

Since every ideal  $I$  in the Noetherian ring  $k[x_1, x_2, \dots, x_n]$  is finitely generated, say  $I = (f_1, f_2, \dots, f_q)$ , it follows from (3) that  $\mathcal{Z}(I) = \mathcal{Z}(f_1) \cap \mathcal{Z}(f_2) \cap \dots \cap \mathcal{Z}(f_q)$ , i.e., *each affine algebraic set is the intersection of a finite number of hypersurfaces in  $\mathbb{A}^n$* . Note that this “geometric” property in affine  $n$ -space is a consequence of an “algebraic” property of the corresponding coordinate ring (namely, Hilbert’s Basis Theorem).

If  $V$  is an algebraic set in affine  $n$ -space, then there may be many ideals  $I$  such that  $V = \mathcal{Z}(I)$ . For example, in affine 2-space over  $\mathbb{R}$  the  $y$ -axis is the locus of the ideal  $(x)$  of  $\mathbb{R}[x, y]$ , and also the locus of  $(x^2)$ ,  $(x^3)$ , etc. More generally, the zeros of any polynomial are the same as the zeros of all its positive powers, and it follows that  $\mathcal{Z}(I) = \mathcal{Z}(I^k)$  for all  $k \geq 1$ . We shall study the relationship between ideals that determine the same affine algebraic set in the next section when we discuss radicals of ideals.

While the ideal whose locus determines a particular algebraic set  $V$  is not unique, there is a unique largest ideal that determines  $V$ , given by the set of *all* polynomials that vanish on  $V$ . In general, for any subset  $A$  of  $\mathbb{A}^n$  define

$$\mathcal{I}(A) = \{f \in k[x_1, \dots, x_n] \mid f(a_1, a_2, \dots, a_n) = 0 \text{ for all } (a_1, a_2, \dots, a_n) \in A\}.$$

It is immediate that  $\mathcal{I}(A)$  is an *ideal*, and is the unique largest ideal of functions that are identically zero on  $A$ . This defines a correspondence

$$\mathcal{I} : \{\text{subsets in } \mathbb{A}^n\} \rightarrow \{\text{ideals of } k[\mathbb{A}^n]\}.$$

## Examples

- (1) In the Euclidean plane,  $\mathcal{I}(\text{the } x\text{-axis})$  is the ideal generated by  $y$  in the coordinate ring  $\mathbb{R}[x, y]$ .
- (2) Over any field  $k$ , the ideal of functions vanishing at  $(a_1, a_2, \dots, a_n) \in \mathbb{A}^n$  is a maximal ideal since it is the kernel of the surjective ring homomorphism from  $k[x_1, \dots, x_n]$  to the field  $k$  given by evaluation at  $(a_1, a_2, \dots, a_n)$ . It follows that

$$\mathcal{I}((a_1, a_2, \dots, a_n)) = (x_1 - a_1, x_2 - a_2, \dots, x_n - a_n).$$

- (3) Let  $V = \mathcal{Z}(x^3 - y^2)$  in  $\mathbb{A}^2$ . If  $(a, b) \in \mathbb{A}^2$  is an element of  $V$  then  $a^3 = b^2$ . If  $a \neq 0$ , then also  $b \neq 0$  and we can write  $a = (b/a)^2$ ,  $b = (b/a)^3$ . It follows that  $V$  is the set  $\{(a^2, a^3) \mid a \in k\}$ . For any polynomial  $f(x, y) \in k[x, y]$  we can write  $f(x, y) = f_0(x) + f_1(x)y + (x^3 - y^2)g(x, y)$ . For  $f(x, y) \in \mathcal{I}(V)$ , i.e.,  $f(a^2, a^3) = 0$  for all  $a \in k$ , it follows that  $f_0(a^2) + f_1(a^2)a^3 = 0$  for all  $a \in k$ . If  $f_0(x) = a_r x^r + \dots + a_0$  and  $f_1(x) = b_s x^s + \dots + b_0$  then

