Polynomial and Rational Functions on a Variety

Piyush Patil

December 10, 2016

In this chapter, we'll study the algebraic properties of polynomials and rational functions on affine varieties, and their ramifications for the geometric properties of varieties. In just about every domain of mathematics the concept of mappings between structures or spaces, especially those that preserve certain properties, are of great interest (e.g. isomorphisms between groups, linear transformations between vector spaces, etc.). We'll look at polynomial and rational mappings between varieties as extensions of linear transformations, and the resulting theory will add another chapter to the algebra-geometry dictionary from the last chatper.

1 Polynomial Mappings

Before introducing polynomial mappings, recall that we've already studied certain examples of such mappings. For instance, polynomial parameterizations can be viewed as polynomial mappings themselves, seeing as they are mappings between varieties (though often with domain $\mathbb{R}^n$, which can be viewed as the degenerate variety $\mathbf{V}(0)$) with polynomial components. Moreover, the projection mapping π_l trivially has polynomial components (since $\pi_l(a_1, \cdots, a_n) = (a_{l+1}, \cdots, a_n)$) and is a mapping from the variety of an ideal $\mathbf{V}(I)$ to a subset of the variety $\mathbf{V}(I_l)$, where I_l is the l^{th} elimination ideal of I.

(Definition) Polynomial mapping: *Let $V \subset F^n, W \subset F^m$ be varieties. A function $\phi : V \to W$ is a* ***polynomial mapping*** *if*

$$\phi(a_1, \cdots, a_n) = (f_1(a_1, \cdots, a_n), \cdots, f_m(a_1, \cdots, a_n))$$

for polynomials $f_1, \cdots, f_m$. Then we also say that the tuple of polynomials $(f_1, \cdots, f_m)$ ***represents*** *ϕ, and the specific polynomials are* ***components*** *of ϕ.*

Notice that if the polynomial mapping ϕ is represented by $(f_1, \cdots, f_m)$ between varieties V and W, then there are certain restrictions on what the components of ϕ can be in order to maintain it as a mapping from V to W. This is because every point $(f_1(a_1, \cdots, a_n), \cdots, f_m(a_1, \cdots, a_n))$, for $(a_1, \cdots, a_n) \in V$, in the range of ϕ must satisfy the defining equations of W. That is, if $W = \mathbf{V}(g_1, \cdots, g_t)$ then we must have

$$g_1(f_1(a_1, \cdots, a_n), \cdots, f_m(a_1, \cdots, a_n)) = \cdots = g_t(f_1(a_1, \cdots, a_n), \cdots, f_m(a_1, \cdots, a_n)) = 0$$

One convenient consequence of our definition of polynomial mappings is that by studying polynomial mappings between V and W for $W = F$, which are merely just regular polynomial functions, we can understand many properties of general polynomial mappings from V to F^m, since any general polynomial mappings are biult out of m polynomial functions.
Although in this single-dimensional case we don't need to worry about finding representations of polynomial mappings (since they're given by polynomial functions), it's important to note that polynomial mappings don't correspond one-to-one with polynomial functions. That is, multiple (indeed, often infinitely many) polynomial functions often represent the same polynomial mapping. This can be made clear by considering that for a polynomial mapping ϕ from affine variety V to F represented by polynomial function f, polynomial functions given by

$$f + g, g \in \mathbf{I}(V)$$

also represent ϕ, since by design g is zero at every point of V and thus adding it to f doesn't affect ϕ, because the domain of ϕ is V. To extend this idea, we introduce the following result.

