The Nullstellensatz

I will prove a version of the Nullstellensatz that gives somewhat more “geometric” information than just the statement that a proper ideal, J, in the polynomial ring $k[X_1, \dots, X_n]$ has zeros in K^n, where K is any algebraically closed field containing k. This statement is the weak (but not wussy) Nullstellensatz. The strong Nullstellensatz, $I(V(J)) = \operatorname{rad} J$, for any algebraically closed field K containing k, follows by the Rabinowitsch trick, given at the end of this note.

Since any proper ideal is contained in a prime ideal $P \subset k[X_1, \dots, X_n]$, it suffices to prove that prime ideals have zeros. A zero of P in K^n is the same thing as a homomorphism

$$\phi : k[X_1, \dots, X_n]/P \to K,$$

extending the identity inclusion of k into K. Now, $k[x_1, \dots, x_n] = k[X_1, \dots, X_n]/P$ is an integral domain, hence has a transcendence base over k. Specifically, WLOG, we may assume $\{x_1, \dots, x_r\}$ are algebraically independent over k, and that every element of $k[x_1, \dots, x_n]$ is algebraic over (the field of fractions of) $k[x_1, \dots, x_r]$. The ring $k[x_1, \dots, x_r]$ is isomorphic to a polynomial ring in r variables. We allow $r = 0$, which just means that $k[x_1, \dots, x_n] = k[X_1, \dots, X_n]/P$ is an algebraic field extension of k. It is easy to construct homomorphisms $\phi : k[x_1, \dots, x_r] \to K$. Given arbitrary elements $\gamma_j \in K,\ 1 \le j \le r$, there is a homomorphism $\phi : k[x_1, \dots, x_r] \to K$ with $\phi(x_j) = \gamma_j$. I claim that most such ϕ extend to homomorphisms $\Phi : k[x_1, \dots, x_n] = k[X_1, \dots, X_n]/P \to K$, giving us our desired zeros of P. More precisely,

Proposition 1 *There is a non-zero polynomial $a(x_1, \dots, x_r) \in k[x_1, \dots, x_r]$ so that if $a(\gamma_1, \dots, \gamma_r) \neq 0 \in K$, then the homomorphism $\phi : k[x_1, \dots, x_r] \to K$ with $\phi(x_j) = \gamma_j$ extends to*

$$\Phi : k[x_1, \dots, x_n] = k[X_1, \dots, X_n]/P \to K.$$

□

Since K is an infinite field, the polynomial $a(x_1, \dots, x_r)$ is non-zero at most points $(\gamma_1, \dots, \gamma_r) \in K^r$. The proof will show that each ϕ has finitely many extensions Φ. Each extension Φ is a point $(\gamma_1, \dots, \gamma_n) \in V(P) \subset K^n$ whose first r coordinates are $(\gamma_1, \dots, \gamma_r) \in K^r$. Thus we have a picture of the variety $V(P) \subset K^n$ projecting in a finite-to-one manner onto at least the complement of a hypersurface $a(x_1, \dots, x_r) = 0$ in K^r. (Points in the hypersurface may or may not be in the image of $V(P)$.) The transcendence degree, r, of $k[x_1, \dots, x_n] = k[X_1, \dots, X_n]/P$ over k provides an algebraic interpretation of the geometric dimension of the variety $V(P) \subset K^n$, when, say, $K = \mathbb{C}$.

