5

Polynomial and Rational Functions on a Variety

One of the unifying themes of modern mathematics is that in order to understand any class of mathematical objects, one should also study *mappings* between those objects, and especially the mappings which preserve some property of interest. For instance, in linear algebra after studying vector spaces, you also studied the properties of *linear mappings* between vector spaces (mappings that preserve the vector space operations of sum and scalar product).

In this chapter, we will consider mappings between varieties, and the results of our investigation will form another chapter of the "algebra–geometry dictionary" that we started in Chapter 4. The algebraic properties of polynomial and rational functions on a variety yield many insights into the geometric properties of the variety itself. This chapter will also serve as an introduction to (and motivation for) the idea of a quotient ring.

§1 Polynomial Mappings

We will begin our study of functions between varieties by reconsidering two examples that we have encountered previously. First, recall the tangent surface of the twisted cubic curve in $\mathbb{R}^3$. As in equation (1) of Chapter 3, §3 we describe this surface parametrically:

$$\begin{aligned} x &= t + u, \\ y &= t^2 + 2tu, \\ z &= t^3 + 3t^2u. \end{aligned} \tag{1}$$

In functional language, giving the parametric representation (1) is equivalent to defining a mapping

$$\phi : \mathbb{R}^2 \longrightarrow \mathbb{R}^3$$

by

$$\phi(t, u) = (t + u, t^2 + 2tu, t^3 + 3t^2u). \tag{2}$$

The domain of ϕ is an affine variety $V = \mathbb{R}^2$ and the image of ϕ is the tangent surface S.

We saw in §3 of Chapter 3 that S is the same as the affine variety

$$W = \mathbf{V}(x^3z - (3/4)x^2y^2 - (3/2)xyz + y^3 + (1/4)z^2).$$

Hence, our parametrization gives what we might call a *polynomial mapping* between V and W. (The adjective "polynomial" refers to the fact that the component functions of ϕ are polynomials in t and u.)

Second, in the discussion of the geometry of elimination of variables from systems of equations in §2 of Chapter 3, we considered the projection mappings

$$\pi_k : \mathbb{C}^n \longrightarrow \mathbb{C}^{n-k}$$

defined by

$$\pi_k(a_1, \ldots, a_n) = (a_{k+1}, \ldots, a_n).$$

If we have a variety $V = \mathbf{V}(I) \subset \mathbb{C}^n$, then we can also restrict π_k to V and, as we know, $\pi_k(V)$ will be contained in the affine variety $W = \mathbf{V}(I_k)$, where $I_k = I \cap \mathbb{C}[x_{k+1}, \ldots, x_n]$, the kth elimination ideal of I. Hence, we can consider $\pi_k : V \to W$ as a mapping of varieties. Here too, by the definition of π_k we see that the component functions of π_k are polynomials in the coordinates in the domain.

Definition 1. *Let $V \subset k^m$, $W \subset k^n$ be varieties. A function $\phi : V \to W$ is said to be a* **polynomial mapping** *(or* **regular mapping***) if there exist polynomials $f_1, \ldots, f_n \in k[x_1, \ldots, x_m]$ such that*

$$\phi(a_1, \ldots, a_m) = (f_1(a_1, \ldots, a_m), \ldots, f_n(a_1, \ldots, a_m))$$

for all $(a_1, \ldots, a_m) \in V$. We say that the n-tuple of polynomials

$$(f_1, \ldots, f_n) \in (k[x_1, \ldots, x_m])^n$$

represents *ϕ.*

To say that ϕ is a polynomial mapping from $V \subset k^m$ to $W \subset k^n$ represented by $(f_1, \ldots, f_n)$ means that $(f_1(a_1, \ldots, a_m), \ldots, f_n(a_1, \ldots, a_m))$ must satisfy the defining equations of W for all $(a_1, \ldots, a_m) \in V$. For example, consider $V = \mathbf{V}(y - x^2, z - x^3) \subset k^3$ (the twisted cubic) and $W = \mathbf{V}(y^3 - z^2) \subset k^2$. Then the projection $\pi_1 : k^3 \to k^2$ represented by (y, z) gives a polynomial mapping $\pi_1 : V \to W$. This is true because every point in $\pi_1(V) = \{(x^2, x^3) : x \in k\}$ satisfies the defining equation of W.

Of particular interest is the case $W = k$, where ϕ simply becomes a scalar polynomial function defined on the variety V. One reason to consider polynomial functions from V to k is that a general polynomial mapping $\phi : V \to k^n$ is constructed by using any n polynomial functions $\phi : V \to k$ as the components. Hence, if we understand functions $\phi : V \to k$, we understand how to construct all mappings $\phi : V \to k^n$ as well.

To begin our study of polynomial functions, note that, for $V \subset k^m$, Definition 1 says that a mapping $\phi : V \to k$ is a polynomial function if *there exists* a polynomial $f \in k[x_1, \ldots, x_m]$ representing ϕ. In fact, we usually specify a polynomial function by giving an explicit polynomial representative. Thus, finding a representative is not actually the key issue. What we will see next, however, is that the cases where a representative is uniquely determined are very rare. For example, consider the variety

$V = \mathbf{V}(y - x^2) \subset \mathbb{R}^2$. The polynomial $f = x^3 + y^3$ represents a polynomial function from V to $\mathbb{R}$. However, $g = x^3 + y^3 + (y - x^2)$, $h = x^3 + y^3 + (x^4 y - x^6)$, and $F = x^3 + y^3 + A(x, y)(y - x^2)$ for any $A(x, y)$ define *the same polynomial function* on V. Indeed, since $\mathbf{I}(V)$ is the set of polynomials which are zero at every point of V, adding any element of $\mathbf{I}(V)$ to f does not change the values of the polynomial at the points of V. The general pattern is the same.

Proposition 2. *Let $V \subset k^m$ be an affine variety. Then*

(i) *f and $g \in k[x_1, \ldots, x_m]$ represent the same polynomial function on V if and only if $f - g \in \mathbf{I}(V)$.*
(ii) *$(f_1, \ldots, f_n)$ and $(g_1, \ldots, g_n)$ represent the same polynomial mapping from V to k^n if and only if $f_i - g_i \in \mathbf{I}(V)$ for each i, $1 \leq i \leq n$.*

Proof. (i) If $f - g = h \in \mathbf{I}(V)$, then for any $p = (a_1, \ldots, a_m) \in V$, $f(p) - g(p) = h(p) = 0$. Hence, f and g represent the same function on V. Conversely, if f and g represent the same function, then, at every $p \in V$, $f(p) - g(p) = 0$. Thus, $f - g \in \mathbf{I}(V)$ by definition. Part (ii) follows directly from (i). □

Thus, the correspondence between polynomials in $k[x_1, \ldots, x_m]$ and polynomial functions is one-to-one only in the case where $\mathbf{I}(V) = \{0\}$. In Exercise 7, you will show that $\mathbf{I}(V) = \{0\}$ if and only if k is infinite and $V = k^m$.

There are two ways of dealing with this potential ambiguity in describing polynomial functions on a variety:

- In rough terms, we can "lump together" *all* the polynomials $f \in k[x_1, \ldots, x_m]$ that represent the same function on V and think of that collection as a "new object" in its own right. We can then take the collection of polynomials as our description of the function on V.
- Alternatively, we can systematically look for the simplest possible individual polynomial that represents each function on V and work with those "standard representative" polynomials exclusively.

Each of these approaches has its own advantages, and we will consider both of them in detail in later sections of this chapter. We will conclude this section by looking at two further examples to show the kinds of properties of varieties that can be revealed by considering polynomial functions.

Definition 3. *We denote by $k[V]$ the collection of polynomial functions $\phi : V \to k$.*

Since k is a field, we can define a sum and a product function for any pair of functions $\phi, \psi : V \to k$ by adding and multiplying images. For each $p \in V$,

$$\begin{aligned}(\phi + \psi)(p) &= \phi(p) + \psi(p),\\ (\phi \cdot \psi)(p) &= \phi(p) \cdot \psi(p).\end{aligned}$$

Furthermore, if we pick specific representatives $f, g \in k[x_1, \ldots, x_m]$ for ϕ, ψ, respectively, then by definition, the polynomial sum $f + g$ represents $\phi + \psi$ and the polynomial product $f \cdot g$ represents $\phi \cdot \psi$. It follows that $\phi + \psi$ and $\phi \cdot \psi$ are polynomial functions on V.

Thus, we see that $k[V]$ has sum and product operations constructed using the sum and product operations in $k[x_1, \dots, x_m]$. All of the usual properties of sums and products of polynomials also hold for functions in $k[V]$. Thus, $k[V]$ is another example of a *commutative ring*. (See Appendix A for the precise definition.) We will also return to this point in §2.

Now we are ready to start exploring what $k[V]$ can tell us about the geometric properties of a variety V. First, recall from §5 of Chapter 4 that a variety $V \subset k^m$ is said to be *reducible* if it can be written as the union of two nonempty proper subvarieties: $V = V_1 \cup V_2$, where $V_1 \neq V$ and $V_2 \neq V$. For example, the variety $V = \mathbf{V}(x^3 + xy^2 - xz, yx^2 + y^3 - yz)$ in k^3 is reducible since, from the factorizations of the defining equations, we can decompose V as $V = \mathbf{V}(x^2 + y^2 - z) \cup \mathbf{V}(x, y)$. We would like to demonstrate that geometric properties such as reducibility can be "read off" from a sufficiently good algebraic description of $k[V]$. To see this, let

$$f = x^2 + y^2 - z, \quad g = 2x^2 - 3y^4z \in k[x, y, z] \tag{3}$$

and let ϕ, ψ be the corresponding elements of $k[V]$.

Note that neither ϕ nor ψ is identically zero on V. For example, at $(0, 0, 5) \in V$, $\phi(0, 0, 5) = f(0, 0, 5) = -5 \neq 0$. Similarly, at $(1, 1, 2) \in V$, $\psi(1, 1, 2) = g(1, 1, 2) = -4 \neq 0$. However, the product function $\phi \cdot \psi$ is zero at every point of V. The reason is that

$$\begin{aligned} f \cdot g &= (x^2 + y^2 - z)(2x^2 - 3y^4z) \\ &= 2x(x^3 + xy^2 - xz) - 3y^3z(x^2y + y^3 - yz) \\ &\in \langle x^3 + xy^2 - xz, x^2y + y^3 - yz\rangle. \end{aligned}$$

Hence $f \cdot g \in \mathbf{I}(V)$, so the corresponding polynomial function $\phi \cdot \psi$ on V is identically zero.

The product of two nonzero elements of a field or of two nonzero polynomials in $k[x_1, \dots, x_n]$ is never zero. In general, a commutative ring R is said to be an *integral domain* if whenever $a \cdot b = 0$ in R, either $a = 0$ or $b = 0$. Hence, for the variety V in the above example, we see that $k[V]$ is not an integral domain. Furthermore, the existence of $\phi \neq 0$ and $\psi \neq 0$ in $k[V]$ such that $\phi \cdot \psi = 0$ is a direct consequence of the reducibility of V : f in (3) is zero on $V_1 = \mathbf{V}(x^2 + y^2 - z)$, but not on $V_2 = \mathbf{V}(x, y)$, and similarly g is zero on V_2, but not on V_1. This is why $f \cdot g = 0$ at every point of $V = V_1 \cup V_2$. Hence, we see a relation between the geometric properties of V and the algebraic properties of $k[V]$.

The general case of this relation can be stated as follows.

Proposition 4. *Let $V \subset k^n$ be an affine variety. The following statements are equivalent:*

(i) *V is irreducible.*
(ii) *$\mathbf{I}(V)$ is a prime ideal.*
(iii) *$k[V]$ is an integral domain.*

Proof. (i) ⇔ (ii) is Proposition 3 of Chapter 4, §5.

To show (iii) ⇒ (i), suppose that $k[V]$ is an integral domain but that V is reducible. By Definition 1 of Chapter 4, §5, this means that we can write $V = V_1 \cup V_2$, where V_1 and V_2 are proper, nonempty subvarieties of V. Let $f_1 \in k[x_1, \ldots, x_n]$ be a polynomial that vanishes on V_1 but not identically on V_2 and, similarly, let f_2 be identically zero on V_2, but not on V_1. (Such polynomials must exist since V_1 and V_2 are varieties and neither is contained in the other.) Hence, neither f_1 nor f_2 represents the zero function in $k[V]$. However, the product $f_1 \cdot f_2$ vanishes at all points of $V_1 \cup V_2 = V$. Hence, the product function is zero in $k[V]$. This is a contradiction to our hypothesis that $k[V]$ was an integral domain. Hence, V is irreducible.

Finally, for (i) ⇒ (iii), suppose that $k[V]$ is not an integral domain. Then there must be polynomials $f, g \in k[x_1, \ldots, x_n]$ such that neither f nor g vanishes identically on V but their product does. In Exercise 9, you will check that we get a decomposition of V as a union of subvarieties:

$$V = (V \cap \mathbf{V}(f)) \cup (V \cap \mathbf{V}(g)).$$

You will also show in Exercise 9 that, under these hypotheses, neither $V \cap \mathbf{V}(f)$ nor $V \cap \mathbf{V}(g)$ is all of V. This contradicts our assumption that V is irreducible. □

Next we will consider another example of the kind of information about varieties revealed by polynomial mappings. The variety $V \subset \mathbb{C}^3$ defined by

$$\begin{aligned} x^2 + 2xz + 2y^2 + 3y &= 0, \\ xy + 2x + z &= 0, \\ xz + y^2 + 2y &= 0 \end{aligned} \tag{4}$$

is the intersection of three quadric surfaces.

To study V, we compute a Groebner basis for the ideal generated by the polynomials in (4), using the lexicographic order and the variable order $y > z > x$. The result is

$$\begin{aligned} g_1 &= y - x^2, \\ g_2 &= z + x^3 + 2x. \end{aligned} \tag{5}$$

Geometrically, by the results of Chapter 3, §2, we know that the projection of V on the x-axis is onto since the two polynomials in (5) have constant leading coefficients. Furthermore, for each value of x in $\mathbb{C}$, there are unique y, z satisfying equations (4).

We can rephrase this observation using the maps

$$\begin{aligned} \pi &: V \longrightarrow \mathbb{C}, \ (x, y, z) \mapsto x, \\ \phi &: \mathbb{C} \longrightarrow V, \ x \mapsto (x, x^2, -x^3 - 2x). \end{aligned}$$

Note that (5) guarantees that ϕ takes values in V. Both ϕ and π are visibly polynomial mappings. We claim that these maps establish a one-to-one correspondence between the points of the variety V and the points of the variety $\mathbb{C}$.

Our claim will follow if we can show that π and ϕ are inverses of each other. To verify this last claim, we first check that $\pi \circ \phi = \mathrm{id}_{\mathbb{C}}$. This is actually quite clear since

$$(\pi \circ \phi)(x) = \pi(x, x^2, -x^3 - 2x) = x.$$

On the other hand, if $(x, y, z) \in V$, then

$$(\phi \circ \pi)(x, y, z) = (x, x^2, -x^3 - 2x).$$

By (5), we have $y - x^2, z + x^3 + 2x \in \mathbf{I}(V)$ and it follows that $\phi \circ \pi$ defines the *same* mapping on V as $\mathrm{id}_V(x, y, z) = (x, y, z)$.

The conclusion we draw from this example is that $V \in \mathbb{C}^3$ and $\mathbb{C}$ are "isomorphic" varieties in the sense that there is a one-to-one, onto, polynomial mapping from V to $\mathbb{C}$, with a polynomial inverse. Even though our two varieties are defined by different equations and are subsets of different ambient spaces, they are "the same" in a certain sense. In addition, the Groebner basis calculation leading to equation (5) shows that $\mathbb{C}[V] = \mathbb{C}[x]$, in the sense that every $\psi \in \mathbb{C}[V]$ can be (uniquely) expressed by substituting for y and z from (5) to yield a polynomial in x alone. Of course, if we use x as the coordinate on $W = \mathbb{C}$, then $\mathbb{C}[W] = \mathbb{C}[x]$ as well, and we obtain the *same* collection of functions on our two isomorphic varieties.

Thus, the collection of polynomial functions on an affine variety can detect geometric properties such as reducibility or irreducibility. In addition, knowing the structure of $k[V]$ can also furnish information leading toward the beginnings of a *classification* of varieties, a topic we have not broached before. We will return to these questions later in the chapter, once we have developed several different tools to analyze the algebraic properties of $k[V]$.

EXERCISES FOR §1

1. Let V be the twisted cubic in $\mathbb{R}^3$ and let $W = \mathbf{V}(v - u - u^2)$ in $\mathbb{R}^2$. Show that $\phi(x, y, z) = (xy, z + x^2y^2)$ defines a polynomial mapping from V to W. Hint: The easiest way is to use a parametrization of V.
2. Let $V = \mathbf{V}(y - x)$ in $\mathbb{R}^2$ and let $\phi : \mathbb{R}^2 \to \mathbb{R}^3$ be the polynomial mapping represented by $\phi(x, y) = (x^2 - y, y^2, x - 3y^2)$. The image of V is a variety in $\mathbb{R}^3$. Find a system of equations defining the image of ϕ.
3. Given a polynomial function $\phi : V \to k$, we define a *level set* of ϕ to be

$$\phi^{-1}(c) = \{(a_1, \ldots, a_m) \in V : \phi(a_1, \ldots, a_m) = c\},$$

where $c \in k$ is fixed. In this exercise, we will investigate how level sets can be used to analyze and reconstruct a variety. We will assume that $k = \mathbb{R}$, and we will work with the surface

$$\mathbf{V}(x^2 - y^2z^2 + z^3) \subset \mathbb{R}^3.$$

a. Let ϕ be the polynomial function represented by $f(x, y, z) = z$. The image of ϕ is all of $\mathbb{R}$ in this case. For each $c \in \mathbb{R}$, explain why the level set $\phi^{-1}(c)$ is the affine variety defined by the equations:

$$\begin{aligned} x^2 - y^2z^2 + z^3 &= 0, \\ z - c &= 0. \end{aligned}$$

b. Eliminate z between these equations to find the equation of the intersection of V with the plane $z = c$. Explain why your equation defines a hyperbola in the plane $z = c$ if $c \neq 0$, and the y-axis if $c = 0$. (Refer to the sketch of V in §3 of Chapter 1, and see if you can visualize the way these hyperbolas lie on V.)

c. Let $\pi : V \to \mathbb{R}$ be the polynomial mapping $\pi(x, y, z) = x$. Describe the level sets $\pi^{-1}(c)$ in V geometrically for $c = -1, 0, 1$.
d. Do the same for the level sets of $\sigma : V \to \mathbb{R}$ given by $\sigma(x, y, z) = y$.
e. Construct a polynomial mapping $\psi:\mathbb{R}\to V$ and identify the image as a subvariety of V.

4. Let $V = \mathbf{V}(z^2 - (x^2 + y^2 - 1)(4 - x^2 - y^2))$ in $\mathbb{R}^3$ and let $\pi : V \to \mathbb{R}^2$ be the vertical projection $\pi(x, y, z) = (x, y)$.
   a. What is the maximum number of points in $\pi^{-1}(a, b)$ for $(a, b) \in \mathbb{R}^2$?
   b. For which subsets $R \subset \mathbb{R}^2$ does $(a, b) \in R$ imply $\phi^{-1}(a, b)$ consists of two points, one point, no points?
   c. Using part (b) describe and/or sketch V.
5. Show that $\phi_1(x, y, z) = (2x^2 + y^2, z^2 - y^3 + 3xz)$ and $\phi_2(x, y, z) = (2y + xz, 3y^2)$ represent the same polynomial mapping from the twisted cubic in $\mathbb{R}^3$ to $\mathbb{R}^2$.
6. Consider the mapping $\phi : \mathbb{R}^2 \to \mathbb{R}^5$ defined by $\phi(u, v) = (u, v, u^2, uv, v^2)$.
   a. The image of ϕ is a variety S known as an affine Veronese surface. Find implicit equations for S.
   b. Show that the projection $\pi : S \to \mathbb{R}^2$ defined by $\pi(x_1, x_2, x_3, x_4, x_5) = (x_1, x_2)$ is the inverse mapping of $\phi : \mathbb{R}^2 \to S$. What does this imply about S and $\mathbb{R}^2$?
7. This problem characterizes the varieties for which $\mathbf{I}(V) = \{0\}$.
   a. Show that if k is an infinite field and $V\subset k^n$ is a variety, then $\mathbf{I}(V)=\{0\}$ if and only if $V = k^n$.
   b. On the other hand, show that if k is finite, then $\mathbf{I}(V)$ is never equal to $\{0\}$. Hint: See Exercise 4 of Chapter 1, §1.
8. Let $V = \mathbf{V}(xy, xz) \subset \mathbb{R}^3$.
   a. Show that neither of the polynomial functions $f = y^2 + z^3$, $g = x^2 - x$ is identically zero on V, but that their product *is* identically zero on V.
   b. Find $V_1 = V \cap \mathbf{V}(f)$ and $V_2 = V \cap \mathbf{V}(g)$ and show that $V = V_1 \cup V_2$.
9. Let V be an irreducible variety and let ϕ, ψ be functions in $k[V]$ represented by polynomials f, g, respectively. Suppose that $\phi \cdot \psi = 0$ in $k[V]$, but that neither ϕ nor ψ is the zero function on V.
   a. Show that $V = (V \cap \mathbf{V}(f)) \cup (V \cap \mathbf{V}(g))$.
   b. Show that neither $V \cap \mathbf{V}(f)$ nor $V \cap \mathbf{V}(g)$ is all of V and deduce a contradiction.
10. In this problem, we will see that there are no nonconstant polynomial mappings from $V = \mathbb{R}$ to $W = \mathbf{V}(y^2 - x^3 + x) \subset \mathbb{R}^2$. Thus, these varieties are not isomorphic (that is, they are not "the same" in the sense introduced in this section).
    a. Suppose $\phi : \mathbb{R} \to W$ is a polynomial mapping represented by $\phi(t) = (a(t), b(t))$ where $a(t), b(t) \in \mathbb{R}[t]$. Explain why it must be true that $b(t)^2 = a(t)(a(t)^2 - 1)$.
    b. Explain why the two factors on the right of the equation in part (a) must be relatively prime in $\mathbb{R}[t]$.
    c. Using the unique factorizations of a and b into products of powers of irreducible polynomials, show that $b^2 = ac^2$ for some polynomial $c(t) \in \mathbb{R}[t]$ relatively prime to a.
    d. From part (c) it follows that $c^2 = a^2 - 1$. Deduce from this equation that c, a, and, hence, b must be constant polynomials.

