Shandong University Advanced Modern Algebra

Lecture 13: Introduction to Affine Algebraic Geometry

May 19, 2023

Lecturer: Bin Guan

This lecture refers to Chapter 15 in [1]. All the equation numbers without reference labels are from this book.

Throughout this chapter R will denote a commutative ring with $1 \neq 0$.

1 Affine algebraic sets

1.1 Loci of common zeros

The set $\mathbb{A}^n$ of n-tuples of elements of the field k is called **affine n-space** over k. If $x_1, x_2, \ldots, x_n$ are independent variables over k, then the polynomials $f \in k[x_1, x_2, \ldots, x_n]$ can be viewed as k-valued functions $f : \mathbb{A}^n \to k$ on $\mathbb{A}^n$ by evaluating f at the points in $\mathbb{A}^n$:

$$f : \mathbb{A}^n \to k, \qquad (a_1, a_2, \ldots, a_n) \mapsto f(a_1, a_2, \ldots, a_n) \in k.$$

This gives a ring of k-valued functions on $\mathbb{A}^n$, denoted by $k[\mathbb{A}^n]$ and called the **coordinate ring** of $\mathbb{A}^n$. For instance, when $k = \mathbb{R}$ and $n = 2$, the coordinate ring of Euclidean 2-space $\mathbb{R}^2$ is denoted by $\mathbb{R}[\mathbb{A}^2]$ and is the ring of polynomials in two variables, say x and y, acting as real valued functions on $\mathbb{R}^2$ (the usual "coordinate functions").

Each subset S of functions in the coordinate ring $k[\mathbb{A}^n]$ determines a subset $\mathcal{Z}(S)$ of affine space, namely the set of points where all functions in S are simultaneously zero:

$$\mathcal{Z}(S) := \{(a_1, a_2, \ldots, a_n) \in \mathbb{A}^n \mid f(a_1, a_2, \ldots, a_n) = 0 \text{ for all } f \in S\},$$

where $\mathcal{Z}(\emptyset) := \mathbb{A}^n$. A subset V of $\mathbb{A}^n$ is called an **affine algebraic set** (or just an **algebraic set**) if V is the set of common zeros of some set S of polynomials, i.e., if $V = \mathcal{Z}(S)$ for some $S \subseteq k[\mathbb{A}^n]$. In this case $V = \mathcal{Z}(S)$ is called the **locus** of S in $\mathbb{A}^n$. If $S = \{f\}$ or $\{f_1, \ldots, f_n\}$ we shall simply write $\mathcal{Z}(f)$ or $\mathcal{Z}(f_1, \ldots, f_n)$ for $\mathcal{Z}(S)$ and call it the locus of f or $f_1, \ldots, f_n$, respectively.

Example. *The one-point subsets of $\mathbb{A}^n$ for any n are affine algebraic, since $\{(a_1, a_2, \ldots, a_n)\} = \mathcal{Z}(x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$. More generally, any finite subset of $\mathbb{A}^n$ is an affine algebraic set. For example, $\{(0,0),(1,1)\} = \mathcal{Z}(x(x-1), y(y-1), x(y-1), y(x-1))$.*

Exercise ([1] §15.1 Exercise 14)**.** *Show that, if $n = 1$, the affine algebraic sets in $\mathbb{A}^1$ over any field k are $\emptyset$, k, and finite subsets of k.*

Example. *One may define lines, planes, etc. in $\mathbb{A}^n$ — these are **linear algebraic sets**, the loci of sets of linear (degree 1) polynomials of $k[x_1, x_2, \ldots, x_n]$. For example, a line in $\mathbb{A}^3$ is the locus of two linear polynomials of $k[x, y, z]$ that are not multiples of each other. In particular, the coordinate axes, coordinate planes, etc. in $\mathbb{A}^n$ are all affine algebraic sets. For instance, the x-axis in $\mathbb{A}^3$ is the zero set $\mathcal{Z}(y, z)$ and the x, y-plane is the zero set $\mathcal{Z}(z)$.*

*In general the algebraic set $\mathcal{Z}(f)$ of a nonconstant polynomial f is called a **hypersurface** in $\mathbb{A}^n$. Conic sections are familiar algebraic sets in the Euclidean plane $\mathbb{R}^2$. For example, $\mathcal{Z}(xy - 1)$ is the hyperbola $y = 1/x$. Likewise, quadric surfaces such as the ellipsoid defined by the equation $x^2 + \frac{y^2}{4} + \frac{z^2}{9} = 1$ are affine algebraic sets in $\mathbb{R}^3$.*

Exercise ([1] §15.1 Exercises 21 & 22)**.** *Identify each 2×2 matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with entries from k with the point (a, b, c, d) in $\mathbb{A}^4$. Show that the group $\mathrm{SL}_2(k)$ of matrices of determinant 1 is an algebraic set in $\mathbb{A}^4$. In general, $\mathrm{SL}_n(k)$ is an affine algebraic set in $\mathbb{A}^{n^2}$.*

Note that the locus of a single polynomial of the form $f - g$ is the same as the solutions in affine n-space of the equation $f = g$, so affine algebraic sets are the solution sets to systems of polynomial equations, and as a result occur frequently in mathematics.

There are easily verified properties of affine algebraic sets:

Proposition. *Let S and T be subsets of $k[\mathbb{A}^n]$.*

*(1) $\mathcal{Z}$ is inclusion reversing (i.e., **contravariant**): if $S \subseteq T$ then $\mathcal{Z}(T) \subseteq \mathcal{Z}(S)$.*

(2) $\mathcal{Z}(S) = \mathcal{Z}(I)$, where $I = (S)$ is the ideal in $k[\mathbb{A}^n]$ generated by the subset S.

(3) An arbitrary intersection of affine algebraic sets is an algebraic set: if $\{S_\alpha \mid \alpha \in \lambda\}$ is any collection of subsets of $k[\mathbb{A}^n]$, then $\cap_\alpha \mathcal{Z}(S_\alpha) = \mathcal{Z}(\cup_\alpha S_\alpha)$.

(4) The union of two affine algebraic sets (and by induction, the union of a finite number of affine algebraic sets) is again an affine algebraic set, in fact $\mathcal{Z}(I) \cup \mathcal{Z}(J) = \mathcal{Z}(IJ)$, where I and J are ideals and IJ is their product.

