THE IDEAL-VARIETY CORRESPONDENCE IN AFFINE AND PROJECTIVE SPACE

ARON DAW

1. Introduction

Classical algebraic geometry is the study of zeros of polynomials and their relation to special subsets in polynomial rings. We will define geometric objects, called *varieties*, as zeros of polynomials. We will also define *ideals* as sets of polynomials that satisfy certain properties. We will examine a way of mapping varieties to ideals and ideals to varieties. These maps will eventually allow us to build a correspondence between varieties and ideals. We will first build and examine this correspondence in affine space, and then we will extend our results to projective space.

The reader will be assumed to know about basic proof structure and common terminology that comes along with set maps, like injective (one-to-one) and bijective. While we will not delve deeply into most of the proofs, at times it will be useful to know. Also, ideals are objects commonly studied in ring theory. While we do discuss everything the reader needs to know in relation to ideals, some exposure to ring theory and ideals, or at least groups and subgroups, would be helpful. We also will be talking about and using abstract fields. If the reader is unfamiliar with abstract fields, they can think of the real numbers $\mathbb{R}$ instead of an abstract field k in almost every instance where an abstract field k is used. Occasionally, we will require the field to be algebraically closed as a hypothesis for some theorems. If the reader is unfamiliar with that notion, simply think of the complex numbers $\mathbb{C}$. Also, the theorems which do require the field to be algebraically closed will be discussed the least in depth (as their proofs are long or complicated, and will be skipped), but they are some of the most beautiful results as well.

2. Polynomials, Affine Space, and Affine Varieties

In this section we introduce the geometric side of algebraic geometry. Intuitively, (that is to say, not precisely) we will be considering points, curves, surfaces, and more in n-dimensional space. We will examine their unions and intersections and how to describe these objects with equations. First we define the space in which we place these objects.

Definition 2.1 (Affine Space)**.** Given a field k and a positive integer n, we define **n-dimensional affine space over** k to be the set

$$k^n = \{(a_1, a_2, \ldots, a_n) \mid a_1, a_2, \ldots, a_k \in k\}.$$

Date: July 4, 2017.

In the special case of $n = 1$ or 2, we call this space the **affine line** or the **affine plane** over k, respectively. We want to study geometric objects within affine space. The objects we study are the zeros of polynomials over k. To define a polynomial, first we define monomials.

Definition 2.2 (Monomial)**.** A **monomial** in $x_1, x_2, ..., x_n$ is a product of the form

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n},$$

where each α_i is a non-negative integer. The **total degree** of the monomial is $\alpha_1 + \cdots + \alpha_n$.

To simplify the notation as we move to polynomials, first we let $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$ and then set

$$x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}.$$

We let $|\alpha| = \alpha_1 + \cdots + \alpha_n$ denote the total degree of x^α. Now we are ready to define polynomials.

Definition 2.3 (Polynomial)**.** A **polynomial** in $x_1, ..., x_n$ with coefficients in a field k is a finite linear combination of monomials with coefficients in k. We write a generic polynomial f as

$$f = \sum_\alpha c_\alpha x^\alpha,$$

where the sum is over a finite number of n-tuples $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$ and $c_\alpha \in k$. We define the **degree** $\deg(f)$ to be the maximum $|\alpha|$ such that c_α is non-zero.

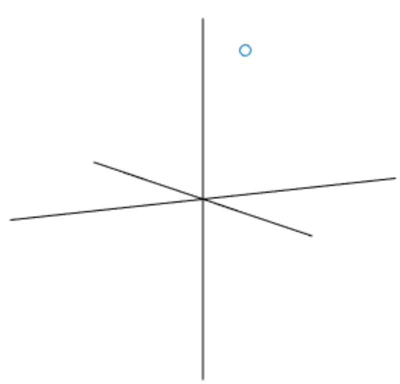
Note that the set of all polynomails in $x_1, x_1, ..., x_n$ is precisely the polynomial ring $k[x_1, x_2, ..., x_n]$. This foreshadows the relationship between the geometric objects we are about to define and the world of algebra. Now that we have polynomials, we are ready to define affine varieties, which are geometric objects that sit in affine space.

Definition 2.4 (Affine variety)**.** Let k be a field, and let $f_1, f_2, ..., f_s$ be polynomials in $k[x_1, ..., x_n]$. We set

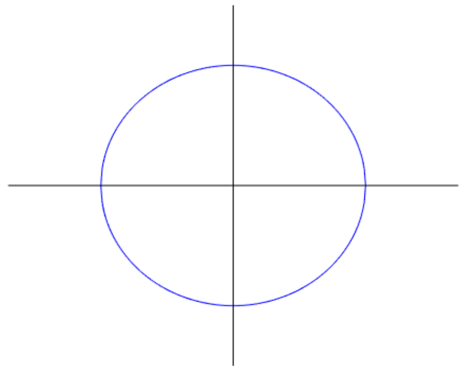
$$\mathbb{V}(f_1, ..., f_s) = \{(a_1, a_2, ..., a_n) \in k^n \mid f_i(a_1, ..., a_n) = 0 \text{ for all } 1 \leq i \leq s\},$$

and we call $\mathbb{V}(f_1, ..., f_s)$ the **affine variety** defined by $f_1, ..., f_s$.

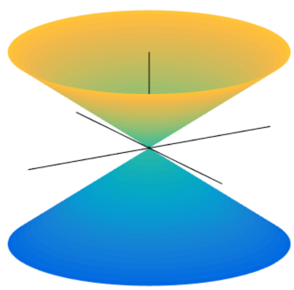
Example 2.5. The following are a few examples of varieties in $\mathbb{R}^2$ and $\mathbb{R}^3$, along with the equations used to define them. First, a single point in $\mathbb{R}^3$ is a variety. For example, $\mathbb{V}((x-1)^2 + (y-1)^2 + (z-2)^2) = \{(1, 1, 2)\}$. The point is circled in blue, for visibility. Note that we could have also found this point as $\mathbb{V}(x - 1, y - 1, z - 2)$.



Next, a circle in $\mathbb{R}^2$, given by $\mathbb{V}(x^2 + y^2 - 1)$.



We can also look at more complicated conics in $\mathbb{R}^3$, for example this cone given by $\mathbb{V}(z^2 - x^2 - y^2)$.



As we start to imagine these geometric objects, we might ask ourselves what sort of operations we can do with them. Can we take intersections? Can we take unions? The answer to both of those questions is yes.

Lemma 2.6. *If $V, W \subseteq k^n$ are affine varieties, then so are $V \cup W$ and $V \cap W$.*

Finding polynomials that describe the intersection or union is quite simple. To illustrate, we'll examine a simple case; if f and g are polynomials in $k[x_1, ...x_n]$ then $\mathbb{V}(f) \cup \mathbb{V}(g) = \mathbb{V}(fg)$. As for intersections, we can simply take $\mathbb{V}(f, g)$. Or, when working over the reals, we can write the intersection as $\mathbb{V}(f^2 + g^2)$. The same idea can be applied to any variety in $\mathbb{R}^n$, meaning that any variety in $\mathbb{R}^n$ can be described by a single equation!

