Rend. Sem. Mat. Univ. Pol. Torino - Vol. 65, 3 (2007)

J.M. Almira

NULLSTELLENSATZ REVISITED

Abstract. In this note we give a new proof of Hilbert's Nullstellensatz, based on the use of Gröbner basis. The proof has two variants. The first one uses the fundamental theorem of algebra and the second one uses Gelfand-Mazur's theorem.

1. Introduction

Quite recently several new proofs of the Nullstellensatz and the Fundamental Theorem of Algebra have appeared in the literature. This is a happy fact, since both results are, in some sense, a keystone for classical algebraic geometry and a better understanding of both is to be acknowledged.

The main goal of this note is to present another proof of the Nullstellensatz which, from our point of view, is so easy to understand that, at least from a pedagogical view, it should have some value. We do not claim that our proof is essentially new, since it is based on well known ideas, but we have not been able to locate any textbook or article where this proof appears.

We use a basic result on integral dependence on polynomial rings, which can be combined with the properties of the division algorithm with respect to a Gröbner basis of an ideal. Our proof has essentially two variants: one which uses the fundamental theorem of algebra and the other, more surprising, which depends on a well known result from functional analysis. In particular, we prove that Gelfand-Mazur Theorem implies both the Nullstellensatz and the Fundamental Theorem of Algebra.

2. Gröbner basis and the division algorithm

We recall that a monomial order is a total order $<$ over the set $\mathbb{N}^n$ (which induces a total order on the monomials in the indeterminates $\{x_1, \cdots, x_n\}$) with the following two additional properties:

O_1 If $\mathbf{a} < \mathbf{b}$ and $\mathbf{c} \in \mathbb{N}^n$, then $\mathbf{a} + \mathbf{c} < \mathbf{b} + \mathbf{c}$.

O_2 All nonempty subset of $\mathbb{N}^n$ has a minimum with respect to this order.

For example, we can associate to the ordering $x_n > \cdots > x_1$ of the indeterminates the lexicographic order defined by $\mathbf{a} = (a_1, \cdots, a_n) >_{lex} \mathbf{b} = (b_1, \cdots, b_n)$ if and only if $a_{k_0} - b_{k_0} > 0$, where $k_0 = \max\{k \in \{1, \cdots, n\} : a_k - b_k \neq 0\}$ and the graduated lexicographic order $<_{grlex}$ given by:

$$\mathbf{a} >_{grlex} \mathbf{b} \Leftrightarrow |\mathbf{a}| = \sum_{i=1}^{n} |a_i| > |\mathbf{b}| = \sum_{i=1}^{n} |b_i| \text{ or } |\mathbf{a}| = |\mathbf{b}| \text{ and } \mathbf{a} >_{lex} \mathbf{b}. \tag{1}$$

Given an ideal I of $\mathbb{C}[x_1, \cdots, x_n]$, the Hilbert basis theorem claims that there exists a finite set of polynomials $\{f_i\}_{i=1}^k$, called a Hilbert basis, such that $I =< f_1, \cdots, f_k >$.

Given a monomial order $<$ and a non zero polynomial $f \in \mathbb{C}[x_1, \cdots, x_n]$, the leading term $\mathbf{Lt}(f)$ is the greatest monomial, with respect to the monomial order $<$, appearing in the expansion of f as a sum of monomials of distinct multi-degree. If $I \neq < 0 >$ the initial ideal $\mathbf{Lt}(I)$ is the monomial ideal formed by the leading terms $\mathbf{Lt}(f)$ for $0 \neq f \in I$. A Hilbert basis of I is called a Gröbner basis if the leading terms of its elements define a Hilbert basis of the monomial ideal $\mathbf{Lt}(I)$. In the 1960's Buchberger, which was a student of Gröbner, gave an algorithm to compute a Gröbner basis of the ideal I in terms of a given Hilbert basis of I and proved the following fundamental result:

THEOREM 1 (Buchberger). *Given I an ideal of $\mathbb{C}[x_1, \cdots, x_n]$ and $\{g_1, \cdots, g_s\}$ a Gröbner basis of I, the following claims hold true:*

(*a*) *For all $f \in \mathbb{C}[x_1, \cdots, x_n]$ there exists $h_1, \cdots, h_s, r \in \mathbb{C}[x_1, \cdots, x_n]$ such that $f = h_1 g_1 + \cdots + h_s g_s + r$. Moreover, the polynomial r in this expression is uniquely determined by f and no term appearing in r is divisible by $\mathbf{Lt}(g_i)$, for $i = 1, \ldots, s$.*

(*b*) *There is an algorithm which computes the polynomials h_i and r above.*

For the proof of Theorem 1 we strongly recommend the very nice book by Cox, Little and O'Shea, [5, pages 59-65].

