The Nullstellensatz

The classical Nullstellensatz is a theorem about "algebraic sets" (i.e. the set of zeros of a set of polynomials) in affine space. Roughly, it says that if $k=\bar{k}$, there is a one-to-one correspondence

$$\text{algebraic sets in } \mathbb{A}^n \longleftrightarrow \text{radical ideals in } k[x_1,\dots,x_n].$$

We will prove a much more general version, and then show how it implies the classical version.

Def: R is a Jacobson ring if every prime ideal of R is the intersection of maximal ideals.

Ex: 1.) A local ring is Jacobson $\Leftrightarrow$ the max'l ideal is the only prime.

2.) If R is a PID, then all the nonzero prime ideals are maximal. So R is Jacobson as long as the Jacobson radical is 0.

Notation: If S is an R algebra (w/ $\alpha: R \to S$ the corr. morphism), and $I \subseteq S$ an ideal, we'll write $I \cap R$ to mean $\alpha^{-1}(I)$, even if α is not an inclusion.

Thm (General Nullstellensatz): Let R be a Jacobson ring. If S is a f.g. R-algebra, then S is also a Jacobson ring. Moreover, if $n \subseteq S$ is a maximal ideal then $m := n \cap R$ is a maximal ideal

of R, and S/n is a finite extension field of R/m.
(i.e. $\dim_{R/m} S/n < \infty$)

Note that this can fail if R is not Jacobson:

Ex: Let $R = k[t]_{(t)}$, $S = R[x]$. Then $n = (xt - 1) \subseteq S$ is maximal, since $S/n \cong k(t)$.

But $n \cap R = 0$, which clearly isn't maximal.

Before we prove the theorem, we need to prove the following lemma about Jacobson rings:

Lemma: Let R be a ring. TFAE:

a.) R is Jacobson.

b.) If P is a prime of R and $S := R/P$ contains $b \neq 0$ s.t. $S[b^{-1}]$ is a field, then S is a field.

Pf: a.) $\Rightarrow$ b.) Since R is Jacobson, so is S. S is an integral domain, 0 is prime, so the Jacobson radical must be 0.

Since $S[b^{-1}]$ is a field, only (0) is prime. Thus, the only prime ideal in S avoiding $\{1, b, b^2, \ldots\}$ is 0. Thus, any other prime ideal contains b, so 0 must be max'l, so S is a field.

b.) $\Rightarrow$ a.) Let $Q \subsetneq R$ be prime, and I the intersection of maximal ideals containing Q. WTS $I = Q$.

Assume $I \neq Q$, and choose $f \in I - Q$. By Zorn's lemma, find a prime P max'l among primes containing P but not f. Then P isn't max'l in $R \Rightarrow R/P$ isn't a field.

$PR[f^{-1}]$ is max'l in $R[f^{-1}]$ though, so $\frac{R[f^{-1}]}{PR[f^{-1}]} = (R/P)[f^{-1}]$ is a field. But then R/P is a field, which is a contradiction.

Thus $I = Q$, so R is Jacobson. $\square$

Now we prove the Nullstellensatz:

Pf of Nullstellensatz: First assume R is a field and $S = R[x]$. Then S is a PID, so we just have to show 0 is the intersection of prime ideals. Since no polynomial can have infinitely many irreducible factors, we just have to show S has infinitely many prime ideals.

If there were only finitely many irred. polynomials f_i (up to mult. by a unit), then $\prod f_i + 1$ has positive degree, so it's not a unit, and it has no prime factors.

Thus, S has infinitely many prime ideals, which are max'l, so (0) is the Jacobson radical.

Now we show the second statement holds in this special case: if $n \subseteq S$ is maximal, then $n = (f)$, some irreducible, monic polynomial. Then $R \cap n = 0$, the only max'l ideal of R.

$S/(f)$ has dimension $\deg(f)$ over R, so it's a finite extension.

We now move to a more general case: Let R be a Jacobson ring, and suppose S is generated as an R-algebra by a single element. We will prove the theorem for this case and then do induction on the number of generators.

For the first statement, we use the lemma. We want to show that if $P \subseteq S$ is prime and $S' = S/P$ contains $b \neq 0$ s.t. $S'[b^{-1}]$ is a field, then S' is a field.

Set $R' = R/R \cap P \hookrightarrow S'$. We can then replace S by S' and R by R', an integral domain contained in S, and we want to show that if $S[b^{-1}]$ is a field, so is S.

In fact, we'll show R is a field in this case too, and S a finite extension of R.

