Lecturas Matemáticas
Volumen **34** *(1) (2013), páginas 77–82*
ISSN 0120–1980

Una prueba sencilla del teorema de los ceros de Hilbert usando bases de Gröbner

A simple proof of Hilbert's Nullstellensatz based on Gröbner bases

Lev Glebsky
Instituto de Investigación en Comunicación Óptica. UASLP, San Luis Potosí, México.
Carlos Jacob Rubio-Barrios
Facultad de Matemáticas, UADY, Mérida, México.

Resumen. Se presenta una demostración sencilla del teorema de los ceros de Hilbert usando las bases de Gröbner para polinomios sobre dominios de ideales principales.

Key words and phrases. Gröbner bases, Nullstellensatz.

Abstract. The aim of this paper is to present an easy proof of Hilbert's Nullstellensatz using Gröbner bases for polynomials over principal ideal domains.

2010 AMS Mathematics Subject Classification. 13-01, 13P10

1. Introducción

En la literatura existen varias pruebas del famoso teorema de los ceros de Hilbert (*Nullstellensatz*) usando bases de Gröbner (véase por ejemplo [2] y [5]). Sin embargo, la demostración presentada aquí consiste en considerar el anillo de polinomios $k[x_1, \ldots, x_n]$ como $k[x_1][x_2, \ldots, x_n]$ y aplicar la teoría de las bases de Gröbner no sobre el campo k, sino sobre el dominio de ideales principales $k[x_1]$.

La demostración que se presenta en esta nota no es necesariamente más corta o más simple que la dada en [3]. Sin embargo, tiene la ventaja de que puede ser estudiada por su sencillez, en los primeros temas de un curso básico

de geometría algebraica. La prueba dada en [3] utiliza el resultante como herramienta principal, sin embargo, hay una dualidad entre esa demostración y la dada aquí, misma que explicaremos en la siguiente sección.

A lo largo de todo el texto k denotará un campo. Un término en las variables $x_1, x_2, \ldots, x_n$ es un producto de la forma:

$$x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n},$$

donde los exponentes a_i son enteros no negativos. Denotaremos $\mathbf{x}^{\mathbf{a}} = x_1^{a_1} \cdots x_n^{a_n}$ con $\mathbf{a} = (a_1, \ldots, a_n)$.

Un monomio en las variables $x_1, x_2, \ldots, x_n$ es una expresión de la forma $\alpha \mathbf{x}^{\mathbf{a}}$, donde $\alpha \in k$.

Un polinomio en las variables $x_1, x_2, \ldots, x_n$ es una k-combinación lineal de términos en las variables $x_1, x_2, \ldots, x_n$. El conjunto de los polinomios en las variables $x_1, x_2, \ldots, x_n$ es denotado por $k[\mathbf{x}]$ donde $\mathbf{x} = (x_1, x_2, \ldots, x_n)$.

De aquí en adelante vamos a suponer que tenemos un orden de términos fijo $\preceq$.

Dado $f \in k[\mathbf{x}]$ denotaremos por tp(f) al término principal de f y por mp(f) al monomio principal de f. Es claro que mp(f) $= \alpha$tp(f) para algún $\alpha \in k$. Para un ideal $I \subseteq k[\mathbf{x}]$ definimos TP(I) $= \{\text{tp(f)} \mid \text{f} \in \text{I}\}$ y MP(I) $= \{\text{mp(f)} \mid \text{f} \in \text{I}\}$.

Definición 1.1. $\Gamma \subset I - \{0\}$ es una base de Gröbner fuerte para I, si para cada $m \in$ MP(I) existe $g \in \Gamma$ tal que mp(g) $\mid$ m.

Para una demostración del siguiente resultado, se puede consultar [1].

Proposición 1.2. *Sea R un dominio de ideales principales y sea I un ideal de $R[x_1, \ldots, x_n]$. Entonces, I tiene una base de Gröbner fuerte finita. Más aún, si Γ es una base de Gröbner fuerte para I, entonces $I = \langle \Gamma \rangle$. En particular, si $R = k$ entonces $I = k[\mathbf{x}]$ si y sólo si $\Gamma \cap k \neq \emptyset$.*

Supongamos que $\phi : R_1 \to R_2$ es un homomorfismo de anillos. El homomorfismo ϕ tiene el levantamiento natural (que vamos a denotar por el mismo símbolo ϕ) hasta el homomorfismo $\phi : R_1[\mathbf{x}] \to R_2[\mathbf{x}]$, que está definido por $\phi(\alpha_1 \mathbf{x}^{\mathbf{a}_1} + \alpha_2 \mathbf{x}^{\mathbf{a}_2} + \cdots) = \phi(\alpha_1)\mathbf{x}^{\mathbf{a}_1} + \phi(\alpha_2)\mathbf{x}^{\mathbf{a}_2} + \cdots$.

