4

The Algebra–Geometry Dictionary

In this chapter, we will explore the correspondence between ideals and varieties. In §§1 and 2, we will prove the Nullstellensatz, a celebrated theorem which identifies exactly which ideals correspond to varieties. This will allow us to construct a "dictionary" between geometry and algebra, whereby any statement about varieties can be translated into a statement about ideals (and conversely). We will pursue this theme in §§3 and 4, where we will define a number of natural algebraic operations on ideals and study their geometric analogues. In keeping with the computational emphasis of this course, we will develop algorithms to carry out the algebraic operations. In §§5 and 6, we will study the more important algebraic and geometric concepts arising out of the Hilbert Basis Theorem: notably the possibility of decomposing a variety into a union of simpler varieties and the corresponding algebraic notion of writing an ideal as an intersection of simpler ideals.

§1 Hilbert's Nullstellensatz

In Chapter 1, we saw that a variety $V \subset k^n$ can be studied by passing to the ideal

$$\mathbf{I}(V) = \{f \in k[x_1, \ldots, x_n] : f(x) = 0 \text{ for all } x \in V\}$$

of all polynomials vanishing on V. That is, we have a map

$$\begin{array}{ccc} \text{affine varieties} & & \text{ideals} \\ V & \longrightarrow & \mathbf{I}(V). \end{array}$$

Conversely, given an ideal $I \subset k[x_1, \ldots, x_n]$, we can define the set

$$\mathbf{V}(I) = \{x \in k^n : f(x) = 0 \text{ for all } f \in I\}.$$

The Hilbert Basis Theorem assures us that $\mathbf{V}(I)$ is actually an affine variety, for it tells us that there exists a finite set of polynomials $f_1, \ldots, f_s \in I$ such that $I = \langle f_1, \ldots, f_s \rangle$, and we proved in Proposition 9 of Chapter 2, §5 that $\mathbf{V}(I)$ is the set of common roots of these polynomials. Thus, we have a map

$$\begin{array}{ccc} \text{ideals} & & \text{affine varieties} \\ I & \longrightarrow & \mathbf{V}(I). \end{array}$$

These two maps give us a correspondence between ideals and varieties. In this chapter, we will explore the nature of this correspondence.

The first thing to note is that this correspondence (more precisely, the map $\mathbf{V}$) is not one-to-one: different ideals can give the same variety. For example, $\langle x\rangle$ and $\langle x^2\rangle$ are different ideals in $k[x]$ which have the same variety $\mathbf{V}(x) = \mathbf{V}(x^2) = \{0\}$. More serious problems can arise if the field k is not algebraically closed. For example, consider the three polynomials 1, $1 + x^2$, and $1 + x^2 + x^4$ in $\mathbb{R}[x]$. These generate different ideals

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

but each polynomial has no real roots, so that the corresponding varieties are all empty:

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

Examples of polynomials in two variables without real roots include $1 + x^2 + y^2$ and $1 + x^2 + y^4$. These give different ideals in $\mathbb{R}[x, y]$ which correspond to the empty variety.

Does this problem of having different ideals represent the empty variety go away if the field k is algebraically closed? It does in the one-variable case when the ring is $k[x]$. To see this, recall from §5 of Chapter 1 that any ideal I in $k[x]$ can be generated by a single polynomial because $k[x]$ is a principal ideal domain. So we can write $I = \langle f\rangle$ for some polynomial $f \in k[x]$. Then $\mathbf{V}(I)$ is the set of roots of f; that is, the set of $a \in k$ such that $f(a) = 0$. But since k is algebraically closed, every nonconstant polynomial in $k[x]$ has a root. Hence, the only way that we could have $\mathbf{V}(I) = \emptyset$ would be to have f be a nonzero constant. In this case, $1/f \in k$. Thus, $1 = (1/f)\cdot f \in I$, which means that $g = g \cdot 1 \in I$ for all $g \in k[x]$. This shows that $I = k[x]$ is the only ideal of $k[x]$ that represents the empty variety when k is algebraically closed.

A wonderful thing now happens: the same property holds when there is more than one variable. In any polynomial ring, algebraic closure is enough to guarantee that the only ideal which represents the empty variety is the entire polynomial ring itself. This is the *Weak Nullstellensatz*, which is the basis of (and is equivalent to) one of the most celebrated mathematical results of the late nineteenth century, Hilbert's Nullstellensatz. Such is its impact that, even today, one customarily uses the original German name *Nullstellensatz*: a word formed, in typical German fashion, from three simpler words: Null (=Zero), Stellen (=Places), Satz (=Theorem).

Theorem 1 (The Weak Nullstellensatz). *Let k be an algebraically closed field and let $I \subset k[x_1, \ldots, x_n]$ be an ideal satisfying $\mathbf{V}(I) = \emptyset$. Then $I = k[x_1, \ldots, x_n]$.*

Proof. To prove that an ideal I equals $k[x_1, \ldots, x_n]$, the standard strategy is to show that the constant polynomial 1 is in I. This is because if $1 \in I$, then by the definition of an ideal, we have $f = f \cdot 1 \in I$ for every $f \in k[x_1, \ldots, x_n]$. Thus, knowing that $1 \in I$ is enough to show that I is the whole polynomial ring.

Our proof is by induction on n, the number of variables. If $n = 1$ and $I \subset k[x]$ satisfies $\mathbf{V}(I) = \emptyset$, then we already showed that $I = k[x]$ in the discussion preceding the statement of the theorem.

Now assume the result has been proved for the polynomial ring in $n - 1$ variables, which we write as $k[x_2, \ldots, x_n]$. Consider any ideal $I = \langle f_1, \ldots, f_s \rangle \subset k[x_1, \ldots, x_n]$ for which $\mathbf{V}(I) = \emptyset$. We may assume that f_1 is not a constant since, otherwise, there is nothing to prove. So, suppose f_1 has total degree $N \geq 1$. We will next change coordinates so that f_1 has an especially nice form. Namely, consider the linear change of coordinates

$$
\begin{aligned}
x_1 &= \tilde{x}_1, \\
x_2 &= \tilde{x}_2 + a_2\tilde{x}_1, \\
&\;\;\vdots \\
x_n &= \tilde{x}_n + a_n\tilde{x}_1.
\end{aligned}
\tag{1}
$$

where the a_i are as-yet-to-be-determined constants in k. Substitute for $x_1, \ldots, x_n$ so that f_1 has the form

$$
\begin{aligned}
f_1(x_1, \ldots, x_n) &= f_1(\tilde{x}_1, \tilde{x}_2 + a_2\tilde{x}_1, \ldots, \tilde{x}_n + a_n\tilde{x}_1) \\
&= c(a_2, \ldots, a_n)\tilde{x}_1^N + \text{ terms in which } \tilde{x}_1 \text{ has degree} < N.
\end{aligned}
$$

We will leave it as an exercise for the reader to show that $c(a_2, \ldots, a_n)$ is a nonzero polynomial expression in $a_2, \ldots, a_n$. In the exercises, you will also show that an algebraically closed field is infinite. Thus we can choose $a_2, \ldots, a_n$ so that $c(a_2, \ldots, a_n) \neq 0$ by Proposition 5 of Chapter 1, §1.

With this choice of $a_2, \ldots, a_n$, under the coordinate change (1) every polynomial $f \in k[x_1, \ldots, x_n]$ goes over to a polynomial $\tilde{f} \in k[\tilde{x}_1, \ldots, \tilde{x}_n]$. In the exercises, we will ask you to check that the set $\tilde{I} = \{\tilde{f} : f \in I\}$ is an ideal in $k[\tilde{x}_1, \ldots, \tilde{x}_n]$. Note that we still have $\mathbf{V}(\tilde{I}) = \emptyset$ since if the transformed equations had solutions, so would the original ones. Furthermore, if we can show that $1 \in \tilde{I}$, then $1 \in I$ will follow since constants are unaffected by the $\tilde{}$ operation.

Hence, it suffices to prove that $1 \in \tilde{I}$. By the previous paragraph, $f_1 \in I$ transforms to $\tilde{f}_1 \in \tilde{I}$ with the property that

$$
\tilde{f}_1(\tilde{x}_1, \ldots, \tilde{x}_n) = c(a_2, \ldots, a_n)\tilde{x}_1^N + \text{ terms in which } \tilde{x}_1 \text{ has degree} < N,
$$

where $c(a_2, \ldots, a_n) \neq 0$. This allows us to use a corollary of the Geometric Extension Theorem (see Corollary 4 of Chapter 3, §2), to relate $\mathbf{V}(\tilde{I})$ with its projection into the subspace of k^n with coordinates $\tilde{x}_2, \ldots, \tilde{x}_n$. As we noted in Chapter 3, the Extension Theorem and its corollaries hold over any algebraically closed field. Let

$$
\pi_1 : k^n \to k^{n-1}
$$

be the projection mapping onto the last $n - 1$ components. If we set $\tilde{I}_1 = \tilde{I} \cap k[\tilde{x}_2, \ldots, \tilde{x}_n]$ as usual, then the corollary states that partial solutions in k^{n-1} always extend, i.e., $\mathbf{V}(\tilde{I}_1) = \pi_1(\mathbf{V}(\tilde{I}))$. This implies that $\mathbf{V}(\tilde{I}_1) = \pi_1(\mathbf{V}(\tilde{I})) = \pi_1(\emptyset) = \emptyset$.

By the induction hypothesis, it follows that $\tilde{I}_1 = k[\tilde{x}_2, \ldots, \tilde{x}_n]$. But this implies that $1 \in \tilde{I}_1 \subset \tilde{I}$, and the proof is complete. $\square$

In the special case when $k = \mathbb{C}$, the Weak Nullstellensatz may be thought of as the "Fundamental Theorem of Algebra for multivariable polynomials"—every system of polynomials that generates an ideal strictly smaller than $\mathbb{C}[x_1, \ldots, x_n]$ has a common zero in $\mathbb{C}^n$.

The Weak Nullstellensatz also allows us to solve the *consistency problem* from §2 of Chapter 1. Recall that this problem asks whether a system

$$\begin{aligned} f_1 &= 0, \\ f_2 &= 0, \\ &\vdots \\ f_s &= 0 \end{aligned}$$

of polynomial equations has a common solution in $\mathbb{C}^n$. The polynomials fail to have a common solution if and only if $\mathbf{V}(f_1, \ldots, f_s) = \emptyset$. By the Weak Nullstellensatz, the latter holds if and only if $1 \in \langle f_1, \ldots, f_s \rangle$. Thus, to solve the consistency problem, we need to be able to determine whether 1 belongs to an ideal. This is made easy by the observation that for any monomial ordering, $\{1\}$ *is the only reduced Groebner basis for the ideal* $\langle 1 \rangle$.

To see this, let $\{g_1, \ldots, g_t\}$ be a Groebner basis of $I = \langle 1 \rangle$. Thus, $1 \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$, and then Lemma 2 of Chapter 2, §4 implies that 1 is divisible by some $\mathrm{LT}(g_i)$, say $\mathrm{LT}(g_1)$. This forces $\mathrm{LT}(g_1)$ to be constant. Then every other $\mathrm{LT}(g_i)$ is a multiple of that constant, so that $g_2, \ldots, g_t$ can be removed from the Groebner basis by Lemma 3 of Chapter 2, §7. Finally, since $\mathrm{LT}(g_1)$ is constant, g_1 itself is constant since every nonconstant monomial is >1 (see Corollary 6 of Chapter 2, §4). We can multiply by an appropriate constant to make $g_1 = 1$. Our reduced Groebner basis is thus $\{1\}$.

To summarize, we have the following **consistency algorithm**: if we have polynomials $f_1, \ldots, f_s \in \mathbb{C}[x_1, \ldots, x_n]$, we compute a reduced Groebner basis of the ideal they generate with respect to any ordering. If this basis is $\{1\}$, the polynomials have no common zero in $\mathbb{C}^n$; if the basis is not $\{1\}$, they must have a common zero. Note that the algorithm works over any algebraically closed field.

If we are working over a field k which is not algebraically closed, then the consistency algorithm still works in one direction: if $\{1\}$ is a reduced Groebner basis of $\langle f_1, \ldots, f_s \rangle$, then the equations $f_1 = \cdots = f_s = 0$ have no common solution. The converse is not true, as shown by the examples preceding the statement of the Weak Nullstellensatz.

Inspired by the Weak Nullstellensatz, one might hope that the correspondence between ideals and varieties is one-to-one provided only that one restricts to algebraically closed fields. Unfortunately, our earlier example $\mathbf{V}(x) = \mathbf{V}(x^2) = \{0\}$ works over *any* field. Similarly, the ideals $\langle x^2, y \rangle$ and $\langle x, y \rangle$ (and, for that matter, (x^n, y^m) where n and m are integers greater than one) are different but define the same variety: namely, the single point $\{(0, 0)\} \subset k^2$. These examples illustrate a basic reason why different ideals can define the same variety (equivalently, that the map $\mathbf{V}$ can fail to be one-to-one): namely, a power of a polynomial vanishes on the same set as the original polynomial. The Hilbert Nullstellensatz states that over an algebraically closed field, this is the *only* reason that different ideals can give the same variety: if a polynomial f vanishes at all points of some variety $\mathbf{V}(I)$, then some power of f must belong to I.

Theorem 2 (Hilbert's Nullstellensatz). *Let k be an algebraically closed field. If $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ are such that $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$, then there exists an integer $m \geq 1$ such that*

$$f^m \in \langle f_1, \ldots, f_s \rangle$$

(and conversely).

Proof. Given a nonzero polynomial f which vanishes at every common zero of the polynomials $f_1, \ldots, f_s$, we must show that there exists an integer $m \geq 1$ and polynomials $A_1, \ldots, A_s$ such that

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

The most direct proof is based on an ingenious trick. Consider the ideal

$$\tilde{I} = \langle f_1, \ldots, f_s, 1 - yf \rangle \subset k[x_1, \ldots, x_n, y],$$

where $f, f_1, \ldots, f_s$ are as above. We claim that

$$\mathbf{V}(\tilde{I}) = \emptyset.$$

To see this, let $(a_1, \ldots, a_n, a_{n+1}) \in k^{n+1}$. Either

- $(a_1, \ldots, a_n)$ is a common zero of $f_1, \ldots, f_s$, or
- $(a_1, \ldots, a_n)$ is not a common zero of $f_1, \ldots, f_s$.

In the first case $f(a_1, \ldots, a_n) = 0$ since f vanishes at any common zero of $f_1, \ldots, f_s$. Thus, the polynomial $1 - yf$ takes the value $1 - a_{n+1} f(a_1, \ldots, a_n) = 1 \neq 0$ at the point $(a_1, \ldots, a_n, a_{n+1})$. In particular, $(a_1, \ldots, a_n, a_{n+1}) \notin \mathbf{V}(\tilde{I})$. In the second case, for some i, $1 \leq i \leq s$, we must have $f_i(a_1, \ldots, a_n) \neq 0$. Thinking of f_i as a function of $n + 1$ variables which does not depend on the last variable, we have $f_i(a_1, \ldots, a_n, a_{n+1}) \neq 0$. In particular, we again conclude that $(a_1, \ldots, a_n, a_{n+1}) \notin \mathbf{V}(\tilde{I})$. Since $(a_1, \ldots, a_n, a_{n+1}) \in k^{n+1}$ was arbitrary, we conclude that $\mathbf{V}(\tilde{I}) = \emptyset$ as claimed.

Now apply the Weak Nullstellensatz to conclude that $1 \in \tilde{I}$. That is,

$$(2) \qquad 1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, y) f_i + q(x_1, \ldots, x_n, y)(1 - yf)$$

for some polynomials $p_i, q \in k[x_1, \ldots, x_n, y]$. Now set $y = 1/f(x_1, \ldots, x_n)$. Then relation (2) above implies that

$$(3) \qquad 1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, 1/f) f_i.$$

Multiply both sides of this equation by a power f^m, where m is chosen sufficiently large to clear all the denominators. This yields

$$f^m = \sum_{i=1}^{s} A_i f_i, \tag{4}$$

for some polynomials $A_i \in k[x_1, \ldots, x_n]$, which is what we had to show. □

EXERCISES FOR §1

1. Recall that $\mathbf{V}(y - x^2, z - x^3)$ is the twisted cubic in $\mathbb{R}^3$.
   a. Show that $\mathbf{V}((y - x^2)^2 + (z - x^3)^2)$ is also the twisted cubic.
   b. Show that any variety $\mathbf{V}(I) \subset \mathbb{R}^n$, $I \subset \mathbb{R}[x_1, \ldots, x_n]$, can be defined by a single equation (and hence by a principal ideal).
2. Let $J = \langle x^2 + y^2 - 1, y - 1\rangle$. Find $f \in \mathbf{I}(\mathbf{V}(J))$ such that $f \notin J$.
3. Under the change of coordinates (1), a polynomial $f(x_1, \ldots, x_n)$ of total degree N goes over into a polynomial of the form
   $$\tilde{f} = c(a_2, \ldots, a_n)\tilde{x}_1^N + \text{terms in which } \tilde{x}_1 \text{ has degree } < N.$$
   We want to show that $c(a_2, \ldots, a_n)$ is a nonzero polynomial in $a_2, \ldots, a_n$.
   a. Write $f = h_N + h_{N-1} + \cdots + h_0$ where each h_i, $0 \le i \le N$, is homogeneous of degree i (that is, where each monomial in h_i has total degree i). Show that after the coordinate change (1), the coefficient $c(a_2, \ldots, a_n)$ of $\tilde{x}_1^N$ in $\tilde{f}$ is $h_N(1, a_2, \ldots, a_n)$.
   b. Let $h(x_1, \ldots, x_n)$ be a homogeneous polynomial. Show that h is the zero polynomial in $k[x_1, \ldots, x_n]$ if and only if $h(1, x_2, \ldots, x_n)$ is the zero polynomial in $k[x_2, \ldots, x_n]$.
   c. Conclude that $c(a_2, \ldots, a_n)$ is not the zero polynomial in $a_2, \ldots, a_n$.
4. Prove that an algebraically closed field k must be infinite. Hint: Given n elements $a_1, \ldots, a_n$ of a field k, can you write down a nonconstant polynomial $f \in k[x]$ with the property that $f(a_i) = 1$ for all i?
5. Establish that $\tilde{I}$ as defined in the proof of the Weak Nullstellensatz is an ideal of $k[\tilde{x}_1, \ldots, \tilde{x}_n]$.
6. In deducing Hilbert's Nullstellensatz from the Weak Nullstellensatz, we made the substitution $y = 1/f(x_1, \ldots, x_n)$ to deduce relations (3) and (4) from (2). Justify this rigorously. Hint: In what set is $1/f$ contained?
7. The purpose of this exercise is to show that if k is any field which is not algebraically closed, then any variety $V \subset k^n$ can be defined by a single equation.
   a. If $f = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ is a polynomial of degree n in x, define the *homogenization* f^h of f with respect to some variable y to be the homogeneous polynomial $f^h = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}xy^{n-1} + a_ny^n$. Show that f has a root in k if and only if there is $(a, b) \in k^2$ such that $(a, b) \neq (0, 0)$ and $f^h(a, b) = 0$. Hint: Show that $f^h(a, b) = b^n f^h(a/b, 1)$ when $b \neq 0$.
   b. If k is not algebraically closed, show that there exists $f \in k[x, y]$ such that the variety defined by $f = 0$ consists of just the origin $(0, 0) \in k^2$. Hint: Choose a polynomial in $k[x]$ with no root in k and consider its homogenization.
   c. If k is not algebraically closed, show that for each integer $s > 0$ there exists $f \in k[x_1, \ldots, x_s]$ such that the only solution of $f = 0$ is the origin $(0, \ldots, 0) \in k^s$. Hint: Use induction and part (b) above. See also Exercise 1.
   d. If $W = \mathbf{V}(g_1, \ldots, g_s)$ is any variety in k^n, where k is not algebraically closed, then show that W can be defined by a single equation. Hint: Consider the polynomial $f(g_1, \ldots, g_s)$ where f is as above.

