = X_1 \cup X_2$ is a decomposition of X as a union of nonempty proper closed subsets. Then each ideal $I(X_i)$ contains $I(X)$ properly. So, we can choose functions $f_i \in I(X_i) \backslash I(X)$. Then the product $f_1 f_2 \in I(X)$, so the ideal $I(X)$ is not prime. ∎

Corollary 1.4.4: *There is a one-to-one correspondence between irreducible algebraic sets in* $\mathbf{A}^n$ *and prime ideals in* $k[x_1, \ldots, x_n]$.

Theorem 1.4.5: *Let* X *be an algebraic set in* $\mathbf{A}^n$. *Then there exists a unique collection of irreducible algebraic sets* $X_1, \ldots, X_m$ *such that*

(i) $X = X_1 \cup X_2 \cup \cdots \cup X_m$, *and*
(ii) $X_i \subset X_j$ *if and only if* $i = j$.

Proof: (Existence) Suppose the theorem does not hold for an algebraic set X. In particular, X must be reducible. Write $X = X_1 \cup Y_1$. The theorem must also fail for at least one of the pieces in this decomposition; say, X_1. Now write $X_1 = X_2 \cup Y_2$ and repeat. In this way, one constructs an infinite decreasing chain of algebraic sets

$$X \supset X_1 \supset X_2 \supset \cdots.$$

However, the chain of associated ideals

$$I(X) \subset I(X_1) \subset I(X_2) \subset \cdots$$

must terminate, by Hilbert's Basis Theorem. Therefore, X has a finite decomposition as a union of irreducibles. The condition prohibiting containments can be realized by throwing out any redundant items in the decomposition.

(Uniqueness) Suppose

$$X = \bigcup_i X_i = \bigcup_j Y_j$$

are two irredundant decompositions of X as a union of irreducible algebraic sets. For each i, we can write

$$X_i = X_i \cap X = X_i \cap (\bigcup_j Y_j) = \bigcup_j (X_i \cap Y_j).$$

Because X_i is irreducible, there exists some j with the property that $X_i = X_i \cap Y_j \subset Y_j$. By interchanging the roles of the decompositions, there exists some i' with

$$X_i \subset Y_j \subset X_{i'}.$$

Because the decompositions are irredundant, this last chain of inclusions must actually consist of equalities, and the result follows. ∎

Corollary 1.4.6: *Let* $f \in k[x_1, \ldots, x_n]$. *Write*

$$f = f_1^{n_1} \cdots f_s^{n_s}$$

as a product of irreducible factors. Then

$$Z(f) = Z(f_1) \cup \cdots \cup Z(f_s)$$

is the unique decomposition of its zero set into irreducible components. Furthermore,

$$I(Z(f)) = (f_1 f_2 \cdots f_s).$$

Proof: The function f_1 must vanish on some component X_1 of X. But then $X_1 \subset Z(f_1)$, which forces $X_1 = Z(f_1) \cap X$. ∎

Definition 1.4.7. An algebraic set defined by one polynomial in $\mathbf{A}^n$ is called a *hypersurface* . The irreducible hypersurfaces are in one-to-one correspondence with the irreducible polynomials.

Theorem 1.4.8: *The product of two irreducible algebraic sets is irreducible.*

Proof: Let X and Y be irreducible, and suppose that $X \times Y = Z_1 \cup Z_2$ is a decomposition of the product. For each point $x \in X$, we have

$$Y = x \times Y = ((x \times Y) \cap Z_1) \cup ((x \times Y) \cap Z_2).$$

So, at least one of the factors on the right contains this copy of the irreducible set Y. Now define $X_i \subset X$ to be the set of all $x \in X$ such that $x \times Y \subset Z_i$. We have already observed that $X = X_1 \cup X_2$. However, X is also irreducible and the X_i are closed subsets. Therefore, we must have $X = X_1$ and $X \times Y = Z_1$. ∎

Definition 1.4.9. An *affine algebraic variety* over an algebraically closed field k is an irreducible algebriac set in $\mathbf{A}^n$ with the induced topology and the (reduced) induced structure.

Examples.

(i) $\mathbf{A}^n$ is a variety.
(ii) Among the curves of the first section, only (v), (x), and (xi) are not varieties.
(iii) A point is a variety; two points are not.