We study the connections between Gröbner bases and the maximal ideals of the ring $\mathbb{C}[x_1, \cdots, x_n]$. We introduce some notation in order to state a key Lemma.

Let I be an ideal of $\mathbb{C}[x_1, \cdots, x_n]$ and let $A : \mathbb{C}^n \to \mathbb{C}^n$ be an invertible linear map, so that A defines a change of coordinates $x_j = \sum_{i=1}^n a_{i,j} y_i$ (we use the notation $\mathbf{x} = A\mathbf{y}$). We consider, associated to I and A, the ideal $I_A = \{f_A(\mathbf{y}) = f(A\mathbf{y}) : f(\mathbf{x}) \in I\} \subset \mathbb{C}[y_1, \cdots, y_n]$.

LEMMA 1. *Given I a maximal ideal of $\mathbb{C}[x_1, \cdots, x_n]$, there exists a linear change of coordinates A such that, for the graduated lexicographic order $<_{grlex}$ defined in* (1)*, the initial ideal $\mathbf{Lt}(I_A)$ of I_A of $\mathbb{C}[y_1, \cdots, y_n]$ contains monomials of the form $y_k^{n_k}$ for some $n_k \in \mathbb{N}$ and $k = 1, \ldots, n$.*

Proof. We divide the proof in three steps:

Step 1. *Given $f \in \mathbb{C}[x_1, \cdots, x_n]$ a polynomial of total degree d, there exists a change of coordinates A of the form*

$$x_n = y_n, \quad x_{n-1} = y_{n-1} + a_{n-1} y_n, \quad \cdots, \quad x_1 = y_1 + a_1 y_n \tag{2}$$

(with $a_1, \cdots, a_n \in \mathbb{C}$) such that the polynomial f_A, which has total degree d, satisfies

$$f_A = y_n^d + \text{ terms of degree smaller than } d \text{ in } \mathbb{C}[y_1, \ldots, y_{n-1}][y_n]. \tag{3}$$

This is a well known fact. Its proof can be located, for example, in [5, p. 169].

Step 2. *Let $I \subset \mathbb{C}[x_1, \cdots, x_n]$ be a prime ideal which contains an element f of the form*

$$f = x_n^d + \text{ terms of degree smaller than } d \text{ in } \mathbb{C}[x_1, \ldots, x_{n-1}][x_n]. \tag{4}$$

If I is a maximal ideal of $\mathbb{C}[x_1, \cdots, x_n]$ then $J = I \cap \mathbb{C}[x_1, \cdots, x_{n-1}]$ is also a maximal ideal of $\mathbb{C}[x_1, \cdots, x_{n-1}]$. In this particular case we have that $J \neq (0)$.

We use a basic result about integral dependence which asserts that if $A \subset B$ is an extension of integral domains and if B is integral over A (which means that the elements of B are solutions of equations $p(x) = 0$, for $p \in A[x]$ a monic polynomial) then B is a field if an only if A is so (see, [3, Proposition. 5.7, page 61]).

The ring $A := \mathbb{C}[x_1, \cdots, x_{n-1}]/J$ can be identified with a subring of $B := \mathbb{C}[x_1, \cdots, x_n]/I$ by the map $h : A \to B$ which sends $x_i + J \in A$ to $x_i + I \in B$, for $i = 1, \cdots, n-1$. The rings A, B are integral domains since if I is a prime ideal then $J = h^{-1}(I)$ is also a prime ideal. By step 1 there exists an element $f \in I$ of the form (4); this implies that $t_n := x_n + I$ is integral over A, hence also $B = A[t_n]$ is integral over A. It follows that B is a field (i.e., I is maximal) if and only if A is a field (i.e., J is maximal).