Example 1 Consider $P = (XY^2 - 1) \subset k[X, Y]$. Then $\{x\}$ is a transcendence base of $k[x, y] = k[X, Y]/(XY^2 - 1)$ over k. For every $\gamma \neq 0 \in K$, there are two points (γ, ν_1) and $(\gamma, \nu_2) \in V(P) \subset K^2$ with first coordinate γ. The plane curve $xy^2 - 1 = 0$ projects in a two-to-one manner onto the complement of $x = 0$ in K^1. Draw yourself a picture here (over $k = K = \mathbb{R}$ anyway). □

So, how do we prove the proposition? Using the “going up” theorem for integral ring extensions, that’s how. Notice if $k[x_1, \dots, x_r] \subset k[x_1, \dots, x_n] = k[X_1, \dots, X_n]/P$ is an integral ring extension, then any ring homomorphism $\phi : k[x_1, \dots, x_r] \to K$ extends to $\Phi : k[x_1, \dots, x_n] = k[X_1, \dots, X_n]/P \to K$. Namely, let $Q_0 = \ker \phi \subset k[x_1, \dots, x_r]$. The going up theorem states that there is a prime ideal $Q \subset k[x_1, \dots, x_n] = k[X_1, \dots, X_n]/P$ with $Q \cap k[x_1, \dots, x_r] = Q_0$. Then $k[x_1, \dots, x_n]/Q$ is an integral, hence algebraic, extension of its subring $k[x_1, \dots, x_r]/Q_0$. The same statement holds for the fields of fractions of these two integral domains. Since K is algebraically closed, the embedding $k[x_1, \dots, x_r]/Q_0 \subset K$ induced by ϕ extends to an embedding $k[x_1, \dots, x_n]/Q \subset K$, which defines $\Phi : k[x_1, \dots, x_n] \to K$, with $\ker \Phi = Q$.

In the general case, $k[x_1,\dots,x_r] \subset k[x_1,\dots,x_n]$ is only an algebraic extension of integral domains. Each x_{r+j} satifies some polynomial equation over $k[x_1,\dots,x_r]$ with, say, a non-zero leading coefficient $a_j(x_1,\dots,x_r) \in k[x_1,\dots,x_r]$. Let

$$a = a(x_1,\dots,x_r) = \prod_j a_j(x_1,\dots,x_r).$$

Then $k[x_1,\dots,x_r,1/a] \subset k[x_1,\dots,x_n,1/a]$ is an integral ring extension, since now each x_{r+j} will satisfy a monic polynomial with coefficients in $k[x_1,\dots,x_r,1/a]$. The going up argument of the previous paragraph applies to show that every $\phi : k[x_1,\dots,x_r,1/a] \to K$ extends to $\Phi : k[x_1,\dots,x_n,1/a] \to K$. Clearly, given ϕ, there will be at most finitely many choices for each $\Phi(x_{r+j})$, since x_{r+j} satisfies a monic polynomial with coefficients in $k[x_1,\dots,x_r,1/a]$. The homomorphism $\phi : k[x_1,\dots,x_r,1/a] \to K$ is nothing more than a point $(\gamma_1,\dots,\gamma_r) \in K^r$ with $a(\gamma_1,\dots,\gamma_r) \neq 0$, and we've proved each of these extends to finitely many points $(\gamma_1,\dots,\gamma_n) \in V(P) \subset K^n$. Thus, we have proved exactly the proposition stated above, which includes the weak Nullstellensatz.

Corollary 1 *The prime ideal $P \subset k[X_1,\dots,X_n]$ is a maximal ideal if and only if $r = 0$, that is, if and only if $k[X_1,\dots,X_n]/P$ is an algebraic field extension of k.* □

The "if" direction is obvious, a maximal algebraically independent subset of the $\{x_i\}$ will be empty. Obviously in this case $k[X_1,\dots,X_n]/P$ is isomorphic to a subfield of the algebraic closure of k.

Conversely, assuming only that P is a maximal ideal, so that $k[X_1,\dots,X_n]/P$ is some field extension of k, apply the proof of the Nullstellensatz above when the algebraically closed field K is the algebraic closure of k. That proof constructs a ring homomorphism $\Phi : k[X_1,\dots,X_n]/P \to K$, which must be an embedding, that is, injective, since $k[X_1,\dots,X_n]/P$ is a field. Thus the field $k[X_1,\dots,X_n]/P$ is indeed algebraic over k.

