

7 Decompositions

Copyright © 2023, Gregory G. Smith
Last updated: 5 March 2023

Methodological reductionism posits that the best scientific strategy is to reduce explanations to the smallest possible entities. A geometric incarnation of this idea involves decomposing affine subvarieties into a union of irreducible ones. Algebraically, this concept involves decomposing an ideal into an intersection of primary ideal (which are related to, but not quite the same as, powers of prime ideals).

7.0 The Closure Theorem

How do we finally prove the Closure Theorem 3.2.5? Equipped with the Nullstellensatz, we confirm our geometric interpretation for elimination ideals.

7.0.0 Lemma. *For any subset U in \mathbb{A}^n , the affine subvariety $V(I(U))$ is the smallest subvariety that contains U .*

Proof. Suppose that X is an affine subvariety in \mathbb{A}^n containing the subset U . Applying the inclusion-reversing operators, we see that $I(X) \subseteq I(U)$ and $V(I(U)) \subseteq V(I(X)) = X$. Thus, affine subvariety $V(I(U))$ is contained in every affine subvariety that contains U . \square

7.0.1 Theorem (Closure). *Let \mathbb{K} be an algebraically closed field and let I be an ideal in the ring $\mathbb{K}[x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m]$. For the projection $\pi_2: \mathbb{A}^{n+m} \rightarrow \mathbb{A}^m$ onto the last m components, the Zariski closure of the image $\pi_2(V(I))$ is $V(I \cap \mathbb{K}[y_1, y_2, \dots, y_m])$.*

Proof. Let $X := V(I)$ and set $J := I \cap \mathbb{K}[y_1, y_2, \dots, y_m]$. It is enough to prove that $V(J) = V(I(\pi_2(X)))$.

\supseteq : The definitions of X and J give the inclusion $\pi_2(X) \subseteq V(J)$. Since

Lemma 7.0.0 establishes that $V(I(\pi_2(X)))$ is the smallest variety containing the subset $\pi_2(X)$, it follows that $V(J) \supseteq V(I(\pi_2(X)))$.

\subseteq : Consider an element f in the ideal $I(\pi_2(X))$. Viewing f as a polynomial in the larger ring $\mathbb{K}[x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m]$, we have $f(a_1, a_2, \dots, a_{n+m}) = 0$ for any point $(a_1, a_2, \dots, a_{n+m})$ in X . Applying the Hilbert Nullstellensatz 6.0.2, there is a positive integer ℓ such that $f^\ell \in I$. Since the variables x_1, x_2, \dots, x_n do not appear in f , we see that $f^\ell \in J$. It follows that $f \in \sqrt{J}$ and $I(\pi_2(X)) \subseteq \sqrt{J}$. We see that $V(J) = V(\sqrt{J}) \subseteq V(I(\pi_2(X)))$. \square

We also encounter sets which are not affine subvarieties when taking the difference of two affine subvarieties.

7.0.2 Definition. For any ideals I and J in $S := \mathbb{K}[x_1, x_2, \dots, x_n]$, the *colon ideal* is the set $(I : J) := \{f \in S \mid fg \in I \text{ for all } g \in J\}$.

7.0.3 Example. We have $(\langle xz, yz \rangle : \langle z \rangle) = \langle x, y \rangle$. ◇

7.0.4 Proposition. For any ideals I and J in the ring S , the set $(I : J)$ is an ideal. Moreover, we have $I \subseteq (I : J)$.

Proof. For any two polynomials f_1 and f_2 in the set $(I : J)$, it follows that, for any polynomial g in the ideal J , we have $f_1 g \in I$ and $f_2 g \in I$. Suppose that h_1 and h_2 are ring elements in S . Since I is an ideal, we have $(h_1 f_1 + h_2 f_2) g = h_1 f_1 g + h_2 f_2 g \in I$ for any element g in the ideal J , which implies that $h_1 f_1 + h_2 f_2 \in (I : J)$. Thus, the set $I : J$ is an ideal in the ring S .