(5) $\mathcal{Z}(0) = \mathbb{A}^n$ and $\mathcal{Z}(1) = \emptyset$ (here 0 and 1 denote constant functions).

Proof. Exercises ([1] §15.1 Exercise 13). □

Properties (3), (4) and (5) in the proposition are the axioms for the **closed sets** in a **topology** on $\mathbb{A}^n$. This topology is called the **Zariski topology** on affine n-space.

Exercise ([1] §15.2 Exercise 22)**.** *Prove that $\mathrm{GL}_n(k)$ is an open affine algebraic set in $\mathbb{A}^{n^2}$ and can be embedded as a closed affine algebraic set in $\mathbb{A}^{n^2+1}$. In particular, deduce that the set $k^\times$ of nonzero elements in $\mathbb{A}^1$ embeds into $\mathbb{A}^2$ as the hyperbola $xy = 1$.*

The Zariski topology is quite "coarse" in the sense that there are "relatively few" closed (or open) sets. For example, for the Zariski topology on $\mathbb{A}^1$ the only closed sets are $\emptyset$, k and the finite sets, and so the nonempty open sets are the complements of finite sets. If k is an infinite field it follows that in the Zariski topology any two nonempty open sets in $\mathbb{A}^1$ have nonempty intersection.

In the language of point-set topology, the Zariski topology is always T_1 (points are closed sets), but for infinite fields the Zariski topology is never T_2 (Hausdorff), i.e., two distinct points never belong to two disjoint open sets (cf. [1] §15.2 Exercise 11). For example, when $k = \mathbb{R}$, a nonempty Zariski open set is just the real line $\mathbb{R}$ with some finite number of points removed, and any two such sets have (infinitely many) points in common.

Note also that the Zariski open (respectively, closed) sets in $\mathbb{R}$ are also open (respectively, closed) sets with respect to the usual Euclidean topology. The converse is not true; for example the interval $[0, 1]$ is closed in the Euclidean topology but is not closed in the Zariski topology. In this sense the Euclidean topology on $\mathbb{R}$ is much "finer": there are many more open sets in the Euclidean topology, in fact the collection of Euclidean open (respectively, closed) sets properly contains the collection of Zariski open (respectively, closed) sets.

Exercise ([1] §15.2 Exercise 27)**.** *When k is an infinite field, prove that the Zariski topology on k^2 is not the same as taking the Zariski topology on k and then forming the product topology on $k \times k$.* [Hint: By [1] §15.1 Exercise 14, in the product topology on $k \times k$, the closed sets in $k \times k$ are finite unions of sets of the form $\{a\} \times \{b\}$, $\{a\} \times k$ and $k \times \{b\}$, for any $a, b \in k$.]

1.2 Coordinate rings

By property (2) in the above proposition, every affine algebraic set is the algebraic set corresponding to an ideal of the coordinate ring. Thus we may consider

$$\mathcal{Z} : \{\text{ideals of } k[\mathbb{A}^n]\} \longrightarrow \{\text{affine algebraic sets in } \mathbb{A}^n\}.$$

Recall that, every ideal I in the Noetherian ring $k[x_1, x_2, \ldots, x_n]$ is finitely generated, say $I = (f_1, f_2, \ldots, f_q)$. It follows from property (3) that $\mathcal{Z}(I) = \mathcal{Z}(f_1) \cap \mathcal{Z}(f_2) \cap \cdots \cap \mathcal{Z}(f_q)$, 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 $k \geq 1$.

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

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

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

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

Example. *Over any field k, the ideal of functions vanishing at $(a_1, a_2, \ldots, a_n) \in \mathbb{A}^n$ is a maximal ideal since it is the kernel of the surjective ring homomorphism from $k[x_1, \ldots, x_n]$ to the field k given by evaluation at $(a_1, a_2, \ldots, a_n)$. It follows that*

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

Example. *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 $\{(t^2, t^3) \mid t \in k\}$.*

For any polynomial $f(x, y) \in k[x, y] = k[x][y]$ we can write

$$f(x, y) = f_0(x) + f_1(x)y + (x^3 - y^2)g(x, y).$$

For any $f(x, y) \in \mathcal{I}(V)$ (i.e., $f(t^2, t^3) = 0$ for all $t \in k$), it follows that $f_0(t^2) + f_1(t^2)t^3 = 0$ for all $t \in k$. If k is infinite, the polynomial $f_0(t^2) + f_1(t^2)t^3$ has infinitely many zeros if and only if all its 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

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

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 the polynomial $x(x - 1) \in \mathcal{I}(V)$. in fact $\mathcal{I}(V) = \mathfrak{m}_1\mathfrak{m}_2$ where $\mathfrak{m}_1 = (x, y)$ and $\mathfrak{m}_2 = (x - 1, y - 1)$ (cf. [1] §15.1 Exercise 15).

The following properties of the map $\mathcal{I}$ (and relations between the maps $\mathcal{Z}$ and $\mathcal{I}$) are very easy exercises.

Proposition. *Let A and B be subsets of $\mathbb{A}^n$.*

*(6) $\mathcal{I}$ is also **contravariant**: if $A \subseteq B$ then $\mathcal{I}(B) \subseteq \mathcal{I}(A)$.*

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

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

(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) $\mathcal{Z}(\mathcal{I}(\mathcal{Z}(I))) = \mathcal{Z}(I)$ and $\mathcal{I}(\mathcal{Z}(\mathcal{I}(A))) = \mathcal{I}(A)$, i.e., 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 $\mathcal{I}(V)$.

Proof. Exercises ([1] §15.1 Exercise 13). □

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.

Exercise ([1] §15.1 Exercise 18)**.** *If $k = \mathbb{F}_q$ is the finite field with q elements, show that $\mathcal{I}(\mathbb{A}^1)$ is the nontrivial ideal in $k[x]$ generated by $x^q - x$.*

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 $\overline{f} := f + \mathcal{I}(V)$ giving the elements of the quotient $k[V]$ are precisely the restrictions to V of ordinary polynomial functions $f : \mathbb{A}^n \to k$ (which helps to explain the notation $k[V]$).