$$f_0(x^2) + x^3 f_1(x^2) = (a_r x^{2r} + \dots + a_0) + (b_s x^{2s+3} + \dots + b_0 x^3)$$

and this polynomial is 0 for every  $a \in k$ . If  $k$  is infinite, this polynomial has infinitely many zeros, which can happen only if all of the coefficients are zero. The coefficients of the terms of even degree are the coefficients of  $f_0(x)$  and the coefficients of the terms of odd degree are the coefficients of  $f_1(x)$ , so it follows that  $f_0(x)$  and  $f_1(x)$  are both 0. It follows that  $f(x, y) = (x^3 - y^2)g(x, y)$ , and so

$$\mathcal{I}(V) = (x^3 - y^2) \subset k[x, y].$$

If  $k$  is finite, however, there may be elements in  $\mathcal{I}(V)$  not lying in the ideal  $(x^3 - y^2)$ . For example, if  $k = \mathbb{F}_2$ , then  $V$  is simply the set  $\{(0, 0), (1, 1)\}$  and so  $\mathcal{I}(V)$  contains the polynomial  $x(x - 1)$  (cf. Exercise 15).

The following properties of the map  $\mathcal{I}$  are very easy exercises. Let  $A$  and  $B$  be subsets of  $\mathbb{A}^n$ .

(6) If  $A \subseteq B$  then  $\mathcal{I}(B) \subseteq \mathcal{I}(A)$  (i.e.,  $\mathcal{I}$  is also *contravariant*).

(7)  $\mathcal{I}(A \cup B) = \mathcal{I}(A) \cap \mathcal{I}(B)$ .

(8)  $\mathcal{I}(\emptyset) = k[x_1, \dots, x_n]$  and, if  $k$  is infinite,  $\mathcal{I}(\mathbb{A}^n) = 0$ .

Moreover, there are easily verified relations between the maps  $\mathcal{Z}$  and  $\mathcal{I}$ :

(9) If  $A$  is any subset of  $\mathbb{A}^n$  then  $A \subseteq \mathcal{Z}(\mathcal{I}(A))$ , and if  $I$  is any ideal then  $I \subseteq \mathcal{I}(\mathcal{Z}(I))$ .

(10) If  $V = \mathcal{Z}(I)$  is an affine algebraic set then  $V = \mathcal{Z}(\mathcal{I}(V))$ , and if  $I = \mathcal{I}(A)$  then  $\mathcal{I}(\mathcal{Z}(I)) = I$ , i.e.,  $\mathcal{Z}(\mathcal{I}(\mathcal{Z}(I))) = \mathcal{Z}(I)$  and  $\mathcal{I}(\mathcal{Z}(\mathcal{I}(A))) = \mathcal{I}(A)$ .

The last relation shows that the maps  $\mathcal{Z}$  and  $\mathcal{I}$  act as inverses of each other provided one restricts to the collection of affine algebraic sets  $V = \mathcal{Z}(I)$  in  $\mathbb{A}^n$  and to the set of ideals in  $k[\mathbb{A}^n]$  of the form  $\mathcal{I}(V)$ . In the case where the field  $k$  is algebraically closed we shall (in the following two sections) characterize those ideals  $I$  that are of the form  $\mathcal{I}(V)$  for some affine algebraic set  $V$  in terms of purely ring-theoretic properties of the ideal  $I$  (this is the famous “Zeros Theorem” of Hilbert, cf. Theorem 32).

**Definition.** If  $V \subseteq \mathbb{A}^n$  is an affine algebraic set the quotient ring  $k[\mathbb{A}^n]/\mathcal{I}(V)$  is called the *coordinate ring of  $V$* , and is denoted by  $k[V]$ .