8. Let k be an arbitrary field and let S be the subset of all polynomials in $k[x_1, \ldots, x_n]$ that have no zeros in k^n. If I is any ideal in $k[x_1, \ldots, x_n]$ such that $I \cap S = \emptyset$, show that $\mathbf{V}(I) \neq \emptyset$. Hint: When k is not algebraically closed, use the previous exercise.
9. (A generalization of Exercise 5.) Let A be an $n \times n$ matrix with entries in k. Suppose that $x = A\tilde{x}$ where we are thinking of x and $\tilde{x}$ as column vectors. Define a map

$$\alpha_A : k[x_1, \ldots, x_n] \longrightarrow k[\tilde{x}_1, \ldots, \tilde{x}_n]$$

by sending $f \in k[x_1, \ldots, x_n]$ to $\tilde{f} \in k[\tilde{x}_1, \ldots, \tilde{x}_n]$, where $\tilde{f}$ is the polynomial defined by $\tilde{f}(\tilde{x}) = f(A\tilde{x})$.
   a. Show that α_A is k-linear, i.e., show that $\alpha_A(rf+sg) = r\alpha_A(f)+s\alpha_A(g)$ for all $r, s \in k$ and all $f, g \in k[x_1, \ldots, x_n]$.
   b. Show that $\alpha_A(f \cdot g) = \alpha_A(f) \cdot \alpha_A(g)$ for all $f, g \in k[x_1, \ldots, x_n]$. [As we will see in Definition 8 of Chapter 5, §2, a map between rings which preserves addition and multiplication and also preserves the multiplicative identity is called a *ring homomorphism*. Since it is clear that $\alpha_A(1) = 1$, this shows that α_A is a ring homomorphism.]
   c. Find conditions on the matrix A which guarantee that α_A is one-to-one and onto.
   d. Is the image $\{\alpha_A(f) : f \in I\}$ of an ideal $I \subset k[x_1, \ldots, x_n]$ necessarily an ideal in $k[\tilde{x}_1, \ldots, \tilde{x}_n]$? Give a proof or a counterexample.
   e. Is the inverse image $\{f \in k[x_1, \ldots, x_n] : \alpha_A(f) \in \tilde{I}\}$ of an ideal $\tilde{I}$ in $k[\tilde{x}_1, \ldots, \tilde{x}_n]$ an ideal in $k[x_1, \ldots, x_n]$? Give a proof or a counterexample.
   f. Do the conclusions of parts a-e change if we allow the entries in the $n \times n$ matrix A to be elements of $k[\tilde{x}_1, \ldots, \tilde{x}_n]$?
10. In Exercise 1, we encountered two ideals in $\mathbb{R}[x, y]$ which give the same nonempty variety. Show that one of these ideals is contained in the other. Can you find two ideals in $\mathbb{R}[x, y]$, neither contained in the other, which give the same nonempty variety? Can you do the same for $\mathbb{R}[x]$?

§2 Radical Ideals and the Ideal–Variety Correspondence

To further explore the relation between ideals and varieties, it is natural to recast Hilbert's Nullstellensatz in terms of ideals. Can we characterize the kinds of ideals that appear as the ideal of a variety? That is, can we identify those ideals that consist of *all* polynomials which vanish on some variety V? The key observation is contained in the following simple lemma.

Lemma 1. *Let V be a variety. If $f^m \in \mathbf{I}(V)$, then $f \in \mathbf{I}(V)$.*

Proof. Let $x \in V$. If $f^m \in \mathbf{I}(V)$, then $(f(x))^m = 0$. But this can happen only if $f(x) = 0$. Since $x \in V$ was arbitrary, we must have $f \in \mathbf{I}(V)$. □

Thus, an ideal consisting of *all* polynomials which vanish on a variety V has the property that if some power of a polynomial belongs to the ideal, then the polynomial itself must belong to the ideal. This leads to the following definition.

Definition 2. *An ideal I is* **radical** *if $f^m \in I$ for some integer $m \geq 1$ implies that $f \in I$.*

Rephrasing Lemma 1 in terms of radical ideals gives the following statement.

Corollary 3. $\mathbf{I}(V)$ *is a radical ideal.*

On the other hand, Hilbert's Nullstellensatz tells us that the only way that an arbitrary ideal I can fail to be the ideal of all polynomials vanishing on $\mathbf{V}(I)$ is for I to contain powers f^m of polynomials f which are not in I—in other words, for I to fail to be a radical ideal. This suggests that there is a one-to-one correspondence between affine varieties and radical ideals. To clarify this and get a sharp statement, it is useful to introduce the operation of taking the radical of an ideal.

Definition 4. *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. The* **radical** *of I, denoted $\sqrt{I}$, is the set*

$$\{f : f^m \in I \text{ for some integer } m \geq 1\}.$$

Note that we always have $I \subset \sqrt{I}$ since $f \in I$ implies $f^1 \in I$ and, hence, $f \in \sqrt{I}$ by definition. It is an easy exercise to show that an ideal I is radical if and only if $I = \sqrt{I}$. A somewhat more surprising fact is that the radical of an ideal is always an ideal. To see what is at stake here, consider, for example, the ideal $J = \langle x^2, y^3 \rangle \subset k[x, y]$. Although neither x nor y belongs to J, it is clear that $x \in \sqrt{J}$ and $y \in \sqrt{J}$. Note that $(x \cdot y)^2 = x^2 y^2 \in J$ since $x^2 \in J$; thus, $x \cdot y \in \sqrt{J}$. It is less obvious that $x + y \in \sqrt{J}$. To see this, observe that

$$(x + y)^4 = x^4 + 4x^3 y + 6x^2 y^2 + 4xy^3 + y^4 \in J$$

because $x^4, 4x^3 y, 6x^2 y^2 \in J$ (they are all multiples of x^2) and $4xy^3, y^4 \in J$ (because they are multiples of y^3). Thus, $x + y \in \sqrt{J}$. By way of contrast, neither xy nor $x + y$ belong to J.

Lemma 5. *If I is an ideal in $k[x_1, \ldots, x_n]$, then $\sqrt{I}$ is an ideal in $k[x_1, \ldots, x_n]$ containing I. Furthermore, $\sqrt{I}$ is a radical ideal.*

Proof. We have already shown that $I \subset \sqrt{I}$. To show $\sqrt{I}$ is an ideal, suppose $f, g \in \sqrt{I}$. Then there are positive integers m and l such that $f^m, g^l \in I$. In the binomial expansion of $(f + g)^{m+l-1}$ every term has a factor $f^i g^j$ with $i + j = m + l - 1$. Since either $i \geq m$ or $j \geq l$, either f^i or g^j is in I, whence $f^i g^j \in I$ and every term in the binomial expansion is in I. Hence, $(f + g)^{m+l-1} \in I$ and, therefore, $f + g \in \sqrt{I}$. Finally, suppose $f \in \sqrt{I}$ and $h \in k[x_1, \ldots, x_n]$. Then $f^m \in I$ for some integer $m \geq 1$. Since I is an ideal, we have $(h \cdot f)^m = h^m f^m \in I$. Hence, $hf \in \sqrt{I}$. This shows that $\sqrt{I}$ is an ideal. In Exercise 4, you will show that $\sqrt{I}$ is a radical ideal. □

We are now ready to state the ideal-theoretic form of the Nullstellensatz.

Theorem 6 (The Strong Nullstellensatz). *Let k be an algebraically closed field. If I is an ideal in $k[x_1, \ldots, x_n]$, then*

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

Proof. We certainly have $\sqrt{I} \subset \mathbf{I}(\mathbf{V}(I))$ because $f \in \sqrt{I}$ implies that $f^m \in I$ for some m. Hence, f^m vanishes on $\mathbf{V}(I)$, which implies that f vanishes on $\mathbf{V}(I)$. Thus, $f \in \mathbf{I}(\mathbf{V}(I))$.

Conversely, suppose that $f \in \mathbf{I}(\mathbf{V}(I))$. Then, by definition, f vanishes on $\mathbf{V}(I)$. By Hilbert's Nullstellensatz, there exists an integer $m \geq 1$ such that $f^m \in I$. But this means that $f \in \sqrt{I}$. Since f was arbitrary, $\mathbf{I}(\mathbf{V}(I)) \subset \sqrt{I}$. This completes the proof. □

It has become a custom, to which we shall adhere, to refer to Theorem 6 as *the* Nullstellensatz with no further qualification. The most important consequence of the Nullstellensatz is that it allows us to set up a "dictionary" between geometry and algebra. The basis of the dictionary is contained in the following theorem.

Theorem 7 (The Ideal–Variety Correspondence). *Let k be an arbitrary field.*

(i) *The maps*

$$\text{affine varieties} \xrightarrow{\mathbf{I}} \text{ideals}$$

and

$$\text{ideals} \xrightarrow{\mathbf{V}} \text{affine varieties}$$

are inclusion-reversing, i.e., if $I_1 \subset I_2$ are ideals, then $\mathbf{V}(I_1) \supset \mathbf{V}(I_2)$ and, similarly, if $V_1 \subset V_2$ are varieties, then $\mathbf{I}(V_1) \supset \mathbf{I}(V_2)$. Furthermore, for any variety V, we have

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

so that $\mathbf{I}$ is always one-to-one.

(ii) *If k is algebraically closed, and if we restrict to radical ideals, then the maps*

$$\text{affine varieties} \xrightarrow{\mathbf{I}} \text{radical ideals}$$

and

$$\text{radical ideals} \xrightarrow{\mathbf{V}} \text{affine varieties}$$

are inclusion-reversing bijections which are inverses of each other.

Proof. (i) In the exercises you will show that $\mathbf{I}$ and $\mathbf{V}$ are inclusion-reversing. It remains to prove that $\mathbf{V}(\mathbf{I}(V)) = V$ when $V = \mathbf{V}(f_1, \ldots, f_s)$ is a subvariety of k^n. Since every $f \in \mathbf{I}(V)$ vanishes on V, the inclusion $V \subset \mathbf{V}(\mathbf{I}(V))$ follows directly from the definition of $\mathbf{V}$. Going the other way, note that $f_1, \ldots, f_s \in \mathbf{I}(V)$ by the definition of $\mathbf{I}$, and, thus, $\langle f_1, \ldots, f_s \rangle \subset \mathbf{I}(V)$. Since $\mathbf{V}$ is inclusion-reversing, it follows that $\mathbf{V}(\mathbf{I}(V)) \subset \mathbf{V}(\langle f_1, \ldots, f_s \rangle) = V$. This proves the desired equality $\mathbf{V}(\mathbf{I}(V)) = V$, and, consequently, $\mathbf{I}$ is one-to-one since it has a left inverse.

(ii) Since $\mathbf{I}(V)$ is radical by Corollary 3, we can think of $\mathbf{I}$ as a function which takes varieties to radical ideals. Furthermore, we already know $\mathbf{V}(\mathbf{I}(V)) = V$ for any variety V. It remains to prove $\mathbf{I}(\mathbf{V}(I)) = I$ whenever I is a radical ideal. This is easy: the Nullstellensatz tells us $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$, and I being radical implies $\sqrt{I} = I$ (see

Exercise 4). This gives the desired equality. Hence, **V** and **I** are inverses of each other and, thus, define bijections between the set of radical ideals and affine varieties. The theorem is proved. □

As a consequence of this theorem, any question about varieties can be rephrased as an algebraic question about radical ideals (and conversely), provided that we are working over an algebraically closed field. This ability to pass between algebra and geometry will give us considerable power.

In view of the Nullstellensatz and the importance it assigns to radical ideals, it is natural to ask whether one can compute generators for the radical from generators of the original ideal. In fact, there are three questions to ask concerning an ideal $I = \langle f_1, \ldots, f_s \rangle$:

- (Radical Generators) Is there an algorithm which produces a set $\{g_1, \ldots, g_m\}$ of polynomials such that $\sqrt{I} = \langle g_1, \ldots, g_m \rangle$?
- (Radical Ideal) Is there an algorithm which will determine whether I is radical?
- (Radical Membership) Given $f \in k[x_1, \ldots, x_n]$, is there an algorithm which will determine whether $f \in \sqrt{I}$?

The existence of these algorithms follows from work of HERMANN (1926) [see also MINES, RICHMAN, and RUITENBERG (1988) and SEIDENBERG (1974, 1984) for more modern expositions]. Unfortunately, the algorithms given in these papers for the first two questions are not very practical and would not be suitable for using on a computer. However, work by GIANNI, TRAGER and ZACHARIAS (1988) has led to an algorithm implemented in AXIOM and REDUCE for finding the radical of an ideal. This algorithm is described in detail in Theorem 8.99 of BECKER and WEISPFENNING (1993). A different algorithm for radicals, due to EISENBUD, HUNEKE and VASCONCELOS (1992), has been implemented in Macaulay 2.

For now, we will settle for solving the more modest *radical membership problem*. To test whether $f \in \sqrt{I}$, we could use the ideal membership algorithm to check whether $f^m \in I$ for all integers $m > 0$. This is not satisfactory because we might have to go to very large powers of m, and it will never tell us if $f \notin \sqrt{I}$ (at least, not until we work out *a priori* bounds on m). Fortunately, we can adapt the proof of Hilbert's Nullstellensatz to give an algorithm for determining whether $f \in \sqrt{\langle f_1, \ldots, f_s \rangle}$.

Proposition 8 (Radical Membership). *Let k be an arbitrary field and let $I = \langle f_1, \ldots, f_s \rangle \subset k[x_1, \ldots, x_n]$ be an ideal. Then $f \in \sqrt{I}$ if and only if the constant polynomial 1 belongs to the ideal $\tilde{I} = \langle f_1, \ldots, f_s, 1 - yf \rangle \subset k[x_1, \ldots, x_n, y]$ (in which case, $\tilde{I} = k[x_1, \ldots, x_n, y]$).*

Proof. From equations (2), (3), and (4) in the proof of Hilbert's Nullstellensatz in §1, we see that $1 \in \tilde{I}$ implies $f^m \in I$ for some m, which, in turn, implies $f \in \sqrt{I}$. Going the other way, suppose that $f \in \sqrt{I}$. Then $f^m \in I \subset \tilde{I}$ for some m. But we also have $1 - yf \in \tilde{I}$, and, consequently,

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

as desired. □

Proposition 8, together with our earlier remarks on determining whether 1 belongs to an ideal (see the discussion of the consistency problem in §1), immediately leads to the **radical membership algorithm**. That is, to determine if $f \in \sqrt{\langle f_1, \ldots, f_s \rangle} \subset k[x_1, \ldots, x_n]$, we compute a reduced Groebner basis of the ideal $\langle f_1, \ldots, f_s, 1 - yf \rangle \subset k[x_1, \ldots, x_n, y]$ with respect to some ordering. If the result is $\{1\}$, then $f \in \sqrt{I}$. Otherwise, $f \notin \sqrt{I}$.

As an example, consider the ideal $I = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1 \rangle$ in $k[x, y]$. Let us test if $f = y - x^2 + 1$ lies in $\sqrt{I}$. Using lex order on $k[x, y, z]$, one checks that the ideal

$$\tilde{I} = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1, 1 - z(y - x^2 + 1) \rangle \subset k[x, y, z]$$

has reduced Groebner basis $\{1\}$. It follows that $y - x^2 + 1 \in \sqrt{I}$ by Proposition 8.

Indeed, using the division algorithm, we can check what power of $y - x^2 + 1$ lies in I:

$$\begin{aligned}
\overline{y - x^2 + 1}^G &= y - x^2 + 1, \\
\overline{(y - x^2 + 1)^2}^G &= -2x^2y + 2y, \\
\overline{(y - x^2 + 1)^3}^G &= 0,
\end{aligned}$$

where $G = \{x^4 - 2x^2 + 1, y^2\}$ is a Groebner basis for I with respect to lex order and $\overline{p}^G$ is the remainder of p on division by G. As a consequence, we see that $(y - x^2 + 1)^3 \in I$, but no lower power of $y - x^2 + 1$ is in I (in particular, $y - x^2 + 1 \notin I$).

We can also see what is happening in this example geometrically. As a set, $\mathbf{V}(I) = \{(\pm 1, 0)\}$, but (speaking somewhat imprecisely) every polynomial in I vanishes to order at least 2 at each of the two points in $\mathbf{V}(I)$. This is visible from the form of the generators of I if we factor them:

$$xy^2 + 2y^2 = y^2(x + 2) \quad \text{and} \quad x^4 - 2x^2 + 1 = (x^2 - 1)^2.$$

Even though $f = y - x^2 + 1$ also vanishes at $(\pm 1, 0)$, f only vanishes to order 1 there. We must take a higher power of f to obtain an element of I.

We will end this section with a discussion of the one case where we can compute the radical of an ideal, which is when we are dealing with a principal ideal $I = \langle f \rangle$. Recall that a polynomial f is said to be *irreducible* if it has the property that whenever $f = g \cdot h$ for some polynomials g and h, then either g or h is a constant. We saw in §5 of Chapter 3 that any polynomial f can always be written as a product of irreducible polynomials. By collecting the irreducible polynomials which differ by constant multiples of one another, we can write f in the form

$$f = c f_1^{a_1} \cdots f_r^{a_r}, \quad c \in k,$$

where the f_i's $1 \leq i \leq r$, are *distinct* irreducible polynomials. That is, where f_i and f_j are not constant multiples of one another whenever $i \neq j$. Moreover, this expression for f is *unique* up to reordering the f_i's and up to multiplying the f_i's by constant multiples. (This is just a restatement of Theorem 5 of Chapter 3, §5.) If we have f expressed as a product of irreducible polynomials, then it is easy to write down an explicit expression for the radical of the principal ideal generated by f.