Proposición 1.3. *Sean R_1 y R_2 anillos, y sea Γ una base de Gröbner fuerte para un ideal $I \subseteq R_1[\mathbf{x}]$. Si $\phi : R_1 \to R_2$ es un homomorfismo sobreyectivo tal que $\phi(a)$ no es 0 y tampoco es un divisor de cero para todo $a \in$ MP(Γ), entonces $\phi(\Gamma)$ es una base de Gröbner fuerte para $\phi(I)$.*

Demostración. Como ϕ es sobreyectivo, $\phi(I)$ es un ideal de $R_2[\mathbf{x}]$. El resultado se sigue fácilmente de la siguiente afirmación.

Afirmación. Para cada $h \in \phi(I)$ existe $f \in I \cap \phi^{-1}(h)$ tal que tp(f) $=$ tp(h).

En efecto, la afirmación implica que $\mathrm{mp(h)}$ es divisible por $\mathrm{mp}(\phi(\mathrm{g})) = \phi(\mathrm{mp(g)})$ para un $g \in \Gamma$ tal que $\mathrm{mp(g)} \mid \mathrm{mp(f)}$. Entonces, basta demostrar la afirmación. Lo haremos por contradicción. Sea $h \in \phi(I)$ y supongamos que para todo $f \in I$, con $h = \phi(f)$ tenemos que $\mathrm{tp(h)} \neq \mathrm{tp(f)}$. Entre estos f elegimos uno que tiene el menor término principal, digamos f_m. Tenemos que $\phi(\mathrm{mp}(\mathrm{f_m})) = 0$. Por otra parte, podemos eliminar $\mathrm{mp}(\mathrm{f_m})$ por un $g \in \Gamma$: $f' = f_m - \dfrac{\mathrm{mp}(\mathrm{f_m})}{\mathrm{mp(g)}} g$. Pero $\phi(\dfrac{\mathrm{mp}(\mathrm{f_m})}{\mathrm{mp(g)}}) = 0$ ($\phi(\mathrm{mp(g)})$ no es un divisor de cero). Entonces, $\phi(f') = h$, lo que contradice la minimalidad de f_m. □

2. **Resultados Principales**

El teorema de los ceros de Hilbert relaciona $I(V(I))$ con I cuando el campo k es algebraicamente cerrado.

Si I es un ideal de un anillo A, el *radical* $\sqrt{I}$ de I se define como:

$$\sqrt{I} = \{f \in k[\mathbf{x}] \mid f^r \in I, \text{ para algún } r \in \mathbb{Z}^+\}$$

el cual es un ideal de A.

Teorema 2.1 (Teorema de los ceros de Hilbert)**.** *Sean k un campo algebraicamente cerrado e $I \subset k[\mathbf{x}]$ un ideal. Entonces $I(V(I)) = \sqrt{I}$.*

Este teorema es importante porque muestra una relación entre la geometría y el álgebra: las soluciones de un sistema de ecuaciones polinomiales son objetos geométricos y los ideales y radicales son objetos algebraicos.

Nuestro objetivo es demostrar el teorema 2.1. Pero antes vamos a probar una versión débil del mismo. Un ideal I del anillo A se llama ideal no trivial si $I \neq A$.

Teorema 2.2 (Teorema débil de los ceros de Hilbert)**.** *Supongamos que $I \subsetneq k[\mathbf{x}]$ es un ideal no trivial y k es un campo algebraicamente cerrado. Entonces existe una solución de I en k, es decir, $\exists\, \alpha \in k^n \ \forall f \in I, \ \ f(\alpha) = 0$.*

Para la demostración usaremos el homomorfismo evaluación en $a \in k$, $\mathrm{ev_a} : \mathrm{k[x_1, \ldots, x_n]} \to \mathrm{k[x_2, \ldots, x_n]}$ definido por $f(x_1, x_2, \ldots, x_n) \mapsto f(a, x_2, \ldots, x_n)$.

