# El teorema de los ceros de Hilbert (segunda lección)

**Alexey Beshenov (cadadr@gmail.com)**

**Universidad de El Salvador. 8 de marzo de 2018**

Sea $k$ un cuerpo algebraicamente cerrado. En esta lección vamos a deducir del teorema de los ceros débil ($V(\mathfrak{a}) = \emptyset$ implica $\mathfrak{a} = k[X_1, \ldots, X_n]$) que

$$I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}.$$

## 1 Álgebra conmutativa: localización

Ahora para deducir otra variante del teorema de los ceros, necesitamos revisar el concepto de la localización de anillos conmutativos.

**1.1. Definición.** Sea $A$ un anillo conmutativo. Se dice que $S \subset A$ es un **subconjunto multiplicativo** si $1 \in S$ y para todo $s, t \in S$ se tiene $st \in S$.

La **localización** de $A$ respecto a $S$ es un anillo $S^{-1}A$ junto con un homomorfismo $i\colon A \to S^{-1}A$ que satisface la siguiente propiedad universal: los elementos $i(S) \subset S^{-1}A$ son invertibles y todo morfismo $\phi\colon A \to B$ tal que $\phi(S)$ es invertible en $B$ se factoriza de modo único por $S^{-1}A$:

$$\begin{tikzcd} A \arrow[r, "\phi"] \arrow[d, "i"'] & B \\ S^{-1}A \arrow[ur, dashed, "\exists!"'] & \end{tikzcd}$$

Como siempre, la propiedad universal define a $S^{-1}A$ de modo único salvo isomorfismo único. Para ver que la localización siempre existe, necesitamos dar alguna construcción particular de $S^{-1}A$. Consideremos la siguiente relación sobre el conjunto $A \times S$:

$$(f, s) \sim (f', s') \iff t\,(fs' - sf') = 0 \text{ para algún } t \in S.$$

**1.2. Lema.** *$\sim$ es una relación de equivalencia.*

*Demostración.* La relación es reflexiva. Tenemos

$$1 \cdot (fs - sf) = 0.$$

Aquí hemos usado el hecho de que $1 \in S$. La relación es simétrica: si $(f, s) \sim (f', s')$, entonces

$$t\,(fs' - sf') = 0$$

para algún $t \in S$. Luego, multiplicando la identidad de arriba por $-1$, se obtiene

$$t\,(sf' - fs') = 0.$$

Por fin, supongamos que $(f_1, s_1) \sim (f_2, s_2)$ y $(f_2, s_2) \sim (f_3, s_3)$. Esto quiere decir que existen algunos $t_1, t_2 \in S$ tales que

$$t_1\,(f_1 s_2 - s_1 f_2) = 0, \quad t_2\,(f_2 s_3 - s_2 f_3) = 0.$$

Entonces

$$\begin{aligned} s_2\,t_1\,t_2\,(f_1 s_3 - f_3 s_1) &= t_1\,t_2\,s_3\,f_1\,s_2 - \cancel{t_1\,t_2\,s_3\,f_2\,s_1} + \cancel{t_1\,t_2\,s_1\,f_2\,s_3} - t_1\,t_2\,s_1\,s_2\,f_3 \\ &= t_1\,t_2\,s_3\,(f_1 s_2 - f_2\,s_1) + t_1\,t_2\,s_1\,(f_2 s_3 - s_2 f_3) = 0. \end{aligned}$$

■

**1.3. Comentario.** Note que si $A$ no tiene divisores de cero y $0 \notin S$, entonces se puede omitir el factor $t$ en la identidad "$t\,(fs' - sf') = 0$". Si en $A$ hay divisores de cero, este factor es necesario para asegurar que $\sim$ sea una relación de equivalencia.

**1.4. Construcción.** Consideremos el conjunto cociente

$$S^{-1}A := (A \times S)/\sim$$

y denotemos la clase de equivalencia de $(f, s)$ por un símbolo $\frac{f}{s}$. Se ve que $S^{-1}A$ es un anillo conmutativo respecto a las operaciones

$$\frac{f}{s} + \frac{f'}{s'} = \frac{fs' + sf'}{ss'}, \quad \frac{f}{s} \cdot \frac{f'}{s'} = \frac{ff'}{ss'}.$$

**1.5. Ejercicio.** *Verifique que las fórmulas de arriba tienen sentido para las clases de equivalencia.*

El cero en $S^{-1}A$ es $\frac{0}{1}$ y la identidad es $\frac{1}{1}$. Luego, se ve que el homomorfismo natural

$$\begin{aligned} i\colon A &\to S^{-1}A, \\ f &\mapsto \frac{f}{1}. \end{aligned}$$

satisface la propiedad universal de la localización.

