Proof: For any ideal I, the ideal rad I is finitely generated since R is Noetherian. If $a_1, \ldots, a_m$ are generators of rad I, then by definition of the radical, for each i we have $a_i^{k_i} \in I$ for some positive integer k_i. Let k be the maximum of all the k_i. Then the ideal $(\operatorname{rad} I)^{km}$ is generated by elements of the form $a_1^{d_1} a_2^{d_2} \cdots a_m^{d_m}$ where $d_1 + \cdots + d_m = km$, and each of these elements has at least one factor $a_i^{d_i}$ with $d_i \geq k$. Then $a_i^{d_i} \in I$, hence each generator of $(\operatorname{rad} I)^{km}$ lies in I, and so $(\operatorname{rad} I)^{km} \subseteq I$.

The Zariski Topology

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 $\mathcal{I}(\mathcal{Z}(I)) = I$. The elements of the ring $k[\mathbb{A}^n]/\mathcal{I}(V)$ give k-valued functions on V and, since k has no nilpotent elements, powers of nonzero functions are also nonzero functions. Put another way, the ring $k[\mathbb{A}^n]/\mathcal{I}(V)$ has no nilpotent elements, so by Proposition 11, the ideal $\mathcal{I}(V)$ is always a radical ideal.

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 (by Corollary 13), 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. It is perhaps surprising that the presence of polynomials in one variable that have no zeros is the *only* obstruction to a radical ideal (in *any* number of variables) not being of the form $\mathcal{I}(V)$. This is shown by the next theorem, which 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. *(Hilbert's Nullstellensatz)* Let E be an algebraically closed field. Then $\mathcal{I}(\mathcal{Z}(I)) = \operatorname{rad} I$ for every ideal I of $E[x_1, x_2, \ldots, x_n]$. Moreover, the maps $\mathcal{Z}$ and $\mathcal{I}$ in the correspondence

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

are bijections that are inverses of each other.

Proof: This will be proved in the next section (cf. Theorem 32).

Example

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. Exercise 9).

One particular consequence of the Nullstellensatz is that for any *proper* ideal I we have $\mathcal{Z}(I) \neq \emptyset$ since rad $I \neq k[\mathbb{A}^n]$. Hence 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).

We next see that the affine algebraic sets define a topology on affine n-space. Recall that a *topological space* is any set X together with a collection of subsets $\mathcal{T}$ of X, called the *closed sets* in X, satisfying the following axioms:

(i) an arbitrary intersection of closed sets is closed: if $S_i \in \mathcal{T}$ for i in any index set, then $\cap S_i \in \mathcal{T}$,

(ii) a finite union of closed sets is closed: if $S_1, \ldots, S_q \in \mathcal{T}$ then $S_1 \cup \cdots \cup S_q \in \mathcal{T}$, and

(iii) the empty set and the whole space are closed: $\emptyset, X \in \mathcal{T}$.

A subset U of X is called *open* if its complement, $X - U$, is closed (i.e., $X - U \in \mathcal{T}$). The axioms for a topological space are often (equivalently) phrased in terms of the collection of open sets in X.

There are many examples of topological spaces, and a wealth of books on topology. A fixed set X may have a number of different topologies on it, and the collections of closed sets need not be related in these different structures. On any set X there are always at least two topologies: the so-called discrete topology in which every subset of X is closed (i.e., $\mathcal{T}$ is the collection of *all* subsets of X), and the so-called trivial topology in which the only closed sets are $\emptyset$ and X required by axiom (iii).

Suppose now that $X = \mathbb{A}^n$ is affine n-space over an arbitrary field k. Then the collection $\mathcal{T}$ consisting of all the affine algebraic sets in $\mathbb{A}^n$ satisfies the three axioms for a topological space — these are precisely properties (3), (4) and (5) of algebraic sets in the preceding section. It follows that these sets can be taken to be the closed sets in a topology on $\mathbb{A}^n$:

Definition. 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 $\mathbb{A}^n$.

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 (cf. Exercise 14 in Section 1), 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. the exercises). 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.

The Zariski topology on $\mathbb{A}^n$ is defined so that the affine algebraic subsets of $\mathbb{A}^n$ are closed. In other words, the topology is defined by the zero sets of the ideals in the coordinate ring of $\mathbb{A}^n$. 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

$$\mathcal{Z} : \{\,\text{ideals in } k[V]\,\} \longrightarrow \{\,\text{algebraic subsets of } V\,\}$$
$$\mathcal{I} : \{\,\text{subsets of } V\,\} \longrightarrow \{\,\text{ideals in } k[V]\,\}$$

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 $k[V]$. By the Lattice Isomorphism Theorem, the ideals of $k[V]$ are the ideals of $k[x_1, \dots, x_n]$ that contain $\mathcal{I}(V)$ taken mod $\mathcal{I}(V)$. If J is the complete preimage in $k[x_1, \dots, x_n]$ of $\overline{J}$, then the locus of J in $\mathbb{A}^n$ is the same as the locus of $\overline{J}$ in V. It follows that this definition of the Zariski topology on V is just the *subspace topology* for $V \subseteq \mathbb{A}^n$. (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.) 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.

If V and W are two affine algebraic spaces, then since a morphism $\varphi : V \to W$ is defined by polynomial functions, it is easy to see that φ is *continuous* with respect to the Zariski topologies on V and W (cf. Exercise 27 in Section 1, which shows that the inverse image of a Zariski closed set under a morphism is Zariski closed). In fact the Zariski topology is the coarsest topology in which points are closed and for which polynomial maps are continuous. There exist maps that are continuous with respect to the Zariski topology that are not morphisms, however (cf. Exercise 17).

We have the usual topological notions of closure and density with respect to the Zariski topology.

Definition. 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.

For example, if $k = \mathbb{R}$, the algebraic sets in $\mathbb{A}^1$ are $\emptyset$, $\mathbb{R}$, and finite subsets of $\mathbb{R}$ by Exercise 14 in Section 1. The Zariski closure of any infinite set A of real numbers is then all of $\mathbb{A}^1$ and A is Zariski dense in $\mathbb{A}^1$.