Elementary proof of the Nullstellensatz.

Joseph Bernstein **September 2012**

In this note we give an elementary proof of the Nullstellensatz. This proof is based on Noether's Lemma and is completely elementary - it does not use Zorn's lemma, notion of integral domain, Hilbert's basis theorem or Nakayama Lemma. It gives an essentially effective computational procedure that starting with a proper ideal J constructs one of its zeroes.

Probably the main "new" tool in this proof is an old observation in commutative algebra that it is better to study modules over an algebra than ideals of the algebra.

Fix a field K and consider the algebra $C = K[x_1, ..., x_n]$ of polynomials in n variables. Each polynomial $f \in C$ defines a polynomial functions on the affine space $\mathbf{A}^n(K) = \{a = (a_1, ..., a_n) |\ a_i \in K\}$. For any point $a = (a_1, ..., a_n)$ we denote by ev_a the evaluation morphism $ev_a : C \to K$ given by $f \mapsto f(a)$. Note that this defines a bijection of the set $\mathbf{A}^n(K)$ with the set $Mor_{K-algebras}(C, K)$.

For every point $a \in \mathbf{A}^n(K)$ we denote by $\mathfrak{m}_a \subset C$ the corresponding maximal ideal, $\mathfrak{m}_a := Ker(ev_a)$.

Our results are based on the following strategy - we consider a non zero finitely generated C-module M and try to show that some quotients of M are non zero.

Our central result is the following

Theorem 1. Let M be a non zero finitely generated C-module.

(i) For any linear form $u \in C$ (i.e. a linear combination $u = \sum c_i x_i$ with $c_i \in K$) there exists a monic polynomial $Q \in K[t]$ such that the module $M/Q(u)M$ is not zero.

(ii) If the field K is algebraically closed we can choose Q to be a polynomial of degree 1. In other words, there exists a constant $a \in K$ such that the module $M/(u - a)M$ is not zero.

Statement (ii) easily follows from (i). Indeed, we can write $Q = \prod(t - \lambda_i)$. Since the operator $Q(u) = \prod(u - \lambda_i)$ on the module M is not epimorphic we see that one of the operators $u - \lambda_i$ is not epimorphic, that proves (ii).

Let us see some corollaries of this theorem.

Corollary. Suppose the field K is algebraically closed and M is a non zero finitely generated C-module. Then there exists a point $a = (a_1, ..., a_n) \in \mathbf{A}^n(K)$ such that the module $M/\mathfrak{m}_a M$ is not zero.

Indeed, applying the theorem consequentially to linear forms $x_1, x_2, ..., x_n$ we find numbers $a_1, ..., a_n \in K$ such that the module $M/\sum(x_i - a_i)M$ is not zero. The ideal generated by elements $x_i - a_i$ is the ideal $\mathfrak{m}_a$ for the point $a = (a_1, ..., a_n)$ which proves the corollary.

This statement immediately implies

Theorem 2 (Nullstellensatz). Let $J \subset C$ be an ideal that does not contain 1. If K is algebraically closed then J has a zero, i.e. there exists a point $a \in \mathbf{A}^n(K)$ such that $ev_a(J) = 0$.

Indeed, consider the non-zero C-module $M = C/J$. The corollary states that there exists a point $a \in \mathbf{A}^n(K)$ such that $M/\mathfrak{m}_a M \neq 0$. But this means that $J + \mathfrak{m}_a \neq C$ and, since the ideal $\mathfrak{m}_a$ is maximal, this implies that $J \subset \mathfrak{m}_a$.

Remark. For an arbitrary field K the same arguments prove the following results

Theorem 3. (i) Let M be a non-zero finitely generated module over the algebra $C = K[x_1, ..., x_n]$. Then there exist monic polynomials $Q_i \in K[t]$ such that the module $M/\sum Q_i(x_i)M$ is not zero.

(ii) Let $J \subset C$ be an ideal that does not contain 1. Then there exists a finite field extension $L \supset K$ and a point $a \in \mathbf{A}^n(L)$ such that $ev_a(J) = 0$.

In fact Theorem 1 has the following natural generalization (see the proof bellow)

Theorem 4. (i) Let M be a non zero finitely generated C-module and $T : M \to M$ its endomorphism. Then we can find a monic polynomial $Q \in K[t]$ such that the C-module $M/Q(T)M$ is not zero.

(ii) If the field K is algebraically closed then there exists a constant $a \in K$ such that the module $M/(T - a)M$ is not zero.

Our proof of the Theorem 1 is based on

Emmy Noether's Lemma. Let $f \in C$ be a non-zero polynomial of degree d. Suppose that the field K is infinite (in fact we only need that the cardinality of the field K is larger than d).

Then one can make a linear change of coordinates $x_i = \sum a_{ij} y_j$ such that in coordinate system (y_i) we have $f = cF$, where $c \in K$ and F is a monic polynomial of degree d with respect to the last coordinate y_n (explicitly this means that $F = y_n^d + \sum_{i<d} P_i(y_1, ..., y_{n-1}) \cdot y_n^i$.

