is not an algebraic set. Finding the equations for the smallest algebraic set containing these points is referred to as *implicitization*, since it amounts to finding a ('smallest') collection of equations satisfied by the $b_i$ (the 'implicit' algebraic relations).

By Proposition 16, this algebraic set is the Zariski closure of $\varphi(\mathbb{A}^n)$ and is the zero set of $\ker \tilde{\varphi}$. By Proposition 8 this kernel is given by $\mathcal{A} \cap k[y_1, \ldots, y_m]$, where $\mathcal{A}$ is the ideal in $k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ generated by the polynomials $y_1 - \varphi_1, \ldots, y_m - \varphi_m$. If we compute the reduced Gröbner basis $G$ for $\mathcal{A}$ with respect to the lexicographic monomial ordering $x_1 > \cdots > x_n > y_1 > \cdots > y_m$, then the polynomials of $G$ lying in $k[y_1, \ldots, y_m]$ generate $\ker \tilde{\pi}$. The zero set of these polynomials defines the Zariski closure of $\varphi(\mathbb{A}^n)$ and therefore give the implicitization.

For an explicit example, consider the points $A = \{(a^2, a^3) \mid a \in \mathbb{R}\}$ in $\mathbb{R}^2$. Using coordinates $x, y$ for $\mathbb{R}^2$ and $t$ for $\mathbb{R}^1$, the ideal $\mathcal{A}$ in $\mathbb{R}[x, y, z, t]$ is $(x - t^2, y - t^3)$. The only element of the reduced Gröbner basis for $\mathcal{A}$ for the ordering $t > x > y$ lying in $\mathbb{R}[x, y]$ is $x^3 - y^2$, so $\mathcal{Z}(x^3 - y^2)$ is the smallest algebraic set in $\mathbb{R}^2$ containing $A$.

**Example: (Projections of Algebraic Sets)**

Suppose $V \subseteq \mathbb{A}^n$ is an algebraic set and $m < n$. Let $\pi : V \to \mathbb{A}^m$ be the morphism projecting onto the first $m$ coordinates:

$$\pi((a_1, a_2, \ldots, a_n)) = (a_1, a_2, \ldots, a_m).$$

If we use coordinates $x_1, \ldots, x_n$ in $k[V]$ and coordinates $y_1, \ldots, y_m$ in $k[\mathbb{A}^m]$, the $k$-algebra homomorphism corresponding to $\pi$ is given by the map

$$\tilde{\pi} : k[y_1, \ldots, y_m] \longrightarrow k[x_1, \ldots, x_n]/\mathcal{I}(V)$$
$$y_i \longmapsto x_i.$$

Suppose $V = \mathcal{Z}(I)$ and $I = (f_1, \ldots, f_s)$. The Zariski closure of $\pi(V)$ is the zero set of $\ker \tilde{\pi} = \mathcal{A} \cap k[y_1, \ldots, y_m]$ where $\mathcal{A}$ is the ideal in $k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ generated by the polynomials $y_1 - x_1, \ldots, y_m - x_m$ together with a set of generators for $\mathcal{I}(V)$. The polynomials involving only $y_1, \ldots, y_m$ in the reduced Gröbner basis $G$ for $\mathcal{A}$ with respect to the lexicographic monomial ordering $x_1 > \cdots > x_n > y_1 > \cdots > y_m$ are generators for the Zariski closure of $\pi(V)$.

If $k$ is algebraically closed we can actually do better with the help of the Nullstellensatz, which gives $\mathcal{I}(V) = \operatorname{rad} I$. Then it is straightforward to see that we obtain the same zero set if in the ideal $\mathcal{A}$ we replace the generators for $\mathcal{I}(V)$ by the generators $f_1, \ldots, f_s$ of $I$ (cf. Exercise 46).

For an explicit example, consider projection onto the first two coordinates of $V = \mathcal{Z}(xy - z^2, xz - y, x^2 - z)$ in $\mathbb{C}^3$. Using $u, v$ as coordinates in $\mathbb{C}^2$, we find the reduced Gröbner basis $G$ for the ideal $(u - x, v - y, xy - z^2, xz - y, x^2 - z)$ for the ordering $x > y > z > u > v$ contains only the polynomial $u^3 - v$ in $\mathbb{C}[u, v]$. The smallest algebraic set containing $\pi(V)$ is then the cubic $v = u^3$.

