December 23rd, 2015

A proof of the strong form of the Nullstellensatz

Dr. V. Di Proietto

In the following k is an *algebraically closed field.* Let $A = k[x_1, \dots, x_n]$ be the polynomial ring in n variables with coefficients in k and let $I \subset A$ be an ideal. We denote by

$$Z(I) = \{a \in k^n \mid f(a) = 0, \text{ for all } f \in I\}$$

the zero set of I. If $I = (f_1, \dots, f_r)$, then $Z(I) = \{a \in k^n \mid f_i(a) = 0, \text{ for all } i = 1, \dots, r\}$. Further we set

$$I(Z(I)) = \{f \in A \mid f(a) = 0, \text{ for all } a \in Z(I)\}.$$

Notice that $I(Z(I))$ is an ideal in A, which contains the radical $\sqrt{I}$ of I.

Proposition 1. *Let k be an algebraically closed field and let $I \subset A := k[x_1, \dots, x_n]$ be an ideal. We have a bijection*

$$Z(I) \xrightarrow{\simeq} \{\textit{maximal ideals in } A/I\}, \quad (a_1, \dots, a_n) \mapsto (\bar{x}_1 - a_1, \dots, \bar{x}_n - a_n).$$

In particular, $Z(I) \neq \emptyset \Leftrightarrow I \neq (1)$.

Proof. First we show that if $(a_1, \dots, a_n)$ is an element of $Z(I)$, then $(\bar{x}_1 - a_1, \dots, \bar{x}_n - a_n)$ is a maximal ideal of A/I. It is enough to show that $(x_1 - a_1, \dots, x_n - a_n)$ is a maximal ideal of $k[x_1, \dots, x_n]$ which contains I. We show first that $(x_1 - a_1, \dots, x_n - a_n)$ is a maximal ideal of $k[x_1, \dots, x_n]$. The k-linear map $t_a : k[x_1, \dots, x_n] \to k[x_1, \dots, x_n]$ sending x_i to $x_i - a_i$ for every $i = 1, \dots, n$ is an isomorphism of rings because the k-linear map sending x_i to $x_i + a_i$ is its inverse, and it is an homomorphism of rings. So it is enough to show that the ideal $(x_1, \dots, x_n)$ is maximal. We consider the k-linear map ev_0 "evaluation at 0" from $k[x_1, \dots x_n]$ to k sending x_i to 0 for every $i = 1, \dots, n$. This is surjective and its kernel is a maximal ideal. The ideal $(x_1, \dots, x_n)$ is in the kernel, and if g is a polynomial which is in the kernel of ev_0, then $g(x_1, \dots, x_n)$ is a polynomial with zero constant term, which means that $g(x_1, \dots, x_n) \in (x_1, \dots, x_n)$, hence the ideal $(x_1, \dots, x_n)$ is the kernel of ev_0. Hence $(x_1, \dots, x_n)$ is a maximal ideal of $k[x_1, \dots, x_n]$. Moreover $\mathrm{ev}_0 = \mathrm{ev}_a \circ t_a$ where ev_a is the k-linear map "evaluation in a" from $k[x_1, \dots x_n]$ to k which sends x_i to a_i for every $i = 1, \dots, n$; hence $(x_1 - a_1, \dots, x_n - a_n)$ is the kernel of ev_a. To show that $(x_1 -$

$a_1, \ldots, x_n - a_n)$ contains I let $f \in I$, then $f(a_1, \ldots, a_n) = 0$ for every $a \in Z(I)$, so $f \in \mathrm{Ker}(\mathrm{ev}_a)$ and hence $f \in (x_1 - a_1, \ldots, x_n - a_n)$.