For any $f \in I$ and any $g \in S$, we have $fg \in I$ because I is an ideal. Hence, for any $f \in I$ and any $g \in J$, we have $fg \in I$, so $f \in (I : J)$. □

7.0.5 Lemma. For any affine subvarieties X and Y satisfying $X \subseteq Y$, we have $Y = X \cup \overline{Y \setminus X}$.

Proof. We prove containment in both directions.

\supseteq : Since $Y \setminus X \subseteq Y$ and Y is an affine subvariety, we have $\overline{Y \setminus X} \subseteq Y$.

As $X \subseteq Y$, we deduce that $Y \supseteq X \cup \overline{Y \setminus X}$.

\subseteq : As $X \subseteq Y$, we see that $Y = X \cup (Y \setminus X)$. Since $Y \setminus X \subseteq \overline{Y \setminus X}$, we have $Y \subseteq X \cup \overline{Y \setminus X}$. □

Adding to our dictionary, we have a geometric interpretation for colon ideals.

7.0.6 Theorem. For any ideals I and J in the ring $S := \mathbb{K}[x_1, x_2, \dots, x_n]$, we have $\overline{V(I) \setminus V(J)} \subseteq V(I : J)$. When the field \mathbb{K} is algebraically closed and $I = \sqrt{I}$, we also have $\overline{V(I) \setminus V(J)} = V(I : J)$.

Proof. It suffices to prove that $(I : J) \subseteq I(V(I) \setminus V(J))$. The membership $f \in (I : J)$ means that $fg \in I$ for any $g \in J$. For any point $a \in V(I) \setminus V(J)$, we see that $f(a)g(a) = 0$ for all $g \in J$. Since $a \notin V(J)$, there exists $g \in J$ such that $g(a) \neq 0$, so we deduce that $f(a) = 0$. Therefore, we have $f \in I(V(I) \setminus V(J))$ and $(I : J) \subseteq I(V(I) \setminus V(J))$.

Suppose that $a \in V(I : J)$. It follows that, for any $h \in S$ such that $hg \in I$ for all $g \in J$, we have $h(a) = 0$. Consider $h \in I(V(I) \setminus V(J))$. For any $g \in J$, the product hg vanishes on $V(I)$ because h vanishes on $V(I) \setminus V(J)$ and g vanishes on $V(J)$. By the Strong Nullstellensatz 6.0.5, we see that $hg \in \sqrt{I} = I$ for all $g \in J$. We deduce that $h(a) = 0$ and $a \in V(I(V(I) \setminus V(J)))$, which shows that $V(I : J) \subseteq V(I(V(I) \setminus V(J)))$. □

7.0.7 Lemma. *Let I and J be ideals in S . For the ideal $zI + (1 - z)J$ in the ring $S[z] = \mathbb{K}[z, x_1, x_2, \dots, x_n]$, we have $I \cap J = (zI + (1 - z)J) \cap S$.*

Proof. We prove containment in both directions.

- \subseteq : Consider $f \in I \cap J$. Since $f \in I$ and $f \in J$, we have $zf \in zI$ and $(1 - z)f \in (1 - z)J$, so $f = zf + (1 - z)f \in zI + (1 - z)J$. Since both I and J are ideals in the smaller ring S , it follows that $f \in (zI + (1 - z)J) \cap S$ and $I \cap J \subseteq (zI + (1 - z)J) \cap S$.
- \supseteq : Consider $f \in (zI + (1 - z)J) \cap S$. It follows that $f = g + h$ where $g \in zI$ and $h \in (1 - z)J$. Setting $z = 0$, we see that $f \in J$ and, setting $z = 1$, we see that $f \in I$. We conclude that $f \in I \cap J$ and $I \cap J \supseteq (zI + (1 - z)J) \cap S$. \square

This Lemma together with Elimination Theory yields an algorithm for computing the intersection of two ideals.

7.0.8 Proposition. *Let f be a polynomial in the ring $S := \mathbb{K}[x_1, x_2, \dots, x_n]$ and let I be an ideal in S . For any generators g_1, g_2, \dots, g_r of the ideal $I \cap \langle f \rangle$, the polynomials $g_1/f, g_2/f, \dots, g_r/f$ generate the ideal $(I : \langle f \rangle)$.*

Proof. We prove containment in both directions.