(Theorem) Polynomial mappings are represented by polynomials modulo ideals: *Let $V \subset F^n$ be an affine variety. Then the polynomials $f, g \in F[x_1, \cdots, x_n]$ represent the same polynomial mapping from V to F if and only if $f - g \in \mathbf{I}(V)$. More generally, the polynomial tuples $(f_i), (g_i)$, for $1 \leq i \leq m$, represent the same polynomial mapping from V to F^m if and only if $f_i - g_i \in \mathbf{I}(V), \forall i$.*

- *Proof*: If $f - g \in \mathbf{I}(V)$ then for every $a \in V$, $f(a) - g(a) = 0$. This means that $f(a) = g(a), \forall a \in V$, which means f and g represent the same mapping over V. Conversely, if f, g represent the same mapping, then we must have $f(a) = g(a)$ for every $a \in V$, by definition, which means $f(a) - g(a) = 0$ which implies $f - g \in \mathbf{I}(V)$. □

Notice that this implies that polynomial mappings are uniquely represented by polynomials if and only if $\mathbf{I}(V) = \{0\}$, which is only the case if F is infinite and $V = F^n$. There are two potential ways to deal with this ambiguity of representations of polynomial mappings: we could lump together all the representations of a polynomial mapping into a set and treat the set as a structure in its own right, as some kind of aggregate representation of the mapping, or we could try to define some notion of the simplest possible representation of a mapping and use that as the canonical representation. We'll introduce both of these concepts. Before proceeding, we introduce some notation - let $F[V]$ denote the set of polynomial mappings taken from V to F. If we define sum and product operations on $F[V]$ with

$$\forall a \in V : (\phi + \psi)(a) = \phi(a) + \psi(a), (\phi\psi)(a) = \phi(a)\psi(a)$$

for $\phi, \psi \in F[V]$. It's not difficult to see that all the usual sum and product properties for polynomials in $F[x_1, \cdots, x_n]$ extend to $F[V]$, which means $F[V]$ is a commutative ring. Let's look at what we can learn about the geometric properties of V by studying $F[V]$.

The precise algebraic structure of $F[V]$ tells us about the reducibility of V. Specifically, if $F[V]$ displays multiplicative pathological behavior, then the underlying variety V is reducible, where by pathological behavior we specifically refer to the product of non-zero elements being zero (in well-behaved rings, of course, we expect that the product of elements can only be zero if one of the elements is zero). This is because if V is reducible as $V = V_1 \cup V_2$, then we can find polynomials which are zero over V_1 but not V_2, say f_1, and likewise polynomials which are zero over V_2 but not V_1, say f_2 (f_1 and f_2 must exist since V_1, V_2 are distinct varieties not contained in each other, because V is reducible). Then neither f_1 nor f_2 is zero over $V_1 \cup V_2 = V$, but their product is, which means the polynomial mappings represented by f_1 and f_2 are the multiplicative pathological elements referred to earlier. The specific term for rings which don't display this pathological behavior is defined below.

(Definition) Integral domain: *A commutative ring R is an **integral domain** if*

$$\forall r, s \in R : rs = 0 \to r = 0 \text{ or } s = 0$$

Thus, it follows that V is irreducible if and only if $F[V]$ is an integral domain. The reason $F[V]$ not being an integral domain is sufficient for V to be reducible is that if f_1, f_2 are non-zero polynomials whose product is zero over V, then we can factor V into

$$V = (V \cap \mathbf{V}(f_1)) \cup (V \cap \mathbf{V}(f_2))$$

2 Quotients of Polynomial Rings

We've already seen that two polynomials represent the same mapping whenever their difference is zero over the domain (and that this extends to mappings represented by an arbitrary number of polynomials), which is reminiscent of modular arithmetic from number theory, in which two integers are "the same" (i.e. congruent) if their difference is zero when the base is divided out. Modular arithmetic is deeply related to the operation of division and factoring, and in group theory the idea is extended and applied to groups, forming quotient groups. Quotient groups are essentially groups formed from a base group G "modulo" another group H; specifically, the structure is given by lumping together elements that are "congruent modulo H" in the sense that both elements lie in the same coset of H, similar to how modular reductions are formed by lumping together integers which are congruent modulo the base.