Example 2.7 (Twisted Cubic)**.** The following is a nice example displaying intersections and unions of varieties. We will be working in $\mathbb{R}^3$. First we will display the varieties given by $\mathbb{V}(y - x^2)$ and $\mathbb{V}(z - x^3)$ in Figure 1 and 2 respectively. Then we show the union of the two, given by $\mathbb{V}((y - x^2)(z - x^3))$, in Figure 3. Finally, we display the twisted cubic in Figure 4, which is the intersection of $\mathbb{V}(y - x^2)$ and $\mathbb{V}(z - x^3)$. We can describe this variety as $\mathbb{V}(y - x^2, z - x^3)$ or $\mathbb{V}((y - x^2)^2 + (z - x^3)^2)$. The descriptions are equivalent.

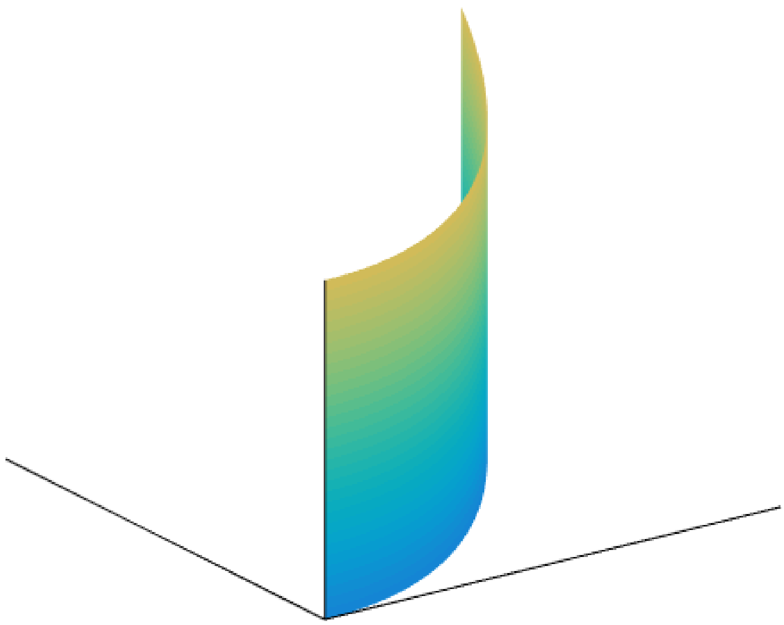


FIGURE 1. The surface $\mathbb{V}(y - x^2)$

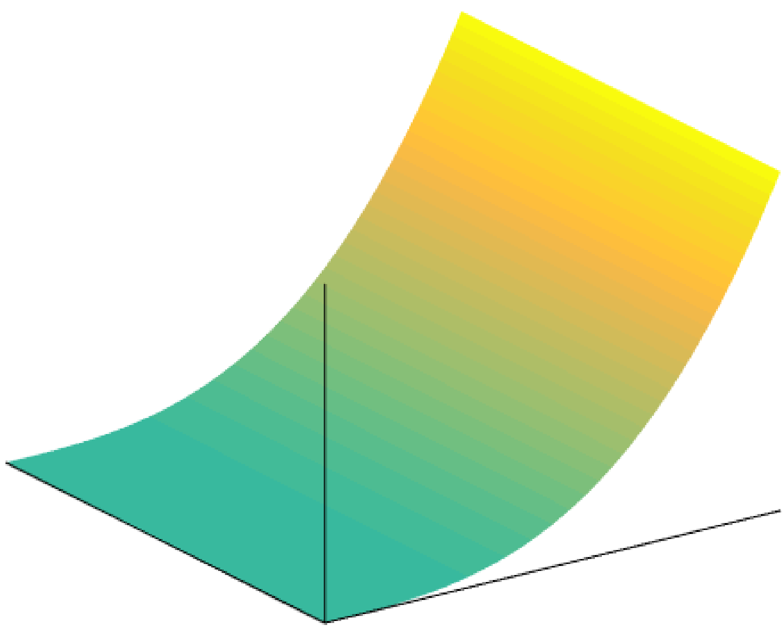


FIGURE 2. The surface $\mathbb{V}(z - x^3)$

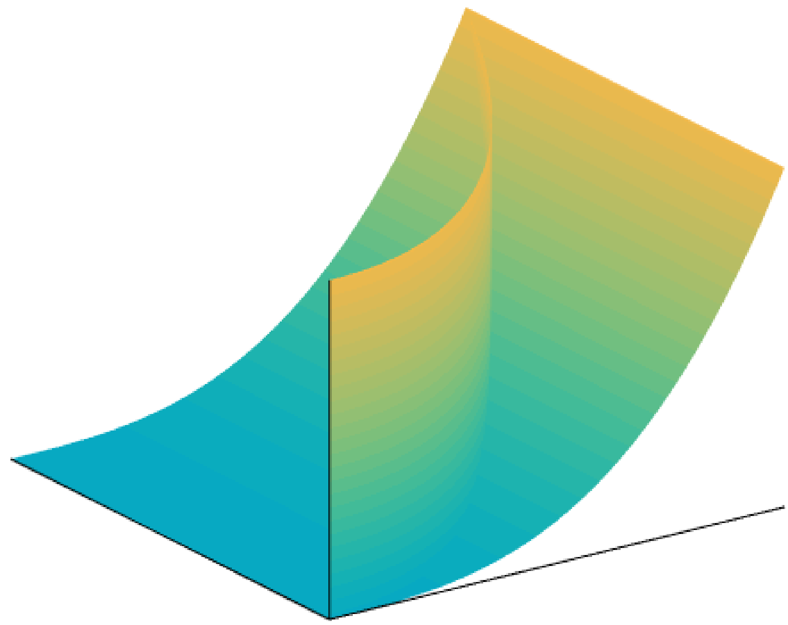


FIGURE 3. The union of the two surfaces, $\mathbb{V}((y-x^2)(z-x^3))$

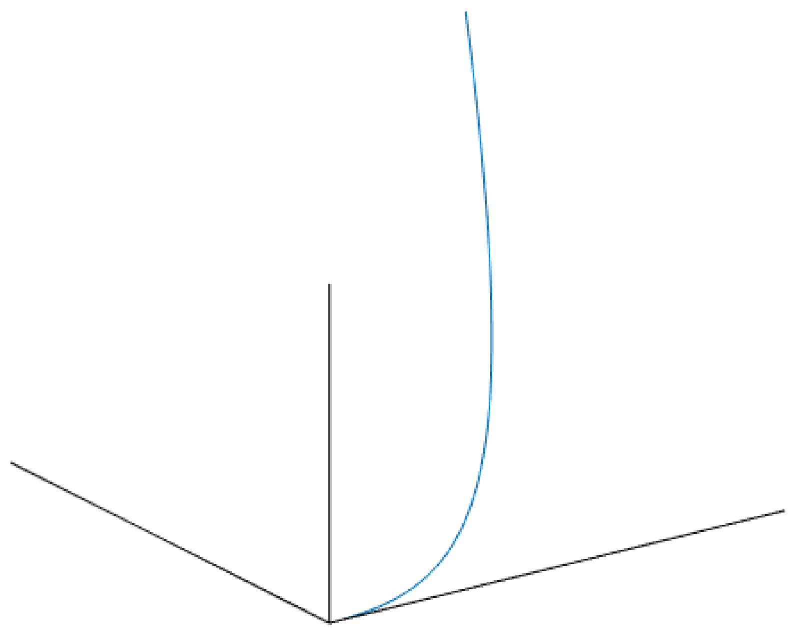


FIGURE 4. The twisted cubic, $\mathbb{V}(y-x^2, z-x^3)$

The last question we should ask about varieties is what sets are *not* varieties. We saw a variety which was just a single point. We can use the above lemma to take a finite union varieties of single points, but we cannot take an infinite union and be certain the resulting set is a variety. As we union more and more points, the degree of a polynomial that vanishes at these points increases and eventually tends to infinity. Since we require our polynomials to be of finite degree, we cannot create a variety that includes only a set of infinitely many separated points. We can always resort to $\mathbb{V}(0)$ which gives us the entire set k^n, but this is not a particularly interesting case.

