Lecture 4-2: Radical ideals, varieties, and the Nullstellensatz

April 2, 2025

I will tighten the correspondence between ideals in polynomial rings and algebraic sets, heading toward the Nullstellensatz, the first major result of algebraic geometry.

Let k be an infinite field. We have seen that to any ideal I of $P_n = k[x_1, \ldots, x = n]$ one can attach the set $\mathcal{Z}(I) \subset \mathbf{A}^n$ of common zeros of the polynomials in I, and conversely so any set $S \subset \mathbf{A}^n$ one can attach the ideal $\mathcal{I}(S)$ of polynomials in P_n vanishing on S. It is natural to hope that the maps $I \to \mathcal{Z}(I), S \to \mathcal{I}(S)$ would be inverses of each other, but we see at once that this is false: the only subsets in the range of the first map are Zariski closed ones, so that one must at least restrict to closed subsets S. What is less obvious is that one needs to restrict the ideals too: the principal ideals $I_1 = (x^2)$ and $I_2 = (x)$ in P_1 have $\mathcal{Z}(I_1) = \mathcal{Z}(I_2) = \{0\}$. Finally, one needs additional hypotheses on k: the ideal $J = (x^2 + 1)$ in $\mathbb{R}[x]$ has $\mathcal{Z}(J) = \emptyset$.

I address ideals first. Given an ideal I in any commutative ring R we set rad $I = \sqrt{I} = \{x \in R : x^n \in I$ for some $n\}$. We say that I is radical if $\sqrt{I} = I$. Then we have

Proposition, p.673

$\sqrt{I}$ is the unique smallest radical ideal containing I. If $R = P_m$, a polynomial ring over a field k, then the ideal $\mathcal{I}(S)$ of any algebraic set S is radical.

Indeed, if $a, b \in \sqrt{I}$, with $a^n, b^m \in I$, then the binomial theorem (valid in any commutative ring) shows that all terms of $(a+b)^{n+m}$ lie in I, whence $a + b \in \sqrt{I}$. Also $(ra)^n \in I$ for any $r \in R$ and if $c^r \in \sqrt{I}$ for some integer r, then $c^{rs} \in I$ for some r, s, so that $\sqrt{I}$ is indeed an ideal and the smallest radical one containing I. The second assertion is clear.

Next we study the geometric side more closely.

Definition, p. 679

An algebraic set $V \subset \mathbf{A}^n$ is called *irreducible*, or a *variety*, if it is not the union of two proper algebraic subsets.

Proposition, p. 680

An algebraic set $V \subset \mathbf{A}^m$ is irreducible if and only if its ideal $\mathcal{I}(V)$ is prime. Every algebraic set is uniquely the union $V_1 \cup \cdots \cup V_n$ of irreducible subsets such that $V_i \not\subseteq V_j$ with $i \neq j$.

Proof.

Recall first that an ideal I of a commutative ring R is prime if we have $xy \in I$ if and only if $x \in I$ or $y \in I$, for $x, y \in R$. Suppose first that $V = V_1 \cup V_2$ is reducible. Since the V_i are proper subsets of V there are $f_1, f_2 \notin I$ vanishing on V_1, V_2, respectively, so that $f_1 f_2$ vanishes on $V_1 \cup V_2 = I$ and $f_1 f_2 \in I$, so that I is not prime. Conversely, if I is not prime, let $f_1 f_2 \in I$ but $f_1, f_2 \notin I$. Then $V_1 = \mathcal{Z}(f_1) \cap V$, $V_2 = \mathcal{Z}(f_2) \cap V$ are proper subsets (their corresponding ideals containing polynomials not in I) whose union is V, so that V is reducible. For the second assertion, let $\mathcal{S}$ be the collection of nonempty algebraic subsets of $\mathbf{A}^m$ that are not finite unions of varieties. Choose $S \in \mathcal{S}$ with $I = \mathcal{I}(S)$ maximal; this is possible since P_m is Noetherian. Then $V_0 = \mathcal{Z}(I)$ is a minimal element of $\mathcal{S}$, which must be reducible, so that it is the union $S_1 \cup S_2$ of two proper algebraic subsets, whose ideals must be strictly larger than I. The construction then forces S_1, S_2 to be finite unions of varieties, whence so is S, a contradiction. $\square$

Proof.

Thus every algebraic set is a finite union of varieties V_i; we can then omit varieties contained in others to arrive at a decomposition $V = V_1 \cup \cdots \cup V_n$ with $V_i \not\subseteq V_j$ for $i \neq j$. Given a second such decomposition $U_1 \cup \cdots \cup U_r$ of V, each V_i is the union of its intersections with the U_j, forcing one of these intersections to be all of V_i, so that $V_i \subseteq U_j$; similarly every U_i lies some V_k. But then we must have $n = r$ and the U_i are a permutation of the V_j, as claimed. □

The V_i are called the irreducible components of V. Note that, unlike connected components of topological spaces, irreducible components can overlap; for example, the union of two intersecting lines in $\mathbb{R}^2$ or $\mathbb{C}^2$ is an algebraic set whose components are the lines.