For the sake of completeness we will present the (standard) proof of this lemma bellow.

Proof of Theorem 1. In steps 1-3 we prove the theorem 1 for an infinite field K. In step 4 we explain how o treat finite fields. In Step 5 we present a proof of Noether's lemma.

Step 1. In case $n = 0$ we have $u = 0$ and we take $Q := t$.

So we assume that $n > 0$ and, using induction, we assume that the Theorem 1 holds for all polynomial algebras with number of variables less than n.

Step 2. First we will prove a lemma that is a weak form of the Theorem 1.

Lemma. There exists some nonzero linear form $v \in C$ and a monic polynomial $R \in K[t]$ such that the module $M/R(v)M$ is not zero.

In order to prove this lemma we can replace the module M by its non-zero quotient generated by one element. Hence we can assume that $M \simeq C/J$ for some ideal $J \subsetneqq C$.

If $J = 0$ we take $v := x_1, R := t$. So assume $J \neq 0$. Choose a non zero polynomial $f \in J$ and denote its degree by d. Using Noether's lemma find a coordinate system (y_i) such that $f = cF$, where F is a polynomial monic in the variable y_n.

If $n = 1$ we tale $v := y_1$ and $R := F$ (in this case this is a polynomial in one variable).

If $n > 1$ then the algebra C/fC, and hence its quotient M, are finitely generated modules over the algebra $B = K[y_1, ..., y_{n-1}]$ for which the Theorem 1 is already established. Now take $v := y_1$, find a monic polynomial $Q \in K[t]$ such that $M/Q(y_1)M$ is not zero and set $R := Q$.

Step 3. We are given a linear form u and would like to find a monic polynomial Q such that $M/Q(u)M$ is not zero. By step 2 we can find a non-zero form v and a monic polynomial R such that the quotient module $M/R(v)M$ is not zero. We can replace M by its non zero quotient $M/R(v)M$ and assume that $R(v)M = 0$.

Now consider two cases.

Case 1. The form u is proportional to v, i.e. $u = cv$ for some $c \in K$.

If $R = t^d + \sum_{i<d} a_i t^i$ then we set $Q := t^d + \sum_{i<d} c^{d-i} a_i t^i$. Since $Q(u) = c^d R(v)$ we see that $M/Q(u)M$ is not zero.

Case 2. The form u is not proportional to v. Then we can choose a linear coordinate system $(z_1, ..., z_n)$ such that $v = z_n$ and u is a linear form in the algebra $B = K[z_1, ..., z_{n-1}]$.

Since $R(y_n)M = 0$ we see that the module M is finitely generated over the algebra B. By induction in n we can find a monic polynomial Q such that $M/Q(u)M$ is not zero.

This finishes the proof of the Theorem 1 for infinite fields.

Step 4. Proof of the Theorem 1 for a finite field K.

We have a C-module $M = C/J$ and a linear form $u \in C$. Let Ω be an algebraic closure of the field K. Let us make an extension of scalars from K to Ω. Then we get algebra $C' = \Omega[x_1, ..., x_n]$, C'-module M' and a linear form $u \in C'$. Note that the module M' is finitely generated and non zero.

Since the field Ω is infinite we can find a monic polynomial $Q' \in \Omega[t]$ such that $M'/Q'(u)M'$ is not zero. Since Q' has finite number of coefficients they all lie in some finite field extension $L \supset K$. Using this it is easy to find a monic polynomial $Q \in K[t]$ that is divisible by Q' in $L[t]$.

Since $M'/Q'(u)M'$ is non zero we see that $M'/Q(u)M'$ is non zero. But this module is the extension of scalars from a C-module $M/Q(u)M$ and hence this last module is also non zero.

Step 5. Proof of Noether's lemma.

Let us write $f = f_d + f'$, where f_d is a homogeneous polynomial of degree d and f' is a polynomial of degree less than d. Since K is infinite and the polynomial f_d is non zero there exists a point $a \in \mathbf{A}^n(K)$ such that the value $c = f_d(a)$ is not equal to 0.

Replacing f by $c^{-1}f$ we can assume that $f_d(a) = 1$. Let us choose a coordinate system (y_i) such that the point a has coordinates $(0, 0, ..., 0, 1)$. Then it is clear that in this coordinate system the homogeneous polynomial f_d is monic of degree d in the variable y_n. Since the degree of the polynomial f' is less than d this implies that f is monic of degree d in the variable y_n.

Proof of Theorem 4.

Given a C-module M and its endomorphism T we extend the action of the algebra C on the module M to the action of the algebra $C' = C[s] = K[x_1, ..., x_n, s]$, where s acts as the operator T. Now the theorem 4 follow from the Theorem 1 applied to the algebra C', the C'-module M and the linear form $s \in C'$.