Proposition 9. *Let $f \in k[x_1, \ldots, x_n]$ and $I = \langle f \rangle$ the principal ideal generated by f. If $f = cf_1^{a_1} \cdots f_r^{a_r}$ is the factorization of f into a product of distinct irreducible polynomials, then*

$$\sqrt{I} = \sqrt{\langle f \rangle} = \langle f_1 f_2 \cdots f_r \rangle.$$

Proof. We first show that $f_1 f_2 \cdots f_r$ belongs to $\sqrt{I}$. Let N be an integer strictly greater than the maximum of $a_1, \ldots, a_r$. Then

$$(f_1 f_2 \cdots f_r)^N = f_1^{N-a_1} f_2^{N-a_2} \cdots f_r^{N-a_r} f$$

is a polynomial multiple of f. This shows that $(f_1 f_2 \cdots f_r)^N \in I$, which implies that $f_1 f_2 \cdots f_r \in \sqrt{I}$. Thus $\langle f_1 f_2 \cdots f_r \rangle \subset \sqrt{I}$.

Conversely, suppose that $g \in \sqrt{I}$. Then there exists a positive integer M such that $g^M \in I$. This means that $g^M = h \cdot f$ for some polynomial h. Now suppose that $g = g_1^{b_1} g_2^{b_2} \cdots g_s^{b_s}$ is the factorization of g into a product of distinct irreducible polynomials. Then $g^M = g_1^{b_1 M} g_2^{b_2 M} \cdots g_s^{b_s M}$ is the factorization of g^M into a product of distinct irreducible polynomials. Thus,

$$g_1^{b_1 M} g_2^{b_2 M} \cdots g_s^{b_s M} = h \cdot f_1^{a_1} f_2^{a_2} \cdots f_r^{a_r}.$$

But, by unique factorization, the irreducible polynomials on both sides of the above equation must be the same (up to multiplication by constants). Since the $f_1, \ldots, f_r$ are irreducible; each f_i, $1 \leq i \leq r$ must be equal to a constant multiple of some g_j. This implies that g is a polynomial multiple of $f_1 f_2 \cdots f_r$ and, therefore g is contained in the ideal $\langle f_1 f_2 \cdots f_r \rangle$. The proposition is proved. □

In view of Proposition 9, we make the following definition:

Definition 10. *If $f \in k[x_1, \ldots, x_n]$ is a polynomial, we define the* **reduction** *of f, denoted f_{red}, to be the polynomial such that $\langle f_{red} \rangle = \sqrt{\langle f \rangle}$. A polynomial is said to be* **reduced** *(or* **square-free***) if $f = f_{red}$.*

Thus, f_{red} is the polynomial f with repeated factors "stripped away." So, for example, if $f = (x + y^2)^3(x - y)$, then $f_{red} = (x + y^2)(x - y)$. Note that f_{red} is only unique up to a constant factor in k.

The usefulness of Proposition 9 is mitigated by the requirement that f be factored into irreducible factors. We might ask if there is an algorithm to compute f_{red} from f without factoring f first. It turns out that such an algorithm exists.

To state the algorithm, we will need the notion of a greatest common divisor of two polynomials.

Definition 11. *Let $f, g \in k[x_1, \ldots, x_n]$. Then $h \in k[x_1, \ldots, x_n]$ is called a* **greatest common divisor** *of f and g, and denoted $h = \mathrm{GCD}(f, g)$, if*

(i) *h divides f and g.*

(ii) *If p is any polynomial which divides both f and g, then p divides h.*

It is easy to show that GCD(f, g) exists and is unique up to multiplication by a nonzero constant in k (see Exercise 9). Unfortunately, the one-variable algorithm for finding the GCD (that is, the Euclidean Algorithm) does not work in the case of several variables. To see this, consider the polynomials xy and xz in $k[x, y, z]$. Clearly, $\mathrm{GCD}(xy, xz) = x$. However, no matter what term ordering we use, dividing xy by xz gives 0 plus remainder xy and dividing xz by xy gives 0 plus remainder xz. As a result, neither polynomial "reduces" with respect to the other and there is no next step to which to apply the analogue of the Euclidean Algorithm.

Nevertheless, there is an algorithm for calculating the GCD of two polynomials in several variables. We defer a discussion of it until the next section after we have studied intersections of ideals. For the purposes of our discussion here, let us assume that we have such an algorithm. We also remark that given polynomials $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, one can define $\mathrm{GCD}(f_1, f_2, \ldots, f_s)$ exactly as in the one-variable case. There is also an algorithm for computing $\mathrm{GCD}(f_1, f_2, \ldots, f_s)$.

Using this notion of GCD, we can now give a formula for computing the radical of a principal ideal.

Proposition 12. *Suppose that k is a field containing the rational numbers $\mathbb{Q}$ and let $I = \langle f \rangle$ be a principal ideal in $k[x_1, \ldots, x_n]$. Then $\sqrt{I} = \langle f_{red} \rangle$, where*

$$f_{red} = \frac{f}{\mathrm{GCD}\left(f, \dfrac{\partial f}{\partial x_1}, \dfrac{\partial f}{\partial x_2}, \ldots, \dfrac{\partial f}{\partial x_n}\right)}.$$

Proof. Writing f as in Proposition 9, we know that $\sqrt{I} = \langle f_1 f_2 \cdots f_r \rangle$. Thus, it suffices to show that

$$\mathrm{GCD}\left(f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right) = f_1^{a_1-1} f_2^{a_2-1} \cdots f_r^{a_r-1}. \tag{1}$$

We first use the product rule to note that

$$\frac{\partial f}{\partial x_j} = f_1^{a_1-1} f_2^{a_2-1} \cdots f_r^{a_r-1}\left(a_1 \frac{\partial f_1}{\partial x_j} f_2 \cdots f_r + \cdots + a_r f_1 \cdots f_{r-1} \frac{\partial f_r}{\partial x_j}\right).$$

This proves that $f_1^{a_1-1} f_2^{a_2-1} \cdots f_r^{a_r-1}$ divides the GCD. It remains to show that for each i, there is some $\frac{\partial f}{\partial x_j}$ which is not divisible by $f_i^{a_i}$.

Write $f = f_i^{a_i} h_i$, where h_i is not divisible by f_i. Since f_i is nonconstant, some variable x_j must appear in f_i. The product rule gives us

$$\frac{\partial f_i}{\partial x_j} = f_i^{a_i-1}\left(a_1 \frac{\partial f_i}{\partial x_j} h_i + f_i \frac{\partial h_i}{\partial x_j}\right).$$

If this expression is divisible by $f_i^{a_i}$, then $\frac{\partial f_i}{\partial x_j} h_i$ must be divisible by f_i. Since f_i is irreducible and does not divide h_i, this forces f_i to divide $\frac{\partial f_i}{\partial x_j}$. In Exercise 13, you will show that $\frac{\partial f_i}{\partial x_j}$ is nonzero since $\mathbb{Q} \subset k$ and x_j appears in f_i. As $\frac{\partial f_i}{\partial x_j}$ also has smaller total degree than f_i, it follows that f_i cannot divide $\frac{\partial f_i}{\partial x_j}$. Consequently, $\frac{\partial f}{\partial x_j}$ is not divisible by $f_i^{a_i}$, which proves (1), and the proposition follows. □

It is worth remarking that for fields which do not contain $\mathbb{Q}$, the above formula for f_{red} may fail (see Exercise 13).

EXERCISES FOR §2

1. Given a field k (not necessarily algebraically closed), show that $\sqrt{\langle x^2, y^2\rangle} = \langle x, y\rangle$ and, more generally, show that $\sqrt{\langle x^n, y^m\rangle} = \langle x, y\rangle$ for any positive integers n and m.
2. Let f and g be distinct nonconstant polynomials in $k[x, y]$ and let $I = \langle f^2, g^3\rangle$. Is it necessarily true that $\sqrt{I} = \langle f, g\rangle$? Explain.
3. Show that $\langle x^2 + 1\rangle \subset \mathbb{R}[x]$ is a radical ideal, but that $\mathbf{V}(x^2 + 1)$ is the empty variety.
4. Let I be an ideal in $k[x_1, \dots, x_n]$, where k is an arbitrary field.
   a. Show that $\sqrt{I}$ is a radical ideal.
   b. Show that I is radical if and only if $I = \sqrt{I}$.
   c. Show that $\sqrt{\sqrt{I}} = \sqrt{I}$.
5. Prove that $\mathbf{I}$ and $\mathbf{V}$ are inclusion-reversing.
6. Let I be an ideal in $k[x_1, \dots, x_n]$.
   a. In the special case when $\sqrt{I} = \langle f_1, f_2\rangle$, with $f_i^{m_i} \in I$, prove that $f^{m_1+m_2-1} \in I$ for all $f \in \sqrt{I}$.
   b. Now prove that for any I, there exists m_0 such that $f^{m_0} \in I$ for all $f \in \sqrt{I}$. Hint: Write $\sqrt{I} = \langle f_1, \dots, f_s\rangle$.
7. Determine whether the following polynomials lie in the following radicals. If the answer is yes, what is the smallest power of the polynomial that lies in the ideal?
   a. Is $x + y \in \sqrt{\langle x^3, y^3, xy(x + y)\rangle}$?
   b. Is $x^2 + 3xz \in \sqrt{\langle x + z, x^2y, x - z^2\rangle}$?
8. Show that if f_m and f_{m+1} are homogeneous polynomials of degree m and $m + 1$, respectively, with no common factors [i.e., $\mathrm{GCD}(f_m, f_{m+1}) = 1$], then $h = f_m + f_{m+1}$ is irreducible.
9. Given $f, g \in k[x_1, \dots, x_n]$, use unique factorization to prove that $\mathrm{GCD}(f, g)$ exists. Also prove that $\mathrm{GCD}(f, g)$ is unique up to multiplication by a nonzero constant of k.
10. Prove the following ideal-theoretic characterization of $\mathrm{GCD}(f, g)$: given f, g, h in $k[x_1, \dots, x_n]$, then $h = \mathrm{GCD}(f, g)$ if and only if h is a generator of the smallest principal ideal containing $\langle f, g\rangle$ (that is, if $\langle h\rangle \subset J$, whenever J is a principal ideal such that $J \supset \langle f, g\rangle$).
11. Find a basis for the ideal
$$\sqrt{\langle x^5 - 2x^4 + 2x^2 - x, x^5 - x^4 - 2x^3 + 2x^2 + x - 1\rangle}.$$
Compare with Exercise 17 of Chapter 1, §5.
12. Let $f = x^5 + 3x^4y + 3x^3y^2 - 2x^4y^2 + x^2y^3 - 6x^3y^3 - 6x^2y^4 + x^3y^4 - 2xy^5 + 3x^2y^5 + 3xy^6 + y^7 \in \mathbb{Q}[x, y]$. Compute $\sqrt{\langle f\rangle}$.
13. A field k has *characteristic zero* if it contains the rational numbers $\mathbb{Q}$; otherwise, k has *positive characteristic*.
   a. Let k be the field $\mathbb{F}_2$ from Exercise 1 of Chapter 1, §1. If $f = x_1^2 + \cdots + x_n^2 \in \mathbb{F}_2[x_1, \dots, x_n]$, then show that $\frac{\partial f}{\partial x_i} = 0$ for all i. Conclude that the formula given in Proposition 12 may fail when the field is $\mathbb{F}_2$.

b. Let k be a field of characteristic zero and let $f \in k[x_1, \ldots, x_n]$ be nonconstant. If the variable x_j appears in f, then prove that $\frac{\partial f}{\partial x_j} \neq 0$. Also explain why $\frac{\partial f}{\partial x_j}$ has smaller total degree than f.

14. Let $J = \langle xy, (x - y)x \rangle$. Describe $\mathbf{V}(J)$ and show that $\sqrt{J} = \langle x \rangle$.
15. Prove that $I = \langle xy, xz, yz \rangle$ is a radical ideal. Hint: If you divide $f \in k[x, y, z]$ by xy, xz, yz, what does the remainder look like? What does f^m look like?

§3 Sums, Products, and Intersections of Ideals

Ideals are algebraic objects and, as a result, there are natural algebraic operations we can define on them. In this section, we consider three such operations: sum, intersection, and product. These are binary operations: to each pair of ideals, they associate a new ideal. We shall be particularly interested in two general questions which arise in connection with each of these operations. The first asks how, given generators of a pair of ideals, one can compute generators of the new ideals which result on applying these operations. The second asks for the geometric significance of these algebraic operations. Thus, the first question fits the general computational theme of this book; the second, the general thrust of this chapter. We consider each of the operations in turn.

Sums of Ideals

Definition 1. *If I and J are ideals of the ring $k[x_1, \ldots, x_n]$, then the* **sum** *of I and J, denoted $I + J$, is the set*

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

Proposition 2. *If I and J are ideals in $k[x_1, \ldots, x_n]$, then $I + J$ is also an ideal in $k[x_1, \ldots, x_n]$. In fact, $I + J$ is the smallest ideal containing I and J. Furthermore, if $I = \langle f_1, \ldots, f_r \rangle$ and $J = \langle g_1, \ldots, g_s \rangle$, then $I + J = \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$.*

Proof. Note first that $0 = 0 + 0 \in I + J$. Suppose $h_1, h_2 \in I + J$. By the definition of $I + J$, there exist $f_1, f_2 \in I$ and $g_1, g_2 \in J$ such that $h_1 = f_1 + g_1, h_2 = f_2 + g_2$. Then, after rearranging terms slightly, $h_1 + h_2 = (f_1 + f_2) + (g_1 + g_2)$. But $f_1 + f_2 \in I$ because I is an ideal and, similarly, $g_1 + g_2 \in J$, whence $h_1 + h_2 \in I + J$. To check closure under multiplication, let $h \in I + J$ and $l \in k[x_1, \ldots, x_n]$ be any polynomial. Then, as above, there exist $f \in I$ and $g \in J$ such that $h = f + g$. But then $l \cdot h = l \cdot (f + g) = l \cdot f + l \cdot g$. Now $l \cdot f \in I$ and $l \cdot g \in J$ because I and J are ideals. Consequently, $l \cdot h \in I + J$. This shows that $I + J$ is an ideal.

If H is an ideal which contains I and J, then H must contain all elements $f \in I$ and $g \in J$. Since H is an ideal, H must contain all $f + g$, where $f \in I, g \in J$. In particular, $H \supset I + J$. Therefore, every ideal containing I and J contains $I + J$ and, thus, $I + J$ must be the smallest such ideal. Finally, if $I = \langle f_1, \ldots, f_r \rangle$ and $J = \langle g_1, \ldots, g_s \rangle$, then $\langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$ is an ideal containing I and J, so that

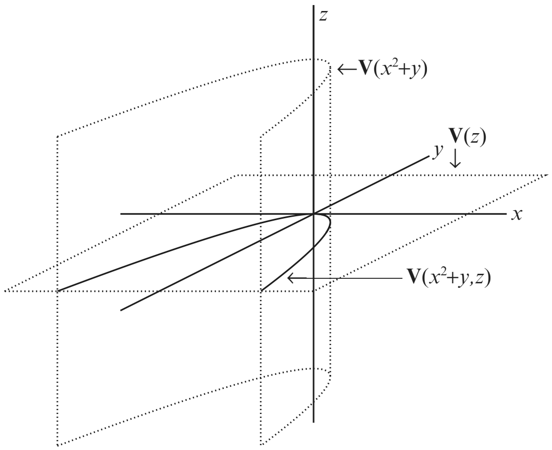
$I + J \subset \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$. The reverse inclusion is obvious, so that $I + J = \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$. □

The following corollary is an immediate consequence of Proposition 2.

Corollary 3. *If $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$, then*

$$\langle f_1, \ldots, f_r \rangle = \langle f_1 \rangle + \cdots + \langle f_r \rangle.$$

To see what happens geometrically, let $I = \langle x^2 + y \rangle$ and $J = \langle z \rangle$ be ideals in $\mathbb{R}^3$. We have sketched $\mathbf{V}(I)$ and $\mathbf{V}(J)$ below. Then $I + J = \langle x^2 + y, z \rangle$ contains both $x^2 + y$ and z. Thus, the variety $\mathbf{V}(I + J)$ must consist of those points where both $x^2 + y$ and z vanish. That is, it must be the intersection of $\mathbf{V}(I)$ and $\mathbf{V}(J)$.



The same line of reasoning generalizes to show that addition of ideals corresponds geometrically to taking intersections of varieties.

Theorem 4. *If I and J are ideals in $k[x_1, \ldots, x_n]$, then $\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J)$.*

Proof. If $x \in \mathbf{V}(I + J)$, then $x \in \mathbf{V}(I)$ because $I \subset I + J$; similarly, $x \in \mathbf{V}(J)$. Thus, $x \in \mathbf{V}(I) \cap \mathbf{V}(J)$ and we conclude that $\mathbf{V}(I + J) \subset \mathbf{V}(I) \cap \mathbf{V}(J)$.

To get the opposite inclusion, suppose $x \in \mathbf{V}(I) \cap \mathbf{V}(J)$. Let h be any polynomial in $I + J$. Then there exist $f \in I$ and $g \in J$ such that $h = f + g$. We have $f(x) = 0$ because $x \in \mathbf{V}(I)$ and $g(x) = 0$ because $x \in \mathbf{V}(J)$. Thus, $h(x) = f(x) + g(x) = 0 + 0 = 0$. Since h was arbitrary, we conclude that $x \in \mathbf{V}(I + J)$. Hence, $\mathbf{V}(I + J) \supset \mathbf{V}(I) \cap \mathbf{V}(J)$. □

An analogue of Theorem 4, stated in terms of generators was given in Lemma 2 of Chapter 1, §2.

Products of Ideals

In Lemma 2 of Chapter 1, §2, we encountered the fact that an ideal generated by the products of the generators of two other ideals corresponds to the union of varieties:

$$\mathbf{V}(f_1, \ldots, f_r) \cup \mathbf{V}(g_1, \ldots, g_s) = \mathbf{V}(f_i g_j, 1 \le i \le r, 1 \le j \le s).$$

Thus, for example, the variety $\mathbf{V}(xz, yz)$ corresponding to an ideal generated by the product of the generators of the ideals, $\langle x, y \rangle$ and $\langle z \rangle$ in $k[x, y, z]$ is the union of $\mathbf{V}(x, y)$ (the z-axis) and $\mathbf{V}(z)$ (the xy-plane). This suggests the following definition.

