The Algebra-Geometry Dictionary

Piyush Patil

December 14, 2016

In this chapter, we will more deeply explore the connection between polynomial ideals and affine varieties. We'll identify precisely which ideals correspond (in some sense) to which varieties. Whereas ideals are very significant objects of study in algebra (indeed, they're the central object of study in ring theory), varieties are essentially geometric objects, represented as unions of hypersurfaces in n-dimensional space, composed of points in an affine space. Thus, giving a strong correspondence between ideals and varieties allows us to map geometric statements about varieties to algebraic statements about ideals, and vice versa, giving rise to an algebra-geometry dictionary of sorts. We'll define some natural algebraic operations on ideals, and study their geometric analogs for varieties, and strive to produce algorithms for computing these operations. We'll also use the machinery developed in this chapter to prove the closure theorem from the last chapter.
The primary result of this chapter will be the Nullstellensatz, which is German for "theorem of zeros" and is a foundational result in algebraic geometry and constructs a fundamental bridge between algebra and geometry.

1 Hilbert's Nullstellensatz

We've already seen that we can associate an affine variety V with the ideal of the variety,

$$\mathbf{I}(V) := \{f \in F[x_1, \cdots, x_n] \text{ s.t. } \forall a \in V : f(a) = 0\}$$

Moreover, we can associate a polynomial ideal I with the affine variety,

$$\mathbf{V}(I) := \{a \in F^n \text{ s.t.} \forall f \in I : f(a) = 0\}$$

Note that because the Hilbert basis theorem guarantees that I is finitely generated by some $f_1, \cdots, f_s$, we can be certain that $\mathbf{V}(f_1, \cdots, f_s)$ is an affine variety. In this section, we'll further study this correspondence. Specifically, we'll study if this correspondence is one-to-one, and if not, why and how it can be made so.
Clearly, affine varieties V must pass to unique polynomial ideals, $\mathbf{I}(V)$, but conversely, ideals I do not pass to unique affine varieties $\mathbf{V}(I)$, as the following example shows

$$\langle x \rangle \neq \langle x^2 \rangle \text{ but } \mathbf{V}(x) = \mathbf{V}(x^2)$$

The situation gets worse if the underlying field is not algebraically closed (i.e. not every polynomial has a root), since then countless ideals correspond to the empty variety:

$$I_1 := \langle 1 \rangle = \mathbb{R}[x], I_2 = \langle 1 + x^2 \rangle, I_3 = \langle 1 + x^2 + x^4 \rangle$$

are distinct, but

$$\mathbf{V}(I_1) = \mathbf{V}(I_2) = \mathbf{V}(I_3) = \emptyset$$

It's easy to show that in the one variable case, the problem of multiple ideals mapping to the empty ideal goes away when the underlying field is algebraically closed. This follows easily because $F[x]$ is a principal ideal domain, which means, as we proved in chapter one, that

$$\forall I \subset F[x] : \exists f \in F[x] \text{ s.t. } I = \langle f \rangle$$

Thus, $\mathbf{V}(I)$ is simply the set of zeros of f, which is guaranteed by definition to be non-empty if F is algebraically closed. Let's now prove that the same is true in a several variables.

(Theorem) Weak Nullstellensatz: *In an algebraically closed field, every proper ideal has a non-empty zero set. Formally, let F be an algebraically closed field. Then if ideal $I \subset F[x_1, \cdots, x_n]$ maps to $\mathbf{V}(I) = \emptyset$, $I = F[x_1, \cdots, x_n]$.*

- *Proof*: We'll prove the contrapositive, that for any proper subset I of $F[x_1, \cdots, x_n]$, $\mathbf{V}(I) = \emptyset$. Define

$$I_{x_n = a_n} := \{f(x_1, \cdots, x_{n-1}, a_n), f \in I\}$$

for some $a_n \in F$. Clearly, $I_{x_n=a_n}$ is an ideal in $F[x_1, \cdots, x_{n-1}]$; if we can prove that $I_{x_n=a_n} \neq F[x_1, \cdots, x_{n-1}]$, then it follows inductively that

$$(I_{x_n=a_n})_{x_{n-1}=a_{n-1}} \neq F[x_1, \cdots, x_{n-2}], \cdots, J \neq F$$

where

$$J := ((I_{x_n=a_n})_{\cdots})_{x_1=a_1} = \{f(a_1, \cdots, a_n), f \in I\} \subset F$$

Since the only ideals in F are $\{0\}$ and F itself, and if we assume as above that $J \neq F$, we must have $J = \{0\}$, which implies that $f(a_1, \cdots, a_n) = 0, \forall f \in I$ and thus that $(a_1, \cdots, a_n) \in \mathbf{V}(I)$.
Thus, if we can inductively link I down to the base case of $J \subset F$, through the $((I_{x_n=a_n})_{\cdots})$, we'll be able to use the a_i themselves to show that $\mathbf{V}(I)$ is not empty. Of course, the inductive step of proving that such an a_n exists still remains to be proven. To prove that there exists and $a_n \in F$ for which $I_{x_n=a_n} \neq F[x_1, \cdots, x_{n-1}]$, we divide the proof into two cases, depending on whether $I \cap F[x_n]$ is trivially non-empty or not.
Case 1: Suppose $I \cap F[x_n] \neq \{0\}$. Then for any non-zero $f \in I \cap F[x_n]$, noting that f is not a constant polynomial since if it were we'd have $1 \in I \cap F[x_n] \to 1 \in I \to I = F[x_1, \cdots, x_n]$. Since F is algebraically closed, f is guaranteed to have some number, say m, of zeros. Then we can write

$$f(x_n) = c\prod_{i=1}^{m}(x_n - b_i)^{\alpha_i}, c \neq 0, b_i \in F, \alpha_i \in \mathbb{Z}_{\geq 0}$$

We'll prove that one of the b_i's is the a_n we seek. Assume for the sake of contradiction that none of the zeros of f fit the criterion for a_n, so that $\forall i \in \{1, \cdots, m\} : I_{x_n=b_i} = F[x_1, \cdots, x_{n-1}]$. Then

$$\forall i \in \{1, \cdots, m\} : 1 \in I_{x_n=b_i} \to \exists B_i \in I \text{ s.t. } B_i(x_1, \cdots, x_{n-1}, b_i) = 1$$

We can use this to prove that $1 \in I$ by first expanding B_i:

$$1 = B_i(x_1, \cdots, x_{n-1}, b_i) = B_i(x_1, \cdots, x_{n-1}, x_n - (x_n - b_i)) = B_i(x_1, \cdots, x_n) + A_i \cdot (x_n - b_i)$$

for some $A_i \in F[x_1, \cdots, x_n]$. However, we don't necessarily know that $A_i \in I$, so we haven't yet shown that $1 \in I$. But since the above is true for every zero b_i, we have

$$\to 1 = \prod_{i=1}^{m}(B_i + A_i \cdot (x_n - b_i))^{\alpha_i} = \left(\prod_{i=1}^{m} A_i\right) \cdot \prod_{i=1}^{m}(x_n - b_i)^{\alpha_i} + B = c^{-1} f \prod_{i=1}^{m} A_i + B$$

where B is some linear combination of powers of $(x_n - b_i)$ and B_i, both of which are in I and therefore implying $B \in I$. Then, since $f \in I$, we have

$$c^{-1} f \prod_{i=1}^{m} A_i + B = 1 \in I \to I = F[x_1, \cdots, x_{n-1}]$$

which is a contradiction.
Case 2: In this edge case, suppose $I \cap F[x_n] = \{0\}$. The proof that $I_{x_n=a_n} \neq F[x_1, \cdots, x_{n-1}]$, for some suitable a_n, is similar to the justification behind the extension theorem. Let $G = \{g_i, 1 \leq i \leq t\}$ be a Groebner basis for I with respect to the lexicographic ordering $x_1 > \cdots > x_n$, so that

$$G_{x_n=a_n} := \{g_i(x_1, \cdots, x_{n-1}, a_n)\}$$

is a basis for $I_{x_n=a_n}$. Since we can write

$$g_i(x_1, \cdots, x_n) = c_i(x_n) x_1^{\alpha_1} \cdots x_{n-1}^{\alpha_{n-1}} + r_i$$

where $c_i \in F[x_n]$ and $r_i \in F[x_1, \cdots, x_n]$. As in the extension theorem, we seek an a_n for which the c_i's don't simultaneously vanish. Since algebraically closed fields are infinite, we can choose an a_n such that $c_i(a_n) \neq 0, \forall i$.
Let's show that $G_{x_n=a_n}$ is a Groebner basis for $I_{x_n=a_n}$, because then it follows that no $\text{LT}(g_i(x_1, \cdots, x_{n-1}, a_n)$ divides 1 (since $c_i(a_n) \neq 0$), which implies $1 \notin I_{x_n=a_n}$, which implies $I_{x_n=a_n} \neq F[x_1, \cdots, x_{n-1}]$, proving the theorem. We'll use Buchberger's criterion to prove that $G_{x_n=a_n}$ is a Groebner basis: consider the S-polynomial of some $g_i, g_j \in G$, $S(g_i, g_j) \in I$. Write the polynomial in terms of the Groebner basis,

$$S(g_i, g_j) = \sum_{i=1}^{t} h_i g_i$$

for some $h_i \in F[x_1, \cdots, x_n]$. Then

$$S(g_i, \cdots, g_j)(x_1, \cdots, x_{n-1}, a_n) = \sum_{i=1}^{t} h_i(x_1, \cdots, x_{n-1}, a_n) g_i(x_1, \cdots, x_{n-1}, a_n)$$

Thus, $G_{x_n=a_n}$ divides $S(g_i, g_j)(x_1, \cdots, x_{n-1}, a_n)$ for every $g_i(x_1, \cdots, x_{n-1}, a_n), g_j(x_1, \cdots, x_{n-1}, a_n) \in G_{x_n=a_n}$, which proves that $G_{x_n=a_n}$ is a Groebner basis for $I_{x_n=a_n}$, which proves the theorem. $\square$

The weak Nullstellensatz allows us to algorithmically check whether or not a system of polynomial equations in $\mathbb{C}[x_1, \cdots, x_n]$ has a solution or not. This follows from the observation that $\{1\}$ is the only reduced Groebner basis for $F[x_1, \cdots, x_n]$. Thus, to check if $f_1, \cdots, f_s \in \mathbb{C}[x_1, \cdots, x_n]$ have a common zero, we can compute a reduced Groebner basis for $I = \langle f_1, \cdots, f_s \rangle$ - if this basis is $\{1\}$, then $I = \mathbb{C}[x_1, \cdots, x_n]$ which means the polynomials have no common zero; otherwise, they do. Even if the field underlying $f_1, \cdots, f_s$ isn't algebraically closed, we can still conclude that if $\{1\}$ is the reduced Groebner basis of I then there is no common zero, though we can't conclude anything about other direction. The problem framed above, of checking if a system of equations has a solution, is known as the *consistency problem*, as we are checking if the equations are *consistent*.
However, we gave two examples for why the mapping of ideals to varieties is not one-to-one, and although working over algebraically closed fields takes care of the issue of mapping ideals to empty varieties, we still have to worry about instances such as

$$\langle x^n, y^m \rangle, m, n \in \mathbb{Z}_{>0}$$

which are distinct ideals for any positive integers n, m but which all map to the variety $\{(0, 0)\}$. The full form of Hilbert's Nullstellensatz essentially states that examples such as this, dealing with powers of polynomials (which of course doesn't change the affine variety since 0 raised to any power is 0), are the *only* reason for the mapping from ideals to varieties not being one-to-one even over algebraically closed fields.