Note that $k[V]$ is a Noetherian ring since the quotient of a Noetherian ring is also Noetherian. If x_i denotes the i^{th} coordinate function on $\mathbb{A}^n$ (projecting an n-tuple onto its i^{th} component), then the restriction $\overline{x_i}$ of x_i to V (which also just gives the i^{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 $\overline{x_1}, \dots, \overline{x_n}$ (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.*

In the quotient ring $\mathbb{R}[V]$ we have $xy = 1$, so $\mathbb{R}[V] \cong \mathbb{R}[x, 1/x]$. For any function $\overline{f} \in \mathbb{R}[V]$ and any $(a,b) \in V$ we have $\overline{f}(a,b) = f(a, 1/a)$ for any preimage $f \in \mathbb{R}[x,y]$ of $\overline{f}$.

1.3 Morphisms of algebraic sets

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

$$\varphi\Big((a_1, \ldots, a_n)\Big) = \Big(\varphi_1(a_1, \ldots, a_n), \ldots, \varphi_m(a_1, \ldots, a_n)\Big)$$

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

Note that in general $\varphi_1, \ldots, \varphi_m$ 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 $W = \mathbb{A}^1$.

Exercise ([1] §15.1 Exercise 25)**.** *Suppose $V \subseteq \mathbb{A}^n$ is an affine algebraic set and $f \in k[V]$. The **graph** of f is the collection of points $\big\{\big(a_1, \ldots, a_n, f(a_1, \ldots, a_n)\big)\big\}$ in $\mathbb{A}^{n+1}$. Prove that the graph of f is an affine algebraic set isomorphic to V.* [Hint: The morphism in one direction maps $(a_1, \ldots, a_n)$ to $\big(a_1, \ldots, a_n, f(a_1, \ldots, a_n)\big)$.]

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

$$\tilde{\varphi} : k[W] \to k[V], \quad f \mapsto f \circ \varphi := F \circ \varphi + \mathcal{I}(V) \text{ for any polynomial } F \text{ with } f = F + \mathcal{I}(W).$$

It is easy to check that $\tilde{\varphi}$ is a k-algebra homomorphism. Note also the contravariant nature of $\tilde{\varphi}$: the morphism from V to W induces a k-algebra homomorphism from $k[W]$ to $k[V]$.

Theorem ([1] §15.1 Theorem 6)**.** *Let $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$ be affine algebraic sets. Then there is a bijective correspondence*

$$\{\textit{morphisms } \varphi : V \to W \textit{ as algebraic sets}\} \longleftrightarrow \{k\textit{-algebra homomorphisms } \tilde{\varphi} : k[W] \to k[V]\}.$$

More precisely,

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

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

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

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

Proof. Exercise. □

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 $k[W] = k[x, y]/(x^3 - y^2)$ (it is at this point we need k to be infinite) and the associated k-algebra homomorphism of coordinate rings is determined by

$$\tilde{\varphi} : k[W] \to k[V], \quad x \mapsto x^2, \quad y \mapsto x^3.$$

The image of $\tilde{\varphi}$ is the subalgebra $k[x^2, x^3] = k + x^2k[x] \subsetneq k[x]$, so in particular $\tilde{\varphi}$ is not surjective. Hence $\tilde{\varphi}$ 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.

Exercise. *Show that for any field k the hyperbola $\mathcal{Z}(xy - 1)$ is not isomorphic to an affine line $\mathbb{A}^1$.*

The bijection in the above theorem 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 ([1] §15.1 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 $\tilde{\varphi}^{-1}(\mathcal{I}(\{v\})) = \mathcal{I}(\{w\})$.*

The above Theorem and Corollary 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.

2 Connections between geometry and algebra

2.1 Radicals and Hilbert's Nullstellensatz

Since the zeros of a polynomial f are the same as the zeros of the powers $f^2, f^3, \ldots$ in general there are many different ideals in the ring $k[x_1, x_2, \ldots, x_n]$ whose zero locus define the same algebraic set V in affine n-space. This leads to the notion of the radical of an ideal, which can be defined in any commutative ring:

Definition. *Let I be an ideal in a commutative ring R.*

(1) The ***radical*** *of I, denoted by $\sqrt{I}$ or $\operatorname{rad} I$, is the collection of elements in R some power of which lie in I, i.e.,*

$$\sqrt{I} = \operatorname{rad} I := \{a \in R \mid a^k \in I \text{ for some } k \geq 1\}.$$

(2) The radical of the zero ideal is called the ***nilradical*** *of R. (Note that $a \in R$ is in the nilradical of R if and only if some power of a is 0, so the nilradical of R is the set of all nilpotent elements of R.)*

(3) An ideal I is called a ***radical ideal*** *if $I = \operatorname{rad} I$.*

Example. *In the ring of integers* $\mathbb{Z}$*, the ideal* (a) *is a radical ideal if and only if* a *is square-free or zero. More generally, if* $a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ *with* $k_i \geq 1$ *for all* i*, is the prime factorization of the positive integer* a*, then* $\operatorname{rad}(a) = (p_1 p_2 \cdots p_r)$*.*

More generally, in any U.F.D. R*,* $\operatorname{rad}(a) = (p_1 p_2 \cdots p_r)$ *if* $a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ *is the unique factorization of* a *into distinct irreducibles.*

Theorem ([1] §15.2 Corollary 13)**.** *Prime (and hence also maximal) ideals are radical.*

We saw in the preceding section that if we restrict to the set of ideals I of $k[\mathbb{A}^n]$ arising as the ideals associated with some algebraic set V, i.e., with $I = \mathcal{I}(V)$, then the maps $\mathcal{Z}$ (from such ideals to algebraic sets) and $\mathcal{I}$ (from algebraic sets to ideals) are inverses of each other: $\mathcal{Z}(\mathcal{I}(V)) = V$ and $\mathcal{I}(\mathcal{Z}(I)) = I$.

By definition, the ideal $\mathcal{I}(V)$ is always a radical ideal. But for arbitrary fields k, it is in general not true that every radical ideal is the ideal of some algebraic set, i.e., of the form $\mathcal{I}(V)$ for some algebraic set V. For example, the ideal $(x^2 + 1)$ in $\mathbb{R}[x]$ is maximal, hence is a radical ideal, but is not the ideal of any algebraic set — if it were, then $x^2 + 1$ would have to vanish on that set, but x^2+1 has no zeros in $\mathbb{R}$. A similar construction works for any field k that is not algebraically closed — there exists an irreducible polynomial $p(x)$ of degree at least 2 in $k[x]$, which then generates the maximal (hence radical) ideal $(p(x))$ in $k[x]$ that has no zeros in k.