The construction of $F[V]$ in the last section can be viewed as a special case of the above group theoretic idea of a quotient, since we formed $F[V]$ by lumping together polynomials which are "congruent modulo an ideal I", in the sense that their difference is in I, where $I = \mathbf{I}(V)$. In this section we'll extend the theory of quotients of polynomial rings, and consider their applications to answering the question of how to resolve the ambiguity in polynomial representations of mappings.

(Definition) Congruent: *Given an ideal I, polynomials f, g are **congruent modulo** I if $f - g \in I$.*

- *Notation*: If f, g are congruent modulo I, we write $f \equiv g \pmod{I}$. The main reason this definition is useful is that it defined an equivalence relation on $F[x_1, \cdots, x_n]$.

The fact that congruence modulo an ideal is an equivalence relation is significant. Any equivalence relation on a set partitions the set into disjoint subsets known as equivalence classes, since the subsets are formed by lumping all equivalent elements together. For the ideal I, we denote the equivalence class of polynomial f with

$$[f] = \{g \in F[x_1, \cdots, x_n] \text{ s.t. } g \equiv f \pmod{I}\}$$

In accordance with our motivation, when its the case that $I = \mathbf{I}(V)$ for some variety V, polynomials f and g are congruent modulo I if and only if they define the same mapping over V. Thus, the equivalence class $[f]$ is the "lumping together" of all the ambiguous representations of a polynomial mapping that we alluded to in the last section.

(Theorem) Polynomial equivalence classes define mappings: *Polynomial mappings $\phi : V \to F$ bijectively correspond to the equivalence classes of polynomials under congruence modulo $\mathbf{I}(V)$.*

- *Proof*: This is a direct corollary of congruence modulo $\mathbf{I}(V)$ being an equivalence relation.

We can now extend the idea of group theoretic quotients to polynomial ideals. Intuitively, we want to partition the full polynomial space $F[x_1, \cdots, x_n]$ into disjoint lumps which are the "multiples" of I, extending the intuitive notion of dividing the space by the ideal.

(Definition) Ideal quotient: *The* ***quotient*** *of $F[x_1, \cdots, x_n]$ modulo I, denoted $F[x_1, \cdots, x_n]/I$, is the set of equivalence classes modulo I:*

$$F[x_1, \cdots, x_n]/I = \{[f] \text{ for } F[x_1, \cdots, x_n]\}$$

Notice that this resolves the ambiguity in which polynomials represent a polynomial mapping. However, quotient ideals are interesting mathematical structures in their own right, and we may ask if we can treat equivalence classes as polynomial-like objects in their own right. To do so, we need to define some notion of addition and multiplication on equivalence classes. A natural formulation is

$$[f] + [g] = [f + g], [f][g] = [fg]$$

It can be proven that the above operations are *well-defined*, meaning that if we chose different $f' \in [f], g' \in [g]$ then we would still have

$$[f'] + [g'] = [f' + g'], [f'][g'] = [f'g']$$

It follows that $F[x_1, \cdots, x_n]/I$ is itself a commutative ring under the above operations.
We motivated the entire concept of quotient ideals with the starting example of $F[V]$, regarding both as a way to extend the idea of division and group theoretic quotients to polynomials and ideals. To connect these ideas with affine varieties, we'll show that not only was $F[V]$ our motivation for quotient ideals, but that the two are actually intimately related - in some sense, $F[V]$ and $F[x_1, \cdots, x_n]/\mathbf{I}(V)$ are actually the same ring (specifically, the two are isomorphic).