(Theorem) Hilbert's Nullstellensatz: *Let F be an algebraically closed field. Then for any $I \subset F[x_1, \cdots, x_n]$,*

$$f \in \mathbf{I}(\mathbf{V}(I)) \iff \exists m \text{ s.t. } f^m \in I$$

• *Proof*: If $f^m \in I$ then clearly $f \in \mathbf{I}(\mathbf{V}(I))$, so let's prove the other direction. Let $I = \langle f_1, \cdots, f_s \rangle$. If f is a non-zero polynomial which vanishes at every common zero of $f_1, \cdots, f_s$, then consider the ideal

$$J := \langle f_1, \cdots, f_s, 1 - yf \rangle \subset F[x_1, \cdots, x_n, y]$$

Then we have $\mathbf{V}(J) = \emptyset$, since for any point $(a_1, \cdots, a_{n+1}) \in F^{n+1}$, either $(a_1, \cdots, a_n)$ is a simultaneous zero of $f_1, \cdots, f_s$ or it isn't. If it is, then $f(a_1, \cdots, a_n) = 0$ as well, and so $1 - yf$ has the value 1 at $(a_1, \cdots, a_{n+1})$, and so $(a_1, \cdots, a_{n+1}) \notin \mathbf{V}(J)$. If it's not, then $f_i(a_1, \cdots, a_n) \neq 0$ for some i, which is to say, $f_i(a_1, \cdots, a_n, a_{n+1}) \neq 0$, which again shows $(a_1, \cdots, a_{n+1}) \notin \mathbf{V}(J)$. Thus, $\mathbf{V}(J) = \emptyset$, and therefore $1 \in J$ by the weak Nullstellensatz.

It follows that there are polynomials $p_i, q \in F[x_1, \cdots, x_n, y]$ such that

$$1 = \sum_{i=1}^{s} (p_i(x_1, \cdots, x_n, y) f_i + q(x_1, \cdots, x_n, y)(1 - yf)) = \sum_{i=1}^{s} p_i(x_1, \cdots, x_n, \frac{1}{f}) f_i$$

where we set $y := \frac{1}{f}$. The above summation expresses a rational function whose denominator is some power of f; if we multiply both sides of the equation by f^m for m sufficiently large to clear the denominator of the rational function, we have

$$f^m = \sum_{i=1}^{s} A_i f_i$$

for some polynomials $A_i \in F[x_1, \cdots, x_n]$, which shows $f^m \in I$. $\square$

• *Intuition*: $\mathbf{V}(I)$, for polynomial ideal I, denotes the zero set of every polynomial in I, i.e. the set of points at which every polynomial in I simultaneously vanishes, whereas $\mathbf{I}(V)$, for affine variety V, denotes the set of polynomials which simultaneously vanishes at every point in V. Thus, $\mathbf{I}(\mathbf{V}(I))$ represents the set of polynomials which vanish over the set of points over which polynomials in I vanish. It seems intuitively the this statement is useless and merely refers to I itself, but it turns out there are polynomials not in I which nonetheless vanish at every single point polynomials in I vanish at. A trivial example of such polynomials are lower powers of polynomials: if $(f(x))^m = 0$ at some $x \in F$, then obviously $(f(x))^k = 0$ for any $k \leq m$. The above theorem simply states that when F is algebraically closed, so that every polynomial is guaranteed a zero (this prevents unexpected behavior), these trivial examples are the only examples, and discarding our discussion on lower polynomial powers, $\mathbf{I}(\cdot)$ and $\mathbf{V}(\cdot)$, which are already guaranteed to be right inverses, are also left inverses (when viewed as functions over sets of points and sets of polynomials).

2 Radical Ideals and the Ideal-Variety Correspondence

Hilbert's Nullstellensatz provides insight into which polynomials vanish over an affine variety, and the relationship of those polynomials to the underlying ideal of the affine variety; in this section, we'll recast the Nullstellensatz in terms of ideals in

order to study the nature of those ideals which consist of all, not just some, of the polynomials that vanish over a variety. The key observation of interest in this section is that although it doesn't necessarily follow from the axioms of ideals that if a power of a polynomial is in an ideal then so is the polynomial, this does hold true when all the polynomials in the ideal share a zero set. A more formal statement of this observation follows below.

(Theorem) Polynomial Powers in Ideals: *Let V be an affine variety. Then, for positive integer m,*

$$f^m \in \mathbf{I}(V) \rightarrow f \in \mathbf{I}(V)$$

- *Proof*: For all $a \in V$, if $f^m \in \mathbf{I}(V)$ then $(f(a))^m = 0$, which implies that $f(a) = 0$, which implies that $f \in \mathbf{I}(V)$. $\square$

Let's wrap this idea in a concise definition so we can use it more compactly.

(Definition) Radical ideal: *A polynomial ideal I is **radical** if*

$$f^m \in I \rightarrow f \in I$$

- Thus, the above theorem can be restated as: ideals of affine varieties are radical.
- *Motivation*: The main motivation for this definition is simply to allow us to recast the Nullstellensatz in a more natural, compact, ideal-centric form. Moreover, Hilbert's Nullstellensatz tells us that $f \in \mathbf{I}(\mathbf{V}(I))$ if and only if $f^m \in I$, for some m, which means that I fails to contain all the polynomials over which $\mathbf{V}(I)$ vanishes precisely when $m > 1$ for some polynomials which vanish over the variety, which is equivalent to saying that I contains polynomial powers but not the base polynomial itself. Given our definition above, this seems to indicate that although there's no one-to-one correspondence from ideals to varieties, even over an algebraically closed field, there's a one-to-one correspondence between affine varieties and radical ideals.

The motivation for the definition of radical ideals naturally leads to the following definition.

(Definition) Radical of an ideal: *The **radical of polynomial ideal** I, denoted $\sqrt{I}$, is defined as*

$$\sqrt{I} := \{f \text{ where } f^m \in I \text{ for some } m\}$$

- It follows that $\sqrt{I}$ is an ideal, that it's radical, and that it contains I. Moreover, I is radical if and only if $I = \sqrt{I}$.

Let's now use the above definition to give an ideal-theoretic definition of Hilbert's Nullstellensatz, called the strong Nullstellensatz.

(Theorem) Strong Nullstellensatz: *Let F be an algebraically closed field and I be a polynomial ideal over F. Then*

$$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$$

- *Proof*: Clearly, $\sqrt{I} \subset \mathbf{I}(\mathbf{V}(I))$ since $f \in \sqrt{I} \rightarrow f^m \in I$ for some $m \rightarrow \forall a \in \mathbf{V}(I) : (f(a))^m = 0 \rightarrow f(a) = 0 \rightarrow f \in \mathbf{I}(\mathbf{V}(I))$. To prove the other direction, suppose $f \in \mathbf{I}(\mathbf{V}(I))$, so that by definition, $\forall a \in \mathbf{V}(I) : f(a) = 0$. Then Hilbert's Nullstellensatz implies that $f^m \in I$ for some m, which implies $f \in \sqrt{I}$, proving the theorem. $\square$

We are now ready to set up the algebra-geometry dictionary alluded to in this chapter's introduction. Below are some foundational and deep results on the relationship between the mapping from affine varieties to polynomial ideals given by $\mathbf{I}(\cdot)$ and the mapping from polynomial ideals to affine varieties given by $\mathbf{V}(\cdot)$.

(Theorem) Ideal-Variety Correspondence: *Let F be a field.*

1. The maps
$$\mathbf{V}: \text{ affine varieties } \rightarrow \text{ polynomial ideals}$$
$$\mathbf{I}: \text{ polynomial ideals} \rightarrow \text{affine varieties}$$
are inclusion-reversing, so that $I_1 \subset I_2 \rightarrow \mathbf{V}(I_2) \subset \mathbf{V}(I_1)$ and $V_1 \subset V_2 \rightarrow \mathbf{I}(V_2) \subset \mathbf{I}(V_1)$.
2. For any affine variety V, $\mathbf{V}(\mathbf{I}(V)) = V$, which is to say, $\mathbf{I}(\cdot)$ is one-to-one. Conversely, although $\mathbf{V}(\cdot)$ is not one-to-one, it is true that for any polynomial ideal I, $\mathbf{V}(\sqrt{I}) = \mathbf{V}(I)$.
3. If F is algebraically closed and we restrict the maps $\mathbf{V}(\cdot), \mathbf{I}(\cdot)$ to radical ideals rather than all polynomial ideals, then
$$\mathbf{V}: \text{ affine varieties } \rightarrow \text{ radical ideals}$$
$$\mathbf{I}: \text{ radical ideals} \rightarrow \text{affine varieties}$$
are bijective inverses.

• *Proof*: To prove (1), consider that if $I_1 \subset I_2$, then every polynomial in I_1 must vanish over $\mathbf{V}(I_2)$ by definition, since those polynomials are contained in I_2. Similarly, if $V_1 \subset V_2$, then any polynomial which vanishes over V_2 must vanish over all of V_1 too, which shows that $\mathbf{I}(V_2) \subset \mathbf{V}(I_1)$.

To prove (2), let $V = \mathbf{V}(f_1, \cdots, f_s)$ be an affine variety. Then $V \subset \mathbf{V}(\mathbf{I}(V))$ by definition. To prove the other direction, note that by definition, $f_1, \cdots, f_s \in \mathbf{I}(V)$ which means $\langle f_1, \cdots, f_s \rangle \subset \mathbf{I}(V)$, which means, by (1), that $\mathbf{V}(\mathbf{I}(V)) \subset \mathbf{V}(\langle f_1, \cdots, f_s \rangle) = V$. To prove that $\mathbf{V}(\sqrt{I}) = \mathbf{V}(I)$, first note that $\mathbf{V}(\sqrt{I}) \subset \mathbf{V}(I)$ since $I \subset \sqrt{I}$ implies that if every polynomial in $\sqrt{I}$ is zero over a set of points, so is every polynomial of I, which are of course contained in the former. To prove that $\mathbf{V}(I) \subset \mathbf{V}(\sqrt{I})$, recall that $\mathbf{V}(I)$ is the set of points over which every polynomial $f \in I$ is simultaneously zero, which means f^m is zero over those points for any power of f, which shows that $\mathbf{V}(I) \subset \mathbf{V}(\sqrt{I})$.

To prove (4), we simply have to prove that $\mathbf{I}(\mathbf{V}(I)) = I$ for radical ideal I, since (2) proves the other direction. By the strong Nullstellensatz, $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I} = I$ since I is radical, proving the theorem. □

This correspondence is important because it allows us to translate questions about varieties to questions about ideals, and vice versa, assuming we're working over an algebraically closed field. Given the strong Nullstellensatz's dependence on radical ideals, it's natural to extend the main ideal-theoretic questions we studied in the last chapter to radical ideals. Specifically, we'll study the following questions about radical ideals.

1. *Radical generators*: Given a polynomial ideal I, can we algorithmically find a finite basis for $\sqrt{I}$ (which is guaranteed to exist by the Hilbert basis theorem)?
2. *Radical ideal test*: Is there an algorithm to determine if a given ideal is radical?
3. *Radical membership*: Given polynomial ideal I, can we algorithmically determine if $f \in \sqrt{I}$? Notice that this question is automatically answered if we can answer the first question.

All of the above algorithms exist; let's investigate the radical membership problem. This question can be answered when we have a finite basis for the ideal I, by adapting Hilbert's proof of Hilbert's Nullstellensatz.

(Theorem) Solution to radical membership: *Given a polynomial ideal $I = \langle f_1, \cdots, f_s \rangle \subset F[x_1, \cdots, x_n, y]$, $f \in \sqrt{I}$ if and only if $1 \in \langle f_1, \cdots, f_s, 1 - yf \rangle \subset F[x_1, \cdots, x_n, y]$.*

• *Proof*: Letting $J := \langle f_1, \cdots, f_s, 1-yf \rangle$, it's clear that $1 \in J$ implies that $J = F[x_1, \cdots, x_n, y]$, of which $f \in F[x_1, \cdots, x_n]$ is obviously a member. Conversely, if $f \in \sqrt{I}$, then $f^m \in I \subset J$ for some m. Then

$$1 = y^m f^m - (1 - y^m f^m) = y^m f^m - (1 - yf) \cdot (1 + yf + \cdots + y^{m-1} f^{m-1}) \in J$$

since $f^m, (1 - yf) \in J$. □

As in the consistency problem from the last section, we can thus algorithmically solve the radical membership problem by computing a reduced Groebner basis for $\langle f_1, \cdots, f_s, 1 - yf \rangle$ and checking if its $\{1\}$. Finally, let's investigate one special case in which we can solve the radical generators problem: principal ideals. It follows from the theory of principal ideal domains (namely, from the unique factorization theorem), that any polynomial can be expressed as a product of irreducible polynomials, where f is irreducible if $f = g \cdot h \rightarrow$ either g, h, or both are constant. We'll use this fact in the following solution to the radical generators problem.

