El teorema de los ceros de Hilbert
(primera lección)

Alexey Beshenov (cadadr@gmail.com)

Universidad de El Salvador. 6 de marzo de 2018

En estos apuntes voy a revisar un par de resultados básicos de la geometría algebraica y álgebra conmutativa: el teorema de los ceros (*Nullstellensatz*) y el teorema de la base (*Basissatz*) de Hilbert.

1 Conjuntos algebraicos afines e ideales

En un primer intento, se puede decir que la geometría algebraica estudia los sistemas de ecuaciones polinomiales. A partir de ahora vamos a trabajar sobre un cuerpo fijo k. Denotemos el **espacio afín de dimensión** n **sobre** k por

$$\mathbb{A}^n(k) := \{\underline{x} = (a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in k\}.$$

1.1. Definición. Para una colección de polinomios en n variables con coeficientes en k

$$f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$$

el **conjunto algebraico afín** correspondiente es dado por sus ceros comunes:

$$V(f_1, \ldots, f_m) := \{\underline{x} \in \mathbb{A}^n(k) \mid f_1(\underline{x}) = \cdots = f_m(\underline{x}) = 0\} \subseteq \mathbb{A}^n(k).$$

Es muy incomodo trabajar con polinomios particulares: diferentes colecciones de polinomios pueden tener los mismos ceros. A saber,

1) si $f(\underline{x}) = 0$ y $g(\underline{x}) = 0$, entonces $(f+g)(\underline{x}) = 0$;

2) si $f(\underline{x}) = 0$ y h es cualquier polinomio, entonces $(h \cdot f)(\underline{x}) = 0$.

Para resolver este problema, se puede pasar a los ideales en el anillo de polinomios.

1.2. Definición. Sea A un anillo conmutativo. Un **ideal** en A es un subconjunto no vacío $\mathfrak{a} \subset A$ tal que

1) si $f, g \in \mathfrak{a}$, entonces $f + g \in \mathfrak{a}$;

2) si $f \in \mathfrak{a}$ y $h \in A$ es cualquier elemento del anillo, entonces $hf \in \mathfrak{a}$.

Se dice que $\mathfrak{a}$ es un **ideal propio** si $\mathfrak{a} \neq A$.

Esto es equivalente a decir que $\mathfrak{a}$ es un A-submódulo de A (es decir, $\mathfrak{a}$ es un subgrupo abeliano de A que es también cerrado respecto a la multiplicación por los elementos de A).

1.3. Definición. Para una colección de elementos $f_1, \ldots, f_m \in A$ el **ideal generado por** $f_1, \ldots, f_m$ es el conjunto

$$(f_1, \ldots, f_m) := \{h_1 f_1 + \cdots + h_m f_m \mid h_1, \ldots, h_m \in A\}.$$

De esta definición debe de ser claro lo siguiente.

1.4. Ejercicio. *Demuestre que* $(f_1, \ldots, f_m)$ *es un ideal, y es precisamente el ideal mínimo en* A *que contiene* $f_1, \ldots, f_m$.

El mismo ideal puede tener diferentes generadores, y por esto será útil definir los conjuntos algebraicos para ideales.

1.5. Definición. Para un ideal $\mathfrak{a} \subset k[X_1, \ldots, X_n]$ el **conjunto algebraico afín** correspondiente es dado por los ceros comunes de los polinomios en $\mathfrak{a}$:

$$V(\mathfrak{a}) := \{\underline{x} \in \mathbb{A}^n(k) \mid f(\underline{x}) = 0 \text{ para todo } f \in \mathfrak{a}\} \subseteq \mathbb{A}^n(k).$$

De la nuestra discusión está clara la siguiente propiedad.

1.6. Observación. *Para una colección de polinomios* $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$ *se tiene* $V(f_1, \ldots, f_m) = V(\mathfrak{a})$, *donde* $\mathfrak{a} = (f_1, \ldots, f_m)$ *es el ideal generado por* $f_1, \ldots, f_m$.

De esta manera, pasando a los ideales, nos hemos deshecho de la dependencia de polinomios concretos. Ahora tenemos otro problema: a priori no está claro si todo ideal en $k[X_1, \ldots, X_n]$ es de la forma $(f_1, \ldots, f_m)$ para una colección finita de polinomios; es decir, que nuestros conjuntos algebraicos $V(\mathfrak{a}) \subset \mathbb{A}^n(k)$ no forman una clase más grande que los conjuntos $V(f_1, \ldots, f_m)$. El teorema de la base de Hilbert nos ayudará a resolver esta duda.

