A proof of Hilbert's Nullstellensatz based on Gröbner bases

L.Glebsky

June 29, 2012

Abstract

The aim of this note is to present an easy proof of Hilbert's Nullstellensatz using Gröbner basis. I believe, that the proof has some methodical advantage in a course on Gröbner bases.

Key words: Hilbert's Nullstellensatz, Gröbner bases. **AMS** classification: 13-01, 13P10

1 Introduction and main results

The aim of this note is to present an easy proof of the Hilbert's Nullstellensatz using Gröbner bases. The prove presented here may be not shorter or simpler then one given in [3], however, I believe, it has some methodical advantage in a course on Gröbner bases. Other proofs using Gröbner bases were published in [2] and [5]. The proof presented in [3] uses the resultant as the main tool. It leads to some duality between our proof and the proof of [3] that will be explained at the end of the section.

Our proof is a sequence of propositions each of them is a good exercise on Gröbner bases. As the strong Hilbert's Nullstellensatz follows from the weak one by the Rabinowitz trick, we prove only

Theorem 1 (Hilbert's Nullstellensatz (weak))**.** *Let k be an algebraically closed field. Then any nontrivial ideal $I \subsetneq k[x_1, \dots, x_n]$ has a solution $a \in k^n$ (that is $f(a) = 0$ for any $f \in I$).*

It turns out that for our exposition it is more natural to use Gröbner bases not only for polynomials over a field k but also over a ring $k[x]$ of polynomials in one variable. It allows us to consider $k[x_1, x_2, \dots, x_n]$ as $k[x_1][x_2, \dots, x_n]$ and write a short proof for Lemma 2. On the other hand, $k[x]$ is an Euclidean domain, particularly, a principle ideal domain (PID). The theory of Gröbner bases for polynomials over a PID is almost the same as for polynomials over a field: one can use the same reduction process, Buchberger's algorithm, etc., see, [1]. Particularly, it allows us to find the polynomial q of Lemma 2 constructively, that provides us a constructive proof of the weak Hilbert's Nullstellensatz. In the present exposition we prove the existence of a solution for a nontrivial ideal only and not discuss the constructivity. The only facts about Gröbner bases we use without proof are contained in Proposition 3. Proposition 3 seems to be more elementary than the Buchberger's algorithm and can be proved using the Dickson lemma, see [4].

First of all we need some notations. Let k be a field, $a \in k$. Let $ev_a : k[x_1, x_2, \dots, x_n] \to k[x_2, \dots, x_n]$ denote the evaluation homomorphism $ev_a : f(x_1, x_2, \dots, x_n) \to f(a, x_2, ..., x_n)$. The proof is based on the following lemmas.

Lemma 1. *Let k be an algebraically closed field, $I \subseteq k[x_1, \dots, x_n]$ be an ideal, such that $I \cap k[x_1] = \langle p \rangle$ and $p \in k[x] \setminus k$. Then there exists $a \in k$, $p(a) = 0$ such that $ev_a(I) \neq k[x_2, \dots, x_n]$.*

The following lemma is valid for any field.

Lemma 2. *Let k be a field, $I \subseteq k[x_1, \dots, x_n]$ be an ideal, such that $I \cap k[x_1] = \{0\}$. Then there exists a non-zero polynomial $q \in k[x_1]$ such that $ev_a(I) \neq k[x_2, \dots, x_n]$ for any $a \in k$, $q(a) \neq 0$.*

Corollary 1. *Let k be an infinite field, $I \subseteq k[x_1, \dots, x_n]$ be an ideal, such that $I \cap k[x_1] = \{0\}$. Then $ev_a(I) \neq k[x_2, \dots, x_n]$ for some $a \in k$.*

It is clear that Lemma 1 and Corollary 1 imply the (weak) Hilbert's Nullstellensatz by induction. The duality with the proof of [3] is that in [3] the induction goes the other direction. Precisely, in [3] the following statement is proved. Let $I \subsetneq k[x_1, x_2, \dots, x_n]$ be an ideal. After some change of variables, if $(a_2, a_3, \dots, a_n)$ is a solution to $I \cap k[x_2, \dots, x_n]$ then $\{f(x, a_2, \dots, a_n) \mid f \in I\} \neq k[x]$.

2 Gröbner bases and some construction

This section is a short introduction to Gröbner bases. I include it in order to make the exposition reasonably closed. For details one may consult [1, 4, 5].

In what follows R denotes a ring with unity. An expression of the form $\alpha x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ with $\alpha \in R$ and $k_i \in \mathbb{N}$ we call monomial. An expression of the form $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ or 1 we call term. So, a polynomial in $R[x_1, x_2, \dots, x_n]$ is a sum of monomials or an R-linear combination of terms.

Definition 1. *A total order $\preceq$ of terms is said to be a term order if $1 \preceq t$ and $t_1 \preceq t_2$ implies $tt_1 \preceq tt_2$ for any terms t, t_1, t_2.*

For example, the lexicographic order is a term order. Another interesting term order: let $(\alpha_1, \alpha_2, \dots \alpha_n) \in \mathbb{R}^n$ be independent over $\mathbb{Q}$. Then the map $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n} \to \alpha_1 k_1 + \alpha_2 k_2 + \dots + \alpha_n k_n$ is injective and induces a term order.