(Theorem) Solution to radical generators for principal ideals: *Let $I = \langle f \rangle$ be a principal polynomial ideal. If we factorize f into irreducible polynomials as $f = c f_1^{\alpha_1} \cdots f_s^{\alpha_s}$ then*

$$\sqrt{I} = \langle f_1 \cdots f_s \rangle$$

• *Proof*: It follows that $f_1 \cdots f_s \in \sqrt{I}$ because if we choose $m > \max \alpha_i$ then we have

$$(f_1 \cdots f_s)^m = f_1^{m-\alpha_1} \cdots f_s^{m-\alpha_s} \cdot f \in \langle f \rangle = I$$

. Thus, $\langle f_1 \cdots f_s \rangle \subset \sqrt{I}$. Let's now show that any polynomial in the ideal is a multiple of $f_1 \cdots f_s$. If $g \in \sqrt{I}$, then $g^m \in I$ for some m, so that $g^m = hf = ch f_1^{\alpha_1} \cdots f_s^{\alpha_s}$ for some h, so that each f_i is an irreducible factor of g^m and therefore of g. Thus, g is a multiple of $f_1 \cdots f_s$, which proves $g \in \langle f_1 \cdots f_s \rangle$. □

In accordance with the above theorem, we define the "reduced" form of a polynomial as the result of stripping away any extraneous or duplicate factors.

(Definition) Reduction of a polynomial: *We define the **reduction** of a polynomial f, denoted f_{red}, by*

$$\langle f_{red} \rangle = \sqrt{\langle f \rangle}$$

so that $f_{red} = f_1 \cdots f_s$ *where* $f = cf_1^{\alpha_1} \cdots f_s^{\alpha_s}$. f *is* ***reduced*** *or* ***square-free*** *if* $f = f_{red}$.

Since factoring polynomials is, as with factoring integers, computationally difficult, we present an algorithm for computing the reduction of a polynomial without factoring it.

(Theorem) Algorithm for polynomial reduction: *Let* F *be a field containing the rational numbers, and let* $I = \langle f \rangle \subset F[x_1, \cdots, x_n]$. *Then*

$$f_{red} = \frac{f}{\gcd(f, \frac{\partial f}{\partial x_1}, \cdots, \frac{\partial f}{\partial x_n})}$$

- *Proof*: Let $f = cf_1^{\alpha_1} \cdots f_s^{\alpha_s}$. We'll show that

$$\gcd\left(f, \frac{\partial f}{\partial x_1}, \cdots, \frac{\partial f}{\partial x_n}\right) = f_{-1} := f_1^{\alpha_1 - 1} \cdots f_s^{\alpha_s - 1}$$

from which it follows that $f_{red} = f_1 \cdots f_s$ as desired. First notice that by the product rule for differentiation,

$$\frac{\partial f}{\partial x_i} = f_{-1} \cdot \sum_{j=1}^{s} \left(\alpha_j f_1 \cdots f_{j-1} \frac{\partial f_j}{\partial x_i} f_{j+1} \cdots f_s\right) \to f_{-1} \mid \gcd\left(f, \frac{\partial f}{\partial x_1}, \cdots, \frac{\partial f}{\partial x_n}\right)$$

since f_{-1} divides both f and all of the partial derivatives. To prove that f_{-1} is the largest divisor of the gcd, we'll show that increasing the power of any f_i in f_{-1} by even one causes it to no longer divide the gcd; from this this it follows that since $f = f_1^{\alpha_1} \cdots f_s^{\alpha_s}$, f_{-1} must be the gcd. In other words, we'll prove that

$$\forall i : f_i^{\alpha_i} \nmid \frac{\partial f}{\partial x_j} \text{ for some } j$$

Let $f = f_i^{\alpha_i} h_i$ for some h_i, not divisible by f_i (so α_i is the maximal power for which f_i divides f). Then

$$\frac{\partial f}{\partial x_j} = f_i^{\alpha_i - 1}\left(a_i \frac{\partial f_i}{\partial x_j} + f_i \frac{\partial h_i}{\partial x_j}\right)$$

We want to show that there's some j not divisible by $f_i^{\alpha_i}$, which is to say, f_i does not divide $a_i \frac{\partial f_i}{\partial x_j} h_i + f_i \frac{\partial h_i}{\partial x_j}$, which is equivalent to saying f_i doesn't divide $\frac{\partial f_i}{\partial x_j}$, since f_i doesn't divide h_i and is irreducible. This is trivially true for polynomials f_i, since the derivative has smaller degree than the original, except TODO

3 Sums, Products, and Intersections of Ideals

In this section, we lay the groundwork which will allow us to treat ideals as algebraic objects in their own right, by defining binary operations on them which will allow us to intuitively associate a new ideal with a pair of ideals in a natural extension of binary operations on numbers. The main questions we'll study are if we can link the generators of the new ideal to the generators of the old ideals, and if the binary operations have any geometric interpretation or significance.

3.1 Ideal Sums

Here we extend polynomial summation to polynomial ideals.

(Definition) Sum of ideals: *Let* I *and* J *be ideals of* $F[x_1, \cdots, x_n]$. *We define the* ***sum*** *of* I *and* J *to be*

$$I + J := \{f + g, f \in I \text{ and } g \in J\}$$

- *Proof that* $I + J$ *is an ideal*: Clearly $0 = 0 + 0 \in I + J$. To show additive closure, consider $h_1, h_2 2 \in I + J$, for which there exist $f_1, f_2 \in I$, $g_1, g_2 \in J$ such that $h_1 = f_1 + g_1$ and $h_2 = f_2 + g_2$. It follows that $h_1 + h_2 = (f_1 + f_2) + (g_1 + g_2) \in I + J$. Finally, for any $h \in I + J$ we have $h = f + g$ for some $f \in I, g \in J$, so that $ph = p \cdot (f + g) = pf + pg \in I + J$ for any $p \in F[x_1, \cdots, x_n]$. $\square$
- *Proof that* $I + J$ *is the smallest ideal containing* I, J: Let H be an ideal containing I and J. Then H must contain every combination of $f + g$ for $f \in I$ and $g \in J$ since H is an ideal containing f and g. Thus, H contains $I + J$.

Let's answer the first question posed above, concerning the generators of $I + J$.

(Theorem) Ideal sums have combined generators: *Let* $I = \langle f_1, \cdots, f_s \rangle$ *and* $J = \langle g_1, \cdots, g_t \rangle$. *Then* $I + J =$

$\langle f_1, \cdots, f_s, g_1, \cdots, g_t \rangle$.

• *Proof*: Clearly, $\langle f_1, \cdots, f_s, g_1, \cdots, g_t \rangle$ is an ideal containing I and J, and hence contains $I+J$ too. The reverse inclusion is trivial as well, since any polynomial in $\langle f_1, \cdots, f_s, g_1, \cdots, g_t \rangle$ can be expressed as a sum between a linear combination of the f_i's and a linear combination of the g_j's, and hence a sum of a polynomial in I and one in J, which must be in $I+J$ by definition. □

• *Corollary*: $\langle f_1, \cdots, f_s \rangle = \langle f_1 \rangle + \cdots + \langle f_s \rangle$.

Let's now examine what summation does to for the corresponding affine varieties.

(Theorem) Ideal summation corresponds to variety intersection: *Let I, J by ideals of $F[x_1, \cdots, x_n]$. Then $\mathbf{V}(I+J) = \mathbf{V}(I) \cap \mathbf{V}(J)$.*

• *Proof*: For any $a \in \mathbf{V}(I+J)$, clearly $I \subset I+J$ and $J \subset I+J$ imply $a \in \mathbf{V}(I)$ and $a \in \mathbf{V}(J)$. Conversely, if a is in both $\mathbf{V}(I)$ and $\mathbf{V}(J)$ then since every polynomial h in $I+J$ can be expressed as $h = f+g$ for $f \in I, g \in J$, with $f(a) = g(a) = 0$, $h(a) = 0$ and so every polynomial in $I+J$ is zero at a, so $a \in \mathbf{V}(I+J)$ which proves the opposite inclusion. The theorem follows. □

• Geometrically this is intuitive since the sum of the ideals has more generators than the original ideals, meaning its affine variety is more restricted; it must be zero at every point both I and J are, and thus is the intersection.

3.2 Ideal Products

Similar to the definition of ideal summation, we'll give an equally natural notion of ideal products in this section. Recall that in previous chapters we found that the affine variety of a set of polynomial products is the union of varieties of individual polynomials; that is, in some sense, the varieties of ideals split over union for pairwise polynomial multiplication:

$$\mathbf{V}(f_i g_j) = \mathbf{V}(f_i) \cup \mathbf{V}(g_j), 1 \leq i \leq s, 1 \leq j \leq t$$

This nicely supports our intuition for the following definition of ideal products.

(Definition) Product of ideals: *Let I, J be ideals of $F[x_1, \cdots, x_n]$. We define their **product** as the ideal of all linear combinations of polynomials from I and J:*

$$IJ = \left\{ \sum_{i=1}^{r} f_i g_j, f_i \in I, g_j \in J \right\}$$

• It follows that the product is generated by the pairwise products of the generators of I and J, so that if $I = I = \langle f_1, \cdots f_s \rangle, J = \langle g_1, \cdots, g_t \rangle$ then

$$IJ = \langle f_i g_j, 1 \leq i \leq s, 1 \leq j \leq t \rangle$$

We can also prove a corresponding theorem to the link between ideal summation and their varieties.

(Theorem) Ideal products correspond to variety union: *If I, J are ideals in $F[x_1, \cdots, x_n]$, then $\mathbf{V}(IJ) = \mathbf{V}(I) \cup \mathbf{V}(J)$.*

• *Proof*: Suppose $a \in \mathbf{V}(IJ)$, so that $f(a)g(a) = 0$ for any $f \in I, g \in J$. If $f(a) = 0$ for every $f \in I$, then obviously $a \in \mathbf{V}(I) \cup \mathbf{V}(J)$, but if there's an f for which $f(a) \neq 0$ then we must have $g(a) = 0$ for every $g \in J$, since otherwise there would exist f, g with $f(a)g(a) \neq 0$. Thus, $a \in \mathbf{V}(I) \cup \mathbf{V}(J)$. Conversely, if a is in the union, then it must belong to at least one of $\mathbf{V}(I)$ or $\mathbf{V}(J)$, so that either $f(a) = 0$ for every $f \in I$ or $g(a) = 0$ for every $g \in J$; in either case, the product $f(a)g(a) = 0$ for any combination of $f \in I, g \in J$, and so $a \in \mathbf{V}(IJ)$. □

3.3 Ideal Intersection

Finally, we study the notion of ideal intersection. This doesn't require any special definitions, as the standard definition of set theoretic intersection applies perfectly well to ideals, but the intersection of two ideals does have some interesting properties, and the operation is, in many ways, more primitive than either summation or multiplication of ideals. Before we proceed, let's first that ideal intersections are in fact ideals.