For the second statement of the theorem, we make the same reduction and assume S is a field. Then we want exactly that R is a field and S is finite over it. Thus, the same proof proves both.

Since S is gen. by a single element t over R, write $S = R[x]/Q$ for some prime Q, s.t. t is the image of x.

First we claim $Q \neq 0$. Otherwise, $\exists\, b \in R[x]$ s.t. $R[x][b^{-1}]$ is a field. If K is the field of fractions of R, then $K[x][b^{-1}]$ is also a field. But we already showed $K[x]$ is Jacobson, so this contradicts the lemma.

Thus, $Q \neq 0$, and $S[b^{-1}] = \frac{R[x]}{Q}[b^{-1}]$ is a field, so $S[b^{-1}] = \frac{K[x]}{QK[x]}[b^{-1}]$. But $K[x]/QK[x]$ is already a field, so $S[b^{-1}] = K[x]/QK[x]$ and it's finite-dimensional over K.

Let $p(x) \in Q$ be a nonzero polynomial. Since $S = R[x]/Q$, we have

$$p(t) = p_n t^n + \dots + p_0 = 0 \text{ in } S.$$

If we invert p_n, then we see $S[p_n^{-1}]$ is integral over $R[p_n^{-1}]$.

b satisfies some equation w/ coefficients in R too:

$$q(b) = q_m b^m + \dots + q_0 = 0.$$

S is a domain, so we can factor out a power of b if necessary s.t. $q_0 \neq 0$.

Then $\left(\frac{1}{b}\right)^m + \left(\frac{q_1}{q_0}\right)\left(\frac{1}{b}\right)^{m-1} + \dots + \left(\frac{q_m}{q_0}\right) = 0$ by dividing by $q_0 b^m$.

Thus $S[b^{-1}]$ is integral over $R[p_n q_0^{-1}]$ (since $S[b^{-1}]$ is already a field).

But then by the previous section, since R is a domain, $R[p_n q_0^{-1}]$ is a field. Since R is Jacobson, R is a field, by the lemma.

Thus, $S[b^{-1}]$ is integral over R, so S is, so S is a field (again by corollary in previous section), and S is finite/R since it's integral and generated as an R alg. by one element.

For the general case, we do induction on the number of generators r of S as an R algebra. Assume $r>1$, and that it holds for algebras w/ $\leq r-1$ generators.

Let S' be the subalgebra of S generated by $r-1$ of the generators of S. Then S' is Jacobson by induction. But then S' generated by one elt as an S' algebra, so by the $r=1$ case, S' is Jacobson.

If $n \subseteq S$ is a max'l ideal, then also by the $r=1$ case $n \cap S'$ is max'l, so $n \cap R$ is as well, by induction.

$R/R\cap n \subseteq S'/S'\cap n$ and $S'/S'\cap m \subseteq S/n$ are finite field extensions,

so by transitivity, $R/R\cap n \subseteq S/n$ is finite. $\square$

From this, we get much more accessible statements dealing with polynomial rings over a field and "algebraic sets". First we need a few definitions.

Algebraic sets

Let k be a field.

Def: If $\{f_i\} \subseteq k[x_1, \ldots, x_m]$, then

$$Z(f_1, \ldots, f_m) := \{(a_1, \ldots, a_n) \in k^n \mid f_i(a_1, \ldots, a_n) = 0 \quad \forall \ i\}.$$

This is called an algebraic set in k^n (which in this context can be written $\mathbb{A}^n$).

Check: $Z(f_1, \ldots, f_m) = Z(I) = Z(\sqrt{I})$, where $I = (f_1, \ldots, f_m)$

Def: If $X \subseteq k^n$, $I(X) = \{f \in k[x_1, \ldots, x_n] \mid f(p) = 0 \quad \forall \ p \in X\}$.

Check: $I(X)$ is a (radical) ideal, and $Z(I(Z(J))) = Z(J)$, for any ideal $J \subseteq k[x_1, \ldots, x_n]$.

Notice that if $(a_1, \ldots, a_n) \in k^n$, $R = k[x_1, \ldots, x_n]$, then the map

$$\begin{aligned} R &\longrightarrow R \\ x_i &\longmapsto x_i - a_i \end{aligned}$$

is an isomorphism, and thus induces an isomorphism

$$\frac{R}{(x_1,\dots,x_n)} \xrightarrow{\cong} \frac{R}{(x_1-a_1,\dots,x_n-a_n)}.$$

The evaluation map $R \to k$, $f \mapsto f(0,\dots,0)$ is a surjection w/ kernel $(x_1,\dots,x_n)$,

so $(x_1-a_1,\dots,x_n-a_n)$ is always a max'l ideal.