Un caso muy particular es el siguiente.

**1.6. Ejemplo.** Si $A$ es un dominio de integridad y $S = A \setminus \{0\}$, entonces la localización correspondiente es el **cuerpo de fracciones** $\operatorname{Frac} A$. En este caso el homomorfismo canónico $i\colon A \to \operatorname{Frac} A$ es inyectivo. ▲

Lo peor que se puede hacer es invertir el cero.

**1.7. Observación.** $S^{-1}A = 0$ *si y solamente si* $0 \in S$.

*Demostración.* Si $0 \in S$, entonces $i(0) = 0 \in S^{-1}A$ es invertible. Pero en este caso

$$1 = 0 \cdot 0^{-1} = 0,$$

así que el anillo $S^{-1}A$ es trivial. Viceversa, si $S^{-1}A = 0$, entonces $\frac{1}{1} = \frac{0}{1}$, lo que significa que

$$t\,(1 \cdot 1 - 1 \cdot 0) = 0$$

para algún $t \in S$. Pero esta identidad implica que $t = 0$. ■

Nos va a interesar la situación cuando en $A$ se invierte un solo elemento y todas sus potencias.

**1.8. Ejemplo.** Para $f \in A$ podemos considerar el conjunto multiplicativo $S := \{f^n \mid n = 0,1,2,\ldots\}$. En este caso la localización $S^{-1}A$ se denota por $A_f$. Tenemos $A_f = 0$ si y solamente si $f^n = 0$ para algún $n = 1,2,3,\ldots$, es decir, si y solamente si $f$ es un nilpotente. ▲

Hay otro modo de construir la localización: considerar el anillo de polinomios $A[X]$ y luego tomar su cociente por la relación $fX = 1$.

**1.9. Proposición.** *La aplicación*

$$A \rightarrowtail A[X] \twoheadrightarrow A[X]/(fX-1)$$

*satisface la propiedad universal de la localización y por lo tanto*

$$A[X]/(fX-1) \cong A_f.$$

*Demostración.* De hecho, $f$ es invertible en $A[X]/(fX-1)$. Sea $\phi\colon A \to B$ otro homomorfismo tal que $\phi(f)$ es invertible. Entonces, existe un homomorfismo

$$\begin{aligned} &A[X] \to B, \\ &\sum_i g_i\, X^i \mapsto \sum_i \phi(g_i)\, \left(\frac{1}{\phi(f)}\right)^i, \end{aligned}$$

que envía $fX - 1$ a $\phi(f)\,\frac{1}{\phi(f)} - 1 = 0$ y por lo tanto induce un homomorfismo $A[X]/(fX-1) \to B$. Esta es una factorización única de $\phi$ por $A[X]/(fX-1)$. ■

# 2 Teorema de los ceros en la forma $I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$

Para un conjunto algebraico $V(\mathfrak{a}) \subset \mathbb{A}^n(k)$ se puede considerar el ideal $I(V(\mathfrak{a})) \subset k[X_1,\ldots,X_n]$. Sería interesante ver cuál es la relación entre $\mathfrak{a}$ y $I(V(\mathfrak{a}))$. En general este último ideal es más grande que $\mathfrak{a}$: por ejemplo, si el polinomio $f^n$ se anula sobre $V$, entonces $f$ también se anula. Esto motiva el concepto del radical.

**2.1. Definición.** Sea $A$ un anillo conmutativo. El **radical** de un ideal $\mathfrak{a} \subset A$ es dado por

$$\sqrt{\mathfrak{a}} := \{f \in k[X_1,\ldots,X_n] \mid f^n \in \mathfrak{a} \text{ para algún } n = 1,2,3,\ldots\}.$$

**2.2. Ejercicio.** *Verifique que $\sqrt{\mathfrak{a}}$ es un ideal y que $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$.*

**2.3. Definición.** Si para un ideal $\mathfrak{a} \subseteq A$ se cumple $\mathfrak{a} = \sqrt{\mathfrak{a}}$, entonces se dice que $\mathfrak{a}$ es un **ideal radical**.

He aquí una caracterización de ideales radicales.

**2.4. Definición.** Si un anillo conmutativo $A$ no tiene nilpotentes no nulos (es decir, elementos $f \neq 0$ tales que $f^n = 0$ para algún $n = 2,3,4,\ldots$), se dice que $A$ es **reducido**.