(Theorem) Intersection of ideals is an ideal: *Let I, J be ideals of $F[x_1, \cdots, x_n]$. Then $I \cap J$ is an ideal.*

• *Proof*: Clearly, $0 \in I \cap J$ since $0 \in I$ and $0 \in J$. Moreover, for $f, g \in I \cap J$, we must have $f, g \in I$ and $f, g \in J$, so $f+g \in I$ and $f+g \in J$, so $f+g \in I \cap J$. Finally, for any $f \in I \cap J$, $f \in I, f \in J \rightarrow hf \in I, hf \in J \rightarrow hf \in I \cap J$ for any polynomial h, which proves the theorem. □

Finding generators for ideal intersections is trickier than finding generators for ideal sums or products. Given the factorizations of the generators of I and J it's easier to compute generators for $I \cap J$, but factoring polynomials is difficult

in general. Instead, we'll make use of a clever trick which will allow us to reduce the problem to finding a certain kind of elimination ideal. We'll "lift" the ideals I, J of $F[x_1, \cdots, x_n]$ to a higher-dimensional space $F[x_1, \cdots, x_n, t]$ by introducing a new variable t, and designing an ideal which, once t is eliminated, reduces to the intersection of I and J. Before doing so, let's introduce some notation: if $f(t) \in F[t]$ is a polynomial in t, and I is an ideal of $F[x_1, \cdots, x_n]$ then we denote

$$fI := \{fg, g \in I\} \subset F[x_1, \cdots, x_n, t]$$

Note that this is a simple elementwise multiplication, which we denote fI for notational convenience, and is very different from the ideal product $\langle f \rangle \cdot I$ as defined in the last subsection. As one would expect, if $I = \langle f_1, \cdots, f_s \rangle$ then $fI = \langle ff_1, \cdots, ff_s \rangle$. Moreover, $\forall a \in F, g \in fI : g(x_1, \cdots, x_n, a) \in I$, so that eliminating t by replacing it with any element of the underlying field brings us back down to I where we started; this is true simply because if $g(x_1, \cdots, x_n, t) = f(t)h(x_1, \cdots, x_n)$ for $h \in I$ then $g(x_1, \cdots, x_n, a) = f(a)h(x_1, \cdots, x_n) \in I$ because $f(a) \in F$ is a constant.
To design an ideal of $F[x_1, \cdots, x_n, t]$ as described above, i.e. which reduces to $I \cap J$ when t is eliminated, notice that given $f(t)I$, we have $f(a)I = I$ for any $a \in F$ (the same, of course, holds for J), with the exception that $0I = \{0\}$, so that if a is a root of f then we destroy the ideal I completely. Because $g(x_1, \cdots, x_n, a) \in I$ for any $g \in f(t)I$, if we can design an ideal which reduces to I in one case and reduces to J in another, then it would follow that any polynomial in the ideal was in both I and J, giving our reduction; to do this, we can use polynomials f, g which are complementary in the sense that $f(a) = 0 \rightarrow g(a) = 1, g(a) = 0 \rightarrow f(a) = 1$, so that the sum of fI and gJ would reduce to I in one case and J in another. Taking the simplest instance, consider

$$tI + (1 - t)J$$

At $t = 0$ we reduce to I and at $t = 1$ we reduce to J, so that polynomials in the above ideal belong to both I and J. To ensure that polynomials which are already in $I \cap J$ are also captured in the above ideal, we have to filter by the extra polynomials which contain t. This leads us to the following theorem, which provides the foundation for an algorithm to determine the generators of the intersection between two ideals.

(Theorem) Explicit Representation of Ideal Intersection: *Let I and J be ideals of $F[x_1, \cdots, x_n]$. Then*

$$I \cap J = (tI + (1 - t)J) \cap F[x_1, \cdots, x_n]$$

• *Proof*: The proof is a more rigorous version of the argument laid out above. First, suppose $f \in I \cap J$. Then $f \in I \rightarrow tf \in tI$ and $f \in J \rightarrow (1-t)f \in J$, so $f = (tf + (1-t)f \in tI + (1-t)J) \cap F[x_1, \cdots, x_n]$ (since $f \in F[x_1, \cdots, x_n]$). Conversely, suppose $f \in (tI + (1-t)J) \cap F[x_1, \cdots, x_n]$, so that $f(x_1, \cdots, x_n) = g(x_1, \cdots, x_n, t) + h(x_1, \cdots, x_n, t)$ for $g \in tI, h \in (1-t)J$. Then it follows that $f(x_1, \cdots, x_n) = g(x_1, \cdots, x_n, 0) + h(x_1, \cdots, x_n, 0) = 0 + h(x_1, \cdots, x_n, 0) \in 0I + (1 - 0)J = J$ and $f(x_1, \cdots, x_n) = g(x_1, \cdots, x_n, 1) + h(x_1, \cdots, x_n, 1) = g(x_1, \cdots, x_n) + 0 \in 1I + (1-1)J = I$, since $g \in tI \rightarrow g(x_1, \cdots, x_n, 0) \in 0I = \{0\} \rightarrow g(x_1, \cdots, x_n, 0) = 0$ and similarly $h \in (1-t)J \rightarrow h(x_1, \cdots, x_n, 1) \in 0J = \{0\} \rightarrow h(x_1, \cdots, x_n, 1) = 0$. It follows that $f \in I \cap J$, which proves the theorem. □

We can use the above result to develop an algorithm for determining generators of $I \cap J$: given $I = \langle f_1, \cdots, f_s \rangle, J = \langle g_1, \cdots, g_t \rangle$, we can consider $\langle tf_1, \cdots, tf_s, (1-t)g_1, \cdots, (1-t)g_t \rangle$, and then compute a Groebner basis with respect to $x_1 > \cdots > x_n > t$ and filter by polynomials which don't contain t. However, as mentioned above, when we can factor the generators of the ideals, finding generators for the intersection is easier - we can make use of the least common multiple. We finish the section with a few significant properties of ideal intersections, their associated varieties, and the least common multiple.

(Theorem) Intersection of Principal Ideals: *Let $I = \langle f \rangle, J = \langle g \rangle$ be principal ideals. Then $I \cap J = \langle h \rangle$ is principal. Moreover, $h = lcm(f, g)$.*
• *Proof*: TODO

Thus, we can compute the least common multiple of f, g by computing a basis for $\langle f \rangle$ and $\langle g \rangle$. We can use this to compute the greatest common divisor, by exploiting the identity

$$fg = \gcd(f, g) \cdot \text{lcm}(f, g)$$

In practice, of course, more efficient algorithms are used.

(Theorem) Variety of intersection is union of varieties: *Let I, J be ideals of $F[x_1, \cdots, x_n]$. Then*

$$\mathbf{V}(I \cap J) = \mathbf{V}(I) \cup \mathbf{V}(J)$$

• *Proof*: If a is in the union, then either $f(a) = 0$ for every $f \in I$ or $f(a) = 0$ for every $f \in J$; in either case, $f(a) = 0$ for every $f \in I \cap J$. The opposite inclusion follows because $IJ \subset I \cap J$ and because $\mathbf{V}(\cdot)$ is inclusion reversing. □

(Theorem) Radical splits over intersection: *Let I, J be ideals of $F[x_1, \cdots, x_n]$. Then*

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

• *Proof*: Suppose $f \in \sqrt{I \cap J}$, so that $f^m \in I \cap J$ for some m. Clearly, we have $f^m \in I$ and $f^m \in J$, which means $f \in \sqrt{I}$ and $f \in \sqrt{J}$ and hence $f \in \sqrt{I} \cap \sqrt{J}$. Conversely, if $f \in \sqrt{I} \cap \sqrt{J}$ then $f^{m_1} \in I, f^{m_2} \in J$ for some m_1, m_2. It follows that $f^{m_1+m_2} \in I \cap J$ and therefore $f \in \sqrt{I \cap J}$. □

4 Zariski Closures, Ideal Closures, and Saturations

Clearly, there are many sets which are not affine varieties, even sets one might expect to be varieties, such as projections of varieties or the set theoretic difference of two varieties. However, whether or not a set $S \subset F^n$ is a variety, $\mathbf{I}(S)$ is guaranteed to be an ideal (in fact, it's a radical ideal), which means $\mathbf{V}(\mathbf{I}(S))$ is guaranteed to be a variety. Similar to our study of parameterizations in which we identified the smallest varieties containing the image of a parameterization, in this section we'll study the smallest varieties containing certain kinds of generic sets. First, we prove the following intuitive and elegant theorem about $\mathbf{V}(\mathbf{I}(S))$.

(Theorem) Smallest variety containing a set: *Let S be a subset of F^n. Then $V = \mathbf{V}(\mathbf{I}(S))$ is the smallest variety containing S (here "smallest" is used in the usual sense - if W is an affine variety containing S then W contains V too).*

• *Proof*: Let W be an affine variety containing S. Since $\mathbf{I}(\cdot)$ and $\mathbf{V}(\cdot)$ are inclusion-reversing maps, it follows that $S \subset W \rightarrow \mathbf{I}(W) \subset \mathbf{I}(S) \rightarrow \mathbf{V}(\mathbf{I}(S)) = V \subset \mathbf{V}(\mathbf{I}(W)) = W$, which proves the theorem (the last step follows from the ideal-variety correspondence theorem). □.

Let's now define the structure alluded to above - the smallest variety containing a set.

(Definition) Zariski closure: *The **Zariski closure** of a subset of affine space is the smallest affine variety containing the set.*

• *Notation*: If S is a subset of a field or power of a field (i.e. $S \subset F^n$) then we denote the Zariski closure of S with $\overline{S}$.

• *Corollary*: Notice that if $S \subset F^n$ then $\overline{S} = \mathbf{V}(\mathbf{I}(S))$.

• *Properties of Zariski closures*:

1. $\mathbf{I}(\overline{S}) = \mathbf{I}(S)$
2. $S \subset T \rightarrow \overline{S} \subset \overline{T}$
3. $\overline{S \cup T} = \overline{S} \cup \overline{T}$

Zariski closures are precisely the algebraic machinery we need to prove the closure theorem from the last chapter. We restate and prove the theorem below.

(Theorem) Closure theorem: *Let F be an algebraically closed field and $V = \mathbf{V}(f_1, \cdots, f_s)$ be a variety in F^n. Then $\mathbf{V}(I_l)$ is the Zariski closure of $\pi_l(V)$ (recall that $I_l = \langle f_1, \cdots, f_s \rangle \cup F[x_{l+1}, \cdots, x_n]$ is the l^{th} elimination ideal of $I := \langle f_1, \cdots, f_s \rangle$ and π_l is the projection map from F^n to the last $n-1$ coordinates). In other words, $\mathbf{V}(I_l) = \overline{\pi_l(V)}$.*

• *Proof*: Seeing as $\pi_1(V)$ is a subset of F^n, the smallest variety containing the set is $V' := \mathbf{V}(\mathbf{I}(\pi_l(V)))$, so we must show $\mathbf{V}(I_l) = V'$. It was proven in the last chapter that $\pi_l(V) \subset \mathbf{V}(I_l)$, so it follows that $\mathbf{V}(\pi_l(V)) = V' \subset \mathbf{V}(\mathbf{V}(I_l)) = \mathbf{V}(I_l)$. Thus, we need only show that $\mathbf{V}(I_l) \subset V'$. To show this, we'll show that $\mathbf{I}(\pi_l(V)) \subset \sqrt{I_l}$, from which it will follow that $\mathbf{V}(I_l) = \mathbf{V}(\sqrt{I_l}) \subset \mathbf{V}(\mathbf{I}(\pi_l(V))) = V'$.
Suppose $f \in \mathbf{I}(\pi_l(V))$, which means $f(a_{l+1}, \cdots, a_l) = 0$ for any $(a_{l+1}, \cdots, a_l)$ in F^{n-l}; then, viewing f as a polynomial in $F[x_1, \cdots, x_n]$, we have $f(a_1, \cdots, a_n) = 0$ for any $(a_1, \cdots, a_n)$ in F^n, which means $f \in \mathbf{I}(V)$. It follows by Hilbert's Nullstellensatz that $f \in \sqrt{\langle f_1, \cdots, f_s \rangle}$, so that $f^m \in \langle f_1, \cdots, f_s \rangle$ for some m, which implies that $f^m \in \langle f_1, \cdots, f_s \rangle \cap F[x_{l+1}, \cdots, x_n] = I_l$ since f doesn't contain any of the first l variables and hence neither does f^m. This proves that $f \in \sqrt{I_l}$, which proves the theorem. □

In general, when $S \subset V$ for affine variety V and $\overline{S} = V$, we say S is **Zariski dense** in V. Thus, when the underlying field is algebraically closed, we know that $\pi_l(V)$ is Zariski dense in $\mathbf{V}(I_l)$. Next, we'll introduce two additional concepts, which are general enough to be definitons in their own right but which also help us compute the ideal corresponding to the Zariski closure of the difference of two varieties. Let's start with the first.

(Definition) Ideal quotient: *Let I, J be ideals of $F[x_1, \cdots, x_n]$. Then the **ideal quotient** of I and J, denoted $I : J$, is defined*

$$I : J = \{f \in F[x_1, \cdots, x_n] \text{ for which } \forall g \in J : fg \in I\}$$

• *Motivation*: In a loose sense, the above definition captures the notion of dividing the ideal I by the ideal J. We can arrive at this definition by taking every polynomial g in J, and keeping the quotient of every polynomial in I divisible by g and g. Thus, this is a form of an ideal-theoretic division, in which we take every polynomial h in I divisible by some polynomial in g and keep the quotient of the divsion of h by g (which, since $h = fg$ (because g divides h) for some f, is f). Lastly, notice that the above definition can be written

$$I : J = \{f \in F[x_1, \cdots, x_n] \text{ s.t. } fJ \subset I\}$$

where fJ is defined as element-wise multiplication; the above formulation suggests that $I : J$ consists of the quotients of the "division" of I by J, where we extend the notion of divisibility of numbers of polynomials, where f divides g if $\exists h$ s.t. $g = hf$ to ideals, where J divides I if $\exists f$ s.t. $fJ \subset I$. Moreover, the definition seems to be a natural extension of divisibility considering its relationship to ideal multiplication: just as $hf = g \iff f = \frac{g}{h}$, we have $KJ \subset I \iff K \subset I : J$ for ideals I, J, K, further supporting the intuitive idea that the colon in ideal quotients acts as a sort of ideal theoretic division.