§2 Quotients of Polynomial Rings

The construction of $k[V]$ given in §1 is a special case of what is called the quotient of $k[x_1, \ldots, x_n]$ modulo an ideal I. From the word *quotient*, you might guess that the issue is to define a division operation, but this is *not* the case. Instead, forming the quotient will indicate the sort of "lumping together" of polynomials that we mentioned in §1 when describing the elements $\phi \in k[V]$. The quotient construction is a fundamental tool in commutative algebra and algebraic geometry, so if you pursue these subjects further, the acquaintance you make with quotient rings here will be valuable.

To begin, we introduce some new terminology.

Definition 1. *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal, and let $f, g \in k[x_1, \ldots, x_n]$. We say f and g are* **congruent modulo** *I, written*

$$f \equiv g \bmod I,$$

if $f - g \in I$.

For instance, if $I = \langle x^2 - y^2, x + y^3 + 1\rangle \subset k[x, y]$, then $f = x^4 - y^4 + x$ and $g = x + x^5 + x^4y^3 + x^4$ are congruent modulo I since

$$\begin{aligned} f - g &= x^4 - y^4 - x^5 - x^4y^3 - x^4 \\ &= (x^2 + y^2)(x^2 - y^2) - (x^4)(x + y^3 + 1) \in I. \end{aligned}$$

The most important property of the congruence relation is given by the following proposition.

Proposition 2. *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. Then congruence modulo I is an equivalence relation on $k[x_1, \ldots, x_n]$.*

Proof. Congruence modulo I is reflexive since $f - f = 0 \in I$ for every $f \in k[x_1, \ldots, x_n]$. To prove symmetry, suppose that $f \equiv g \bmod I$. Then $f - g \in I$, which implies that $g - f = (-1)(f - g) \in I$ as well. Hence, $g \equiv f \bmod I$ also. Finally, we need to consider transitivity. If $f \equiv g \bmod I$ and $g \equiv h \bmod I$, then $f - g, g - h \in I$. Since I is closed under addition, we have $f - h = f - g + g - h \in I$ as well. Hence, $f \equiv h \bmod I$. □

An equivalence relation on a set S partitions S into a collection of disjoint subsets called equivalence classes. For any $f \in k[x_1, \ldots, x_n]$, the class of f is the set

$$[f] = \{g \in k[x_1, \ldots, x_n] : g \equiv f \bmod I\}.$$

The definition of congruence modulo I and Proposition 2 makes sense for *every* ideal $I \subset k[x_1, \ldots, x_n]$. In the special case that $I = \mathbf{I}(V)$ is the ideal of the variety V, then by Proposition 2 of §1, it follows that $f \equiv g \bmod \mathbf{I}(V)$ if and only if f and g define the same function on V. In other words, the "lumping together" of polynomials that define the same function on a variety V is accomplished by passing to the equivalence classes for the congruence relation modulo $\mathbf{I}(V)$. More formally, we have the following proposition.

Proposition 3. *The distinct polynomial functions $\phi : V \to k$ are in one-to-one correspondence with the equivalence classes of polynomials under congruence modulo $\mathbf{I}(V)$.*

Proof. This is a corollary of Proposition 2 of §1 and the (easy) proof is left to the reader as an exercise. □

We are now ready to introduce the quotients mentioned in the title of this section.

Definition 4. *The* **quotient** *of* $k[x_1, \ldots, x_n]$ *modulo I, written* $k[x_1, \ldots, x_n]/I$*, is the set of equivalence classes for congruence modulo I:*

$$k[x_1, \ldots, x_n]/I = \{[f] : f \in k[x_1, \ldots, x_n]\}.$$

For instance, take $k = \mathbb{R}, n = 1$, and $I = \langle x^2 - 2\rangle$. We may ask whether there is some way to describe all the equivalence classes for congruence modulo I. By the division algorithm, every $f \in \mathbb{R}[x]$ can be written as $f = q \cdot (x^2 - 2) + r$, where $r = ax + b$ for some $a, b \in \mathbb{R}$. By the definition, $f \equiv r \bmod I$ since $f - r = q \cdot (x^2 - 2) \in I$. Thus, every element of $\mathbb{R}[x]$ belongs to one of the equivalence classes $[ax + b]$, and $\mathbb{R}[x]/I = \{[ax + b] : a, b \in \mathbb{R}\}$. In §3, we will extend the idea used in this example to a method for dealing with $k[x_1, \ldots, x_n]/I$ in general.

Because $k[x_1, \ldots, x_n]$ is a ring, given any two classes $[f], [g] \in k[x_1, \ldots, x_n]/I$, we can attempt to define sum and product operations *on classes* by using the corresponding operations on elements of $k[x_1, \ldots, x_n]$. That is, we can try to define

$$(1) \qquad \begin{aligned} [f] + [g] &= [f + g] \quad (\text{sum in } k[x_1, \ldots, x_n]), \\ [f] \cdot [g] &= [f \cdot g] \quad (\text{product in } k[x_1, \ldots, x_n]). \end{aligned}$$

We must check, however, that these formulas actually make sense. We need to show that if we choose different $f' \in [f]$ and $g' \in [g]$, then the class $[f' + g']$ is the same as the class $[f + g]$. Similarly, we need to check that $[f' \cdot g'] = [f \cdot g]$.

Proposition 5. *The operations defined in equations* (1) *yields the same classes in* $k[x_1, \ldots, x_n]/I$ *on the right-hand sides no matter which* $f' \in [f]$ *and* $g' \in [g]$ *we use. (We say that the operations on classes given in (1) are* **well-defined** *on classes.)*

Proof. If $f' \in [f]$ and $g' \in [g]$, then $f' = f + a$ and $g' = g + b$, where $a, b \in I$. Hence,

$$f' + g' = (f + a) + (g + b) = (f + g) + (a + b).$$

Since we also have $a + b \in I$ (I is an ideal), it follows that $f' + g' \equiv f + g \bmod I$, so $[f' + g'] = [f + g]$. Similarly,

$$f' \cdot g' = (f + a) \cdot (g + b) = fg + ag + fb + ab.$$

Since $a, b \in I$, we have $ag + fb + ab \in I$. Thus, $f' \cdot g' \equiv f \cdot g \bmod I$, so $[f' \cdot g'] = [f \cdot g]$. □

To illustrate this result, consider the sum and product operations in $\mathbb{R}[x]/\langle x^2 - 2\rangle$. As we saw earlier, the classes $[ax+b]$, $a, b \in \mathbb{R}$ form a complete list of the elements of

$\mathbb{R}[x]/\langle x^2-2\rangle$. The sum operation is defined by $[ax+b]+[cx+d] = [(a+c)x+(b+d)]$. Note that this amounts to the usual vector sum on ordered pairs of real numbers. The product operation is also easily understood. We have

$$\begin{aligned}[ax+b]\cdot[cx+d] &= [acx^2+(ad+bc)x+bd]\\ &= [(ad+bc)x+(bd+2ac)],\end{aligned}$$

as we can see by dividing the quadratic polynomial in the first line by x^2-2 and using the remainder as our representative of the class of the product.

Once we know that the operations in (1) are well-defined, it follows immediately that all of the axioms for a commutative ring are satisfied in $k[x_1,\ldots,x_n]/I$. This is so because the sum and product in $k[x_1,\ldots,x_n]/I$ are defined in terms of the corresponding operations in $k[x_1,\ldots,x_n]$, where we know that the axioms do hold. For example, to check that sums are associative in $k[x_1,\ldots,x_n]/I$, we argue as follows: if $[f],[g],[h]\in k[x_1,\ldots,x_n]/I$, then

$$\begin{aligned}([f]+[g])+[h] &= [f+g]+[h]\\ &= [(f+g)+h] \quad \text{[by (1)]}\\ &= [f+(g+h)] \quad (\text{by associativity in } k[x_1,\ldots,x_n])\\ &= [f]+[g+h]\\ &= [f]+([g]+[h]).\end{aligned}$$

Similarly, commutativity of addition, associativity, and commutativity of multiplication, and the distributive law all follow because polynomials satisfy these properties. The additive identity is $[0]\in k[x_1,\ldots,x_n]/I$, and the multiplicative identity is $[1]\in k[x_1,\ldots,x_n]/I$. To summarize, we have sketched the proof of the following theorem.

Theorem 6. *Let I be an ideal in $k[x_1,\ldots,x_n]$. The quotient $k[x_1,\ldots,x_n]/I$ is a commutative ring under the sum and product operations given in* (1).

Next, given a variety V, we would like to relate the quotient ring $k[x_1,\ldots,x_n]/\mathbf{I}(V)$ to the ring $k[V]$ of polynomial functions on V. It turns out that these two rings are "the same" in the following sense.

Theorem 7. *The one-to-one correspondence between the elements of k[V] and the elements of $k[x_1,\ldots,x_n]/\mathbf{I}(V)$ given in Proposition 3 preserves sums and products.*

Proof. Let $\Phi : k[x_1,\ldots,x_n]/\mathbf{I}(V)\to k[V]$ be the mapping defined by $\Phi([f])=\phi$, where ϕ is the polynomial function represented by f. Since every element of $k[V]$ is represented by some polynomial, we see that Φ is onto. To see that Φ is also one-to-one, suppose that $\Phi([f])=\Phi([g])$. Then by Proposition 3, $f\equiv g \bmod \mathbf{I}(V)$. Hence, $[f]=[g]$ in $k[x_1,\ldots,x_n]/\mathbf{I}(V)$.

To study sums and products, let $[f],[g]\in k[x_1,\ldots,x_n]/\mathbf{I}(V)$. Then $\Phi([f]+[g]) = \Phi([f+g])$ by the definition of sum in the quotient ring. If f represents the polynomial function ϕ and g represents ψ, then $f+g$ represents $\phi+\psi$. Hence,

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

Thus, Φ preserves sums. Similarly,

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

Thus, Φ preserves products as well.

The inverse correspondence Ψ also preserves sums and products by a similar argument, and the theorem is proved. □

The result of Theorem 7 illustrates a basic notion from abstract algebra. The following definition tells us what it means for two rings to be essentially the same.

Definition 8. *Let R, S be commutative rings.*

(i) *A mapping $\phi : R \to S$ is said to be a* **ring isomorphism** *if:*

a. *ϕ preserves sums: $\phi(r+r') = \phi(r) + \phi(r')$ for all $r, r' \in R$.*
b. *ϕ preserves products: $\phi(r\cdot r') = \phi(r)\cdot\phi(r')$ for all $r, r' \in R$.*
c. *ϕ is one-to-one and onto.*

(ii) *Two rings R, S are* **isomorphic** *if there exists an isomorphism $\phi : R \to S$. We write $R \cong S$ to denote that R is isomorphic to S.*

(iii) *A mapping $\phi : R \to S$ is a* **ring homomorphism** *if ϕ satisfies properties (a) and (b) of (i), but not necessarily property (c), and if, in addition, ϕ maps the multiplicative identity $1 \in R$ to $1 \in S$.*

In general, a "homomorphism" is a mapping that preserves algebraic structure. A ring homomorphism $\phi : R \to S$ is a mapping that preserves the addition and multiplication operations in the ring R.

From Theorem 7, we get a ring isomorphism $k[V] \cong k[x_1,\ldots,x_n]/\mathbf{I}(V)$. A natural question to ask is what happens if we replace $\mathbf{I}(V)$ by some other ideal I which defines V. [From Chapter 4, we know that there are *lots* of ideals I such that $V = \mathbf{V}(I)$.] Could it be true that *all* the quotient rings $k[x_1,\ldots,x_n]/I$ are isomorphic to $k[V]$? The following example shows that the answer to this question is *no*. Let $V = \{(0,0)\}$. We saw in Chapter 1, §4 that $\mathbf{I}(V) = \mathbf{I}(\{(0,0)\}) = \langle x, y\rangle$. Thus, by Theorem 7, we have $k[x,y]/\mathbf{I}(V) \cong k[V]$.

Our first claim is that the quotient ring $k[x,y]/\mathbf{I}(V)$ is isomorphic to the field k. The easiest way to see this is to note that a polynomial function on the one-point set $\{(0,0)\}$ can be represented by a constant since the function will have only one function value. Alternatively, we can derive the same fact algebraically by constructing a mapping

$$\Phi : k[x,y]/\mathbf{I}(V) \longrightarrow k$$

by setting $\Phi([f]) = f(0,0)$ (the constant term of the polynomial). We will leave it as an exercise to show that Φ is a ring isomorphism.

Now, let $I = \langle x^3+y^2, 3y^4\rangle \subset k[x,y]$. It is easy to check that $\mathbf{V}(I) = \{(0,0)\} = V$. We ask whether $k[x,y]/I$ is also isomorphic to k. A moment's thought shows that this is not so. For instance, consider the class $[y] \in k[x,y]/I$. Note that $y \notin I$, a fact which can be checked by finding a Groebner basis for I (use any monomial order) and computing a remainder. In the ring $k[x, y]/I$, this shows that $[y] \neq [0]$. But we also have $[y]^4 = [y^4] = [0]$ since $y^4 \in I$. Thus, there is an element of $k[x, y]/I$ which is not zero itself, but whose fourth power is zero. In a field, this is impossible. We conclude that $k[x, y]/I$ is not a field. But this says that $k[x, y]/\mathbf{I}(V)$ and $k[x, y]/I$ cannot be isomorphic rings since one is a field and the other is not. (See Exercise 8.)

In a commutative ring R, an $a \in R$ such that $a^n = 0$ for some $n \geq 1$ is called a *nilpotent element*. The example just given is actually quite representative of the kind of difference that can appear when we compare $k[x_1, \ldots, x_n]/\mathbf{I}(V)$ with $k[x_1, \ldots, x_n]/I$ for another ideal I with $\mathbf{V}(I) = V$. If I is not a radical ideal, there will be elements $f \in \sqrt{I}$ which are not in I itself. Thus, in $k[x_1, \ldots, x_n]/I$, we will have $[f] \neq [0]$, whereas $[f]^n = [0]$ for the $n > 1$ such that $f^n \in I$. The ring $k[x_1, \ldots, x_n]/I$ *will* have nonzero nilpotent elements, whereas $k[x_1, \ldots, x_n]/\mathbf{I}(V)$ never does. $\mathbf{I}(V)$ is always a radical ideal, so $[f]^n = 0$ if and only if $[f] = 0$.

Since a quotient $k[x_1, \ldots, x_n]/I$ is a commutative ring in its own right, we can study other facets of its ring structure as well, and, in particular, we can consider ideals in $k[x_1, \ldots, x_n]/I$. The definition is the same as the definition of ideals in $k[x_1, \ldots, x_n]$.

Definition 9. *A subset I of a commutative ring R is said to be an* **ideal** *in R if it satisfies*

(i) $0 \in I$ *(where 0 is the zero element of R).*
(ii) *If a, b* $\in I$*, then* $a + b \in I$.
(iii) *If* $a \in I$ *and* $r \in R$*, then* $r \cdot a \in I$.

There is a close relation between ideals in the quotient $k[x_1, \ldots, x_n]/I$ and ideals in $k[x_1, \ldots, x_n]$.

Proposition 10. *Let I be an ideal in* $k[x_1, \ldots, x_n]$. *The ideals in the quotient ring* $k[x_1, \ldots, x_n]/I$ *are in one-to-one correspondence with the ideals of* $k[x_1, \ldots, x_n]$ *containing I (that is, the ideals J satisfying* $I \subset J \subset k[x_1, \ldots, x_n]$*).*

Proof. First, we give a way to produce an ideal in $k[x_1, \ldots, x_n]/I$ corresponding to each J containing I in $k[x_1, \ldots, x_n]$. Given an ideal J in $k[x_1, \ldots, x_n]$ containing I, let J/I denote the set $\{[j] \in k[x_1, \ldots, x_n]/I : j \in J\}$. We claim that J/I is an ideal in $k[x_1, \ldots, x_n]/I$. To prove this, first note that $[0] \in J/I$ since $0 \in J$. Next, let $[j], [k] \in J/I$. Then $[j] + [k] = [j + k]$ by the definition of the sum in $k[x_1, \ldots, x_n]/I$. Since $j, k \in J$, we have $j + k \in J$ as well. Hence, $[j] + [k] = J/I$. Finally, if $[j] \in J/I$ and $[r] \in k[x_1, \ldots, x_n]/I$, then $[r] \cdot [j] = [r \cdot j]$ by the definition of the product in $k[x_1, \ldots, x_n]/I$. But $r \cdot j \in J$ since J is an ideal in $k[x_1, \ldots, x_n]$. Hence, $[r] \cdot [j] \in J/I$. As a result, J/I is an ideal in $k[x_1, \ldots, x_n]/I$.

If $\tilde{J} \subset k[x_1, \ldots, x_n]/I$ is an ideal, we next show how to produce an ideal $J \subset k[x_1, \ldots, x_n]$ which contains I. Let $J = \{j \in k[x_1, \ldots, x_n] : [j] \in \tilde{J}\}$. Then we have $I \subset J$ since $[i] = [0] \in \tilde{J}$ for any $i \in I$. It remains to show that J is an ideal of $k[x_1, \ldots, x_n]$. First note that $0 \in I \subset J$. Furthermore, if $j, k \in J$, then $[j], [k] \in \tilde{J}$ implies that $[j] + [k] = [j + k] \in \tilde{J}$. It follows that $j + k \in J$. Finally, if $j \in J$ and

$r \in k[x_1, \ldots, x_n]$, then $[j] \in \tilde{J}$, so $[r][j] = [rj] \in \tilde{J}$. But this says $rj \in J$, and, hence, J is an ideal in $k[x_1, \ldots, x_n]$.

We have thus shown that there are correspondences between the two collections of ideals:

$$\begin{aligned} &\{J : I \subset J \subset k[x_1, \ldots, x_n]\} \qquad \{\tilde{J} \subset k[x_1, \ldots, x_n]/I\} \\ (2) \qquad &\qquad\qquad\qquad J \longrightarrow J/I = \{[j] : j \in J\} \\ &J = \{j : [j] \in \tilde{J}\} \longleftarrow \tilde{J}. \end{aligned}$$

We leave it as an exercise to prove that each of these arrows is the inverse of the other. This gives the desired one-to-one correspondence. □

For example, consider the ideal $I = \langle x^2 - 4x + 3\rangle$ in $R = \mathbb{R}[x]$. We know from Chapter 1 that R is a principal ideal domain. That is, every ideal in R is generated by a single polynomial. The ideals containing I are precisely the ideals generated by polynomials that *divide* $x^2 - 4x + 3$. Hence, the quotient ring R/I has exactly four ideals in this case:

ideals in R/I	ideals in R containing I
$\{[0]\}$	I
$\langle[x-1]\rangle$	$\langle x-1\rangle$
$\langle[x-3]\rangle$	$\langle x-3\rangle$
R/I	R

As in another example earlier in this section, we can compute in R/I by computing remainders with respect to $x^2 - 4x + 3$.

As a corollary of Proposition 10, we deduce the following result about ideals in quotient rings, parallel to the Hilbert Basis Theorem from Chapter 2.

Corollary 11. *Every ideal in the quotient ring $k[x_1, \ldots, x_n]/I$ is finitely generated.*

Proof. Let $\tilde{J}$ be any ideal in $k[x_1, \ldots, x_n]/I$. By Proposition 10, $\tilde{J} = \{[j] : j \in J\}$ for an ideal J in $k[x_1, \ldots, x_n]$ containing I. Then the Hilbert Basis Theorem implies that $J = \langle f_1, \ldots, f_s\rangle$ for some $f_i \in k[x_1, \ldots, x_n]$. But then for any $j \in J$, we have $j = h_1 f_1 + \cdots + h_s f_s$ for some $h_i \in k[x_1, \ldots, x_n]$. Hence,

$$\begin{aligned} [j] &= [h_1 f_1 + \cdots + h_s f_s] \\ &= [h_1][f_1] + \cdots + [h_s][f_s]. \end{aligned}$$

As a result, the classes $[f_1], \ldots, [f_s]$ generate $\tilde{J}$ in $k[x_1, \ldots, x_n]/I$. □

In the next section, we will discuss a more constructive method to study the quotient rings $k[x_1, \ldots, x_n]/I$ and their algebraic properties.