Note that for  $V = \mathbb{A}^n$  and  $k$  infinite we have  $\mathcal{I}(V) = 0$ , so this definition extends the previous terminology. The polynomials in  $k[\mathbb{A}^n]$  define  $k$ -valued functions on  $V$  simply by restricting these functions on  $\mathbb{A}^n$  to the subset  $V$ . Two such polynomial functions  $f$  and  $g$  define the *same* function on  $V$  if and only if  $f - g$  is identically 0 on  $V$ , which is to say that  $f - g \in \mathcal{I}(V)$ . Hence the cosets  $\bar{f} = f + \mathcal{I}(V)$  giving the elements of the quotient  $k[V]$  are precisely the restrictions to  $V$  of ordinary polynomial functions  $f$  from  $\mathbb{A}^n$  to  $k$  (which helps to explain the notation  $k[V]$ ). If  $x_i$  denotes the  $i^{\text{th}}$  coordinate function on  $\mathbb{A}^n$  (projecting an  $n$ -tuple onto its  $i^{\text{th}}$  component), then the restriction  $\bar{x}_i$  of  $x_i$  to  $V$  (which also just gives the  $i^{\text{th}}$  component of the elements in  $V$  viewed as a subset of  $\mathbb{A}^n$ ) is an element of  $k[V]$ , and  $k[V]$  is finitely generated as a  $k$ -algebra by  $\bar{x}_1, \dots, \bar{x}_n$  (although this need not be a minimal generating set).

### Example

If  $V = \mathcal{Z}(xy - 1)$  is the hyperbola  $y = 1/x$  in  $\mathbb{R}^2$ , then  $\mathbb{R}[V] = \mathbb{R}[x, y]/(xy - 1)$ . The polynomials  $f(x, y) = x$  (the  $x$ -coordinate function) and  $g(x, y) = x + (xy - 1)$ , which are different functions on  $\mathbb{R}^2$ , define the same function on the subset  $V$ . On the point  $(1/2, 2) \in V$ , for example, both give the value  $1/2$ . In the quotient ring  $\mathbb{R}[V]$  we have  $\bar{x}\bar{y} = 1$ , so  $\mathbb{R}[V] \cong \mathbb{R}[x, 1/x]$ . For any function  $\bar{f} \in \mathbb{R}[V]$  and any  $(a, b) \in V$  we have  $\bar{f}(a, b) = f(a, 1/a)$  for any polynomial  $f \in k[x, y]$  mapping to  $\bar{f}$  in the quotient.

Suppose now that  $V \subseteq \mathbb{A}^n$  and  $W \subseteq \mathbb{A}^m$  are two affine algebraic sets. Since  $V$  and  $W$  are defined by the vanishing of polynomials, the most natural algebraic maps between  $V$  and  $W$  are those defined by polynomials:

**Definition.** A map  $\varphi : V \rightarrow W$  is called a *morphism* (or *polynomial map* or *regular map*) of algebraic sets if there are polynomials  $\varphi_1, \dots, \varphi_m \in k[x_1, x_2, \dots, x_n]$  such that

$$\varphi((a_1, \dots, a_n)) = (\varphi_1(a_1, \dots, a_n), \dots, \varphi_m(a_1, \dots, a_n))$$

for all  $(a_1, \dots, a_n) \in V$ . The map  $\varphi : V \rightarrow W$  is an *isomorphism* of algebraic sets if there is a morphism  $\psi : W \rightarrow V$  with  $\varphi \circ \psi = 1_W$  and  $\psi \circ \varphi = 1_V$ .

Note that in general  $\varphi_1, \varphi_2, \dots, \varphi_m$  are not uniquely defined. For example, both  $f = x$  and  $g = x + (xy - 1)$  in the example above define the same morphism from  $V = \mathcal{Z}(xy - 1)$  to  $W = \mathbb{A}^1$ .