Step 3. *The result holds true.*

To end the proof of the lemma we take into account the facts proved in steps 1 and 2 to guarantee, by an inductive argument, that there exists a linear change of coordinates $A : \mathbb{C}^n \to \mathbb{C}^n$ (obtained by composition of several changes of coordinates of the form (2), the first one concerning all indeterminates, the second one involving only the first $n-1$ indeterminates, etc.) such that the ideal I_A contains elements $f_k \in \mathbb{C}[y_1, \cdots, y_k]$ of total degree $n_k \geq 1$ of the form:

$$f_k = y_k^{n_k} + \text{terms of degree less than } n_k \text{ in } \mathbb{C}[y_1, \cdots, y_{k-1}][y_k], \text{ for } k = 1, \cdots, n.$$

This implies that the monomial ideal $\mathbf{Lt}(I_A)$, with respect to the graduated lexicographic order $<_{grlex}$ above (1), contains the monomials $\{y_k^{n_k}\}_{k=1}^n$. □

3. The Nullstellensatz

Now we are able to prove our main result.

THEOREM 2 (Nullstellensatz). *The maximal ideals of $\mathbb{C}[x_1, \cdots, x_n]$ are precisely the ideals of the form $< x_1 - a_1, \cdots, x_n - a_n >$, for $a_1, \ldots, a_n \in \mathbb{C}$.*

Proof. It is clear that, in order to prove this result for a maximal ideal I it is enough to prove it for the ideal I_A, for A a linear invertible map.

By Lemma 1 and Theorem 1 the set of monomials which appear in the rests of the divisions of polynomials in $\mathbb{C}[y_1, \cdots, y_n]$ by a Gröbner basis of I_A, with respect

to the order $<_{grlex}$, is a finite set. It follows that the field $K = \mathbb{C}[y_1, \cdots, y_n]/I$ is a complex vector space of finite dimension N.

Now we may conclude the proof in two ways:

First, we have shown that $K : \mathbb{C}$ is a finite algebraic field extension, and, by the fundamental theorem of algebra, $K = \mathbb{C}$ and $N = 1$, which means that $\mathbf{Lt}(I_A) = \{y_1, \cdots, y_n\}$. Alternatively, if we denote $A_k := \mathbb{C}[y_1, \ldots, y_k]/I_A \cap \mathbb{C}[y_1, \ldots, y_k]$ we can use step 2 and the fundamental theorem of algebra to show that the sequence of integral ring extensions:

$$\mathbb{C} \to A_1 \to A_2 \to \cdots \to A_n = K$$

is actually a sequence of field isomorphisms.

If follows by any of these two arguments that I_A contains a maximal ideal of the form $(y_1 - b_1, \ldots, y_n - b_n)$ for some $b_1, \ldots, b_n \in \mathbb{C}$. This ends the proof in this case.

The second way to end the proof of the Nullstellensatz is to use the Gelfand-Mazur Theorem from functional analysis. This theorem is at the core of the theory of commutative Banach algebras and has many interesting applications [4], [13]. It claims that the only normed fields that there exists, up to Banach algebra isometries, are $\mathbb{R}$ (the set of real numbers) and $\mathbb{C}$ (the set of complex numbers), both equipped with their standard absolute value. This result was announced by Mazur in 1938 [10] and proved by Gelfand in 1941 [7].

Let us now consider the norm $\|\cdot\|_* : K \to \mathbb{R}^+$ given by $\|a\|_* = \|L_a\|$, where $L_a : K \to K$ is the linear operator given by $L_a(b) = a \cdot b$ and $\|L_a\|$ denotes the standard norm of L_a (i.e. we consider over $K \cong \mathbb{C}^N$ the standard Euclidean norm $\|\cdot\|$ and set $\|L_a\| = \sup_{\|x\|=1} \|L_a(x)\|$). Clearly, $(K, \|\cdot\|_*)$ is a normed field, since

$$\|a \cdot b\|_* = \|L_{a\cdot b}\| = \|L_a L_b\| \leq \|L_a\|\|L_b\| = \|a\|_*\|b\|_*.$$