Definition 5. *If I and J are two ideals in $k[x_1, \ldots, x_n]$, then their* **product***, denoted $I \cdot J$, is defined to be the ideal generated by all polynomials $f \cdot g$ where $f \in I$ and $g \in J$.*

Thus, the product $I \cdot J$ of I and J is the set

$$I \cdot J = \{f_1 g_1 + \cdots + f_r g_r : f_1, \ldots, f_r \in I, g_1, \ldots, g_r \in J, r \text{ a positive integer}\}.$$

To see that this is an ideal, note that $0 = 0 \cdot 0 \in I \cdot J$. Moreover, it is clear that $h_1, h_2 \in I \cdot J$ implies that $h_1 + h_2 \in I \cdot J$. Finally, if $h = f_1 g_1 + \cdots + f_r g_r \in I \cdot J$ and p is any polynomial, then

$$ph = (pf_1)g_1 + \cdots + (pf_r)g_r \in I \cdot J$$

since $pf_i \in I$ for all i, $1 \le i \le r$. Note that the set of products would not be an ideal because it would not be closed under addition. The following easy proposition shows that computing a set of generators for $I \cdot J$ given sets of generators for I and J is completely straightforward.

Proposition 6. *Let $I = \langle f_1, \ldots, f_r \rangle$ and $J = \langle g_1, \ldots, g_s \rangle$. Then $I \cdot J$ is generated by the set of all products of generators of I and J:*

$$I \cdot J = \langle f_i g_j : 1 \le i \le r, 1 \le j \le s \rangle.$$

Proof. It is clear that the ideal generated by products $f_i g_j$ of the generators is contained in $I \cdot J$. To establish the opposite inclusion, note that any polynomial in $I \cdot J$ is a sum of polynomials of the form fg with $f \in I$ and $g \in J$. But we can write f and g in terms of the generators $f_1, \ldots, f_r$ and $g_1, \ldots, g_s$, respectively, as

$$f = a_1 f_1 + \cdots + a_r f_r, \quad g = b_1 g_1 + \cdots + b_s g_s$$

for appropriate polynomials $a_1, \ldots, a_r, b_1, \ldots, b_s$. Thus, fg, and any sum of polynomials of this form, can be written as a sum $\sum c_{ij} f_i g_j$, where $c_{ij} \in k[x_1, \ldots, x_n]$. □

The following proposition guarantees that the product of ideals does indeed correspond geometrically to the operation of taking the union of varieties.

Theorem 7. *If I and J are ideals in $k[x_1, \ldots, x_n]$, then $\mathbf{V}(I \cdot J) = \mathbf{V}(I) \cup \mathbf{V}(J)$.*

Proof. Let $x \in \mathbf{V}(I \cdot J)$. Then $g(x)h(x) = 0$ for all $g \in I$ and all $h \in J$. If $g(x) = 0$ for all $g \in I$, then $x \in \mathbf{V}(I)$. If $g(x) \neq 0$ for some $g \in I$, then we must have $h(x) = 0$ for all $h \in J$. In either event, $x \in \mathbf{V}(I) \cup \mathbf{V}(J)$.

Conversely, suppose $x \in \mathbf{V}(I) \cup \mathbf{V}(J)$. Either $g(x) = 0$ for all $g \in I$ or $h(x) = 0$ for all $h \in J$. Thus, $g(x)h(x) = 0$ for all $g \in I$ and $h \in J$. Thus, $f(x) = 0$ for all $f \in I \cdot J$ and, hence, $x \in \mathbf{V}(I \cdot J)$. □

In what follows, we will often write the product of ideals as IJ rather than $I \cdot J$.

Intersections of Ideals

The operation of forming the intersection of two ideals is, in some ways, even more primitive than the operations of addition and multiplication.

Definition 8. *The* **intersection** $I \cap J$ *of two ideals I and J in* $k[x_1, \ldots, x_n]$ *is the set of polynomials which belong to both I and J.*

As in the case of sums, the set of ideals is closed under intersections.

Proposition 9. *If I and J are ideals in* $k[x_1, \ldots, x_n]$*, then* $I \cap J$ *is also an ideal.*

Proof. Note that $0 \in I \cap J$ since $0 \in I$ and $0 \in J$. If $f, g \in I \cap J$, then $f + g \in I$ because $f, g \in I$. Similarly, $f + g \in J$ and, hence, $f + g \in I \cap J$. Finally, to check closure under multiplication, let $f \in I \cap J$ and h by any polynomial in $k[x_1, \ldots, x_n]$. Since $f \in I$ and I is an ideal, we have $h \cdot f \in I$. Similarly, $h \cdot f \in J$ and, hence, $h \cdot f \in I \cap J$ □

Note that we always have $IJ \subset I \cap J$ since elements of IJ are sums of polynomials of the form fg with $f \in I$ and $g \in J$. But the latter belongs to both I (since $f \in I$) and J (since $g \in J$). However, IJ can be strictly contained in $I \cap J$. For example, if $I = J = \langle x, y \rangle$, then $IJ = \langle x^2, xy, y^2 \rangle$ is strictly contained in $I \cap J = I = \langle x, y \rangle$ ($x \in I \cap J$, but $x \notin IJ$).

Given two ideals and a set of generators for each, we would like to be able to compute a set of generators for the intersection. This is much more delicate than the analogous problems for sums and products of ideals, which were entirely straightforward. To see what is involved, suppose I is the ideal in $\mathbb{Q}[x, y]$ generated by the polynomial $f = (x + y)^4(x^2 + y)^2(x - 5y)$ and let J be the ideal generated by the polynomial $g = (x + y)(x^2 + y)^3(x + 3y)$. We leave it as an (easy) exercise to check that

$$I \cap J = \langle (x + y)^4(x^2 + y)^3(x - 5y)(x + 3y) \rangle.$$

This computation is easy precisely because we were given factorizations of f and g into irreducible polynomials. In general, such factorizations may not be available. So any algorithm which allows one to compute intersections will have to be powerful enough to circumvent this difficulty.

Nevertheless, there is a nice trick which reduces the computation of intersections to computing the intersection of an ideal with a subring (i.e., eliminating variables), a problem which we have already solved. To state the theorem, we need a little notation: if I is an ideal in $k[x_1, \ldots, x_n]$ and $f(t) \in k[t]$ a polynomial in the single variable t, then fI denotes the ideal in $k[x_1, \ldots, x_n, t]$ generated by the set of polynomials $\{f \cdot h : h \in I\}$. This is a little different from our usual notion of product in that the ideal I and the ideal generated by $f(t)$ in $k[t]$ lie in different rings: in fact, the ideal $I \subset k[x_1, \ldots, x_n]$ is *not* an ideal in $k[x_1, \ldots, x_n, t]$ because it is not closed under multiplication by t. When we want to stress that the polynomial $f \in k[t]$ is a polynomial in t alone, we write $f = f(t)$. Similarly, to stress that a polynomial $h \in k[x_1, \ldots, x_n]$ involves only the variables $x_1, \ldots, x_n$, we write $h = h(x)$. Along the same lines, if we are considering a polynomial g in $k[x_1, \ldots, x_n, t]$ and we want to emphasize that it can involve the variables $x_1, \ldots, x_n$ as well as t, we will write $g = g(x, t)$. In terms of this notation, $fI = f(t)I = \langle f(t)h(x) : h(x) \in I\rangle$. So, for example, if $f(t) = t^2 - t$ and $I = \langle x, y\rangle$, then the ideal $f(t)I$ in $k[x, y, t]$ contains $(t^2 - t)x$ and $(t^2 - t)y$. In fact, it is not difficult to see that $f(t)I$ is generated as an ideal by $(t^2 - t)x$ and $(t^2 - t)y$. This is a special case of the following assertion.

Lemma 10.

(i) *If I is generated as an ideal in $k[x_1, \ldots, x_n]$ by $p_1(x), \ldots, p_r(x)$, then $f(t)I$ is generated as an ideal in $k[x_1, \ldots, x_n, t]$ by $f(t) \cdot p_1(x), \ldots, f(t) \cdot p_r(x)$.*

(ii) *If $g(x, t) \in f(t)I$ and a is any element of the field k, then $g(x, a) \in I$.*

Proof. To prove the first assertion, note that any polynomial $g(x, t) \in f(t)I$ can be expressed as a sum of terms of the form $h(x, t) \cdot f(t) \cdot p(x)$ for $h \in k[x_1, \ldots, x_n, t]$ and $p \in I$. But because I is generated by $p_1, \ldots, p_r$ the polynomial $p(x)$ can be expressed as a sum of terms of the form $q_i(x)p_i(x)$, $1 \leq i \leq r$. That is,

$$p(x) = \sum_{i=1}^{r} q_i(x)p_i(x).$$

Hence,

$$h(x, t) \cdot f(t) \cdot p(x) = \sum_{i=1}^{r} h(x, t)q_i(x)f(t)p_i(x).$$

Now, for each i, $1 \leq i \leq r$, $h(x, t) \cdot q_i(x) \in k[x_1, \ldots, x_n, t]$. Thus, $h(x, t) \cdot f(t) \cdot p(x)$ belongs to the ideal in $k[x_1, \ldots, x_n, t]$ generated by $f(t) \cdot p_1(x), \ldots, f(t) \cdot p_r(x)$. Since $g(x, t)$ is a sum of such terms,

$$g(x, t) \in \langle f(t) \cdot p_1(x), \ldots, f(t) \cdot p_r(x)\rangle,$$

which establishes (i). The second assertion follows immediately upon substituting $a \in k$ for t. $\square$

Theorem 11. *Let I, J be ideals in $k[x_1, \ldots, x_n]$. Then*

$$I \cap J = (tI + (1 - t)J) \cap k[x_1, \ldots, x_n].$$

Proof. Note that $tI + (1-t)J$ is an ideal in $k[x_1, \dots, x_n, t]$. To establish the desired equality, we use the usual strategy of proving containment in both directions.

Suppose $f \in I \cap J$. Since $f \in I$, we have $t \cdot f \in tI$. Similarly, $f \in J$ implies $(1-t) \cdot f \in (1-t)J$. Thus, $f = t \cdot f + (1-t) \cdot f \in tI + (1-t)J$. Since $I, J \subset k[x_1, \dots, x_n]$, we have $f \in (tI + (1-t)J) \cap k[x_1, \dots, x_n]$. This shows that $I \cap J \subset (tI + (1-t)J) \cap k[x_1, \dots, x_n]$.

To establish containment in the opposite direction, suppose $f \in (tI + (1-t)J) \cap k[x_1, \dots, x_n]$. Then $f(x) = g(x,t) + h(x,t)$, where $g(x,t) \in tI$ and $h(x,t) \in (1-t)J$. First set $t = 0$. Since every element of tI is a multiple of t, we have $g(x,0) = 0$. Thus, $f(x) = h(x,0)$ and hence, $f(x) \in J$ by Lemma 10. On the other hand, set $t = 1$ in the relation $f(x) = g(x,t) + h(x,t)$. Since every element of $(1-t)J$ is a multiple of $1-t$, we have $h(x,1) = 0$. Thus, $f(x) = g(x,1)$ and, hence, $f(x) \in I$ by Lemma 10. Since f belongs to both I and J, we have $f \in I \cap J$. Thus, $I \cap J \supset (tI + (1-t)J) \cap k[x_1, \dots, x_n]$ and this completes the proof. □

The above result and the Elimination Theorem (Theorem 2 of Chapter 3, §1) lead to the following **algorithm for computing intersections of ideals:** if $I = \langle f_1, \dots, f_r \rangle$ and $J = \langle g_1, \dots, g_s \rangle$ are ideals in $k[x_1, \dots, x_n]$, we consider the ideal

$$\langle tf_1, \dots, tf_r, (1-t)g_1, \dots, (1-t)g_s \rangle \subset k[x_1, \dots, x_n, t]$$

and compute a Groebner basis with respect to lex order in which t is greater than the x_i. The elements of this basis which do not contain the variable t will form a basis (in fact, a Groebner basis) of $I \cap J$. For more efficient calculations, one could also use one of the orders described in Exercises 5 and 6 of Chapter 3, §1. An algorithm for intersecting three or more ideals is described in Proposition 6.19 of Becker and Weispfenning (1993).

As a simple example of the above procedure, suppose we want to compute the intersection of the ideals $I = \langle x^2 y \rangle$ and $J = \langle xy^2 \rangle$ in $\mathbb{Q}[x, y]$. We consider the ideal

$$tI + (1-t)J = \langle tx^2 y, (1-t)xy^2 \rangle = \langle tx^2 y, txy^2 - xy^2 \rangle$$

in $\mathbb{Q}[t, x, y]$. Computing the S-polynomial of the generators, we obtain $tx^2y^2 - (tx^2y^2 - x^2y^2) = x^2y^2$. It is easily checked that $\{tx^2y, txy^2 - xy^2, x^2y^2\}$ is a Groebner basis of $tI + (1-t)J$ with respect to lex order with $t > x > y$. By the Elimination Theorem, $\{x^2y^2\}$ is a (Groebner) basis of $(tI + (1-t)J) \cap \mathbb{Q}[x, y]$. Thus,

$$I \cap J = \langle x^2 y^2 \rangle.$$

As another example, we invite the reader to apply the algorithm for computing intersections of ideals to give an alternate proof that the intersection $I \cap J$ of the ideals

$$I = \langle (x+y)^4 (x^2+y)^2 (x-5y) \rangle \quad \text{and} \quad J = \langle (x+y)(x^2+y)^3 (x+3y) \rangle$$

in $\mathbb{Q}[x, y]$ is

$$I \cap J = \langle (x+y)^4 (x^2+y)^3 (x-5y)(x+3y) \rangle.$$

These examples above are rather simple in that our algorithm applies to ideals which are not necessarily principal, whereas the examples given here involve intersections of principal ideals. We shall see a somewhat more complicated example in the exercises.

We can generalize both of the examples above by introducing the following definition.

Definition 12. *A polynomial $h \in k[x_1, \dots, x_n]$ is called a* **least common multiple** *of $f, g \in k[x_1, \dots, x_n]$ and denoted $h = \mathrm{LCM}(f, g)$ if*
(i) *f divides h and g divides h.*
(ii) *h divides any polynomial which both f and g divide.*

For example,

$$\mathrm{LCM}(x^2y, xy^2) = x^2y^2$$

and

$$\begin{aligned}\mathrm{LCM}((x+y)^4(x^2+y)^2(x-5y), (x+y)(x^2+y)^3(x+3y)) \\ = (x+y)^4(x^2+y)^3(x-5y)(x+3y).\end{aligned}$$

More generally, suppose $f, g \in k[x_1, \dots, x_n]$ and let $f = cf_1^{a_1} \dots f_r^{a_r}$ and $g = c'g_1^{b_1} \dots g_s^{b_s}$ be their factorizations into distinct irreducible polynomials. It may happen that some of the irreducible factors of f are constant multiples of those of g. In this case, let us suppose that we have rearranged the order of the irreducible polynomials in the expressions for f and g so that for some l, $1 \le l \le \min(r, s)$, f_i is a constant (nonzero) multiple of g_i for $1 \le i \le l$ and for all $i, j > l$, f_i is not a constant multiple of g_j. Then it follows from unique factorization that

$$\mathrm{LCM}(f, g) = f_1^{\max(a_1,b_1)} \cdots f_l^{\max(a_l,b_l)} \cdot g_{l+1}^{b_{l+1}} \cdots g_s^{b_s} \cdot f_{l+1}^{a_{l+1}} \cdots f_r^{a_r}. \tag{1}$$

[In the case that f and g share no common factors, we have $\mathrm{LCM}(f, g) = f \cdot g$.] This, in turn, implies the following result.

Proposition 13.
(i) *The intersection $I \cap J$ of two principal ideals $I, J \subset k[x_1, \dots, x_n]$ is a principal ideal.*
(ii) *If $I = \langle f \rangle$, $J = \langle g \rangle$ and $I \cap J = \langle h \rangle$, then*

$$h = \mathrm{LCM}(f, g).$$

Proof. The proof will be left as an exercise. □

This result, together with our algorithm for computing the intersection of two ideals immediately gives an **algorithm for computing the least common multiple** of two polynomials. Namely, to compute the least common multiple of two polynomials $f, g \in k[x_1, \dots, x_n]$, we compute the intersection $\langle f \rangle \cap \langle g \rangle$ using our algorithm for computing the intersection of ideals. Proposition 13 assures us that this intersection is a principal ideal (in the exercises, we ask you to prove that the intersection of principal ideals is principal) and that any generator of it is a least common multiple of f and g.

This algorithm for computing least common multiples allows us to clear up a point which we left unfinished in §2: namely, the computation of the greatest common divisor of two polynomials f and g. The crucial observation is the following.

Proposition 14. *Let $f, g \in k[x_1, \dots, x_n]$. Then*

$$\mathrm{LCM}(f, g) \cdot \mathrm{GCD}(f, g) = fg.$$

Proof. See Exercise 5. You will need to express f and g as a product of distinct irreducibles and use the remarks preceding Proposition 13, especially equation (1). □

It follows immediately from Proposition 14 that

$$\mathrm{GCD}(f, g) = \frac{f \cdot g}{\mathrm{LCM}(f, g)}. \tag{2}$$

This gives an **algorithm for computing the greatest common divisor** of two polynomials f and g. Namely, we compute $\mathrm{LCM}(f, g)$ using our algorithm for the least common multiple and divide it into the product of f and g using the division algorithm.

We should point out that the GCD algorithm just described is rather cumbersome. In practice, more efficient algorithms are used [see DAVENPORT, SIRET, and TOURNIER (1993)].

Having dealt with the computation of intersections, we now ask what operation on varieties corresponds to the operation of intersection on ideals. The following result answers this question.

Theorem 15. *If I and J are ideals in $k[x_1, \dots, x_n]$, then $\mathbf{V}(I \cap J) = \mathbf{V}(I) \cup \mathbf{V}(J)$.*

Proof. Let $x \in \mathbf{V}(I) \cup \mathbf{V}(J)$. Then $x \in \mathbf{V}(I)$ or $x \in \mathbf{V}(J)$. This means that either $f(x) = 0$ for all $f \in I$ or $f(x) = 0$ for all $f \in J$. Thus, certainly, $f(x) = 0$ for all $f \in I \cap J$. Hence, $x \in \mathbf{V}(I \cap J)$. Thus, $\mathbf{V}(I) \cup \mathbf{V}(J) \subset \mathbf{V}(I \cap J)$.