For injectivity we now prove that if $(a_1, \ldots, a_n)$, $(b_1, \ldots, b_n)$ are elements of $Z(I)$, and if $(\bar{x}_1 - a_1, \ldots, \bar{x}_n - a_n) = (\bar{x}_1 - b_1, \ldots, \bar{x}_n - b_n)$ in A/I then $(a_1, \ldots, a_n) = (b_1, \ldots, b_n)$. If $(\bar{x}_1 - a_1, \ldots, \bar{x}_n - a_n) = (\bar{x}_1 - b_1, \ldots, \bar{x}_n - b_n)$ in A/I, then by the one-to-one correspondence between ideals of A/I and ideals of A which contain I, we have the following equality of ideals $(x_1 - a_1, \ldots, x_n - a_n) = (x_1 - b_1, \ldots, x_n - b_n)$ in A, but $(x_1 - b_1, \ldots, x_n - b_n) = \mathrm{Ker}(\mathrm{ev}_a)$, hence $b_i = a_i$ for every $i = 1, \ldots, n$.

For surjectivity let M be a maximal ideal of A/I, then this corresponds to an ideal M' of A which contains I, then by the weak form of Nullstellensatz, since k is algebraically closed, the k-linear map $k \hookrightarrow A \to A/M' \cong k$ is an isomorphism. Every k-linear map $A \to k$ is defined by sending x_i to an element a_i for $i = 1, \ldots, n$ where $a_i \in k$ hence its kernel is $(x_1 - a_1, \ldots, x_n - a_n)$. Hence $M' = \mathrm{Ker}(\mathrm{ev}_a) = (x_1 - a_1, \ldots, x_n - a_n)$. Since M' contains I, then every $f \in I$ should verify that $f(a_1, \ldots, a_n) = 0$, which means that $(a_1, \ldots, a_n) \in Z(I)$. $\square$

Proposition 2. *We assume the same hypothesis as before, then*

$$I(Z(I)) = \sqrt{I}.$$

Proof. If $f \in \sqrt{I}$, then there exists an $N \in \mathbb{N}$ such that $f^N \in I$, hence $f^N(a_1, \ldots, a_n) = 0$ for every $a \in Z(I)$, hence $f(a_1, \ldots, a_n) = 0$ for every $(a_1, \ldots, a_n) \in Z(I)$, which means that $f \in I(Z(I))$.

Viceversa we take $f \in I(Z(I))$. We want to show that $f^N \in I$ for some $N \geq 1$. Denote by A_f the ring of fractions of A with respect to the multiplicatively closed subset $S := \{1, f, f^2, f^3, \ldots\}$.

Lemma 3. $S^{-1}A = A_f \cong A[y]/(1 - fy)$

Proof. We apply [AM69, Proposition 3.2]. We consider the map $\varphi : A \to A[y] \to A[y]/(1 - fy)$ given by the composition of the inclusion of A in $A[y]$ and the projection $A[y] \to A[y]/(1 - fy)$. Since $\varphi(f)$ is invertible, by [AM69, Proposition 3.2] φ induces a ring map $A_f \to A[y]/(1 - fy)$. Moreover since $\varphi(a) = 0$ implies that $a = 0$ and since every element of $A[y]/(1 - fy)$ is of the form $g(a)g(f^n)^{-1}$ for some $n \in \mathbb{N}$, the induced map $A_f \to A[y]/(1 - fy)$ is an isomorphism. $\square$

Hence, by lemma 3, A_f is a finitely generated k-algebra. We want to show that $A_f = IA_f$. Suppose that $A_f \neq IA_f$, then there exists a maximal ideal M of A_f/IA_f; this corresponds to a prime ideal P of A which contains I and does not contain f. But the k-linear homomorphism of rings $k \hookrightarrow A/P \to (A/P)_f \cong A_f/M$ is an isomorphism by the weak Nullstellensatz. Hence the localization map $A/P \to (A/P)_f$ is an isomorphism. Hence P is a maximal ideal of A which contains I and does not contain f. This is a contradiction because by proposition 1 $P = (x_1 - a_1, \ldots, x_n - a_n)$, with $(a_1, \ldots, a_n) \in Z(I)$, but $f \in I(Z(I))$; hence $f(a_1, \ldots, a_n) = 0$ hence $f \in (x_1 - a_1, \ldots, x_n - a_n)$, which is the kernel of ev_a.

Hence $A_f = IA_f$, which implies that there exist $N \in \mathbb{N}$ such that $f^N \in I$. □

References

[AM69] M. F Atiyah and I. G Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., 1969.