The next theorem provides a fundamental connection between "geometry" and "algebra", and shows that over an algebraically closed field (such as $\mathbb{C}$) every radical ideal is of the form $\mathcal{I}(V)$. Over these fields the "geometrically defined" ideals $I = \mathcal{I}(V)$ are therefore the same as the radical ideals, which is a "purely algebraic" property of the ideal I (namely that $I = \operatorname{rad} I$).

Theorem ([1] §15.3 Theorems 31 & 32, Hilbert's Nullstellensatz)**.** *Let* $k = \bar{k}$ *be an algebraically closed field. Then*

- $\mathcal{I}(\mathcal{Z}(I)) = \operatorname{rad} I$ *for every ideal* I *of* $k[x_1, x_2, \ldots, x_n]$*. Moreover, the maps* $\mathcal{Z}$ *and* $\mathcal{I}$ *in the correspondence*

$$\{\textit{affine algebraic sets}\} \underset{\mathcal{Z}}{\overset{\mathcal{I}}{\rightleftarrows}} \{\textit{radical ideals}\}$$

  are bijections that are inverses of each other.

- M *is a maximal ideal in the polynomial ring* $k[x_1, x_2, \ldots, x_n]$ *if and only if* $M = (x_1 - a_1, \ldots, x_n - a_n)$ *for some* $a_1, \ldots, a_n \in k$*. Equivalently, the maps* $\mathcal{Z}$ *and* $\mathcal{I}$ *give a bijective correspondence*

$$\{\textit{points in } \mathbb{A}^n\} \underset{\mathcal{Z}}{\overset{\mathcal{I}}{\rightleftarrows}} \{\textit{maximal ideals in } k[\mathbb{A}^n]\}.$$

  Moreover, if I *is any proper ideal in* $k[x_1, x_2, \ldots, x_n]$ *then* $\mathcal{Z}(I) \neq \emptyset$*.*

The last statement of the Nullstellensatz shows that, there always exists at least one common zero ("nullstellen" in German) for all the polynomials contained in a proper ideal (over an algebraically closed field).

The maps $\mathcal{I}$ and $\mathcal{Z}$ in the Nullstellensatz are defined over any field k, and as mentioned are not bijections if k is not algebraically closed. For any field k, however, the map $\mathcal{Z}$ is always surjective and the map $\mathcal{I}$ is always injective (cf. [1] §15.2 Exercise 9).

2.2 The Zariski topology on algebraic sets

Recall that the **Zariski topology** on affine n-space over an arbitrary field k is the topology in which the closed sets are the affine algebraic sets in $\mathbb{A}^n$. A similar definition can be used to define a Zariski topology on any algebraic set V in $\mathbb{A}^n$, as follows.

If $k[V]$ is the coordinate ring of V, then the distinct elements of $k[V]$ define distinct k-valued functions on V and there is a natural way of defining

$$\begin{array}{lll} \mathcal{Z}: & \{\text{ideals in } k[V]\} & \longrightarrow & \{\text{algebraic subsets of } V\} \\ \mathcal{I}: & \{\text{subsets of } V\} & \longrightarrow & \{\text{(radical) ideals in } k[V]\} \end{array}$$

just as for the case $V = \mathbb{A}^n$. For example, if $\overline{J}$ is an ideal in $k[V]$, then $\mathcal{Z}(\overline{J})$ is the set of elements in V that are common zeros of all the functions in the ideal $\overline{J}$. It is easy to verify that the resulting zero sets in V satisfy the three axioms for a topological space, defining a **Zariski topology** on V, where the closed sets are the algebraic subsets, $\mathcal{Z}(\overline{J})$. for any ideal $\overline{J}$ of $k[V]$.

Exercise. *Recall that in a topological space X, the closed sets with respect to the* ***subspace topology*** *of a subspace Y are defined to be the sets $C \cap Y$, where C is a closed set in X. Show that the Zariski topology on V is just the subspace topology for $V \subseteq \mathbb{A}^n$.* (The advantage to the definition of the Zariski topology on V above is that it is defined intrinsically in terms of the coordinate ring $k[V]$ of V, and since the isomorphism type of $k[V]$ does not depend on the affine space $\mathbb{A}^n$ containing V, the Zariski topology on V also depends only on V and not on the ambient affine space in which V may be embedded.)

In fact the Zariski topology is the coarsest topology in which points are closed and for which polynomial maps are continuous.

Exercise. *(1) If V and W are two affine algebraic spaces, show that a morphism $\varphi : V \to W$ is continuous with respect to the Zariski topologies on V and W* (cf. [1] §15.1 Exercise 27, which shows that the inverse image of a Zariski closed set under a morphism is Zariski closed).

(2) ([1] §15.2 Exercise 17) *Show that there are Zariski continuous maps from $\mathbb{A}^1$ to itself that are not polynomials.*

If $\varphi : V \to W$ is a morphism of algebraic sets, the image $\varphi(V)$ of V need not be an algebraic subset of W, i.e., need not be Zariski closed in W. For example the projection of the hyperbola $V = \mathcal{Z}(xy - 1)$ in $\mathbb{R}^2$ onto the x-axis has image $\mathbb{R}^1 - \{0\}$, which as we have just seen is not an affine algebraic set.

We have the usual topological notions of closure and density with respect to the Zariski topology: For any subset A of $\mathbb{A}^n$, the **Zariski closure** of A is the smallest algebraic set containing A. If $A \subseteq V$ for an algebraic set V, then A is **Zariski dense** in V if the Zariski closure of A is V.

Example. *If $k = \mathbb{R}$, the algebraic sets in $\mathbb{A}^1$ are $\emptyset$, $\mathbb{R}$, and finite subsets of $\mathbb{R}$ (by [1] §15.1 Exercise 14). The Zariski closure of any infinite set A of real numbers is then all of $\mathbb{A}^1$, and A is Zariski dense in $\mathbb{A}^1$.*

Proposition ([1] §15.2 Proposition 15)**.** *The Zariski closure of a subset A in $\mathbb{A}^n$ is $\mathcal{Z}(\mathcal{I}(A))$.*

Proof. Certainly $A \subseteq \mathcal{Z}(\mathcal{I}(A))$. For any algebraic set $V \supseteq A$, we have $\mathcal{I}(V) \subseteq \mathcal{I}(A)$ and $\mathcal{Z}(\mathcal{I}(A)) \subseteq \mathcal{Z}(\mathcal{I}(V)) = V$, so $\mathcal{Z}(\mathcal{I}(A))$ is the smallest algebraic set containing A. □

The next result shows that the Zariski closure of the image of a morphism is determined by the kernel of the associated k-algebra homomorphism.