EXERCISES FOR §2

1. Let $I = \langle f_1, \ldots, f_s \rangle \subset k[x_1, \ldots, x_n]$. Describe an algorithm for determining whether $f \equiv g \bmod I$ using techniques from Chapter 2.
2. Prove Proposition 3.
3. Prove Theorem 6. That is, show that the other axioms for a commutative ring are satisfied by $k[x_1, \ldots, x_n]/I$.
4. In this problem, we will give an algebraic construction of a field containing $\mathbb{Q}$ in which 2 has a square root. Note that the field of real numbers is one such field. However, our construction will not make use of the *limit* process necessary, for example, to make sense of an infinite decimal expansion such as the usual expansion $\sqrt{2} = 1.414\ldots$. Instead, we will work with the polynomial $x^2 - 2$.
   a. Show that every $f \in \mathbb{Q}[x]$ is congruent modulo the ideal $I = \langle x^2 - 2 \rangle \subset \mathbb{Q}[x]$ to a unique polynomial of the form $ax + b$, where $a, b \in \mathbb{Q}$.
   b. Show that the class of x in $\mathbb{Q}[x]/I$ is a square root of 2 in the sense that $[x]^2 = [2]$ in $\mathbb{Q}[x]/I$.
   c. Show that $F = \mathbb{Q}[x]/I$ is a field. Hint: Using Theorem 6, the only thing left to prove is that every nonzero element of F has a multiplicative inverse in F.
   d. Find a subfield of F isomorphic to $\mathbb{Q}$.
5. In this problem, we will consider the addition and multiplication operations in the quotient ring $\mathbb{R}[x]/\langle x^2 + 1 \rangle$.
   a. Show that every $f \in \mathbb{R}[x]$ is congruent modulo $I = \langle x^2 + 1 \rangle$ to a unique polynomial of the form $ax + b$, where $a, b \in \mathbb{R}$.
   b. Construct formulas for the addition and multiplication rules in $\mathbb{R}[x]/\langle x^2+1 \rangle$ using these polynomials as the standard representatives for classes.
   c. Do we know another way to describe the ring $\mathbb{R}[x]/(x^2+1)$ (that is, another well-known ring isomorphic to this one?). Hint: What is $[x]^2$?
6. Show that $\mathbb{R}[x]/\langle x^2 - 4x + 3 \rangle$ is not an integral domain.
7. It is possible to define a quotient ring R/I whenever I is an ideal in a commutative ring R. The general construction is the same as the one we have given for $k[x_1, \ldots, x_n]/I$. Here is one simple example.
   a. Let $I = \langle p \rangle$ in $R = \mathbb{Z}$, where p is a prime number. Show that the relation of congruence modulo p, defined by
   $$m \equiv n \bmod p \iff p \text{ divides } m - n$$
   is an equivalence relation on $\mathbb{Z}$, and list the different equivalence classes. We will denote the set of equivalence classes by $\mathbb{Z}/\langle p \rangle$.
   b. Construct sum and product operations in $\mathbb{Z}/\langle p \rangle$ by the analogue of equation (1) and then prove that they are well-defined by adapting the proof of Proposition 5.
   c. Explain why $\mathbb{Z}/\langle p \rangle$ is a commutative ring under the operations you defined in part (b).
   d. Show that the finite field $\mathbb{F}_p$ introduced in Chapter 1 is isomorphic as a ring to $\mathbb{Z}/\langle p \rangle$.
8. In this problem, we study how ring homomorphisms interact with multiplicative inverses in a ring.
   a. Show that every ring isomorphism $\phi : R \to S$ takes the multiplicative identity in R to the multiplicative identity in S, that is $\phi(1) = 1$.
   b. Show that if $r \in R$ has a multiplicative inverse, then for any ring homomorphism $\phi : R \to S$, $\phi(r^{-1})$ is a multiplicative inverse for $\phi(r)$ in the ring S.
   c. Show that if R and S are isomorphic as rings and R is a field, then S is also a field.

9. Prove that the map $f \mapsto f(0,0)$ induces a ring isomorphism $k[x,y]/\langle x,y\rangle \cong k$. Hint: An efficient proof can be given using Exercise 16.
10. This problem illustrates one important use of nilpotent elements in rings. Let $R = k[x]$ and let $I = (x^2)$.
    a. Show that $[x]$ is a nilpotent element in R/I and find the smallest power of $[x]$ which is equal to zero.
    b. Show that every class in R/I has a unique representative of the form $b + a\epsilon$, where $a, b \in k$ and ϵ is shorthand for $[x]$.
    c. Given $b + a\epsilon \in R/I$, we can define a mapping $R \to R/I$ by substituting $x = b + a\epsilon$ in each element $f(x) \in R$. For instance, with $b + a\epsilon = 2 + \epsilon$ and $f(x) = x^2$, we obtain $(2+\epsilon)^2 = 4 + 4\epsilon + \epsilon^2 = 4\epsilon + 4$. Show that
    $$f(b + a\epsilon) = f(b) + a \cdot f'(b)\epsilon, \tag{3}$$
    where f' is the formal derivative of the polynomial f. (Thus, derivatives of polynomials can be constructed in a purely algebraic way.)
    d. Suppose $\epsilon = [x] \in k[x]/\langle x^3\rangle$. Derive a formula analogous to (3) for $f(b + a\epsilon)$.
11. Let R be a commutative ring. Show that the set of nilpotent elements of R forms an ideal in R. Hint: To show that the sum of two nilpotent elements is also nilpotent, you can expand a suitable power $(a+b)^k$ using the distributive law. The result is formally the same as the usual binomial expansion.
12. This exercise will show that the two mappings given in (2) are inverses of each other.
    a. If $I \subset J$ is an ideal of $k[x_1, \ldots, x_n]$, show that $J = \{f \in k[x_1, \ldots, x_n] : [f] \in J/I\}$, where $J/I = \{[j] : j \in J\}$. Explain how your proof uses the assumption $I \subset J$.
    b. If $\tilde{J}$ is an ideal of $k[x_1, \ldots, x_n]/I$, show that $\tilde{J} = \{[f] \in k[x_1, \ldots, x_n]/I : f \in J\}$, where $J = \{j : [j] \in \tilde{J}\}$.
13. Let R and S be commutative rings and let $\phi : R \to S$ be a ring homomorphism.
    a. If $J \subset S$ is an ideal, show that $\phi^{-1}(J)$ is an ideal in R.
    b. If ϕ is an isomorphism of rings, show that there is a one-to-one, inclusion-preserving correspondence between the ideals of R and the ideals of S.
14. This problem studies the ideals in some quotient rings.
    a. Let $I = \langle x^3 - x\rangle \subset R = \mathbb{R}[x]$. Determine the ideals in the quotient ring R/I using Proposition 10. Draw a diagram indicating which of these ideals are contained in which others.
    b. How does your answer change if $I = \langle x^3 + x\rangle$?
15. This problem considers some special quotient rings of $\mathbb{R}[x,y]$.
    a. Let $I = \langle x^2, y^2\rangle \subset \mathbb{R}[x,y]$. Describe the ideals in $\mathbb{R}[x,y]/I$. Hint: Use Proposition 10.
    b. Is $\mathbb{R}[x,y]/\langle x^3, y\rangle$ isomorphic to $\mathbb{R}[x,y]/\langle x^2, y^2\rangle$?
16. Let $\phi : k[x_1, \ldots, x_n] \to S$ be a ring homomorphism. The set $\{r \in k[x_1, \ldots, x_n] : \phi(r) = 0 \in S\}$ is called the *kernel* of ϕ, written $\ker(\phi)$.
    a. Show that $\ker(\phi)$ is an ideal in $k[x_1, \ldots, x_n]$.
    b. Show that the mapping υ from $k[x_1, \ldots, x_n]/\ker(\phi)$ to S defined by $\upsilon([r]) = \phi(r)$ is well-defined in the sense that $\upsilon([r]) = \upsilon([r'])$ whenever $r \equiv r' \bmod \ker(\phi)$.
    c. Show that υ is a ring homomorphism.
    d. (The Isomorphism Theorem) Assume that ϕ is onto. Show that υ is a one-to-one and onto ring homomorphism. As a result, we have $S \cong k[x_1, \ldots, x_n]/\ker(\phi)$ when $\phi : k[x_1, \ldots, x_n] \to S$ is onto.
17. Use Exercise 16 to give a more concise proof of Theorem 7. Consider the mapping $\phi : k[x_1, \ldots, x_n] \to k[V]$ that takes a polynomial to the element of $k[V]$ that it represents. Hint: What is the kernel of ϕ?

§3 Algorithmic Computations in $k[x_1, \ldots, x_n]/I$

In this section, we will use the division algorithm to produce simple representatives of equivalence classes for congruence modulo I, where $I \subset k[x_1, \ldots, x_n]$ is an ideal. These representatives will enable us to develop an explicit method for computing the sum and product operations in a quotient ring $k[x_1, \ldots, x_n]/I$. As an added dividend, we will derive an easily checked criterion to determine when a system of polynomial equations over $\mathbb{C}$ has only *finitely many* solutions.

The basic idea that we will use is a direct consequence of the fact that the remainder on division of a polynomial f by a *Groebner basis* G for an ideal I is uniquely determined by the polynomial f. (This was Proposition 1 of Chapter 2, §6.) Furthermore, we have the following basic observations reinterpreting the result of the division and the form of the remainder.

Proposition 1. *Fix a monomial ordering on* $k[x_1, \ldots, x_n]$ *and let* $I \subset k[x_1, \ldots, x_n]$ *be an ideal. As in Chapter 2, §5,* $\langle \text{LT}(I)\rangle$ *will denote the ideal generated by the leading terms of elements of I.*

(i) *Every* $f \in k[x_1, \ldots, x_n]$ *is congruent modulo* I *to a unique polynomial r which is a k-linear combination of the monomials in the complement of* $\langle \text{LT}(I)\rangle$.

(ii) *The elements of* $\{x^\alpha : x^\alpha \notin \langle \text{LT}(I)\rangle\}$ *are "linearly independent modulo I." That is, if*

$$\sum_\alpha c_\alpha x^\alpha \equiv 0 \bmod I,$$

where the x^α *are all in the complement of* $\langle \text{LT}(I)\rangle$, *then* $c_\alpha = 0$ *for all* α.

Proof. (i) Let G be a Groebner basis for I and let $f \in k[x_1, \ldots, x_n]$. By the division algorithm, the remainder $r = \overline{f}^G$ satisfies $f = q + r$, where $q \in I$. Hence, $f - r = q \in I$, so $f \equiv r \bmod I$. The division algorithm also tells us that r is a k-linear combination of the monomials $x^\alpha \notin \langle \text{LT}(I)\rangle$. The uniqueness of r follows from Proposition 1 of Chapter 2, §6.

(ii) The argument to establish this part of the proposition is essentially the same as the proof of the uniqueness of the remainder in Proposition 1 of Chapter 2, §6. We leave it to the reader to carry out the details. □

Historically, this was actually the first application of Groebner bases. Buchberger's thesis concerned the question of finding "standard sets of representatives" for the classes in quotient rings. We also note that if $I = \mathbf{I}(V)$ for a variety V, Proposition 1 gives standard representatives for the polynomial functions $\phi \in k[V]$.

Example 2. Let $I = \langle xy^3 - x^2, x^3y^2 - y\rangle$ in $\mathbb{R}[x, y]$ and use graded lex order. We find that

$$G = \{x^3y^2 - y, x^4 - y^2, xy^3 - x^2, y^4 - xy\}$$

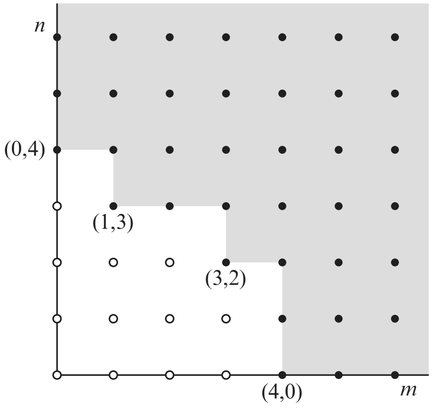
is a Groebner basis for I. Hence, $\langle \text{LT}(I)\rangle = \langle x^3y^2, x^4, xy^3, y^4\rangle$. As in Chapter 2, §4, we can draw a diagram in $\mathbb{Z}^2_{\geq 0}$ to represent the exponent vectors of the monomials in $\langle \text{LT}(I)\rangle$ and its complement as follows. The vectors

$$\begin{aligned}\alpha(1) &= (3, 2),\\ \alpha(2) &= (4, 0),\\ \alpha(3) &= (1, 3),\\ \alpha(4) &= (0, 4)\end{aligned}$$

are the exponent vectors of the generators of $\langle \text{LT}(I)\rangle$. Thus, the elements of

$$((3, 2) + \mathbb{Z}^2_{\geq 0}) \cup ((4, 0) + \mathbb{Z}^2_{\geq 0}) \cup ((1, 3) + \mathbb{Z}^2_{\geq 0}) \cup ((0, 4) + \mathbb{Z}^2_{\geq 0})$$

are the exponent vectors of monomials in $\langle \text{LT}(I)\rangle$. As a result, we can represent the monomials in $\langle \text{LT}(I)\rangle$ by the integer points in the shaded region in $\mathbb{Z}^2_{\geq 0}$ given below:



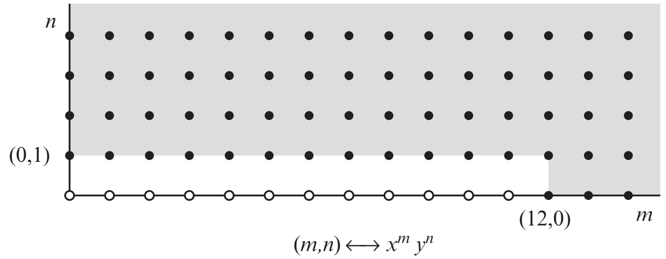
$(m,n) \longleftrightarrow x^m\, y^n$

Given any $f \in \mathbb{R}[x, y]$. Proposition 1 implies that the remainder $\overline{f}^G$ will be a $\mathbb{R}$-linear combination of the 12 monomials $1, x, x^2, x^3, y, xy, x^2y, x^3y, y^2, xy^2, x^2y^2, y^3$ *not* contained in the shaded region. Note that in this case the remainders all belong to a finite-dimensional vector subspace of $\mathbb{R}[x, y]$.

We may also ask what happens if we use a different monomial order in $\mathbb{R}[x, y]$ with the same ideal. If we use lex order instead of grlex, with the variables ordered $y > x$, we find that a Groebner basis in this case is

$$G = \{y - x^7, x^{12} - x^2\}.$$

Hence, for this monomial order, $\langle \text{LT}(I)\rangle = \langle y, x^{12}\rangle$, and $\langle \text{LT}(I)\rangle$ contains all the monomials with exponent vectors in the shaded region on the next page. Thus, for every $f \in \mathbb{R}[x, y]$, we see that $\overline{f}^G \in \text{Span}(1, x, x^2, \ldots, x^{11})$.



Note that $\langle \text{LT}(I) \rangle$ and the remainders can be completely different depending on which monomial order we use. In both cases, however, the possible remainders form the elements of a 12-dimensional vector space. The fact that the dimension is the same in both cases is no accident, as we will soon see. No matter what monomial order we use, for a given ideal I, we will always find the same *number* of monomials in the complement of $\langle \text{LT}(I) \rangle$ (in the case that this number is finite).

Example 3. For the ideal considered in Example 2, there were only finitely many monomials in the complement of $\langle \text{LT}(I) \rangle$. This is actually a very special situation. For instance, consider $I = \langle x - z^2, y - z^3 \rangle \subset k[x, y, z]$. Using lex order, the given generators for I already form a Groebner basis, so that $\langle \text{LT}(I) \rangle = \langle x, y \rangle$. The set of possible remainders modulo I is thus the set of all k-linear combinations of the powers of z. In this case, we recognize I as the ideal of a twisted cubic curve in k^3. As a result of Proposition 1, we see that every polynomial function on the twisted cubic can be uniquely represented by a polynomial in $k[z]$. Hence, the space of possible remainders is not finite-dimensional and $\mathbf{V}(I)$ is a curve. What can you say about $\mathbf{V}(I)$ for the ideal in Example 2?

In any case, we can use Proposition 1 in the following way to describe a portion of the algebraic structure of the quotient ring $k[x_1, \ldots, x_n]/I$.

Proposition 4. *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. Then $k[x_1, \ldots, x_n]/I$ is isomorphic as a k-vector space to $S = \text{Span}(x^\alpha : x^\alpha \notin \langle \text{LT}(I) \rangle)$.*

Proof. By Proposition 1, the mapping $\Phi : k[x_1, \ldots, x_n]/I \to S$ defined by $\Phi([f]) = \overline{f}^G$ defines a one-to-one correspondence between the classes in $k[x_1, \ldots, x_n]/I$ and the elements of S. Hence, it remains to check that Φ preserves the vector space operations. Consider the sum operation in $k[x_1, \ldots, x_n]/I$ introduced in §2. If $[f], [g]$ are elements of $k[x_1, \ldots, x_n]/I$, then using Proposition 1, we can "standardize" our polynomial representatives by computing remainders with respect to a Groebner basis G for I. By Exercise 12 of Chapter 2, §6, we have $\overline{f + g}^G = \overline{f}^G + \overline{g}^G$, so that if

$$\overline{f}^G = \sum_\alpha c_\alpha x^\alpha \quad \text{and} \quad \overline{g}^G = \sum_\alpha d_\alpha x^\alpha$$

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

$$(1) \qquad \overline{f+g}^G = \sum_\alpha (c_\alpha + d_\alpha)x^\alpha.$$

We conclude that with the standard representatives, the sum operation in $k[x_1, \ldots, x_n]/I$ is the same as the vector sum in the k-vector space $S = \text{Span}(x^\alpha : x^\alpha \notin \langle \text{LT}(I)\rangle)$. Further, if $c \in k$, we leave it as an exercise to prove that $\overline{c \cdot f}^G = c \cdot \overline{f}^G$ (this is an easy consequence of the uniqueness part of Proposition 1). It follows that

$$\overline{c \cdot f}^G = \sum_\alpha c c_\alpha x^\alpha,$$

which shows that multiplication by c in $k[x_1, \ldots, x_n]/I$ is the same as scalar multiplication in S. This shows that the map Φ is linear and hence is a vector space isomorphism. □

The product operation in $k[x_1, \ldots, x_n]/I$ is slightly less straightforward. The reason for this is clear, however, if we consider an example. Let I be the ideal

$$I = \langle y + x^2 - 1, xy - 2y^2 + 2y\rangle \subset \mathbb{R}[x, y].$$

If we compute a Groebner basis for I using lex order with $x > y$, then we get

$$(2) \qquad G = \{x^2 + y - 1, xy - 2y^2 + 2y, y^3 - (7/4)y^2 + (3/4)y\}.$$

Thus, $\langle \text{LT}(I)\rangle = \langle x^2, xy, y^3\rangle$, and $\{1, x, y, y^2\}$ forms a basis for the vector space of remainders modulo I. Consider the classes of $f = 3y^2 + x$ and $g = x - y$ in $\mathbb{R}[x, y]/I$. The product of $[f]$ and $[g]$ is represented by $f \cdot g = 3xy^2 + x^2 - 3y^3 - xy$. However, this polynomial cannot be the standard representative of the product function because it contains monomials that are *in* $\langle \text{LT}(I)\rangle$. Hence, we should *divide* again by G, and the remainder $\overline{f \cdot g}^G$ will be the standard representative of the product. We have

$$\overline{3xy^2 + x^2 - 3y^3 - xy}^G = (-11/4)y^2 - (5/4)y + 1,$$

which is in $\text{Span}(1, x, y, y^2)$ as we expect.

The above discussion gives a completely algorithmic way to handle computations in $k[x_1, \ldots, x_n]/I$. To summarize, we have proved the following result.

Proposition 5. *Let I be an ideal in $k[x_1, \ldots, x_n]$ and let G be a Groebner basis for I with respect to any monomial order. For each $[f] \in k[x_1, \ldots, x_n]/I$, we get the standard representative $\overline{f} = \overline{f}^G$ in $S = \text{Span}(x^\alpha : x^\alpha \notin \langle \text{LT}(I)\rangle)$. Then:*

(i) $[f] + [g]$ *is represented by* $\overline{f} + \overline{g}$.

(ii) $[f] \cdot [g]$ *is represented by* $\overline{\overline{f} \cdot \overline{g}}^G \in S$.

We will conclude this section by using the ideas we have developed to give an algorithmic criterion to determine when a variety in $\mathbb{C}^n$ contains only a finite number of points or, equivalently, to determine when a system of polynomial equations has only a finite number of solutions in $\mathbb{C}^n$. (As in Chapter 3, we must work over an algebraically closed field to ensure that we are not "missing" any solutions of the equations with coordinates in a larger field $K \supset k$.)

Theorem 6. *Let $V = \mathbf{V}(I)$ be an affine variety in $\mathbb{C}^n$ and fix a monomial ordering in $\mathbb{C}[x_1, \ldots, x_n]$. Then the following statements are equivalent:*

(i) *V is a finite set.*

(ii) *For each i, $1 \leq i \leq n$, there is some $m_i \geq 0$ such that $x_i^{m_i} \in \langle \mathrm{LT}(I) \rangle$.*

(iii) *Let G be a Groebner basis for I. Then for each i, $1 \leq i \leq n$, there is some $m_i \geq 0$ such that $x_i^{m_i} = \mathrm{LM}(g_i)$ for some $g_i \in G$.*

(iv) *The $\mathbb{C}$-vector space $S = \mathrm{span}(x^\alpha : x^\alpha \notin \langle \mathrm{LT}(I) \rangle)$ is finite-dimensional.*

(v) *The $\mathbb{C}$-vector space $\mathbb{C}[x_1, \ldots, x_n]/I$ is finite-dimensional.*

Proof. (i) ⇒ (ii) If $V = \emptyset$, then $1 \in I$ by the Weak Nullstellensatz. In this case, we can take $m_i = 0$ for all i. If V is nonempty, then for a fixed i, let a_j, $j = 1, \ldots, k$, be the distinct complex numbers appearing as i-th coordinates of points in V. Form the one-variable polynomial

$$f(x_i) = \prod_{j=1}^{k} (x_i - a_j).$$

By construction, f vanishes at every point in V, so $f \in \mathbf{I}(V)$. By the Nullstellensatz, there is some $m \geq 1$ such that $f^m \in I$. But this says that the leading monomial of f^m is in $\langle \mathrm{LT}(I) \rangle$. Examining our expression for f, we see that $x_i^{km} \in \langle \mathrm{LT}(I) \rangle$.

(ii) ⇒ (iii) $x_i^{m_i} \in \langle \mathrm{LT}(I) \rangle$. Since G is a Groebner basis of I, $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g) \rangle : g \in G$. By Lemma 2 of Chapter 2, §4, there is some $g_i \in G$, such that $\mathrm{LT}(g_i)$ divides $x_i^{m_i}$. But this implies that $\mathrm{LT}(g_i)$ is a power of x_i, as claimed. The opposite implication follows directly from the definition of $\langle \mathrm{LT}(g) \rangle$.

(ii) ⇒ (iv) If some power $x_i^{m_i} \in \langle \mathrm{LT}(I) \rangle$ for each i, then the monomials $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ for which some $\alpha_i \geq m_i$ are all in $\langle \mathrm{LT}(I) \rangle$. The monomials in the complement of $\langle \mathrm{LT}(I) \rangle$ must have $\alpha_i \leq m_i - 1$ for each i. As a result, the number of monomials in the complement of $\langle \mathrm{LT}(I) \rangle$ can be at most $m_1 \cdot m_2 \cdots m_n$.

