A SHORT PROOF OF THE NULLSTELLENSATZ

AVRAHAM AIZENBUD

Abstract. We give a short proof of Hilbert's Nullstellensatz. The ideas in the argument are not new. I learned them from [Avn, Tao], and they probably go back to Weil. Yet I have not found this prove in the literature, and the proofs I have found seem longer.

Theorem 1 (Hilbert's Nullstellensatz). *Let K be an algebraically closed field and $\{p_i\}$ be a collection of polynomials in n variables with coefficients in K. Assume that the system $\{p_i = 0\}$ has a solution in some extension L/K. Then it also has a solution in K.*

For the proof, we will need the following lemmas:

Lemma 2. *Let K be an infinite field and $p \neq 0$ be a polynomial in n variables $x_1, \dots, x_n$ with coefficients in K. Then there exist $\alpha_1, \dots, \alpha_n \in K$ such that $p(\alpha_1, \dots, \alpha_n) \neq 0$*

Proof. The proof is by induction. The case $n = 1$ follows from Bezout's little theorem. For general n, consider p as a polynomial in x_n with coefficients in $K[x_1, \dots, x_{n-1}]$. Let $a \in K[x_1, \dots, x_{n-1}]$ be its highest coefficient. By induction, there exist $\alpha_1, \dots, \alpha_{n-1}$ such that $a(\alpha_1, \dots, \alpha_{n-1}) \neq 0$. Consider the polynomial $f(x) = p(\alpha_1, \dots, \alpha_{n-1}, x)$. This is a non-zero polynomial, and thus as in the case $n = 1$ we have $\alpha_n \in K$ such that $p(\alpha_1, \dots, \alpha_n) = f(\alpha_n) \neq 0$. □

Lemma 3. *Let K be a field and let $L = K\langle\alpha_1, \dots, \alpha_n\rangle$ be its finitely generated extension. Then L is isomorphic over K to a finite extension of the field of rational functions in several variables with coefficients in K.*

Proof. Let $\alpha_1, \dots \alpha_n$ be the generators of L over K. We can order them so that there exists $m \leq n$ satisfying:

- α_i is transcendental over the field $K\langle\alpha_1, \dots, \alpha_{i-1}\rangle$, for all $i \leq m$,
- α_i is algebraic over $K\langle\alpha_1, \dots, \alpha_{i-1}\rangle$ for all $i > m$.

This implies that $K\langle\alpha_1, \dots, \alpha_m\rangle$ is isomorphic over K to the field of rational functions in m variables and L is its finite extension. □

Proof of the theorem. Let $(\alpha_1, \dots, \alpha_n) \in L^n$ be a solution of the system. Let $L' = K\langle\alpha_1, \dots, \alpha_n\rangle$ be the subfield of L generated over K by $\alpha_1, \dots, \alpha_n$. Clearly the system has a solution in L'. By Lemma 3, we can identify L' with a finite extension of the field of rational functions $K(x_1, \dots, x_m)$. Let $e_1, \dots, e_l$ be a basis of L' over $K(x_1, \dots, x_m)$ and assume $e_1 = 1$. We can write $\alpha_i = \sum_j a_{ij} e_j$ and $e_i e_j = \sum_o b_{ijo} e_o$, where $b_{ijo}, a_{ij} \in K(x_1, \dots, x_m)$. Let $f \in K[x_1, \dots, x_m]$ be the common denominator of b_{ijo}, a_{ij}. By Lemma 2, we have $\beta_1, \dots, \beta_m \in K$ such that $f(\beta_1, \dots, \beta_m) \neq 0$. Define ring structure on $A := K^m$ by $g_i g_j = \sum b_{ijo}(\beta_1, \dots, \beta_m) g_o$ where g_i is the standard basis of K^m. Let $s_i = \sum a_{ij}(\beta_1, \dots, \beta_m) g_j \in A$. The element $(s_1, \dots, s_n) \in A^n$ is a solution of the system. Let F be quotient of A by a maximal ideal. We get a solution of the system in F. On the other hand, F is a finite field over K. Since K is algebraically closed, this implies that $F \cong K$. □

Date: October 3, 2017.

Acknowledgments. I am grateful to Nir Avni, Joseph Bernstein, Inna Entova-Aizenbud and Eitan Sayag for interesting and educational conversations on this topic.

References

[Avn] N. Avni *Private communication.*

[Tao] T. Tao *Infinite fields, finite fields, and the Ax-Grothendieck theorem*, Blog post. See https://terrytao.wordpress.com/2009/03/07/infinite-fields-finite-fields-and-the-ax-grothendieck-theorem/

Avraham Aizenbud, Faculty of Mathematical Sciences, Weizmann Institute of Science, 76100 Rehovot, Israel

E-mail address: aizenr@gmail.com

URL: http://aizenbud.org