Section 1.5 Rational Functions

Definition 1.5.1. Let X be an affine algebraic variety over an algebraically closed field k. Then $I(X)$ is a prime ideal, so $A(X)$ is an integral domain. Define $k(X)$ to be the field of fractions of the integral domain $A(X)$. Elements of $k(X)$ are called *rational functions* on X.

Definition 1.5.2. A rational function $\varphi \in k(X)$ is called *regular at a point* $x \in X$ if it can be represented in the form $\varphi = f/g$ where f, $g \in A(X)$ and $g(x) \neq 0$.

Proposition 1.5.3: *Let X be an algebraic variety. Then*

$$A(X) = \{\varphi \in k(X) : \varphi \text{ is regular at all points } x \in X\}.$$

Proof: Write S for the set on the right-hand side. Clearly, $A(X) \subset S$. Conversely, suppose $\varphi \in S$. Then for each $x \in X$, we can write $\varphi = f_x/g_x$ with $g_x(x) \neq 0$. Now consider the ideal

$$I = (I(X), g_x : x \in X) \subset k[x_1, \dots, x_n].$$

Since

$$Z(I) = \{x \in X : \varphi \text{ is not regular at } x\},$$

the Weak Nullstellensatz implies that $I = (1)$. Reducing modulo $I(X)$, one has a relation

$$1 = \sum u_i g_{x_i},$$

for some $u_i \in A(X)$. Multiplying by φ yields

$$\varphi = \sum u_i f_{x_i} \in A(X).$$

∎

Definition 1.5.4. Any open subset of an affine variety is called a *quasi-affine variety* . If $S \subset \mathbf{A}^n$ is any quasi-affine variety, then it has a ring of functions defined by

$$A(S) = \frac{\{\varphi \in k(\mathbf{A}^n) : \varphi \text{ is regular at all } s \in S\}}{\{\varphi \in k(\mathbf{A}^n) : \varphi(s) = 0 \text{ at all } s \in S\}}.$$

By the proposition, if X is an affine variety, then this definition agrees with the previous one.

Examples.

(i) Consider the quasi-affine variety $U = \mathbf{A}^1 \backslash \{0\}$. Since U is open in the irreducible variety $\mathbf{A}^1$, it is irreducible and dense. Therefore, $A(U)$ is a subring of $k(\mathbf{A}^1) = k(x)$. In order to determine which rational functions $\varphi = f(x)/g(x)$ are regular on U, we only need to determine which polynomials $g(x)$ are zero only at the point 0. Since these polynomials consist only of the powers of x, we see that $A(U) = k[x, x^{-1}]$. We recognize this ring of functions as the coordinate ring of the affine plane curve V defined by $xy = 1$. Moreover, projection on the x-coordinate is a topological homeomorphism $V \to U$ that is an isomorphism on the ring of regular functions. In this way, we can identify the quasi-affine variety U with the affine variety V.

(ii) Let's try to repeat the previous example in a larger dimension. This time, take $U = \mathbf{A}^2 \backslash \{(0, 0)\}$. The same analysis shows that $A(U)$ is a subring of $k(X)$. Writing a rational function $\varphi = f(x, y)/g(x, y)$ as a quotient of relatively prime polynomials, we see that φ is not regular on the zero set $Z(g)$. If g is a nonconstant polynomial, then we have seen that this zero set is infinite. It follows that $A(U) \approx A(\mathbf{A}^1) = k[x, y]$, and that this isomorphism is induced by the inclusion map (which is **not** a homeomorphism). Since coordinate rings determine their varieties up to isomorphism, it follows that the quasi-affine variety U is not isomorphic to any affine variety.

Lemma 1.5.5: *The complement of a hypersurface in* $\mathbf{A}^n$ *is an affine variety. Moreover, if* $U = \mathbf{A}^n \backslash Z(f)$*, then*

$$A(U) = k[x_1, \ldots, x_n, 1/f] = A(\mathbf{A}^n)_f.$$

Proof: Let $V \subset \mathbf{A}^{n+1}$ be defined by $V = Z(x_{n+1}f - 1)$. There is a commutative diagram

$$\begin{array}{cccc} U = & \mathbf{A}^n \backslash Z(f) & \subset & \mathbf{A}^n \\ & \downarrow \varphi \uparrow \psi & & \uparrow pr \\ & V & \subset & \mathbf{A}^{n+1} \end{array}$$

where

$$\varphi(a_1, \ldots, a_n) = (a_1, \ldots, a_n, 1/f(a_1, \ldots, a_n)),$$

and

$$\psi(a_1, \ldots, a_{n+1}) = (a_1, \ldots, a_n).$$

It is easy to check that $\varphi \circ \psi = 1$, that $\psi \circ \varphi = 1$, and that φ and ψ induce isomorphisms on the rings of functions. ∎