(iv) ⇒ (v) follows from Proposition 4.

(v) ⇒ (i) To show that V is finite, it suffices to show that for each i there can be only finitely many distinct i-th coordinates for the points of V. Fix i and consider the classes $[x_i^j]$ in $\mathbb{C}[x_1, \ldots, x_n]/I$, where $j = 0, 1, 2, \ldots$. Since $\mathbb{C}[x_1, \ldots, x_n]/I$ is finite-dimensional, the $[x_i^j]$ must be linearly *dependent* in $\mathbb{C}[x_1, \ldots, x_n]/I$. That is, there exist constants c_j (not all zero) and some m such that

$$\sum_{j=0}^{m} c_j [x_i^j] = \left[\sum_{j=0}^{m} c_j x_i^j \right] = [0].$$

However, this implies that $\sum_{j=0}^{m} c_j x_i^j \in I$. Since a nonzero polynomial can have only finitely many roots in $\mathbb{C}$, this shows that the points of V have only finitely many different i-th coordinates.

We note that the hypothesis $k = \mathbb{C}$ was used only in showing that (i) $\Rightarrow$ (ii). The other implications are true even if k is not algebraically closed. □

A judicious choice of monomial ordering can sometimes lead to a very easy determination that a variety is finite. For example, consider the ideal

$$I = \langle x^5 + y^3 + z^2 - 1, x^2 + y^3 + z - 1, x^4 + y^5 + z^6 - 1\rangle.$$

Using grlex, we see that $x^5, y^3, z^6 \in \langle \text{LT}(I)\rangle$ since those are the leading monomials of the three generators. By part (ii) of the theorem, we know that $\mathbf{V}(I)$ is finite (even without computing a Groebner basis). If we actually wanted to determine which points were in $\mathbf{V}(I)$, we would need to do elimination, for instance, by computing a lexicographic Groebner basis. This can be a time-consuming calculation, even for a computer algebra system.

The criterion given in part (ii) of Theorem 6 also leads to the following quantitative estimate of the number of solutions of a system of equations when that number is finite.

Proposition 7. *Let $I \subset \mathbb{C}[x_1, \ldots, x_n]$ be an ideal such that for each i, some power $x_i^{m_i} \in \langle \text{LT}(I)\rangle$. Then the number of points of $\mathbf{V}(I)$ is at most $m_1 \cdot m_2 \cdots m_n$.*

Proof. This is an easy consequence of Proposition 8 below. See Exercise 8. □

Here is a pair of examples to illustrate the proposition. First consider the variety $V = \mathbf{V}(I)$, where $I = \langle y - x^7, x^{12} - x\rangle$. For $y > x$, the lexicographic Groebner basis for this ideal is $G = \{y - x^7, x^{12} - x\}$. Hence, in the notation of the theorem, we have $m_1 = 12$ and $m_2 = 1$ as the smallest powers of the two variables contained in $\langle \text{LT}(I)\rangle$. By solving the equations from G, we see that V actually contains $12 = m_1 \cdot m_2$ points in this case:

$$V = \{(0, 0)\} \cup \{(\zeta, \zeta^7) : \zeta^{11} = 1\}.$$

(Recall that there are 11 distinct 11th roots of unity in $\mathbb{C}$.)

On the other hand, consider the variety $V = \mathbf{V}(x^2 + y - 1, xy - 2y^2 + 2y)$ in $\mathbb{C}^2$. From the lexicographic Groebner basis computed in (2) for this ideal, we see that $m_1 = 2$ and $m_2 = 3$ are the smallest powers of x and y, respectively, contained in $\langle \text{LT}(I)\rangle$. However, V contains only $4 < 2 \cdot 3$ points in $\mathbb{C}^2$:

$$V = \{(\pm 1, 0), (0, 1), (-1/2, 3/4)\}.$$

Can you explain the reason(s) for the difference between $m_1 \cdot m_2$ and the cardinality of V in this example?

We can improve the bound given in Proposition 7 as follows.

Proposition 8. *Let $I \subset \mathbb{C}[x_1, \ldots, x_n]$ be an ideal such that $V = \mathbf{V}(I)$ is a finite set.*

(i) *The number of points in V is at most* $\dim(\mathbb{C}[x_1, \ldots, x_n]/I)$ *(where* "dim" *means dimension as a vector space over $\mathbb{C}$).*

(ii) *If I is a radical ideal, then equality holds, i.e., the number of points in V is exactly* $\dim(\mathbb{C}[x_1, \ldots, x_n]/I)$.

Proof. We first show that given distinct points $p_1, \ldots, p_m \in \mathbb{C}^n$, there is a polynomial $f_1 \in \mathbb{C}[x_1, \ldots, x_n]$ with $f_1(p_1) = 1$ and $f_1(p_2) = \cdots = f_1(p_m) = 0$. To prove this, note that if $a \neq b \in \mathbb{C}^n$, then they must differ at some coordinate, say the j-th, and it follows that $g = (x_j - b_j)/(a_j - b_j)$ satisfies $g(a) = 1, g(b) = 0$. If we apply this observation to each pair $p_1 \neq p_i, i \geq 2$, we get polynomials g_i such that $g_i(p_1) = 1$ and $g_i(p_i) = 0$ for $i \geq 2$. Then $f_1 = g_2 \cdot g_3 \cdots g_m$ has the desired property.

In the argument just given, there is nothing special about p_1. If we apply the same argument with p_1 replaced by each of $p_1, \ldots, p_m$ in turn, we get polynomials $f_1, \ldots, f_m$ such that $f_i(p_i) = 1$ and $f_i(p_j) = 0$ for $i \neq j$.

Now we can prove the proposition. Suppose that $V = \{p_1, \ldots, p_m\}$, where the p_i are distinct. Then we get $f_1, \ldots, f_m$ as above. If we can prove that $[f_1], \ldots, [f_m] \in \mathbb{C}[x_1, \ldots, x_n]/I$ are linearly independent, then

$$(3) \qquad m \leq \dim(\mathbb{C}[x_1, \ldots, x_n]/I)$$

will follow, and the first part of the proposition will be proved.

To prove linear independence, suppose that $\sum_{i=1}^m a_i[f_i] = [0]$ in $\mathbb{C}[x_1, \ldots, x_n]/I$, where $a_i \in \mathbb{C}$. Back in $\mathbb{C}[x_1, \ldots, x_n]$, this means that $g = \sum_{i=1}^m a_i f_i \in I$, so that g vanishes at all points of $V = \{p_1, \ldots, p_m\}$. Then, for $1 \leq j \leq m$, we have

$$0 = g(p_j) = \sum_{i=1}^m a_i f_i(p_j) = 0 + a_j f_j(p_j) = a_j,$$

and linear independence follows.

Finally, suppose that I is radical. To prove that equality holds in (3), it suffices to show that $[f_1], \ldots, [f_m]$ form a basis of $\mathbb{C}[x_1, \ldots, x_n]/I$. Since we just proved linear independence, we only need to show that they span. Thus, let $[g] \in \mathbb{C}[x_1, \ldots, x_n]/I$ be arbitrary, and set $a_i = g(p_i)$. Then consider $h = g - \sum_{i=1}^m a_i f_i$. One easily computes $h(p_j) = 0$ for all j, so that $h \in \mathbf{I}(V)$. By the Nullstellensatz, $\mathbf{I}(V) = \mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$ since $\mathbb{C}$ is algebraically closed, and since I is radical, we conclude that $h \in I$. Thus $[h] = [0]$ in $\mathbb{C}[x_1, \ldots, x_n]/I$, which implies $[g] = \sum_{i=1}^m a_i[f_i]$. The proposition is now proved. □

To see why this proposition represents an improvement over Corollary 7, consider Example 2 from the beginning of this section. Using grlex, we found $x^4, y^4 \in \langle \mathrm{LT}(I) \rangle$, so the $\mathbf{V}(I)$ has $\leq 4 \cdot 4 = 16$ points by Corollary 7. Yet Example 2 also shows that $\mathbb{C}[x, y]/I$ has dimension 12 over $\mathbb{C}$. Thus Proposition 8 gives a better bound of 12.

For any ideal I, we have $\mathbf{V}(I) = \mathbf{V}(\sqrt{I})$. Thus, when $\mathbf{V}(I)$ is finite, Proposition 8 shows how to find the exact number of solutions over $\mathbb{C}$, provided we know $\sqrt{I}$. Although radicals are hard to compute in general, $\sqrt{I}$ is relatively easy to find when I satisfies the conditions of Theorem 6. For a description of the algorithm, see Theorem 8.20 of Becker and Weispfenning (1993). This subject (and its relation to solving equations) is also discussed in Cox, Little and O'Shea (1998).

Theorem 6 shows how we can characterize "zero-dimensional" varieties (varieties containing only finitely many points) using the properties of $\mathbb{C}[x_1, \ldots, x_n]/I$. In

Chapter 9, we will take up the general question of assigning a *dimension* to a general variety, and some of the ideas introduced here will be useful.

EXERCISES FOR §3

1. Complete the proof of part (ii) of Proposition 1.
2. In Proposition 5, we stated a method for computing $[f] \cdot [g]$ in $k[x_1, \ldots, x_n]/I$. Could we simply compute $\overline{f \cdot g}^G$ rather than first computing the remainders of f and g separately?
3. Let $I = \langle x^4y - z^6, x^2 - y^3z, x^3z^2 - y^3 \rangle$ in $k[x, y, z]$.
   a. Using lex order, find a Groebner basis G for I and a collection of monomials that spans the space of remainders modulo G.
   b. Repeat part (a) for grlex order. How do your sets of monomials compare?
4. Use the division algorithm and the uniqueness part of Proposition 1 to prove that $\overline{c \cdot f}^G = c \cdot \overline{f}^G$ whenever $f \in [x_1, \ldots, x_n]$ and $c \in k$.
5. Let $I = \langle y + x^2 - 1, xy - 2y^2 + 2y \rangle \subset \mathbb{R}[x, y]$. (This is the ideal used in the example following Proposition 4.)
   a. Construct a vector space isomorphism $\mathbb{R}[x, y]/I \cong \mathbb{R}^4$.
   b. Using the lexicographic Groebner basis given in (2), compute a "multiplication table" for the elements $\{[1], [x], [y], [y^2]\}$ in $\mathbb{R}[x, y]/I$. (Express each product as a linear combination of these four classes.)
   c. Is $\mathbb{R}[x, y]/I$ a field? Why or why not?
6. Let $V = \mathbf{V}(x_3 - x_1^2, x_4 - x_1x_2, x_2x_4 - x_1x_5, x_4^2 - x_3x_5) \subset \mathbb{C}^5$.
   a. Using any convenient monomial order, determine a collection of monomials spanning the space of remainders modulo a Groebner basis for the ideal generated by the defining equations of V.
   b. For which i is there some $m_i \geq 0$ such that $x_i^{m_i} \in \langle \text{LT}(I) \rangle$?
   c. Is V a finite set? Why or why not?
7. Let I be any ideal in $k[x_1, \ldots, x_n]$.
   a. Suppose that $S = \text{Span}(x^\alpha : x^\alpha \notin \langle \text{LT}(I) \rangle)$ is a k-vector space of finite dimension d for some choice of monomial order. Show that the dimension of $k[x_1, \ldots, x_n]/I$ as a k-vector space is equal to d.
   b. Deduce from part (a) that the number of monomials in the complement of $\langle \text{LT}(I) \rangle$ is independent of the choice of the monomial order, when that number is finite.
8. Prove Proposition 7 using Propositions 4 and 8 and the proof of (ii) ⇒ (iv) of Theorem 6.
9. Suppose that $I \subset k[x_1, \ldots, x_n]$ is an ideal such that for each i, $x_i^{m_i} \in \langle \text{LT}(I) \rangle$. State and prove a criterion that can be used to determine when $\mathbf{V}(I)$ contains *exactly* $m_1 \cdot m_2 \cdots m_n$ points in $\mathbb{C}^n$. Does your criterion somehow take the multiplicity of the roots into account?
10. Most computer algebra systems contain routines for simplifying radical expressions. For example, instead of writing
$$r = \frac{1}{x + \sqrt{2} + \sqrt{3}},$$
most systems would allow you to rationalize the denominator and rewrite r as a quotient of polynomials in x, where $\sqrt{2}$ and $\sqrt{3}$ appear in the coefficients only in the numerator. The idea behind one method used here is as follows.
    a. Explain why r can be seen as a rational function in x, whose coefficients are elements of the quotient ring $R = \mathbb{Q}[y_1, y_2]/\langle y_1^2 - 2, y_2^2 - 3 \rangle$. Hint: See Exercise 4 from §2 of this chapter.

b. Compute a Groebner basis G for $I = \langle y_1^2 - 2, y_2^2 - 3\rangle$ and construct a multiplication table for the classes of the monomials spanning the possible remainders modulo G (which should be $\{[1], [y_1], [y_2], [y_1 y_2]\}$).

c. Now, to rationalize the denominator of r, we can try to solve the following equation

$$(4) \qquad (x[1] + [y_1] + [y_2]) \cdot (a_0[1] + a_1[y_1] + a_2[y_2] + a_3[y_1 y_2]) = [1],$$

where a_0, a_1, a_2, a_3 are rational functions of x with rational number coefficients. Multiply out (4) using your table from part (b), match coefficients, and solve the resulting linear equations for a_0, a_1, a_2, a_3. Then

$$a_0[1] + a_1[y_1] + a_2[y_2] + a_3[y_1 y_2]$$

gives the rationalized expression for r.

11. In this problem, we will establish a fact about the number of monomials of total degree less than or equal to d in $k[x_1, \ldots, x_n]$ and relate this to the intuitive notion of the dimension of the variety $V = k^n$.

a. Explain why every monomial in $k[x_1, \ldots, x_n]$ is in the complement of $\langle \mathrm{LT}(\mathbf{I}(V))\rangle$ for $V = k^n$.

b. Show that for all $d, n \geq 0$, the number of distinct monomials of degree less than or equal to d in $k[x_1, \ldots, x_n]$ is the binomial coefficient $\binom{n+d}{n}$. (This generalizes part (a) of Exercise 5 in Chapter 2, §1.)

c. When n is fixed, explain why this number of monomials grows like d^n as $d \to \infty$. Note that the *exponent* n is the same as the intuitive dimension of the variety $V = k^n$, for which $k[V] = k[x_1, \ldots, x_n]$.

12. In this problem, we will compare what happens with the monomials not in $\langle \mathrm{LT}(I)\rangle$ in two examples where $\mathbf{V}(I)$ is not finite, and one where $\mathbf{V}(I)$ is finite.

a. Consider the variety $\mathbf{V}(I) \subset \mathbb{C}^3$, where $I = \langle x^2 + y, x - y^2 + z^2, xy - z\rangle$. Compute a Groebner basis for I using lex order, and, for $1 \leq d \leq 10$, tabulate the number of monomials of degree $\leq d$ that are not in $\langle \mathrm{LT}(I)\rangle$. Note that by Theorem 6, $\mathbf{V}(I)$ is a finite subset of $\mathbb{C}^3$. Hint: It may be helpful to try to visualize or sketch a 3-dimensional analogue of the diagrams in Example 2 for this ideal.

b. Repeat the calculations of part a for $J = \langle x^2 + y, x - y^2 + z^2\rangle$. Here, $\mathbf{V}(J)$ is not finite. How does the behavior of the number of monomials of degree $\leq d$ in the complement of $\langle \mathrm{LT}(J)\rangle$ (as a function of d) differ from the behavior in part (a)?

c. Let $H_J(d)$ be the number of monomials of degree $\leq d$ in the complement of $\langle \mathrm{LT}(J)\rangle$. Can you guess a power k such that $H_J(d)$ will grow roughly like d^k as d grows?

d. Now repeat parts (b) and (c) for the ideal $K = \langle x^2 + y\rangle$.

e. Using the intuitive notion of the dimension of a variety that we developed in Chapter 1, can you see a pattern here? We will return to these questions in Chapter 9.

13. Let k be any field, and suppose $I \subset k[x_1, \ldots, x_n]$ has the property that $k[x_1, \ldots, x_n]/I$ is a finite-dimensional vector space over k.

a. Prove that $\dim(k[x_1, \ldots, x_n]/\sqrt{I}) \leq \dim(k[x_1, \ldots, x_n]/I)$. Hint: Show that $I \subset \sqrt{I}$ induces a map of quotient rings $k[x_1, \ldots, x_n]/I \to k[x_1, \ldots, x_n]/\sqrt{I}$ which is onto.

b. Show that the number of points in $\mathbf{V}(I)$ is at most $\dim(k[x_1, \ldots, x_n]/\sqrt{I})$.

c. Give an example to show that equality need not hold in part (b) when k is not algebraically closed.

§4 The Coordinate Ring of an Affine Variety

In this section, we will apply the algebraic tools developed in §§2 and 3 to study the ring $k[V]$ of polynomial functions on an affine variety $V \subset k^n$. Using the isomorphism $k[V] \cong k[x_1, \ldots, x_n]/\mathbf{I}(V)$ from §2, we will frequently identify $k[V]$ with the quotient ring $k[x_1, \ldots, x_n]/\mathbf{I}(V)$. Thus, given a polynomial $f \in k[x_1, \ldots, x_n]$, we let $[f]$ denote the polynomial function in $k[V]$ represented by f.

In particular, each variable x_i gives a polynomial function $[x_i] : V \to k$ whose value at a point $p \in V$ is the i-th coordinate of p. We call $[x_i] \in k[V]$ the i-th *coordinate function* on V. Then the isomorphism $k[V] \cong k[x_1, \ldots, x_n]/\mathbf{I}(V)$ shows that the coordinate functions generate $k[V]$ in the sense that any polynomial function on V is a k-linear combination of products of the $[x_i]$. This explains the following terminology.

Definition 1. *The* **coordinate ring** *of an affine variety $V \subset k^n$ is the ring $k[V]$.*

Many results from previous sections of this chapter can be rephrased in terms of the coordinate ring. For example:

- Proposition 4 from §1: A variety is irreducible if and only if its coordinate ring is an integral domain.
- Theorem 6 from §3: Over $k = \mathbb{C}$, a variety is finite if and only if its coordinate ring is finite-dimensional as a $\mathbb{C}$-vector space.

In the "algebra–geometry" dictionary of Chapter 4, we related varieties in k^n to ideals in $k[x_1, \ldots, x_n]$. One theme of Chapter 5 is that this dictionary still works if we replace k^n and $k[x_1, \ldots, x_n]$ by a general variety V and its coordinate ring $k[V]$. For this purpose, we introduce the following definitions.

Definition 2. *Let $V \subset k^n$ be an affine variety.*

(i) *For any ideal $J = \langle \phi_1, \ldots, \phi_s \rangle \subset k[V]$, we define*

$$\mathbf{V}_V(J) = \{(a_1, \ldots, a_n) \in V : \phi(a_1, \ldots, a_n) = 0 \textit{ for all } \phi \in J\}.$$

We call $\mathbf{V}_V(J)$ a **subvariety** *of V.*

(ii) *For each subset $W \subset V$, we define*

$$\mathbf{I}_V(W) = \{\phi \in k[V] : \phi(a_1, \ldots, a_n) = 0 \textit{ for all } (a_1, \ldots, a_n) \in W\}.$$

For instance, let $V = \mathbf{V}(z - x^2 - y^2) \subset \mathbb{R}^3$. If we take $J = \langle [x] \rangle \subset \mathbb{R}[V]$, then

$$W = \mathbf{V}_V(J) = \{(0, y, y^2) : y \in \mathbb{R}\} \subset V$$

is a subvariety of V. Note that this is the same as $\mathbf{V}(z - x^2 - y^2, x)$ in $\mathbb{R}^3$. Similarly, if we let $W = \{(1, 1, 2)\} \subset V$, then we leave it as an exercise to show that

$$\mathbf{I}_V(W) = \langle [x - 1], [y - 1] \rangle.$$

Given a fixed affine variety V, we can use $\mathbf{I}_V$ and $\mathbf{V}_V$ to relate subvarieties of V to ideals in $k[V]$. The first result we get is the following.

Proposition 3. *Let $V \subset k^n$ be an affine variety.*

(i) *For each ideal $J \subset k[V]$, $W = \mathbf{V}_V(J)$ is an affine variety in k^n contained in V.*
(ii) *For each subset $W \subset V, \mathbf{I}_V(W)$ is an ideal of $k[V]$.*
(iii) *If $J \subset k[V]$ is an ideal, then $J \subset \sqrt{J} \subset \mathbf{I}_V(V_V(J))$.*
(iv) *If $W \subset V$ is a subvariety, then $W = \mathbf{V}_V(I_V(W))$.*

Proof. To prove (i), we will use the one-to-one correspondence of Proposition 10 of §2 between the ideals of $k[V]$ and the ideals in $k[x_1, \dots, x_n]$ containing $\mathbf{I}(V)$. Let $\tilde{J} = \{f \in k[x_1, \dots, x_n] : [f] \in J\} \subset k[x_1, \dots, x_n]$ be the ideal corresponding to $J \subset k[V]$. Then $\mathbf{V}(\tilde{J}) \subset V$, since $\mathbf{I}(V) \subset \tilde{J}$. But we also have $\mathbf{V}(\tilde{J}) = \mathbf{V}_V(J)$ by definition since the elements of $\tilde{J}$ represent the functions in J on V. Thus, W (considered as a subset of k^n) is an affine variety in its own right.

The proofs of (ii), (iii), and (iv) are similar to arguments given in earlier chapters and the details are left as an exercise. Note that the definition of the radical of an ideal is the same in $k[V]$ as it is in $k[x_1, \dots, x_n]$. □

We can also show that the radical ideals in $k[V]$ correspond to the radical ideals in $k[x_1, \dots, x_n]$ containing $\mathbf{I}(V)$.