- \subseteq : For any polynomial p in the ideal $\langle f \rangle$, there is a polynomial q in S such that $p = qf$. For any polynomial h in the ideal $\langle g_1/f, g_2/f, \dots, g_r/f \rangle$ and any p in $\langle f \rangle$, it follows that

$$ph = qfh \in \langle g_1, g_2, \dots, g_r \rangle = I \cap \langle f \rangle \subseteq I,$$

so $h \in (I : \langle f \rangle)$.

- \supseteq : Suppose that $h \in (I : \langle f \rangle)$, which means that $hf \in I$. As $hf \in \langle f \rangle$, we have $hf \in I \cap \langle f \rangle$. Since $I \cap \langle f \rangle = \langle g_1, g_2, \dots, g_r \rangle$, there exists polynomials q_1, q_2, \dots, q_r in S such that $hf = \sum_{i=1}^r q_i g_i$. As $g_i \in \langle f \rangle$, each g_i/f is a polynomial in S and we conclude that $h = \sum_{i=1}^r q_i (g_i/f)$ whence $f \in \langle g_1/f, g_2/f, \dots, g_r/f \rangle$. \square

This leads to an algorithm for computing a Gröbner basis of a colon ideal. Given $I = \langle f_1, \dots, f_\ell \rangle$ and $J = \langle g_1, \dots, g_r \rangle$ to compute a Gröbner basis of $(I : J)$, we first compute a Gröbner basis of $\langle f_1, f_2, \dots, f_\ell \rangle \cap \langle g_i \rangle$. We can do this by finding a Gröbner basis of $\langle t f_1, \dots, t f_\ell, (1 - t)g_i \rangle$ with respect to an eliminate order for t . We divide each of these elements by g_i to get a basis for $(I : \langle g_i \rangle)$. Finally, we compute a basis for $(I : J)$ by applying an intersection algorithm $r - 1$ times, computing

$$\begin{aligned} (I : \langle g_1, g_2 \rangle) &= (I : \langle g_1 \rangle) \cap (I : \langle g_2 \rangle), \\ (I : \langle g_1, g_2, g_3 \rangle) &= (I : \langle g_1, g_2 \rangle) \cap (I : \langle g_3 \rangle), \\ &\vdots \end{aligned}$$

7.1 Decomposition of Varieties

How do we break an affine subvariety into irreducible pieces?

7.1.0 Lemma. *Every decreasing chain of affine subvarieties is eventually stationary. Equivalently, any nonempty set of affine subvarieties contains a minimal element (with respect to inclusion).*

Proof. The Hilbert Basis Theorem 2.0.0 demonstrates that every ascending chain of ideals in the ring $S := \mathbb{K}[x_1, x_2, \dots, x_n]$ is eventually stationary, so the dictionary between ideals and affine subvarieties yields the assertion. \square

7.1.1 Proposition. *Any nonempty affine subvariety X in \mathbb{A}^n is a finite union $X = X_1 \cup X_2 \cup \cdots \cup X_r$ of irreducible affine subvarieties. Requiring that $X_i \not\subseteq X_j$ for all $i \neq j$, the subvarieties X_i are uniquely determined. These subvarieties are called the irreducible components of X .*

Proof. We first show the existence of such a representation for X . Let \mathcal{S} be the set of nonempty closed subsets of \mathbb{A}^n which *cannot* be written as a finite union of irreducible closed subsets. Suppose that \mathcal{S} is nonempty. Hence, the set \mathcal{S} contains a minimal element Y . The definition of \mathcal{S} implies that Y is not irreducible. Hence, we can write $Y = Y' \cup Y''$ where Y' and Y'' are proper closed subsets of Y . By the minimality of Y , each of Y' and Y'' can be expressed as a finite union of closed irreducible subsets, whence Y also can which is a contradiction. We conclude that every closed set X can be written as a union $X = X_1 \cup X_2 \cup \cdots \cup X_r$ of irreducible subsets. By throwing away a few if necessary, we may assume $X_j \not\subseteq X_i$ for all $i \neq j$.

