on $\varphi(a_1, \ldots, a_n)$. By property (10) of the maps $\mathcal{Z}$ and $\mathcal{I}$ above, this means that $\varphi(a_1, \ldots, a_n) \in \mathcal{Z}(\mathcal{I}(W)) = W$, which proves that φ maps a point in V to a point in W. It follows that $\varphi = (F_1, \ldots, F_m)$ is a morphism from V to W. Since the F_i are well defined modulo $\mathcal{I}(V)$, this morphism from V to W does not depend on the choice of the F_i. Furthermore, the morphism φ induces the original k-algebra homomorphism Φ from $k[W]$ to $k[V]$, i.e., $\widetilde{\varphi} = \Phi$, since both homomorphisms take the value $F_i + \mathcal{I}(V)$ on $x_i + \mathcal{I}(W) \in k[W]$. This proves the first two statements in the following theorem.

Theorem 6. Let $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$ be affine algebraic sets. Then there is a bijective correspondence

$$\left\{ \begin{matrix} \text{morphisms from } V \text{ to } W \\ \text{as algebraic sets} \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} k\text{-algebra homomorphisms} \\ \text{from } k[W] \text{ to } k[V] \end{matrix} \right\}.$$

More precisely,

(1) Every morphism $\varphi : V \to W$ induces an associated k-algebra homomorphism $\widetilde{\varphi} : k[W] \to k[V]$ defined by $\widetilde{\varphi}(f) = f \circ \varphi$.

(2) Every k-algebra homomorphism $\Phi : k[W] \to k[V]$ is induced by a unique morphism $\varphi : V \to W$, i.e., $\Phi = \widetilde{\varphi}$.

(3) If $\varphi : V \to W$ and $\psi : W \to U$ are morphisms of affine algebraic sets, then $\widetilde{\psi \circ \varphi} = \widetilde{\varphi} \circ \widetilde{\psi} : k[U] \to k[V]$.

(4) The morphism $\varphi : V \to W$ is an isomorphism if and only if $\widetilde{\varphi} : k[W] \to k[V]$ is a k-algebra isomorphism.

Proof: The proof of (3) is left as an exercise and (4) is then immediate.

Example

For any infinite field k let $V = \mathbb{A}^1$ and let $W = \mathcal{Z}(x^3 - y^2) = \{(a^2, a^3) \mid a \in k\}$. The map $\varphi : V \to W$ defined by $\varphi(a) = (a^2, a^3)$ is a morphism from V to W. Note that φ is a bijection. The coordinate rings are $k[V] = k[x]$ and $k[W] = k[x, y]/(x^3 - y^2)$ (by the computations in a previous example — it is at this point we need k to be infinite) and the associated k-algebra homomorphism of coordinate rings is determined by

$$\begin{aligned} \widetilde{\varphi} : k[W] &\longrightarrow k[V] \\ x &\mapsto x^2 \\ y &\mapsto x^3. \end{aligned}$$

The image of $\widetilde{\varphi}$ is the subalgebra $k[x^2, x^3] = k + x^2k[x]$ of $k[x]$, so in particular $\widetilde{\varphi}$ is not surjective. Hence $\widetilde{\varphi}$ is not an isomorphism of coordinate rings, and it follows that φ is not an isomorphism of algebraic sets, even though the morphism φ is a bijective map. The inverse map is given by $\psi(0, 0) = 0$ and $\psi(a, b) = b/a$ for $b \neq 0$, and this cannot be achieved by a polynomial map.

The bijection in Theorem 6 gives a translation from maps between two geometrically defined algebraic sets V and W into algebraic maps between their coordinate rings. It also allows us to define a morphism intrinsically in terms of V and W without explicit reference to the ambient affine spaces containing them:

Corollary 7. Suppose $\varphi : V \to W$ is a map of affine algebraic sets. Then φ is a morphism if and only if for every $f \in k[W]$ the composite map $f \circ \varphi$ is an element of $k[V]$ (as a k-valued function on V). When φ is a morphism, $\varphi(v) = w$ with $v \in V$ and $w \in W$ if and only if $\widetilde{\varphi}^{-1}(\mathcal{I}(\{v\})) = \mathcal{I}(\{w\})$.

