The Nullstellensatz

We recall that a ring R has an ideal, $J(R)$, called the *Jacobson radical*. It is the intersection of all maximal ideals. A ring is a *Jacobson ring* if $J(R/P) = (0)$ for every prime ideal P of R. We've already seen some examples of Jacobson rings: $\mathbb{Z}$, $k[x]$, k a field (why? think about it!). We note that if R is Jacobson then the correspondence theorem immediately gives that R/I is Jacobson for every proper ideal I of R.

We will prove a very general version of the Nullstellensatz. Before we do this, recall that if R is a ring, then S is an R-*algebra* if S is a ring and there is a ring homomorphism $\alpha : R \to S$ sending 1_R to 1_S. In general, α need not be injective (for fields it is, however). Thus $\alpha(R)$, the image of R under α is in general a homomorphic image of R; i.e., it is isomorphic to $R/\mathrm{Ker}(\alpha)$. Nevertheless, when we speak of R we will mean $\alpha(R)$, even though it is not necessarily isomorphic to R. This will not create any problems, since we will be concerned with maximal ideals of $\alpha(R)$ and by the correspondence theorem maximal ideals of $\alpha(R)$ correspond to maximal ideals of R that contain the kernel of α. Thus we will assume without loss of generality that α is injective and we will identify R with $\alpha(R) \subseteq S$.

Theorem: (General form of Nullstellensatz) Let R be a Jacobson ring and let S be a finitely generated R-algebra. Then S is a Jacobson ring and if M is a maximal ideal of S then $N := M \cap R$ is a maximal ideal of R and S/M is a finite field extension of R/N.

Before we continue, we note that $R \subseteq S$ and if we look at the composition of the injection $R \to S$ with the surjection $S \to S/M$, then N is in the kernel of this and so we get an injective map from R/N into S/M. Thus we can regard R/N as a subfield of S/M.

The Rabinowitch trick

The Rabinowitch trick is often stated in forms that make it look like more of a trick. We use the following version from Eisenbud, which simply gives a reformulation of the Jacobson property.

Theorem: Let R be a ring. Then R is a Jacobson ring if and only if whenever P is a prime ideal of R and $T := R/P$ has the property that T_b is a field for some nonzero $b \in T$ then T is a field.

Proof. Suppose first that R is Jacobson and P is a prime ideal of R. Let $T = R/P$ and suppose that T_b is a field. Since the prime ideals of T_b are in bijective correspondence with the prime ideals of T that do not contain b, we see that every nonzero prime ideal of T contains b. It follows that if T is not a field then every maximal ideal of T contains b and so the Jacobson radical of T contains b; a contradiction, since $J(T) = (0)$, since R is Jacobson.

Suppose next that whenever P is a prime ideal of R and $T := R/P$ has the property that T_b is a field for some nonzero $b \in T$ then T is a field. Let P be a prime ideal of R. We claim that $S := R/P$ has zero Jacobson radical. To see this, suppose not. Then there is some nonzero $b \in S$ such that every maximal ideal contains b. Then there is a bijection between prime ideals of S_b and prime ideals of S that do not contain b. Let Q' be a maximal ideal of S_b. Then there is a prime ideal Q of S that does not contain b with $QS_b = Q'$. Let $T = S/Q$. By construction, every nonzero prime ideal of T contains the image of b in T. Thus T_b has only the zero prime ideal and hence it is a field. It follows that T is a field. But this is a contradiction since every maximal ideal of S is a nonzero maximal ideal of T that contains b. □

Strategy of proof of Nullstellensatz

The main steps are as follows.

(1) Show that the Nullstellensatz holds when $S = R[x]$;
(2) Use induction to show that it holds for $S = R[x_1, \ldots, x_n]$;
(3) Show that the Nullstellensatz holds for homomorphic images of $R[x_1, \ldots, x_n]$.

Every finitely generated R-algebra is isomorphic to an algebra of the form $R[x_1, \ldots, x_n]/I$ for some ideal I (a homomorphic image) and so we get the result from (1)–(3).

We observe that (1) is the only difficult step. Let's see this now.

Proof of (2) and (3) from (1). (2): Suppose that the Nullstellensatz holds for $S = R[x_1, \ldots, x_d]$ with $d < n$. Let $T = R[x_1, \ldots, x_{n-1}]$. Then by the inductive hypothesis T is Jacobson. Thus $S = R[x_1, \ldots, x_n] = T[x_n]$ is Jacobson by applying step (1) using $R = T$ (which is Jacobson). Thus if M is a maximal ideal of S then $N := M \cap T$ is a maximal ideal of T and S/M is a finite extension of T/N. But by the inductive hypothesis, $N' := N \cap R$ is a maximal ideal of R and T/N is a finite extension of R/N' and hence S/M is a finite extension of T/N.