Corollary 1.5.6: *Let $f \in A(X)$ be a function on an affine algebraic variety X. Then $U = X \backslash Z(f)$ is an affine variety and*

$$A(U) = A(X)_f = A(X)[1/f].$$

Lemma 1.5.7: *Let X be an algebraic set. Then there exists a basis for the topology on X consisting of affine open algebraic sets.*

Proof: Let $U \subset X$ be any open subset, and let $P \in U$ be a point. Since P and $X \backslash U$ are disjoint closed subsets in X, there must exist a function $f \in A(X)$ with $f(P) = 1$ and $f \in I(X \backslash U)$. Then $X \backslash U \subset Z(f)$, so

$$P \in X \backslash Z(f) \subset U$$

gives an affine open neighborhood of P inside U. ∎

Lemma 1.5.8: *Let X be an algebraic variety. Let $U \subset X$ be a nonempty open subset. If φ, $\psi \in A(X)$ are regular functions such that $\varphi|_U = \psi|_U$ agree on U, then $\varphi = \psi$.*

Proof: Let $\rho = (\varphi, \psi) : X \to \mathbf{A}^1 \times \mathbf{A}^1 = \mathbf{A}^2$. By hypothesis, the image $\rho(U)$ is contained in the diagonal, Δ, which is an algebraic set defined by $x = y$. Since U is dense in X (by irreducibility), and Δ is closed, we have

$$\rho(X) \subset \rho(\bar{U}) \subset \Delta$$

and, therefore, $\varphi = \psi$. ∎

Theorem 1.5.9: *Let X be an algebraic variety. Then*

$$k(X) = \frac{\{(U, f) : U \text{ is a nonempty open subset of } X \text{ and } f : U \to \mathbf{A}^1\}}{(U, f) \sim (V, g) \text{ iff } f|_{U \cap V} = g|_{U \cap V}}$$

Proof: Since the affine opens form a basis for the topology, we only need to consider affine opens in the description. If U and V are nonempty opens, then so is their intersection (by irreducibility). Therefore, $\sim$ is an equivalence relation. By definition, every element in the set on the right-hand side comes from a rational function. But every rational function $\varphi \in k(X)$ has at least one representation $\varphi = f/g$, yielding a pair $(X \backslash Z(g), f/g)$. ∎

Section 1.6 Birationality

Definition 1.6.1. An algebraic variety X is called *rational* if $k(X)$ is isomorphic to the field of rational functions $k(x_1, \ldots, x_n) = k(\mathbf{A}^n)$.

Examples.

(i) Let $X = Z(xy - 1) \subset \mathbf{A}^2$. Then the function field of $A(X) = k[x, x^{-1}]$ is clearly isomorphic to $k(X)$. In fact, projection on the x-coordinate defines a morphism $X \to \mathbf{A}^1$ that induces an isomorphism of function fields.

(ii) Let $X = Z(y^2 - x^3 - x^2) \subset \mathbf{A}^2$. In the previous chapter, we constructed a morphism $\mathbf{A}^1 \to X$ given by the equations

$$x = m^2 - 1$$

and

$$y = m^3 - m.$$

This morphism defines an injection

$$A(X) \to k[m] \subset k(m),$$

and hence induces a map $k(X) \to k(m)$. The inverse of this map on function fields is given by $m = x/y$.