Proposition ([1] §15.2 Proposition 16)**.** *Suppose $\varphi : V \to W$ is a morphism of algebraic sets and $\tilde{\varphi} : k[W] \to k[V]$ is the associated k-algebra homomorphism of coordinate rings. Then* $\ker \tilde{\varphi} = \mathcal{I}(\varphi(V))$*, and the Zariski closure of $\varphi(V)$ is the zero set in W of* $\ker \tilde{\varphi}$*. In particular, the homomorphism $\tilde{\varphi}$ is injective if and only if $\varphi(V)$ is Zariski dense in W.*

2.3 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. 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. 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. An irreducible affine algebraic set is called an **affine variety**.

Example. *If k is an infinite field, then the varieties in $\mathbb{A}^1$ are the whole space and the one-point subsets. What are the varieties in $\mathbb{A}^1$ in the case of a finite field k?*

Proposition ([1] §15.2 Proposition 17 & Corollary 18)**.** *The affine algebraic set V is irreducible if and only if $\mathcal{I}(V)$ is a prime ideal, if and only if its coordinate ring $k[V]$ is an integral domain.*

Proof. Exercise. □

Example. *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.*

The hyperbola $xy = 1$ in $\mathbb{R}^2$ is a variety since 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. [1] §15.2 Exercises 12 & 13).

Exercise ([1] §15.2 Exercise 15)**.** *Suppose V is a hypersurface in $\mathbb{A}^n$ and $\mathcal{I}(V) = (f)$ for some nonconstant polynomial $f \in k[x_1, x_2, \ldots, x_n]$. Prove that V is a variety if and only if f is irreducible.*

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

$$k(V) := \{f/g \mid f, g \in k[V],\ g \neq 0\}.$$

The elements of $k(V)$ are called **rational functions** on V. The **dimension** of a variety V, denoted $\dim V$, is defined to be the transcendence degree of $k(V)$ over k.

Example. *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.*

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. [1] §15.1 Exercise 23). 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.

From the Nullstellensatz we have a dictionary between geometric and ring-theoretic objects over the algebraically closed field k:

Geometry	**Algebra**
affine algebraic set V	coordinate ring $k[V]$
points of V	maximal ideals of $k[V]$
affine algebraic subsets in V	radical ideals of $k[V]$
subvarieties in V	prime ideals in $k[V]$
morphism $\varphi : V \to W$	k-algebra homomorphism $\tilde{\varphi} : k[W] \to k[V]$

2.4 Local rings of affine algebraic varieties

Let k be an algebraically closed field and let V be an affine variety over k with coordinate ring $\mathcal{O}_V = k[V]$ and field of rational functions $k(V)$.

The elements of $k[V]$ can be considered as k-valued functions on V, and if the denominator doesn't vanish, the same is true for an element of $k(V)$ (which helps to explain the terminology for this field). Since the same element of $k(V)$ may be written in the form f/g in several ways (since $k[V]$ is an integral domain, $f/g = f_1/g_1$ if and only if $fg_1 = f_1g$), we make the following definition:

Definition. *We say $f/g \in k(V)$ is **regular at** v or **defined at the point** $v \in V$ if there is some $f_1, g_1 \in k[V]$ with $f/g = f_1/g_1$ and $g_1(v) \neq 0$.* (If f_2, g_2 is another such pair with $g_2(v) \neq 0$, then $f_1(v)/g_1(v) = f_2(v)/g_2(v)$ as elements of k, so whenever f/g is regular at v there is a well-defined way of specifying its value in k at v.)

For each point $v \in V$ the collection of rational functions on V that are defined at v,

$$\mathcal{O}_{v,V} \coloneqq \{f/g \in k(V) \mid f/g \textit{ is regular at } v, \textit{ i.e. } f/g = f_1/g_1 \textit{ with } g_1(v) \neq 0\},$$

*is called the **local ring** of V at v. In particular, $\mathcal{O}_{v,V}$ is a local ring with unique maximal ideal $\mathfrak{m}_{v,V}$, where*

$$\mathfrak{m}_{v,V} \coloneqq \{f/g \in \mathcal{O}_{v,V} \mid f/g = f_1/g_1 \textit{ with } f_1(v) = 0,\ g_1(v) \neq 0\}$$

is the set of rational functions on V that are defined and equal to 0 at v.

For any point $v \in V$, a rational function f/g is regular at v if and only if $f/g = f_1/g_1$ for some $f_1, g_1 \in k[V]$ with $g_1 \notin \mathcal{I}(v)$, the ideal of functions on V that are zero at v. This means that the set $\mathcal{O}_{v,V}$ of rational functions that are defined at v is the same as the **localization** of $\mathcal{O}_V = k[V]$ at the maximal ideal $\mathcal{I}(v) = \{g \in k[V] \mid g(v) = 0\}$. This shows that $\mathcal{O}_{v,V}$ depends intrinsically on the ring $k[V]$ and is independent of the embedding of V in a particular affine space.

Since $\mathcal{O}_{v,V}$ is a localization of the Noetherian integral domain $k[V]$ at a prime ideal, $\mathcal{O}_{v,V}$ is also a Noetherian integral domain. Note also that $\mathcal{O}_{v,V}/\mathfrak{m}_{v,V} \cong k[V]/\mathcal{I}(v) \cong k$ by [1] §15.4 Proposition 46(5).

Recall that the polynomial maps from V to k are also referred to as the **regular** maps of V to k. This is because these are precisely the rational functions on V that are regular everywhere (cf. [1] §15.4 Proposition 51). The corresponding algebraic property of this is that, any integral domain R is the intersection of its localizations at all its maximal ideals (cf. [1] §15.4 Proposition 48).