On the other hand, note that since $IJ \subset I \cap J$, we have $\mathbf{V}(I \cap J) \subset \mathbf{V}(IJ)$. But $\mathbf{V}(IJ) = \mathbf{V}(I) \cup \mathbf{V}(J)$ by Theorem 7 and we immediately obtain the reverse inequality. □

Thus, the intersection of two ideals corresponds to the same variety as the product. In view of this and the fact that the intersection is much more difficult to compute than the product, one might legitimately question the wisdom of bothering with the intersection at all. The reason is that intersection behaves much better with respect to the operation of taking radicals: the product of radical ideals need not be a radical ideal (consider IJ where $I = J$), but the intersection of radical ideals is always a radical ideal. The latter fact follows upon applying the following proposition to radical ideals.

Proposition 16. *If I, J are any ideals, then*

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

Proof. If $f \in \sqrt{I \cap J}$, then $f^m \in I \cap J$ for some integer $m > 0$. Since $f^m \in I$, we have $f \in \sqrt{I}$. Similarly, $f \in \sqrt{J}$. Thus, $\sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J}$.

To establish the reverse inclusion, suppose $f \in \sqrt{I} \cap \sqrt{J}$. Then, there exist integers $m, p > 0$ such that $f^m \in I$ and $f^p \in J$. Thus $f^{m+p} = f^m f^p \in I \cap J$, so $f \in \sqrt{I \cap J}$. □

EXERCISES FOR §3

1. Show that in $\mathbb{Q}[x, y]$, we have

$$\begin{aligned}\langle (x+y)^4(x^2+y)^2(x-5y)\rangle \cap \langle (x+y)(x^2+y)^3(x+3y)\rangle \\ = \langle (x+y)^4(x^2+y)^3(x-5y)(x+3y)\rangle.\end{aligned}$$

2. Prove formula (1) for the least common multiple of two polynomials f and g.
3. Prove assertion (i) of Proposition 13. That is, show that the intersection of two principal ideals is principal.
4. Prove assertion (ii) of Proposition 13. That is, show that the least common multiple of two polynomials f and g in $k[x_1, \ldots, x_n]$ is the generator of the ideal $\langle f\rangle \cap \langle g\rangle$.
5. Prove Proposition 14. That is, show that the least common multiple of two polynomials times the greatest common divisor of the same two polynomials is the product of the polynomials. Hint: Use the remarks following the statement of Proposition 14.
6. Let $I_1, \ldots, I_r$ and J be ideals in $k[x_1, \ldots, x_n]$. Show the following:
   a. $(I_1 + I_2)J = I_1 J + I_2 J$.
   b. $(I_1 \cdots I_r)^m = I_1^m \cdots I_r^m$.
7. Let I and J be ideals in $k[x_1, \ldots, x_n]$, where k is an arbitrary field. Prove the following:
   a. If $I^\ell \subset J$ for some integer $\ell > 0$, then $\sqrt{I} \subset \sqrt{J}$.
   b. $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$.
8. Let

$$f = x^4 + x^3y + x^3z^2 - x^2y^2 + x^2yz^2 - xy^3 - xy^2z^2 - y^3z^2$$

   and

$$g = x^4 + 2x^3z^2 - x^2y^2 + x^2z^4 - 2xy^2z^2 - y^2z^4.$$

   a. Use a computer algebra program to compute generators for $\langle f\rangle \cap \langle g\rangle$ and $\sqrt{\langle f\rangle\langle g\rangle}$.
   b. Use a computer algebra program to compute GCD(f, g).
   c. Let $p = x^2 + xy + xz + yz$ and $q = x^2 - xy - xz + yz$. Use a computer algebra program to calculate $\langle f, g\rangle \cap \langle p, q\rangle$.
9. For an arbitrary field, show that $\sqrt{IJ} = \sqrt{I \cap J}$. Give an example to show that the product of radical ideals need not be radical. Give an example to show that $\sqrt{IJ}$ can differ from $\sqrt{I}\sqrt{J}$.

10. If I is an ideal in $k[x_1, \ldots, x_n]$ and $\langle f(t)\rangle$ is an ideal in $k[t]$, show that the ideal $f(t)I$ defined in the text is the product of the ideal $\tilde{I}$ generated by all elements of I in $k[x_1, \ldots, x_n, t]$ and the ideal $\langle f(t)\rangle$ generated by $f(t)$ in $k[x_1, \ldots, x_n, t]$.
11. Two ideals I and J of $k[x_1, \ldots, x_n]$ are said to be *comaximal* if and only if $I + J = k[x_1, \ldots, x_n]$.
    a. Show that if $k = \mathbb{C}$, then I and J are comaximal if and only if $\mathbf{V}(I) \cap \mathbf{V}(J) = \emptyset$. Give an example to show that this is false in general.
    b. Show that if I and J are comaximal, then $IJ = I \cap J$.
    c. Is the converse to part (b) true? That is, if $IJ = I \cap J$, does it necessarily follow that I and J are comaximal? Proof or counterexample?
    d. If I and J are comaximal, show that I and J^2 are comaximal. In fact, show that I^r and J^s are comaximal for all positive integers r and s.
    e. Let $I_1, \ldots, I_r$ be ideals in $k[x_1, \ldots, x_n]$ and suppose that I_i, and $J_i = \cap_{j\neq i} I_j$ are comaximal for all i. Show that
$$I_1^m \cap \cdots \cap I_r^m = (I_1 \cdots I_r)^m = (I_1 \cap \cdots \cap I_r)^m$$
    for all positive integers m.
12. Let I, J be ideals in $k[x_1, \ldots, x_n]$ and suppose that $I \subset \sqrt{J}$. Show that $I^m \subset J$ for some integer $m > 0$. Hint: You will need to use the Hilbert Basis Theorem.
13. Let A be an $m \times n$ constant matrix and suppose that $x = Ay$, where we are thinking of $x \in k^m$ and $y \in K^n$ as column vectors. As in Exercise 9 of §1, define a map
$$\alpha_A : k[x_1, \ldots, x_m] \to k[y_1, \ldots, y_n]$$
    by sending $f \in k[x_1, \ldots, x_m]$ to $\alpha_A(f) \in k[y_1, \ldots, y_n]$, where $\alpha_A(f)$ is the polynomial defined by $\alpha_A(f)(y) = f(Ay)$.
    a. Show that the set $\{f \in k[x_1, \ldots, x_m] : \alpha_A(f) = 0\}$ is an ideal in $k[x_1, \ldots, x_m]$. [This set is called the *kernel* of α_A and denoted $\ker(\alpha_A)$.]
    b. If I is an ideal $k[x_1, \ldots, x_n]$, show that the set $\alpha_A(I) = \{\alpha_A(f) : f \in I\}$ need not be an ideal in $k[y_1, \ldots, y_n]$. [We will often write $\langle\alpha_A(I)\rangle$ to denote the ideal in $k[y_1, \ldots, y_n]$ generated by the elements of $\alpha_A(I)$—it is called the *extension* of I to $k[y_1, \ldots, y_n]$.]
    c. Show that if I' is an ideal in $k[y_1, \ldots, y_n]$, the set $\alpha_A^{-1}(I') = \{f \in k[x_1, \ldots, x_m] : \alpha_A(f) \in I'\}$ is an ideal in $k[x_1, \ldots, x_m]$ (often called the *contraction* of I').
14. Let A and α_A be as above and let $K = \ker(\alpha_A)$. Let I and J be ideals in $k[x_1, \ldots, x_m]$. Show that:
    a. $I \subset J$ implies $\langle\alpha_A(I)\rangle \subset \langle\alpha_A(J)\rangle$.
    b. $\langle\alpha_A(I + J)\rangle = \langle\alpha_A(I)\rangle + \langle\alpha_A(J)\rangle$.
    c. $\langle\alpha_A(IJ)\rangle = \langle\alpha_A(I)\rangle\langle\alpha_A(J)\rangle$.
    d. $\langle\alpha_A(I \cap J)\rangle \subset \langle\alpha_A(I)\rangle \cap \langle\alpha_A(J)\rangle$ with equality if $I \supset K$ or $J \supset K$ and α_A is onto.
    e. $\langle\alpha_A(\sqrt{I})\rangle \subset \sqrt{\langle\alpha_A(I)\rangle}$ with equality if $I \supset K$ and α_A is onto.
15. Let A, α_A, and $K = \ker(\alpha_A)$ be as above. Let I' and J' be ideals in $k[y_1, \ldots, y_n]$. Show that:
    a. $I' \subset J'$ implies $\alpha_A^{-1}(I') \subset \alpha_A^{-1}(J')$.
    b. $\alpha_A^{-1}(I' + J') = \alpha_A^{-1}(I') + \alpha_A^{-1}(J')$.
    c. $\alpha_A^{-1}(I'J') \supset (\alpha_A^{-1}(I'))(\alpha_A^{-1}(J'))$, with equality if the right-hand side contains K.
    d. $\alpha_A^{-1}(I' \cap J') = \alpha_A^{-1}(I') \cap \alpha_A^{-1}(J')$.
    e. $\alpha_A^{-1}(\sqrt{I'}) = \sqrt{\alpha_A^{-1}(I')}$.

§4 Zariski Closure and Quotients of Ideals

We have already seen a number of examples of sets which are not varieties. Such sets arose very naturally in Chapter 3, where we saw that the projection of a variety need not be a variety, and in the exercises in Chapter 1, where we saw that the (set-theoretic) difference of varieties can fail to be a variety.

Whether or not a set $S \subset k^n$ is an affine variety, the set

$$\mathbf{I}(S) = \{f \in k[x_1, \dots, x_n] : f(a) = 0 \text{ for all } a \in S\}$$

is an ideal in $k[x_1, \dots, x_n]$ (check this!). In fact, it is radical. By the ideal–variety correspondence, $\mathbf{V}(\mathbf{I}(S))$ is a variety. The following proposition states that this variety is the smallest variety that contains the set S.

Proposition 1. *If $S \subset k^n$, the affine variety $\mathbf{V}(\mathbf{I}(S))$ is the smallest variety that contains S [in the sense that if $W \subset k^n$ is any affine variety containing S, then $\mathbf{V}(\mathbf{I}(S)) \subset W$].*

Proof. If $W \supset S$, then $\mathbf{I}(W) \subset \mathbf{I}(S)$ (because $\mathbf{I}$ is inclusion-reversing). But then $\mathbf{V}(\mathbf{I}(W)) \supset \mathbf{V}(\mathbf{I}(S))$ (because $\mathbf{V}$ is inclusion-reversing). Since W is an affine variety, $\mathbf{V}(\mathbf{I}(W)) = W$ by Theorem 7 from §2, and the result follows. □

This proposition leads to the following definition.

Definition 2. *The* **Zariski closure** *of a subset of affine space is the smallest affine algebraic variety containing the set. If $S \subset k^n$, the Zariski closure of S is denoted $\overline{S}$ and is equal to $\mathbf{V}(\mathbf{I}(S))$.*

We also note that $I(\overline{S}) = I(S)$. The inclusion $I(\overline{S}) \subset I(S)$ follows from $S \subset \overline{S}$. Going the other way, $f \in I(S)$ implies $S \subset \mathbf{V}(f)$. Then $S \subset \overline{S} \subset \mathbf{V}(f)$ by Definition 2, so that $f \in I(\overline{S})$.

A natural example of Zariski closure is given by elimination ideals. We can now prove the first assertion of the Closure Theorem (Theorem 3 of Chapter 3, §2).

Theorem 3. *Let k be an algebraically closed field. Suppose $V = \mathbf{V}(f_1, \dots, f_s) \subset k^n$, and let $\pi_l : k^n \longrightarrow k^{n-l}$ be projection onto the last $n - l$ components. If I_l is the lth elimination ideal $I_l = \langle f_1, \dots, f_s\rangle \cap k[x_{l+1}, \dots, x_n]$, then $\mathbf{V}(I_l)$ is the Zariski closure of $\pi_l(V)$.*

Proof. In view of Proposition 1, we must show that $\mathbf{V}(I_l) = \mathbf{V}(\mathbf{I}(\pi_l(V)))$. By Lemma 1 of Chapter 3, §2, we have $\pi_l(V) \subset \mathbf{V}(I_l)$. Since $\mathbf{V}(\mathbf{I}(\pi_l(V)))$ is the smallest variety containing $\pi_l(V)$, it follows immediately that $\mathbf{V}(\mathbf{I}(\pi_l(V))) \subset \mathbf{V}(I_l)$.

To get the opposite inclusion, suppose $f \in \mathbf{I}(\pi_l(V))$, i.e., $f(a_{l+1}, \dots, a_n) = 0$ for all $(a_{l+1}, \dots, a_n) \in \pi_l(V)$. Then, considered as an element of $k[x_1, x_2, \dots, x_n]$, we certainly have $f(a_1, a_2, \dots, a_n) = 0$ for all $(a_1, \dots, a_n) \in V$. By Hilbert's Nullstellensatz, $f^N \in \langle f_1, \dots, f_s\rangle$ for some integer N. Since f does not depend on $x_1, \dots, x_l$, neither does f^N, and we have $f^N \in \langle f_1, \ldots, f_s \rangle \cap k[x_{l+1}, \ldots, x_n] = I_l$. Thus, $f \in \sqrt{I_l}$, which implies $\mathbf{I}(\pi_l(V)) \subset \sqrt{I_l}$. It follows that $\mathbf{V}(I_l) = \mathbf{V}(\sqrt{I_l}) \subset \mathbf{V}(\mathbf{I}(\pi_l(V)))$, and the theorem is proved. □

Another context in which we encountered sets which were not varieties was in taking the difference of varieties. For example, let $W = \mathbf{V}(K)$ where $K \subset k[x, y, z]$ is the ideal $\langle xz, yz \rangle$ and $V = \mathbf{V}(I)$ where $I = \langle z \rangle$. Then we have already seen that W is the union of the xy-plane and the z-axis. Since V is the xy-plane, $W - V$ is the z-axis with the origin removed (because the origin also belongs to the xy-plane). We have seen in Chapter 1 that this is not a variety. The z-axis [$= \mathbf{V}(x, y)$] is the smallest variety containing $W - V$.

We could ask if there is a general way to compute the ideal corresponding to the Zariski closure $\overline{W - V}$ of the difference of two varieties W and V. The answer is affirmative, but it involves a new algebraic construction on ideals.

To see what the construction involves let us first note the following.

Proposition 4. *If V and W are varieties with $V \subset W$, then $W = V \cup (\overline{W - V})$.*

Proof. Since W contains $W - V$ and W is a variety, it must be the case that the smallest variety containing $W - V$ is contained in W. Hence, $\overline{W - V} \subset W$. Since $V \subset W$ by hypothesis, we must have $V \cup (\overline{W - V}) \subset W$.

To get the reverse containment, note that $V \subset W$ implies $W = V \cup (W - V)$. Since $W - V \subset \overline{W - V}$, the desired inclusion $W \subset V \cup \overline{W - V}$ follows immediately. □

Our next task is to study the ideal-theoretic analogue of $\overline{W - V}$. We start with the following definition.

Definition 5. *If I, J are ideals in $k[x_1, \ldots, x_n]$, then $I : J$ is the set*

$$\{f \in k[x_1, \ldots, x_n] : fg \in I \text{ for all } g \in J\}$$

and is called the **ideal quotient** *(or* **colon ideal***) of I by J.*

So, for example, in $k[x, y, z]$ we have

$$\begin{aligned}
\langle xz, yz \rangle : \langle z \rangle &= \{f \in k[x, y, z] : f \cdot z \in \langle xz, yz \rangle\} \\
&= \{f \in k[x, y, z] : f \cdot z = Axz + Byz\} \\
&= \{f \in k[x, y, z] : f = Ax + By\} \\
&= \langle x, y \rangle.
\end{aligned}$$

Proposition 6. *If I, J are ideals in $k[x_1, \ldots, x_n]$, then $I : J$ is an ideal in $k[x_1, \ldots, x_n]$ and $I : J$ contains I.*

Proof. To show $I : J$ contains I, note that because I is an ideal, if $f \in I$, then $fg \in I$ for all $g \in k[x_1, \ldots, x_n]$ and, hence, certainly $fg \in I$ for all $g \in J$. To show that $I : J$ is an ideal, first note that $0 \in I : J$ because $0 \in I$. Let $f_1, f_2 \in I : J$. Then $f_1 g$ and $f_2 g$ are in I for all $g \in J$. Since I is an ideal $(f_1 + f_2)g = f_1 g + f_2 g \in I$ for all $g \in J$. Thus, $f_1 + f_2 \in I : J$. To check closure under multiplication is equally straightforward: if $f \in I : J$ and $h \in k[x_1, \ldots, x_n]$, then $fg \in I$ and, since I is an ideal, $hfg \in I$ for all $g \in J$, which means that $hf \in I : J$. □

The following theorem shows that the ideal quotient is indeed the algebraic analogue of the Zariski closure of a difference of varieties.

Theorem 7. *Let I and J be ideals in* $k[x_1, \ldots, x_n]$. *Then*

$$\mathbf{V}(I : J) \supset \overline{\mathbf{V}(I) - \mathbf{V}(J)}.$$

If, in addition, k is algebraically closed and I is a radical ideal, then

$$\mathbf{V}(I : J) = \overline{\mathbf{V}(I) - \mathbf{V}(J)}.$$

Proof. We claim that $I : J \subset \mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))$. For suppose that $f \in I : J$ and $x \in \mathbf{V}(I) - \mathbf{V}(J)$. Then $fg \in I$ for all $g \in J$. Since $x \in \mathbf{V}(I)$, we have $f(x)g(x) = 0$ for all $g \in J$. Since $x \notin \mathbf{V}(J)$, there is some $g \in J$ such that $g(x) \neq 0$. Hence, $f(x) = 0$ for any $x \in \mathbf{V}(I) - \mathbf{V}(J)$. Hence, $f \in \mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))$ which proves the claim. Since $\mathbf{V}$ is inclusion-reversing, we have $\mathbf{V}(I : J) \supset \mathbf{V}(\mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J)))$. This proves the first part of the theorem.

Now, suppose that k is algebraically closed and that $I = \sqrt{I}$. Let $x \in \mathbf{V}(I : J)$. Equivalently,

$$\text{(1)} \qquad \text{if } hg \in I \text{ for all } g \in J, \text{ then } h(x) = 0.$$

Now let $h \in \mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))$. If $g \in J$, then hg vanishes on $\mathbf{V}(I)$ because h vanishes on $\mathbf{V}(I) - \mathbf{V}(J)$ and g on $\mathbf{V}(J)$. Thus, by the Nullstellensatz, $hg \in \sqrt{I}$. By assumption, $I = \sqrt{I}$, and hence, $hg \in I$ for all $g \in J$. By (1), we have $h(x) = 0$. Thus, $x \in \mathbf{V}(\mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J)))$. This establishes that

$$\mathbf{V}(I : J) \subset \mathbf{V}(\mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))),$$

and completes the proof. □

The proof of Theorem 7 yields the following corollary that holds over any field.