• As expected, $I : J$ is itself an ideal, which furthermore contains I. Geometrically, ideal quotients correspond to to set difference between varieties:

$$\mathbf{I}(V) : \mathbf{I}(W) = \mathbf{I}(V - W)$$

for affine varieties V, W.

Let's prove some interesting and rather elegant consequences of the above definition.

(Theorem) Ideal quotients and Zariski closures of differences of varieties: *Let I, J be ideals of $F[x_1, \cdots, x_n]$ and V, W be varieties in F^n. Then the following hold.*

1. $\mathbf{V}(I) = \mathbf{V}(I + J) \cup \mathbf{V}(I : J)$
2. $V = (V \cap W) \cup \overline{V - W}$
3. $\overline{\mathbf{V}(I) - \mathbf{V}(J)} \subset \mathbf{V}(I : J)$

• *Proof*: We'll use (2) and (3) to prove (1), so let's start with (2).
Since V is a variety which obviously contains $V - W$, by definition the smallest variety containing $V - W$ must be contained in V, so $\overline{V - W} \subset V$. Clearly, $V \cap W \subset V$, so it follows that $\overline{V - W} \cup (V \cap W) \subset V$. To prove the reverse inclusion, simply note that identity $V = (V \cap W) \cup (V - W)$ (this identity is a symbolic statement of the fact that V is composed of the elements in V which are also in$W$ and those that aren't), taken with the identity $V - W \subset \overline{V - W}$ implies $V \subset (V \cap W) \cup \overline{V - W}$.
To prove (3), we'll show that $I : J \subset \mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))$, from which it follows that $\mathbf{V}(\mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))) = \overline{\mathbf{V}(I) - \mathbf{V}(J)} \subset \mathbf{V}(I : J)$ since $\mathbf{V}(\cdot)$ is inclusion-reversing. Suppose $f \in I : J$ and $a \in \mathbf{V}(I) - \mathbf{V}(J)$. Since $fg \in I$ for any $g \in J$ and since $a \in \mathbf{V}(I)$, we have $f(a)g(a)$ for every $g \in J$, which means $f(a) = 0$ for every $a \in \mathbf{V}(I) - \mathbf{V}(J)$, since $a \notin \mathbf{V}(J) \to \exists g \in J$ for which $g(a) \neq 0$ which forces $f(a) = 0$. This shows that $f \in \mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))$, proving the claim.
Let's now prove (1). Since the variety of ideal addition split over intersection, as proven in the last chapter, we know that $\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J)$. Applying (2) on $V = \mathbf{V}(I), W = \mathbf{V}(J)$, we have

$$\mathbf{V}(I) = (\mathbf{V}(I) \cap \mathbf{V}(J)) \cup \overline{\mathbf{V}(I) - \mathbf{V}(J)} \subset \mathbf{V}(I + J) \cup \mathbf{V}(I : J)$$

where the inclusion in the last step follows from (3). We know that from the properties of ideal summation, $I \subset I + J \to \mathbf{V}(I+J) \subset \mathbf{V}(I)$, and since $I \subset I : J$ we have $\mathbf{V}(I : J) \subset \mathbf{V}(I)$, proving $\mathbf{V}(I+J) \cup \mathbf{V}(I : J) \subset \mathbf{V}(I)$, from which (1) follows. □

An interesting question we might ask is under what conditions the third relationship becomes equality. This is a natural question because $\mathbf{V}(I + J)$ from part (1) in the above theorem "matches up" with the $V \cap W$ in part (2), since $\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J)$; if we imagine V as the variety of I and W as the variety of J then, parts (1) and (2) of the above theorem would be exactly equivalent if $\overline{V - W}$ similarly matched up with $\mathbf{V}(I : J)$, which is precisely equivalent to part (3) of the theorem being an equality rather than containment. In general, we don't have equality, but in many cases we can force equality if we consider higher powers of J. That is, there is a power m for which $I : J^m = \overline{\mathbf{V}(I) - \mathbf{V}(J)}$.
Thus, we can turn part (3) of the theorem into an equality by completely dividing out J from I, which causes parts (1) and (2) to reduce to each other. It's this idea that motivates the following definition.

(Definition) Saturation of an ideal: *Let I, J be ideals of $F[x_1, \cdots, x_n]$. We define the **saturation** of I and J, denoted $I : J^\infty$, with*

$$I : J^\infty = \{f \in F[x_1, \cdots, x_n] \text{ where } \forall g \in J : fg^m \in I \text{ for some } m\} = \{f \in F[x_1, \cdots, x_n] \text{ where } fJ^m \subset I \text{ for some } m\}$$

• *Motivation*: Extending the intuition of ideal quotients as the result of an elementwise division of polynomials in I by the ideal J, the saturation of an ideal is the division by the largest possible power of J, analogous to completely dividing a

power from an integer (e.g. $k^p \mid n$ but $k^{p+1} \nmid n$). Here, we use the term "largest possible power" of J in the following sense - as we successively divide by larger powers of J, we get an ascending chain of ideals; the saturation is the stabilization point:

$$I : J \subset I : J^2 \subset I : J^3 \subset \cdots \subset I : J^N \subset I : J^{N+1}$$

(note that it makes sense that $I : J^k \subset I : J^{k+1}$, since $J^{k+1} \subset J^k$ and quotient is meant to be a form of ideal division) We're guaranteed that for some N we have $I : J^N = I : J^{N+1} = I : JN + 2 = \cdots$ and it follows from the definition above that $I : J^\infty = I : J^N$. Of course, it also follows that $I : J^\infty$ is a polynomial ideal itself.

- *Properties*: Some properties of ideal saturation with respect to the entire field $F[x_1, \cdots, x_n]$:

1. $I : F[x_1, \cdots, x_n] = I : F[x_1, \cdots, x_n]^\infty = I$
2. $J \subset I \iff I : J = F[x_1, \cdots, x_n]$
3. $J \subset \sqrt{I} \iff I : J^\infty = F[x_1, \cdots, x_n]$

(Theorem) Radical of saturation of an ideal: *Let I, J be polynomial ideals. Then $\sqrt{I : J^\infty} = \sqrt{I} : J$.*

- *Proof*: Let's first show that $\sqrt{I : J^\infty} \subset \sqrt{I} : J$. For any $f \in \sqrt{I : J^\infty}$,

$$f^m \in I : J^\infty \text{for some } m, \rightarrow \forall g \in J : f^m g^n \in I \text{for some } n, \rightarrow (fg)^{\max(m,N)} \in I \rightarrow fg \in \sqrt{I} \rightarrow f \in \sqrt{I} : J$$

Conversely, if $f \in \sqrt{I} : J$, then

$$\forall g \in J : fg \in \sqrt{I} \rightarrow f^m g^m \in I \text{ for some } m \ \rightarrow f^m \in I : J^\infty \rightarrow f \in \sqrt{I : J^\infty}$$

which proves the theorem. □

Let's now examine the relation of saturations to geometry.

(Theorem) Ideal saturations and Zariski closures of differences of varieties: *Let I, J be ideals of $F[x_1, \cdots, x_n]$. Then*

1. $\mathbf{V}(I) = \mathbf{V}(I + J) \cup \mathbf{V}(I : J^\infty)$
2. $\overline{\mathbf{V}(I) - \mathbf{V}(J)} \subset \mathbf{V}(I : J^\infty)$, with equality if F is algebraically closed.

- *Proof*:
  - *Corollary*: If F is algebraically closed and I is radical, then $\mathbf{V}(I : J) = \overline{\mathbf{V}(I) - \mathbf{V}(J)}$.

Thus, when F is algebraically closed, the results of the above theorem and the theorem on ideal quotients and Zariski closures of variety differences show that the two decompositions

$$\mathbf{V}(I) = \mathbf{V}(I + J) \cup \mathbf{V}(I : J^\infty) = (\mathbf{V}(I) \cap \mathbf{V}(J)) \cup \overline{\mathbf{V}(I) - \mathbf{V}(J)}$$

are precisely the same. In other words, $I : J^\infty$ is the ideal-theoretic analog of $\overline{\mathbf{V} - \mathbf{V}(J)}$ (recall that earlier we discussed that because $\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J)$ the other two respective terms in the two decompositions are similarly analogous). We'll wrap up the section with some useful results which help in the computation of ideal quotients and saturations, followed by an algorithm for computing generators of quotients and saturations.

(Theorem) Quotient over ideal sum splits into intersection: *Let I and $J_i, 1 \leq i \leq n$ be polynomial ideals. Then*

$$I : \left(\sum_{i=1}^n J_i \right) = \bigcap_{i=1}^n (I : J_i)$$
$$I : \left(\sum_{i=1}^n J_i \right)^\infty = \bigcap_{i=1}^n (I : J_i)^\infty$$

- *Proof*: TODO
- *Corollary*: It follows as a corollary that $I : \langle f_1, \cdots, f_s \rangle = \bigcap_{i=1}^s (I : \langle f_i \rangle)$ and that $I : \langle f_1, \cdots, f_s \rangle^\infty = \bigcap_{i=1}^s (I : \langle f_i \rangle^\infty)$.

Let's now investigate how to compute generators of ideal quotients and saturations. The corollary to the above theorem shows that in order to compute generators, it's sufficient to consider principal ideals only. This leads us to the following two theorems.

(Theorem) Generators of ideal quotients: *For polynomial ideal I and $f \in F[x_1, \cdots, x_n]$, let $I \cap \langle f \rangle = \langle f_1, \cdots, f_s \rangle$. Then*

$$I : \langle f \rangle = \left\langle \frac{f_1}{f}, \cdots, \frac{f_s}{f} \right\rangle$$

- *Proof*: Suppose $g \in \left\langle \frac{f_i}{f} \right\rangle$ so that

$$g = \sum_i \frac{f_i}{f}$$

Then $\forall h \in \langle f \rangle : \exists q_f$ s.t. $h = q_f f$, so we have

$$\forall h \in \langle f \rangle : hg = q_f fg = q_f \sum_i f_i \to g \in I \cap \langle f \rangle \subset I$$

which shows that $g \in I : \langle f \rangle$. Conversely, suppose that $g \in I : \langle f \rangle$, so that we have $gf \in I$. Clearly, $gf \in \langle f \rangle$, so $gf \in I \cap \langle f \rangle$. Then

$$gf = \sum_i h_i f_i \to g = \sum_i h_i \frac{f_i}{f} \text{ for } h_i \in F[x_1, \cdots, x_n]$$

since f_i is a generator of $\langle f \rangle$, and so is divisible by f. It follows that $g \in \langle \frac{f_i}{f} \rangle$ as desired. $\square$

- *Intuition*: When considering principal ideals, which have the property of containing only elements which are multiples of their generator, the definition of ideal quotients reduces to

$$I : \langle f \rangle = \{g \in F[x_1, \cdots, x_n] \text{ s.t. } : g\langle f \rangle \in I\} = \{g \in F[x_1, \cdots, x_n] \text{ s.t. } \langle fg \rangle \subset I\} = \{g \in F[x_1, \cdots, x_n] \text{ s.t. } fg \in I\}$$

Thus, we want to consider polynomials in I which are divisible by f. Because $I : \langle f \rangle$ is, intuitively, the result of dividing I by multiples of f, it's an elegant and natural result that we can find a basis for $I : \langle f \rangle$ simply by taking the basis for polynomials in I which are divisible by f and "dividing out" the f.