## Affine Varieties

We next consider the question of whether an algebraic set can be decomposed into smaller algebraic sets and the corresponding algebraic formulation in terms of its coordinate ring.

**Definition** A nonempty affine algebraic set $V$ is called *irreducible* if it cannot be written as $V = V_1 \cup V_2$, where $V_1$ and $V_2$ are proper algebraic sets in $V$. An irreducible affine algebraic set is called an affine *variety*.

Equivalently, an algebraic set (which is a closed set in the Zariski topology) is irreducible if it cannot be written as the union of two proper, closed subsets.

**Proposition 17.**

**(1)** The affine algebraic set $V$ is irreducible if and only if $\mathcal{I}(V)$ is a prime ideal.

**(2)** Every nonempty affine algebraic set $V$ may be written uniquely in the form

$$V = V_1 \cup V_2 \cup \cdots \cup V_q$$

where each $V_i$ is irreducible, and $V_i \not\subseteq V_j$ for all $j \neq i$ (i.e., the decomposition is "minimal" or "irredundant").

*Proof:* Let $I = \mathcal{I}(V)$ and suppose first that $V = V_1 \cup V_2$ is reducible, where $V_1$ and $V_2$ are proper closed subsets. Since $V_1 \neq V$, there is some function $f_1$ that vanishes on $V_1$ but not on $V$, i.e., $f_1 \in \mathcal{I}(V_1) - I$. Similarly, there is a function $f_2 \in \mathcal{I}(V_2) - I$. Then $f_1 f_2$ vanishes on $V_1 \cup V_2 = V$, so $f_1 f_2 \in I$ which shows that $I$ is not a prime ideal. Conversely, if $I$ is not a prime ideal, there exists $f_1, f_2 \in k[\mathbb{A}^n]$ such that $f_1 f_2 \in I$ but neither $f_1$ nor $f_2$ belongs to $I$. Let $V_1 = \mathcal{Z}(f_1) \cap V$ and $V_2 = \mathcal{Z}(f_2) \cap V$. Since the intersection of closed sets is closed, $V_1$ and $V_2$ are algebraic sets. Since neither $f_1$ nor $f_2$ vanishes on $V$, both $V_1$ and $V_2$ are proper subsets of $V$. Because $f_1 f_2 \in I$, $V \subseteq \mathcal{Z}(f_1 f_2) = \mathcal{Z}(f_1) \cup \mathcal{Z}(f_2)$, and so $V$ is reducible. This proves (1).

To prove (2), let $\mathcal{S}$ be the collection of nonempty algebraic sets that cannot be written as a finite union of irreducible algebraic sets, and suppose by way of contradiction that $\mathcal{S} \neq \emptyset$. Let $I_0$ be a maximal element of the corresponding set of ideals, $\{\mathcal{I}(V) \mid V \in \mathcal{S}\}$, which exists (by Theorem 2) since $k[\mathbb{A}^n]$ is Noetherian. Then $V_0 = \mathcal{Z}(I_0)$ is a *minimal* element of $\mathcal{S}$. Since $V_0 \in \mathcal{S}$, it cannot be irreducible by the definition of $\mathcal{S}$. On the other hand, if $V_0 = V_1 \cup V_2$ for some proper, closed subsets $V_1, V_2$ of $V_0$, then by the minimality of $V_0$ both $V_1$ and $V_2$ may be written as finite unions of irreducible algebraic sets. Then $V_0$ may be written as a finite union of irreducible algebraic sets, a contradiction. This proves $\mathcal{S} = \emptyset$, i.e., every affine algebraic set has a decomposition into affine varieties.

To prove uniqueness, suppose $V$ has two decompositions into affine varieties (where redundant terms have been removed from each decomposition):

$$V = V_1 \cup V_2 \cup \cdots \cup V_r = U_1 \cup U_2 \cup \cdots \cup U_s.$$

Then $V_1$ is contained in the union of the $U_i$. Since $V_1 \cap U_i$ is an algebraic set for each $i$, we obtain a decomposition of $V_1$ into algebraic subsets:

$$V_1 = (V_1 \cap U_1) \cup (V_1 \cap U_2) \cup \cdots \cup (V_1 \cap U_s).$$

Since $V_1$ is irreducible, we must have $V_1 = V_1 \cap U_j$ for some $j$, i.e., $V_1 \subseteq U_j$. By the symmetric argument we have $U_j \subseteq V_{j'}$ for some $j'$. Thus $V_1 \subseteq V_{j'}$, so $j' = 1$ and $V_1 = U_j$. Applying a similar argument for each $V_i$ it follows that $r = s$ and that $\{V_1, \ldots, V_r\} = \{U_1, \ldots, U_s\}$. This completes the proof.