Corollary 8. *Let V and W be varieties in* k^n. *Then*

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

Proof. In Theorem 7, we showed that $I : J \subset \mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))$. If we apply this to $I = \mathbf{I}(V)$ and $J = \mathbf{I}(W)$, we obtain $\mathbf{I}(V) : \mathbf{I}(W) \subset \mathbf{I}(V - W)$. The opposite inclusion follows from the definition of ideal quotient. □

The following proposition takes care of some of the more obvious properties of ideal quotients. The reader is urged to translate the statements into terms of varieties (upon which they become completely obvious).

Proposition 9. *Let I, J, and K be ideals in $k[x_1, \ldots, x_n]$. Then:*
(i) $I : k[x_1, \ldots, x_n] = I$.
(ii) $IJ \subset K$ *if and only if* $I \subset K : J$.
(iii) $J \subset I$ *if and only if* $I : J = k[x_1, \ldots, x_n]$.

Proof. The proof is left as an exercise. □

The following useful proposition relates the quotient operation to the other operations we have defined:

Proposition 10. *Let I, I_i, J, J_i, and K be ideals in $k[x_1, \ldots, x_n]$ for $1 \leq i \leq r$. Then*

$$\left(\bigcap_{i=1}^{r} I_i\right) : J = \bigcap_{i=1}^{r} (I_i : J), \tag{2}$$

$$I : \left(\sum_{i=1}^{r} J_i\right) = \bigcap_{i=1}^{r} (I : J_i), \tag{3}$$

$$(I : J) : K = I : JK. \tag{4}$$

Proof. We again leave the (straightforward) proofs to the reader. □

If f is a polynomial and I an ideal, we often write $I : f$ instead of $I : \langle f \rangle$. Note that a special case of (3) is that

$$I : \langle f_1, f_2, \ldots, f_r \rangle = \bigcap_{i=1}^{r} (I : f_i). \tag{5}$$

We now turn to the question of how to compute generators of the ideal quotient $I : J$ given generators of I and J. The following observation is the key step.

Theorem 11. *Let I be an ideal and g an element of $k[x_1, \ldots, x_n]$. If $\{h_1, \ldots, h_p\}$ is a basis of the ideal $I \cap \langle g \rangle$, then $\{h_1/g, \ldots, h_p/g\}$ is a basis of $I : \langle g \rangle$.*

Proof. If $a \in \langle g \rangle$, then $a = bg$ for some polynomial b. Thus, if $f \in \langle h_1/g, \ldots, h_p/g \rangle$, then

$$af = bgf \in \langle h_1, \ldots, h_p \rangle = I \cap \langle g \rangle \subset I.$$

Thus, $f \in I : \langle g \rangle$. Conversely, suppose $f \in I : \langle g \rangle$. Then $fg \in I$. Since $fg \in \langle g \rangle$, we have $fg \in I \cap \langle g \rangle$. If $I \cap \langle g \rangle = \langle h_1, \ldots, h_p \rangle$, this means $fg = \sum r_i h_i$ for some polynomials r_i. Since each $h_i \in \langle g \rangle$, each h_i/g is a polynomial, and we conclude that $f = \sum r_i(h_i/g)$, whence $f \in \langle h_1/g, \ldots, h_p/g \rangle$. □

This theorem, together with our procedure for computing intersections of ideals and equation (5), immediately leads to an **algorithm for computing a basis of an ideal quotient.** Namely, given $I = \langle f_1, \ldots, f_r \rangle$ and $J = \langle g_1, \ldots, g_s \rangle = \langle g_1 \rangle + \cdots + \langle g_s \rangle$, to compute a basis of $I : J$, we first compute a basis for $I : \langle g_i \rangle$ for each i. In view of Theorem 11, we first compute a basis of $\langle f_1, \ldots, f_r \rangle \cap \langle g_i \rangle$. Recall that we do this by finding a Groebner basis of $\langle tf_1, \ldots, tf_r, (1-t)g_i \rangle$ with respect to a lex order in which t precedes all the x_i and retaining all basis elements which do not depend on t (this is our algorithm for computing ideal intersections). Using the division algorithm, 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 the intersection algorithm $s - 1$ times, computing first a basis for $I : \langle g_1, g_2 \rangle = (I : \langle g_1 \rangle) \cap (I : \langle g_2 \rangle)$, then a basis for $I : \langle g_1, g_2, g_3 \rangle = (I : \langle g_1, g_2 \rangle) \cap (I : \langle g_3 \rangle)$, and so on.

EXERCISES FOR §4

1. Find the Zariski closure of the following sets:
   a. The projection of the hyperbola $\mathbf{V}(xy - 1)$ in $\mathbb{R}^2$ onto the x-axis.
   b. The boundary of the first quadrant in $\mathbb{R}^2$.
   c. The set $\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 4\}$.
2. Let $f = (x + y)^2(x - y)(x + z^2)$ and $g = (x + z^2)^3(x - y)(z + y)$. Compute generators for $\langle f \rangle : \langle g \rangle$.
3. Let I and J be ideals. Show that if I is radical ideal, then $I : J$ is radical and $I : J = I : \sqrt{J}$.
4. Give an example to show that the hypothesis that I is radical is necessary for the conclusion of Theorem 7 to hold. Hint: Examine the proof to see where we used this hypothesis.
5. Prove Proposition 9 and find geometric interpretations of each of its assertions.
6. Prove Proposition 10 and find geometric interpretations of each of its assertions.
7. Let A be an $m \times n$ constant matrix and suppose that $x = Ay$ where we are thinking of $x \in k^m$ and $y \in k^n$ as column vectors. As in Exercises 9 of §1 and 13 of §3, define a map

$$\alpha_A : k[x_1, \ldots, x_m] \longrightarrow k[y_1, \ldots, y_n]$$

   by sending $f \in k[x_1, \ldots, x_m]$ to $\alpha_A(f) \in k[y_1, \ldots, y_n]$, where $\alpha_A(f)$ is the polynomial defined by $\alpha_A(f)(y) = f(Ay)$.
   a. Show that $\alpha_A(I : J) \subset \alpha_A(I) : \alpha_A(J)$ with equality if $I \supset K$ where $K = \ker(\alpha_A)$.
   b. Show that $\alpha_A^{-1}(I' : J') = \alpha_A^{-1}(I') : \alpha_A^{-1}(J')$ when α_A is onto.
8. Let $I \subset k[x_1, \ldots, x_n]$ be an ideal, and fix $f \in k[x_1, \ldots, x_n]$. Then the *saturation* of I with respect to f is the set

$$I : f^\infty = \{g \in k[x_1, \ldots, x_n] : f^m g \in I \text{ for some } m > 0\}.$$

   a. Prove that $I : f^\infty$ is an ideal.
   b. Prove that we have the ascending chain of ideals $I : f \subset I : f^2 \subset I : f^3 \subset \cdots$.
   c. By part b and the Ascending Chain Condition (Theorem 7 of Chapter 2, §5), we have $I : f^N = I : f^{N+1} = \cdots$ for some integer N. Prove that $I : f^\infty = I : f^N$.

d. Prove that $I : f^\infty = I : f^m$ if and only if $I : f^m = I : f^{m+1}$.
e. Use part d to describe an algorithm for computing the saturation $I : f^\infty$.

9. As in Exercise 8, let $I = \langle f_1, \dots, f_s \rangle \subset k[x_1, \dots, x_n]$ and fix $f \in k[x_1, \dots, x_n]$. If y is a new variable, set

$$\tilde{I} = \langle f_1, \dots, f_s, 1 - fy \rangle \subset k[x_1, \dots, x_n, y].$$

a. Prove that $I : f^\infty = \tilde{I} \cap k[x_1, \dots, x_n]$. Hint: See the proof of Proposition 8 of §2.
b. Use the result of part a to describe a second algorithm for computing $I : f^\infty$.

10. Using the notation of Exercise 8, prove that $I : f^\infty = k[x_1, \dots, x_n]$ if and only if $f \in \sqrt{I}$. Note that Proposition 8 of §2 is an immediate corollary of Exercises 9 and 10.

§5 Irreducible Varieties and Prime Ideals

We have already seen that the union of two varieties is a variety. For example, in Chapter 1 and in the last section, we considered $\mathbf{V}(xz, yz)$, which is the union of a line and a plane. Intuitively, it is natural to think of the line and the plane as "more fundamental" than $\mathbf{V}(xz, yz)$. Intuition also tells us that a line or a plane are "irreducible" or "indecomposable" in some sense: they do not obviously seem to be a union of finitely many simpler varieties. We formalize this notion as follows.

Definition 1. *An affine variety $V \subset k^n$ is* **irreducible** *if whenever V is written in the form $V = V_1 \cup V_2$, where V_1 and V_2 are affine varieties, then either $V_1 = V$ or $V_2 = V$.*

Thus, $\mathbf{V}(xz, yz)$ is not an irreducible variety. On the other hand, it is not completely clear when a variety is irreducible. If this definition is to correspond to our geometric intuition, it is clear that a point, a line, and a plane ought to be irreducible. For that matter, the twisted cubic $\mathbf{V}(y - x^2, z - x^3)$ in $\mathbb{R}^3$ appears to be irreducible. But how do we prove this? The key is to capture this notion algebraically: if we can characterize ideals which correspond to irreducible varieties, then perhaps we stand a chance of establishing whether a variety is irreducible

The following notion turns out to be the right one.

Definition 2. *An ideal $I \subset k[x_1, \dots, x_n]$ is* **prime** *if whenever $f, g \in k[x_1, \dots, x_n]$ and $fg \in I$, then either $f \in I$ or $g \in I$.*

If we have set things up right, an irreducible variety will correspond to a prime ideal and conversely. The following theorem assures us that this is indeed the case.

Proposition 3. *Let $V \subset k^n$ be an affine variety. Then V is irreducible if and only if $\mathbf{I}(V)$ is a prime ideal.*

Proof. First, assume that V is irreducible and let $fg \in \mathbf{I}(V)$. Set $V_1 = V \cap \mathbf{V}(f)$ and $V_2 = V \cap \mathbf{V}(g)$; these are affine varieties because an intersection of affine varieties is a variety. Then $fg \in \mathbf{I}(V)$ easily implies that $V = V_1 \cup V_2$. Since V is irreducible, we have either $V = V_1$ or $V = V_2$. Say the former holds, so that $V = V_1 = V \cap \mathbf{V}(f)$. This implies that f vanishes on V, so that $f \in \mathbf{I}(V)$. Thus, $\mathbf{I}(V)$ is prime.

Next, assume that $\mathbf{I}(V)$ is prime and let $V = V_1 \cup V_2$. Suppose that $V \neq V_1$. We claim that $\mathbf{I}(V) = \mathbf{I}(V_2)$. To prove this, note that $\mathbf{I}(V) \subset \mathbf{I}(V_2)$ since $V_2 \subset V$. For the opposite inclusion, first note that $\mathbf{I}(V) \subsetneqq \mathbf{I}(V_1)$ since $V_1 \subsetneqq V$. Thus, we can pick $f \in \mathbf{I}(V_1) - \mathbf{I}(V)$. Now take any $g \in \mathbf{I}(V_2)$. Since $V = V_1 \cup V_2$, it follows that fg vanishes on V, and, hence, $fg \in \mathbf{I}(V)$. But $\mathbf{I}(V)$ is prime, so that f or g lies in $\mathbf{I}(V)$. We know that $f \notin \mathbf{I}(V)$ and, thus, $g \in \mathbf{I}(V)$. This proves $\mathbf{I}(V) = \mathbf{I}(V_2)$, whence $V = V_2$ because $\mathbf{I}$ is one-to-one. Thus, V is an irreducible variety. □

It is an easy exercise to show that every prime ideal is radical. Then, using the ideal–variety correspondence between radical ideals and varieties, we get the following corollary of Proposition 3.

Corollary 4. *When k is algebraically closed, the functions $\mathbf{I}$ and $\mathbf{V}$ induce a one-to-one correspondence between irreducible varieties in k^n and prime ideals in $k[x_1, \ldots, x_n]$.*

As an example of how to use Proposition 3, let us prove that the ideal $\mathbf{I}(V)$ of the twisted cubic is prime. Suppose that $fg \in \mathbf{I}(V)$. Since the curve is parametrized by (t, t^2, t^3), it follows that, for all t,

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

This implies that $f(t, t^2, t^3)$ or $g(t, t^2, t^3)$ must be the zero polynomial, so that f or g vanishes on V. Hence, f or g lies in $\mathbf{I}(V)$, proving that $\mathbf{I}(V)$ is a prime ideal. By the proposition, the twisted cubic is an irreducible variety in $\mathbb{R}^3$. One proves that a straight line is irreducible in the same way: first parametrize it, then apply the above argument.

In fact, the above argument holds much more generally.

Proposition 5. *If k is an infinite field and $V \subset k^n$ is a variety defined parametrically*

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

where $f_1, \ldots, f_n$ are polynomials in $k[t_1, \ldots, t_m]$, then V is irreducible.

Proof. As in §3 of Chapter 3, we let $F : k^m \longrightarrow k^n$ be defined by

$$F(t_1, \ldots, t_m) = (f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m)).$$

Saying that V is defined parametrically by the above equations means that V is the Zariski closure of $F(k^m)$. In particular, $\mathbf{I}(V) = \mathbf{I}(F(k^m))$.

For any polynomial $g \in k[x_1, \ldots, x_n]$, the function $g \circ F$ is a polynomial in $k[t_1, \ldots, t_m]$. In fact, $g \circ F$ is the polynomial obtained by "plugging the polynomials $f_1, \ldots, f_n$ into g":

$$g \circ F = g(f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m)).$$

Because k is infinite, $\mathbf{I}(V) = \mathbf{I}(F(k^m))$ is the set of polynomials in $k[x_1, \ldots, x_n]$ whose composition with F is the zero polynomial in $k[t_1, \ldots, t_m]$:

$$\mathbf{I}(V) = \{g \in k[x_1, \ldots, x_n] : g \circ F = 0\}.$$

Now suppose that $gh \in \mathbf{I}(V)$. Then $(gh) \circ F = (g \circ F)(h \circ F) = 0$. (Make sure you understand this.) But, if the product of two polynomials in $k[t_1, \ldots, t_m]$ is the zero polynomial, one of them must be the zero polynomial. Hence, either $g \circ F = 0$ or $h \circ F = 0$. This means that either $g \in \mathbf{I}(V)$ or $h \in \mathbf{I}(V)$. This shows that $\mathbf{I}(V)$ is a prime ideal and, therefore, that V is irreducible. □

With a little care, the above argument extends still further to show that any variety defined by a *rational* parametrization is irreducible.

Proposition 6. *If k is an infinite field and V is a variety defined by the rational parametrization*

$$\begin{aligned} x_1 &= \frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \\ &\vdots \\ x_n &= \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)}, \end{aligned}$$

where $f_1, \ldots, f_n, g_1, \ldots, g_n \in k[t_1, \ldots, t_m]$, then V is irreducible.

Proof. Set $W = \mathbf{V}(g_1 g_2 \cdots g_n)$ and let $F : k^m - W \to k^n$ defined by

$$F(t_1, \ldots, t_m) = \left(\frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \ldots, \frac{f_n(t_n, \ldots, t_m)}{g_n(t_1, \ldots, t_m)} \right).$$

Then V is the Zariski closure of $F(k^m - W)$, which implies that $\mathbf{I}(V)$ is the set of $h \in k[x_1, \ldots, x_n]$ such that the function $h \circ F$ is zero for all $(t_1, \ldots, t_m) \in k^m - W$. The difficulty is that $h \circ F$ need not be a polynomial, and we, thus, cannot directly apply the argument in the latter part of the proof of Proposition 5.

We can get around this difficulty as follows. Let $h \in k[x_1, \ldots, x_n]$. Since

$$g_1(t_1, \ldots, t_m) g_2(t_1, \ldots, t_m) \cdots g_n(t_1, \ldots, t_m) \neq 0$$

for any $(t_1, \ldots, t_m) \in k^m - W$, the function $(g_1 g_2 \cdots g_n)^N (h \circ F)$ is equal to zero at precisely those values of $(t_1, \ldots, t_m) \in k^m - W$ for which $h \circ F$ is equal to zero. Moreover, if we let N be the total degree of $h \in k[x_1, \ldots, x_n]$, then we leave it as an exercise to show that $(g_1 g_2 \cdots g_n)^N (h \circ F)$ is a polynomial in $k[t_1, \ldots, t_m]$. We deduce that $h \in \mathbf{I}(V)$ if and only if $(g_1 g_2 \cdots g_n)^N (h \circ F)$ is zero for all $t \in k^m - W$. But, by Exercise 11 of Chapter 3, §3, this happens if and only if $(g_1 g_2 \cdots g_n)^N (h \circ F)$ is the zero polynomial in $k[t_1, \ldots, t_m]$. Thus, we have shown that

$$h \in \mathbf{I}(V) \quad \text{if and only if} \quad (g_1 g_2 \cdots g_n)^N (h \circ F) = 0 \in k[t_1, \ldots, t_m].$$

Now, we can continue with our proof that $\mathbf{I}(V)$ is prime. Suppose $p, q \in k[x_1, \ldots, x_n]$ are such that $p \cdot q \in \mathbf{I}(V)$. If the total degrees of p and q are M and N, respectively, then the total degree of $p \cdot q$ is $M + N$. Thus, $(g_1 g_2 \cdots g_n)^{M+N} (p \circ F) \cdot (p \circ F) = 0$. But the former is a product of the polynomials $(g_1 g_2 \cdots g_n)^M (p \circ F)$ and $(g_1 g_2 \cdots g_n)^N (q \circ F)$ in $k[t_1, \ldots, t_m]$. Hence one of them must be the zero polynomial. In particular, either $p \in \mathbf{I}(V)$ or $q \in \mathbf{I}(V)$. This shows that $\mathbf{I}(V)$ is a prime ideal and, therefore, that V is an irreducible variety. □

The simplest variety in k^n given by a parametrization is a single point $\{(a_1, \ldots, a_n)\}$. In the notation of Proposition 5, it is given by the parametrization in which each f_i is the constant polynomial $f_i(t_1, \ldots, t_m) = a_i$, $1 \leq i \leq n$. It is clearly irreducible and it is easy to check that $\mathbf{I}(\{(a_1, \ldots, a_n)\}) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ (see Exercise 7), which implies that the latter is prime. The ideal $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ has another distinctive property: it is maximal in the sense that the only ideal which strictly contains it is the whole ring $k[x_1, \ldots, x_n]$. Such ideals are important enough to merit special attention.