(iii) Suppose the characteristic of the field k differs from 3. Then the curve $Z(x^3 + y^3 - 1)$ is **not** a rational curve. To see this, suppose that it is rational. Then we could write

$$x = p(t)/r(t), \text{and } y = q(t)/r(t),$$

where p, q, $r \in k[t]$ are relatively prime polynomials. Now the equations

$$\begin{aligned} p^3 + q^3 - r^3 \quad &= 0 \\ 3p^2p' + 3q^2q' - 3r^2r' \quad &= 0 \end{aligned}$$

can be viewed as a linear system

$$\begin{pmatrix} p & q & -r \\ p' & q' & -r' \end{pmatrix} \begin{pmatrix} p^2 \\ q^2 \\ r^2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} .$$

Since $p \neq 0$, this system is equivalent to

$$\begin{pmatrix} p & q & -r \\ 0 & pq' - qp' & rp' - pr' \end{pmatrix} \begin{pmatrix} u \\ v \\ w \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} ,$$

whose general solution is

$$\begin{pmatrix} u \\ v \\ w \end{pmatrix} = C \begin{pmatrix} rq' - qr' \\ pr' - rp' \\ pq' - qp' \end{pmatrix} .$$

By symmetry, we can assume that

$$deg(r) \leq deg(q) \leq deg(p).$$

Since p^2, q^2 and r^2 are relatively prime, we conclude that

$$p^2 \text{divides } rq' - qr'.$$

Therefore,

$$2deg(p) \leq deg(r) + deg(q) - 1.$$

This contradicts the assumption we made about the degrees, and so no such polynomials can exist. Note that this proof immediately generalizes to show that $Z(x^n + y^n - 1)$ is not a rational curve if $n > 2$ and the characteristic of k is relatively prime to n.

(iv) The surface $Z(x^3 + y^3 + z^3 - 1)$ in $\mathbf{A}^3$ is rational. To see this, consider the lines

$$\begin{aligned} L = \quad & Z(z - 1, x + y) \\ M = \quad & Z(z - \omega, x + \omega y), \end{aligned}$$

where ω is a primitive cube root of unity. Then L and $M \subset X$, but $L \cap M = \emptyset$. Now choose a plane $E \subset \mathbf{A}^3$ that contains neither L nor M. Every point $x \in \mathbf{A}^3 \backslash L \backslash M$ uniquely determines a line $N(x, L, M)$ that contains x and has a nonempty intersection with both L and M. Thus, one gets a morphism

$$\mathbf{A}^3 \backslash L \backslash M \to \mathbf{A}^2$$

by

$$x \mapsto N(x, L, M) \cap E.$$

This map restricts to a well-defined morphism everywhere on X. Since $N(x, L, M) \cap X$ generically determines a unique point of $X \backslash L \backslash M$, the map induces an isomorphism of function fields $k(X) \approx k(\mathbf{A}^2)$.

Remark 1.6.2. A variety X is called *unirational* if $k(X) \subset k(t_1, \ldots, t_n)$. For a long time, it was an open question whether unirational implies rational. For $n = 1$ or $n = 2$, it does. Among other examples, Clemens and Griffiths showed that the threefold $Z(x^3 + y^3 + z^3 + w^3 - 1)$ is unirational but not rational. It is still unknown if $Z(x^3 + y^3 + z^3 + u^3 + v^3 - 1)$ is rational, unirational, or neither.

Definition 1.6.3. Two varieties X and Y are called *birationally isomorphic* if their function fields are isomorphic.

Notice that a variety is rational if and only if it is birationally isomorphic to $\mathbf{A}^n$.

Lemma 1.6.4: *Let $U \subset X$ be a nonempty open subset of an algebraic variety X. Then U is birationally isomorphic to X.*

Proof: Shrink U further and assume that it is an affine open subset. Then $A(U) = A(X)[1/f]$ clearly has the same field of fractions that $A(X)$ has. ∎

Definition 1.6.5. A *rational mapping* $\varphi : X \dashrightarrow Y$ between algebraic varieties is defined as a collection of rational functions $\varphi_i \in k(X)$ such that

$$g(\varphi_1(x), \ldots, \varphi_m(x)) = 0$$

whenever $g \in I(Y)$ and all the φ_i are regular at the point $x \in X$.

Since each φ_i is regular on a nonempty open set, so is φ. A rational map is called *dominant* if $\varphi(U)$ is dense in Y for any nonempty open subset U contained in the domain of regularity of φ.