Proposition 4. *An ideal $J \subset k[V]$ is radical if and only if the corresponding ideal $\tilde{J} = \{f \in k[x_1, \dots, x_n] : [f] \in J\} \subset k[x_1, \dots, x_n]$ is radical.*

Proof. Assume J is radical, and let $f \in k[x_1, \dots, x_n]$ satisfy $f^m \in \tilde{J}$ for some $m \geq 1$. Then $[f^m] = [f]^m \in J$. Since J is a radical ideal, this implies that $[f] \in J$. Hence, $f \in J$, so $\tilde{J}$ is also a radical ideal. Conversely, if $\tilde{J}$ is radical and $[f]^m \in J$, then $[f^m] \in J$, so $f^m \in \tilde{J}$. Since $\tilde{J}$ is radical, this shows that $f \in \tilde{J}$. Hence, $[f] \in J$ and J is radical. □

Rather than discuss the complete "ideal–variety" correspondence (as we did in Chapter 4), we will confine ourselves to the following result which highlights some of the important properties of the correspondence.

Theorem 5. *Let k be an algebraically closed field and let $V \subset k^n$ be an affine variety.*

(i) (**The Nullstellensatz in** $k[V]$) *If J is any ideal in* $k[V]$, *then*

$$\mathbf{I}_V(\mathbf{V}_V(J)) = \sqrt{J} = \{[f] \in k[V] : [f]^m \in J\}.$$

(ii) *The correspondences*

$$\begin{tikzcd} \left\{\begin{matrix} \textit{affine subvarieties} \\ W \subset V \end{matrix}\right\} \arrow[r, shift left, "\mathbf{I}_V"] & \left\{\begin{matrix} \textit{radical ideals} \\ J \subset k[V] \end{matrix}\right\} \arrow[l, shift left, "\mathbf{V}_V"'] \end{tikzcd}$$

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

(iii) *Under the correspondence given in* (ii), *points of V correspond to maximal ideals of k[V].*

Proof. (i) Let J be an ideal of $k[V]$. By the correspondence of Proposition 10 of §2, J corresponds to the ideal $\tilde{J} \subset k[x_1, \ldots, x_n]$ as in the proof of Proposition 4, where $\mathbf{V}(\tilde{J}) = \mathbf{V}_V(J)$. As a result, if $[f] \in \mathbf{I}_V(\mathbf{V}_V(J))$, then $f \in \mathbf{I}(\mathbf{V}(\tilde{J}))$. By the Nullstellensatz in $k^n, \mathbf{I}(\mathbf{V}(\tilde{J})) = \sqrt{\tilde{J}}$, so $f^m \in \tilde{J}$ for some $m \geq 1$. But then, $[f^m] = [f]^m \in J$, so $[f] \in \sqrt{J}$ in $k[V]$. We have shown that $\mathbf{I}_V(\mathbf{V}_V(J)) \subset \sqrt{J}$. Since the opposite inclusion holds for any ideal, our Nullstellensatz in $k[V]$ is proved.

(ii) follows from (i) as in Chapter 4.

(iii) is proved in the same way as Theorem 11 of Chapter 4, §5. □

Next, we return to the general topic of a *classification* of varieties that we posed in §1. What should it mean for two affine varieties to be "isomorphic"? One reasonable answer is given in the following definition.

Definition 6. *Let $V \subset k^m$ and $W \subset k^n$ be affine varieties. We say that V and W are* **isomorphic** *if there exist polynomial mappings $\alpha : V \to W$ and $\beta : W \to V$ such that $\alpha \circ \beta = \mathrm{id}_W$ and $\beta \circ \alpha = \mathrm{id}_V$. (For any variety V, we write id_V for the identity mapping from V to itself. This is always a polynomial mapping.)*

Intuitively, varieties that *are* isomorphic should share properties such as irreducibility, dimension, etc. In addition, subvarieties of V should correspond to subvarieties of W, and so forth. For instance, saying that a variety $W \subset k^n$ is isomorphic to $V = k^m$ implies that there is a one-to-one and onto polynomial mapping $\alpha : k^m \to W$ with a polynomial inverse. Thus, we have a polynomial *parametrization* of W with especially nice properties! Here is an example, inspired by a technique used in geometric modeling, which illustrates the usefulness of this idea.

Example 7. Let us consider the two surfaces

$$\begin{aligned} Q_1 &= \mathbf{V}(x^2 - xy - y^2 + z^2) = \mathbf{V}(f_1), \\ Q_2 &= \mathbf{V}(x^2 - y^2 + z^2 - z) = \mathbf{V}(f_2) \end{aligned}$$

in $\mathbb{R}^3$. (These might be boundary surfaces of a solid region in a shape we were designing, for example.) To study the *intersection curve* $C = \mathbf{V}(f_1, f_2)$ of the two surfaces, we could proceed as follows. Neither Q_1 nor Q_2 is an especially simple surface, so the intersection curve is fairly difficult to visualize directly. However, as usual, we are *not limited* to using the particular equations f_1, f_2 to define the curve! It is easy to check that $C = \mathbf{V}(f_1, f_1 + cf_2)$, where $c \in \mathbb{R}$ is any nonzero real number. Hence, the surfaces $F_c = \mathbf{V}(f_1 + cf_2)$ also contain C. These surfaces, together with Q_2, are often called the elements of the *pencil* of surfaces determined by Q_1 and Q_2. (A pencil of varieties is a one-parameter family of varieties, parametrized by the points of k. In the above case, the parameter is $c \in \mathbb{R}$.)

If we can find a value of c making the surface F_c particularly simple, then understanding the curve C will be correspondingly easier. Here, if we take $c = -1$, then F_{-1} is defined by

$$\begin{aligned} 0 &= f_1 - f_2 \\ &= z - xy. \end{aligned}$$

The surface $Q = F_{-1} = \mathbf{V}(z - xy)$ is much easier to understand because it is *isomorphic as a variety* to $\mathbb{R}^2$ [as is the graph of any polynomial function $f(x, y)$]. To see this, note that we have polynomial mappings:

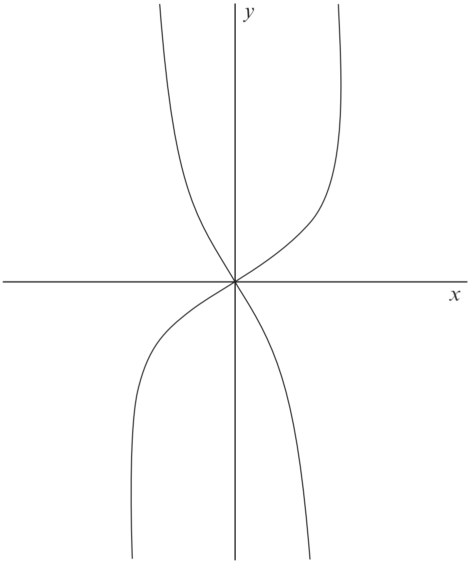
$$\begin{aligned} \alpha : \mathbb{R}^2 &\longrightarrow Q, \\ (x, y) &\mapsto (x, y, xy), \\ \pi : Q &\longrightarrow \mathbb{R}^2, \\ (x, y, z) &\mapsto (x, y), \end{aligned}$$

which satisfy $\alpha \circ \pi = \mathrm{id}_Q$ and $\pi \circ \alpha = \mathrm{id}_{\mathbb{R}^2}$.

Hence, curves on Q can be reduced to plane curves in the following way. To study C, we can project to the curve $\pi(C) \subset \mathbb{R}^2$, and we obtain the equation

$$x^2y^2 + x^2 - xy - y^2 = 0$$

for $\pi(C)$ by substituting $z = xy$ in either f_1 or f_2. Note that π and α restrict to give isomorphisms between C and $\pi(C)$, so we have not really lost anything by projecting in this case.



In particular, each point (a, b) on $\pi(C)$ corresponds to exactly one point (a, b, ab) on C. In the exercises, you will show that $\pi(C)$ can also be parametrized as

$$\begin{aligned} x &= \frac{-t^2 + t + 1}{t^2 + 1}, \\ y &= \frac{-t^2 + t + 1}{t(t + 2)}. \end{aligned} \tag{1}$$

From this we can also obtain a parametrization of C via the mapping α.

Given the above example, it is natural to ask how we can tell whether two varieties are isomorphic. One way is to consider the relation between their coordinate rings

$$k[V] \cong k[x_1, \ldots, x_m]/\mathbf{I}(V) \quad \text{and} \quad k[W] \cong k[y_1, \ldots, y_n]/\mathbf{I}(W).$$

The fundamental observation is that if we have a polynomial mapping $\alpha : V \to W$, then every polynomial function $\phi : W \to k$ in $k[W]$ gives us another polynomial function $\phi \circ \alpha : V \to k$ in $k[V]$. This will give us a map from $k[W]$ to $k[V]$ with the following properties.

Proposition 8. *Let V and W be varieties (possibly in different affine spaces).*

(i) *Let $\alpha : V \to W$ be a polynomial mapping. Then for every polynomial function $\phi : W \to k$, the composition $\phi \circ \alpha : V \to k$ is also a polynomial function. Furthermore, the map $\alpha^* : k[W] \to k[V]$ defined by $\alpha^*(\phi) = \phi \circ \alpha$ is a ring homomorphism which is the identity on the constant functions $k \subset k[W]$. (Note that α^* "goes in the opposite direction" from α since α^* maps functions on W to functions on V. For this reason we call α^* the* **pullback mapping** *on functions.)*

(ii) *Conversely, let $f : k[W] \to k[V]$ be a ring homomorphism which is the identity on constants. Then there is a unique polynomial mapping $\alpha : V \to W$ such that $f = \alpha^*$.*

Proof. (i) Suppose that $V \subset k^m$ has coordinates $x_1, \ldots, x_m$ and $W \subset k^n$ has coordinates $y_1, \ldots, y_n$. Then $\phi : W \to k$ can be represented by a polynomial $f(y_1, \ldots, y_n)$, and $\alpha : V \to W$ can be represented by an n-tuple of polynomials:

$$\alpha(x_1, \ldots, x_m) = (a_1(x_1, \ldots, x_m), \ldots, a_n(x_1, \ldots, x_m)).$$

We compute $\phi \circ \alpha$ by substituting $\alpha(x_1, \ldots, x_m)$ into ϕ. Thus,

$$(\phi \circ \alpha)(x_1, \ldots, x_m) = f(a_1(x_1, \ldots, x_m), \ldots, a_n(x_1, \ldots, x_m)),$$

which is a polynomial in $x_1, \ldots, x_m$. Hence, $\phi \circ \alpha$ is a polynomial function on V.

It follows that we can define $\alpha^* : k[W] \to k[V]$ by the formula $\alpha^*(\phi) = \phi \circ \alpha$. To show that α^* is a ring homomorphism, let ψ be another element of $k[W]$, represented by a polynomial $g(y_1, \ldots, y_n)$. Then

$$\begin{aligned}(\alpha^*(\phi + \psi))(x_1, \ldots, x_m) &= f(a_1(x_1, \ldots, x_m), \ldots, a_n(x_1, \ldots, x_m))\\ &\quad + g(a_1(x_1, \ldots, x_m), \ldots, a_n(x_1, \ldots, x_m))\\ &= \alpha^*(\phi)(x_1, \ldots, x_m) + \alpha^*(\psi)(x_1, \ldots, x_m).\end{aligned}$$

Hence, $\alpha^*(\phi + \psi) = \alpha^*(\phi) + \alpha^*(\psi)$, and $\alpha^*(\phi \cdot \psi) = \alpha^*(\phi) \cdot \alpha^*(\psi)$ is proved similarly. Thus, α^* is a ring homomorphism.

Finally, consider $[a] \in k[W]$ for some $a \in k$. Then $[a]$ is a constant function on W with value a, and it follows that $\alpha^*([a]) = [a] \circ \alpha$ is constant on V, again with value a. Thus, $\alpha^*([a]) = [a]$, so that α^* is the identity on constants.

(ii) Now let $f : k[W] \to k[V]$ be a ring homomorphism which is the identity on the constants. We need to show that f comes from a polynomial mapping $\alpha : V \to W$. Since $W \subset k^n$ has coordinates $y_1, \ldots, y_n$, we get coordinate functions $[y_i] \in k[W]$.

Then $f([y_i]) \in k[V]$, and since $V \subset k^m$ has coordinates $x_1, \ldots, x_m$, we can write $f([y_i]) = [a_i(x_1, \ldots, x_m)] \in k[V]$ for some polynomial $a_i \in k[x_1, \ldots, x_m]$. Then consider the polynomial mapping

$$\alpha = (a_1(x_1, \ldots, x_m), \ldots, a_n(x_1, \ldots, x_m)).$$

We need to show that α maps V to W and that $f = \alpha^*$.

Given any polynomial $F \in k[y_1, \ldots, y_n]$, we first claim that

$$[F \circ \alpha] = f([F]) \tag{2}$$

in $k[V]$. To prove this, note that

$$[F \circ \alpha] = [F(a_1, \ldots, a_n)] = F([a_1], \ldots, [a_n]) = F(f([y_1]), \ldots, f([y_n])),$$

where the second equality follows from the definition of sum and product in $k[V]$, and the third follows from $[a_i] = f([y_i])$. But $[F] = [F(y_1, \ldots, y_n)]$ is a k-linear combination of products of the $[y_i]$, so that

$$F(f([y_1]), \ldots, f([y_n])) = f([F(y_1, \ldots, y_n)]) = f([F])$$

since f is a ring homomorphism which is the identity on k (see Exercise 10). Equation (2) follows immediately.

We can now prove that α maps V to W. Given a point $(c_1, \ldots, c_m) \in V$, we must show that $\alpha(c_1, \ldots, c_m) \in W$. If $F \in \mathbf{I}(W)$, then $[F] = 0$ in $k[W]$, and since f is a ring homomorphism, we have $f([F]) = 0$ in $k[V]$. By (2), this implies that $[F \circ \alpha]$ is the zero function on V. In particular,

$$[F \circ \alpha](c_1, \ldots, c_m) = F(\alpha(c_1, \ldots, c_m)) = 0.$$

Since F was an arbitrary element of $\mathbf{I}(W)$, this shows $\alpha(c_1, \ldots, c_m) \in W$, as desired.

Once we know α maps V to W, equation (2) implies that $[F] \circ \alpha = f([F])$ for any $[F] \in k[W]$. Since $\alpha^*([F]) = [F] \circ \alpha$, this proves $f = \alpha^*$. It remains to show that α is uniquely determined. So suppose we have $\beta : V \to W$ such that $f = \beta^*$. If β is represented by

$$\beta(x_1, \ldots, x_m) = (b_1(x_1, \ldots, x_m), \ldots, b_n(x_1, \ldots, x_m)),$$

then note that $\beta^*([y_i]) = [y_i] \circ \beta = [b_i(x_1, \ldots, x_m)]$. A similar computation gives $\alpha^*([y_i]) = [a_i(x_1, \ldots, x_m)]$, and since $\alpha^* = f = \beta^*$, we have $[a_i] = [b_i]$ for all i. Then a_i and b_i give the same polynomial function on V, and, hence, $\alpha = (a_1, \ldots, a_n)$ and $\beta = (b_1, \ldots, b_n)$ define the same mapping on V. This shows $\alpha = \beta$, and uniqueness is proved. □

Now suppose that $\alpha : V \to W$ and $\beta : W \to V$ are inverse polynomial mappings. Then $\alpha \circ \beta = \mathrm{id}_W$, where $\mathrm{id}_W : W \to W$ is the identity map. By general properties of functions, this implies $(\alpha \circ \beta)^*(\phi) = \mathrm{id}_W^*(\phi) = \phi \circ \mathrm{id}_W = \phi$ for all $\phi \in k[W]$. However, we also have

$$\begin{aligned}(\alpha \circ \beta)^*(\phi) &= \phi \circ (\alpha \circ \beta) = (\phi \circ \alpha) \circ \beta \\ &= \alpha^*(\phi) \circ \beta = \beta^*(\alpha^*(\phi)) = (\beta^* \circ \alpha^*)(\phi).\end{aligned} \tag{3}$$

Hence, $(\alpha \circ \beta)^* = \beta^* \circ \alpha^* = \mathrm{id}_{k[W]}$ as a mapping from $k[W]$ to itself. Similarly, one can show that $(\beta \circ \alpha)^* = \alpha^* \circ \beta^* = \mathrm{id}_{k[V]}$. This proves the first half of the following theorem.

Theorem 9. *Two affine varieties $V \subset k^m$ and $W \subset k^n$ are isomorphic if and only if there is an isomorphism $k[V] \cong k[W]$ of coordinate rings which is the identity on constant functions.*

Proof. The above discussion shows that if V and W are isomorphic varieties, then $k[V] \to k[W]$ as rings. Proposition 8 shows that the isomorphism is the identity on constants.

For the converse, we must show that if we have a ring isomorphism $f : k[W] \to k[V]$ which is the identity on k, then f and f^{-1} "come from" inverse polynomial mappings between V and W. By part (ii) of Proposition 8, we know that $f = \alpha^*$ for some $\alpha : V \to W$ and $f^{-1} = \beta^*$ for $\beta : W \to V$. We need to show that α and β are inverse mappings. First consider the composite map $\alpha \circ \beta : W \to W$. This is clearly a polynomial map, and, using the argument from (3), we see that for any $\phi \in k[W]$,

$$(\alpha \circ \beta)^*(\phi) = \beta^*(\alpha^*(\phi)) = f^{-1}(f(\phi)) = \phi. \tag{4}$$

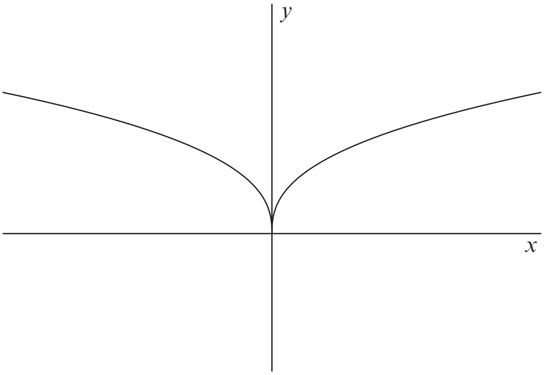
It is also easy to check that the identity map $\mathrm{id}_W : W \to W$ is a polynomial map on W, and we saw above that $\mathrm{id}_W^*(\phi) = \phi$ for all $\phi \in k[W]$. From (4), we conclude that $(\alpha \circ \beta)^* = \mathrm{id}_W^*$, and then $\alpha \circ \beta = \mathrm{id}_W$ follows from the uniqueness statement of part (ii) of Proposition 8. In a similar way, one proves that $\beta \circ \alpha = \mathrm{id}_V$, and hence α and β are inverse mappings. This completes the proof of the theorem. □

We conclude with several examples to illustrate isomorphisms of varieties and the corresponding isomorphisms of their coordinate rings.

Let A be an invertible $n \times n$ matrix with entries in k and consider the linear mapping $L_A : k^n \to k^n$ defined by $L_A(x) = Ax$, where Ax is the matrix product. From Exercise 9 of Chapter 4, §1, we know that L_A^* is a ring isomorphism from $k[x_1, \ldots, x_n]$ to itself. Hence, by the theorem, L_A is an isomorphism of varieties taking k^n to itself. (Such isomorphisms are often called *automorphisms* of a variety.) In Exercise 9, you will show that if V is any subvariety of k^n, then $L_A(V)$ is a subvariety of k^n isomorphic to V since L_A restricts to give an isomorphism of V onto $L_A(V)$. For example, the curve we studied in the final example of §1 of this chapter was obtained from the "standard" twisted cubic curve in $\mathbb{C}^3$ by an invertible linear mapping. Refer to equation (5) of §1 and see if you can identify the mapping L_A that was used.

Next, let $f(x, y) \in k[x, y]$ and consider the *graph* of the polynomial function on k^2 given by f [that is, the variety $V = \mathbf{V}(z - f(x, y)) \subset k^3$]. Generalizing what we said concerning the variety $\mathbf{V}(z - xy)$ in analyzing the curve given in Example 7, it will always be the case that a graph V is isomorphic as a variety to k^2. The reason is that the projection on the (x, y)-plane $\pi : V \to k^2$, and the parametrization of the graph given by $\alpha : k^2 \to V, \alpha(x, y) = (x, y, f(x, y))$ are inverse mappings. The isomorphism of coordinate rings corresponding to α just consists of substituting $z = f(x, y)$ into every polynomial function $F(x, y, z)$ on V.

Finally, consider the curve $V = \mathbf{V}(y^5 - x^2)$ in $\mathbb{R}^2$.



We claim that V is *not* isomorphic to $\mathbb{R}$ as a variety, even though there is a one-to-one polynomial mapping from V to $\mathbb{R}$ given by projecting V onto the x-axis. The reason lies in the coordinate ring of $V : \mathbb{R}[V] = \mathbb{R}[x, y]/\langle y^5 - x^2\rangle$. If there were an isomorphism $\alpha : \mathbb{R} \to V$, then the "pullback" $\alpha^* : \mathbb{R}[V] \to \mathbb{R}[u]$ would be a ring isomorphism given by

$$\alpha^*([x]) = c(u),$$
$$\alpha^*([y]) = d(u),$$

where $c(u), d(u) \in \mathbb{R}[u]$ are polynomials. Since $y^5 - x^2$ represents the zero function on V, we must have $\alpha^*([y^5 - x^2]) = (d(u))^5 - (c(u))^2 = 0$ in $\mathbb{R}[u]$.

We may assume that $c(0) = d(0) = 0$ since the parametrization α can be "arranged" so that $\alpha(0) = (0, 0) \in V$. But then let us examine the possible polynomial solutions

$$c(u) = c_1u + c_2u^2 + \cdots, \quad d(u) = d_1u + d_2u^2 + \cdots$$

of the equation $(c(u))^2 = (d(u))^5$. Since $(d(u))^5$ contains no power of u lower than u^5, the same must be true of $(c(u))^2$. However,

$$(c(u))^2 = c_1^2u^2 + 2c_1c_2u^3 + (c_2^2 + 2c_1c_3)u^4 + \cdots .$$

The coefficient of u^2 must be zero, which implies $c_1 = 0$. The coefficient of u^4 must also be zero, which implies $c_2 = 0$ as well. Since $c_1, c_2 = 0$, the smallest power of u that can appear in c^2 is u^6, which implies that $d_1 = 0$ also.