Definition 7. *An ideal $I \subset k[x_1, \ldots, x_n]$ is said to be* **maximal** *if $I \neq k[x_1, \ldots, x_n]$ and any ideal J containing I is such that either $J = I$ or $J = k[x_1, \ldots, x_n]$.*

In order to streamline statements, we make the following definition.

Definition 8. *An ideal $I \subset k[x_1, \ldots, x_n]$ is called* **proper** *if I is not equal to $k[x_1, \ldots, x_n]$.*

Thus, an ideal is maximal if it is proper and no other proper ideal strictly contains it. We now show that any ideal of the form $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ is maximal.

Proposition 9. *If k is any field, an ideal $I \subset k[x_1, \ldots, x_n]$ of the form*

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

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

Proof. Suppose that J is some ideal strictly containing I. Then there must exist $f \in J$ such that $f \notin I$. We can use the division algorithm to write f as $A_1(x_1 - a_1) + \cdots + A_n(x_n - a_n) + b$ for some $b \in k$. Since $A_1(x_1 - a_1) + \cdots + A_n(x_n - a_n) \in I$ and

$f \notin I$, we must have $b \neq 0$. However, since $f \in J$ and since $A_1(x_1 - a_1) + \cdots + A_n(x_n - a_n) \in I \subset J$, we also have

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

Since b is nonzero, $1 = 1/b \cdot b \in J$, So $J = k[x_1, \ldots, x_n]$. $\square$

Since

$$\mathbf{V}(x_1 - a_1, \ldots, x_n - a_n) = \{(a_1, \ldots, a_n)\},$$

every point $(a_1, \ldots, a_n) \in k^n$ corresponds to a maximal ideal of $k[x_1, \ldots, x_n]$, namely $\langle x_1 - a_1, \ldots, x_n - a_n\rangle$. The converse does not hold if k is not algebraically closed. In the exercises, we ask you to show that $\langle x^2 + 1\rangle$ is maximal in $\mathbb{R}[x]$. The latter does not correspond to a point of $\mathbb{R}$. The following result, however, holds in any polynomial ring.

Proposition 10. *If k is any field, a maximal ideal in $k[x_1, \ldots, x_n]$ is prime.*

Proof. Suppose that I is a proper ideal which is not prime and let $fg \in I$, where $f \notin I$ and $g \notin I$. Consider the ideal $\langle f\rangle + I$. This ideal strictly contains I because $f \notin I$. Moreover, if we were to have $\langle f\rangle + I = k[x_1, \ldots, x_n]$, then $1 = cf + h$ for some polynomial c and some $h \in I$. Multiplying through by g would give $g = cfg + hg \in I$ which would contradict our choice of g. Thus, $I + \langle f\rangle$ is a proper ideal containing I, so that I is not maximal. $\square$

Note that Propositions 9 and 10 together imply that $\langle x_1 - a_1, \ldots, x_n - a_n\rangle$ is prime in $k[x_1, \ldots, x_n]$ even if k is not infinite. Over an algebraically closed field, it turns out that every maximal ideal corresponds to some point of k_n.

Theorem 11. *If k is an algebraically closed field, then every maximal ideal of $k[x_1, \ldots, x_n]$ is of the form $\langle x_1 - a_1, \ldots, x_n - a_n\rangle$ for some $a_1, \ldots, a_n \in k$.*

Proof. Let $I \subset k[x_1, \ldots, x_n]$ be maximal. Since $I \neq k[x_1, \ldots, x_n]$, we have $\mathbf{V}(I) \neq \emptyset$ by the Weak Nullstellensatz (Theorem 1 of §1). Hence, there is some point $(a_1, \ldots, a_n) \in \mathbf{V}(I)$. This means that every $f \in I$ vanishes at $(a_1, \ldots, a_n)$, so that $f \in \mathbf{I}(\{(a_1, \ldots, a_n)\})$. Thus, we can write

$$I \subset \mathbf{I}(\{(a_1, \ldots, a_n)\}).$$

We have already observed that $\mathbf{I}(\{(a_1, \ldots, a_n)\}) = \langle x_1 - a_1, \ldots, x_n - a_n\rangle$ (see Exercise 7), and, thus, the above inclusion becomes

$$I \subset \langle x_1 - a_1, \ldots, x_n - a_n\rangle \subsetneq k[x_1, \ldots, x_n].$$

Since I is maximal, it follows that $I = \langle x_1 - a_1, \ldots, x_n - a_n\rangle$. $\square$

Note the proof of Theorem 11 uses the Weak Nullstellensatz. It is not difficult to see that it is, in fact, equivalent to the Weak Nullstellensatz.

We have the following easy corollary of Theorem 11.

Corollary 12. *If k is an algebraically closed field, then there is a one-to-one correspondence between points of k^n and maximal ideals of $k[x_1, \ldots, x_n]$.*

Thus, we have extended our algebra–geometry dictionary. Over an algebraically closed field, every nonempty irreducible variety corresponds to a proper prime ideal, and conversely. Every point corresponds to a maximal ideal, and conversely.

EXERCISES FOR §5

1. If $h \in k[x_1, \ldots, x_n]$ has total degree N and if F is as in Proposition 6, show that $(g_1 g_2 \ldots g_n)^N (h \circ F)$ is a polynomial in $k[t_1, \ldots, t_m]$.
2. Show that a prime ideal is radical.
3. Show that an ideal I is prime if and only if for any ideals J and K such that $JK \subset I$, either $J \subset I$ or $K \subset I$.
4. Let $I_1, \ldots, I_n$ be ideals and P a prime ideal containing $\bigcap_{i=1}^n I_i$. Then prove that $P \supset I_i$ for some i. Further, if $P = \bigcap_{i=1}^n I_i$, show that $P = I_i$ for some i.
5. Express $f = x^2 z - 6y^4 + 2xy^3 z$ in the form $f = f_1(x, y, z)(x + 3) + f_2(x, y, z)(y - 1) + f_3(x, y, z)(z - 2)$ for some $f_1, f_2, f_3 \in k[x, y, z]$.
6. Let k be an infinite field.
   a. Show that any straight line in k^n is irreducible.
   b. Prove that any linear subspace of k^n is irreducible. Hint: Parametrize and use Proposition 5.
7. Show that
$$\mathbf{I}(\{(a_1, \ldots, a_n)\}) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle.$$
8. Show the following:
   a. $\langle x^2 + 1 \rangle$ is maximal in $\mathbb{R}[x]$.
   b. If $I \subset \mathbb{R}[x_1, \ldots, x_n]$ is maximal, show that $\mathbf{V}(I)$ is either empty or a point in $\mathbb{R}^n$. Hint: Examine the proof of Theorem 11.
   c. Give an example of a maximal ideal I in $\mathbb{R}[x_1, \ldots, x_n]$ for which $\mathbf{V}(I) = \emptyset$. Hint: Consider the ideal $\langle x_1^2 + 1, x_2, \ldots, x_n \rangle$.
9. Suppose that k is a field which is not algebraically closed.
   a. Show that if $I \subset k[x_1, \ldots, x_n]$ is maximal, then $\mathbf{V}(I)$ is either empty or a point in k^n. Hint: Examine the proof of Theorem 11.
   b. Show that there exists a maximal ideal I in $k[x_1, \ldots, x_n]$ for which $\mathbf{V}(I) = \emptyset$. Hint: See the previous exercise.
   c. Conclude that if k is not algebraically closed, there is always a maximal ideal of $k[x_1, \ldots, x_n]$ which is not of the form $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$.
10. Prove that Theorem 11 implies the Weak Nullstellensatz.
11. If $f \in \mathbb{C}[x_1, \ldots, x_n]$ is irreducible, then $\mathbf{V}(f)$ is irreducible.
12. Prove that if I is any proper ideal in $\mathbb{C}[x_1, \ldots, x_n]$, then $\sqrt{I}$ is the intersection of all maximal ideals containing I. Hint: Use Theorem 11.

§6 Decomposition of a Variety into Irreducibles

In the last section, we saw that irreducible varieties arise naturally in many contexts. It is natural to ask whether an arbitrary variety can be built up out of irreducibles. In this section, we explore this and related questions.

We begin by translating the *Ascending Chain Condition* (ACC) for ideals (see §5 of Chapter 2) into the language of varieties.

Proposition 1 (The Descending Chain Condition). *Any descending chain of varieties*

$$V_1 \supset V_2 \supset V_3 \supset \cdots$$

in k^n must stabilize. That is, there exists a positive integer N such that $V_N = V_{N+1} = \cdots$.

Proof. Passing to the corresponding ideals gives an ascending chain of ideals

$$\mathbf{I}(V_1) \subset \mathbf{I}(V_2) \subset \mathbf{I}(V_3) \subset \cdots .$$

By the ascending chain condition for ideals (see Theorem 7 of Chapter 2, §5), there exists N such that $\mathbf{I}(V_N) = \mathbf{I}(V_{N+1}) = \cdots$. Since $\mathbf{V}(\mathbf{I}(V)) = V$ for any variety V, we have $V_N = V_{N+1} = \cdots$. □

We can use Proposition 1 to prove the following basic result about the structure of affine varieties.

Theorem 2. *Let $V \subset k^n$ be an affine variety. Then V can be written as a finite union*

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

where each V_i is an irreducible variety.

Proof. Assume that V is an affine variety which cannot be written as a finite union of irreducibles. Then V is not irreducible, so that $V = V_1 \cup V_1'$, where $V \neq V_1$ and $V \neq V_1'$. Further, one of V_1 and V_1' must not be a finite union of irreducibles, for otherwise V would be of the same form. Say V_1 is not a finite union of irreducibles. Repeating the argument just given, we can write $V_1 = V_2 \cup V_2'$, where $V_1 \neq V_2$, $V_1 \neq V_2'$, and V_2 is not a finite union of irreducibles. Continuing in this way gives us an infinite sequence of affine varieties

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

with

$$V \neq V_1 \neq V_2 \neq \cdots .$$

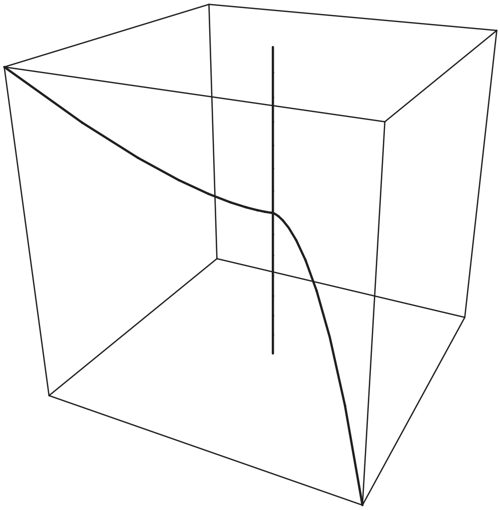
This contradicts Proposition 1. □

As a simple example of Theorem 2, consider the variety $\mathbf{V}(xz, yz)$ which is a union of a line (the z-axis) and a plane (the xy-plane), both of which are irreducible by

Exercise 6 of §5. For a more complicated example of the decomposition of a variety into irreducibles, consider the variety

$$V = \mathbf{V}(xz - y^2, x^3 - yz).$$

Here is a sketch of this variety.



The picture suggests that this variety is not irreducible. It appears to be a union of two curves. Indeed, since both $xz - y^2$ and $x^3 - yz$ vanish on the z-axis, it is clear that the z-axis $\mathbf{V}(x, y)$ is contained in V. What about the other curve $V - \mathbf{V}(x, y)$?

By Theorem 7 of §4, this suggests looking at the ideal quotient

$$\langle xz - y^2, x^3 - yz\rangle : \langle x, y\rangle.$$

(At the end of the section we will see that $\langle xz - y^2, x^3 - yz\rangle$ is a radical ideal.) We can compute this quotient using our algorithm for computing ideal quotients (make sure you review this algorithm). By equation (5) of §4, the above is equal to

$$(I : x) \cap (I : y),$$

where $I = \langle xz - y^2, x^3 - yz\rangle$. To compute $I : x$, we first compute $I \cap \langle x\rangle$ using our algorithm for computing intersections of ideals. Using lex order with $z > y > x$, we obtain

$$I \cap \langle x\rangle = \langle x^2z - xy^2, x^4 - xyz, x^3y - xz^2, x^5 - xy^3\rangle.$$

We can omit $x^5 - xy^3$ since it is a combination of the first and second elements in the basis. Hence

$$
\begin{aligned}
I : x &= \left\langle \frac{x^2z - xy^2}{x}, \frac{x^4 - xyz}{x}, \frac{x^3y - xz^2}{x} \right\rangle \\
&= \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle \qquad (1)\\
&= I + \langle x^2y - z^2 \rangle.
\end{aligned}
$$

Similarly, to compute $I : \langle y \rangle$, we compute

$$I \cap \langle y \rangle = \langle xyz - y^3, x^3y - y^2z, x^2y^2 - yz^2 \rangle,$$

which gives

$$
\begin{aligned}
I : y &= \left\langle \frac{xyz - y^3}{y}, \frac{x^3y - y^2z}{y}, \frac{x^2y^2 - yz^2}{y} \right\rangle \\
&= \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle \\
&= I + \langle x^2y - z^2 \rangle \\
&= I : x
\end{aligned}
$$

(Do the computations using a computer algebra system.) Since $I : x = I : y$, we have

$$I : \langle x, y \rangle = \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle.$$

The variety $W = \mathbf{V}(xz - y^2, x^3 - yz, x^2y - z^2)$ turns out to be an irreducible curve. To see this, note that it can be parametrized as (t^3, t^4, t^5) [it is clear that $(t^3, t^4, t^5) \in W$ for any t—we leave it as an exercise to show every point of W is of this form], so that W is irreducible by Proposition 5 of the last section. It then follows easily that

$$V = \mathbf{V}(x, y) \cup W$$

(see Theorem 7 of §4), which gives decomposition of V into irreducibles.

Both in the above example and the case of $\mathbf{V}(xz, yz)$, it appears that the decomposition of a variety is unique. It is natural to ask whether this is true in general. It is clear that, to avoid trivialities, we must rule out decompositions in which the same irreducible component appears more than once, or in which one irreducible component contains another. This is the aim of the following definition.

Definition 3. *Let $V \subset k^n$ be an affine variety. A decomposition*

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

where each V_i is an irreducible variety, is called a **minimal decomposition** *(or, sometimes, an* **irredundant union***) if $V_i \not\subset V_j$ for $i \neq j$.*

With this definition, we can now prove the following uniqueness result.

Theorem 4. *Let $V \subset k^n$ be an affine variety. Then V has a minimal decomposition*

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

(so each V_i is an irreducible variety and $V_i \not\subset V_j$ for $i \neq j$). Furthermore, this minimal decomposition is unique up to the order in which $V_1, \ldots, V_m$ are written.

Proof. By Theorem 2, V can be written in the form $V = V_1 \cup \ldots \cup V_m$, where each V_i is irreducible. Further, if a V_i lies in some V_j for $i \neq j$, we can drop V_i, and V will be the union of the remaining V_j's for $j \neq i$. Repeating this process leads to a minimal decomposition of V.

To show uniqueness, suppose that $V = V_1' \cup \cdots \cup V_l'$ is another minimal decomposition of V. Then, for each V_i in the first decomposition, we have

$$V_i = V_i \cap V = V_i \cap (V_1' \cup \cdots \cup V_l') = (V_i \cap V_1') \cup \cdots \cup (V_i \cap V_l').$$

Since V_i is irreducible, it follows that $V_i = V_i \cap V_j'$ for some j, i.e., $V_i \subset V_j'$. Applying the same argument to V_j' (using the V_i's to decompose V) shows that $V_j' \subset V_k$ for some k, and, thus,

$$V_i \subset V_j' \subset V_k.$$

By minimality, $i = k$, and it follows that $V_i = V_j'$. Hence, every V_i appears in $V = V_1' \cup \cdots \cup V_l'$, which implies $m \leq l$. A similar argument proves $l \leq m$, and $m = l$ follows. Thus, the V_i''s are just a permutation of the V_i's, and uniqueness is proved. □

We remark that the uniqueness part of Theorem 4 is false if one does not insist that the union be finite. (A plane P is the union of all the points on it. It is also the union of some line in P and all the points not on the line—there are infinitely many lines in P with which one could start.) This should alert the reader to the fact that although the proof of Theorem 4 is easy, it is far from vacuous: one makes subtle use of finiteness (which follows, in turn, from the Hilbert Basis Theorem).

Theorems 2 and 4 can also be expressed purely algebraically using the one-to-one correspondence between radical ideals and varieties.

Theorem 5. *If k is algebraically closed, then every radical ideal in $k[x_1, \ldots, x_n]$ can be written uniquely as a finite intersection of prime ideals, $I = P_1 \cap \cdots \cap P_r$, where $P_i \not\subset P_j$ for $i \neq j$. (As in the case of varieties, we often call such a presentation of a radical ideal a* **minimal decomposition** *or an* **irredundant intersection***).*

Proof. Theorem 5 follows immediately from Theorems 2 and 4 and the ideal–variety correspondence. □

We can also use ideal quotients from §4 to describe the prime ideals that appear in the minimal representation of a radical ideal.

Theorem 6. *If k is algebraically closed and I is a proper radical ideal such that*

$$I = \bigcap_{i=1}^{r} P_i$$

is its minimal decomposition as an intersection of prime ideals, then the P_i's are precisely the proper prime ideals that occur in the set $\{I : f \ : \ f \in k[x_1, \ldots, x_n]\}$.

Proof. First, note that since I is proper, each P_i is also a proper ideal (this follows from minimality).

For any $f \in k[x_1, \ldots, x_n]$, we have

$$I : f = \left(\bigcap_{i=1}^{r} P_i\right) : f = \bigcap_{i=1}^{r} (P_i : f)$$

by equation (2) of §4. Note also that for any prime ideal P, either $f \in P$, in which case $P : f = \langle 1 \rangle$, or $f \notin P$, in which case $P : f = P$ (see Exercise 3).

Now suppose that $I : f$ is a proper prime ideal. By Exercise 4 of §5, the above formula for $I : f$ implies that $I : f = P_i : f$ for some i. Since $P_i : f = P_i$ or $\langle 1 \rangle$ by the above observation, it follows that $I : f = P_i$.

To see that every P_i can arise in this way, fix i and pick $f \in \left(\bigcap_{j \neq i}^{r} P_j\right) - P_i$; such an f exists because $\bigcap_{i=1}^{r} P_i$ is minimal. Then $P_i : f = P_i$ and $P_j : f = \langle 1 \rangle$ for $j \neq i$. If we combine this with the above formula for $I : f$, then it follows easily that $I : f = P_i$. □

We should mention that Theorems 5 and 6 hold for any field k, although the proofs in the general case are different (see Corollary 10 of §7).