Aside from disjoint points, one might ask about strange continuous shapes. For example, if we were working in $\mathbb{R}^2$ and we wanted to include every point in the unit disc in our variety, we would be forced to include all of $\mathbb{R}^2$. The reasoning is similar to the one above, in that any polynomial that is zero on the whole unit disc is necessarily zero everywhere. We will explore this topic later when we discuss the *Zariski closure* of a set, which is the smallest variety that contains all the points of a set. But to discuss the Zariski closure, we must first step to the algebra side of algebraic geometry.

3. Ideals

First we define an ideal, and then we start to build a connection between varieties and ideals.

Definition 3.1 (Ideal)**.** A subset $I \subseteq k[x_1, ..., x_n]$ is an **ideal** if:

(1) $0 \in I$.
(2) If $f, g \in I$ then $f + g \in I$.
(3) If $f \in I$ and $h \in k[x_1, ..., x_n]$, then $hf \in I$.

Example 3.2. For a non-example of an ideal, consider all polynomials of even degree in $k[x]$. We can break the ideal properties in two ways. First we can take the polynomials $x^2 + x$ and the polynomial $-x^2$, both of which have even degree. When we add them, we get the polynomial x, which is not of even degree. We can also break the ideal property by multiplying an even degree polynomial by an odd one. Remember, we don't just need the ideal to be closed under multiplication, we need the ideal to be closed under multiplication *by any polynomial in* $k[x]$. So we can take the polynomial x^2 and multiply by $x \in k[x]$, yielding x^3, which is not an even degree polynomial.

Example 3.3. The set $\{0\} \subset k[x_1, ..., x_n]$ is an ideal, as is the entire ring $k[x_1, ..., x_n]$. These are considered the trivial and improper ideals of $k[x_1, ..., x_n]$, respectively.

Example 3.4. For an example of a proper ideal, consider all polynomials which are divisible by $x^2 + 1$. It's an easy exercise to check that the ideal properties hold.

Now we introduce the ideal *generated by* a set of polynomials. This will be the smallest ideal that contains all of the polynomials in our set.

Definition 3.5 (Ideal generated by)**.** Let $f_1, ..., f_s$ be polynomials in $k[x_1, ..., x_n]$. Then the **ideal generated by** $f_1, ..., f_s$ is

$$\langle f_1, ..., f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i \mid h_1, ..., h_s \in k[x_1, ..., x_n] \right\}.$$

We call $f_1, ..., f_s$ a **basis** of the ideal $\langle f_1, ..., f_s \rangle$.

Crucially, the ideal generated by a set of polynomials is, in fact, an ideal. We now will start to consider what happens when we take the variety of an ideal. An ideal is simply a set of polynomials (with certain nice properties) so we are definitely allowed to take the variety of an ideal. As we build more theory, it will be useful to think of $\mathbb{V}$ as a map from the land of ideals to the land of varieties. Since we are planning to take the variety of an ideal, we want to check that our choice of how to represent the ideal does not affect the variety we obtain.

It is sometimes possible to represent an ideal in multiple ways. Suppose we have $f_1, ..., f_s$ and $g_1, ..., g_t$ such that $I = \langle f_1, ..., f_s \rangle = \langle g_1, ..., g_t \rangle$. We might be worried that $\mathbb{V}(f_1, ..., f_s)$ does not equal $\mathbb{V}(g_1, ..., g_t)$, but it is straightforward to see that they are the same. Say there exists a point $a \in k^n$ such that $f_i(a) = 0$ for $1 \leq i \leq s$. Then, by looking at the definition of the ideal generated by $f_1, ..., f_s$, it is clear that $f(a) = 0$ for all $f \in I$. But $g_1, ..., g_t \in I$, so $g_i(a) = 0$ for $1 \leq i \leq t$, and we have that $a \in \mathbb{V}(g_1, ..., g_t)$. This argument can easily be flipped, and we get that $\mathbb{V}(f_1, ..., f_s) = \mathbb{V}(g_1, ..., g_t)$.

It might appear that instead of taking the variety of an ideal, we simply took the variety of the basis of an ideal. It turns out these are one in the same! Clearly if a point is a zero of all polynomials in an ideal, it is a zero of the polynomials that form a basis for that ideal. Going in the other direction, if a point is a zero of all polynomials of a basis for an ideal, we can look at the definition of what it means to be an ideal generated by those polynomials and deduce quickly that the point is a zero for all polynomials in the ideal. Symbolically, $\mathbb{V}(f_1, ..., f_s) = \mathbb{V}(\langle f_1, ..., f_s \rangle)$.

Now we have a map, denoted $\mathbb{V}$, that takes ideals to varieties. We will now define a map going the other way, from the land of varieties to the land of ideals.

Definition 3.6. Let $S \subset k^n$. Define

$$\mathbb{I}(S) = \{f \in k[x_1, ..., x_n] \mid f(a_1, ..., a_n) = 0 \text{ for all } (a_1, ..., a_n) \in S\}.$$

We call $\mathbb{I}(S)$ the **ideal of** S.

Note that (crucially) $\mathbb{I}(S)$ is an ideal for any $S \subseteq k^n$. This gives us a map from the land of varieties back to the land of ideals.

Immediately we have new questions to ask. If one variety sits inside another, what happens when we map over to ideals? What about containments of ideals mapped to varieties? What happens when we map a variety to an ideal and back to a variety again? What happens when we map an ideal to a variety and back to an ideal? We will address all of these questions.

Proposition 3.7. *If I, J are ideals in $k[x_1, ..., x_n]$ with $I \subseteq J$, then $\mathbb{V}(I) \supseteq \mathbb{V}(J)$.*

To see this, consider the definition of the variety map. As the size of the ideal increases, we place further restrictions on the points in the variety, as the points are required to be zeros of a larger number of polynomials.

We should note that one may have $\mathbb{V}(I) = \mathbb{V}(J)$ even if $I \neq J$. As an example, working over $\mathbb{R}$, note that $\mathbb{V}(x^2) = \{0\} = \mathbb{V}(x)$. We produced the same variety from two different ideals. This means that we lose information when taking the variety map. Figuring out why we lost information and how to avoid losing that information will be discussed in future sections. But first, a few notes on the ideal map.