Proof: We first prove that if φ is any map from V to W such that $\widetilde{\varphi}$ is a k-algebra homomorphism then $\varphi(v) = w$ if and only if $\widetilde{\varphi}^{-1}(\mathcal{I}(\{v\})) = \mathcal{I}(\{w\})$, which will in particular establish the second statement. Note that $\varphi(v) = w$ if and only if every polynomial f vanishing at w vanishes at $\varphi(v)$ (by property (10) above: $\{w\} = \mathcal{Z}(\mathcal{I}(\{w\}))$). Since f vanishes at $\varphi(v)$ if and only if $\widetilde{\varphi}(f)$ vanishes at v, this is equivalent to the statement that $\widetilde{\varphi}(f) \in \mathcal{I}(\{v\})$ for every $f \in \mathcal{I}(\{w\})$, i.e., $\widetilde{\varphi}(\mathcal{I}(\{w\})) \subseteq \mathcal{I}(\{v\})$, or $\mathcal{I}(\{w\}) \subseteq \widetilde{\varphi}^{-1}(\mathcal{I}(\{v\}))$. Since both $\mathcal{I}(\{w\})$ and $\mathcal{I}(\{v\})$ are maximal ideals, this is equivalent to $\widetilde{\varphi}^{-1}(\mathcal{I}(\{v\})) = \mathcal{I}(\{w\})$.

We now prove the first statement. If φ is a morphism, then $f \circ \varphi \in k[V]$ for every $f \in k[W]$. For the converse, observe first that composition with any map $\varphi : V \to W$ defines a k-algebra homomorphism $\widetilde{\varphi}$ from the k-algebra of k-valued functions on W to the k-algebra of k-valued functions on V (this is immediate from the pointwise definition of the addition and multiplication of functions). If $f \circ \varphi \in k[V]$ for every $f \in k[W]$, then $\widetilde{\varphi}$ is a k-algebra homomorphism from $k[W]$ to $k[V]$, so by the proposition, $\widetilde{\varphi} = \widetilde{\Phi}$ for a unique morphism $\Phi : V \to W$. Also, since $\widetilde{\varphi}$ is a k-algebra homomorphism from $k[W]$ to $k[V]$ it follows by what we have already shown that $\varphi(v) = w$ if and only if $\widetilde{\varphi}^{-1}(\mathcal{I}(\{v\})) = \mathcal{I}(\{w\})$. Because $\widetilde{\varphi} = \widetilde{\Phi}$, this is equivalent to $\widetilde{\Phi}^{-1}(\mathcal{I}(\{v\})) = \mathcal{I}(\{w\})$, and so $\Phi(v) = w$. Hence φ and Φ define the same map on V and so φ is a morphism, completing the proof.

Corollary 7 and the last part of Theorem 6 show that the isomorphism type of the coordinate ring of V (as a k-algebra) does not depend on the embedding of V in a particular affine n-space.

Computations in Affine Algebraic Sets and k-algebras

The theory of Gröbner bases developed in Section 9.6 is very useful in computations involving affine algebraic sets, for example in computing in the coordinate rings $k[\mathbb{A}^n]/\mathcal{I}(V)$. When $n > 1$ it can be difficult to describe the elements in this quotient ring explicitly. By Theorem 23 in Section 9.6, each polynomial f in $k[\mathbb{A}^n]$ has a unique remainder after general polynomial division by the elements in a Gröbner basis for $\mathcal{I}(V)$, and this remainder therefore serves as a unique representative for the coset $\bar{f}$ of f in the quotient $k[\mathbb{A}^n]/\mathcal{I}(V)$.

Examples

(1) In the example $W = \mathcal{Z}(x^3 - y^2)$ above, we showed $I = \mathcal{I}(W) = (x^3 - y^2)$ for any infinite field k and so $k[W] = k[x, y]/(x^3 - y^2)$. Here $x^3 - y^2$ gives a Gröbner basis for I with respect to the lexicographic monomial ordering with $y > x$, so every polynomial $f = f(x, y)$ can be written uniquely in the form $f(x, y) = f_0(x) + f_1(x)y + f_I$ with $f_0(x), f_1(x) \in k[x]$ and $f_I \in I$. Then $f_0(x) + f_1(x)y$ gives a unique representative for $\bar{f}$ in $k[W]$. With respect to the lexicographic monomial ordering with $x > y$,

$x^3 - y^2$ is again a Gröbner basis for I, but now the remainder representing $\bar{f}$ in $k[W]$ is of the form $h_0(y) + h_1(y)x + h_2(y)x^2$.