2 El teorema de la base de Hilbert

2.1. Definición. Se dice que un módulo M sobre un anillo conmutativo A es **noetheriano** si toda cadena ascendente de submódulos

$$M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M$$

se estabiliza eventualmente; es decir, $M_i = M_{i+1}$ para todo i suficientemente grande ($i \geq i_0$ para algún índice i_0).

Se dice que un anillo conmutativo A es **noetheriano** si A es noetheriano como un módulo sobre sí mismo; es decir, si toda cadena ascendente de ideales

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq A$$

se estabiliza eventualmente.

2.2. Ejemplo. Si $A = k$ es un cuerpo, entonces es noetheriano, puesto que 0 y k son los únicos ideales en k. ▲

2.3. Teorema (Teorema de la base de Hilbert). *Si* A *es un anillo noetheriano, entonces el anillo de polinomios* $A[X]$ *es también noetheriano.*

Demostración. Consideremos una cadena ascendente de ideales

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq A[X].$$

Necesitamos ver que esta se estabiliza.

Sea $\mathfrak{a}_{i,d}$ el ideal de los elementos de A que aparecen como los coeficientes mayores de los polinomios de grado d en $\mathfrak{a}_i$. Tenemos

$$\mathfrak{a}_{i,d} \subseteq \mathfrak{a}_{i',d'} \quad \text{si } i \leq i' \text{ y } d \leq d'.$$

Entre los $\mathfrak{a}_{i,d}$ hay un número finito de ideales distintos. Supongamos lo contrario. En este caso una familia infinita de ideales distintos corresponde a un subconjunto infinito de los índices dobles $(i,d) \in \mathbb{N} \times \mathbb{N}$ y entre ellos se puede escoger una cadena infinita (i_k, d_k) con

$$i_0 \le i_1 \le i_2 \le \cdots, \quad d_0 \le d_1 \le d_2 \le \cdots$$

De aquí se obtiene una cadena ascendente

$$\mathfrak{a}_{i_0,d_0} \subsetneq \mathfrak{a}_{i_1,d_1} \subsetneq \mathfrak{a}_{i_2,d_2} \subsetneq \cdots \subsetneq A$$

pero esto contradice nuestra hipótesis que A es noetheriano.

Entonces, existe un índice i tal que

$$\mathfrak{a}_{i,d} = \mathfrak{a}_{i+1,d} = \mathfrak{a}_{i+2,d} = \cdots$$

para todo d.

Supongamos que $f \in \mathfrak{a}_{i'}$ para $i' \ge i$. Veamos por inducción sobre $d = \deg f$ que $f \in \mathfrak{a}_i$. Como la base de inducción se puede considerar el caso de $d = -\infty$; es decir, $f = 0$. Para el paso inductivo, por lo que hemos demostrado, existe un polinomio $g \in \mathfrak{a}_i$ que tiene el mismo coeficiente mayor que f y el mismo grado d. Luego, $\deg(f-g) < d$ y por la hipótesis de inducción $f - g \in \mathfrak{a}_i$, así que $f \in \mathfrak{a}_i$. ■

2.4. Corolario. *Si A es un anillo noetheriano, entonces el anillo de polinomios $A[X_1, \ldots, X_n]$ es noetheriano. En particular, si $A = k$ es un cuerpo, el anillo $k[X_1, \ldots, X_n]$ es noetheriano.*

Demostración. Se sigue por inducción sobre n y el teorema precedente, puesto que

$$k[X_1, \ldots, X_n] \cong k[X_1, \ldots, X_{n-1}][X_n].$$

■

2.5. Proposición. *Un anillo conmutativo A es noetheriano si y solamente si todo ideal $\mathfrak{a} \subseteq A$ es finitamente generado; es decir,*

$$\mathfrak{a} = (f_1, \ldots, f_m)$$

para algunos $f_1, \ldots, f_m \in A$.

Demostración. Supongamos que existe un ideal $\mathfrak{a} \subset A$ que no es finitamente generado. Entonces, en $\mathfrak{a}$ se puede encontrar una cadena de ideales

$$(f_1) \subsetneq (f_1, f_2) \subsetneq (f_1, f_2, f_3) \subsetneq \cdots \subsetneq \mathfrak{a}$$

A saber, se puede empezar por cualquier f_1 (por ejemplo $f_1 = 0$) y luego por inducción, ya que $(f_1, \ldots, f_n) \neq \mathfrak{a}$ por nuestra hipótesis, podemos escoger $a_{n+1} \in \mathfrak{a} \setminus (f_1, \ldots, f_n)$. La existencia de una cadena ascendente que no se estabiliza significa que el anillo no es noetheriano.