(Theorem) Generators of ideal saturations: *Let $I = \langle f_1, \cdots, f_s \rangle$ be a polynomial ideal and $f \in F[x_1, \cdots, x_n]$. Then*

$$I : \langle f \rangle^\infty = \langle f_1, \cdots, f_s, 1 - fy \rangle \cap F[x_1, \cdots, x_n]$$

- *Proof*: Let $J = \langle f_1, \cdots, f_s, 1 - fy \rangle \subset F[x_1, \cdots, x_n, y]$. TODO
- *Corollary*: The elimination theorem implies that if G is a Groebner basis for J with respect to $y > x_1 > \cdots > x_n$ then $G \cap F[x_1, \cdots, x_n]$ is a basis for $I : \langle f \rangle^\infty$.

We can use the above two theorems to algorithmically compute bases for ideal quotients and saturations. For ideal quotients, given $I = \langle f_1, \cdots, f_s \rangle$ and $J = \langle g_1, \cdots, g_t \rangle$, we can compute a basis for $I : J$ by first computing bases for each $I : \langle g_j \rangle$ using the above theorem (specifically, we can compute a basis for $I \cap \langle g_i \rangle$ (we studied how to do this algorithmically when we covered the computation of ideal intersections in the last chapter) and dividing every term in the basis by g_i) and then putting the bases together by inductively applying the ideal intersection algorithm $t - 1$ times, since

$$I : \langle g_1, g_2 \rangle = (I : \langle g_1 \rangle) \cap (I : \langle g_2 \rangle)$$

We can compute bases for the saturation $I : J^\infty$ by first computing bases for each $I : \langle g_i \rangle^\infty$ using the above theorem (specifically, compute a Groebner basis G for $\langle f_1, \cdots, f_s, 1 - g_i y \rangle$ and computing $G \cap F[x_1, \cdots, x_n]$) and then putting the bases back together the same way we did in computing bases for ideal quotients, i.e. by inductively applying the intersection algorithm $t - 1$ times.

5 Irreducible Varieties and Prime Ideals

We already know that the union of two varieties is itself a variety; moreover, many varieties can be decomposed into the union of sub-varieties. Because a variety can be viewed as the intersection of all the zero sets of the polynomials generating the variety, often times varieties will end up being unions of separate continuous structures. For example, $\mathbf{V}(xy, yz)$ is the union of a line and a plane in $\mathbb{R}^3$. Intuitively, the line and plane, and by extension other such continuous structures, are more fundamental units than the variety they compose, and can't be broken down further the way we broke down $\mathbf{V}(xz, yz)$. In this section, we'll formalize and study these intuitive notions of fundamental varieties and decomposing varieties into fundamental sub-varieties, similar to decomposing integers into prime factors or polynomials into irreducible elements.

(Definition) Irreducible: *An affine variety V is **irreducible** if*

$$V = V_1 \cup V_2 \to V = V_1 \text{ or } V = V_2$$

for any affine varieties V_1, V_2.

• *Motivation*: Intuitively, this formalizes the notion that V can't be broken down into sub-varieties, and is itself an "unbreakable" continuous structure. This is done with the constraint that any decomposition of V into further subvarieties is vacuous.

Let's now extend this definition to ideals, which incidentally also connects with the same idea of irreducibility from ring theory.

(Definition) Prime ideal: *A polynomial ideal $I \subset F[x_1, \cdots, x_n]$ is **prime** if*

$$\forall f, g \in F[x_1, \cdots, x_n] : fg \in I \to f \in I \text{ or } g \in I$$

• *Motivation*: This extends an older, roundabout definition of integer primality, which goes $p \in \mathbb{P} \iff \forall n, m \in \mathbb{Z} : p = nm \to p = n$ or $p = m$. This is a good choice of definition to base the above one off, as we can't use the traditional definition based on factorization since we don't have any appropriate notion of "factoring" an ideal.

Ideally, our intuitive notions of primality and irreducibility for ideals and varieties, respectively, should be compatible. This next theorem shows that this is indeed the case.

(Theorem) Irreducible varieties correspond with prime ideals: *An affine variety V is irreducible if and only if $\mathbf{I}(V)$ is prime.*

• *Proof*: Suppose V is irreducible, and consider a polynomial $fg \in \mathbf{I}(V)$. Letting $V_1 = V \cap \mathbf{V}(f), V_2 = V \cap \mathbf{V}(g)$, we obtain the identity $V = V_1 \cup V_2$, since $V_1 \cup V_2 = (V \cap \mathbf{V}(f)) \cup (V \cap \mathbf{V}(g))$ is the set of points in V over which both f and g are zero, which is to say, the set of points over which fg is zero, which is, by definition, V. Since V is irreducible, we can assume $V = V_1$, so that $V = V \cap \mathbf{V}(f) \to \mathbf{V}(f) \subset V \to f$ vanishes over V, which means $f \in \mathbf{I}(V)$, and therefore $\mathbf{I}(V)$ is prime.

Conversely, suppose $\mathbf{I}(V)$ is prime, and let $V = V_1 \cup V_2$ for affine varieties V_1, V_2. If $V \neq V_1$, then it follows that $\mathbf{I}(V) = \mathbf{V}(V_2)$ which means $V = V_2$, proving that either $V = V_1$ or $V = V_2$. To see why $\mathbf{I}(V) = \mathbf{V}(V_2)$, note that $V_2 \subset V \to \mathbf{I}(V) \subset \mathbf{I}(V_2)$, so we need only prove the opposite inclusion. Similarly, $\mathbf{I}(V) \subset \mathbf{I}(V_1)$, but isn't equal to either one. Let $f \in \mathbf{I}(V_1) - \mathbf{I}(V)$ and $g \in \mathbf{I}(V_2)$, so that $V = V_1 \cup V_2 \to fg$ vanishes on V, and therefore $fg \in \mathbf{I}(V)$, which means, since $\mathbf{I}(V)$ is prime, one of f, g lie in $\mathbf{I}(V)$. It can't be f due to the way we chose f, so we must have $g \in \mathbf{I}(V)$, and hence $\mathbf{I}(V_2) \subset \mathbf{I}(V)$, proving the theorem. □

• *Corollary*: It follows that when F is algebraically closed, $\mathbf{I}(\cdot)$ and $\mathbf{V}(\cdot)$ induce a one-to-one correspondence between irreducible varieties and prime ideals.

Next, let's look at an intuitive way to characterize if a variety is irreducible or not.

(Theorem) Irreducibility and Zariski subsets: *A variety V is irreducible if and only if for every variety $W \subset V$, $V - W$ is Zariski dense in V.*

• *Proof*: Suppose V is irreducible, so that we can decompose $V = W \cup \overline{V - W}$. But V is irreducible and by assumption $V \neq W$, so $V = \overline{V - W}$, showing that the set difference is Zariski dense in V. Conversely, suppose $V = V_1 \cup V_2$. If $V_1 \neq V$ then by assumption the set difference $\overline{V - V_1} = V$. However, $V = V_1 \cup V_2 \to V - V_1 \subset V_2 \to \overline{V - V_1} \subset V_2 \to V \subset V_2$ and therefore $V = V_2$. Thus, either $V_1 = V$ or $V_2 = V$, showing that V is irreducible. □

The above theorem on the correspondence between prime ideals and irreducible varieties has an interesting application to polynomial parameterizations, because the ideal of the variety defined by such a paramaterization can be shown to be prime. This is because any product of polynomials fg that's zero on the paramaterization must have either f or g or both be zero at infinitely many points, since the paramaterization is, of course, continuous and therefore uncountable. Thus, at least one of f, g is the zero polynomial and hence in the ideal. Let's show that this argument holds more generally.

(Theorem) Polynomial Paramaterizations are Irreducible: *Let V be a variety defined parametrically by*

$$\begin{aligned} x_1 &= f_1(t_1, \cdots, t_m) \\ &\vdots \\ x_n &= f_n(t_1, \cdots, t_m) \end{aligned}$$

for polynomials $f_1, \cdots, f_n$. Then V is irreducible.

• *Proof*: As in the previous chapter, define $f : F^m \to F^n$ by $f(t_1, \cdots, t_m) = (f_1(t_1, \cdots, t_m), \cdots, f_n(t_1, \cdots, t_m))$, so that V is the Zariski closure of $f(F^m)$, and therefore $\mathbf{I}(V) = \mathbf{I}(f(F^m))$. The key observations we'll use to show that $\mathbf{I}(V)$ is prime, and therefore V is irreducible, are that

$$\forall g \in F[x_1, \cdots, x_n] : g \circ f = g(f(t_1, \cdots, t_m)) = g(f_1(t_1, \cdots, t_m), \cdots, f_n(t_1, \cdots, t_m)) \in F[x_1, \cdots, x_n]$$

and

$$\forall g, h \in F[x_1, \cdots, x_n] : (gh) \circ f = g(f(t_1, \cdots, t_m))h(f(t_1, \cdots, t_m)) = (g \circ f)(h \circ f)$$

It follows that for any polynomial $gh \in \mathbf{I}(V)$, $(gh) \circ f = (g \circ f)(h \circ f) = 0 \rightarrow g \circ f = 0$ or $h \circ f = 0$, which means either $g \in \mathbf{I}(V)$ or $h \in \mathbf{I}(V)$. This proves that $\mathbf{I}(V)$ is a prime ideal, which proves the theorem. $\square$

This theorem aligns with the intuition for "fundamental" varieties we discussed in the beginning of this section, by showing that the continuous, connected structures, which are precisely by the range of polynomial parameterizations, from which varieties are often built are, seeing as they clearly can't be themselves broken into further continuous structures, the fundamental units of varieties, in that they are guaranteed to be irreducible. Of course, there are continuous structures in space which can't be defined by polynomial parameterizations, such as those given by rational parameterizations. Though this idea is not true in general, it does extend to rational parameterizations, as the next theorem shows.

(Theorem) Rational Parameterizations are Irreducible: *Let F be an infinite field and V be the variety of the rational parameterization*

$$x_1 = \frac{f_1(t_1, \cdots, t_m)}{g_1(t_1, \cdots, t_m)}$$

$$\vdots$$

$$x_n = \frac{f_n(t_1, \cdots, t_m)}{g_n(t_1, \cdots, t_m)}$$

for polynomials $f_1, \cdots, t_n, g_1, \cdots, g_n \in F[t_1, \cdots, t_m]$. Then V is irreducible.

• *Proof*: As in the previous chapter, we'll define f to be the mapping given by the above parameterization. To avoid dividing by zero, we exclude the zeros of the g_i's, and thus define

$$f : F^m - W \rightarrow F^n \text{ by } f(t_1, \cdots, t_m) = \left(\frac{f_1(t_1, \cdots, t_m)}{g_1(t_1, \cdots, t_m)}, \cdots, \frac{f_n(t_1, \cdots, t_m)}{g_n(t_1, \cdots, t_m)} \right)$$

where $W = \mathbf{V}(g_1 \cdots g_n)$. Then, as before, V is the Zariski closure of $f(F^m - W)$, i.e. the range of f, which means $\mathbf{I}(V)$ is the set of polynomials h for which $h \circ f = 0$ over $F^m - W$. We can't simply apply the same argument from the case of polynomial parameterizations because $h \circ f$ may be rational, not polynomial. We can get around this by "clearing" the denominators as follows. Since by definition $g_1 \cdots g_n \neq 0$ on $F^m - W$, it follows that $\forall h \in F[x_1, \cdots, x_n] : (g_1 \cdots g_n)^N (h \circ f)$ is a polynomial in $F[t_1, \cdots, t_m]$, and has the exact same zeros as $h \circ f$. Thus,

$$h \in \mathbf{I}(V) \iff (g_1 \cdots g_n)^N (h \circ f) = 0$$

where N is the total degree of h. We can use this lemma to show that $\mathbf{I}(V)$ is prime. For any $p, q \in \mathbf{I}(V)$, with respective degrees M, N, we have

$$(g_1 \cdots g_n)^{M+N}(pq \circ f) = (g_1 \cdots g_n)^{M+N}(p \circ f)(q \circ f) = 0$$

which means one of $(g_1 \cdots g_n)^{M+N} p, (g_1 \cdots g_n)^{M+N} q$ must be the zero polynomial. This shows that either $p \in \mathbf{I}(V)$ or $q \in \mathbf{I}(V)$, which proves that $\mathbf{I}(V)$ is prime, proving the theorem. $\square$

We'll finish up this section by introducing another important concept in ideal theory relating to an intuitive notion of the size of an ideal. To motivate this definition, consider the simplest variety in F^n - the variety consisting of a single point, $\{(a_1, \cdots, a_n)\}$, which we can view as given by the parameterization

$$f_1 = a_1$$

$$\vdots$$

$$f_n = a_n$$

Clearly, the variety is irreducible, and its ideal is given by $\langle x_1 - a_1, \cdots, x_n - a_n \rangle$. This ideal has another distinctive property: it's maximal in the sense that the only ideal which contains the ideal is the entire ring $F[x_1, \cdots, x_n]$.

