Lecture 5-10: Noether normalization and the proof of the Nullstellensatz

May 10, 2024

As previously promised, we prove the Nullstellensatz, using the Noether Normalization Lemma.

We begin by recalling the notion of integrality from an earlier discussion of character theory. Given commutative rings $A \subset B$ we say that $b \in B$ is integral over A if we have $b^n + \sum_{i=0}^{n-1} a_i b^i = 0$ for some $a_0, \ldots, a_{n-1} \in A$. We have already seen that the set of elements in B integral over A is a subring containing A; we call it the integral closure of A in B (DF, p. 691) and denote it by $\overline{A}$. The integral closure of $\overline{A}$ in B is then just $\overline{A}$. An integral domain is called integrally closed or normal if it is integrally closed in its quotient field. For example, we previously showed that $\mathbb{Z}$ is integrally closed; the same argument shows that any unique factorization domain is integrally closed.

We need a simple lemma.

Proposition; DF, p. 694

If A and B are integral domains with B integral over A (that is, every element of B integral over A), then A is a field if and only if B is.

If A is a field and $b \in B$ with $b \neq 0$ satisfies $b^n + \sum_{i=0}^{n-1} a_i b^i = 0$, then by cancelling a suitable power of b we may assume that $a_0 \neq 0$, whence b has the multiplicative inverse $-a_0^{-1}(b^{n-1} + \sum_{i=1}^{n-1} a_i b^{i-1})$.

Conversely, if B is a field, then any $a \in A$ with $a \neq 0$ has a multiplicative inverse a^{-1} in B, which must be integral over A, so that $a^{-n} + \sum i = 0^{n-1} c_i a^{-i} = 0$ for some $c_i \in A$. Multiplying by a^{n-1}, we see that $a^{-1} \in A$, as desired.

Now we are ready to prove

Theorem; Noether Normalization Lemma; DF, p. 699

Let k be a field and suppose that $A = k[r_1, \ldots, r_n]$ is a finitely generated k-algebra. Then for some $m \leq n$ there are elements $y_1 \ldots, y_m$ algebraically independent over k such that A is integral and finitely generated as a module over the k-subalgebra $k[y_1, \ldots, y_m]$.

Proof.

By induction on n. If the r_i are already algebraically independent then there is nothing to prove. Otherwise there is a nonzero f in the polynomial ring $P_n = k[x_1, \ldots, x_n]$, say of degree d, with $f(r_1, \ldots, r_n) = 0$. Renumbering the variables if necessary, we may assume that f is a nonconstant polynomial in x_n with coefficients in $k[x_1 \ldots, x_{n-1}]$. We now change variables, transforming f into a monic polynomial in x_n whose coefficients lie in a subring of A generated by $n - 1$ elements. □

Proof.

Define integers $\alpha_i = (1+d)^i$ and new variables $X_i = x_i - x_n^{\alpha_i}$ for $1 \leq i \leq n-1$. Let $g(X_1, \ldots, X_{n-1}, x_n) = f(X_1 + x_n^{\alpha_1}, \ldots, X_{n-1} + x_n^{\alpha_{n-1}}, x_n)$, so that g is a polynomial in the X_i and x_n. Each monomial term of f contributes a single term of the form a constant times x_n^e to g for some e. The choice of α_i guarantees that different terms of f give different values of e. Hence if N is the highest power of x_n that occurs in g then we have $g = cx_n^N + \sum_{i=0}^{N-1} h_i(X_1, \ldots, X_{n-1})x_n^i$ for some nonzero c. Setting $s_i = r_i - r_n^{\alpha_i}$, we get $\frac{1}{c}g(s_1 \ldots, s_{n-1}, r_n) = \frac{1}{c}f(r_1, \ldots, r_n) = 0$, so that r_n is integral over $B = k[s_1, \ldots, s_{n-1}]$. Each r_i for $1 \leq i \leq n-1$ is also integral over $B[r_n]$, so A is integral over $B[r_n]$ and thus also over B. An appeal to the inductive hypothesis completes the proof. □

It follows at once form this lemma and the preceding one that a finitely generated k-algebra A that is a field is a finite extension of k, since Noether normalization implies that A is integral over a polynomial ring $k[y_1, \ldots, y_m]$, which is a field if and only if $m = 0$. Then we get

Theorem: Weak Nullstellensatz, DF, p. 700

If k is algebraically closed and I is a proper ideal in a polynomial ring $P_n = k[x_1, \ldots, x_n]$ then $\mathcal{V}(I) \neq \emptyset$.

Proof.

Enlarge I to a maximal ideal M of P_n. Then the coordinate ring P_n/M is a finitely generated k-algebra that is a field, whence by algebraic closure it must be isomorphic to k. If the surjection from P_n to k sends the variable x_i to $a_i \in k$, then $\mathcal{Z}(M)$ is the point $(a_1, \ldots, a_n) \in k^n$, whence $\mathcal{Z}(M)$ and $\mathcal{Z}(I)$ are nonempty. □

Finally we are ready to prove the full Nullstellensatz.