Theorem 1.6.6: *There is a natural equivalence between the category of algebraic varieties with dominant rational maps and the category of finitely generated field extensions of k.*

Proof: Let $\varphi : X \dashrightarrow Y$ be a dominant rational map, and let $U \subset X$ be a nonempty open set where φ is regular. Then

$$\varphi^{\#} : A(Y) \to A(U) \subset k(X).$$

If $\varphi^{\#}(g) = 0$, then $g = 0$, since $\varphi(U)$ is dense in Y. So, $\varphi^{\#}$ is an embedding of an integral domain into a field. By the universal property of the field of fractions, $\varphi^{\#}$ extends uniquely to a homomorphism of fields

$$\varphi^* : k(Y) \to k(X).$$

Conversely, let $\psi : k(Y) \to k(X)$ be any homomorphism of fields. Restrict to the subring $A(Y) = k[y_1, \ldots, y_m]/I(Y)$. Then

$$(\psi(y_1), \ldots, \psi(y_m))$$

is a rational map from X to Y. It is easy to check that these two procedures are inverses. ∎

Proposition 1.6.7: *Two varieties X and Y are birationally isomorphic if and only if they contain isomorphic open subsets.*

Proof: One direction is immediate from the lemma before the theorem. The other follows by interpreting maps of function fields as morphisms defined on open subsets and applying the previous theorem. ∎

Theorem 1.6.8: *Every algebraic variety is birationally isomorphic to a hypersurface.*

Proof: Since $k(X)/k$ is a separable extension of fields, it has a separating transcendence basis $t_1, \ldots, t_n \in k(X)$. In other words, $k(X)$ is a finite separable algebraic field extension of the rational function field $k(t_1, \ldots, t_n)$. By the primitive element theorem, we can write

$$k(X) = k(t_1, \ldots, t_n)[s]/(\text{minimal polynomial of } s).$$

By clearing denominators in the coefficients of the minimal polynomial, we can assume the coefficients live in the ring of polynomials. Now define

$$A(Y) = k[t_1, \ldots, t_n, s]/(\text{minimal polynomial of } s).$$

Then Y is a hypersurface and $k(Y) = k(X)$. ∎

Section 1.7 Projective Space

Before trying to define projective space, we consider an example.

Example 1.7.1. Consider the affine plane curve X defined by

$$y^2 - y + x^2 + x + 2xy = 0.$$

The point $(x, y) = (0, 0)$ clearly satisfies this equation, so it lies on X. Look at the intersection between X and a line $y = mx$ passing through the origin. We have

$$m^2x^2 - mx + x^2 + x + 2xmx = 0$$

or

$$(m^2 + 2m + 1)x^2 + (1 - m)x = 0$$

There are, therefore, two solutions. Either $x = y = 0$ or $x = (m - 1)/(m + 1)^2$ and $y = (m^2 - m)/(m + 1)^2$.

For most lines, we get exactly two intersection points. (When $m = 1$, we get a single point counted with multiplicity two.) This result makes sense since X is a curve of degree 2, and lines have degree 1. the only problem arises when $x = -1$, when the second intersection point disappears because we are trying to divide by zero. Algebraic geometers are bothered when a discrete invariant (like the number of points of intersection) jumps in the middle of a continuous process. In this case, the extra intersection point has escaped to infinity. One of the points of introducing the notion of projective space is to bring it back.

Definition 1.7.2. We define *projective n-space* over an algebraically closed field k, and denote by $\mathbf{P}^n_k$, the set of lines through the origin in $\mathbf{A}^{n+1}_k$.

Remark 1.7.3. We can give an explicit description of $\mathbf{P}^n_k$ in terms of coordinates. To give a line through the origin, you must pick a point $x = (x_0, \ldots, x_n) \in \mathbf{A}^{n+1}_k$ with at least one nonzero coordinate. Any other point (except the origin) on the line is related to x by being a scalar multiple of it. In other words, any other point has the form $ax = (ax_0, \ldots, ax_n)$ for some nonzero element $a \in k$. Thus, the points of projective space are equivalence classes arising from the equivalence relation on $\mathbf{A}_k^{n+1} \backslash \{(0, \ldots, 0)\}$ given by identifying $x \sim ax$. We will write $(x_0 : \ldots : x_n)$ for one of these equivalence classes, and will refer to each coordinate as a *homogeneous coordinate* .