Para la otra dirección, supongamos que todo ideal en A es finitamente generado. Sea

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq A$$

una cadena ascendente de ideales. Entonces, la unión

$$\mathfrak{a} := \bigcup_{i \ge 0} \mathfrak{a}_i$$

es también un ideal y $\mathfrak{a} = (f_1, \ldots, f_m)$ para algunos $f_1, \ldots, f_m \in A$. Pero cada uno de estos elementos pertenece a algún ideal de la cadena, así que $\{f_1, \ldots, f_m\} \subset \mathfrak{a}_i$ para algún índice i. Luego, $\mathfrak{a}_i = (f_1, \ldots, f_m)$ y

$$\mathfrak{a}_i = \mathfrak{a}_{i+1} = \mathfrak{a}_{i+2} = \cdots$$

■

Entonces, todo ideal en el anillo $k[X_1, \ldots, X_n]$ es finitamente generado. Un ejemplo típico de anillo *no noetheriano* es el anillo $k[X_1, X_2, X_3, \ldots]$ de polinomios en una cantidad numerable de variables. Un ideal no finitamente generado en este caso es $(X_1, X_2, X_3, \ldots)$.

3 Algunas versiones del teorema de los ceros

Para todo ideal $\mathfrak{a}$ hemos definido el conjunto $V(\mathfrak{a}) \subseteq \mathbb{A}^n(k)$. En la otra dirección, a todo subconjunto $X \subseteq \mathbb{A}^n(k)$ se puede asociar el ideal de los polinomios que se anulan sobre X.

3.1. Definición. Para un subconjunto $X \subset \mathbb{A}^n(k)$, sea

$$I(X) := \{f \in k[X_1, \ldots, X_n] \mid f(\underline{x}) = 0 \text{ para todo } \underline{x} \in X\}.$$

Se ve que $I(X)$ es un ideal en $k[X_1, \ldots, X_n]$. En particular, es finitamente generado.

Entonces, tenemos dos aplicaciones:

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

Notemos las siguientes propiedades.

1) Si $\mathfrak{a} \subseteq \mathfrak{b}$, entonces $V(\mathfrak{b}) \subseteq V(\mathfrak{a})$. De hecho, cuando añadimos más polinomios, el conjunto de los nulos comunes se vuelve más pequeño.

2) Si $V \subseteq W$, entonces $I(W) \subseteq I(V)$; si añadimos más puntos, tenemos menos polinomios que se anulan sobre nuestro conjunto.

3) $\mathfrak{a} \subseteq I(V(\mathfrak{a}))$. En general, la inclusión es estricta. Más adelante vamos a aclarar la relación entre $\mathfrak{a}$ y $I(V(\mathfrak{a}))$ cuando k es algebraicamente cerrado.

   Un ejemplo particular para cuerpos no algebraicamente cerrados: en $\mathbb{R}[X]$ tenemos

$$I(V(X^2+1)) = I(\emptyset) = \mathbb{R}[X] \supsetneq (X^2+1).$$

4) $X \subseteq V(I(X))$. Si X no es un conjunto algebraico, tenemos $X \subsetneq V(I(X))$.

3.2. Ejercicio. *Obviamente,*

$$I(\emptyset) = k[X_1, \ldots, X_n], \quad V(0) = \mathbb{A}^n(k), \quad V(1) = V(k[X_1, \ldots, X_n]) = \emptyset.$$

Demuestre que

$$I(\mathbb{A}^n(k)) = (0), \quad \textit{si } k \textit{ es un cuerpo infinito.}$$

Encuentre un contraejemplo para cuerpos finitos.

3.3. Ejercicio. *Demuestre que*

$$VIV(\mathfrak{a}) = V(\mathfrak{a}) \quad y \quad IVI(X) = I(X).$$

Un caso especial es cuando el ideal $I(V)$ se construye para un conjunto $V = \{\underline{x}\}$ que consiste en un punto. En este caso el ideal $I(\{\underline{x}\})$ es maximal.