In what follows we assume that some term order is fixed. Let $\operatorname{lt}(f)$ be a leading term of f (with respect to the fixed term order). Let $\operatorname{lm}(f)$ be the leading monomial of f ($\operatorname{lt}(\operatorname{lm}(f)) = \operatorname{lt}(f)$). Let $\operatorname{Lm}(I) = \{\operatorname{lm}(f) \mid f \in I\}$.

Definition 2. *Let $I \subset R[x_1 \dots x_n]$ be an ideal. $\Gamma \subset I \setminus \{0\}$ is called a strong Gröbner basis for I if for any $m \in \operatorname{Lm}(I)$ there exists $g \in \Gamma$ such that $\operatorname{lm}(g) \mid m$.*

A Gröbner basis is a generating set of an ideal and has several nice properties.

Proposition 3. *Let R be a PID. Then for any ideal $I \subseteq R[x_1, \dots, x_n]$ there exists a finite strong Gröbner basis. If Γ is a strong Gröbner basis for I then*

- *$I = \langle \Gamma \rangle$ (Γ generates I);*
- *If $R = k$ is a field then I is trivial ($I = k[x_1, \dots, x_n]$) if and only if $\Gamma \cap k \neq \emptyset$.*

Let $\phi : R_1 \to R_2$ be a morphism of rings R_1 and R_2. It has the natural lift to the morphism $\phi : R_1[x_1, \dots, x_n] \to R_2[x_1, \dots, x_n]$.

Proposition 4. *Let Γ be a strong Gröbner basis for an ideal $I \subseteq R_1[x_1, x_2, \dots, x_n]$. Let $\phi : R_1 \to R_2$ be a surjective morphism such that $\phi(a)$ neither 0 nor a zero divisor for any $a \in \operatorname{Lm}(\Gamma)$. Then $\phi(\Gamma)$ is a strong Gröbner basis for $\phi(I)$*

Proof. As ϕ is surjective, $\phi(I)$ is an ideal in $R_2[x_1, \dots, x_n]$. The proposition easily follows from

Statement. For any $h \in \phi(I)$ there exists $f \in I \cap \phi^{-1}(h)$ such that $\operatorname{lt}(f) = \operatorname{lt}(h)$.

Indeed, in this case $\operatorname{lm}(h)$ is divisible by $\operatorname{lm}(\phi(g)) = \phi(\operatorname{lm}(g))$ for a $g \in \Gamma$ such that $\operatorname{lm}(g) | \operatorname{lm}(f)$. So, it suffices to show the statement. We show it by contradiction. Let $h \in \phi(I)$ contradict the statement, that is, for any $f \in I$, $h = \phi(f)$ one has $\operatorname{lt}(h) \neq \operatorname{lt}(f)$. Let f_m has minimum leading term among all such f. One has $\phi(\operatorname{lm}(f_m)) = 0$. On the other hand, we can eliminate $\operatorname{lm}(f_m)$ by some $g \in \Gamma$: $f' = f_m - \frac{\operatorname{lm}(f_m)}{\operatorname{lm}(g)} g$. But $\phi(\frac{\operatorname{lm}(f_m)}{\operatorname{lm}(g)}) = 0$ ($\phi(\operatorname{lm}(g))$ is not a zero divisor). So, $\phi(f') = h$, contradiction with the minimality. □

3 Prove of Lemma 1

Proposition 5. *Let k be a field, $f_1, f_2 \in k[x_1]$, $G = \{g_1, g_2, \dots, g_r\} \subset k[x_1, x_2 \dots, x_n]$. Let $gcd(f_1, f_2) = 1$. Then $\langle f_1 f_2, G \rangle = \langle f_1, G \rangle \cap \langle f_2, G \rangle$*

Proof. Let $Q_1, Q_2 \in k[x_1]$ be such that $Q_1 f_1 + Q_2 f_2 = 1$. We use the method $I \cap J = \langle zI, (1-z)J \rangle \cap k[x_1, \dots, x_n]$ where z is a new variable. Now:

$$\langle zf_1, (z-1)f_2, zg_1, \dots, zg_r, (z-1)g_1, \dots (z-1)g_r \rangle \underset{a}{=} \langle zf_1, (z-1)f_2, g_1, \dots, g_r \rangle \underset{b}{=}$$

$$\langle f_1 f_2, Q_2 f_2 - z, g_1, \dots, g_r \rangle$$

Equality **(a)** is valid due to $g_i = zg_i - (z-1)g_i$ y zg_i and $(z-1)g_i$ are multiples of g_i. For equality **(b)** it suffices to show that that $\langle zf_1, (1-z)f_2 \rangle = \langle f_1 f_2, Q_2 f_2 - z \rangle$.