Proposition 3.8. *Let V, W be varieties in k^n. Then:*

(1) $V \subset W$ if and only if $\mathbb{I}(V) \supset \mathbb{I}(W)$.
(2) $V = W$ if and only if $\mathbb{I}(V) = \mathbb{I}(W)$.

We can see that the ideal map behaves in some ways "better" than the variety map. Strict containment is preserved under the map, and equality is now an equivalence as opposed to only a one-way implication.

The proof of the proposition is not difficult. First suppose $V \subseteq W$. Then any polynomial which is zero on all of W must also be zero on V, so $\mathbb{I}(V) \supseteq \mathbb{I}(W)$. Now suppose $\mathbb{I}(V) \supseteq \mathbb{I}(W)$. Since W is a variety there exist $f_1, ..., f_s$ such that $W = \{a \in k^n \mid f_i(a) = 0 \text{ for all } 1 \leq i \leq s\}$. So $f_1, ..., f_s \in \mathbb{I}(W) \subseteq \mathbb{I}(V)$, so all of the f_i's are zero on V. We know W is the collection of *all* of the common zeros of the f_i's, and V is a subset of those common zeros, so $V \subseteq W$. So we have the $V \subseteq W$ if and only if $\mathbb{I}(V) \supseteq \mathbb{I}(W)$. Statement (2) follows directly from what we've proven. Then statement (2) can be used to make the inequality strict, and we're done.

We can use Proposition 3.8 to prove some neat facts about how the ideal map interacts with the operations on varieties we looked at earlier.

Proposition 3.9. *Let V, W be varieties in $k[x_1, ..., x_n]$. Then*

(1) $\mathbb{I}(V \cap W) \supseteq \mathbb{I}(V) \cup \mathbb{I}(W)$.
(2) $\mathbb{I}(V \cup W) \subseteq \mathbb{I}(V) \cap \mathbb{I}(W)$.

We get both statements rather quickly; for the first, $V \cap W$ is a variety inside both V and W, so the ideal generated by such a variety must contain both ideals generated by V and W respectively as per Proposition 3.8. Getting inclusion on the second comes directly from Proposition 3.8 as well.

We will now discuss operations on ideals. Recall that when we first dealt with varieties, we quickly asked questions about what kind of operations we could do with varieties. We showed that intersections and unions of varieties are also varieties. We are now going to look at operations on ideals, but now there is another piece to the puzzle. We will examine not only the operations we can do with ideals, but also how the operations interact with the variety map. But first, the operations for ideals:

Definition 3.10 (Sum of Ideals)**.** If I and J are ideals in $k[x_1, ..., x_n]$ then we define the **sum** of I and J to be

$$I + J = \{f + g \mid f \in I, g \in J\}.$$

A few quick facts about the sum of two ideals:

(1) $I + J$ is also an ideal.
(2) $I + J$ is the smallest ideal containing both I and J.
(3) If $I = \langle f_1, ..., f_s \rangle$ and $J = \langle g_1, ..., g_t \rangle$, then $I + J = \langle f_1, ..., f_s, g_1, ..., g_t \rangle$.

We use the sum of two ideals instead of the union because union does not preserve the ideal property. In other words, the union of two ideals is not necessarily an ideal, so instead we look at the smallest ideal containing the union, which happens to be the sum. Nevertheless, the union of ideals is occasionally brought up, so we will define it briefly.

Definition 3.11 (Union of Ideals)**.** If I and J are ideals in $k[x_1, ..., x_n]$ then we define the **union** of I and J to be

$$I \cup J = \{f \mid f \in I \text{ or } f \in J\}.$$

In other words, the union of two ideals is simply their union as sets. A few quick facts about the union of two ideals:

(1) In general, $I \cup J$ is not necessarily an ideal.
(2) $I \cup J \subseteq I + J$.

We now have the sum, which is in some ways a "nicer" version of the union of two ideals. It turns out the intersection of two ideals is quite useful, so we will discuss the intersection more than the union, but the intersection is still not perfect. First of all, the intersection of two ideals may be very difficult to compute. Because of that, we will first define the product of two ideals, which is contained in the intersection, but is easier to compute.

Definition 3.12 (Product of Ideals)**.** If I and J are ideals in $k[x_1, ..., x_n]$ then we define the **product** of I and J to be the ideal generated by the sum of all polynomials $f \cdot g$ where $f \in I$ and $g \in J$. In set notation,

$$IJ = \left\{ \sum_{i=1}^{r} f_i g_i \mid f_i \in I, g_i \in J, r \text{ some positive integer} \right\}.$$

A few quick facts about the product of two ideals:

(1) IJ is also an ideal.
(2) If $I = \langle f_1, ..., f_s \rangle$ and $J = \langle g_1, ..., g_t \rangle$, then $IJ = \langle f_i g_j \mid 1 \leq i \leq s, 1 \leq j \leq t \rangle$.

Definition 3.13 (Intersection of Ideals)**.** If I and J are ideals in $k[x_1, ..., x_n]$ then we define the **intersection** of I and J to be

$$I \cap J = \{f \mid f \in I, f \in J\}.$$

In other words, the intersection of two ideals is simply their intersection as sets. A few quick facts about the intersection of two ideals:

(1) $I \cap J$ is also an ideal.
(2) $IJ \subseteq I \cap J$.

We will now see what happens when we take the variety map for each of these operations.

Proposition 3.14. *Let I, J be ideals in $k[x_1, ..., x_n]$. Then:*

(1) $\mathbb{V}(I + J) = \mathbb{V}(I \cup J) = \mathbb{V}(I) \cap \mathbb{V}(J)$.
(2) $\mathbb{V}(IJ) = \mathbb{V}(I \cap J) = \mathbb{V}(I) \cup \mathbb{V}(J)$.

The statements are simple, but there is a lot to unpack. Let's first examine statement (1). It is rather easy to show that $\mathbb{V}(I + J) = \mathbb{V}(I \cup J)$. But more importantly, notice we get this really nice comparison with the intersection of varieties that we discussed earlier. We knew before that if V and W were affine varieties, then $V \cap W$ was as well, and we know that there is a set of polynomials which generate each of those varieties. In fact, we can say there is an *ideal* generating each variety, because taking the variety map of a set of polynomials is the same as taking the variety map of the ideal generated by those polynomials. So we can compute the the intersection of the varieties be first doing an operation on those ideals and then taking the variety map! In other words, we have an algebraic tool that lets us do operations on varieties. In fact, it gives a very simple proof of part of Proposition 2.6 by defining the ideal which generates the intersection of the varieties when we take the variety map.

For the second statement there are similar nice properties. First of all, the ideal product acts the same as the intersection of ideals when we take the variety map. Since the ideal product can be calculated, we now have a straightforward way of finding an ideal which constructs the intersection of two varieties when we take the variety map. In other words, we have an algebraic tool which computes intersections of varieties.

The reader might be wondering why we even discuss the intersection of ideals when the product of two ideals seems to accomplish the same thing but is actually computable. It turns out that the intersection of ideals commutes with an operation we call "taking the radical" of an ideal, which will be discussed thoroughly in the next section.