That is, there's an injection $\mathbb{A}^n \to \mathrm{Spec}(R)$, with image contained in the set of max'l ideals.

In fact, if $X = Z(I) \subseteq \mathbb{A}^n$, then $(a_1,\dots,a_n) \in X \iff f(a_1,\dots,a_n) = 0 \ \forall f \in I$

$\iff (x_1-a_1,\dots,x_n-a_n) \in V(I)$.

i.e. the algebraic sets of $\mathbb{A}^n$ are the closed sets of $\mathrm{Spec}(R)$ intersected w/ the image of $\mathbb{A}^n$, and in this way $\mathbb{A}^n$ inherits the Zariski topology.

In fact, if $k = \bar{k}$, and $X \subseteq \mathbb{A}^n$ an algebraic set, we'll see that there is a one-to-one correspondence between points of X and closed points (i.e. max'l ideals) in $\mathrm{Spec}\left(\frac{R}{I(X)}\right)$.

Note: If $k \neq \bar{k}$, we can have more max'l ideals in $\mathrm{Spec}(R)$.

For instance, $\frac{\mathbb{R}[x]}{(x^2+1)} \cong \mathbb{C}$, so (x^2+1) is maximal!

With these definitions, this is an easy corollary of the Nullstellensatz.

Cor: Let $k=\bar{k}$. For each $p=(a_1,\dots,a_n)\in \mathbb{A}^n$, define

$$m_p := (x_1-a_1,\dots,x_n-a_n)\subseteq k[x_1,\dots,x_n].$$

If X is an algebraic set, then every maximal ideal of $k[x_1,\dots,x_n]/I(X)$ is of the form $m_p/I(X)$ for some $p\in X$.

In particular, the points of X are in one-to-one correspondence w/ the max'l ideals of $k[x_1,\dots,x_n]/I(X)$.

Pf: Let $S=k[x_1,\dots,x_n]$. Suppose $n\subseteq S$ is a maximal ideal.

Apply the Nullstellensatz w/ $R=k$ (clearly Jacobson), and we get

$0=n\cap R$ and S/n is finite (and thus algebraic) over k.

But $k=\bar{k}$, so $S/n=k$.

Let a_i be the image of x_i under the map $S=S/n=k$.

Let $p=(a_1,\dots,a_n)$. Then $m_p\subseteq n$, but n is maximal, so $n=m_p$.

We are done since every max'l ideal of $S/I(X)$ is of the form $m_p/I(X)$ for $I(X)\subseteq m_p$, so $p\in Z(m_p)\subseteq X$. $\square$

Now we prove the classical statement of the Nullstellensatz:

Classical Nullstellensatz: Let $k=\bar{k}$. If $I\subseteq k[x_1,\dots,x_n]$ is an ideal,

then $\mathcal{I}(\mathcal{Z}(I)) = \operatorname{rad} I$.

Thus, the correspondences

$$I \longmapsto \mathcal{Z}(I) \quad \text{and} \quad X \longmapsto \mathcal{I}(X)$$

induce a bijection between the collection of algebraic subsets of $\mathbb{A}^n$, and radical ideals of $k[x_1, \ldots, x_n]$.

Pf: By the previous corollary, the points of $\mathcal{Z}(I)$ correspond to the maximal ideals of $k[x_1, \ldots, x_n]$ containing I.

Thus, $\mathcal{I}(\mathcal{Z}(I))$ is the intersection of the maximal ideals that contain I. By the Nullstellensatz, $S = k[x_1, \ldots, x_n]$ is Jacobson, so every prime ideal that contains I is the intersection of max'l ideal, so $\mathcal{I}(\mathcal{Z}(I)) = \operatorname{rad} I$.

$\mathcal{Z}(\mathcal{I}(X)) = X$ follows from definition of algebraic set, and we just showed that if I is radical $\mathcal{I}(\mathcal{Z}(I)) = I$.

Thus, $\mathcal{I}$ and $\mathcal{Z}$ are inverse bijections between alg. sets and radical ideals. □

Note: In classical AG, $\mathcal{Z}(I) \cong \mathcal{Z}(\operatorname{rad} I)$ as algebraic sets, whereas if I isn't radical, $\underset{\text{Spec}(R/I)}{V(I)} \neq \underset{\text{Spec}(R/\operatorname{rad} I)}{V(\operatorname{rad} I)}$ even though they are the same set-theoretically (even topologically!). The

difference is that the ring is part of the data w/ a scheme while it isn't with an algebraic set.