It follows that u cannot be in the image of α^* since the image of α^* consists of polynomials in $c(u)$ and $d(u)$. This is a contradiction since α^* was supposed to be a ring isomorphism *onto* $\mathbb{R}[u]$. Thus, our two varieties are not isomorphic. In the exercises, you will derive more information about $\mathbb{R}[V]$ by the method of §3 to yield another proof that $\mathbb{R}[V]$ is not isomorphic to a polynomial ring in one variable.

EXERCISES FOR §4

1. Let C be the twisted cubic curve in k^3.
   a. Show that C is a subvariety of the surface $S = \mathbf{V}(xz - y^2)$.
   b. Find an ideal $J \subset k[S]$ such that $C = \mathbf{V}_S(J)$.

2. Let $V \subset \mathbb{C}^n$ be a nonempty affine variety.
   a. Let $\phi \in \mathbb{C}[V]$. Show that $\mathbf{V}_V(\phi) = \emptyset$ if and only if ϕ is invertible in $\mathbb{C}[V]$ (which means that there is some $\psi \in \mathbb{C}[V]$ such that $\phi\psi = [1]$ in $\mathbb{C}[V]$).
   b. Is the statement of part (a) true if we replace $\mathbb{C}$ by $\mathbb{R}$? If so, prove it; if not, give a counterexample.
3. Prove parts (ii), (iii), and (iv) of Proposition 3.
4. Let $V = \mathbf{V}(y - x^n, z - x^m)$, where m, n are any integers ≥ 1. Show that V is isomorphic as a variety to k by constructing explicit inverse polynomial mappings $\alpha : k \to V$ and $\beta : V \to k$.
5. Show that any surface in k^3 with a defining equation of the form $x - f(y, z) = 0$ or $y - g(x, z) = 0$ is isomorphic as a variety to k^2.
6. Let V be a variety in k^n defined by a single equation of the form $x_n - f(x_1, \ldots, x_{n-1}) = 0$. Show that V is isomorphic as a variety to k^{n-1}.
7. In this exercise, we will derive the parametrization (1) for the projected curve $\pi(C)$ from Example 7.
   a. Show that every hyperbola in $\mathbb{R}^2$ whose asymptotes are horizontal and vertical and which passes through the points (0, 0) and (1, 1) is defined by an equation of the form
   $$xy + tx - (t+1)y = 0$$
   for some $t \in \mathbb{R}$.
   b. Using a computer algebra system, compute a Groebner basis for the ideal generated by the equation of $\pi(C)$, and the above equation of the hyperbola. Use lex order with the variables ordered $x > y > t$.
   c. The Groebner basis will contain one polynomial depending on y, t only. By collecting powers of y and factoring, show that this polynomial has $y = 0$ as a double root, $y = 1$ as a single root, and one root which depends on $t : y = \frac{-t^2+t+1}{t(t+2)}$.
   d. Now consider the other elements of the basis and show that for the "movable" root from part (c) there is a unique corresponding x value given by the first equation in (1).

The method sketched in Exercise 7 probably seems exceedingly *ad hoc*, but it is an example of a general pattern that can be developed with some more machinery concerning algebraic curves. Using the complex projective plane to be introduced in Chapter 8, it can be shown that $\pi(C)$ is contained in a projective algebraic curve with *three* singular points similar to the one at (0, 0) in the sketch. Using the family of conics passing through all three singular points and any one additional point, we can give a rational parametrization for *any* irreducible quartic curve with three singular points as in this example. However, *nonsingular* quartic curves have no such parametrizations.

8. Let $Q_1 = \mathbf{V}(x^2 + y^2 + z^2 - 1)$, and $Q_2 = \mathbf{V}((x - 1/2)^2 - 3y^2 - 2z^2)$ in $\mathbb{R}^3$.
   a. Using the idea of Example 7 and Exercise 5, find a surface in the pencil defined by Q_1 and Q_2 that is isomorphic as a variety to $\mathbb{R}^2$.
   b. Describe and/or sketch the intersection curve $Q_1 \cap Q_2$.
9. Let $\alpha : V \to W$ and $\beta : W \to V$ be inverse polynomial mappings between two isomorphic varieties V and W. Let $U = \mathbf{V}_V(I)$ for some ideal $I \subset k[V]$. Show that $\alpha(U)$ is a subvariety of W and explain how to find an ideal $J \subset k[W]$ such that $\alpha(U) = \mathbf{V}_W(J)$.
10. Let $f : k[V] \to k[W]$ be a ring homomorphism of coordinate rings which is the identity on constants. Suppose that $V \subset k^m$ with coordinates $x_1, \ldots, x_m$. If $F \in k[x_1, \ldots, x_m]$, then prove that $f([F]) = F(f([x_1]), \ldots, f([x_m]))$. Hint: Express $[F]$ as a k-linear combination of products of the $[x_i]$.
11. This exercise will study the example following Definition 2 where $V = \mathbf{V}(z - x^2 - y^2) \subset \mathbb{R}^3$.

a. Show that the subvariety $W = \{(1, 1, 2)\} \subset V$ is equal to $\mathbf{V}_V([x-1], [y-1])$. Explain why this implies that $\langle [x-1], [y-1] \rangle \subset \mathbf{I}_V(W)$.
b. Prove that $\langle [x-1], [y-1] \rangle = \mathbf{I}_V(W)$. Hint: Show that V is isomorphic to $\mathbb{R}^2$ and use Exercise 9.

12. Let $V = \mathbf{V}(y^2 - 3x^2z + 2) \subset \mathbb{R}^3$ and let L_A be the linear mapping on $\mathbb{R}^3$ defined by the matrix

$$A = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

a. Verify that L_A is an isomorphism from $\mathbb{R}^3$ to $\mathbb{R}^3$.
b. Find the equation of the image of V under L_A.

13. In this exercise, we will rotate the twisted cubic in $\mathbb{R}^3$.

a. Find the matrix A of the linear mapping on $\mathbb{R}^3$ that rotates every point through an angle of $\pi/6$ counterclockwise about the z-axis.
b. What are the equations of the image of the standard twisted cubic curve under the linear mapping defined by the rotation matrix A?

14. This exercise will outline another proof that $V = \mathbf{V}(y^5 - x^2) \subset \mathbb{R}^2$ is not isomorphic to $\mathbb{R}$ as a variety. This proof will use the algebraic structure of $\mathbb{R}[V]$. We will show that there is no ring isomorphism from $\mathbb{R}[V]$ to $\mathbb{R}[t]$. (Note that $\mathbb{R}[t]$ is the coordinate ring of $\mathbb{R}$.)

a. Using the techniques of §3, explain how each element of $\mathbb{R}[V]$ can be uniquely represented by a polynomial of the form $a(y) + b(y)x$, where $a, b \in \mathbb{R}[y]$.
b. Express the product $(a + bx)(a' + b'x)$ in $\mathbb{R}[V]$ in the form given in part (a).
c. Aiming for a contradiction, suppose that there were some ring isomorphism $\alpha : \mathbb{R}[t] \to \mathbb{R}[V]$. Since α is assumed to be onto, $x = \alpha(f(t))$ and $y = \alpha(g(t))$ for some polynomials f, g. Using the unique factorizations of f, g and the product formula from part (b), deduce a contradiction.

15. Let $V \subset \mathbb{R}^3$ be the tangent surface of the twisted cubic curve.

a. Show that the usual parametrization of V sets up a one-to-one correspondence between the points of V and the points of $\mathbb{R}^2$. Hint: Recall the discussion of V in Chapter 3, §3. In light of part (a), it is natural to ask whether V is *isomorphic* to $\mathbb{R}^2$. We will show that the answer to this question is *no*.
b. Show that V is singular at each point on the twisted cubic curve by using the method of Exercise 12 of Chapter 3, §4. (The tangent surface has what is called a "cuspidal edge" along this curve.)
c. Show that if $\alpha : \mathbb{R}^2 \to V$ is *any* polynomial parametrization of V, and $\alpha(a, b)$ is contained in the twisted cubic itself, then the derivative matrix of α must have rank strictly less than 2 at (a, b) (in other words, the columns of the derivative matrix must be linearly dependent there). (Note: α need not be the standard parametrization, although the statement will be true also for that parametrization.)
d. Now suppose that the polynomial parametrization α has a polynomial inverse mapping $\beta : V \to \mathbb{R}^2$. Using the chain rule from multivariable calculus, show that part (c) gives a contradiction if we consider (a, b) such that $\alpha(a, b)$ is on the twisted cubic.

§5 Rational Functions on a Variety

The ring of integers can be embedded in many fields. The *smallest* of these is the field of rational numbers $\mathbb{Q}$ because $\mathbb{Q}$ is formed by constructing fractions $\frac{m}{n}$, where $m, n \in \mathbb{Z}$.

Nothing more than integers was used. Similarly, the polynomial ring $k[x_1, \ldots, x_n]$ is included as a subring in the field of *rational functions*

$$k(x_1, \ldots, x_n) = \left\{ \frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} : f, g \in k[x_1, \ldots, x_n], g \neq 0 \right\}.$$

Generalizing these examples, if R is any integral domain, then we can form what is called the *quotient field*, or *field of fractions* of R, denoted $QF(R)$. The elements of $QF(R)$ are thought of as "fractions" r/s, where $r, s \in R$ and $s \neq 0$. We add and multiply elements of $QF(R)$ as we do rational numbers or rational functions:

$$r/s + t/u = (ru + ts)/su \quad \text{and} \quad r/s \cdot t/u = rt/su.$$

Note that the assumption that R is an integral domain ensures that the denominators of the sum and product will be nonzero. In addition, two of these fractions r/s and r'/s' represent the same element in the field of fractions if $rs' = r's$. It can be checked easily that $QF(R)$ satisfies all the axioms of a field (see Exercise 1). Furthermore, $QF(R)$ contains the subset $\{r/1 : r \in R\}$ which is a subring isomorphic to R itself. Hence, the terminology "quotient field, or field of fractions of R" is fully justified.

Now if $V \subset k^n$ is an *irreducible* variety, then we have seen in §1 that the coordinate ring $k[V]$ is an integral domain. The field of fractions $QF(k[V])$ is given the following name.

Definition 1. *Let V be an irreducible affine variety in k^n. We call $QF(k[V])$ the* **function field** *(or* **field of rational functions***) on V, and we denote this field by $k(V)$.*

Note the consistency of our notation. We use $k[x_1, \ldots, x_n]$ for a polynomial ring and $k[V]$ for the coordinate ring of V. Similarly, we use $k(x_1, \ldots, x_n)$ for a rational function field and $k(V)$ for the function field of V.

We can write the function field $k(V)$ of $V \subset k^n$ explicitly as

$$\begin{aligned} k(V) &= \{\phi/\psi : \phi, \psi \in k[V], \psi \neq 0\} \\ &= \{[f]/[g] : f, g \in k[x_1, \ldots, x_n], g \notin \mathbf{I}(V)\}. \end{aligned}$$

As with any rational function, we must be careful to avoid zeros of the denominator if we want a well-defined function value in k. Thus, an element $\phi/\psi \in k(V)$ defines a function only on the complement of $\mathbf{V}_V(\psi)$.

The most basic example of the function field of a variety is given by $V = k^n$. In this case, we have $k[V] = k[x_1, \ldots, x_n]$ and, hence,

$$k(V) = k(x_1, \ldots, x_n).$$

We next consider some more complicated examples.

Example 2. In §4, we showed that the curve

$$V = \mathbf{V}(y^5 - x^2) \subset \mathbb{R}^2$$

is not isomorphic to $\mathbb{R}$ because the coordinate rings of V and $\mathbb{R}$ are not isomorphic. Let us see what we can say about the function field of V. To begin, note that by the method of §2, we can represent the elements of $\mathbb{R}[V]$ by remainders modulo $G = \{y^5 - x^2\}$, which is a Groebner basis for $\mathbf{I}(V)$ with respect to lex order with $x > y$ in $\mathbb{R}[x, y]$. Then $\mathbb{R}[V] = \{a(y) + xb(y) : a, b \in \mathbb{R}[y]\}$ as a real vector space, and multiplication is defined by

$$(a + xb) \cdot (c + xd) = (ac + y^5 \cdot bd) + x(ad + bc). \tag{1}$$

In Exercise 2, you will show that V is irreducible, so that $\mathbb{R}[V]$ is an integral domain.

Now, using this description of $\mathbb{R}[V]$, we can also describe the function field $\mathbb{R}(V)$ as follows. If $c + xd \neq 0$ in $\mathbb{R}[V]$, then in the function field we can write

$$\begin{aligned}\frac{a+xb}{c+xd} &= \frac{a+xb}{c+xd} \cdot \frac{c-xd}{c-xd}\\ &= \frac{(ac - y^5bd) + x(bc - ad)}{c^2 - y^5d^2}\\ &= \frac{ac - y^5bd}{c^2 - y^5d^2} + x\frac{bc - ad}{c^2 - y^5d^2}.\end{aligned}$$

This is an element of $\mathbb{R}(y) + x\mathbb{R}(y)$. Conversely, it is clear that every element of $\mathbb{R}(y)+x\mathbb{R}(y)$ defines an element of $\mathbb{R}(V)$. Hence, the field $\mathbb{R}(V)$ can be identified with the set of functions $\mathbb{R}(y)+x\mathbb{R}(y)$, where the addition and multiplication operations are defined as before in $\mathbb{R}[V]$, only using rational functions of y rather than polynomials.

Now consider the mappings:

$$\begin{aligned}\alpha &: V \longrightarrow \mathbb{R},\ (x, y) \mapsto x/y^2,\\ \beta &: \mathbb{R} \longrightarrow V,\ u \mapsto (u^5, u^2).\end{aligned}$$

Note that α is defined except at $(0, 0) \in V$, whereas β is a polynomial parametrization of V. As in §4, we can use α and β to define mappings "going in the opposite direction" on functions. However, since α itself is defined as a rational function, we will not stay within $\mathbb{R}[V]$ if we compose α with a function in $\mathbb{R}[u]$. Hence, we will consider the maps

$$\begin{aligned}\alpha^* &: \mathbb{R}(u) \longrightarrow \mathbb{R}(V),\ f(u) \mapsto f(x/y^2),\\ \beta^* &: \mathbb{R}(V) \longrightarrow \mathbb{R}(u),\ a(y) + xb(y) \mapsto a(u^2) + u^5b(u^2).\end{aligned}$$

We claim that α^* and β^* are inverse ring isomorphisms. That α^* and β^* preserve sums and products follows by the argument given in the proof of Proposition 8 from §4. To check that α^* and β^* are inverses, first we have that for any $f(u) \in \mathbb{R}(u)$, $\alpha^*(f) = f(x/y^2)$. Hence, $\beta^*(\alpha^*(f)) = f(u^5/(u^2)^2) = f(u)$. Therefore, $\beta^* \circ \alpha^*$ is the identity on $\mathbb{R}(u)$. Similarly, if $a(y) + xb(y) \in \mathbb{R}(V)$, then $\beta^*(a + xb) = a(u^2) + u^5b(u^2)$, so

$$\begin{aligned}\alpha^*(\beta^*(a + xb)) &= a((x/y^2)^2) + (x/y^2)^5b((x/y^2)^2)\\ &= a(x^2/y^4) + (x^5/y^{10})b(x^2/y^4).\end{aligned}$$

However, in $\mathbb{R}(V)$, $x^2 = y^5$, so $x^2/y^4 = y$, and $x^5/y^{10} = xy^{10}/y^{10} = x$. Hence, $\alpha^* \circ \beta^*$ is the identity on $\mathbb{R}(V)$. Thus, α^*, β^* define ring isomorphisms between the *function fields* $\mathbb{R}(V)$ and $\mathbb{R}(u)$.

Example 2 shows that it is possible for two varieties to have the same (i.e., isomorphic) function fields, even when they are not isomorphic. It also gave us an example of a rational mapping between two varieties. Before we give a precise definition of a rational mapping, let us look at another example.

Example 3. Let $Q = \mathbf{V}(x^2 + y^2 - z^2 - 1)$, a hyperboloid of one sheet in $\mathbb{R}^3$, and let $W = \mathbf{V}(x + 1)$, the plane $x = -1$. Let $p = (1, 0, 0) \in Q$. For any $q \in Q - \{p\}$, we construct the line L_q joining p and q, and we define a mapping ϕ to W by setting

$$\phi(q) = L_q \cap W$$

if the line intersects W. (If the line does not intersect W, then $\phi(q)$ is undefined.) We can find an algebraic formula for ϕ as follows. If $q = (x_0, y_0, z_0) \in Q$, then L_q is given in parametric form by

$$\begin{aligned} x &= 1 + t(x_0 - 1),\\ y &= ty_0,\\ z &= tz_0. \end{aligned} \tag{2}$$

At $\phi(q) = L_q \cap W$, we must have $1 + t(x_0 - 1) = -1$, so $t = \frac{-2}{x_0-1}$. From (2), it follows that

$$\phi(q) = \left(-1, \frac{-2y_0}{x_0 - 1}, \frac{-2z_0}{x_0 - 1}\right). \tag{3}$$

This shows that ϕ is defined on all of Q except for the points on the two lines

$$Q \cap \mathbf{V}(x - 1) = \{(1, t, t) : t \in \mathbb{R}\} \cup \{(1, t, -t) : t \in \mathbb{R}\}.$$

We will call $\phi : Q - \mathbf{V}_Q(x - 1) \to W$ a *rational mapping* on Q since the components of ϕ are rational functions. [We can think of them as elements of $\mathbb{R}(Q)$ if we like.]

Going in the other direction, if $(-1, a, b) \in W$, then the line L through $p = (1, 0, 0)$ and $(-1, a, b)$ can be parametrized by

$$\begin{aligned} x &= 1 - 2t,\\ y &= ta,\\ z &= tb, \end{aligned}$$

Computing the intersections with Q, we find

$$L \cap Q = \left\{(1, 0, 0), \left(\frac{a^2 - b^2 - 4}{a^2 - b^2 + 4}, \frac{4a}{a^2 - b^2 + 4}, \frac{4b}{a^2 - b^2 + 4}\right)\right\}.$$

Thus, if we let H denote the hyperbola $\mathbf{V}_W(a^2 - b^2 + 4)$, then we can define a second rational mapping

$$\psi : W - H \longrightarrow Q$$

by

$$\psi(-1,a,b) = \left(\frac{a^2-b^2-4}{a^2-b^2+4}, \frac{4a}{a^2-b^2+4}, \frac{4b}{a^2-b^2+4}\right). \tag{4}$$

From the geometric descriptions of ϕ and ψ, $\phi \circ \psi$ is the identity mapping on the subset $W - H \subset W$. Similarly, we see that $\psi \circ \phi$ is the identity on $Q - \mathbf{V}_Q(x-1)$. Also, using the formulas from equations (3) and (4), it can be checked that $\phi^* \circ \psi^*$ and $\psi^* \circ \phi^*$ are the identity mappings on the function fields. (We should mention that as in the second example, Q and W are *not* isomorphic varieties. However this is not an easy fact to prove given what we know.)

We now introduce some general terminology that was implicit in the above examples.

Definition 4. *Let $V \subset k^m$ and $W \subset k^n$ be irreducible affine varieties. A* **rational mapping** *from V to W is a function ϕ represented by*

$$\phi(x_1,\ldots,x_m) = \left(\frac{f_1(x_1,\ldots,x_m)}{g_1(x_1,\ldots,x_m)},\ldots,\frac{f_n(x_1,\ldots,x_m)}{g_n(x_1,\ldots,x_m)}\right), \tag{5}$$

where $f_i/g_i \in k(x_1,\ldots,x_m)$ satisfy:

(i) *ϕ is defined at some point of V.*

(ii) *For every $(a_1,\ldots,a_m) \in V$ where ϕ is defined, $\phi(a_1,\ldots,a_m) \in W$.*

Note that a rational mapping ϕ from V to W may fail to be a *function* from V to W in the usual sense because, as we have seen in the examples, ϕ may not be defined everywhere on V. For this reason, many authors use a special notation to indicate a rational mapping:

$$\phi : V \dashrightarrow W.$$

We will follow this convention as well. By condition (i), the set of points of V when the rational mapping ϕ in (5) is defined includes $V - \mathbf{V}_V(g_1\cdots g_n) = V - (\mathbf{V}_V(g_1) \cup \cdots \cup \mathbf{V}_V(g_n))$, where $\mathbf{V}_V(g_1\cdots g_n)$ is a proper subvariety of V.

Because rational mappings are not defined everywhere on their domains, we must exercise some care in studying them. In particular, we will need the following precise definition of when two rational mappings are to be considered equal.

Definition 5. *Let $\phi, \psi : V \dashrightarrow W$ be rational mappings represented by*

$$\phi = \left(\frac{f_1}{g_1},\ldots,\frac{f_n}{g_n}\right) \quad \textit{and} \quad \psi = \left(\frac{h_1}{k_1},\ldots,\frac{h_n}{k_n}\right).$$

Then we say that $\phi = \psi$ if for each i, $1 \le i \le n$,

$$f_i k_i - h_i g_i \in \mathbf{I}(V).$$

We have the following geometric criterion for the equality of rational mappings.

Proposition 6. *Two rational mappings $\phi, \psi : V \dashrightarrow W$ are equal if and only if there is a proper subvariety $V' \subset V$ such that ϕ and ψ are defined on $V - V'$ and $\phi(p) = \psi(p)$ for all $p \in V - V'$.*

Proof. We will assume that $\phi = (f_1/g_1, \ldots, f_n/g_n)$ and $\psi = (h_1/k_1, \ldots, h_n/k_n)$. First, suppose that ϕ and ψ are equal as in Definition 5 and let $V_1 = \mathbf{V}_V(g_1 \cdots g_n)$ and $V_2 = \mathbf{V}_V(k_1 \cdots k_n)$. By hypothesis, V_1 and V_2 are proper subvarieties of V, and since V is irreducible, it follows that $V' = V_1 \cup V_2$ is also a proper subvariety of V. Then ϕ and ψ are defined on $V - V'$, and since $f_i k_i - h_i g_i \in \mathbf{I}(V)$, it follows that f_i/g_i and h_i/k_i give the same function on $V - V'$. Hence, the same is true for ϕ and ψ.