As further motivation for the next section, we should recap what we have so far. We have algebraic objects called ideals and geometric objects called varieties. We have maps that take varieties to ideals and ideals to varieties. On top of that, we can look at Proposition 3.7 and Proposition 3.8 and notice some symmetry in that the inclusions flip when we take the variety map or the ideal map. We say that these maps are inclusion-reversing. Similarly, there is some nice symmetry between Proposition 2.6 and Proposition 3.9 in that the maps flip intersections to unions and unions to intersections. Now we might wonder how close we are to actually having a bijection between ideals and varieties. In other words, when does $\mathbb{I}(\mathbb{V}(I)) = I$ or $\mathbb{V}(\mathbb{I}(V)) = V$? The next section at least partially answers those questions.

4. Radical Ideals, the Nullstellensatz, and the Correspondence between Ideals and Varieties

We begin by noting an interesting property of ideals created by mapping a variety to an ideal with the ideal map. To start, a simple example.

Example 4.1 ($\mathbb{I}(\mathbb{V}(x^n, y^m)) = \langle x, y\rangle$)**.** Consider the variety $\mathbb{V}(x^n, y^m) \subset \mathbb{R}^2$ for some positive integers n, m. After some thought, it should be clear that $\mathbb{V}(x^n, y^m) = \{(0,0)\}$. We know that $x^n = 0$ only when $x = 0$, and $y^m = 0$ only when $y = 0$. So when we map back to the ideal side of things we get $\mathbb{I}(\{(0,0)\}) = \langle x, y\rangle$.

While the above property is nice, it only applies in very specific cases. Can it be extended? Consider the ideal we started with, $\langle x^n, y^m\rangle$. Note that for the ideal we ended with, $\langle x, y\rangle$, we can take any element in that ideal, raise it to a large enough power, and it will be in the original ideal! It's simple to see for the basis elements, x and y, as we simply need to raise them to the power of n and m respectively, but it actually works for any element of the ideal. So in some way $\langle x, y\rangle$ is an extension of $\langle x^n, y^m\rangle$ which contains all polynomials that can be made to lie in $\langle x^n, y^m\rangle$ by raising them to a power. Let's define this property more precisely and more generally.

Definition 4.2 (Radical Ideal)**.** An ideal I is **radical** if $f \in I$ whenever $f^m \in I$ for some $m \geq 1$.

It turns out all ideals created using the ideal map have this property!

Lemma 4.3. *Let V be a variety. Then $\mathbb{I}(v)$ is a radical ideal.*

The proof is very simple. Pick any $a \in V$. If $f^m \in \mathbb{I}(V)$, then $(f(a))^m = 0$, but that implies $f(a) = 0$, so $f \in \mathbb{I}(V)$. We can also take any ideal and extend it to a radical ideal.

Definition 4.4 (Radical of an Ideal)**.** Let $I \subset k[x_1, ..., x_n]$ be an ideal. The **radical of** I is

$$\sqrt{I} = \{f \mid f^m \in I \text{ for some } m \geq 1\}.$$

As one might expect, the radical of I is a radical ideal.

As mentioned briefly at end of the previous chapter, intersections of ideals play nicely with the operation of taking the radical of an ideal. Specifically, the operations commute.

Proposition 4.5 (Radical and Intersections Commute)**.** *If I, J are ideals, then*

$$\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}.$$

For an example of the process of taking the radical of an ideal, we can simply reference the example at the beginning of the section: $\langle x, y\rangle = \sqrt{\langle x^n, y^m\rangle}$. Note that we originally found the ideal $\langle x, y\rangle$ by mapping $\langle x^n, y^m\rangle$ to the variety side of things, and then back to the ideal side of things. This process actually always produces the radical of the original ideal, provided we are in an algebraically closed field. This result is called The Strong Nullstellensatz.

Theorem 1 (The Strong Nullstellensatz)**.** *Let k be an algebraically closed field. If I is an ideal in $k[x_1, ..., x_n]$, then*

$$\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}.$$

The proof is rather long, so it will be skipped entirely. Before moving on to an important consequence of the theorem, we will take a quick look a the Weak Nullstellenstaz, which is used in proving the Strong Nullstellensatz. The proof is also rather involved, so we will skip it, but the result is rather nice.

Theorem 2 (The Weak Nullstellensatz)**.** *Let k be an algebraically closed field. If I is an ideal in $k[x_1, ..., x_n]$ satisfying $\mathbb{V}(I) = \varnothing$, then $I = k[x_1, ..., x_n]$.*

As a consequence of the Strong Nullstellensatz, we have partially answered the question of when $\mathbb{I}(\mathbb{V}(I)) = I$. Specifically, if I is already radical, then taking the radical of I does nothing. Now we just need to discuss when $\mathbb{V}(\mathbb{I}(V)) = V$.

Proposition 4.6. *Let V be an affine variety. Then*

$$\mathbb{V}(\mathbb{I}(V)) = V.$$

Showing $V \subseteq \mathbb{V}(\mathbb{I}(V))$ is very quick, and the other inclusion involves using the inclusion-reversing properties of the ideal and variety maps. Consequently, this proof also shows that $\mathbb{I}$ is one-to-one.

We always have that the maps $\mathbb{V}$ and $\mathbb{I}$ are inclusion reversing, and now we have that $\mathbb{V}(\mathbb{I}(V)) = V$ for any affine variety V, but when we restrict to considering only radical ideals, we got the following beautiful result.

Theorem 3 (The Ideal-Variety Correspondence)**.** *Let k be an algebraically closed field. When we restrict to radical ideals, the maps $\mathbb{I} : \{\text{affine varieties}\} \to \{\text{radical ideals}\}$ and $\mathbb{V} : \{\text{radical ideals}\} \to \{\text{affine varieties}\}$ are mutually inverse, inclusion-reversing bijections.*

The result follows directly from the Strong Nullstellensatz and the previous result about varieties.

At the end of the first section, the idea of Zariski closure was brought up in the context of asking what could *not* be a variety. Another way of asking this question is, given a subset S in k^n, what is the smallest variety that contains S?

Proposition 4.7. *Let $S \subset k^n$. Then $\mathbb{V}(\mathbb{I}(S))$ is the smallest variety that contains S. We call $\mathbb{V}(\mathbb{I}(S))$ the* ***Zariski closure*** *of S, and denote it $\overline{S}$.*

The proof is rather neat. We already know that $\mathbb{V}(\mathbb{I}(S))$ is a variety. Suppose W is a variety and $W \supseteq S$. Then $\mathbb{I}(W) \subseteq \mathbb{I}(S)$ since $\mathbb{I}$ is inclusion reversing. Then $\mathbb{V}(\mathbb{I}(W)) \supseteq \mathbb{V}(\mathbb{I}(S))$ since $\mathbb{V}$ is inclusion reversing. But $\mathbb{V}(\mathbb{I}(W)) = W$ since W is an affine variety. So $W \supseteq \mathbb{V}(\mathbb{I}(S))$, and we're done.

While certainly a cool result, in practice this is difficult to calculate, except in advantageous situations. For example, we know that over the real numbers if a polynomial is zero on an interval, then it is zero everywhere. So if a variety in $\mathbb{R}^n$ contains an open ball in n dimensions, the variety must be all of $\mathbb{R}^n$.