It follows from Gelfand-Mazur's theorem that there exists an isometry of Banach algebras $\tau : K \to \mathbb{C}$. Of course, this implies that $N = 1$ since τ is also an isomorphism of $\mathbb{C}$-vector spaces and $\dim_{\mathbb{C}} K = N$. This ends the proof. □

REMARK 1. We should note that there are proofs of Gelfand-Mazur theorem which do not use the fundamental theorem of algebra nor any other result, like the well known Liuoville's principle, which is at the heart of other demonstration of this result. In fact, although the most extended proof of Gelfand-Mazur's theorem uses Liouville's theorem (see [12]), fortunately there are other proofs. Concretely, those by Kametami [8] and Rickart [11] are based on the continuity properties of the product in a Banach algebra and the fact that for every $n \in \mathbb{N}$ the polynomial $x^n - 1$ is decomposable in linear factors over the set of complex numbers, which is a result weaker than the fundamental theorem of algebra (and easy to prove if you know Euler's formula $e^{i\theta} = \cos\theta + \mathbf{i}\sin\theta$). This gives its significance to our proof that Gelfand-Mazur's theorem implies the fundamental theorem of algebra and, on the other hand, also allows to interpret that both results are indeed equivalent, since the fundamental theorem of

algebra implies the existence of the n-th roots of unity. The proofs by Kametami and Rickart have also the advantage that they belong to the so called "elementary proofs" of Gelfand-Mazur's theorem. Indeed they can be explained at the second year undergraduate level in a mathematics faculty.

REMARK 2. As we have already noted, the proof we have presented in this paper has essentially two variants: one which uses the fundamental theorem of algebra and the other one based on the Gelfand-Mazur's theorem. It is interesting to note that the first of these variants is still valid for a proof of the Nullstellensatz in its strongest version, where the result is stated for ideals of $\mathbb{K}[x_1, \cdots, x_n]$, where $\mathbb{K}$ is any algebraically closed field. Meanwhile, the proof based on Gelfand-Mazur's theorem is only valid for $\mathbb{K} = \mathbb{C}$.

Acknowledgement. The author is quite grateful to the referee, since his (her) comments have been very useful to improve the readability of this note.

References

[1] ALMIRA J.M., JIMÉNEZ M. AND DEL TORO N., *Another topological proof of the Fundamental Theorem of Algebra*, Elemente der Math. **57** (2002), 32–37.

[2] ARRONDO E., *Another elementary proof of the Nullstellensatz*, Amer. Math. Monthly **113** (2) (2006), 169–171.

[3] ATIYAH M.F. AND MCDONALD I.G., *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, 1969.

[4] BONSALL F.F. AND DUNCAN J., *Complete normed algebras*, Springer-Verlag, New-York 1973.

[5] COX D., LITTLE J., O'SHEA D., *Ideals, varieties and algorithms*, Springer, 1997.

[6] FINE B. AND ROSENBERGER G., *The Fundamental Theorem of Algebra*, Undergraduate Texts in Mathematics, Springer-Verlag 1997.

[7] GELFAND I., *Normierte Ringe*, Mat. Sbornik N. S. **9** (51) (1941), 3–24.

[8] KAMETAMI S., *An elementary proof of the fundamental theorem of normed fields*, J. Math. Soc. Japan **4** (1) (1952) 96-99.

[9] PETER MAY J., *Munshi's proof of the Nullstellensatz*, Amer. Math. Monthly **110** (2003), 133–140.

[10] MAZUR S., *Sur les anneaux linéaires*, C. R. Acad. Sci. Paris **207** (1938), 1025–1027.

[11] RICKART C.E., *An elementary proof of a fundamental theorem in the theory of Banach algebras*, Michigan Math. J. **5** (1958), 75–78.

[12] RUDIN W., *Real and complex analysis*, McGraw-Hill Inc., 1976.

[13] ZELAZKO W., *Banach Algebras*, Elsevier, 1973.

AMS Subject Classification: 14A-xx, 41Q-xx.

J. M. ALMIRA, Departmento de Mathemáticas, Universidad de Jaén. E.P.S. Linares,
C/ Alfonso X el Sabio 28, 23700 Linares (Jaén), SPAIN
e-mail: jmalmira@ujaen.es

Lavoro pervenuto in redazione il 31.05.2006 e, in forma definitiva, il 06.11.2006.