The description we have just given of projective space using coordinates is external; next, we want to investigate an internal description. Let $U_0 = \{(x_0 : \ldots, x_n) \in \mathbf{P}_k^n : x_0 \neq 0\}$. Because the lead coordinate is nonzero, we can divide by it to normalize the representative of an equivalence class of a point in U_0. In other words,

$$(x_0 : \ldots : x_n) \sim (1 : \frac{x_1}{x_0} : \frac{x_2}{x_0} : \ldots : \frac{x_n}{x_0}).$$

The normalized form of the homogeneous coordinates of points on U_0 is unique, and we get a natural bijection between U_0 and $\mathbf{A}_k^n = k^n$.

Let

$$Z_0 = \mathbf{P}_k^n \backslash U_0 = \{(x_0 : \ldots : x_n) : x_0 = 0\} \approx \mathbf{P}_k^{n-1}.$$

Thus, we can think about building $\mathbf{P}_k^n$ by starting (internally) with affine n-space $\mathbf{A}_k^n$ and adding something at infinity; namely, Z_0. In particular,

1. $\mathbf{P}_k^0$ is just a point.
2. $\mathbf{P}_k^1$ is obtained by adding a single point to the affine line.
3. $\mathbf{P}_k^2$ is obtained by adding a copy of $\mathbf{P}_k^1$ to the affine plane. In other words, we add one point for each direction of a line through the origin of the affine plane.

It's time to start thinking about a topology on projective space. Start with a polynomial $f \in k[x_0, \ldots, x_n]$. It makes perfect sense to talk about where f takes on the value zero on affine space, but it makes no sense to discuss this on projective space. The problem, of course, is that f might vanish on one representative of an equivalence class, but not on other representatives.

Definition 1.7.4. We say that $f \in k[x_0, \ldots, x_n]$ is a *homogeneous form* if there exists a non-negative integer d such that

$$f(ax_0, \ldots, ax_n) = a^d f(x_0, \ldots, x_n)$$

for all $a \in k^*$ and for all $x_0, \ldots, x_n$.

Remark 1.7.5. A homogeneous form cannot be thought of as a function on the points of projective space. However, the property $f(x_0, \ldots, x_n) = 0$ is well-defined independently of the choice of a representative of an equivalence class in $\mathbf{P}_k^n$.

Definition 1.7.6. Let $S \subset k[x_0, \ldots, x_n]$ be any set of homogeneous polynomials. Define the *projective zero set* associated to S to be

$$V(S) = \{x = (x_0, \ldots, x_n) \in \mathbf{P}_k^n : f(x) = 0 \; \forall f \in S\}.$$

Remark 1.7.7. The ideal $< S >$ generated by a set of homogeneous elements is called a *homogeneous ideal* . Not every element of a homogeneous ideal is homogeneous. For example, the homogeneous ideal $< x, y^2 > \subset k[x, y]$ contains the nonhomogeneous element $x + y^2$.

Remark 1.7.8. It is not possible for every homogeneous ideal to pick out a nonempty set of points in projective space. For example, consider the maximal ideal $I = < x_0, \ldots, x_n >$. It is trivial to check that $V(I) = \emptyset$, since each point of projective space must have at least one nonzero coordinate. We call I the *irrelevant ideal* .

Definition 1.7.9. Define a *closed algebraic set* in $\mathbf{P}^n_k$ to be the projective zero set associated to some homogeneous ideal. With these as the closed sets, we get a topology on projective space called the *Zariski topology* .

Proposition 1.7.10: *There is a bijection between closed algebraic sets in $\mathbf{P}^n_k$ and radical homogeneous ideals in $k[x_0, \ldots, x_n]$, except for the irrelevant ideal.*

Proof: For each subset $Y \subset \mathbf{P}^n_k$, we let $J(Y)$ be the ideal generated by all homogeneous polynomials that vanish at all points of Y. It is easy to see that $J(Y)$ is always a radical ideal. It is also easy to check that $V(J(Y)) = \bar{Y}$ is the closure in the Zariski topology.

The main point is now to check that $I = J(V(I))$ whenever I is a radical homogeneous ideal. To proceed, we can forget the grading and homogeneity for a moment, and look instead at the affine variety $Z(I)$ that it defines in $\mathbf{A}^{n+1}_k$. There are three possibilities:

1. $Z(I)$ is empty. By the weak Nullstellensatz, this can only happen if $I = k[x_0, \ldots, x_n]$, in which case we also have that $V(I)$ is empty.
2. $Z(I)$ only contains the origin. Again using the affine results, this can only happen if I is the irrelevant maximal ideal, and so $V(I)$ is again empty.
3. $Z(I)$ is a union of lines through the origin. In this case, we have $J(V(I)) = I(Z(I))$. By Hilbert's Nullstellensatz, we have $I(Z(I)) = rad(I) = I$.