5. Irreducible Varieties and Prime Ideals

In section 2 we showed that unions of affine varieties are affine varieties. Sometimes we can decompose a variety into a union of strictly smaller varieties. For example, $\mathbb{V}(xy) = \mathbb{V}(x) \cup \mathbb{V}(y)$. But then we cannot decompose $\mathbb{V}(x)$ or $\mathbb{V}(y)$ in the same way (assuming we're not working over a finite field). When we cannot decompose varieties into a finite union of strictly smaller varieties we call that variety irreducible.

Definition 5.1 (Irreducible Variety)**.** Let $V \subseteq k^n$ be an affine variety. We call V **irreducible** if the only way to write $V = V_1 \cup V_2$ for some affine varieties V_1, V_2 is with either $V_1 = V$ or $V_2 = V$.

For simple varieties, like $\mathbb{V}(xy)$, it is easy to determine if the variety is irreducible or not. For more complicated varieties, like the twisted cubic we saw earlier, $\mathbb{V}(y - x^2, z - x^3)$, it is more complicated. Can we use our algebraic geometry tools to determine if a variety is irreducible? Yes, we can. We begin with a helpful definition.

Definition 5.2 (Prime Ideal)**.** Let $I \subset k[x_1, ..., x_n]$ be an ideal. We say I is **prime** if whenever $fg \in I$ for some $f, g \in k[x_1, ..., x_n]$, either $f \in I$ or $g \in I$.

The definitions for a prime ideal and irreducible variety are similar in structure, which is a subtle hint towards the following proposition.

Proposition 5.3. *Let $V \subset k^n$ be an affine variety. Then V is irreducible if and only if $\mathbb{I}(V)$ is a prime ideal.*

We have quickly moved the question from checking if a variety is irreducible to checking if an ideal is prime. Now we can prove that the twisted cubic is an irreducible variety. Let $V = \mathbb{V}(y - x^2, z - x^3)$. Note that the twisted cubic is parameterized by (t, t^2, t^3). Suppose $fg \in \mathbb{I}(V)$. Then for all t,

$$f(t, t^2, t^3)g(t, t^2, t^3) = 0.$$

One can show that this implies either $f(t, t^2, t^3)$ or $g(t, t^2, t^3)$ must be the zero polynomial, which implies that either f or g vanishes on V. So $f \in \mathbb{I}(V)$ or $g \in \mathbb{I}(V)$, which proves $\mathbb{I}(V)$ is a prime ideal. Then we simply apply Proposition 5.3 and we're done: the twisted cubic is an irreducible variety.

We now have algebraic tools to check if a variety is irreducible. We have actually stumbled across something even deeper. Suppose briefly that I is a prime ideal and $f^m \in I$ for some polynomial f. Since I is prime, we know that either $f \in I$ or $f^{m-1} \in I$. If $f \notin I$, then $f^{m-1} \in I$. By repeating the argument on f^{m-1}, we get that $f^{m-2} \in I$, and so on, and so on, until eventually the prime property of I forces $f \in I$. This means that every prime ideal is a radical ideal! By combining this fact with Proposition 5.3 and Theorem 3, we get the following corollary.

Corollary 5.4. *Let k be an algebraically closed field. Then the maps $\mathbb{I}$ and $\mathbb{V}$ induce a one-to-one correspondence between irreducible varieties in k^n and prime ideals in $k[x_1, ..., x_n]$.*

Those familiar with ring theory will be familiar with maximal ideals. An ideal being maximal is a stronger requirement than an ideal being prime in the sense that all maximal ideals are prime ideals. Because of that, there are some useful algebraic geometry concepts which involve maximal ideals.

Definition 5.5. Let $I \subset k[x_1, ..., x_n]$ be a proper ideal. We say I is **maximal** if whenever an ideal $J \supseteq I$, either $J = I$ or $J = k[x_1, ..., x_n]$.

In other words, a maximal ideal is a proper ideal that is maximal under inclusion of proper ideals. As mentioned earlier, it is a well known fact from ring theory that all maximal ideals are prime ideals.

Proposition 5.6. *If k is any field, every maximal ideal in $k[x_1, ..., x_n]$ is prime.*

For a specific example of a maximal ideal, we have the following proposition.

Proposition 5.7. *If k is any field, any ideal $I \subset k[x_1, ..., x_n]$ of the form*

$$I = \langle x_1 - a_1, ..., x_n - a_n \rangle$$

where $a_1, ..., a_n \in k$, is maximal.

Note, if I is such an ideal, $\mathbb{V}(I) = (a_1, ..., a_n) \in k^n$. In other words, such a maximal ideal corresponds to a point in k^n. When is this correspondence one-to-one? The following theorem gives us a clue.

Theorem 4. *If k is an algebraically closed field, then every maximal ideal in $k[x_1, ..., x_n]$ is of the form $\langle x_1 - a_1, ..., x_n - a_n \rangle$ for some $a_1, ..., a_n \in k$.*

This theorem quickly yields the following corollary,

Corollary 5.8. *If k an algebraically closed field, there is a one-to-one correspondence between maximal ideals in $k[x_1, ..., x_n]$ and points in k^n.*

In this section we have explored more properties of the ideal and variety maps we created in the earlier sections and found some very powerful results in the Nullstellensatz and the ideal-variety correspondence when we restrict to radical ideals. We also examined an even stronger correspondence when we looked at just prime or just maximal ideals. These maps are very interesting, and we have discovered many neat properties on the algebra side of things, but so far we have not played too much with the geometry. We have only been looking at affine varieties in affine space. In the next section we examine projective space and projective varieties. Wonderfully, many of our results still hold (with some minor modifications) and sometimes we actually get even nicer properties!

6. Projective Space and the Projective Ideal-Variety Correspondence

Projective space comes up in many areas of mathematics. There are many ways to introduce the ideas of projective space. We will focus on two. The first method is most naturally brought up when considering intersections of lines. The following statement should be familiar when working in $\mathbb{R}^n$:

In $\mathbb{R}^n$, any two non-parallel lines intersect at exactly one point.

To construct projective space, we make this true for any two lines and remove the non-parallel hypothesis. Where do parallel lines intersect? We say they intersect *at infinity.* So to construct projective space from Euclidean space ($\mathbb{R}^n$), we add a set of points at infinity.

Note that parallel lines intersect at *a* point at infinity. It might seem tempting to say that the lines $y = x$ and $y = x + 1$ intersect once at "positive infinity" and once at "negative infinity" (if such things could be defined in multiple dimensions), but remember that we want any two lines to intersect at *exactly one point.* So either way that we move along the line, we are moving toward the same point at infinity.

To form a clearer picture, let's examine 2-dimensional projective space over the real numbers. We can (and will) extend our definition to be over any field, but the real numbers are more familiar for most people. Notationally, we say that $\mathbb{P}^2(\mathbb{R})$ is 2-dimensional projective space over the real numbers.