- $\langle zf_1, (1-z)f_2\rangle \subseteq \langle f_1f_2, Q_2f_2 - z\rangle$. Indeed, $zf_1 = [f_1f_2]\,Q_2 - [Q_2f_2 - z]\,f_1$ and $(1-z)f_2 = [f_1f_2]\,Q_1 + [Q_2f_2 - z]\,f_2$.
- $\langle zf_1, (1-z)f_2\rangle \supseteq \langle f_1f_2, Q_2f_2 - z\rangle$. Indeed, $f_1f_2 = [zf_1]\,f_2 + [(1-z)f_2]\,f_1$ and $Q_2f_2 - z = [(1-z)f_2]\,Q_2 - [zf_1]\,Q_1$.

Now, $\langle f_1f_2, Q_2f_2 - z, g_1, \ldots, g_r\rangle \cap k[x_1, x_2, \ldots, x_n] = \langle f_1f_2, g_1, \ldots, g_r\rangle$. Indeed, let $f = pf_1f_2 + p_0(Q_2f_2 - z) + \sum p_i g_i$ be independent of z. Substituting $z = Q_2f_2$ we get $f \in \langle f_1f_2, g_1, \ldots, g_r\rangle$. $\square$

By induction, Proposition 5 implies that

$$\langle \prod_{j=1}^{k} (x_1 - a_j)^{c_j}, G\rangle = \bigcap_{j=1}^{k} \langle (x_1 - a_j)^{c_j}, G\rangle \tag{1}$$

Definition 3. *Let I be an ideal. The set $\sqrt{I} = \{f \mid f^n \in I$ for some $n \in \mathbb{N}\}$ is called the radical of I. It is easy to check that $\sqrt{I}$ is an ideal.*

Proposition 6. *$I = k[x_1, \ldots, x_n]$ if and only if $\sqrt{I} = k[x_1, \ldots, x_n]$*

Proof. We prove only the '$\Longleftarrow$' implication of the proposition. Let $1 \in \sqrt{I}$. So, $1 = 1^n \in I$ and, consequently, $I = k[x_1, \ldots, x_n]$. $\square$

Corollary 2. *Let k be an algebraically closed field, $f \in k[x_1]$, $G \subset k[x_1, \ldots, x_n]$. Suppose, that $\langle f, G\rangle \neq k[x_1, \ldots, x_n]$. Then there exists $a \in k$, $f(a) = 0$, such that $\langle (x_1 - a), G\rangle \neq k[x_1, \ldots, x_n]$.*

Proof. Let $\langle f, G\rangle \neq k[x_1, \ldots, x_n]$. By formula 1 $\langle (x_1 - a)^d, G\rangle \neq k[x_1, \ldots, x_n]$ for some a, $f(a) = 0$ and $d \in \mathbb{N}$. Clearly, $\langle (x_1 - a), G\rangle \subset \sqrt{\langle (x_1 - a)^d, G\rangle}$. $\square$

Now Lemma 1 follows due to $k[x_1, \ldots, x_n]/\langle (x_1 - a), G\rangle \sim k[x_2, \ldots, x_n]/\,ev_a(\langle G\rangle)$ so, $\langle (x_1 - a), G\rangle \neq k[x_1, \ldots, x_n]$ if and only if $ev_a(\langle (x_1 - a), G\rangle) \neq k[x_2, \ldots, x_n]$.

4 Proof of Lemma 2

Consider $k[x_1, \ldots, x_n]$ as $k[x_1][x_2, \ldots, x_n]$. So, now the polynomials has $x_2, \ldots, x_n$ as the variables and $k[x_1]$ as a ring of coefficients. Let Γ be a finite strong Gröbner basis for an ideal $I \subset k[x_1][x_2, \ldots, x_n]$. Let $q \in k[x_1]$ be the product of leading coefficients of all $g \in \Gamma$. If $q(a) \neq 0$ then $ev_a(\Gamma)$ is a Gröbner basis of $ev_a(I)$ by Proposition 4. Now, $\Gamma \cap k[x_1] \subseteq I \cap k[x_1] = \emptyset$ and, consequently, $ev_a(\Gamma) \cap k = \emptyset$. The Lemma 2 follows by Propositions 3.

Acknowledgment. The author is grateful to David Cox for pointing out an error in the previous version. The author is also grateful to J.M. Almira, L. Robbiano and E. Gordon for useful observations.

References

[1] Adams, William W., Loustaunau P., An introduction to Gröbner bases, ISBN 0-8218-3804-0, AMS 1996

[2] Almira J.M., Nullstellensatz revisited, *Rend. Sem. Mat. Univ. Pol. Torino* **65**, no. 3 (2007)

[3] Arrondo, Enrique Another elementary proof of the Nullstellensatz. *Amer. Math. Monthly* **113** (2006), no. 2, 169171,

[4] David Cox, John Little, Donal O'Shea, Ideals, Varieties, and Algorithms, ISBN 0-387-94680-2, Springer, 1996

[5] Martin Kreuzer, Lorenzo Robbiano, Computational Commutative Algebra 1, ISBN: 978-3-540-67733-8, Springer-Verlag Berlin Heidelberg, 2008

Instituto de Investigación en Comunicación Óptica Universidad Autónoma de San Luis Potosí
Av. Karakorum 1470, Lomas 4a 78210 San Luis Potosi, Mexico
e-mail:glebsky@cactus.iico.uaslp.mx