Suppose $X = X'_1 \cup X'_2 \cup \cdots \cup X'_\ell$ is another representation. Since $X'_1 \subseteq X$, we have $X'_1 = \bigcup_{i=1}^r (X'_1 \cap X_i)$. Because X'_1 is irreducible, there exists an index i such that $X'_1 \subseteq X_i$; say $i = 1$. By symmetry, we also have $X_1 \subseteq X'_j$ for some j . It follows that $X'_1 \subseteq X'_j$, so we deduce that $j = 1$ and $X_1 = X'_1$. Setting $Z := \overline{(X \setminus X_1)}$, we obtain then $Z = X_2 \cup X_3 \cup \cdots \cup X_r$ and $Z = X'_2 \cup X'_3 \cup \cdots \cup X'_\ell$. Proceeding by induction on r , we obtain uniqueness of the X_i . \square

7.1.2 Examples.

(i) $V(xy, xz) = V(x) \cup V(y, z)$.

(ii) $V(xz - y^2, x^3 - yz) = V(x, y) \cup V(xz - y^2, x^3 - yz, z^2 - x^2y)$ \diamond

7.1.3 Corollary. *Let \mathbb{K} be an algebraically closed field. Every radical ideal I in $S := \mathbb{K}[x_1, x_2, \dots, x_n]$ is uniquely expressed as a finite intersection of prime ideals; $I = P_1 \cap P_2 \cap \cdots \cap P_r$ where $P_i \not\subseteq P_j$ for all $i \neq j$.*

Proof. Follows immediately from the proposition and the dictionary between affine subvarieties in \mathbb{A}^n and ideals in S . \square

How do we extend this to all ideals?

7.1.4 Definition. An ideal I in S is *primary* if $I \neq \langle 1 \rangle$ and the relation $fg \in I$ implies that either $f \in I$ or $g^m \in I$ for some positive integer m . Equivalently, the ideal I is primary if and only if the quotient S/I is nonzero and every zerodivisor is nilpotent.

7.1.5 Lemma. *For any primary ideal I in S , its radical \sqrt{I} is prime and it is the smallest prime ideal containing I .*

Proof. As $I \subseteq \sqrt{I}$, it suffices to show \sqrt{I} is prime. Given $fg \in \sqrt{I}$, there exists a positive integer m such that $(fg)^m \in I$. Since I is primary, either $f^m \in I$ or $g^{m\ell} \in I$ for some positive integer ℓ , so we deduce that either $f \in \sqrt{I}$ or $g \in \sqrt{I}$. \square

For a prime ideal P and a primary ideal I satisfying $\sqrt{I} = P$, we say that the ideal I is *P-primary*.

7.1.6 Example. The primary ideals in the ring \mathbb{Z} are $\langle 0 \rangle$ and $\langle p^m \rangle$ where p is prime integer and m is a positive integer. \diamond

7.1.7 Example. Consider the ring $\mathbb{K}[x, y]$. For the monomial ideal $I := \langle x, y^2 \rangle$, the quotient is $S/I \cong \mathbb{K}[y]/\langle y^2 \rangle$. The zero divisors are all multiples of y which are nilpotent. Hence, the ideal I is primary and its radical is $P = \langle x, y \rangle$. We have $\langle x^2, xy, y^2 \rangle = P^2 \subset I \subset P$ so that this primary ideal is not a power of a prime ideal. \diamond

7.1.8 Definition. An ideal I in S is *irreducible* if the relation $I = I_1 \cap I_2$ implies that $I = I_1$ or $I = I_2$.

7.1.9 Lemma. Any ideal I in S is a finite intersection of irreducible ideals.

Proof. Suppose otherwise: the set of ideals in S that are not a finite intersection of irreducible ideals is not empty. Hence, this set has a maximal element I . Since I is reducible, we have $I = I_1 \cap I_2$ where $I \subset I_j$. Maximality implies that each I_j is a finite intersection of irreducible ideals. It follows that the same holds for I which is a contradiction. \square

7.1.10 Lemma. Every irreducible ideal I in S is primary.

Proof. Suppose that I is an irreducible ideal and $f, g \in I$ where $f \notin I$. Consider the chain of ideals $(I : \langle g \rangle) \subseteq (I : \langle g^2 \rangle) \subseteq \dots \subseteq (I : \langle g^j \rangle) \subseteq \dots$. Since S is noetherian, there exists a positive integer N such that $(I : \langle g^N \rangle) = (I : \langle g^{N+1} \rangle)$.