We start with good old $\mathbb{R}^2$. Now, we want to add a point at infinity for each set of parallel lines. Loosely, $\mathbb{P}^2(\mathbb{R}) = \mathbb{R}^2 \cup \{\text{one point for each equivalence class of parallel lines}\}$. Conveniently, we can use slope as a representative for each equivalence class of parallel lines, as any two parallel lines have the same slope. An astute reader might notice that slope can take any real value as well as ∞. That certainly seems like a copy of $\mathbb{R}^1$ with a point at infinity, which seems like it might be $\mathbb{P}^1(\mathbb{R})$. And in fact it is! So, loosely, $\mathbb{P}^2(\mathbb{R}) = \mathbb{R}^2 \cup \mathbb{P}^1(\mathbb{R})$. This generalizes to higher dimensions as well, where $\mathbb{P}^n(\mathbb{R}) = \mathbb{R}^n \cup \mathbb{P}^{n-1}(\mathbb{R})$.

The first way of thinking about projective space (which we just saw) is very useful when considering intersections of lines and curves in space. The second will provide another geometric view of projective space and will more easily allow for coherently labeling the points of n-dimensional projective space. We will also take this opportunity to rigorously define projective space over *any* field k, although it is perhaps easiest to imagine over the real numbers.

Definition 6.1 (n-dimensional projective space over any field k)**.** Let k be a field. **Projective space over k of dimension n** is

$$\mathbb{P}^n(k) = (k^{n+1} \setminus \{0\}) / \sim$$

where $(x_0, x_1, ..., x_n) \sim (x'_0, x'_1, ..., x'_n)$ if and only if there exists a $\lambda \in k, \lambda \neq 0$, such that $(x_0, x_1, ..., x_n) = \lambda(x'_0, x'_1, ..., x'_n)$.

Each non-zero $(n+1)$-tuple $(x_0, ..., x_n) \in k^{n+1}$ defines a point p in $\mathbb{P}^n(k)$, and we call $(x_0, ..., x_n)$ the homogeneous coordinates of p.

The definition may seem complicated, but hopefully the following observation will help make things clearer. The points are considered equivalent under the equivalence relation $\sim$ if and only if they are on the same line through the origin. So,

$$\mathbb{P}^n(k) \simeq \{\text{lines through the origin in } k^{n+1}\}$$

The fact that this definition is equivalent to the first interpretation of projective space may not be intuitively obvious. Let's examine the case of $\mathbb{P}^2(\mathbb{R})$ again and piece them together.

Picture $\mathbb{R}^3$. Now add the plane defined by $z = 1$ to the picture (Note a plane is a copy of $\mathbb{R}^2$). Notice that almost all lines that pass through the origin in $\mathbb{R}^3$ also pass through that plane at some point. If we let the points of the plane at $z = 1$ be our representatives for the lines through the origin which intersect the plane, we now have our copy of $\mathbb{R}^2 \subset \mathbb{P}^2(\mathbb{R})$. Now we just need to account for the points "at infinity" as we described them earlier. Consider the lines which do *not* intersect the plane $z = 1$. Those lines have to live entirely in the xy-plane. By considering the xy-plane as $\mathbb{R}^2$, we can uniquely identify each line with a slope as we did above, again giving us a copy of $\mathbb{P}^1(\mathbb{R})$. So, at least for $\mathbb{P}^2(\mathbb{R})$, we have successfully translated our new definition to the old one.

We will now discuss some important aspects of the homogeneous coordinates as we defined them above. The most important thing to keep in mind is that the homogeneous coordinates exist in $k^{n+1}\backslash\{0\}$, meaning that we must ensure that our coordinate is not the zero vector. The easiest way to ensure this is to fix a coordinate to be nonzero. For example, suppose we are working in $\mathbb{P}^n(k)$, and fix $x_0 = a \neq 0$, so x_0 is our nonzero coordinate. Note that we can then divide each coordinate by a and obtain the same point, since we say that two points, $(x_0, ..., x_n)$ and $(x'_0, ..., x'_n)$ are equal if there exists a $\lambda \neq 0$ such that $(x_0, ..., x_n) = \lambda(x'_0, ..., x'_n)$. In this case, we are simply setting $\lambda = a$. So, without loss of generality, we can fix $x_0 = 1$. Now we are examining the following set of coordinates:

$$\{(1, x_1, ..., x_n) \mid x_1, ..., x_n \in k\}$$

Note this looks exactly like k^n. Now we notice that when we fixed x_0 to be non-zero, we threw out many points. Specifically, we threw out the points that had $x_0 = 0$. After some careful thought, it should be clear that $\mathbb{P}^n(k)\backslash\{(1, x_1, ..., x_n) \mid x_1, ..., x_n \in k\} \simeq \mathbb{P}^{n-1}(k)$. To see this, consider that we started with $n+1$ coordinates that must not all be zero (and with an equivalence relation), and now we have n coordinates that must not all be zero (and with the same equivalence relation). These remarks lead us to make the following definition and observations.

Definition 6.2. For each $i = 0, ..., n$, let

$$U_i = \{(x_0, ..., x_n) \in \mathbb{P}^n(k) \mid x_i \neq 0\}.$$

Then:

(1) $U_i \simeq k^n$.
(2) $(\mathbb{P}^n(k) \backslash U_i) \simeq \mathbb{P}^{n-1}(k)$.
(3) $\mathbb{P}^n(k) = \cup_{i=0}^n U_i$.

Now we want to define varieties in projective space. Importantly, we must restrict to a certain subset of polynomials, the reason for which will be clear shortly. First, recall that we defined a polynomial as a finite sum of monomials, and each monomial has a total degree.

Definition 6.3 (Homogeneous Polynomial)**.** We say that a polynomial f is **homogeneous** if f is a finite linear combination of monomials of the same total degree α.

Why do we need each monomial to have the same total degree? Consider that we want the polynomial to be well-defined in projective space, and in projective space two points are considered the same if there is a non-zero constant $\lambda \in k$ such that one point is equal to λ times the other. When we calculate $f(\lambda x_0, ..., \lambda x_n)$ for some homogeneous polynomial f, each monomial term pops out a factor of λ^α in front. We can then factor the λ^α term out, and noting that $\lambda^\alpha \neq 0$, we can conclude that $f(x_0, \ldots, x_n) = 0$ if and only if $f(\lambda x_0, \ldots, \lambda x_n) = 0$. In other words, while the *value* of polynomial at a point in projective space is not well defined, whether or not a homogeneous polynomial *vanishes* at a point is well defined.

Now that we have well-defined polynomials in projective space, we can define projective varieties the same as we did affine varieties (except now we require all polynomials be homogeneous).

Definition 6.4 (Projective Variety)**.** Let k be a field. Let $f_1, ..., f_s \in k[x_0, ..., x_n]$ be homogeneous polynomials. We define

$$\mathbb{V}(f_1, ..., f_s) = \{(a_0, ..., a_n) \in \mathbb{P}^n(k) \mid f_i(a_0, ..., a_n) = 0 \text{ for all } 0 \leq i \leq s\}.$$

We call $\mathbb{V}(f_1, ..., f_s)$ the **projective variety** defined by $f_1, ..., f_s$.