Conversely, suppose that ϕ and ψ are defined and equal (as functions) on $V - V'$. This implies that for each i, we have $f_i/g_i = h_i/k_i$ on $V - V'$. Then $f_i k_i - h_i g_i$ vanishes on $V - V'$, which shows that $V = \mathbf{V}(f_i k_i - h_i g_i) \cup V'$. Since V is irreducible and V' is a proper subvariety, this forces $V = \mathbf{V}(f_i k_i - h_i g_i)$. Thus, $f_i k_i - h_i g_i \in \mathbf{I}(V)$, as desired. □

As an example, recall from Example 3 that we had rational maps $\phi : Q \dashrightarrow W$ and $\psi : W \dashrightarrow Q$ such that $\phi \circ \psi$ was the identity on $W - H \subset W$. By Proposition 6, this proves that $\phi \circ \psi$ equals the identity map id_W in the sense of Definition 5.

We also need to be careful in dealing with the composition of rational mappings.

Definition 7. *Given $\phi : V \dashrightarrow W$ and $\psi : W \dashrightarrow Z$, we say that $\psi \circ \phi$ is* **defined** *if there is a point $p \in V$ such that ϕ is defined at p and ψ is defined at $\phi(p)$.*

When a composition $\psi \circ \phi$ is defined, it gives us a rational mapping as follows.

Proposition 8. *Let $\phi : V \dashrightarrow W$ and $\psi : W \dashrightarrow Z$ be rational mappings such that $\psi \circ \phi$ is defined. Then there is a proper subvariety $V' \subset V$ such that:*
(i) *ϕ is defined on $V - V'$ and ψ is defined on $\phi(V - V')$.*
(ii) *$\psi \circ \phi : V \dashrightarrow Z$ is a rational mapping defined on $V - V'$.*

Proof. Suppose that ϕ and ψ are represented by

$$\phi(x_1, \ldots, x_m) = \left(\frac{f_1(x_1, \ldots, x_m)}{g_1(x_1, \ldots, x_m)}, \ldots, \frac{f_n(x_1, \ldots, x_m)}{g_n(x_1, \ldots, x_m)}\right).$$
$$\psi(y_1, \ldots, y_n) = \left(\frac{h_1(y_1, \ldots, y_n)}{k_1(y_1, \ldots, y_n)}, \ldots, \frac{h_l(y_1, \ldots, y_n)}{k_l(y_1, \ldots, y_n)}\right).$$

Then the j-th coordinate of $\psi \circ \phi$ is

$$\frac{h_j(f_1/g_1, \ldots, f_n/g_n)}{k_j(f_1/g_1, \ldots, f_n/g_n)},$$

which is clearly a rational function in $x_1, \ldots, x_m$. To get a quotient of polynomials, we can write this as

$$\frac{P_j}{Q_j} = \frac{(g_1 \cdots g_n)^M h_j(f_1/g_1, \ldots, f_n/g_n)}{(g_1 \ldots g_n)^M k_j(f_1/g_1, \cdots, f_n/g_n)},$$

when M is sufficiently large.

Now set

$$V' = \mathbf{V}_V([Q_1 \cdots Q_l g_1 \cdots g_n]) \subset V.$$

It should be clear that ϕ is defined on $V - V'$ and ψ is defined on $\phi(V - V')$. It remains to show that $V' \neq V$. But by assumption, there is $p \in V$ such that $\phi(p)$ and $\psi(\phi(p))$ are defined. This means that $g_i(p) \neq 0$ for $1 \leq i \leq n$ and

$$k_j(f_1(p)/g_1(p), \ldots, f_n(p)/g_n(p)) \neq 0$$

for $1 \leq j \leq l$. It follows that $Q_j(p) \neq 0$ and consequently, $p \in V - V'$. □

In the exercises, you will work out an example to show how $\psi \circ \phi$ can fail to be defined. Basically, this happens when the domain of definition of ψ lies outside the image of ϕ.

Examples 2 and 3 illustrate the following alternative to the notion of *isomorphism* of varieties.

Definition 9.

(i) *Two irreducible varieties $V \subset k^m$ and $W \subset k^n$ are said to be* **birationally equivalent** *if there exist rational mappings $\phi : V \dashrightarrow W$ and $\psi : W \dashrightarrow V$ such that $\phi \circ \psi$ is defined (as in Definition 7) and equal to the identity map* id_W *(as in Definition 5), and similarly for $\psi \circ \phi$.*

(ii) *A* **rational variety** *is a variety that is birationally equivalent to k^n for some n.*

Just as isomorphism of varieties can be detected from the coordinate rings, birational equivalence can be detected from the function fields.

Theorem 10. *Two irreducible varieties V and W are birationally equivalent if and only if there is an isomorphism of function fields $k(V) \cong k(W)$ which is the identity on k. (By definition, two fields are isomorphic if they are isomorphic as commutative rings.)*

Proof. The proof is similar to what we did in Theorem 9 of §4. Suppose first that V and W are birationally equivalent via $\phi : V \dashrightarrow W$ and $\psi : W \dashrightarrow V$. We will define a pullback mapping $\phi^* : k(W) \to k(V)$ by the rule $\phi^*(f) = f \circ \phi$ and show that ϕ^* is an isomorphism. Unlike the polynomial case, it is not obvious that $\phi^*(f) = f \circ \phi$ exists for all $f \in k(W)$—we need to prove that $f \circ \phi$ is defined at some point of W.

We first show that our assumption $\phi \circ \psi = \mathrm{id}_W$ implies the existence of a proper subvariety $W' \subset W$ such that

$$\begin{aligned} &\psi \text{ is defined on } W - W',\\ (6)\qquad &\phi \text{ is defined on } \psi(W - W'),\\ &\phi \circ \psi \text{ is the identity function on } W - W'. \end{aligned}$$

To prove this, we first use Proposition 8 to find a proper subvariety $W_1 \subset W$ such that ψ is defined on $W - W_1$ and ϕ is defined on $\psi(W - W_1)$. Also, from Proposition 6, we get a proper subvariety $W_2 \subset W$ such that $\phi \circ \psi$ is the identity function on $W - W_2$. Since W is irreducible, $W' = W_1 \cup W_2$ is a proper subvariety, and it follows easily that (6) holds for this choice of W'.

Given $f \in k(W)$, we can now prove that $f \circ \phi$ is defined. If f is defined on $W - W'' \subset W$, then we can pick $q \in W - (W' \cup W'')$ since W is irreducible. From (6), we get $p = \psi(q) \in V$ such that $\phi(p)$ is defined, and since $\phi(p) = q \notin W''$, we also know that f is defined at $\phi(p)$. By Definition 4, $\phi^*(f) = f \circ \phi$ exists as an element of $k(V)$.

This proves that we have a map $\phi^* : k(W) \to k(V)$, and ϕ^* is a ring homomorphism by the proof of Proposition 8 from §4. Similarly, we get a ring homomorphism $\psi^* : k(V) \to k(W)$. To show that these maps are inverses of each other, let us look at

$$(\psi^* \circ \phi^*)(f) = f \circ \phi \circ \psi$$

for $f \in k(W)$. Using the above notation, we see that $f \circ \phi \circ \psi$ equals f as a function on $W - (W' \cup W'')$, so that $f \circ \phi \circ \psi = f$ in $k(W)$ by Proposition 6. This shows that $\psi^* \circ \phi^*$ is the identity on $k(W)$, and a similar argument shows that $\phi^* \circ \psi^* = \mathrm{id}_{k(V)}$. Thus, $\phi^* : k(W) \to k(V)$ is an isomorphism of fields. We leave it to the reader to show that ϕ^* is the identity on the constant functions $k \subset k(W)$.

The proof of the converse implication is left as an exercise for the reader. Once again the idea is basically the same as in the proof of Theorem 9 of §4. □

In the exercises, you will prove that two irreducible varieties are birationally equivalent if there are "big" subsets (complements of proper subvarieties) that can be put in one-to-one correspondence by rational mappings. For example, the curve $V = \mathbf{V}(y^5 - x^2)$ from Example 2 is birationally equivalent to $W = \mathbb{R}$. You should check that $V - \{(0,0)\}$ and $W - \{0\}$ are in a one-to-one correspondence via the rational mappings f and g from equation (1). The birational equivalence between the hyperboloid and the plane in Example 3 works similarly. This example also shows that outside of the "big" subsets, birationally equivalent varieties may be quite different (you will check this in Exercise 14).

As we see from these examples, birational equivalence of irreducible varieties is a *weaker* equivalence relation than isomorphism. By this we mean that the set of varieties birationally equivalent to a given variety will contain many different nonisomorphic varieties. Nevertheless, in the history of algebraic geometry, the classification of varieties up to birational equivalence has received more attention than classification up to isomorphism, perhaps because constructing rational functions on a variety is easier than constructing polynomial functions. There are reasonably complete classifications of irreducible varieties of dimensions 1 and 2 up to birational equivalence, and, recently, significant progress has been made in dimension 3. However, the classification of irreducible varieties of dimension ≥ 4 up to birational equivalence is still incomplete and is an area of current research.

EXERCISES FOR §5

1. Let R be an integral domain, and let $QF(R)$ be the field of fractions of R as described in the text.
   a. Show that addition is well-defined in $QF(R)$. This means that if $r/s = r'/s'$ and $t/u = t'/u'$, then you must show that $(ru + ts)/su = (r'u' + t's')/s'u'$. Hint: Remember what it means for two elements of $QF(R)$ to be equal.
   b. Show that multiplication is well-defined in $QF(R)$.
   c. Show that the field axioms are satisfied for $QF(R)$.
2. As in Example 2, let $V = \mathbf{V}(y^5 - x^2) \subset \mathbb{R}^2$.
   a. Show that $y^5 - x^2$ is irreducible in $\mathbb{R}[x, y]$ and prove that $\mathbf{I}(V) = \langle y^5 - x^2 \rangle$.
   b. Conclude that $\mathbb{R}[V]$ is an integral domain.
3. Show that the singular cubic curve $\mathbf{V}(y^2 - x^3)$ is a rational variety (birationally equivalent to k) by adapting what we did in Example 2.
4. Consider the singular cubic curve $V_c = \mathbf{V}(y^2 - cx^2 + x^3)$ studied in Exercise 8 of Chapter 1, §3. Using the parametrization given there, prove that V_c is a rational variety and find subvarieties $V_c' \subset V_c$ and $W \subset k$ such that your rational mappings define a one-to-one correspondence between $V_c - V_c'$ and $k - W$. Hint: Recall that t in the parametrization of V_c is the slope of a line passing through (0, 0).
5. Verify that the curve $\pi(C)$ from Exercise 7 of §4 is a rational variety. Hint: To define a rational inverse of the parametrization we derived in that exercise, you need to solve for t as a function of x and y on the curve. The equation of the hyperbola may be useful.
6. In Example 3, verify directly that (3) and (4) define inverse rational mappings from the hyperboloid of the one sheet to the plane.
7. Let $S = \mathbf{V}(x^2 + y^2 + z^2 - 1)$ in $\mathbb{R}^3$ and let $W = \mathbf{V}(z)$ be the (x, y)-plane. In this exercise, we will show that S and W are birationally equivalent varieties, via an explicit mapping called the stereographic projection. See also Exercise 6 of Chapter 1, §3.
   a. Derive parametric equations as in (2) for the line L_q in $\mathbb{R}^3$ passing through the north pole (0, 0, 1) of S and a general point $q = (x_0, y_0, z_0) \neq (0, 0, 1)$ in S.
   b. Using the line from part (a) show that $\phi(q) = L_q \cap W$ defines a rational mapping $\phi : S \dashrightarrow \mathbb{R}^2$. This is called the stereographic projection mapping.
   c. Show that the rational parametrization of S given in Exercise 6 of Chapter 1, §3 is the inverse mapping of ϕ.
   d. Deduce that S and W are birationally equivalent varieties and find subvarieties $S' \subset S$ and $W' \subset W$ such that ϕ and ψ put $S - S'$ and $W - W'$ into one-to-one correspondence.
8. In Exercise 10 of §1, you showed that there were no nonconstant polynomial mappings from $\mathbb{R}$ to $V = \mathbf{V}(y^2 - x^3 + x)$. In this problem, you will show that there are no nonconstant *rational* mappings either, so V is not birationally equivalent to $\mathbb{R}$. In the process, we will need to consider polynomials with complex coefficients, so the proof will actually show that $\mathbf{V}(y^2 - x^3 + x) \subset \mathbb{C}^2$ is not birationally equivalent to $\mathbb{C}$ either. The proof will be by contradiction.
   a. Start by assuming that $\alpha : \mathbb{R} \dashrightarrow V$ is a nonconstant rational mapping defined by $\alpha(t) = (a(t)/b(t), c(t)/d(t))$ with a and b relatively prime, c and d relatively prime, and b, d monic. By substituting into the equation of V, show that $b^3 = d^2$ and $c^2 = a^3 - ab^2$.
   b. Deduce that $a, b, a + b$, and $a - b$ are all squares of polynomials in $\mathbb{C}[t]$. In other words, show that $a = A^2, b = B^2, a + b = C^2$ and $a - b = D^2$ for some $A, B, C, D \in \mathbb{C}[t]$.
   c. Show that the polynomials $A, B \in \mathbb{C}[t]$ from part b are nonconstant and relatively prime and that $A^4 - B^4$ is the square of a polynomial in $\mathbb{C}[t]$.

d. The key step of the proof is to show that such polynomials cannot exist using *infinite descent.* Suppose that $A, B \in \mathbb{C}[t]$ satisfy the conclusions of part (c). Prove that there are polynomials $A_1, B_1, C_1 \in \mathbb{C}[t]$ such that

$$\begin{aligned} A - B &= A_1^2 \\ A + B &= B_1^2 \\ A^2 + B^2 &= C_1^2. \end{aligned}$$

e. Prove that the polynomials A_1, B_1 from part (d) are relatively prime and nonconstant and that their degrees satisfy

$$\max(\deg(A_1), \deg(B_1)) \leq \frac{1}{2} \max(\deg(A), \deg(B)).$$

Also show that $A_1^4 - (\sqrt{i}B_1)^4 = A_1^4 + B_1^4$ is the square of a polynomial in $\mathbb{C}[t]$. Conclude that $A_1, \sqrt{i}B_1$ satisfy the conclusions of part (c).

f. Conclude that if such a pair A, B exists, then one can repeat parts d and e infinitely many times with decreasing degrees at each step (this is the “infinite descent”). Explain why this is impossible and conclude that our original polynomials a, b, c, d must be constant.

9. Let V be an irreducible variety and let $f \in k(V)$. If we write $f = \phi/\psi$, where $\phi, \psi \in k[V]$, then we know that f is defined on $V - \mathbf{V}_V(\psi)$. What is interesting is that f might make sense on a larger set. In this exercise, we will work out how this can happen on the variety $V = \mathbf{V}(xz - yw) \subset \mathbb{C}^4$.

a. Prove that $xz - yw \in \mathbb{C}[x, y, z, w]$ is irreducible. Hint: Look at the total degrees of its factors.

b. Use unique factorization in $\mathbb{C}[x, y, z, w]$ to prove that $\langle xz - yw \rangle$ is a prime ideal.

c. Conclude that V is irreducible and that $\mathbf{I}(V) = \langle xz - yw \rangle$.

d. Let $f = [x]/[y] \in \mathbb{C}(V)$ so that f is defined on $V - \mathbf{V}_V([y])$. Show that $\mathbf{V}_V([y])$ is the union of planes $\{(0, 0, z, w) : z, w \in \mathbb{C}\} \cup \{(x, 0, 0, w) : x, w \in \mathbb{C}\}$.

e. Show that $f = [w]/[z]$ and conclude that f is defined everywhere outside of the plane $\{(x, 0, 0, w) : x, w \in \mathbb{C}\}$.

Note that what made this possible was that we had two fundamentally different ways of representing the rational function f. This is part of why rational functions are subtle to deal with.

10. Consider the rational mappings $\phi : \mathbb{R} \dashrightarrow \mathbb{R}^3$ and $\psi : \mathbb{R}^3 \dashrightarrow \mathbb{R}$ defined by

$$\phi(t) = (t, 1/t, t^2) \quad \text{and} \quad \psi(x, y, z) = \frac{x + yz}{x - yz}.$$

Show that $\psi \circ \phi$ is not defined.

11. Complete the proof of Theorem 10 by showing that if V and W are irreducible varieties and $k(V) \cong k(W)$ is an isomorphism of their function fields which is the identity on constants, then there are inverse rational mappings $\phi : V \dashrightarrow W$ and $\psi : W \dashrightarrow V$. Hint: Follow the proof of Theorem 9 from §4.

12. Suppose that $\phi : V \dashrightarrow W$ is a rational mapping defined on $V - V'$. If $W' \subset W$ is a subvariety, then prove that

$$V'' = V' \cup \{p \in V - V' : \phi(p) \in W'\}$$

is a subvariety of V. Hint: Find equations for V'' by substituting the rational functions representing ϕ into the equations for W' and setting the numerators of the resulting functions equal to zero.

13. Suppose that V and W are birationally equivalent varieties via $\phi : V \dashrightarrow W$ and $\psi : W \dashrightarrow V$. As mentioned in the text after the proof of Theorem 10, this means that V and W have "big" subsets that are the same. More precisely, there are proper subvarieties $V_1 \subset V$ and $W_1 \subset W$ such that ϕ and ψ induce inverse bijections between subsets $V - V_1$ and $W - W_1$. Note that Exercises 4 and 7 involved special cases of this result.
    a. Let $V' \subset V$ be the subvariety that satisfies the properties given in (6) for $\phi \circ \psi$. Similarly, we get $W' \subset W$ that satisfies the analogous properties for $\psi \circ \phi$. Let
    $$\mathcal{V} = \{p \in V - V' : \phi(p) \in W - W'\},$$
    $$\mathcal{W} = \{q \in W - W' : \psi(q) \in V - V'\}.$$
    Show that we have bijections $\phi : \mathcal{V} \to \mathcal{W}$ and $\psi : \mathcal{W} \to \mathcal{V}$ which are inverses of each other.
    b. Use Exercise 12 to prove that $\mathcal{V} = V - V_1$ and $\mathcal{W} = W - W_1$ for proper subvarieties V_1 and W_1.

    Parts (a) and (b) give the desired one-to-one correspondence between "big" subsets of V and W.
14. In Example 3, we had rational mappings $\phi : Q \dashrightarrow W$ and $\psi : W \dashrightarrow Q$.
    a. Show that ϕ and ψ induce inverse bijections $\phi : Q - \mathbf{V}_Q(x-1) \to W - H$ and $\psi : W - H \to Q - \mathbf{V}_Q(x-1)$, where $H = \mathbf{V}_W(a^2 - b^2 + 4)$.
    b. Show that H and $\mathbf{V}_Q(x-1)$ are very different varieties that are neither isomorphic nor birationally equivalent.

§6 (Optional) Proof of the Closure Theorem

This section will complete the proof of the Closure Theorem begun in §2 of Chapter 3. We will use many of the concepts introduced in Chapters 4 and 5, including irreducible varieties and prime ideals from Chapter 4 and quotient rings and fields of fractions from this chapter.

We begin by recalling the basic situation. Let k be an algebraically closed field, and be let $\pi_l : k^n \to k^{n-l}$ be projection onto the last $n-l$ components. If $V = \mathbf{V}(I)$ is an affine variety in k^n, then we get the l-th elimination ideal $I_l = I \cap k[x_{l+1}, \ldots, x_n]$, and §4 of Chapter 4 proved the first part of the Closure Theorem, which asserts that $\mathbf{V}(I_l)$ is the smallest variety in k^{n-l} containing $\pi_l(V)$. In the language of Chapter 4, this says that $\mathbf{V}(I_l)$ is the Zariski closure of $\pi_l(V)$.

The remaining part of the Closure Theorem tells us that $\pi_l(V)$ fills up "most" of $\mathbf{V}(I_l)$ in the following sense.

Theorem 1 (The Closure Theorem, second part). *Let k be algebraically closed, and let $V = \mathbf{V}(I) \subset k^n$. If $V \neq \emptyset$, then there is an affine variety $W \subsetneq \mathbf{V}(I_l)$ such that*

$$\mathbf{V}(I_l) - W \subset \pi_l(V).$$

Proof. In Chapter 3, we proved this for $l = 1$ using resultants. Before tackling the case $l > 1$, we note that $\mathbf{V}(I_l)$ depends only on V since it is the Zariski closure of $\pi_l(V)$. This means that *any* defining ideal I of V gives the same $\mathbf{V}(I_l)$. In particular, since

$V = \mathbf{V}(\mathbf{I}(V))$, we can replace I with $\mathbf{I}(V)$. Hence, if V is irreducible, we can assume that I is a prime ideal.

Our strategy for proving the theorem is to start with the irreducible case. The following observations will be useful:

$$\begin{aligned} I \text{ is prime} &\Longrightarrow I_l \text{ is prime} \\ V \text{ is irreducible} &\Longrightarrow \mathbf{V}(I_l) \text{ is irreducible.} \end{aligned} \tag{1}$$

The first implication is straightforward and is left as an exercise. As for the second, we've seen that we can assume that $I = \mathbf{I}(V)$, so that I is prime. Then I_l is prime, and the algebra–geometry dictionary (Corollary 4 of Chapter 4, §5) implies that $\mathbf{V}(I_l)$ is irreducible.