Lema 2.3. *Sea k algebraicamente cerrado. Supongamos que $I \cap k[x_1] = \langle p \rangle$ para un $p \in k[x] \setminus k$. Entonces existe $a \in k$, con $p(a) = 0$, tal que* $\mathrm{ev_a(I)} \neq \mathrm{k[x_2, \ldots, x_n]}$.

Lema 2.4. *Supongamos que $I \cap k[x_1] = \{0\}$. Entonces existe un polinomio $q \in k[x]$ tal que para todo $a \in k$, con $q(a) \neq 0$, tenemos que* $\mathrm{ev_a(I)} \neq \mathrm{k[x_2, \ldots, x_n]}$.

Demostraremos que los lemas 2.3 y 2.4 implican el teorema 2.2. La idea es la siguiente: Dado $I \subsetneq k[x_1, \ldots, x_n]$ un ideal, aplicando los lemas 2.3 y 2.4 existe $a_1 \in k$ tal que $I_1 = \mathrm{ev_{a_1}(I)} \neq \mathrm{k[x_2, \ldots, x_n]}$. Luego, existe $a_2 \in k$ tal

que $I_2 = \mathrm{ev_{a_2}(I)} \neq \mathrm{k[x_3, \ldots, x_n]}$. Continuando de esta forma, obtenemos una solución $a_1, a_2, \ldots, a_n$.

La dualidad con la demostración presentada en [3] es que la inducción va en la otra dirección. Más precisamente, en [3] se demuestra lo siguiente: Sea $I \subsetneq k[x_1, \ldots, x_n]$ un ideal. Después de un cambio de variables, si $(a_2, \ldots, a_n)$ es una solución de $I \cap k[x_2, \ldots, x_n]$ entonces $\{f(x, a_2, \ldots, a_n) \mid f \in I\} \neq k[x]$.

Demostración del Lema 2.3.

Proposición 2.5. *Sean k un campo, $f_1, f_2 \in k[x_1]$ y $G = \{g_1, g_2, \ldots, g_r\} \subset k[\mathbf{x}]$. Si $\mathrm{mcd(f_1, f_2)} = 1$, entonces $\langle f_1 f_2, G\rangle = \langle f_1, G\rangle \cap \langle f_2, G\rangle$.*

Demostración. Observemos que $\langle f_1, G\rangle + \langle f_2, G\rangle = k[\mathbf{x}]$, pues $Q_1 f_1 + Q_2 f_2 \in \langle f_1, G\rangle + \langle f_2, G\rangle$ y la ecuación $Q_1 f_1 + Q_2 f_2 = 1$ tiene solución. Por lo tanto:

$$\langle f_1, G\rangle \cap \langle f_2, G\rangle = \langle f_1, G\rangle\langle f_2, G\rangle = \langle f_1 f_2, f_1 G, f_2 G\rangle = \langle f_1 f_2, G\rangle.$$

□

Mediante un argumento inductivo, la Proposición 2.5 implica que:

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

Proposición 2.6. *Sea I un ideal de $k[\mathbf{x}]$. Entonces, $I = k[\mathbf{x}]$ si y sólo si $\sqrt{I} = k[\mathbf{x}]$.*

Demostración. Si $\sqrt{I} = k[\mathbf{x}]$, entonces $1 \in \sqrt{I}$. Luego, $1^r \in I$ para algún $r \in \mathbb{Z}^+$, pero $1^r = 1$. Por lo tanto, $1 \in I$ y ası$I = k[\mathbf{x}]$. El recíproco es fácil. □

Corolario 2.7. *Sean k un campo algebraicamente cerrado, $f \in k[x_1]$, $G \subseteq k[x_1, \ldots, x_n]$. Supongamos que $\langle f, G\rangle \neq k[x_1, \ldots, x_n]$. Entonces existe $a \in k$, con $f(a) = 0$, tal que $\langle (x_1 - a), G\rangle \neq k[x_1, \ldots, x_n]$.*

Demostración. Sea $\langle f, G\rangle \neq k[x_1, \ldots, x_n]$. De acuerdo con la relación (1) tenemos que $\langle (x_1 - a)^d, G\rangle \neq k[x_1, \ldots, x_n]$ para algún a tal que $f(a) = 0$ y $d \in \mathbb{N}$. Es claro que $\langle (x_1 - a), G\rangle \subset \sqrt{\langle (x_1 - a)^d, G\rangle}$. □