(Theorem) $F[V]$ and $F[x_1, \cdots, x_n]/\mathbf{I}(V)$ are isomorphic: *There exists a bijective correspondence between $F[V]$ and $F[x_1, \cdots, x_n]$ which preserves the addition and multiplication operations on equivalence classes.*

- *Proof*: To prove this, we constructively provide such a bijection. Let $\Phi : F[x_1, \cdots, x_n]/\mathbf{I}(V) \to F[V]$ be the mapping given by

$$\forall [f] \in F[x_1, \cdots, x_n]/\mathbf{I}(V) : \Phi([f]) = \phi$$

where ϕ is the polynomial mapping represented by f. Every mapping has a polynomial representation, so Φ is surjective. Moreover, if $\Phi([f]) = \Phi([g])$ then f and g represent the same mapping, which means $f \equiv g \pmod{()\mathbf{I}(V)}$, which means $[f] = [g]$, proving that Φ is also injective, and hence bijective. To prove that Φ preseves the equivalence class operations above, we have

$$\Phi([f] + [g]) = \Phi([f + g]) = \phi + \psi = \Phi([f]) + \Phi([g])$$

where ϕ, ψ are the mappings represented by f, g, respectively. Thus, Φ preserves addition. Similarly,

$$\Phi([f][g]) = \Phi([fg]) = \phi\psi = \Phi([f])\Phi([g])$$

so that Φ also preserves multiplication. □

Since $F[x_1, \cdots, x_n]/I$ is a ring in its own right, we might consider its ideals and their relationship to ideals of I. Recall that an ideal of a commutative ring is defined as any set which contains 0 and is closed under addition and scalar multiplication. It turns out that there's a close relationship between polynomial ideals and ideals of a quotient; similar to the isomorphism theorems from group theory, the two structures are intimately related.

(Theorem) Ideals of quotient ideal are isomorphic to polynomial ideals: *Let I be an ideal of $F[x_1, \cdots, x_n]$. Then the ideals of $F[x_1, \cdots, x_n]/I$ are in bijective correspondence with the ideals of $F[x_1, \cdots, x_n]$ which contain I.*

- *Proof*: Let J be an ideal of $F[x_1, \cdots, x_n]$ containing I; we'll first show that J uniquely corresponds to some ideal of $F[x_1, \cdots, x_n]/I$. Let J/I denote the set TODO

Notice that it follows as a corollary that, as with the Hilbert basis theorem, ideals in $F[x_1, \cdots, x_n]/I$ are finitely generated.

3 Algorithmic Computations in $F[x_1, \cdots, x_n]/I$

In this section, we study more explicit, constructive methods of describing ideals of a quotient ring. We'll use the division algorithm to find representative polynomials for an equivalence class, giving us a canonical representation of a polynomial

mapping. These representatives will also help us develop explicit methods for computing sum and product operations in a polynomial quotient ring. The main property of the division algorithm we'll use here is that the remainder of the division of a polynomial f by a Groebner basis G is uniquely determined by f. It's unsurprising that we're investigating remainders on polynomial division, since quotient ideals can be viewed as "dividing out" certain polynomials. Throughout the section, we'll be revisiting the monomial ideal $\langle \mathrm{LT}(I)\rangle$, for an ideal I, as well as its complement $\langle \mathrm{LT}(I)\rangle^C = \{x^\alpha \notin \langle \mathrm{LT}(I)\rangle\}$.
First, we reframe the following basic observation on the division algorithm.

(Theorem) Remainders and congruence: *Fix a monomial ordering on $F[x_1, \cdots, x_n]$, and let I be an ideal of $F[x_1, \cdots, x_n]$. Then*

1. Every $f \in F[x_1, \cdots, x_n]$ is congruent to a unique polynomial r, and r is a linear combination, over F, of monomials in $\langle \mathrm{LT}(I)\rangle^C$.
2. The elements of $\langle \mathrm{LT}(I)\rangle^C$ are linearly independent modulo I, in the sense that

$$\sum_\alpha c_\alpha x^\alpha \equiv 0 \pmod I \iff \forall \alpha : c_\alpha = 0$$

for $x^\alpha \in \langle \mathrm{LT}(I)\rangle^C$.