Suppose  $F$  is a polynomial in  $k[x_1, \dots, x_m]$ . Then  $F \circ \varphi = F(\varphi_1, \varphi_2, \dots, \varphi_m)$  is a polynomial in  $k[x_1, \dots, x_n]$  since  $\varphi_1, \varphi_2, \dots, \varphi_m$  are polynomials in  $x_1, \dots, x_n$ . If  $F \in \mathcal{I}(W)$ , then  $F \circ \varphi((a_1, a_2, \dots, a_n)) = 0$  for every  $(a_1, a_2, \dots, a_n) \in V$  since  $\varphi((a_1, a_2, \dots, a_n)) \in W$ . Thus  $F \circ \varphi \in \mathcal{I}(V)$ . It follows that  $\varphi$  induces a well defined map from the quotient ring  $k[x_1, \dots, x_m]/\mathcal{I}(W)$  to the quotient ring  $k[x_1, \dots, x_n]/\mathcal{I}(V)$ :

$$\begin{aligned}\tilde{\varphi} : k[W] &\rightarrow k[V] \\ f &\mapsto f \circ \varphi\end{aligned}$$

where  $f \circ \varphi$  is given by  $F \circ \varphi + \mathcal{I}(V)$  for any polynomial  $F = F(x_1, \dots, x_m)$  with  $f = F + \mathcal{I}(W)$ . It is easy to check that  $\tilde{\varphi}$  is a  $k$ -algebra homomorphism (for example,  $\tilde{\varphi}(f + g) = (f + g) \circ \varphi = f \circ \varphi + g \circ \varphi = \tilde{\varphi}(f) + \tilde{\varphi}(g)$  shows that  $\tilde{\varphi}$  is additive). Note also the contravariant nature of  $\tilde{\varphi}$ : the morphism from  $V$  to  $W$  induces a  $k$ -algebra homomorphism from  $k[W]$  to  $k[V]$ .

Suppose conversely that  $\Phi$  is any  $k$ -algebra homomorphism from the coordinate ring  $k[W] = k[x_1, \dots, x_m]/\mathcal{I}(W)$  to  $k[V] = k[x_1, \dots, x_n]/\mathcal{I}(V)$ . Let  $F_i$  be a representative in  $k[x_1, \dots, x_n]$  for the image under  $\Phi$  of  $\bar{x}_i \in k[W]$  (i.e.,  $\Phi(x_i \bmod \mathcal{I}(W))$  is  $F_i \bmod \mathcal{I}(V)$ ). Then  $\varphi = (F_1, \dots, F_m)$  defines a polynomial map from  $\mathbb{A}^n$  to  $\mathbb{A}^m$ , and in fact  $\varphi$  is a morphism from  $V$  to  $W$ . To see this it suffices to check that  $\varphi$  maps a point of  $V$  to a point of  $W$  since by definition  $\varphi$  is already defined by polynomials. If  $g \in \mathcal{I}(W) \subset k[x_1, \dots, x_m]$ , then in  $k[W]$  we have

$$g(x_1 + \mathcal{I}(W), \dots, x_m + \mathcal{I}(W)) = g(x_1, \dots, x_m) + \mathcal{I}(W) = \mathcal{I}(W) = 0 \in k[W],$$

and so

$$\Phi(g(x_1 + \mathcal{I}(W), \dots, x_m + \mathcal{I}(W))) = 0 \in k[V].$$

Since  $\Phi$  is a  $k$ -algebra homomorphism, it follows that

$$g(\Phi(x_1 + \mathcal{I}(W)), \dots, \Phi(x_m + \mathcal{I}(W))) = 0 \in k[V].$$

By definition,  $\Phi(x_i + \mathcal{I}(W)) = F_i \bmod \mathcal{I}(V)$ , so

$$g(F_1 \bmod \mathcal{I}(V), \dots, F_m \bmod \mathcal{I}(V)) = 0 \in k[V],$$

i.e.,

$$g(F_1, \dots, F_m) \in \mathcal{I}(V).$$

It follows that  $g(F_1(a_1, \dots, a_n), \dots, F_m(a_1, \dots, a_n)) = 0$  for every  $(a_1, \dots, a_n)$  in  $V$ . This shows that if  $(a_1, \dots, a_n) \in V$ , then every polynomial in  $\mathcal{I}(W)$  vanishes