El lema 2.3 se sigue ahora del isomorfismo:

$$k[x_1, \ldots, x_n]/\langle (x_1 - a), G\rangle \sim k[x_2, \ldots, x_n]/\mathrm{ev_a}(\langle \mathrm{G}\rangle)$$

y de que $\langle (x_1 - a), G\rangle \neq k[x_1, \ldots, x_n]$ si y sólo si

$$\mathrm{ev_a}(\langle \mathrm{(x_1 - a), G}\rangle) \neq \mathrm{k[x_2, \ldots, x_n]}\,.$$

Demostración del Lema 2.4. La idea es considerar $k[\mathbf{x}]$ como

$$k[x_1][x_2, \ldots, x_n]\,.$$

Entonces los polinomios tienen $x_2, \ldots, x_n$ como variables, con coeficientes en el anillo $k[x_1]$. Sea Γ una base de Gröbner fuerte y finita para un ideal $I \subset k[x_1][x_2, \ldots, x_n]$. Sea $q \in k[x_1]$ el producto de los coeficientes principales de todos los $g \in \Gamma$. Si $q(a) \neq 0$ entonces $\mathrm{ev_a}(\Gamma)$ es una base de Gröbner fuerte para $\mathrm{ev_a(I)}$ según la Proposición 1.3. Ahora, $\Gamma \cap k[x_1] \subseteq I \cap k[x_1] = \emptyset$ y, en consecuencia, $\mathrm{ev_a}(\Gamma) \cap \mathrm{k} = \emptyset$. El lema 2.4 se sigue de la proposición 1.2.

Demostración del Teorema 2.1. Demostraremos que el teorema 2.2 implica el teorema 2.1. La inclusión $\sqrt{I} \subseteq I(V(I))$ es clara. Recíprocamente, sea $f \in I(V(I))$. Introducimos una nueva variable z y consideramos el ideal $J = \langle (1 - zf), I\rangle$ de $k[z, \mathbf{x}]$. El ideal J no tiene soluciones (si J tuviera una solución, sería solución de I. Si $\mathbf{x}_0$ es una solución de I, entonces $1 - zf(\mathbf{x}_0) = 1$, que es una contradicción.) Luego, por el teorema 2.2, $1 \in k[z, \mathbf{x}] = J$. Por lo tanto, podemos escribir:

$$1 = q_0(1 - zf) + \sum_{j=1}^{r} q_j g_j, \text{ donde } g_j \in I, q_j \in k[z, \mathbf{x}].$$

Sustituimos $z = \dfrac{1}{f}$ en la ecuación anterior, y después la multiplicamos por f^s, donde s es la mayor potencia de z en $q_1, \ldots q_r$, obteniendo:

$$f^s = \sum_{j=1}^{r} \tilde{q}_j g_j, \text{ donde } g_j \in I, \tilde{q}_j \in k[\mathbf{x}],$$

lo que implica $f^s \in I$ y por lo tanto, $f \in \sqrt{I}$.

Referencias

[1] William W. Adams & Philippe Loustaunau. *An Introduction to Grobner Bases.* 1994, 1996 by the American Mathematical Society.

[2] J. M. Almira. *Nullstellensatz revisited.* Rend. Sem. Mat. Univ. Pol. Torino **65** (3) (2007).

[3] Enrique Arrondo. *Another elementary proof of the Nullstellensatz.* Amer. Math. Montly **113** (2006).

[4] David Cox, John Little, Donal O'Shea. *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra.* New York: Springer–Verlag, 1997, 1992.

[5] Martin Kreuzer, Lorenzo Robbiano. *Computational Commutative Algebra 1.* Berlin/Heidelberg: Springer–Verlag, 2000.

(Recibido en febrero de 2013. Aceptado para publicación en abril de 2013)

Lev Glebsky
Instituto de Investigación en Comunicación Óptica
Universidad Autónoma de San Luis Potosí
Av. Karakorum 1470, Lomas Cuarta Sección, C.P. 78210

San Luis Potosí, S.L.P., México
e-mail: glebsky@cactus.iico.uaslp.mx
Carlos Jacob Rubio-Barrios
Facultad de Matemáticas
Universidad Autónoma de Yucatán
Periférico Norte Tablaje 13615, C.P. 97119
Mérida, Yucatán, México
e-mail: carlos.rubio@uady.mx