- *Proof*: Let G be a Groebner basis for I, and let r be the remainder of the division of f by G. Then for some $q \in I$,

$$f = q + r$$

Hence, $f - r = q \in I \to f \equiv r \pmod I$. The fact that r is a linear combination of monomials not in $\langle \mathrm{LT}(I)\rangle$ follows from the division algorithm theorems we covered early on, as does the uniqueness of r.
The second part of the theorem is obvious, since a polynomial is congruent to zero modulo an ideal if and only if, by definition, it's contained in the ideal, and by definition none of the elements in the sum

$$\sum_\alpha c_\alpha x^\alpha$$

are in $\langle \mathrm{LT}(I)\rangle$. Thus, the only way the above sum could be in I is if the c_α were degenerate, giving the zero polynomial. □

- *Intuition*: The first part of the theorem reinforces our intuition on quotient ideals and polynomial congruence modulo an ideal by showing that as with modular arithmetic, in which every integer is congruent, modulo some modulus n, to a unique residue class equivalent to one of $\{0, \cdots, n-1\}$, every polynomial in the field is congruent to some unique "residue polynomial class" as well. Moreover, the proof demonstrates that this unique residue class can be determined as the remainder modulo division by the modulus (in this case not an integer but rather a Groebner basis of the ideal), as is the case with modular arithmetic over the integers, extending the intuition of modular arithmetic and congruences as circular arithmetic.
The second part of the theorem simply shows that r being a linear combination of elements of $\langle \mathrm{LT}(I)^C\rangle$ is not a coincedence; the elements turn out, to borrow a term from linear algebra, to be linearly independent, and thus their span would cover every such polynomial. We use the complement of $\langle \mathrm{LT}(I)\rangle$ here since r is the remainder of a division by f and thus couldn't consist of any elements generated by $\mathrm{LT}(I)$.

The above theorem gives standard representitatives for polynomial functions $\phi \in F[V]$ in the case that $I = \mathbf{I}(V)$ for some variety V. We can also use this theorem to describe certain aspects of the structure of the quotient ring $F[x_1, \cdots, x_n]/I$.

(Theorem) Quotient rings are generated by monomials not in $\mathbf{LT}(I)$: *Let I be an ideal of $F[x_1, \cdots, x_n]$. Then if we view $F[x_1, \cdots, x_n]/I$ as a vector space over F,*

$$F[x_1, \cdots, x_n]/I \cong \mathrm{span}(x^\alpha \notin \langle \mathrm{LT}(I)\rangle)$$

- *Proof*: Let r_f denote the remainder of the division of f by Groebner basis G of I. We'll give a constructive proof by proving that the mapping $\Phi : F[x_1, \cdots, x_n]/I \to S$, given by $\phi([f]) = r_f$, is an isomorphism. By the first theorem in this section, Φ is one-to-one, so we need only show that it preserves the vector space operations. The remainder operations splits over addition, so $r_{f+g} = r_f + r_g$; furthermore, if we make use of the sum operation defined over quotient rings given by $[f + g] = [f] + [g]$ which we introduced in the last section, then,

$$\Phi([f] + [g]) = \Phi([f + g]) = r_{f+g} = r_f + r_g = \Phi([f]) + \Phi([g])$$

Moreover, if

$$r_f = \sum_\alpha c_\alpha x^\alpha \text{ and } r_g = \sum_\alpha d_\alpha x^\alpha$$

where the sum is over α with $x^\alpha \notin \langle \mathrm{LT}(I) \rangle$, then

$$r_{f+g} = \sum_\alpha (c_\alpha + d_\alpha) x^\alpha$$

which means the sum operation $\Phi([f]) + \Phi([g])$ is precisely the sum operation in $\mathrm{span}(x^\alpha \notin \langle \mathrm{LT}(I) \rangle)$. Φ therefore preserves summation.
Next, we prove that Φ preserves scalar multiplication. Since

$$\Phi([c][f]) = \Phi([cf]) = r_{cf} = cr_f = c\Phi([f])$$

and $r_{cf} = cr_f$ for $c \in F$, it follows that

$$r_{cf} = \sum_\alpha cc_\alpha x^\alpha$$

and hence the scalar multiplication over the span is precisely the one we want. Thus, Φ preserves both operations and is an isomorphism. □