Suppose $\varphi : V \to W$ is a morphism of affine varieties with associated k-algebra homomorphism $\tilde{\varphi} : k[W] \to k[V]$. If $v \in V$ is mapped to $w \in W$ by φ, then it is straightforward to show that $\tilde{\varphi}$ induces a homomorphism (also denoted by $\tilde{\varphi}$) between the corresponding local rings:

$$\tilde{\varphi} : \mathcal{O}_{w,W} \to \mathcal{O}_{v,V} \quad \text{where} \quad \tilde{\varphi}(h/k) = \tilde{\varphi}(h)/\tilde{\varphi}(k),$$

and that under this homomorphism, $\tilde{\varphi}^{-1}(\mathfrak{m}_{v,V}) = \mathfrak{m}_{w,W}$ (a homomorphism of local rings having this property is called a **local homomorphism**). It is also easy to check that, if $\psi \circ \varphi$ is a composition of morphisms, then on the local rings $\widetilde{\psi \circ \varphi} = \tilde{\varphi} \circ \tilde{\psi}$.

3 The prime spectrum of a ring

3.1 The Zariski topology on a spectrum

Throughout this section the term "ring" will mean commutative ring with 1 and all ring homomorphisms $\varphi : R \to S$ will be assumed to map 1_R to 1_S.

We have seen that most of the geometric properties of affine algebraic sets V over k can be translated into algebraic properties of the associated coordinate rings $k[V]$ of k-valued functions on V. In this development we have generally started with geometric properties of the affine algebraic sets and then seen that many of the algebraic properties common to the associated coordinate rings can be defined for arbitrary commutative rings.

Suppose now we try to reverse this, namely start with a general commutative ring as the algebraic object and attempt to define a corresponding "geometric" object by analogy with $k[V]$ and V. Given a commutative ring R, perhaps the most natural analogy with $k[V]$ and V would suggest defining the collection of maximal ideals $\mathfrak{m}$ of R as the "points" of the associated geometric object. Under this definition, if $\tilde{\varphi} : R' \to R$ is a ring homomorphism, then $\tilde{\varphi}^{-1}(M)$ should correspond to the maximal ideal $\mathfrak{m}$. Unfortunately, the inverse image of a maximal ideal by a ring homomorphism in general need not be a maximal ideal (cf. [1] §7.4 Exercise 13). Since the inverse image of a prime ideal under a ring homomorphism (that maps 1 to 1) is prime, this suggests that a better definition might include the prime ideals of R.

Definition. *Let R be a commutative ring with* 1.

- *The* ***spectrum*** *or* ***prime spectrum*** *of R, denoted* $\operatorname{Spec} R$, *is the set of all prime ideals of R.*
- *The set of all maximal ideals of R, denoted* $\operatorname{mSpec} R$, *is called the* ***maximal spectrum*** *of R.*

Example. *If k is a field then* $\operatorname{Spec} k = \operatorname{mSpec} k = \{(0)\}$.

If $R = \mathbb{Z}$ then $\operatorname{Spec} \mathbb{Z} = \{(0)\} \cup \{(p) \mid p > 0$ *is a prime*$\}$, *and* $\operatorname{mSpec} \mathbb{Z} = \operatorname{Spec} \mathbb{Z} - \{(0)\}$.

The elements of $\operatorname{Spec} \mathbb{Z}[x]$ *are the following:*

(a) (0)*;*

(b) (p) *where p is a prime in $\mathbb{Z}$;*

(c) $(f(x))$ *where $1 \neq f \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Q}[x]$, and the g.c.d. of its coefficients is equal to* 1*;*

(d) $(p, g(x))$ *where p is a prime in $\mathbb{Z}$ and g is a monic polynomial that is irreducible* $\bmod\ p$.

The elements of $\operatorname{mSpec} \mathbb{Z}[x]$ *are the primes in* (d) *above.*

In the analogy with $k[V]$ and V when k is algebraically closed, the elements $f \in k[V]$ are functions on V with values in k, obtained by evaluating f at the point v in V. Note that "evaluation at v" defines a homomorphism from $k[V]$ to k with kernel $\mathcal{I}(v)$, and that the value of f at v is the element of k representing f in the quotient $k[V]/\mathcal{I}(V) \cong k$. Put another way, the value of $f \in k[V]$ at $v \in V$ can be viewed as the element $\bar{f} \in k[V]/\mathcal{I}(V) \cong k$. A similar definition can be made in general:

Definition. *If $f \in R$, then the* ***value*** *of f at the point $\mathfrak{p} \in \operatorname{Spec} R$ is the element $f(\mathfrak{p}) := \bar{f} \in R/\mathfrak{p}$.*

Note that the values of f at different points $\mathfrak{p}$ in general lie in different integral domains.

There are analogues of the maps $\mathcal{Z}$ and $\mathcal{I}$ and also for the Zariski topology. For any subset A of R define

$$\mathcal{Z}(A) := \{\mathfrak{p} \in \operatorname{Spec} R \mid A \subseteq \mathfrak{p}\} \subseteq \operatorname{Spec} R,$$

the collection of prime ideals containing A. It is immediate that $\mathcal{Z}(A) = \mathcal{Z}(I)$, where $I = (A)$ is the ideal generated by A, so there is no loss simply in considering $\mathcal{Z}(I)$ where I is an ideal of R. Note that, by definition, $\mathcal{Z}(I)$ consists of the points in $\operatorname{Spec} R$ at which all the functions in I have the value 0.

For any subset Y of $\operatorname{Spec} R$ define

$$\mathcal{I}(Y) := \bigcap_{\mathfrak{p} \in Y} \mathfrak{p} \subseteq R,$$

the intersection of the prime ideals in Y, i.e. $\mathcal{I}(Y)$ consists of the functions in R "vanishing" at all points $\mathfrak{p} \in Y$.

Proposition ([1] §15.5 Proposition 53)**.** *Let R be a commutative ring with 1. The maps $\mathcal{Z}$ and $\mathcal{I}$ between R and $\operatorname{Spec} R$ defined above satisfy*

(1) for any ideal I of R, $\mathcal{Z}(I) = \mathcal{Z}(\operatorname{rad}(I)) = \mathcal{Z}(\mathcal{I}(\mathcal{Z}(I)))$, and $\mathcal{I}(\mathcal{Z}(I)) = \operatorname{rad} I$,

(2) for any ideals I, J of R, $\mathcal{Z}(I \cap J) = \mathcal{Z}(IJ) = \mathcal{Z}(I) \cup \mathcal{Z}(J)$, and

(3) if $\{I_\alpha\}$ is an arbitrary collection of ideals of R, then $\mathcal{Z}(\cup I_\alpha) = \cap \mathcal{Z}(I_\alpha)$.