(Definition) Maximal: *An ideal $I \subset F[x_1, \cdots, x_n]$ is **maximal** if $I \neq F[x_1, \cdots, x_n]$ and for any ideal J which contains I, we have $J = I$ or $J = F[x_1, \cdots, x_n]$.*

(Definition) Proper: *An ideal is proper if it's not equal to its containing ring.*

In accordance with our motivation, we prove the following basic theorem.

(Theorem) Ideals of single points are maximal: *Any ideal of the form* $\langle x_1 - a_1, \cdots, x_n - a_n \rangle$*, for* $(a_1, \cdots, a_n) \in F^n$ *is maximal.*

• *Proof*: Let J be an ideal, not equal to $I := \langle x_1 - a_1, \cdots, x_n - a_n \rangle$, which contains I. Then let $f \in J$ such that $f \notin I$. Applying the division algorithm, we can find polynomials such that

$$f = A_1 \cdot (x_1 - a_1) + \cdots A_n \cdot (x_n - a_n) + b$$

for some $b \in F$. It follows that $b = f - A_1 \cdot (x_1 - a_1) + \cdots A_n \cdot (x_n - a_n) \in J$, which means $1 = \frac{1}{b} \cdot b \in J$ (note that $b \neq 0$ since if it were we'd have $f \in I$), which proves $J = F[x_1, \cdots, x_n]$ and therefore I is maximal. □

(Theorem) Maximal ideals are prime: *Any maximal ideal in* $F[x_1, \cdots, x_n]$ *is prime.*

• *Proof*: Let I be a proper, non-prime ideal of $F[x_1, \cdots, x_n]$. We'll show that I is not maximal, proving the contrapositive. For any $fg \in I$ such that $f, g \notin I$, we'll show that $\langle f \rangle + I$ is a proper ideal containing I. Clearly, $I \subset \langle f \rangle + I$ and the inclusion is proper since $f \notin I$. To show that the ideal is proper, consider that if we had $1 \in \langle f \rangle + I$ then $1 = cf + h$ for some $c \in F[x_1, \cdots, x_n], h \in I$ which means $g = cfg + hg \in I$, a contradiction. Thus, I is not maximal, proving the theorem. □

(Theorem) Maximal ideals correspond to points: *Let* F *be an algebraically closed field. Then every maximal ideal of* $F[x_1, \cdots, x_n]$ *is of the form* $\langle x_1 - a_1, \cdots, x_n - a_n \rangle$ *for some* $(a_1, \cdots, a_n) \in F$*.*

• *Proof*: Let $I \subset F[x_1, \cdots, x_n]$ be a maximal ideal. By the weak Nullstellensatz, $I \neq F[x_1, \cdots, x_n] \rightarrow \mathbf{V}(I) \neq \emptyset$. Since every $f \in I$ vanishes over every point $(a_1, \cdots, a_n) \in \mathbf{V}(I)$ by definition, it follows trivially that

$$f \in \mathbf{I}(\{(a_1, \cdots, a_n)\}) \rightarrow I \subset \mathbf{I}(\{(a_1, \cdots, a_n)\}) = \langle x_1 - a_1, \cdots, x_n - a_n \rangle$$

Since I is maximal and $\langle x_1 - a_1, \cdots, x_n - a_n \rangle \neq F[x_1, \cdots, x_n]$ we have $I = \langle x_1 - a_1, \cdots, x_n - a_n \rangle$, proving the theorem. □

• *Corollary*: Notice that any point in $\mathbf{V}(I)$ will work in the above proof, so the $(a_1, \cdots, a_n)$ is not unique. However, if F is algebraically closed, then the above mapping is indeed one-to-one.

Note that the above theorem extends our algebra-geometry dictionary by showing that maximal ideals correspond with points in the underlying field (assuming the field is algebraically closed). Moreover, every non-empty irreducible variety corresponds to a proper, prime ideal.

6 Decomposition of a Variety into Irreducibles

In the last section, we motivated prime ideals as a general algebraic extension of primes in the integers, asserting that both play the same role. Given the nature of irreducible varieties, and their correspdondence with prime ideals, it isn't surprising that irreducible varieties, like prime ideals, have the same relationship to their containing affine space that prime numbers do with the integers. Specifically, in this section we'll study the analogous extension of the fundamental theorem of arithmetic, and answer the question of whether varieties can be built up out of irreducibles. First, we translate the ascending chain condition into a statement about chains of varieties.

(Theorem) Descending Chain Condition: *Any descending chain of varieties*

$$V_1 \supset V_2 \supset \cdots$$

must stabilize. That is, $\exists N$ *s.t.* $V_N = V_{N+1} = \cdots$*.*

• *Proof*: The statement easily follows from the ascending chain condition. Because passing to ideals is inclusion-reversing, the above descending chain becomes

$$\mathbf{I}(V_1) \subset \mathbf{I}(V_2) \subset \cdots$$

which stabilizes at some N by the ascending chain condition. Since $\mathbf{I}(V_N) = \mathbf{I}(V_{N+1}) = \cdots$, it follows that $V_N = V_{N+1} = \cdots$. □

We now use this theorem to prove what we suspected in the beginning of this section, that every variety can be broken into irreducibles.

(Theorem) Varieties factor into irreducibles: *Let* V *be an affine variety. Then* V *can be written as a finite union of irreducible varieties* V_i

$$V = \bigcup_i V_i$$

• *Proof*: We prove the theorem by contradiction. Suppose V can't be expressed as the union of a finite number of irreducible varieties. Then clearly V is not irreducible (if it were, we could trivially factor it as $V = V$), so we can write

$V = V_1 \cup V_2$ where $V \neq V_1, V \neq V_2$ and with V_1, V_2 not irreducible. Moreover, at least one of V_1, V_2, say V_1, mustn't be expressed as a finite union of irreducibles either, since if both V_1, V_2 are then so is V. But then we can repeat the argument for V_1, finding non-irreducible V_3, V_4 such that $V_1 = V_3 \cup V_4$ with $V_1 \neq V_3, V_1 \neq V_4$. We may repeat this argument for V_3 indefinitely, since at no point can we reach a variety which can be expressed as a finite union of irreducibles, since then V could be too. Thus, we have

$$V_1 \supset V_3 \supset \cdots$$

with every variety in the above chain distinct. This violates the descending chain condition, and therefore V must be expressible as a finite union of irreducibles. □

This theorem cements our geometric intuition of affine varieties as finite unions of continuous structures in n-dimensional affine space, from curves to surfaces and their higher-order analogs. The next natural question to answer is whether such representations are unique. Of course, trivial counterexamples to such unique decompositions are those in which one of the irreducibles is contained in another, since then the smaller variety's inclusion doesn't affect the union. As such, we'll study the uniqueness of non-trivial decompositions, formally defined below.

(Definition) Minimal decomposition: *Let V be an affine variety. A decomposition*

$$V = V_1 \cup \cdots \cup V_m$$

*is a **minimal decomposition** if $V_i \not\subset V_j, \forall i \neq j$. We call the V_i's the **irreducible components** of V.*

(Theorem) Minimal decompositions are unique: *Every affine variety V has a minimal decomposition*

$$V = V_1 \cup \cdots \cup V_m$$

which is unique up to the order in which the irreducible components are written.

• *Proof*: Clearly, minimal decompositions always exist, since we can always express V as a finite union of irreducibles, and can iteratively remove irreducibles which are contained in some other irreducible. To show uniqueness, suppose, in addition to the above minimal decomposition,

$$V = V_1' \cup \cdots \cup V_m'$$

is also a minimal decomposition. It follows that

$$V_1 \subset V \to V_i = V_i \cap V = V_i \cap \bigcup_j V_j' = \bigcup_j (V_i \cap V_j')$$

Since V_i is irreducible, we must have $V_i = V_i \cap V_j'$ for some j, so that $V_i \subset V_j'$. But we can apply the exact same argument to V_j' to find a V_k such that $V_j' \subset V_k$. This means that $V_i \subset V_j' \subset V_k$, but since the decompositions are minimal, $V_i \not\subset V_k$ implies that we must have $V_i = V_j' = V_k$, i.e. $i = k$. This shows that every V_i appears in the second decomposition, and a similar argument for the reverse similarly implies that every V_j' appears in the first decomposition. Therefore, the two decompositions are the same, merely with the order of the varieties changed. This proves that the minimal decomposition is unique. □

It should be noted here that this proof is only possible because the decomposition is finite, and doesn't hold for infinite decompositions. As such, all the theory on irreducibles can be traced back to Hilbert's basis theorem. Before moving on to analogous theorems for reducing ideals to combinations of prime ideals, we give one result which relates irreducible components to Zariski closures.

(Theorem) Zariski density and Irreducible Components: *Let W, V be affine varieties with $W \subset V$. Then $V - W$ is Zariski dense in V (i.e. $\overline{V - W} = V$) if and only if W contains no irreducible component of V.*

• *Proof*: First suppose that W contains none of the irreducible components $V_1, \cdots, V_m$ of V. By definition $V_i \cap W \subset V_i$, and where the containment is strict by assumption. It follows that since V_i is irreducible and strictly contains $V_i \cap W$, the former is Zariski dense in the latter: $\overline{V_i \cap W} = V_i$. It now follows that

$$\overline{V - W} = \overline{\bigcup_i V_i - W} = \overline{\bigcup_i (V_i - (V_i \cap W))} = \bigcup_i \overline{V_i - (V_i \cap W)} = \bigcup_i V_i = V$$

(note that the second equality is a set theoretic identity and the fourth follows from the above) wihch proves that the difference $V - W$ is Zariski dense in V. To prove the other direction, suppose $\overline{V - W} = V$. TODO □

We conclude this section with some analogous results about ideals, revealing a similar structuring that can also be interpreted as an extension of the fundamental theorem of arithmetic.

(Theorem) Radical ideals factor into primes: *If F is algebraically closed then every radical ideal of $F[x_1, \cdots, x_n]$ can be expressed as a finite intersection of prime ideals, none of which contain any other. In other words,*

$$\forall I \subset F[x_1, \cdots, x_n] : I = \sqrt{I} \rightarrow I = \bigcap_i P_i \text{ where } P_i \subset F[x_1, \cdots, x_n] \text{ is prime, and } P_j \not\subset P_i, \text{ for } i \neq j$$

Moreover, the above decomposition is unique.

• *Proof*: Because of the ideal-variety correspondence, this result is a simple corollary of the analagous theorems for vareties. Specifically, since every variety V can be broken down into a minimal finite union of irreducible varieties, and since irreducible varieties correspond to prime ideals, the theorem follows from the fact that every radical ideal is in bijective correspondence with a unique variety. □

Let's now give an explicit description of the prime factorization of ideals.