- *Intuition*: This theorem shows that, in some sense, the quotient ring $F[x_1, \cdots, x_n]/I$ is generated by elements in the complement of $\langle \mathrm{LT}(I) \rangle$ (technically, it's generated by elements which bijectively correspond to elements in the complement). Intuitively, quotient rings take all the polynomials congruent modulo the divisor ideal and collapse them into a single element, so this should be clear from the first theorem of the section, which shows that every polynomial is congruent modulo I to a unique polynomial r. r is a linear combination of monomials in $\langle \mathrm{LT}(I) \rangle^C$, which is to say, it's generated by the basis of $\langle \mathrm{LT}(I) \rangle^C$, which means it's in the span of monomials not in $\langle \mathrm{LT}(I) \rangle$ - this is where the theorem comes from.

We refer to r_f as the *standard representitative* of f in $\mathrm{span}(x^\alpha \notin \langle \mathrm{LT}(I) \rangle)$, so that $[f] + [g]$ is represented by $r_f + r_g$, as shown in the above theorem. Polynomial multiplication is more difficult to find a standard representation for, but it turns out that $[f][g]$ is represented by $r_{r_f r_g}$, the remainder of the division of $r_f \cdot r_g$ on G. One would expect simply $r_f \cdot r_g$ to work as a standard representitative, but it turns out that there are plenty of polynomials for which this quantity contains monomials in $\langle \mathrm{LT}(I) \rangle$.
We'll wrap this section up by applying the ideas we've developed to determining when a variety in $\mathbb{C}^n$ contains finitely many points, which is equivalent to determining when a system of polynomial equations has only a finite number of solutions over $\mathbb{C}^n$. Here's a general starting point.

(Theorem) Finiteness theorem: *Fix a monomial ordering on $F[x_1, \cdots, x_n]$ and let I be an ideal of $F[x_1, \cdots, x_n]$. Then the statements*

1. *There's some $m_i \geq 0$ such that $x_i^{m_i} \in \langle LT(I) \rangle$, for every $1 \leq i \leq n$.*

2. *Let G be a Groebner basis for I. Then there's some $m_i \geq 0$ such that $x_i^{m_i} = LM(g)$ for some $g \in G$, for $1 \leq i \leq n$.*

3. *$\langle LT(I) \rangle^C$ is finite.*

4. *$F[x_1, \cdots, x_n]/I$, viewed as a vector space over F, is finite-dimensional.*

are equivalent. Moreover, if F is algebraically closed, the statements imply that $\mathbf{V}(I)$ is finite.

- *Proof*: TODO
- *Intuition*: This theorem is a statement on when quotient rings are structurally restricted or finite, in some sense, relative to their infinite, continuous, or non-compact counterparts.

The first statement asserts that some power of every variable x_i is in $\langle \mathrm{LT}(I) \rangle$. Since the x_i are the atomic building blocks of all polynomials, if powers m_i of every x_i are in a set, then the only polynomials not in that set are those built out of powers of x_i lower than m_i, i.e. polynomials with total degree less than $\min_i m_i$, which clearly imposes rigid restrictions on the size of the complement. In fact, it forces it to be finite, since the inclusion of powers of every x_i means that almost every (i.e. all but finitely many) polynomials are in $\langle \mathrm{LT}(I) \rangle$, since almost every polynomial can be built out of powers m_i or greater of x_i.
The second statement is similar to the first, showing that the generators of I have leading monomials which are powers of the x_i, meaning the generators of $\langle \mathrm{LT}(I) \rangle$ are powers of the x_i, again implying that almost all polynomials are in the set.
The third and fourth statements are direct statements of finiteness.

We can use the finiteness theorem to determine when systems of polynomial equations have finitely many solutions, as the following theorem demonstrates.