We claim that $(I + \langle g^N \rangle) \cap (I + \langle f \rangle) = I$. Every element in this intersection can be written as $p + a g^N = q + b f$ where $p, q \in I$ and $a, b \in S$. Multiplying by g implies that $p g + a g^{N+1} = q g + b g f$. It follows that $a \in (I : \langle g^{N+1} \rangle) = (I : \langle g^N \rangle)$ and $p + a g^N \in I$.

Since I is irreducible, we deduce that $I = I + \langle g^N \rangle$ or $I = I + \langle f \rangle$. The latter cannot occur because $f \notin I$, so $g^N \in I$. \square

7.1.11 Theorem. Every ideal I in the ring $S := \mathbb{K}[x_1, x_2, \dots, x_n]$ can be written as a finite intersection of primary ideals.

Proof. Combine the above lemmata. \square

7.2 Primary Decomposition

How do we “factor” an ideal in $S := \mathbb{K}[x_1, x_2, \dots, x_n]$?

7.2.0 Definition. A *primary decomposition* of an ideal I in the ring S expresses I as a finite intersection of primary ideals: $I = \bigcap_i Q_i$. It is *irredundant* if the prime ideals $\sqrt{Q_i}$ are all distinct and $\bigcap_{j \neq i} Q_j \not\subseteq Q_i$.

7.2.1 Lemma. Let P be a prime ideal in S . For any P -primary ideals Q_1, Q_2, \dots, Q_m , the intersection $Q = \bigcap_{i=1}^m Q_i$ is also P -primary.

A prime power P^n is not necessarily primary, although its radical is the prime ideal P . Consider the quotient $R = \mathbb{K}[x, y, z]/\langle xy - z^2 \rangle$. Let $\bar{x}, \bar{y}, \bar{z}$ denote the images of x, y and z in the ring R . The ideal $P = \langle \bar{x}, \bar{z} \rangle$ in R is prime because the quotient ring $R/P = \mathbb{K}[x, y, z]/\langle x, y, xy - z^2 \rangle \cong \mathbb{K}[y]$ is a domain. However, the relations $\bar{x}\bar{y} = \bar{z}^2 \in P$, $\bar{x} \notin P^2$, and $\bar{y} \notin \sqrt{P^2} = P$ show that P is not primary.

Proof. Corollary 6.2.8 shows that $\sqrt{Q} = \bigcap_{i=1}^m \sqrt{Q_i} = \bigcap_{i=1}^m P = P$. Given $f g \in Q$ where $g \notin Q$, there exists an index j such that $f g \in Q_j$ and $g \notin Q_j$. It follows that $f \in P$ because Q_j is a P -primary ideal. \square

7.2.2 Corollary. *Every ideal I in the ring S has an irredundant primary decomposition.*

Proof. Theorem 7.1.11 demonstrates that the ideal I has a primary decomposition: $I = \bigcap_{i=1}^m Q_i$. If there are two the primary ideals Q_i and Q_j having the same radical, then Lemma 7.2.1 shows that we may replace them with their intersection $Q_i \cap Q_j$. Iterating this process, we obtain a decomposition with distinct radicals. If we have $\bigcap_{j \neq i} Q_j \subseteq Q_i$ for some i , then we may omit Q_i . \square

7.2.3 Lemma. *Let P be a prime ideal and let Q be a P -primary ideal.*

- (i) *For any $f \in Q$, we have $(Q : \langle f \rangle) = \langle 1 \rangle$.*
- (ii) *For any $f \notin Q$, the ideal $(Q : \langle f \rangle)$ is P -primary, so $(\sqrt{Q} : \langle f \rangle) = P$.*
- (iii) *For any $f \notin P$, we have $(Q : \langle f \rangle) = Q$.*