**Corollary 18.** An affine algebraic set $V$ is a variety if and only if its coordinate ring $k[V]$ is an integral domain.

*Proof:* This follows immediately since $\mathcal{I}(V)$ is a prime ideal if and only if the quotient $k[V] = k[\mathbb{A}^n]/\mathcal{I}(V)$ is an integral domain (Proposition 13 of Chapter 7).

**Definition.** If $V$ is a variety, then the field of fractions of the integral domain $k[V]$ is called the field of *rational functions* on $V$ and is denoted by $k(V)$. The *dimension* of a variety $V$, denoted dim $V$, is defined to be the transcendence degree of $k(V)$ over $k$.

**Examples**

**(1)** Single points in $\mathbb{A}^n$ are affine varieties since their corresponding ideals in $k[\mathbb{A}^n]$ are maximal ideals. The coordinate ring of a point is isomorphic to $k$, which is also the field of rational functions. The dimension of a single point is 0. Any finite set is the union of its single point subsets, and this is its unique decomposition into affine subvarieties.

**(2)** The $x$-axis in $\mathbb{R}^2$ is irreducible since it has coordinate ring $\mathbb{R}[x, y]/(y) \cong \mathbb{R}[x]$, which is an integral domain. Similarly, the $y$-axis and, more generally, lines in $\mathbb{R}^2$ are also irreducible (cf. Exercise 23 in Section 1). Linear sets in $\mathbb{R}^n$ are affine varieties. The field of rational functions on the $x$-axis is the quotient field $\mathbb{R}(x)$ of $\mathbb{R}[x]$, which is why $\mathbb{R}(x)$ is called a rational function field. The dimension of the $x$-axis (or, more generally, any line) is 1.

**(3)** The union of the $x$ and $y$ axes in $\mathbb{R}^2$, namely $\mathcal{Z}(xy)$, is not a variety: $\mathcal{Z}(xy) = \mathcal{Z}(x) \cup \mathcal{Z}(y)$ is its unique decomposition into subvarieties. The corresponding coordinate ring $\mathbb{R}[x, y]/(xy)$ contains zero divisors.

**(4)** The hyperbola $xy = 1$ in $\mathbb{R}^2$ is a variety since we saw in Section 1 that its coordinate ring is the integral domain $\mathbb{R}[x, 1/x]$. Note that the two disjoint branches of the hyperbola (defined by $x > 0$ and $x < 0$) are not subvarieties (cf. also Exercises 12–13).

**(5)** If $V = \mathcal{Z}(l_1, l_2, \ldots, l_m)$ is the zero set of *linear* polynomials $l_1, \ldots, l_m$ in $k[x_1, \ldots, x_m]$ and $V \neq \emptyset$, then $V$ is an affine variety (called a *linear variety*). Note that determining whether $V \neq \emptyset$ is a linear algebra problem.

We end this section with some general ring-theoretic results that were originally motivated by their connection with decomposition questions in geometry.

## Primary Decomposition of Ideals in Noetherian Rings

The second statement in Proposition 17 shows that any ideal of the form $\mathcal{I}(V)$ in $k[\mathbb{A}^n]$ may be written uniquely as a finite intersection of prime ideals, and by Hilbert's Nullstellensatz this applies in particular to all radical ideals when $k$ is algebraically closed. In a large class of commutative rings (including all Noetherian rings) every ideal has a *primary decomposition*, which is a similar decomposition but allows ideals that are analogous to "prime powers" (but see the examples below). This decomposition can be considered as a generalization of the factorization of an integer $n \in \mathbb{Z}$ into the product of prime powers. We shall be primarily concerned with the case of Noetherian rings.

**Definition.** A proper ideal $Q$ in the commutative ring $R$ is called *primary* if whenever $ab \in Q$ and $a \notin Q$, then $b^n \in Q$ for some positive integer $n$. Equivalently, if $ab \in Q$ and $a \notin Q$, then $b \in \text{rad } Q$.

Some of the basic properties of primary ideals are given in the following proposition.