Theorem: Nullstellensatz

If k is algebraically closed and $I \subset P_n$ is a proper ideal, then $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$. In particular the maps $\mathcal{Z}, \mathcal{I}$ define inverse inclusion-reversing bijections between Zariski closed subsets of k^n and radical ideals in P_n.

Proof.

Clearly $\sqrt{I} \subseteq \mathcal{I}(\mathcal{Z}(I))$, so it remains to prove the reverse inclusion. Let $f_1, \ldots, f_m$ be a finite set of generators of I and let $g \in \mathcal{I}(\mathcal{Z}(I))$. Introduce a new variable x_{n+1} and consider the ideal I' generated by $f_1, \ldots, f_m$ and $x_{n+1}g - 1$ in P_{n+1}. At any point of $\mathbf{A}^{n+1}$ where the f_i vanish so too does g, whence $x_{n+1}g - 1$ does not vanish. Hence $\mathcal{Z}(I') = \emptyset$, whence I' must be all of P_{n+1}. Now we have an equation $1 = a_1 f_1 + \cdots + a_m f_m + a_{m+1}(x_{n+1}g - 1)$ for some $a_i \in P_{n+1}$. Setting $y = \frac{1}{x_{n+1}}$ and multiplying by a high power of y we get $y^N = c_1 f_1 + \cdots + c_m f_m + c_{m+1}(g - y)$ for some $c_i \in k[x_1, \ldots, x_n, y]$. Substituting g for y in this last equation shows that $g^N \in I = (f_1, \ldots, f_m)$, so that $g \in \sqrt{I}$, as desired. □

A side benefit of Noether normalization is that it gives us another way to compute the dimension of an algebraic set V: writing the coordinate ring $k[V]$ as a finitely generated integral extension of a polynomial ring $k[y_1, \ldots, y_d]$, we take the dimension of V to be d. This is justified since if V is irreducible then the quotient field of $k[V]$ is a finite extension of the rational function field in d variables over k, so has transcendence degree d. But now it turns out that there is more that we can say about the morphism $V \to \mathbf{A}^d$ giving rise to the inclusion $k[y_1, \ldots, y_d] \subset k[V]$.

As an example of this, consider again the subvariety V of say $\mathbb{C}^2$ defined by the equation $x^3 - y^2 = 0$. We have seen that the coordinate ring of V may be identified with the subring $R = \mathbb{C}[t^2, t^3]$ of $S = \mathbb{C}[t]$; the inclusion of R into S corresponds to the morphism $t \mapsto (t^2, t^3)$ of $\mathbf{A}^1 (= \mathbb{C})$ to V, which is bijective. But we also have the maps $S \to R$ sending t to t^2, or t to t^3; these correspond to the projections π_1, π_2 from V onto its first and second coordinates. These maps are generically two-to-one and three-to one, respectively, though in both cases there is only one preimage of 0, namely the origin $(0, 0)$. Thus these maps are not covering maps of topological spaces; we call them ramified finite covers, since not all fibers have the same size.

More generally, we want to study the relationship between ideals of a ring R and those of a ring S containing R. We call the ring S an extension of R.If I is an ideal of R then it generates an ideal $I^e = IS$ of S, called the extension of I; similarly, given an ideal J of S, its contraction $J^c = J \cap R$ is an ideal of R. Clearly any ideal I of R lies in the contraction I^{ec} of its extension to S and any ideal J of S contains the extension J^{ce} of its contraction to R, but in general we do not get equality in either case. The contraction $P = Q^c$ of a prime ideal Q in S is prime in R, since the quotient R/P, as a subring of S/Q, cannot have zero divisors if S/Q does not. On the other hand, the contraction of a maximal ideal in S need not be maximal in R; nor is it true that every prime ideal of R, or even every maximal ideal, is the contraction of some ideal in S. We focus on maximal ideals here because the Nullstellensatz implies that maximal ideal in the coordinate ring $k[V]$ of an algebraic set V correspond bijectively to points of V.

If S is integral over R, however, then we have more control over the situation. Given a prime ideal P of R that is the contraction Q^c of a prime ideal Q of S, we know that P is maximal if and only if Q is maximal by a previous result, since S/Q is integral over R/P and both are integral domains. If in addition S is finitely generated as a ring over R, say by $s_1, \ldots, s_m$, then given any homomorphism π from R with kernel P to a field K there are only finitely many ways to extend π to S, since each generator must go to a root of a monic polynomial with specified coefficients. It follows that there are only finitely many ideals Q whose contraction is a fixed maximal ideal of P of R, all of them maximal (DF, Corollary 27, p. 695). We will see next time that there is always at least one such ideal Q.