As a corollary, we note that the radical ideal $\mathcal{I}(V)$ of any nonempty algebraic set $V = \cup_{i=1}^{m} V_i$ is a finite intersection of prime ideals $\mathcal{I}(V_i)$. We will later see that every proper radical ideal is $\mathcal{I}(V)$ for some V, so that every radical ideal in P_m is a finite intersection of prime ideals. Conversely, and more generally, it is easy to see that any intersection of prime ideals in any ring is radical.

In fact, any radical ideal I in any ring R is the intersection of prime ideals (Proposition 12, p. 674). This can be taken to be a finite intersection if R is Noetherian.

Finally, we need to assume more about the basefield k to get a bijection between radical ideals in P_m and algebraic subsets of $\mathbf{A}^m$. The additional hypothesis should come as no surprise.

Nullstellensatz: Theorem 32, p. 700

If k is algebraically closed, the maps $I \to \mathcal{Z}(I), S \to \mathcal{I}(S)$ provide inclusion-reversing inverse bijections between Zariski closed subsets of $\mathbf{A}^m$ and radical ideals in P_m.

We will prove this next time, using something called the Noether Normalization Lemma. The German word Nullstellensatz means “zero-places-theorem”.

An ideal P is prime in a ring R if and only if the quotient ring R/P is an integral domain, since $xy = 0$ in this quotient if and only if $x = 0$ or $y = 0$. Thus the coordinate ring $P_m/\mathcal{I}(V)$ of a variety $V \subset \mathbf{A}^m$ has a quotient field $k(V)$, called its (rational) function field, which has a finite transcendence degree over k (being finitely generated as a field). We define the dimension of V to be this transcendence degree (p. 681). This definition agrees with intuition. For example, a 0-dimensional subvariety of $\mathbf{A}^n$ is just a point in this set, while a vector subspace S of k^n has the same dimension as a variety as it does as a vector space. To see this, extend a basis $v_1, \ldots, v_m$ of S to a basis $b_1, \ldots, b_n$ of k^n. The b_i are just linear combinations of standard basis vectors e_i, so that we can take the b_i to be a set of algebraically independent generators of the polynomial ring P_n. Then S is the set of common zeros of the b_j for $j > m$, regarded as linear polynomials, so that the coordinate ring of S identifies with the polynomial ring $k[b_1, \ldots, b_m]$ and its quotient field is the rational function field in m variables over k.

The dimension of an algebraic set V is the maximum dimension of any irreducible component V_i of V; note that it is possible for different components of V to have different dimensions, for example if V is the union of a plane and a line intersecting it but not lying in it. We will see later that a proper subvariety of a variety V always has smaller dimension and that a variety V_d of dimension d always admits a chain of subvarieties $V_0 \subset V_1 \cdots \subset V_d$ such that $\dim V_i = i$.

As a simple example going beyond vector subspaces (to which we will return a number of times), take the subvariety V of $\mathbf{A}^2$ defined by the single equation $x^3 - y^2 = 0$. The polynomial $x^3 - y^2$ generates the full ideal $\mathcal{I}(V)$ of polynomials vanishing on V (see the argument in Example 3, p. 660). A typical point on V takes the form $(a, b) \in k^2$ with $a^3 = b^2$; if $a \neq 0$, then $b \neq 0$ and we can write $a = (b/a)^2, b = (b/a)^3$. Thus every point in V takes the form (t^2, t^3) for a unique $t \in k$, for even if $a = b = 0$ we can take $t = 0$. It follows that V is indeed irreducible, with function field $k(t)$ (the field of rational functions in one variable). The coordinate ring $k[V]$ of V may be identified with the subring $k[t^2, t^3]$ of the polynomial ring $P_1 = k[t]$ generated by t^2 and t^3.

It follows that the the map ϕ from $\mathbf{A}^1$ to V sending t to (t^2, t^3), which is clearly a morphism, is bijective, but not an isomorphism, since its inverse is not a morphism. (The corresponding algebra homomorphism, embedding $k[t^2, t^3]$ into $k[t]$, also fails to be an isomorphism.) Thus morphisms of varieties are more subtle than linear maps between vector spaces, since inverses of linear maps are always linear. If we remove the point $(0, 0)$ from V we get a set V' which is isomorphic to $S = k^*$. Now S is not given to us as a variety and in fact is not a subvariety of $\mathbf{A}^1$.

Nevertheless S is isomorphic to a subvariety W of $\mathbf{A}^2$, namely the one given by the equation $xy - 1 = 0$; the isomorphism from W to S is just the first coordinate projection, sending (x, y) to x. Thus nonalgebraic subsets of $\mathbf{A}^n$ can still have the structure of varieties, so that we cannot afford to limit attention to just algebraic subsets of a fixed $\mathbf{A}^n$. Ultimately we are forced, as in manifold theory, to consider topological spaces covered by open sets, each isomorphic to a variety, but which are not themselves varieties. These are called schemes; I will say a bit more about them later.