Note that if we restrict to any part of $\mathbb{P}^n(k)$ which "looks like" k^n, we obtain an affine variety. More precisely, $\mathbb{V}(f_1, ..., f_s) \cap U_i$ can be identified with an affine variety. So, in a sense, we are working over a larger space than k^n, and the results from projective space trickle down to affine space. So all of the results we obtain in projective space imply similar results in affine space.

One might be concerned that the homogeneous polynomial requirement changes things significantly. But actually, any affine variety can be made to sit in projective space in the following way. (We will not go through all of the precise details, but the idea should be clear). Consider any affine variety V in k^n. There is a set of polynomials, all defined on coordinates $(x_1, ..., x_n)$, used to define the variety. Consider any one polynomial f in that set. The polynomial f is a finite linear combination of monomials, each of possibly different total degrees. But, we know there is some maximum total degree α of the monomials in f. Take any term with total degree less than α and multiply it by x_0^d where d is whatever power is required to make the total degree exactly equal α. Do this for each polynomial defining V, and suddenly we have a set of homogeneous polynomials which exactly correspond to the non-homogeneous ones if we set $x_0 = 1$. Clearly we can define a projective variety using these new homogeneous polynomials, and when we restrict to $x_0 = 1$ (or in other words restrict to U_0), we obtain the original variety. So our results in projective space *do* in fact trickle down to affine space.

Now that we have varieties, we want to find corresponding ideals and rebuild the ideal-variety correspondence, but now in projective space. We start be defining a homogeneous ideal, which is required to work over projective space.

Definition 6.5 (Homogeneous Ideal)**.** Let $I \subset k[x_0, ..., x_n]$ be an ideal. We say that I is a **homogeneous ideal** if $I = \langle f_1, ...f_s \rangle$ for some homogeneous polynomials $f_1, ..., f_s$.

But wait! Ideals are closed under addition, and if we add two homogeneous polynomials of different total degree we obtain a non-homogeneous polynomial. So I contains many non-homogeneous polynomials. Is that okay? It turns out it is. While any polynomial in I may not be homogeneous, it is the linear combination of homogeneous polynomials. So, if the homogeneous polynomials are zero on some projective variety, the linear combination of those homogeneous polynomials are also zero on the same projective variety.

Note it is possible to define a homogeneous ideal in another way, by considering "homogeneous components" of each $f \in I$, but there is a theorem which states the two definitions are equivalent. The above definition is good enough for our purposes, and a bit simpler to understand.

In projective space, we obtain many of the same results we did for affine space. First we note that taking the variety map of a homogeneous ideal is the same as taking the variety map of a basis for that ideal. This should seem familiar from the affine case.

Proposition 6.6. *Suppose $f_1, ..., f_s \in k[k_0, ..., x_n]$ are homogeneous polynomials. Let $I = \langle f_1, ..., f_s \rangle$. Then $\mathbb{V}(I) = \mathbb{V}(f_1, ..f_s)$. So $\mathbb{V}(I)$ is a projective variety.*

Now, just like in affine space, we want to define an ideal map which takes us back from varieties to (homogeneous) ideals.

Proposition 6.7. *Let $V \subset \mathbb{P}^n(k)$ be a projective variety. Let*

$$\mathbb{I}(V) = \{f \in k[x_0, ..., x_n] \mid f(a_0, ..., a_n) = 0 \text{ for all } (a_0, ..., a_n) \in V\}.$$

If k is an infinite field, then $\mathbb{I}(V)$ is a homogeneous ideal.

This map is defined the same way as in the affine case, except now we get a homogeneous ideal since we started with a projective variety. Similarly to the affine case, we now get a correspondence between certain homogeneous ideals and projective varieties.

Theorem 5. *Let k be an infinite field. Then the maps $\mathbb{V}$: {homogeneous ideals $\to$ projective varieties} and $\mathbb{I}$: {projective varieties $\to$ homogeneous ideals} are inclusion reversing. Also, for any projective variety V, we have $\mathbb{V}(\mathbb{I}(V)) = V$. In particular, $\mathbb{I}$ is one-to-one.*

We define irreducible varieties exactly the same as we did in the affine case. We get that every projective variety can be expressed uniquely as a union of irreducible projective varieties. We also define the radical of a homogeneous ideal exactly as before. Usefully, we get that the radical of a homogeneous ideal is also homogeneous.

Recall the Weak and Strong Nullstellensatz from the affine case. We get the following corresponding theorems in the projective case:

Theorem 6 (The Projective Weak Nullstellensatz)**.** *Let k be an algebraically closed field and let $I \subset k[x_0, ..., x_n]$ be a homogeneous ideal. Then the following are equivalent:*

(1) $\mathbb{V}(I) \subset \mathbb{P}^n(k)$ is empty.
(2) For each $0 \leq i \leq n$, there exists an integer $m_i \geq 0$ such that $x_i^{m_i} \in I$.
(3) There is some $r \geq 1$ such that $\langle x_0, ..., x_n \rangle^r \subset I$.

Theorem 7. *Let k be an algebraically closed field and let $I \subset k[x_0, ..., x_n]$ be a homogeneous ideal. If $V = \mathbb{V}(I)$ is a nonempty projective variety in $\mathbb{P}^n(k)$, then $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$.*

The previous theorems lead to the following correspondence:

Theorem 8. *Let k be an algebraically closed field. If we restrict to non-empty projective varieties and radical homogeneous ideals properly contained in $\langle x_0, ..., x_n \rangle$, then the maps*

$$\mathbb{V} : \{\text{radical hom. ideals properly contained in } \langle x_0, ..., x_n \rangle\} \to \{\text{nonempty proj. varieties}\}$$

and

$$\mathbb{I} : \{\text{nonempty proj. varieties}\} \to \{\text{radical hom. ideals properly contained in } \langle x_0, ..., x_n \rangle\}$$

are mutually inverse, inclusion-reversing bijections.

Notice in the projective case we did not have to mess with prime ideals! That is an instance of things working "better" in projective space. At this point we have completed the ideal-variety correspondence in projective space.

7. Bézout's Theorem

We conclude with a nice result called *Bézout's Theorem*, which deals with intersections of curves in projective space. The precise statement would require many new definitions, so instead we will sketch the idea of the theorem. In projective space, we have the property that any two lines intersect at a point. Bézout's Theorem extends this result to higher degree polynomials and curves. Specifically, if one curve is defined by a polynomial of degree n, and another defined by a polynomial of degree m, then they will generally intersect at mn points (if we account for multiplicity!). There are select cases where the multiplicity matters. We will illustrate when multiplicity is important with the following example. Picture an ellipse and a parabola. It should be easy to imagine a case where they intersect at 4 points in affine space (accounting for all mn intersection points). If we place the vertex of the parabola inside of the ellipse, it is easy to see that there are two intersections in the affine case, and it turns out we get two intersections at infinity in the projective case. The issue of multiplicity comes up when the vertex of the parabola is tangential to the ellipse. Here we have only one intersection, but in a way it is the "limit" of two intersections coming together. If we double count that intersection, because it has multiplicity two, we retain the 4 intersections we expect. Bézout's Theorem is a precise way of saying that as long as multiplicity is accounted for, two curves of degree n and m intersect at mn points in projective space.

References

[CLO] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms, 3e*, Spring (2007), 551pp.