Now suppose that V is irreducible. We will show that $\pi_l(V)$ has the desired property by using induction on l to prove the following slightly stronger result: given a variety $W_0 \subsetneqq V$, there is a variety $W_l \subsetneqq \mathbf{V}(I_l)$ such that

$$\mathbf{V}(I_l) - W_l \subset \pi_l(V - W_0). \tag{2}$$

We begin with the case $l = 1$. Since $W_0 \neq V$, we can find $(a_1, \ldots, a_n) \in V - W_0$. Then there is $f \in \mathbf{I}(W_0)$ such that $f(a_1, \ldots, a_n) \neq 0$. The polynomial f will play a crucial role in what follows. At this point, the proof breaks up into two cases:

Case I: Suppose that for *all* $(b_2, \ldots, b_n) \in \mathbf{V}(I_1)$, we have $(b_1, b_2, \ldots, b_n) \in V$ for all $b_1 \in k$. In this situation, write f as a polynomial in x_1:

$$f = \sum_{i=0}^{m} g_i(x_2, \ldots, x_n)x_1^i.$$

Now let $W_1 = \mathbf{V}(I_1) \cap \mathbf{V}(g_0, \ldots, g_m)$. This variety is strictly smaller than $\mathbf{V}(I_1)$ since $f(a_1, \ldots, a_n) \neq 0$ implies that $g_i(a_2, \ldots, a_n) \neq 0$ for some i. Thus $(a_2, \ldots, a_n) \in \mathbf{V}(I_1) - W_1$, so that $W_1 \neq \mathbf{V}(I_1)$.

We next show that (2) is satisfied. If $(c_2, \ldots, c_n) \in \mathbf{V}(I_1) - W_1$, then some g_i is nonvanishing at $(c_2, \ldots, c_n)$, so that $f(x_1, c_2, \ldots, c_n)$ is a nonzero polynomial. Since k is infinite (Exercise 4 of Chapter 4, §1), we can find $c_1 \in k$ such that $f(c_1, c_2, \ldots, c_n) \neq 0$. By the assumption of Case I, the point $(c_1, \ldots, c_n)$ is in V, yet it can't be in W_0 since f vanishes on W_0. This proves that $(c_2, \ldots, c_n) \in \pi_1(V - W_0)$, which proves (2) in Case I.

Case II: Suppose that there is *some* $(b_2, \ldots, b_n) \in \mathbf{V}(I_1)$ and *some* $b_1 \in k$ such that $(b_1, b_2, \ldots, b_n) \notin V$. In this situation, we can find $h \in I$ such that $h(b_1, \ldots, b_n) \neq 0$ (h exists because $I = \mathbf{I}(V)$). Write h as a polynomial in x_1:

$$h = \sum_{i=0}^{r} u_i(x_2, \ldots, x_n)x_1^i. \tag{3}$$

Then $h(b_1, \ldots, b_n) \neq 0$ implies $u_i(b_2, \ldots, b_n) \neq 0$ for some i. Thus, $u_i \notin I_1$ for some i. Furthermore, if $u_r \in I_1$, then $h - u_r x_1^r$ is also nonvanishing at $(b_1, \ldots, b_n)$, so that we can replace h with $h - u_r x_1^r$. Repeating this as often as necessary, we can assume $u_r \notin I_1$ in (3).

The next claim we want to prove is the following:

$$\text{(4)} \qquad \text{there exist } v_i \in k[x_2, \ldots, x_n] \text{ such that } \sum_{i=0}^{r} v_i f^i \in I \text{ and } v_0 \notin I_1.$$

To prove this, we will regard f and h as polynomials in x_1 and then divide f by h. But rather than just use the division algorithm as in §5 of Chapter 1, we will replace f with $u_r^{N_1} f$, where N_1 is some positive integer. We claim that if N_1 is sufficiently large, we can divide $u_r^{N_1} f$ without introducing any denominators. This means we get an equation of the form

$$u_r^{N_1} f = qh + v_{10} + v_{11}x_1 + \cdots + v_{1,r-1}x_1^{r-1},$$

where $q \in k[x_1, \ldots, x_n]$ and $v_{1i} \in k[x_2, \ldots, x_n]$. We leave the proof of this as Exercise 2, though the reader may also want to consult §5 of Chapter 6, where this process of *pseudodivision* is studied in more detail. Now do the above "division" not just to f but to all of its powers $1, f, f^2, \ldots, f^r$. This gives equations of the form

$$\text{(5)} \qquad u_r^{N_j} f^j = q_j h + v_{j0} + v_{j1}x_1 + \cdots + v_{j,r-1}x_1^{r-1}$$

for $0 \leq j \leq r$.

Now we will use quotient rings and fields of fractions. We have already seen that $I_1 = \mathbf{I}(\mathbf{V}(I_1))$, so that by §2, the quotient ring $k[x_2, \ldots, x_n]/I_1$ is naturally isomorphic to the coordinate ring $k[\mathbf{V}(I_1)]$. As in §5, this ring is an integral domain since $\mathbf{V}(I_1)$ is irreducible, and hence has a field of fractions, which we will denote by K. We will regard $k[x_2, \ldots, x_n]/I_1$ as a subset of K, so that a polynomial $v \in k[x_2, \ldots, x_n]$ gives an element $[v] \in k[x_2, \ldots, x_n]/I_1 \subset K$. In particular, the zero element of K is $[0]$, where $0 \in k[x_2, \ldots, x_n]$ is the zero polynomial.

The polynomials v_{ji} of (5) give a $(r + 1) \times r$ matrix

$$\begin{pmatrix} [v_{00}] & \ldots & [v_{0,r-1}] \\ \vdots & & \vdots \\ [v_{r0}] & \ldots & [v_{r,r-1}] \end{pmatrix}$$

with entries in K. The rows are $r + 1$ vectors in the r-dimensional vector space K^r, so that the rows are linearly dependent over K. Thus there are $\phi_0, \ldots, \phi_r, \in K$, not all zero, such that $\sum_{j=0}^{r} \phi_j [v_{ji}] = [0]$ in K for $0 \leq i \leq r - 1$. If we write each ϕ_j as a quotient of elements of $k[x_2, \ldots, x_n]/I_1$ and multiply by a common denominator, we can assume that $\phi_j = [w_j]$ for some $w_j \in k[x_2, \ldots, x_n]$. Further, the ϕ_j being not all zero in $k[x_2, \ldots, x_n]/I_1 \subset K$ means that at least one w_j is not in I_1. Then $w_0, \ldots, w_r$ have the property that

$$\sum_{j=0}^{r} [w_j][v_{ji}] = [0],$$

which means that

$$\text{(6)} \qquad \sum_{j=0}^{r} w_j v_{ji} \in I_1.$$

Finally, if we multiply each equation (5) by the corresponding w_j and sum for $0 \le j \le r$, we obtain

$$\sum_{j=0}^{r} w_j u_r^{N_j} f^j \in I$$

by (6) and the fact that $h \in I$. Let $v_j = w_j u_r^{N_j}$. Since $u_r \notin I_1$ and $w_j \notin I_1$ for some j, it follows that $v_j \notin I_1$ for some j since I_1 is prime by (1).

It remains to arrange for $v_0 \notin I_1$. So suppose $v_0, \ldots, v_{t-1} \in I_1$ but $v_t \notin I_1$. It follows that

$$f^t \sum_{j=t}^{r} v_j f^{j-t} \in I.$$

Since I is prime and $f \notin I$, it follows immediately that $\sum_{j=t}^{r} v_j f^{j-t} \in I$. After relabeling so that v_t is v_0, we get (4) as desired.

The condition (4) has the following crucial consequence:

$$\pi_1(V) \cap (k^{n-1} - \mathbf{V}(v_0)) \subset \pi_1(V - W_0). \tag{7}$$

This follows because $\sum_{i=0}^{r} v_i f^i \in I$, so that for any $(c_1, \ldots, c_n) \in V$ we have

$$v_0(c_2, \ldots, c_n) + f(c_1, \ldots, c_n) \sum_{i=1}^{r} v_i(c_2, \ldots, c_n) f(c_1, \ldots, c_n)^{i-1} = 0.$$

Then $v_0(c_2, \ldots, c_n) \neq 0$ forces $f(c_1, \ldots, c_n) \neq 0$, which in turn implies $(c_1, \ldots, c_n) \notin W_0$ (since f vanishes on W_0). From here, (7) follows easily.

We can finally prove (2) in Case II. Since, $u_r, v_0 \notin I_1$ and I_1 is prime, we see that $g = u_r v_0 \notin I_1$. Thus $W_1 = \mathbf{V}(g) \cap \mathbf{V}(I_1) \subsetneqq \mathbf{V}(I_1)$. To show that (2) holds, let $(c_2, \ldots, c_n) \in \mathbf{V}(I_1) - W_1$. This means that both u_r and v_0 are nonvanishing at $(c_2, \ldots, c_n)$.

If $I = \langle f_1, \ldots, f_s \rangle$, then $h \in I$ implies that $I = \langle h, f_1, \ldots, f_s \rangle$. Since $u_r(c_2, \ldots, c_n) \neq 0$, the Extension Theorem proved in Chapter 3 implies that $(c_1, \ldots, c_n) \in V$ for some $c_1 \in \mathbb{C}$. Then by (7) and $v_0(c_2, \ldots, c_n) \neq 0$, we see that $(c_2, \ldots, c_n) \in \pi_1(V - W_0)$, and (2) is proved in Case II.

We have now completed the proof of (2) when $l = 1$. In the exercises, you will explore the geometric meaning of the two cases considered above.

Next, suppose that (2) is true for $l - 1$. To prove that it holds for l, take $W_0 \subsetneqq V$, and apply what we proved for $l = 1$ to find $W_1 \subsetneqq \mathbf{V}(I_1)$ such that

$$\mathbf{V}(I_1) - W_1 \subset \pi_1(V - W_0).$$

Now observe that I_l is the $(l-1)$st elimination ideal of I_1. Furthermore, $\mathbf{V}(I_1)$ is irreducible by (1). Thus, our induction hypothesis, applied to $W_1 \subsetneqq \mathbf{V}(I_1)$, implies that there is $W_l \subsetneqq \mathbf{V}(I_l)$ such that

$$\mathbf{V}(I_l) - W_l \subset \tilde{\pi}_{l-1}(\mathbf{V}(I_1) - W_1),$$

where $\tilde{\pi}_{l-1} : k^{n-1} \to k^{n-l}$ is projection onto the last $(n-1)-(l-1) = n-l$ components. However, since $\pi_l = \tilde{\pi}_{l-1} \circ \pi_1$ (see Exercise 4), it follows that

$$\mathbf{V}(I_l) - W_1 \subset \tilde{\pi}_{l-1}(\mathbf{V}(I_1) - W_1) \subset \tilde{\pi}_{l-1}(\pi_1(V - W_0)) = \pi_1(V - W_0).$$

This completes the proof of (2), so that Theorem 1 is true for all irreducible varieties.

We can now prove the general case of the theorem. Given an arbitrary variety $V \subset k^n$, we can write V as a union of irreducible components (Theorem 2 of Chapter 4, §6):

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

Let V_i' be the Zariski closure of $\pi_l(V_i) \subset k^{n-l}$. We claim that

$$\text{(8)} \qquad \mathbf{V}(I_l) = V_1' \cup \cdots \cup V_m'.$$

To prove this, observe that $V_1' \cup \cdots \cup V_m'$ is a variety containing $\pi_l(V_1) \cup \cdots \cup \pi_l(V_m) = \pi_l(V)$. Since $\mathbf{V}(I_l)$ is the Zariski closure of $\pi_l(V)$, if follows that $\mathbf{V}(I_l) \subset V_1' \cup \cdots \cup V_m'$. For the opposite inclusion, note that for each i, we have $\pi_l(V_i) \subset \pi_l(V) \subset \mathbf{V}(I_l)$, which implies $V_i' \subset \mathbf{V}(I_l)$ since V_i' is the Zariski closure of $\pi_l(V_i)$. From here, (8) follows easily.

From (1), we know each V_i' is irreducible, so that (8) gives a decomposition of $\mathbf{V}(I_l)$ into irreducibles. This need not be a minimal decomposition, and in fact $V_i' = V_j'$ can occur when $i \neq j$. But we can find at least one of them not strictly contained in the others. By relabeling, we can assume $V_1' = \cdots = V_r'$ and $V_1' \not\subset V_i$ for $r+1 \leq i \leq m$.

Applying (2) to the irreducible varieties $V_1, \ldots, V_r$ (with $W_0 = \emptyset$), there are varieties $W_i \subsetneq V_i'$ such that

$$V_i' - W_i \subset \pi_l(V_i), \quad 1 \leq i \leq r$$

since V_i' is the Zariski closure of $\pi_l(V_i)$. If we let $W = W_1 \cup \cdots \cup W_r \cup V_{r+1}' \cup \cdots \cup V_m'$, then $W \subset \mathbf{V}(I_l)$, and one sees easily that

$$\begin{aligned}\mathbf{V}(I_l) - W &= V_1' \cup \cdots \cup V_m' - (W_1 \cup \cdots \cup W_r \cup V_{r+1}' \cup \cdots \cup V_m') \\ &\subset (V_1' - W_1) \cup \cdots \cup (V_r' - W_r) \\ &\subset \pi_l(V_1) \cup \cdots \cup \pi_l(V_r) \subset \pi_l(V).\end{aligned}$$

It remains to show that $W \neq \mathbf{V}(I_l)$. But if W were equal to $\mathbf{V}(I_l)$, then we would have $V_1' \subset W_1 \cup \cdots \cup W_r \cup V_{r+1}' \cup \cdots \cup V_m'$. Since V_1' is irreducible, Exercise 5 below shows that V_1' would lie in one of $W_1, \ldots, W_r, V_{r+1}', \ldots, V_m'$. This is impossible by the way we chose V_1' and W_1. Hence, we have a contradiction, and the theorem is proved. □

We can use the Closure Theorem to give a precise description of $\pi_l(V)$ as follows.

Corollary 2. *Let k be algebraically closed, and let $V \subset k^n$ be an affine variety. Then there are affine varieties $Z_i \subset W_i \subset k^{n-l}$ for $1 \leq i \leq p$ such that*

$$\pi_l(V) = \bigcup_{i=1}^{p} (W_i - Z_i).$$

Proof. If $V = \emptyset$, then we are done. Otherwise let $W_1 = \mathbf{V}(I_l)$. By the Closure Theorem, there is a variety $Z_1 \subsetneqq W_1$ such that $W_1 - Z_1 \subset \pi_l(V)$. Then, back in k^n, consider the set

$$V_1 = V \cap \{(a_1, \ldots, a_n) \in k^n : (a_{l+1}, \ldots, a_n) \in Z_1\}$$

One easily checks that V_1 is an affine variety (see Exercise 7), and furthermore, $V_1 \subsetneqq V$ since otherwise we would have $\pi_l(V) \subset Z_1$, which would imply $W_1 \subset Z_1$ by Zariski closure. Moreover, one can check that

$$\pi_l(V) = (W_1 - Z_1) \cup \pi_l(V_1) \tag{9}$$

(see Exercises 7).

If $V_1 = \emptyset$, then we are done. If V_1 is nonempty, let W_2 be the Zariski closure of $\pi_l(V_1)$. Applying the Closure Theorem to V_1, we get $Z_2 \subsetneqq W_2$ with $W_2 - Z_2 \subset \pi_l(V_1)$. Then, repeating the above construction, we get the variety

$$V_2 = V_1 \cap \{(a_1, \ldots, a_n) \in k^n : (a_{l+1}, \ldots, a_n) \in Z_2\}$$

such that $V_2 \subsetneqq V_1$ and

$$\pi_1(V) = (W_1 - Z_1) \cup (W_2 - Z_2) \cup \pi_l(V_2).$$

If $V_2 = \emptyset$, we are done, if not, we repeat this process again to obtain W_3, Z_3 and $V_3 \subsetneqq V_2$. Continuing in this way, we must eventually have $V_N = \emptyset$ for some N, since otherwise we would get an infinite descending chain of varieties

$$V \supsetneqq V_1 \supsetneqq V_2 \supsetneqq \cdots,$$

which would contradict Proposition 1 of Chapter 4, §6. Once we have $V_N = \emptyset$, the desired formula for $\pi_l(V)$ follows easily. □

In general, a set of the form described in Corollary 2 is called *constructible*.

EXERCISES FOR §6

1. This exercise is concerned with (1) in the proof of Theorem 1.
   a. Prove that I prime implies I_l prime. Your proof should work for any field k.
   b. In the text, we showed V irreducible implies $\mathbf{V}(I_l)$ irreducible when the field is algebraically closed. Give an argument that works over any field k.
2. Let $g, h \in k[x_1, \ldots, x_n]$, and assume that h has positive degree r in x_1, so that $h = \sum_{i=0}^{r} u_i(x_2, \ldots, x_n)x_1^i$. Use induction on the degree of g in x_1 to show that there is some integer N such that $u_r^N g = qh+g'$ where $q, g' \in k[x_1, \ldots, x_n]$ and g' has degree $< r$ in x_1.
3. In this exercise, we will study the geometric meaning of the two cases encountered in the proof of Theorem 1. For concreteness, let us assume that $k = \mathbb{C}$. Recall that we have $V \subset \mathbb{C}^n$ irreducible and the projection $\pi_1 : \mathbb{C}^n \to \mathbb{C}^{n-1}$. Given a point $y \in \mathbb{C}^{n-1}$, let

   $$V_y = \{x \in V : \pi_1(x) = y\}.$$

   We call V_y the *fiber over* y of the projection π_1.
   a. Prove that $V_y \subset \mathbb{C} \times \{y\}$, and that $V_y \neq \emptyset$ if and only if $y \in \pi_1(V)$.
   b. Show that in Case I of the proof of Theorem 1, $\pi_1(V) = \mathbf{V}(I_1)$ and $V_y = \mathbb{C} \times \{y\}$ for all $y \in \pi_1(V)$. Thus, this case means that all nonempty fibers are as big as possible.

c. Show that in Case II, there is a variety $\widetilde{W} \subset \mathbb{C}^{n-1}$ such that $\pi_1(V) \not\subset W$ and every nonempty fiber not over a point of $\widetilde{W}$ is finite. Thus, this case means that "most" nonempty fibers are finite. Hint: If h is as in (3) and $u_r \in I_1$, then let $\widetilde{W} = \mathbf{V}(u_r)$.

d. If $V = \mathbf{V}(x_2 - x_1x_3) \subset \mathbb{C}^3$, then show that "most" fibers V_y consist of a single point. Is there a fiber which is infinite?

4. Given $\pi_1 : k^n \to k^{n-1}, \pi_l : k^n \to k^{n-l}$ and $\tilde{\pi}_{l-1} : k^{n-1} \to k^{n-l}$ as in the proof of Theorem 1, show that $\pi_l = \tilde{\pi}_{l-1} \circ \pi_1$.

5. Let $V \subset k^n$ be an irreducible variety. Then prove the following assertions.

a. If $V_1, V_2 \subset k^n$ are varieties such that $V \subset V_1 \cup V_2$, then either $V \subset V_1$ or $V \subset V_2$.

b. More generally, if $V_1, \ldots, V_m \subset k^n$ are varieties such that $V \subset V_1 \cup \cdots \cup V_m$, then $V \subset V_i$ for some i.

6. In the proof of Theorem 1, the variety $W \subset \mathbf{V}(I_l)$ we constructed was rather large—it contained all but one of the irreducible components of $\mathbf{V}(I_l)$. Show that we can do better by proving that there is a variety $W \subset \mathbf{V}(V_l)$ which contains no irreducible component of $\mathbf{V}(I_l)$ and satisfies $\mathbf{V}(I_l) - W \subset \pi_l(V)$. Hint: First, explain why each irreducible component of $\mathbf{V}(I_l)$ is V_j' for some j. Then apply the construction we did for V_1' to each of these V_j''s.

7. This exercise is concerned with the proof of Corollary 2.

a. Verify that $V_1 = V \cap \{(a_1, \ldots, a_n) \in k^n : (a_{l+1}, \ldots, a_n) \in Z_1\}$ is an affine variety.

b. Verify that $\pi_l(V) = (W_1 - Z_1) \cup \pi_l(V_1)$.

8. Let $V = \mathbf{V}(y - xz) \subset \mathbb{C}^3$. Corollary 2 tells us that $\pi_1(V) \subset \mathbb{C}^2$ is a constructible set. Find an explicit decomposition of $\pi_1(V)$ of the form given by Corollary 2. Hint: Your answer will involve W_1, Z_1 and W_2.

9. When dealing with affine varieties, it is sometimes helpful to use the *minimum principle*, which states that among any collection of varieties in k^n, there is a variety which is minimal with respect to inclusion. More precisely, this means that if we are given varieties $V_\alpha, \alpha \in \mathcal{A}$, where $\mathcal{A}$ is any index set, then there is some $\beta \in \mathcal{A}$ with the property that for any $\alpha \in \mathcal{A}$, $V_\alpha \subset V_\beta$ implies $V_a = V_\beta$.

a. Prove the minimum principle. Hint: Use Proposition 1 of Chapter 4, §6.

b. Formulate and prove an analogous *maximum principle* for ideals in $k[x_1, \ldots, x_n]$.

10. As an example of how to use the minimum principle of Exercise 9, we will give a different proof of Corollary 2. Namely, consider the collection of all varieties $V \subset k^n$ for which $\pi_l(V)$ is not constructible. By the minimum principle, we can find a variety V such that $\pi_l(V)$ is not constructible but $\pi_l(W)$ is constructible for every variety $W \subsetneqq V$. Show how the proof of Corollary 2 up to (9) can be used to obtain a contradiction and thereby prove the corollary.

11. In this exercise, we will generalize Corollary 2 to show that if k is algebraically closed, then $\pi_l(C)$ is constructible whenever C is any constructible subset of k^n.

a. Show that it suffices to show that $\pi_l(V - W)$ is constructible whenever V is an irreducible variety in k^n and $W \subsetneqq V$.

b. If V is irreducible and W_1 is the Zariski closure of $\pi_l(V)$, then (2) implies we can find a variety $Z_1 \subsetneqq W_1$ such that $W_1 - Z_1 \subset \pi_l(V - W)$. If we set $V_1 = \{x \in V : \pi_l(x) \in Z_1\}$ then prove that $V_1 \neq V$ and $\pi_l(V - W) = (W_1 - Z_1) \cup \pi_l(V_1 - W)$.

c. Now use the minimum principle as in Exercise 10 to complete the proof.