The proposition shows that the collection $\{\mathcal{Z}(I) \mid I \text{ is an ideal of } R\}$ satisfies the three axioms for the closed sets of a topology on $\operatorname{Spec} R$. The topology on $\operatorname{Spec} R$ defined by the closed sets $\mathcal{Z}(I)$ for the ideals I of R is called the **Zariski topology** on $\operatorname{Spec} R$.

By definition, the closure in the Zariski topology of the singleton set $\{\mathfrak{p}\}$ in $\operatorname{Spec} R$ consists of all the prime ideals of R that contain $\mathfrak{p}$. In particular, a point $\mathfrak{p}$ in $\operatorname{Spec} R$ is closed in the Zariski topology if and only if the prime ideal $\mathfrak{p}$ is not contained in any other prime ideals of R, i.e., if and only if $\mathfrak{p}$ is a maximal ideal (so the Zariski topology on $\operatorname{Spec} R$ is not generally Hausdorff). The maximal ideals of R are called the **closed points** in $\operatorname{Spec} R$. In terms of the terminology above, the points in $\operatorname{Spec} R$ that are closed in the Zariski topology are precisely the points in $\operatorname{mSpec} R$.

A closed subset of a topological space is **irreducible** if it is not the union of two proper closed subsets, or, equivalently, if every nonempty open set is dense.

Proposition ([1] §15.5 Proposition 54)**.** *The maps $\mathcal{Z}$ and $\mathcal{I}$ define inverse bijections*

$$\begin{aligned}
\{\textit{Zariski closed subsets of } \operatorname{Spec} R\} &\xrightleftharpoons[\mathcal{Z}]{\mathcal{I}} \{\textit{radical ideals in } R\}, \\
\{\textit{Zariski closed points in } \operatorname{Spec} R\} &\xrightleftharpoons{} \{\textit{maximal ideals in } R\}, \\
\{\textit{irreducible subsets of } \operatorname{Spec} R\} &\xrightleftharpoons{} \{\textit{prime ideals in } R\}.
\end{aligned}$$

If $\varphi : R \to S$ is a ring homomorphism mapping 1_R to 1_S and $\mathfrak{p}$ is a prime ideal in S, then $\varphi^{-1}(\mathfrak{p})$ is a prime ideal in R. This defines a map $\varphi^* : \operatorname{Spec} S \to \operatorname{Spec} R$ with $\varphi^*(\mathfrak{p}) := \varphi^{-1}(\mathfrak{p})$.

Proposition ([1] §15.5 Proposition 55)**.** *Every ring homomorphism $\varphi : R \to S$ mapping 1_R to 1_S induces a map $\varphi* : \operatorname{Spec} S \to \operatorname{Spec} R$ that is continuous with respect to the Zariski topologies on $\operatorname{Spec} R$ and $\operatorname{Spec} S$.*

Proof. If $\mathcal{Z}(I) \subseteq \operatorname{Spec} R$ is a Zariski closed subset of $\operatorname{Spec} R$, then it is easy to show that $(\varphi*)^{-1}(\mathcal{Z}(I))$ is the Zariski closed subset $\mathcal{Z}(\varphi(I)S)$ defined by the ideal generated by $\varphi(I)$ in S. Since the inverse image of a closed subset in $\operatorname{Spec} R$ is a closed subset in $\operatorname{Spec} S$, the induced map φ^* is continuous in the Zariski topology. □

While the generalization from affine algebraic sets to $\operatorname{Spec} R$ for general rings R has made matters slightly more complicated, there are (at least) two very important benefits gained by this more general setting. The first is that $\operatorname{Spec} R$ can be considered even for commutative rings R containing nilpotent elements; the second is that $\operatorname{Spec} R$ need not be a k-algebra for any field k, and even when it is, the field k need not be algebraically closed. The fact that many of the properties found in the situation of affine k-algebras hold in more general settings then allows the application of "geometric" ideas to these situations (for example, to $\operatorname{Spec} R$ when R is finite).

Example. *The natural inclusion $\varphi : \mathbb{Z} \to \mathbb{Z}[i]$ induces a map $\varphi^* : \operatorname{Spec} \mathbb{Z}[i] \to \operatorname{Spec} \mathbb{Z}$. The fiber (i.e. preimage) of φ^* over the nonzero prime P in $\mathbb{Z}$ consists of the prime ideals of $\mathbb{Z}[i]$ containing P. If $P = (p)$ where $p = 2$ or p is a prime $\equiv 3 \bmod 4$, then there is only one element in this fiber; if p is a prime $\equiv 1 \bmod 4$, then there are two elements in the fiber: the primes (π) and (π') where $p = \pi\pi'$ in $\mathbb{Z}[i]$ (cf. [1] §8.3 Proposition 18).*

3.2 Affine schemes

The space $\operatorname{Spec} R$ together with its Zariski topology gives a geometric generalization for arbitrary commutative rings of the points in a variety V. We now consider the question of generalizing the ring of rational functions on V.

When V is a variety over the algebraically closed field k, the elements in the quotient field $k(V)$ of the coordinate ring $k[V]$ define the rational functions on V. Each element α in $k(V)$ can in general be written as a quotient a/f of elements $a, f \in k[V]$ in many different ways. The set of points U at which α is regular is an open subset of V; by definition, it consists of all the points $v \in V$ where α can be represented by some quotient a/f with $f(v) \neq 0$, and then the representative a/f defines an element in the local ring $\mathcal{O}_{v,V}$. Note also that the same representative a/f defines α not only at v, but also at all the other points where f is nonzero, namely on the open subset

$$V_f := \{w \in V \mid f(w) \neq 0\} = V - \mathcal{Z}(f)$$

of V. These open sets V_f (called **principal open sets**) for the various possible representatives a/f for α give an open cover of U.

This interpretation of rational functions as functions that are regular on open subsets of V can be generalized to $\operatorname{Spec} R$. We first define the analogues X_f in $X = \operatorname{Spec} R$ of the sets V_f and establish their basic properties.

Definition. *For any $f \in R$ let*

$$X_f := \{\mathfrak{p} \in X = \operatorname{Spec} R \mid f \notin \mathfrak{p}\} = \{\mathfrak{p} \in X \mid f(\mathfrak{p}) \neq 0\}.$$

The set X_f is called a ***principal*** *(or* ***basic****)* ***open set*** *in* $\operatorname{Spec} R$.