**2.5. Proposición.** *Para todo anillo conmutativo $A$ el cociente $A/\mathfrak{a}$ es reducido si y solamente si $\mathfrak{a}$ es un ideal radical.*

*Demostración.* Sea $\mathfrak{a}$ un ideal radical. Supongamos que el elemento $\overline{f} \in A/\mathfrak{a}$ representado por algún $f \in A$ es un nilpotente y $\overline{f}^n = 0$ para algún $n = 1,2,3,\ldots$ Entonces $f^n \in \mathfrak{a}$, pero puesto que $\mathfrak{a}$ es radical, esto implica $f \in \mathfrak{a}$, así que $\overline{f} = 0$ en $A/\mathfrak{a}$.

Viceversa, supongamos que $A/\mathfrak{a}$ es reducido. Sea $f \in A$ un elemento tal que $f^n \in \mathfrak{a}$ para algún $n = 1,2,3,\ldots$ Entonces, $\overline{f}^n = 0$ en $A/\mathfrak{a}$ y por lo tanto $\overline{f} = 0$ y $f \in \mathfrak{a}$. ■

Como hemos notado, para todo subconjunto $V \subset \mathbb{A}^n(k)$ se tiene

$$I(V) = \sqrt{I(V)}$$

—el polinomio $f^n$ es nulo sobre $V$ si y solamente si $f$ es nulo sobre $V$. Sin embargo, no todos los ideales radicales en $k[X_1, \ldots, X_n]$ surgen de esta manera. Por ejemplo, el ideal $(X^2 + 1) \subset \mathbb{R}[X]$ es radical, puesto que el cociente $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$ es reducido (¡es un cuerpo!). Sin embargo, el polinomio $X^2 + 1$ no tiene ceros sobre $\mathbb{A}^1(\mathbb{R})$.

Si tenemos un conjunto algebraico $V(\mathfrak{a})$ que corresponde a un ideal $\mathfrak{a}$, entonces está claro que

$$\sqrt{\mathfrak{a}} \subseteq I(V(\mathfrak{a})).$$

En general, el ideal $I(V(\mathfrak{a}))$ puede ser más grande que el radical $\sqrt{\mathfrak{a}}$, pero esto no sucede cuando el cuerpo $k$ es algebraicamente cerrado.

**2.6. Corolario (Teorema de los ceros, versión 4).** *Sea $k$ un cuerpo algebraicamente cerrado. Entonces, para todo ideal $\mathfrak{a} \subset k[X_1, \ldots, X_n]$ se cumple*

$$I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}.$$

Así que cuando $k$ es algebraicamente cerrado, existe una biyección

$$\{\text{ideales radicales } \mathfrak{a} \subseteq k[X_1, \ldots, X_n]\} \underset{I}{\overset{V}{\rightleftarrows}} \{\text{conjuntos algebraicos } V(\mathfrak{a}) \subseteq \mathbb{A}^n(k)\}$$

*Demostración.* Para $f \in I(V(\mathfrak{a}))$ tenemos que ver que $f \in \sqrt{\mathfrak{a}}$. Es lo mismo que demostrar que $f$ es un nilpotente en el anillo $k[X_1, \ldots, X_n]/\mathfrak{a}$, lo que sucede si y solamente si la localización

$$(k[X_1, \ldots, X_n]/\mathfrak{a})_f$$

es trivial. La localización es isomorfa a

$$(k[X_1, \ldots, X_n]/\mathfrak{a})[Y]/(fY - 1) \cong k[X_1, \ldots, X_n, Y]/(\mathfrak{a}, fY - 1).$$

Luego, tenemos en $\mathbb{A}^{n+1}(k)$

$$V(\mathfrak{a}, fY - 1) = \emptyset,$$

así que el teorema de los ceros débil implica

$$(\mathfrak{a}, fY - 1) = k[X_1, \ldots, X_n, Y].$$

Esto significa que

$$(k[X_1, \ldots, X_n]/\mathfrak{a})_f = 0.$$

■

**2.7. Comentario.** La demostración de $I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$ a partir de la implicación

$$V(\mathfrak{a}) = \emptyset \Rightarrow \mathfrak{a} = k[X_1, \ldots, X_n]$$

es conocida como el **truco de Rabinowitsch**. Su origen es el artículo J.L. Rabinowitsch, "Zum Hilbertschen Nullstellensatz", Math. Ann. 102 (1):520, 1929. En realidad Rabinowitsch fue un seudónimo de George Yuri Rainich (1886–1968), un físico matemático nacido en el imperio ruso que emigró a los Estados Unidos en 1922.

Como hemos visto, el "truco de Rabinowitsch" es nada más la localización.