Proof. Parts (i) and (iii) follow directly from the definitions of a colon ideal and primary ideal. For part (ii), consider $g \in (Q : \langle f \rangle)$, so $f g \in Q$. As $f \notin Q$ and Q is a primary ideal, there exists a positive integer m such that $g^m \in Q$. We see that $Q^m \subseteq (Q : \langle f \rangle) \subseteq P$. Taking radicals, we obtain $\sqrt{Q} : \langle f \rangle = P$. For primarity, suppose that $g h \in (Q : \langle f \rangle)$ where $g \notin P$. It follows that $f g h \in Q$, so we have $f h \in Q$ and $h \in (Q : \langle f \rangle)$. \square

7.2.4 Lemma. *Let I_1, I_2, \dots, I_m be ideals in S and let P be a prime ideal in S . When P contains the intersection $\bigcap_{i=1}^m I_i$, there exists an index j such that $P \supseteq I_j$. When $P = \bigcap_{i=1}^m I_i$, there exists an index j such that $P = I_j$.*

Proof. Suppose that $P \not\supseteq I_i$ for all $1 \leq i \leq m$. For each $1 \leq i \leq m$, there exists $f_i \in I_i$ such that $f_i \notin P$. It follows that the product $f_1 f_2 \cdots f_m$ is contained in $\prod_{i=1}^m I_i \subseteq \bigcap_{i=1}^m I_i$ but is not contained in P . Thus, we deduce that $P \not\supseteq \bigcap_{i=1}^m I_i$. Assuming that $P = \bigcap_{i=1}^m I_i$, there exists an index j such that $P \supseteq I_j \supseteq P$, whence $P = I_j$. \square

7.2.5 Theorem (Lasker–Noether). *Let $I = \bigcap_{i=1}^m Q_i$ be an irredundant primary decomposition. The ideals $P_i := \sqrt{Q_i}$, for all $1 \leq i \leq m$, are precisely the prime ideals appearing in the set $\{\sqrt{I : \langle f \rangle} \mid f \in S\}$.*

Sketch of Proof. For all $f \in S$, we have

$$(I : \langle f \rangle) = (\bigcap_{i=1}^m Q_i) : \langle f \rangle = \bigcap_{i=1}^m (Q_i : \langle f \rangle).$$

which gives $\sqrt{I : \langle f \rangle} = \bigcap_{i=1}^m \sqrt{Q_i : \langle f \rangle} = \bigcap_{f \notin Q_i} P_i$. Suppose that $\sqrt{I : \langle f \rangle}$ is a prime ideal. Hence, there exists an index j such that $\sqrt{I : \langle f \rangle} = P_j$ and every prime ideal of the form $\sqrt{I : \langle f \rangle}$ is one of

the P_j . Conversely, for each index i , there exists $f_i \notin Q_i$ such that $f_i \in \bigcap_{i \neq j} Q_j$ because the decomposition is irredundant. It follows that $\sqrt{I : \langle f_i \rangle} = P_i$. \square

7.2.6 Remark. The prime ideals in this theorem are the *associated* primes of I . An ideal I is primary if and only if it has a unique associated prime ideal. The minimal elements of the set $\{P_1, P_2, \dots, P_m\}$ are called *minimal* associated primes. The others are called *embedded* primes. The minimal primes correspond to the irreducible components of $V(I)$. The embedded primes correspond to subvarieties of the irreducible components. The minimal primes are uniquely determined by the ideal, but the embedded primes are not.

Algebra-Geometric Dictionary

Assume that the coefficient field \mathbb{K} is algebraically closed.

Algebra	Geometry
radical ideals	affine subvarieties
I	$V(I)$
$I(X)$	X
prime ideals	irreducible subvarieties
maximal ideals	points
ascending chain condition	descending chain condition
$I + J$	$V(I) \cap V(J)$
$\sqrt{I(X) + I(Y)}$	$X \cap Y$
IJ	$V(I) \cup V(J)$
$\sqrt{I(X) I(Y)}$	$X \cup Y$
$I \cap J$	$V(I) \cup V(J)$
$I(X) \cap I(Y)$	$X \cup Y$
$I : J$	$\overline{V(I) \setminus V(J)}$
$I(X) : I(Y)$	$\overline{X \setminus Y}$
$\sqrt{I \cap \mathbb{K}[y_1, y_2, \dots, y_m]}$	$\pi_2(\overline{V(I)})$