(Theorem) Prime factors of a radical ideal are principal quotients: *Let F be an algebraically closed field, and a I be a proper radical ideal of $F[x_1, \cdots, x_n]$. If*

$$I = \bigcap_i P_i$$

is the decomposition of I into prime ideals, then the P_i's above are precisely the proper, prime ideals in the set

$$\{I : \langle f \rangle, f \in F[x_1, \cdots, x_n]\}$$

• *Proof*: Let S denote the above set in question. First, notice that for every element of S we can write

$$I : \langle f \rangle = \left(\bigcap_i P_i \right) : \langle f \rangle = \bigcap_i (P_i : \langle f \rangle)$$

We want to show that if the element happens to be both proper and prime, then it corresponds to some P_i. Suppose the above $I : \langle f \rangle$ is proper and prime. Because $I : \langle f \rangle$ is prime, the above equality implies that it's equal to some $P_k : \langle f \rangle$ (this follows from the lemma that if $P = I_1 \cap I_2$ where P is prime and $I_1 = \langle f_i \rangle, I_2 = \langle g_j \rangle$ then $I_1 I_2 = \langle f_i g_j \rangle \subset I_1 \cap I_2 = P \rightarrow f_i g_j \in P \rightarrow f_i \in P, \forall i$ or $g_j \in P, \forall j \rightarrow P = I_1$ or $P = I_2$). But, P_k is prime, which means that if $f \in P_k$ then $P_k : \langle f \rangle = F[x_1, \cdots, x_n]$ (this of course holds for even non-prime P_k) and otherwise if $f \notin P_k$ then $P_k : \langle f \rangle = P_k$ (this follows from P_k being prime). Therefore,

$$I : \langle f \rangle \text{ is proper } \rightarrow I : \langle f \rangle = P_k$$

which proves that the proper, prime elements of S correspond to primes in the decomposition of I.
We have yet to show the converse, that every prime ideal P_k in the minimal decomposition of I corresponds to some prime, proper element of S. The idea behind the proof of this is that we can arrive at P_k simply by dividing any element not in P_k from the decomposition out of I. More precisely, for any such P_k, choose a polynomial f from the minimal decomposition of I above but with P_k removed, i.e. $f \in \bigcap_{i \neq k} P_i - P_k$. Then $I : \langle f \rangle = P_k$, since by design and the fact that $P_k : \langle f \rangle = P_k$ or $F[x_1, \cdots, x_n]$ depending on if $f \in P_k$ proved above implies

$$P_k : \langle f \rangle = P_k \text{ and } P_i : \langle f \rangle = F[x_1, \cdots, x_n], i \neq k$$

and therefore

$$I : \langle f \rangle = \bigcap_i (P_i : \langle f \rangle) = (P_k : \langle f \rangle) \cap \bigcap_{i \neq k} (P_i : \langle f \rangle) = P_k \cap F[x_1, \cdots, x_n] = P_k$$

□

• *Intuition*: First, notice that for polynomials q, f, $q\langle f \rangle \subset I \iff qf \in I$, which means

$$I : \langle f \rangle = \{q \in F[x_1, \cdots, x_n] \text{ s.t. } q\langle f \rangle \subset I\} = \{q \in F[x_1, \cdots, x_n] \text{ s.t. } qf \in I\}$$

which confirms the intuition that $I : \langle f \rangle$ is equivalent to dividing out f from I, in the sense that the polynomials left behind are the divisors of polynomials from I which are divisible by f.
The above result tells us that if we prime factor an ideal, the primes are precisely given by dividing the right polynomials out of I, which makes intuitive sense in accordance with the motivation of minimal decompositions being analogous to prime factorizations for integers, where primes are obviously given by dividing out the right divisors from the integer.

The above two theorems, on prime factors being ideal quotients and on ideals factoring into primes, actually hold for any field, not just over algebraically closed ones, but the proofs are out of scope.

7 Primary Decomposition of Ideals

The previous section gave results on prime decompositions of radical ideals, so it's natural to ask if similar results exist for general ideals. The intersection of prime ideals will always be radical ($f^m \in P \rightarrow$ one of $f, f^2, \cdots, f^{m-1} \in P$, which we can iteratively apply to conclude $f \in P$, for prime ideal P), so there's no use in trying to fully generalize the radical ideal decomposition theorems to arbitrary ideals. Nonetheless, we'll examine the structure of ideals with respect to such irreducible elements in detail in this section.
To study such arbitrary decompositions, we'll need a more subtle yet still powerful notion of irreducibility for ideals.

(Definition) Primary: *A polynomial ideal I is **primary** if $fg \in I$ implies either $f \in I$ or $g^m \in I$ for some power m.*

- Notice that the definition reduces to $fg \in I \rightarrow g \in \sqrt{I}$.

What we've done is simply relaxed the definition of a prime ideal slightly, to account for non-radical ideals, by, in a sense, building the notion of being radical into the definition. It follows that if I is primary, then $\sqrt{I}$ is prime, and furthermore is the smallest prime ideal containing I. This definition allows to make the aforementioned generalization of the radical ideal decomposition theorems from the last section.

(Theorem) Ideal decomposition: *Every polynomial ideal can be written as a finite intersection of primary ideals.*

- *Proof*: We'll first introduce the concept of an *irreducible* ideal with the definition that I is irreducible if $I = I_1 \cap I_2 \rightarrow I = I_1$ or $I = I_2$. Showing that every ideal is the intersection of finitely many irreducible ideals is a simple modification of the proof that varieties factor into irreducible varieties, using the ascending chain condition instead of the descending chain condition; following this, proving that irreducible ideals are primary proves the theorem.
To prove the first claim, assume that I is not irreducible (if it were, we could trivially factor it into irreducibles as $I = I$, proving the claim), so that $I = I_1 \cap I_2$ for $I \neq I_1, I_2$. In order for I to not factor into irreducible ideals, at least one of I_1, I_2, say I_1, mustn't itself factor into irreducible ideals (if both did, I would too), which means we can write $I_1 = I_3 \cap I_4$. We apply the same argument to conclude I_3 can't factor into irreducible ideals either, and so on, indefinitely. Since $I = I_1 \cap I_2 \rightarrow I \subset I_1$, it follows that

$$I \subset I_1 \subset I_3 \subset \cdots$$

which forms an ascending chain of ideals, which must stabilize at some I_N. Then I_N does factor into irreducible ideals, and hence so does every ideal in the chain prior, including I, proving the claim.
To prove that irreducible ideals correspond to primary ideals, suppose I is irreducible, with $fg \in I, f \notin I$, which reduces the proof to proving that $g^m \in I$ for some m. Consider the saturation $I : \langle g \rangle^\infty$, which we know is equal to $I : \langle g \rangle^N = I : \langle g^N \rangle$ for sufficiently large N. Now consider $(I + \langle g^N \rangle) \cap (I + \langle f \rangle)$, which clearly contains I. We can prove that the former contains I, and hence is equal to I, as follows. If h lies in this intersection, then we can write $h = a + bg^N = c + df$ for $a, b \in I$ and polynomials b, d. Then it follows that

$$hg = ag + bg^{N+1} = cg + dfg \in I \text{ since } c, fg \in I$$

$$\rightarrow bg^{N+1} \in I \text{ since } a \in I \rightarrow ag \in I$$

$$\rightarrow b \in I : \langle g \rangle^{N+1} = I : \langle g \rangle^N \rightarrow bg^N \in I \rightarrow a + bg^N = h \in I$$

This proves that $(I + \langle g^N \rangle) \cap (I + \langle f \rangle) = I$ and hence that $I = I + \langle g^N \rangle$ or $I = I + \langle f \rangle$ since I is irreducible. $f \notin I$ so the latter can't be the case; hence, $I = I + \langle g^N \rangle$, which means $g^N \in I$, proving the theorem if we let $m = n$. $\square$

As with varieties, we now define the notion of a minimal decomposition.

(Definition) Primary decomposition: *A **primary decomposition** of ideal I is an expression of I as the finite intersection of primary ideals*

$$I = \bigcap_i Q_i, Q_i \text{ primary}$$

*The decomposition is **minimal** if all the $\sqrt{Q_i}$ are distinct and*

$$\forall i : \bigcap_{j \neq i} Q_j \not\subset Q_i$$

- Notice that the minimality condition is stronger than the corresponding condition for radical ideals and primes.

It follows as a lemma that if I, J are primary ideals with $\sqrt{I} = \sqrt{J}$ then $I \cap J$ is primary as well. We'll use this lemma to prove the following main result of this section.

(Theorem) First Lasker-Noether theorem: *Every polynomial ideal has a minimal primary decomposition.*

- *Proof*: As we just saw, we're guaranteed a primary decomposition of any ideal I of $F[x_1, \cdots, x_n]$:

$$I = \bigcap_i Q_i, \text{ where } Q_i \text{ is primary}$$

The first condition for the decomposition to be minimal is for all the Q_i's to have distinct radicals. This is easy to iteratively enforce if we just apply the above lemma: if Q_j and Q_k have the same radical, replace them both with $Q_j \cap Q_k$, which is also primary by the lemma. Continuing in this manner, we may assume that all the Q_i's have distinct radicals. To enforce the second condition of minimality, suppose for some Q_k contains $\bigcap_{i \neq k} Q_i$. In this case we can simply remove Q_k from the intersection, since the intersection of a set with its superset leaves the set unchanged. Again, continuing in this manner, we can enforce the second minimality condition to obtain a minimal primary decomposition. □

Notice that the minimal primary decomposition, unlike with varieties and radical ideals, need not be unique. However, the second part of the Lasker-Noether theorem tells us that the radicals are in fact uniquely determined, provides an explicit description of them.

(Theorem) Second Lasker-Noether theorem: *Let I have minimal primary decomposition given by Q_i for $1 \leq i \leq r$, and let $P_i = \sqrt{Q_i}$. Then the P_i are precisely the proper prime ideals of the set*

$$\{\sqrt{I : \langle f \rangle}, f \in F[x_1, \cdots, x_n]\}$$

- *Proof*: TODO

8 Proof of the Closure Theorem

TODO

9 Conclusion - The Algebra-Geometry Dictionary

To conclude this chapter, let's take a step back and look at the full algebra-geometry dictionary we've constructed. We've shown that we can pass from the algebraic set of ideals of a polynomial ring to the geometric set of varieties in affine space, and back, by virtue of the maps given by $\mathbf{V}$ and $\mathbf{I}$.

We've seen that the latter mapping, $\mathbf{V}$, from ideals to varieties, is one-to-one, so that every ideal corresponds to a exactly one variety (put another way, every ideal of polynomials has exactly one common zero set). The other map, $\mathbf{I}$, from varieties to ideals, is not one-to-one (put another way, more than one ideal of polynomials might have the same zero set), exemplified by the empty variety, which maps to infinitely many ideals; however, the two mappings become bijective inverses if we restrict ourselves to the set of radical ideals. Moreover, we saw that Hilbert's Nullstellensatz tells us that when working over algebraically closed fields, which solves the problem of empty vareties, the only exceptions preventing the mappings from being full bijective inverses are the simple, direct examples of polynomial powers.

We defined algebraic operators on ideals (summation, product, and intersection), and drew parallels between them and the natural set theoretic operators on varieties. Specifically, we saw that ideal summation corresponds to the intersection of varieties: $\mathbf{V}(I+J) = \mathbf{V}(I) \cap \mathbf{V}(J)$. Furthermore, ideal products correspond to the union of varieties: $\mathbf{V}(IJ) = \mathbf{V}(I) \cup \mathbf{V}(J)$. The same applies to ideal intersection: $\mathbf{V}(I \cap J) = \mathbf{V}(I) \cup \mathbf{V}(J)$. Conversely, $\mathbf{I}(V) \cap \mathbf{I}(W) = \mathbf{I}(V \cup W)$. We saw that the radical of ideal summation corresponds to variety intersection: $\sqrt{\mathbf{I}(V) + \mathbf{I}(W)} = \mathbf{I}(V \cap W)$. Analogously, the radical of an ideal product corresponds to variety union: $\sqrt{\mathbf{I}(V)\mathbf{I}(W)} = \mathbf{I}(V \cup W)$.

We looked at the identities $\mathbf{V}(I) = \mathbf{V}(I+J) \cup \mathbf{V}(I : J)$ and $\overline{\mathbf{V}(I) - \mathbf{V}(J)} \subset \mathbf{V}(I : J)$, which relate ideal quotients to varieties, differences of varieties, and their Zariski closures, and extended these identities to saturations: $\mathbf{V}(I) = \mathbf{V}(I+J) \cup \mathbf{V}(I : J^\infty)$ and $\overline{\mathbf{V}(I) - \mathbf{V}(J)} \subset \mathbf{V}(I : J^\infty)$, where the second containment becomes equality if the underlying field is algebraically closed.

Finally, we extended the natural notion of irreducibility and prime factorization from number theory to both varieties and ideals, defining notions of irreducible varieties and prime ideals, and showing that varieties decompose into minimal irreducible decompositions (under union) while radical ideals decompose into minimal prime decompositions (under intersection). Moreover, we can relax the condition of ideals being radical by relaxing the definition of prime ideals to primary ideals, which have the notion of radicality "built in", allowing us to state that arbitrary ideals decompose into minimal primary decompositions. We defined notions of maximality for ideals, and saw that maximal ideals correspond bijectively to points in affine space.