The result follows from this case-by-case analysis. ∎

Definition 1.7.11. The *affine cone* over a projective variety $Y \subset \mathbf{P}^n_k$ is the closed subset of $\mathbf{A}^{n+1}_k$ defined by $Z(J(Y))$, where we forget that $J(Y)$ is a homogeneous ideal.

Remark 1.7.12. A nonempty projective algebraic set Y is irreducible if and only if its affine cone is irreducible.

Corollary 1.7.13: *Under the bijection of the proposition, nonempty irreducible closed algebraic sets correspond to nonirrelevant proper homogeneous prime ideals.*

Corollary 1.7.14: *Every projective algebraic set can be writtten uniquely as a finite irredundant union of irreducible projective algebraic sets.*

Example 1.7.15. Let's return to the example with which we opened this discussion. Recognizing that we are looking at a parabola, let's straighten it out, and look at the affine plane curve $X = Z(y - x^2)$. When you look at the intersections of this parabola with the lines $y = mx$, one of the two intersection points escapes to infinity as the line becomes vertical. But we can put the affine plane $\mathbf{A}^2_k$ (with coordinates (x, y)) into the projective plane $\mathbf{P}^2_k$ (with coordinates $(X : Y : Z)$) as the open subset where $Z \neq 0$. Normalizing projective coordinates, this means that $x = X/Z$ and $y = Y/Z$, and the affine equation of the curve transforms into

$$\frac{Y}{Z} = \frac{X^2}{Z^2}.$$

Since that equation doesn't give us a homogeneous form, we have to clear denominators in a minimal way to get $YZ - X^2$.

More generally, given any affine ideal $I \subset k[x, y]$, you can associate to each polynomial $f(x, y) \in I$, of degree d, a homogeneous form $f^*(X, Y, Z) = Z^d f(X/Z, Y/Z)$. We let $I^* \subset k[X, Y, Z]$ denote the homogeneous ideal generated by all the homogeneous forms associated to polynomials in I. We then refer to $V(I^*)$ as the *projective closure* of the affine algebraic set $Z(I)$.

In this example, the projective closure of the affine parabola is the curve defined by $YZ - X^2$, and the projective closure of a line $y = mx$ is the projective line defined by $Y = mX$. Letting m go to infinity, this line becomes the "vertical" line $X = 0$, which intersects the projective closure of the parabola in two points:

- the affine origin $(0 : 0 : 1)$, and
- the point $(0 : 1 : 0)$ at infinity on the vertical line.

The next natural question to ask is: what are the maps between projective algebraic sets? In the affine case this was easy: we simply took lists of polynomials (that clearly gave maps from one affine space to another), restricted them to an algebraic subset of the domain, and looked at conditions that ensured that the image landed in another algebraic set. In the projective case, things are not so simple. For example, let's continue looking at the projective conic $C = V(YZ - X^2)$. We can try to map this to the projective line by the formula $(X : Y : Z) \mapsto (X : Z)$. (This is an attempt to extend to the projective setting the map that projects the affine parabola straight down onto the x-axis.) The problem with this formula, however, is that it takes the point $(0 : 1 : 0)$ (which we conveniently added to solve the intersection-counting problem) to the nonexistent point $(0 : 0)$! Perservering, we find for points of C that

$$(X : Z) = (X^2 : XZ) = (YZ : XZ) = (Y : X).$$

Using this formula, the point $(0 : 1 : 0)$ simply maps to $(1 : 0)$. However, this formula takes the perfectly good point $(0 : 0 : 1)$ to the nonexistent point $(0 : 0)$!

This example illustrates a typical phenomenon with maps between projective algebriac sets. It is almost always the case that there is no single formula (defining a map on all of projective space or even on all of the projective set) that works everywhere to define morphisms. Instead, you have to define everything locally and verify that the formulas patch together in a reasonable way. Solving this problem is the subject of the next chapter.