(2) Let $V = \mathcal{Z}(xz+y^2+z^2, xy-xz+yz-2z^2) \subset \mathbb{C}^3$ and $W = \mathcal{Z}(u^3-uv^2+v^3) \subset \mathbb{C}^2$. We shall show later that $I = \mathcal{I}(V) = (xz+y^2+z^2, xy-xz+yz-2z^2) \subset \mathbb{C}[x, y, z]$ and $J = \mathcal{I}(W) = (u^3 - uv^2 + v^3) \subset \mathbb{C}[u, v]$. In this case $u^3 - uv^2 + v^3$ gives a Gröbner basis for J for the lexicographic monomial ordering with $u > v$ similar to the previous example. The situation for I is more complicated. With respect to the lexicographic monomial ordering with $x > y > z$ the reduced Gröbner basis for I is given by

$$g_1 = xy + y^2 + yz - z^2, \qquad g_2 = xz + y^2 + z^2, \qquad g_3 = y^3 - y^2z + z^3.$$

Unique representatives for $\mathbb{C}[V] = \mathbb{C}[x, y, z]/(x^2 + xz + y^2, 2x^2 - xy + xz - yz)$ are given by the remainders after general polynomial division by $\{g_1, g_2, g_3\}$.

We saw already in Section 9.6 that Gröbner bases and elimination theory can be used in the explicit computation of affine algebraic sets $\mathcal{Z}(S)$, or, equivalently, in explicitly solving systems of algebraic equations. The same theory can be used to determine explicitly a set of generators for the image and kernel of a k-algebra homomorphism

$$\Phi : k[y_1, \dots, y_m]/J \longrightarrow k[x_1, \dots, x_n]/I$$

where I and J are ideals. In the particular case when $I = \mathcal{I}(V)$ and $J = \mathcal{I}(W)$ are the ideals associated to affine algebraic sets $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$ then by Theorem 6, the k-algebra homomorphism Φ corresponds to a morphism from V to W, and we shall apply the results here to affine algebraic sets in Section 3.

For $1 \le i \le m$, let $\varphi_i \in k[x_1, \dots, x_n]$ be any polynomial representing the coset $\Phi(\bar{y}_i)$, where as usual we use a bar to denote the coset of an element in a quotient. The polynomials $\varphi_1, \dots, \varphi_n$ are unique up to elements of I. Then the image of a coset $f(y_1, \dots, y_m) + J$ under Φ is the coset $f(\varphi_1, \dots, \varphi_m) + I$. Given any $\varphi_1, \dots, \varphi_n$, the map sending y_i to φ_i induces a k-algebra homomorphism Φ if and only if $f(y_1, \dots, y_m) \in I$ for every $f \in J$, a condition which can be checked on a set of generators for J.

Proposition 8. With notation as above, let $R = k[y_1, \dots, y_m, x_1, \dots, x_n]$ and let $\mathcal{A}$ be the ideal generated by $y_1 - \varphi_1, \dots, y_m - \varphi_m$ together with generators for I. Let G be the reduced Gröbner basis of $\mathcal{A}$ with respect to the lexicographic monomial ordering $x_1 > \cdots > x_n > y_1 > \cdots > y_m$. Then

(a) The kernel of Φ is $\mathcal{A} \cap k[y_1, \dots, y_m]$ modulo J. The elements of G in $k[y_1, \dots, y_m]$ (taken modulo J) generate $\ker \Phi$.

(b) If $f \in k[x_1, \dots, x_n]$, then $\bar{f}$ is in the image of Φ if and only if the remainder after general polynomial division of f by the elements in G is an element $h \in k[y_1, \dots, y_m]$, in which case $\Phi(\bar{h}) = \bar{f}$.

Proof: If we show $\ker \Phi = \mathcal{A} \cap k[y_1, \dots, y_m]$ modulo J then (a) follows by Proposition 30 in Section 9.6. Suppose first that $f \in \mathcal{A} \cap k[y_1, \dots, y_m]$. If $f_1, \dots, f_s$ are generators for I in $k[x_1, \dots, x_n]$, then

$$f(y_1, \dots, y_m) = \sum_{i=1}^{n} a_i(y_i - \varphi_i) + \sum_{j=1}^{s} b_i f_i$$