Since X_f is the complement of the Zariski closed set $\mathcal{Z}(f)$ it is indeed an open set in $\operatorname{Spec} R$ as the name implies. In fact, the principal open sets form a basis for the Zariski topology on $\operatorname{Spec} R$, i.e., every Zariski open set in X is the union of some collection of principal open sets X_f (cf. [1] §15.5 Proposition 56(4)).

We now define an analogue for $X = \operatorname{Spec} R$ of the rational functions on a variety V. As we observed, for the variety V a rational function $\alpha \in k(V)$ is a regular function on some open set U. At each point $v \in U$ there is a representative a/f for α with $f(v) \neq 0$, and this representative is an element in the localization $\mathcal{O}_{v,V} = k[V]_{\mathcal{I}(v)}$. In this way the regular function α on U can be considered as a function from U to the disjoint union of these localizations: the point $v \in U$ is mapped to the representative $a/f \in k[V]_{\mathcal{I}(v)}$. Furthermore the same representative can be used simultaneously not only at v but on the whole Zariski neighborhood V_f of v (so, "locally near v", α is given by a single quotient of elements from $k[V]$). Note that a/f is an element in the localization $k[V]_f$, which is contained in each of the localizations $k[V]_{\mathcal{I}(w)}$ for $w \in V_f$.

We now generalize this to $\operatorname{Spec} R$ by considering the collection of functions s from the Zariski open subset $U \subseteq \operatorname{Spec} R$ to the disjoint union of the localizations $R_{\mathfrak{p}}$ for $\mathfrak{p} \in U$, such that $s(\mathfrak{p}) \in R_{\mathfrak{p}}$ and such that s is given locally by quotients of elements of R. More precisely:

Definition. *Let R be a commutative ring with* 1, *and let $X = \operatorname{Spec} R$. Suppose U is a Zariski open subset of* $\operatorname{Spec} R$. *Define $\mathcal{O}(\emptyset) := 0$. If U is nonempty, define $\mathcal{O}(U)$ to be the set of functions $s : U \to \bigsqcup_{\mathfrak{q} \in U} R_{\mathfrak{q}}$ from U to the disjoint union of the localizations $R_{\mathfrak{q}}$ for $\mathfrak{q} \in U$ with the following two properties:*

- *$s(\mathfrak{q}) \in R_{\mathfrak{q}}$ for every $\mathfrak{q} \in U$, and*
- *for every $\mathfrak{p} \in U$ there is an open neighborhood $X_f \subseteq U$ of $\mathfrak{p}$ and an element a/f^n in the localization R_f defining s on X_f, i.e., $s(\mathfrak{q}) = a/f^n \in R_{\mathfrak{q}}$ for every $\mathfrak{q} \in X_f$.*

It is easy to verify that each $\mathcal{O}(U)$ is a commutative ring with identity (cf. [1] §15.5 Exercise 18), and if U' is an open subset of U, then there is a natural restriction map $\mathcal{O}(U) \to \mathcal{O}(U')$ which is a homomorphism of rings (cf. [1] §15.5 Exercise 19). The collection of rings $\mathcal{O}(U)$ for the Zariski open sets of X together with the restriction maps $\mathcal{O}(U) \to \mathcal{O}(U')$ for $U' \subseteq U$ is called the ***structure sheaf*** *on X, and is denoted simply by $\mathcal{O}$ (or $\mathcal{O}_X$). The elements $s \in \mathcal{O}(U)$ are called the* ***sections*** *of $\mathcal{O}$ over U. The elements of $\mathcal{O}(X)$ are called the* ***global sections*** *of $\mathcal{O}$.*

The next proposition generalizes the result of [1] §15.4 Proposition 51 that the only rational functions on a variety V that are regular everywhere are the elements of the coordinate ring $k[V]$.

Proposition ([1] §15.5 Proposition 57)**.** *Let $X = \operatorname{Spec} R$ and let $\mathcal{O} = \mathcal{O}_X$ be its structure sheaf. The global sections of $\mathcal{O}$ are the elements of R, i.e., $\mathcal{O}(X) \cong R$. More generally, $\mathcal{O}(X_f) \cong R_f$, where X_f is a principal open set in X for some $f \in R$.*

Definition. *Let R be a commutativering with 1. The pair $(\operatorname{Spec} R, \mathcal{O}_{\operatorname{Spec} R})$, consisting of the space* $\operatorname{Spec} R$ *with the Zariski topology together with the structure sheaf $\mathcal{O}_{\operatorname{Spec} R}$ is called an* ***affine scheme****.*

The notion of an affine scheme gives a completely algebraic generalization of the geometry of affine algebraic sets valid for arbitrary commutative rings, and is the starting point for modem algebraic geometry. Theorem 59 in [1] §15.5 shows that the appropriate place to view affine schemes is in the category of locally ringed spaces. Roughly speaking, a **locally ringed space** is a topological space X together with a collection of rings $\mathcal{O}(U)$ for each open subset of X (with a compatible set of homomorphisms $\mathcal{O}(U) \to \mathcal{O}(U')$ if $U' \subseteq U$ and with some local conditions on the sections) such that the **stalks** $\mathcal{O}_P := \varinjlim \mathcal{O}(U)$ (the direct limit of the rings $\mathcal{O}(U)$ for the open sets U of X containing P, where the **direct limit** is defined in [1] §7.6 Exercise 8) are local rings. The morphisms in this category are continuous maps between the topological spaces together with ring homomorphisms between corresponding $\mathcal{O}(U)$ with precisely the same conditions as imposed in the definition of a morphism of affine schemes.

A **scheme** is a locally ringed space in which each point lies in a neighborhood isomorphic to an affine scheme (with some compatibility conditions between such neighborhoods), and is a fundamental object of study in modern algebraic geometry. The affine schemes considered here form the building blocks that are "glued together" to define general schemes in the same way that ordinary Euclidean spaces form the building blocks that are "glued together" to define manifolds in analysis.

Other related exercises in [1]

§15.1	16 19 23 24
§15.2	3 4 6 8 10 16 18 19 20 21 23 45
§15.3	2 3
§15.4	25 26
§15.5	1 2 4 6 7 9 10 11 13 14 18 21 23 31

References

[1] D. S. Dummit and R. M. Foote. *Abstract algebra.* John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.