(Theorem) Finiteness of Varieties: *Let I be an ideal of $F[x_1, \cdots, x_n]$ such that*

$$\forall i \in \{1, \cdots, n\} : \exists m_i \geq 0 \text{ s.t. } x_i^{m_i} \in \langle \mathrm{LT}(I) \rangle$$

Then $|\mathbf{V}(I)| =$ number of points in $\mathbf{V}(I) = \min(d, m_1 \cdots m_n)$ where $d =$ dimension of $F[x_1, \cdots, x_n]/I$. If F is algebraically closed and I is radical then $|\mathbf{V}(I)| = d$.

- *Proof*: TODO

This theorem essentially states that if the conditions of the finiteness theorem are met, then the variety corresponding to the ideal I is finite. It gives specific upper bounds which are in accordance with our intuition for the finiteness theorem.

4 Coordinate Ring of an Affine Variety

In this section, we'll study the ring $F[V]$ of polynomial functions on affine variety V more in depth. We'll make liberal use of the isomorphism $F[V] \cong F[x_1, \cdots, x_n]/\mathbf{I}(V)$, often identifying the former with the latter. As usual, we denote the polynomial function in $F[V]$ representing polynomial $f \in F[x_1, \cdots, x_n]$ with $[f]$. Notice that each variable x_i gives a polynomial function $[x_i] : V \to F$, whose value at $(a_1, \cdots, a_n) \in V$ is a_i. We refer to $[x_i] \in F[V]$ as the i^{th} *coordinate function* on V, and, as one would expect, $F[V]$ is generated by the n coordinate functions, in the sense that every polynomial function on V is a linear combination, over F, of products of the $[x_i]$. With this in mind, we formulate the following useful definition.

(Definition) Coordinate ring: *$F[V]$ is the* ***coordinate ring*** *of affine variety $V \subset F^n$.*

We can now rephrase many of the past results that we've seen in terms of coordinate rings. For example, a variety is irreducible if and only if its coordinate ring is an integral domain. Another example is that over an algebraically closed ring F, a variety is finite if and only if its coordinate ring is finite-dimensional (as a vector space over F). More generally, we'll use our understanding of coordinate rings to extend the algebra-geometry dictionary from the last chapter, which related varieties in F^n to ideals in $F[x_1, \cdots, x_n]$, by replacing the former with any general variety V and the latter with the coordinate ring over V, $F[V]$.

(Definition) Subvariety: *Let $V \subset F^n$ be an affine variety. Define a* ***subvariety*** *of V as*

$$\mathbf{V}_V(J) = \{a \in V \text{ s.t. } \forall \phi \in J : \phi(a) = 0\}$$

where $J = \langle \phi_1, \cdots, \phi_s \rangle \subset F[V]$ is an ideal of polynomial mappings. We also define

$$\mathbf{I}_V(W) = \{\phi \in F[V] \text{ s.t. } \forall a \in W : \phi(a) = 0\}$$

where W is a subset of V.

- *Properties*:

1. Unsurprisingly, $\mathbf{V}_V(J)$ is an affine variety contained in V.
2. $\mathbf{I}_V(W)$ is an ideal of $F[V]$.
3. If J is an ideal, we may extend the Nullstellensatz with $J \subset \sqrt{J} \subset \mathbf{I}_V(\mathbf{V}_V(J))$.
4. If W is a subvariety of V, then $W = \mathbf{V}_V(\mathbf{I}_V(W))$.

We begin the extension of the algebra-geometry dictionary by relating radical ideals in coordinate rings to radical polynomial ideals.

(Theorem) Radical ideals in $F[V]$ correspond with radical polynomial ideals containing $\mathbf{I}(V)$: *Ideal J of $F[V]$ is radical if and only if*

$$J' = \{f \in F[x_1, \cdots, x_n] \text{ s.t. } [f] \in J\}$$

is radical.