(3): If $S = R[x_1, \ldots, x_n]/I$ then by (2) and the remarks we made at the beginning S is Jacobson. We may assume that $I \cap R = (0)$ or else we would work with $R/(I \cap R)$ instead at the beginning. If M is a maximal ideal of S then M corresponds to a maximal ideal M' of $R[x_1, \ldots, x_n]$ that contains I. Then $N := M \cap R = M' \cap R$ and by (2), N is a maximal ideal of R and $S/M \cong R[x_1, \ldots, x_n]/M'$ is a finite extension of R/N. The result follows. □

To prove (1), there are two parts: We must show that if R is Jacobson then $R[x]$ is Jacobson. We must then show that if M is a maximal ideal of $R[x]$ then $M \cap R$ is a maximal ideal of R and $R[x]/M$ is a finite extension of $R/(R \cap M)$. So we do these now. We show that R Jacobson $\implies$ $R[x]$ Jacobson. This is the hardest part and we will notice that if we pay attention to the proof, that the second part falls out for free. There is one extra ingredient that we need that will appear on the third assignment. For now we will call it the black box.

Black box: If $R \subseteq S$ are rings and S is a finite R-module then if S is a field then R is a field.

For now we will assume this and we will come back to this at the end. Now let's do step (1)—this is the trickiest part of the argument.

Step (1) of Nullstellensatz. By the Rabinowitch trick it is enough to show that if $T = R[x]/P$ has the property that T_b is a field then T is a field. We let $R' = R/(P \cap R)$. Then R' is Jacobson since R is Jacobson and R' can be regarded as a subring of T and we may regard $T = R'[x]/Q$ where Q is a prime ideal of $R'[x]$ with $Q \cap R' = (0)$. We first note that Q is not the zero ideal: if it were, we would have $T = R'[x]$ and so T would be a subring of $K[x]$, where K is the field of fractions of $R'[x]$. But then $T_b = R'[x]_b$ would be a subring of $K[x]_b$. Since T_b is a field and it contains K, we see that $R'[x]_b = K[x]_b$ and so $K[x]_b$ is a field. But $K[x]$ is a Jacobson ring (polynomial ring in one variable over a field, which we know is a Jacobson ring) and it is not a field and so $K[x]_b$ cannot be a field by the Rabinowitch trick. Thus Q is nonzero.

Since $(R'[x]/Q)_b$ is a field and $Q \cap R'$ is zero, it contains K. Thus we see that $T_b = (K[x]/QK[x])_b$. Notice that $K[x]/QK[x]$ is a finite extension of K since it is a nonzero prime ideal and hence it is a finite field extension of K. Thus T_b is a finite extension of K. We will show that R' must be equal to K and so $T = K[x]/Q$ with Q nonzero and so T is a field!

Let $f(x) = a_n x^n + \cdots + a_0$ be an element of Q with $a_0, \ldots, a_n \in R'$ and a_n not equal to zero. Then notice that we have $x^n + (a_{n-1}/a_n)x^{n-1} + \cdots + (a_0/a_n) = 0 \bmod Q' := QR'[x]_{a_n}$. Thus the image of x in$T_{a_n} = R'_{a_n}[x]/Q'$ satisfies a monic polynomial. It follows that T_{a_n} is a finite R'_{a_n}-module (with spanning set given by the images of $1, x, x^2, \ldots, x^{n-1}$). Now if T_b is a field then certainly $T_{a_n b}$ is a field, since inverting $a_n b$ is the same as inverting both a_n and b. Now since T_{a_n} is a finite R'_{a_n}-module, it follows that there is a non-trivial relation (why? think about it!)

$$c_m b^m + \cdots + c_0 = 0$$

with $c_0, \ldots, c_m \in R'_{a_n}$. By clearing denominators, we can assume that the c_i are all in R. Since T is an integral domain, we may divide by a power of b if necessary to assume that $c_0 c_m \neq 0$. Then consider the localization $T_{a_n c_0}$. This is a finite $R'_{a_n c_0}$-module (think about it!). Also, we notice that b is invertible in $T_{a_n c_0}$ since we have

$$c_m b^m + \cdots + c_0 = 0 \implies 1 = b(-c_1/c_0 + \cdots - c_m/c_0 b^{m-1})$$

and so b h as an inverse in $T_{a_n c_0}$. Thus $T_{a_n c_0}$ contains T_b. Since it sits between T_b and the field of fractions of T and T_b is a field, we see that $T_{a_n c_0}$ is a field. Also $T_{a_n c_0}$ is a finite $R'_{a_n c_0}$-module. It follows from the black box that $R'_{a_n c_0}$ is also a field. Since R' is Jacobson, the Rabinowitch trick gives that R' is a field and so $T = R'[x]/Q = K[x]/Q$ is a field since Q is a nonzero prime ideal.

For the remaining part, above we showed that if $T = R[x]/Q$ is a field then $R' = R/Q \cap R$ is a field. Thus $P := Q \cap R$ is a maximal ideal of R. We also showed that $T \cong R'[x]/Q'$ with Q' a nonzero ideal and so T is a finite extension of R'. Thus we get the second part for free from the first part. $\square$

This just leaves the black box, and you will see this on the assignment.