Nullstellensatz

1 An easy proof of Nullstellensatz by Munshi

We present the treatment of Nullstellensatz by Munshi. Unfortunately, his original proof involves nightmarish notations. We follow Richard Swan's streamlined exposition.

Definition 1.1. An integral domain R is called a *G-domain* if some localisation $R_a = R[a^{-1}]$ is a field.

Remark 1.2. This is equivalent to the property that the intersection of all non-zero prime ideals is non-zero.

Lemma 1.3. *A polynomial ring $R[X]$ is never a G-domain.*

Proof. We can assume that R is an integral domain. Suppose that $R[X]_f$ is a field. Then obviously $\deg f > 0$ so $1 + f$ is non-zero. Write $(1 + f)^{-1} = g/f^n$. Cross multiplying shows that $1 + f$ divides f^n but $f \equiv -1 \bmod (1 + f)$ which leads to the absurd conclusion that $1 + f$ is a unit. □

We write $U(R)$ (or $R^\times$ for the group of units of a ring R.

Lemma 1.4. *Let $A \subset B$ be an integral extension. Then $A \cap U(B) = U(A)$.*

Proof. Let $a \in A \cap U(B)$. Write $ab = 1$ with $b \in B$ and find an equation $b^n + c_1 b^{n-1} + \cdots = 0$ with all $c_i \in A$. Multiplying by a^{n-1} gives $b = -c_1 - c_2 a - \cdots$ so $b \in A$. □

Corollary 1.5. *Let R be a subring of a field K and assume K is integral over R. Then R is also a field.*

Theorem 1.6. *Let R be an integral domain and $\mathfrak{m}$ be a maximal ideal of $R[X_1, \ldots, X_n]$. If $R \cap \mathfrak{m} = 0$, then there exists a non-zero element $a \in R$ such that R_a is a field and $K = R[X_1, \ldots, X_n]/\mathfrak{m}$ is a finite extension of R_a.*

Corollary 1.7. *Let R be an integral domain and $\mathfrak{m}$ be a maximal ideal of $R[X_1, \ldots, X_n]$. If R is not a G-domain, then $R \cap \mathfrak{m} \neq 0$.*

Proof. (of Theorem 1.6) The case $n = 0$ is trivial. We use induction on n and so can assume that Corollary 1.7 holds for $n - 1$ variables. Using Lemma 1.3 it follows that if $n \geq 1$ then $\mathfrak{m} \cap R[X_i] \neq 0$ for all i. Choose $f_i = aiX_i^{n_i} + \cdots$

in $\mathfrak{m} \cap R[X_i]$ and let $a = \prod a_i$. The image x_i of X_i in K satisfies the monic equation $a_i^{-1} f_i = 0$ over R_a. Since the x_i's generate K over R_a we see that K is integral over R_a. By Corollary 1.5, R_a is a field, and K is finite over it since it is integral and finitely generated over R_a. □

Theorem 1.8 (Nullstellensatz). *Let k be a field, let A be a finitely generated k-algebra, and let $\mathfrak{m} \in \operatorname{Specm}(A)$. Then $A/\mathfrak{m}$ is finite over k.*

Proof. Since A is a factor ring of a polynomial ring $B = k[X_1, \dots, X_n]$, it is enough to prove the theorem for B, but this is a special case of Theorem 1.6. □

For completeness we include some standard consequences.
If $\mathfrak{m} \in \operatorname{Specm}(k[X_1, \dots, X_n])$, we can embed $k[X_1, \dots, X_n]/\mathfrak{m}$ in the algebraic closure $\overline{k}$ of k by Theorem 1.8. The X_i's map to elements a_i's of $\overline{k}$ so $(a_1, \dots, a_n) = Z(\mathfrak{m})$, the zero of $\mathfrak{m}$, in the sense that $f(a_1, \dots, a_n) = 0$ for all f in $\mathfrak{m}$. Moreover, $\mathfrak{m} = \{f \in k[X_1, \dots, X_n] | f(a_1, \dots, a_n) = 0\}$. In particular if k is algebraically closed, then $\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n)$.

Definition 1.9. A commutative ring R is called a *Jacobson ring* if every prime ideal is an intersection of maximal ideals.

Remark 1.10. A Jacobson ring is the same thing as a Hilbert ring.

Theorem 1.11. *Let A be a finitely generated algebra over a field. Then A is a Jacobson ring.*

Proof. Let $\mathfrak{p}$ be a prime ideal of A and let $a \in A \setminus \mathfrak{p}$. We must find a maximal ideal $\mathfrak{q}$ of A such that $p \subset \mathfrak{q}$ and $a \notin \mathfrak{q}$. Let $\mathfrak{m}$ be a maximal ideal of Aa containing $\mathfrak{p}_a$ and let $\mathfrak{q}$ be the contraction of $\mathfrak{m}$ in A. Then $A/\mathfrak{q} \subset A_a/\mathfrak{m}$. Since $A_a/\mathfrak{m}$ is finite over k so is $A/\mathfrak{q}$. Therefore $A/\mathfrak{q}$ is a field, showing that $\mathfrak{q}$ is maximal. It clearly has the required properties. □

Corollary 1.12. *Corollary 1.8. The radical of an ideal $\mathfrak{a}$ in a finitely generated k-algebra A is equal to the intersection of the maximal ideals containing it:* $\operatorname{rad}(\mathfrak{a}) = \cap_{\mathfrak{m} \supset \mathfrak{a}} \mathfrak{m}$. *In particular, if A is reduced, then $\cap \mathfrak{m} \subset \operatorname{Specm}(A) \mathfrak{m} = 0$.*

Theorem 1.13 (Strong Nullstellensatz). *If A is a polynomial ring over a field k and $f \in A$ is 0 at all zeros of $\mathfrak{a}$ in the algebraic closure $\overline{k}$ of k, then some power f^n lies in $\mathfrak{a}$.*