- *Proof*: Suppose J is radical, and that for $f \in F[x_1, \cdots, x_n]$, $f^m \in J'$. Then $[f^m] = [f]^m \in J$, which, since J is radical, implies $[f] \in J$. By definition, this means $f \in J'$, which shows that J' is radical. Conversely, suppose J' is radical and that $[f]^m \in J$, so that $[f^m] \in J$ and hence $f^m \in J'$. Since J' is radical, $f \in J'$ which implies $[f] \in J$, proving J to be radical. □

Moreover, we can use the notions of subvarieties to extend the Nullstellensatz.

(Theorem) Nullstellensatz for coordinate rings: *Let F be an algebraically closed field, and $V \subset F^n$ be an affine variety. Then for any ideal J of $F[V]$,*

$$\mathbf{I}_V(\mathbf{V}_V(J)) = \sqrt{J} = \{[f] \in F[V] \text{ s.t. } [f]^m \in J\}$$

The correspondences

$$\mathbf{I}_V(\cdot): \text{ affine subvarieties of } V \to \text{ radical ideals of } F[V]$$

$$\mathbf{V}_V(\cdot): \text{ radical ideals of } F[V] \to \text{ affine subvarieties of } V$$

are inclusion-reversing, and bijective inverses. Finally, under the above correspondences, points of V correspond to maximal ideals of $F[V]$.

- *Proof*: TODO

Next, we turn to the classification of varieties. To do so, we first formalize a notion of isomorphism for varieties.

(Definition) Variety isomorphism: *Let $V \subset F^m$ and $W \subset F^n$ be affine varieties. V and W are* ***isomorphic*** *if there exist polynomial mappings $\alpha : V \to W$ and $\beta : W \to V$ such that*

$$\alpha \circ \beta = \mathrm{id}_W \textit{ and } \beta \circ \alpha = \mathrm{id}_V$$

where id denotes the identity function on a variety.

This is an intuitive and natural definition of isomorphism, using polynomial mappings to preserve structure. Of course, we expect that isomorphic varieties should share many fundamental properties, such as irreducibility, dimension, and so on, if the mappings are really to be considered as preserving structure. We'll explore and prove precisely which properties are preserved. First, let's answer investigate the question of how to tell when two varieties are isomorphic. One way is to consider the relationship between their coordinate rings.

(Theorem) Constant preserving ring homomorphisms are pullback mappings: *Let $\alpha : V \to W$ be a polynomial mapping, and define its* ***pullback mapping*** *$\alpha^* : F[W] \to F[V]$ by*

$$\alpha^*(\phi) = \phi \circ \alpha \text{ for } \phi \in F[W]$$

Then α^* is a ring homomorphism which acts as the identity on constants (i.e. it maps constant functions to themselves). Moreover, for any ring homomorphism $\Phi : F[W] \to F[V]$ which acts as identity on constants, there exists $\alpha : V \to W$ such that $\Phi = \alpha^*$.

- *Proof*: TODO
- *Intuition*: Pullback mappings are one way to take polynomial mappings and define analogous mappings between the corresponding coordinate rings. We call α^* the pullback mapping because it maps in the opposite direction as α. The mapping itself is defined intuitively - given a fixed polynomial mapping, α^* acts on polynomials by composing α into them, so α^* can be viewed as taking functions and sending them to modified versions where their domain has been transformed by α. The theorem states firstly that such mappings are guaranteed to be homomorphisms, and moreover behave like the identity function on constant functions, which is of course obvious since if ϕ sends all inputs to the same constant, transforming its domain by α won't matter - the result will still map all inputs to the same constant.

The more significant part of the theorem is that any ring homomorphism which acts as the identity on constants is actually a pullback function in disguise.

We can use pullback mappings to answer the question we raised earlier, of how to tell when two varieties are isomorphic.

(Theorem) Isomorphic varieties have pullback isomorphic coordinate rings: *Affine varieties $V \subset F^m$ and $W \subset F^n$ are isomorphic if and only if $F[V]$ and $F[W]$ are isomorphic, and the isomorphism is the identity on constant functions (in other words, the isomorphism is a pullback mapping for some α).*

- *Proof*: TODO