For an example of what these theorems say, consider the ideal $I = \langle xz - y^2, x^3 - yz \rangle$. Recall that the variety $V = \mathbf{V}(I)$ was discussed earlier in this section. For the time being, let us assume that I is radical (eventually we will see that this is true). Can we write I as an intersection of prime ideals?

We start with the geometric decomposition

$$V = \mathbf{V}(x, y) \cup W$$

proved earlier, where $W = \mathbf{V}(xz - y^2, x^3 - yz, x^2y - z^2)$. This suggests that

$$I = \langle x, y \rangle \cap \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle,$$

which is straightforward to prove by the techniques we have learned so far (see Exercise 4). Also, from equation (1), we know that $I : x = \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle$. Thus,

$$I = \langle x, y \rangle \cap (I : x).$$

To represent $\langle x, y \rangle$ as an ideal quotient of I, let us think geometrically. The idea is to remove W from V. Of the three equations defining W, the first two give V. So it makes sense to use the third one, $x^2y - z^2$, and one can check that $I : (x^2y - z^2) = \langle x, y \rangle$ (see Exercise 4). Thus,

$$I = (I : (x^2y - z^2)) \cap (I : x). \tag{2}$$

It remains to show that $I : (x^2y - z^2)$ and $I : x$ are prime ideals. The first is easy since $I : (x^2y - z^2) = \langle x, y \rangle$ is obviously prime. As for the second, we have already seen that $W : \mathbf{V}(xz - y^2, x^3 - yz, x^2y - z^2)$ is irreducible and, in the exercises, you will show that $\mathbf{I}(W) = \langle xz - y^2, x^3 - yz, x^2y - z^2\rangle = I : x$. It follows from Proposition 3 of §5 that $I : x$ is a prime ideal. This completes the proof that (2) is the minimal representation of I as an intersection of prime ideals. Finally, since I is an intersection of prime ideals, we see that I is a radical ideal (see Exercise 1).

The arguments used in this example are special to the case $I = \langle xz - y^2, x^3 - yz\rangle$. It would be nice to have more general methods that could be applied to any ideal. Theorems 2, 4, 5, and 6 tell us that certain decompositions exist, but the proofs give no indication of how to find them. The problem is that the proofs rely on the Hilbert Basis Theorem, which is intrinsically nonconstructive. Based on what we have seen in §§5 and 6, the following questions arise naturally:

- (Primality) Is there an algorithm for deciding if a given ideal is prime?
- (Irreducibility) Is there an algorithm for deciding if a given affine variety is irreducible?
- (Decomposition) Is there an algorithm for finding the minimal decomposition of a given variety or radical ideal?

The answer to all three questions is *yes*, and descriptions of the algorithms can be found in the works of HERMANN (1926), MINES, RICHMAN, and RUITENBERG (1988), and SEIDENBERG (1974, 1984). As in §2, the algorithms in these articles are not very practical. However, the work of GIANNI, TRAGER, and ZACHARIAS (1988) has led to algorithms implemented in AXIOM and REDUCE that answer the above questions. See also Chapter 8 of BECKER and WEISPFENNING (1993) and, for the primality algorithm, §4.4 of ADAMS and LOUSTAUNAU (1994). A different algorithm for studying these questions, based on ideas of EISENBUD, HUNEKE and VASCONCELOS (1992), has been implemented in Macaulay 2.

EXERCISES FOR §6

1. Show that the intersection of any collection of prime ideals is radical.
2. Show that an irredundant intersection of at least two prime ideals is never prime.
3. If $P \subset k[x_1, \ldots, x_n]$ is a prime ideal, then prove that $P : f = P$ if $f \notin P$ and $P : f = \langle 1\rangle$ if $f \in P$.
4. Let $I = \langle xz - y^2, x^3 - yz\rangle$.
   a. Show that $I : (x^2y - z^2) = \langle x, y\rangle$.
   b. Show that $I : (x^2y - z^2)$ is prime.
   c. Show that $I = \langle x, y\rangle \cap \langle xz - y^2, x^3 - yz, z^2 - x^2y\rangle$.
5. Let $J = \langle xz - y^2, x^3 - yz, z^2 - x^2y\rangle \subset k[x, y, z]$, where k is infinite.
   a. Show that every point of $W = V(f)$ is of the form (t^3, t^4, t^5) for some $t \in k$.
   b. Show that $J = \mathbf{I}(W)$. Hint: Compute a Groebner basis for J using lex order with $z > y > x$ and show that every $f \in k[x, y, z]$ can be written in the form
   $$f = g + a + bz + xA(x) + yB(x) + y^2C(x),$$
   where $g \in J, a, b \in k$ and $A, B, C \in k[x]$.
6. Translate Theorem 6 and its proof into geometry.
7. Let $I = \langle xz - y^2, z^3 - x^5\rangle \subset \mathbb{Q}[x, y, z]$.
   a. Express $\mathbf{V}(I)$ as a finite union of irreducible varieties. Hint: You will use the parametrizations (t^3, t^4, t^5) and $(t^3, -t^4, t^5)$.

b. Express I as an intersection of prime ideals which are ideal quotients of I and conclude that I is radical.

8. Let V, W be varieties in k^n with $V \subset W$. Show that each irreducible component of V is contained in some irreducible component of W.
9. Let $f \in \mathbb{C}[x_1, \ldots, x_n]$ and let $f = f_1^{a_1} f_2^{a_2} \ldots f_r^{a_r}$ be the decomposition of f into irreducible factors. Show that $\mathbf{V}(f) = \mathbf{V}(f_1) \cup \cdots \cup \mathbf{V}(f_r)$ is the decomposition of $\mathbf{V}(f)$ into irreducible components and $\mathbf{I}(\mathbf{V}(f)) = (f_1 f_2 \cdots f_r)$. Hint: See Exercise 11 of §5.

§7 (Optional) Primary Decomposition of Ideals

In view of the decomposition theorem proved in §6 for radical ideals, it is natural to ask whether an arbitrary ideal I (not necessarily radical) can be represented as an intersection of simpler ideals. In this section, we will prove the Lasker–Noether decomposition theorem, which describes the structure of I in detail.

There is no hope of writing an arbitrary ideal I as an intersection of prime ideals (since an intersection of prime ideals is always radical). The next thing that suggests itself is to write I as an intersection of powers of prime ideals. This does not quite work either: consider the ideal $I = \langle x, y^2 \rangle$ in $\mathbb{C}[x, y]$. Any prime ideal containing I must contain x and y and, hence, must equal $\langle x, y \rangle$ (since $\langle x, y \rangle$ is maximal). Thus, if I were to be an intersection of powers of prime ideals, it would have to be a power of $\langle x, y \rangle$ (see Exercise 1 for the details).

The concept we need is a bit more subtle.

Definition 1. *An ideal I in $k[x_1, \ldots, x_n]$ is* **primary** *if $fg \in I$ implies either $f \in I$ or some power $g^m \in I$ (for some $m > 0$).*

It is easy to see that prime ideals are primary. Also, you can check that the ideal $I = \langle x, y^2 \rangle$ discussed above is primary (see Exercise 1).

Lemma 2. *If I is a primary ideal, then $\sqrt{I}$ is prime and is the smallest prime ideal containing I.*

Proof. See Exercise 2. □

In view of this lemma, we make the following definition.

Definition 3. *If I is primary and $\sqrt{I} = P$, then we say that I is P-***primary**.

We can now prove that every ideal is an intersection of primary ideals.

Theorem 4. *Every ideal $I \subset k[x_1, \ldots, x_n]$ can be written as a finite intersection of primary ideals.*

Proof. We first define an ideal I to be *irreducible* if $I = I_1 \cap I_2$ implies that $I = I_1$ or $I = I_2$. We claim that every ideal is an intersection of finitely many irreducible ideals.

The argument is an "ideal" version of the proof of Theorem 2 from §6. One uses the ACC rather than the DCC—we leave the details as an exercise.

Next we claim that an irreducible ideal is primary. Note that this will prove the theorem. To see why the claim is true, suppose that I is irreducible and that $fg \in I$ with $f \notin I$. We need to prove that some power of g lies in I. Consider the ideals $I : g^n$ for $n \geq 1$. In the exercises, you will show that $I : g^n \subset I : g^{n+1}$ for all n. Thus, we get the ascending chain of ideals

$$I : g \subset I : g^2 \subset \cdots .$$

By the ascending chain condition, there exists an integer $N \geq 1$ such that $I : g^N = I : g^{N+1}$. We will leave it as an exercise to show that $(I + \langle g^N \rangle) \cap (I + \langle f \rangle) = I$. Since I is irreducible, it follows that $I = I + \langle g^N \rangle$ or $I = I + \langle f \rangle$. The latter cannot occur since $f \notin I$, so that $I = I + \langle g^N \rangle$. This proves that $g^N \in I$. $\square$

As in the case of varieties, we can define what it means for a decomposition to be minimal.

Definition 5. *A* **primary decomposition** *of an ideal I is an expression of I as an intersection of primary ideals: $I = \bigcap_{i=1}^r Q_i$. It is called* **minimal** *or* **irredundant** *if the $\sqrt{Q_i}$ are all distinct and $Q_i \not\supset \bigcap_{j \neq i} Q_j$.*

To prove the existence of a minimal decomposition, we will need the following lemma, the proof of which we leave as an exercise.

Lemma 6. *If I, J are primary and $\sqrt{I} = \sqrt{J}$, then $I \cap J$ is primary.*

We can now prove the first part of the Lasker–Noether decomposition theorem.

Theorem 7 (Lasker–Noether). *Every ideal $I \subset k[x_1, \ldots, x_n]$ has a minimal primary decomposition.*

Proof. By Theorem 4, we know that there is a primary decomposition $I = \bigcap_{i=1}^r Q_i$. Suppose that Q_i and Q_j have the same radical for some $i \neq j$. Then, by Lemma 6, $Q = Q_i \cap Q_j$ is primary, so that in the decomposition of I, we can replace Q_i and Q_j by the single ideal Q. Continuing in this way, eventually all of the Q_i's will have distinct radicals.

Next, suppose that some Q_i contains $\bigcap_{j \neq i} Q_j$. Then we can omit Q_i, and I will be the intersection of the remaining Q_j's for $j \neq i$. Continuing in this way, we can reduce to the case where $Q_i \not\supset \bigcap_{j \neq i} Q_j$ for all i. $\square$

Unlike the case of varieties (or radical ideals), a minimal primary decomposition need not be unique. In the exercises, you will verify that the ideal $\langle x^2, xy \rangle \subset k[x, y]$ has the two distinct minimal decompositions

$$\langle x^2, xy \rangle = \langle x \rangle \cap \langle x^2, xy, y^2 \rangle = \langle x \rangle \cap \langle x^2, y \rangle.$$

Although $\langle x^2, xy, y^2\rangle$ and $\langle x^2, y\rangle$ are distinct, note that they have the same radical. To prove that this happens in general, we will use ideal quotients from §4. We start by computing some ideal quotients of a primary ideal.

Lemma 8. *If I is primary and $\sqrt{I} = P$ and if $f \in k[x_1, \dots, x_n]$, then:*

$$\begin{array}{lll} \text{if } f \in I, & \text{then} & I : f = \langle 1\rangle, \\ \text{if } f \notin I, & \text{then} & I : f \text{ is } P\text{-primary}, \\ \text{if } f \notin P, & \text{then} & I : f = I. \end{array}$$

Proof. See Exercise 7. □

The second part of the Lasker–Noether theorem tells us that the *radicals* of the ideals in a minimal decomposition are uniquely determined.

Theorem 9 (Lasker–Noether). *Let $I = \bigcap_{i=1}^r Q_i$ be a minimal primary decomposition of a proper ideal $I \subset k[x_1, \dots, x_n]$ and let $P_i = \sqrt{Q_i}$. Then the P_i are precisely the proper prime ideals occurring in the set $\{\sqrt{I : f} \ : \ f \in k[x_1, \dots, x_n]\}$.*

Remark. In particular, the P_i are independent of the primary decomposition of I. We say the P_i belong to I.

Proof. The proof is very similar to the proof of Theorem 6 from §6. The details are covered in Exercises 8–10. □

In §6, we proved a decomposition theorem for radical ideals over an algebraically closed field. Using Lasker–Noether theorems, we can now show that these results hold over an arbitrary field k.

Corollary 10. *Let $I = \bigcap_{i=1}^r Q_i$ be a minimal primary decomposition of a proper radical ideal $I \subset k[x_1, \dots, x_n]$. Then the Q_i are prime and are precisely the proper prime ideals occurring in the set $\{I : f \ : \ f \in k[x_1, \dots, x_n]\}$.*

Proof. See Exercise 12. □

The two Lasker–Noether theorems do not tell the full story of a minimal primary decomposition $I = \bigcap_{i=1}^r Q_i$. For example, if P_i is minimal in the sense that no P_j is strictly contained in P_i, then one can show that Q_i is uniquely determined. Thus there is a uniqueness theorem for *some* of the Q_i's [see Chapter 4 of ATIYAH and MACDONALD (1969) for the details]. We should also mention that the conclusion of Theorem 9 can be strengthened: one can show that the P_i's are precisely the proper prime ideals in the set $\{I : f \ : \ f \in k[x_1, \dots, x_n]\}$ [see Chapter 7 of ATIYAH and MACDONALD (1969)].

Finally, it is natural to ask if a primary decomposition can be done constructively. More precisely, given $I = \langle f_1, \dots, f_s\rangle$, we can ask the following:

- (Primary Decomposition) Is there an algorithm for finding bases for the primary ideals Q_i in a minimal primary decomposition of I?
- (Associated Primes) Can we find bases for the associated primes $P_i = \sqrt{Q_i}$?

If you look in the references given at the end of §6, you will see that the answer to these questions is *yes*. Primary decomposition has been implemented in AXIOM, REDUCE, and MACAULAY 2.

EXERCISES FOR §7

1. Consider the ideal $I = \langle x, y^2 \rangle \subset \mathbb{C}[x, y]$.
   a. Prove that $\langle x, y \rangle^2 \subsetneqq I \subsetneqq \langle x, y \rangle$, and conclude that I is not a prime power.
   b. Prove that I is primary.
2. Prove Lemma 2.
3. This exercise is concerned with the proof of Theorem 4. Let $I \subset k[x_1, \dots, x_n]$ be an ideal.
   a. Using the hints given in the text, prove that I is a finite intersection of irreducible ideals.
   b. If $g \in k[x_1, \dots, x_n]$, then prove that $I : g^m \subset I : g^{m+1}$ for all $m \geq 1$.
   c. Suppose that $fg \in I$. If, in addition, $I : g^N = I : g^{N+1}$, then prove that $(I + \langle g^N \rangle) \cap (I + \langle f \rangle) = I$. Hint: Elements of $(I + \langle g^N \rangle) \cap (I + \langle f \rangle)$ can be written as $a + bg^N = c + df$, where $a, c \in I$ and $b, d \in k[x_1, \dots, x_n]$. Now multiply through by g.
4. In the proof of Theorem 4, we showed that every irreducible ideal is primary. Surprisingly, the converse is false. Let I be the ideal $\langle x^2, xy, y^2 \rangle \subset k[x, y]$.
   a. Show that I is primary.
   b. Show that $I = \langle x^2, y \rangle \cap \langle x, y^2 \rangle$ and conclude that I is not irreducible.
5. Prove Lemma 6. Hint: Proposition 16 from §3 will be useful.
6. Let I be the ideal $\langle x^2, xy \rangle \subset \mathbb{Q}[x, y]$.
   a. Prove that
   $$I = \langle x \rangle \cap \langle x^2, xy, y^2 \rangle = \langle x \rangle \cap \langle x^2, y \rangle$$
   are two distinct minimal primary decompositions of I.
   b. Prove that for any $a \in \mathbb{Q}$,
   $$I = \langle x \rangle \cap \langle x^2, y - ax \rangle$$
   is a minimal primary decomposition of I. Thus I has infinitely many distinct minimal primary decompositions.
7. Prove Lemma 8.
8. Prove that an ideal is proper if and only if its radical is.
9. Let I be a proper ideal. Prove that the primes belonging to I are also proper ideals. Hint: Use Exercise 8.
10. Prove Theorem 9. Hint: Adapt the proof of Theorem 6 from §6. The extra ingredient is that you will need to take radicals. Proposition 16 from §3 will be useful. You will also need to use Exercise 9 and Lemma 8.
11. Let $P_1, \dots, P_r$ be the prime ideals belonging to I.
    a. Prove that $\sqrt{I} = \bigcap_{i=1}^r P_i$. Hint: Use Proposition 16 from §3.
    b. Use the ideal of Exercise 4 to show that $\sqrt{I} = \bigcap_{i=1}^r P_i$ need not be a minimal decomposition of $\sqrt{I}$.
12. Prove Corollary 10. Hint: Show that $I : f$ is radical whenever I is.

§8 Summary

The following table summarizes the results of this chapter. In the table, it is supposed that all ideals are radical and that the field is algebraically closed.

ALGEBRA		GEOMETRY
radical ideals		varieties
I	$\longrightarrow$	$\mathbf{V}(I)$
$\mathbf{I}(V)$	$\longleftarrow$	V
addition of ideals		intersection of varieties
$I + J$	$\longrightarrow$	$\mathbf{V}(I) \cap \mathbf{V}(J)$
$\sqrt{\mathbf{I}(V) + \mathbf{I}(W)}$	$\longleftarrow$	$V \cap W$
product of ideals		union of varieties
IJ	$\longrightarrow$	$\mathbf{V}(I) \cup \mathbf{V}(J)$
$\sqrt{\mathbf{I}(V)\mathbf{I}(W)}$	$\longleftarrow$	$V \cup W$
intersection of ideals		union of varieties
$I \cap J$	$\longrightarrow$	$\mathbf{V}(I) \cup \mathbf{V}(J)$
$\mathbf{I}(V) \cap \mathbf{I}(W)$	$\longleftarrow$	$V \cup W$
quotient of ideals		difference of varieties
$I : J$	$\longrightarrow$	$\overline{\mathbf{V}(I) - \mathbf{V}(J)}$
$\mathbf{I}(V) : \mathbf{I}(W)$	$\longleftarrow$	$\overline{V - W}$
elimination of variables		projection of varieties
$\sqrt{I \cap k[x_{l+1}, \ldots, x_n]}$	$\longleftrightarrow$	$\overline{\pi_l(\mathbf{V}(I))}$
prime ideal		irreducible variety
maximal ideal		point of affine space
ascending chain condition		descending chain condition