Corollary 2 *If $k = K$ is algebraically closed, then any maximal ideal $P \subset K[X_1,\dots,X_n]$ is a point ideal, that is, $P = (X_1 - \gamma_1,\dots,X_n - \gamma_n)$, with $\gamma_i \in K$.* □

Namely, we must have $K[X_1,\dots,X_n]/P \cong K$ in this case, the isomorphism being the identity on the constants K. So, for each X_j, some $X_j - \gamma_j \in P$.

We now prove the strong Nullstellensatz.

Proposition 2 *Let $J \subset k[X_1,\dots,X_n]$ be a proper ideal, K the algebraic closure of k (or any algebraically closed field containing k). Let*

$$V(J) = \{\gamma = (\gamma_1,\dots,\gamma_n) \in K^n \mid f(\gamma) = 0 \text{ for all } f \in J\}$$

denote the zeros of J in affine n-space over K. Suppose $g \in k[X_1,\dots,X_n]$ with $g \equiv 0$ on $V(J)$. Then $g^m \in J$ for some $m \geq 1$. In other words, $I(V(J)) = \operatorname{rad} J \subset k[X_1,\dots,X_n]$. □

The proof is called the Rabinowitsch trick. Work in $n+1$ variables over k, $k[X_1,\dots,X_n,t]$, and consider the ideal $(J, 1-tg) \subset k[X_1,\dots,X_n,t]$. By the assumption about g, this ideal has no zeros in K^{n+1}, since the first n coordinates of such a zero would name a point of $V(J)$, at which g vanishes, so $1-tg$ would take the value 1 at such a point of K^{n+1}.

It follows from the weak Nullstellensatz in $n+1$ variables that $1 \in (J, 1-tg) \subset k[X_1,\dots,X_n,t]$. Thus we get a relation in $k[X_1,\dots,X_n,t]$:

$$1 = \sum_j h_j(X_1,\dots,X_n,t) f_j(X_1,\dots,X_n) + h(X_1,\dots,X_n,t)(1-tg).$$

with $f_j \in J$. Since the X_i and t are indeterminates, we can replace t by $1/g$ in the rational function field $k(X_1, \ldots, X_n)$, which gives a formula for 1 with only powers of g in the denominators. Note the last summand in the formula for 1 above disappears. Then, since $f_j \in J$, clearing the denominators gives a formula showing some $g^m \in J$.

Corollary 3 *Let $J = \operatorname{rad} J \subset K[X_1, \ldots, X_n]$ be a radical ideal, K algebraically closed. The maximal ideals of the affine coordinate ring $A(V(J)) = K[X_1, \ldots, X_n]/J$ correspond bijectively with points of the variety $V(J) \subset K^n$.* □

A maximal ideal of $K[X_1, \ldots, X_n]/J$ is just a maximal ideal of $K[X_1, \ldots, X_n]$ that contains J, so this corollary is an immediate consequence of the previous corollary.

One interpretation of this last corollary is that the variety $V(J)$ and its Zariski topology is accessible abstractly as the subspace of maximal ideals in $\operatorname{Spec} A(V(J))$. The affine coordinate ring $A(V(J))$ determines $V(J)$ and its topology internally, you don't need a specific embedding $V(J) \subset K^n$ to make sense of the algebraic geometry of $V(J)$. The category of affine K-varieties and polynomial maps between them becomes the same thing as the opposite of the category of commutative rings that have no nilpotent elements and are finitely generated K-algebras. The duality occurs here because a polynomial mapping between affine varieties $W \to V$ is matched with a homomorphism of rings of K-valued functions which goes in the opposite direction, $A(V) \to A(W)$. Abstractly, if $P \subset A(V)$ is a maximal ideal and $f \in A(V)$, then the "value" $f(P) \in K$ is just the reduction f (modulo P) in the quotient ring $A(V)/P = K$.