3.4. Definición. Sea A un anillo conmutativo. Se dice que un ideal $\mathfrak{m} \subset A$ es **maximal** si $\mathfrak{m} \neq A$ y si hay otro ideal $\mathfrak{a}$ tal que $\mathfrak{m} \subseteq \mathfrak{a} \subseteq A$ se cumple $\mathfrak{a} = \mathfrak{m}$ o $\mathfrak{a} = A$.

El conjunto de todos los ideales maximales en A se llama el **espectro maximal** de A y se denota por $\operatorname{Max}(A)$.

3.5. Ejercicio. *Recuerde el siguiente resultado. Si A es un anillo conmutativo, entonces todo ideal propio $\mathfrak{a} \subsetneq A$ está contenido en algún ideal maximal $\mathfrak{m}$. En particular, todo anillo posee un ideal maximal.*

Esto se deduce del lema de Zorn que es equivalente al axioma de elección.

3.6. Lema. *Un ideal $\mathfrak{m} \subset A$ es maximal si y solamente si el anillo cociente $A/\mathfrak{m}$ es un cuerpo. En este caso*

$$\kappa(\mathfrak{m}) := A/\mathfrak{m}$$

*se llama el **cuerpo residual** de $\mathfrak{m}$.*

3.7. Ejercicio. *Recuerde o demuestre las siguientes propiedades.*

1) *Un anillo conmutativo no nulo A es un cuerpo si y solamente si los únicos ideales de A son 0 y A.*

2) *Si A es un anillo conmutativo y $\mathfrak{a} \subset A$ es un ideal, entonces todos los ideales en $A/\mathfrak{a}$ son de la forma $\mathfrak{b}/\mathfrak{a}$ para $\mathfrak{a} \subseteq \mathfrak{b} \subseteq A$.*

Demostración del lema. Usando el ejercicio, tenemos

$$\begin{aligned} \mathfrak{m} \subset A \text{ es maximal} \iff \text{ no existe } \mathfrak{m} \subsetneq \mathfrak{b} \subsetneq A \iff \text{ no existe } 0 \subsetneq \mathfrak{b}/\mathfrak{m} \subsetneq A/\mathfrak{m} \\ \iff A/\mathfrak{m} \text{ es un cuerpo.} \end{aligned}$$

■

3.8. Proposición. *Para un punto $\underline{x} = (a_1, \ldots, a_n) \in \mathbb{A}^n(k)$ tenemos*

$$I(\{\underline{x}\}) = \mathfrak{m}_{\underline{x}} := (X_1 - a_1, \ldots, X_n - a_n).$$

Este es un ideal maximal.

Demostración. Consideremos el homomorfismo de evaluación en $\underline{x}$

$$\begin{aligned} ev_{\underline{x}} \colon k[X_1, \ldots, X_n] &\to k, \\ f &\mapsto f(a_1, \ldots, a_n). \end{aligned}$$

Por la definición, su núcleo es $I(\{\underline{x}\})$. Luego, todo polinomio $f \in k[X_1, \ldots, X_n]$ puede ser escrito como

$$f(X_1, \ldots, X_n) = g(X_1 - a_1, \ldots, X_n - a_n)$$

para algún $g \in k[X_1, \ldots, X_n]$, y $f(a_1, \ldots, a_n)$ es el término constante de g. Entonces,

$$f \in I(\{\underline{x}\}) \iff f(a_1, \ldots, a_n) = 0 \iff f \in \mathfrak{m}_{\underline{x}},$$

así que

$$\ker ev_{\underline{x}} = I(\{\underline{x}\}) = \mathfrak{m}_{\underline{x}}.$$

Luego, el homomorfismo $ev_{\underline{x}}$ es sobreyectivo y el teorema de isomorfía nos dice que

$$k[X_1, \ldots, X_n]/\mathfrak{m}_{\underline{x}} \cong k.$$

Este es un cuerpo, y por lo tanto $\mathfrak{m}_{\underline{x}}$ es un ideal maximal. ■

En la última demostración hemos visto que el ideal $\mathfrak{m}_{\underline{x}}$ siempre tiene k como su cuerpo residual:

$$\kappa(\mathfrak{m}_{\underline{x}}) := k[X_1, \ldots, X_n]/\mathfrak{m}_{\underline{x}} \cong k.$$

3.9. Ejercicio. *Demuestre que si $\mathfrak{m} \subset k[X_1, \ldots, X_n]$ es un ideal maximal, entonces el conjunto $V(\mathfrak{m})$ consiste en un punto o es vacío.*

3.10. Ejemplo. Para el ideal maximal $(X^2 + 1) \subset \mathbb{R}[X]$ tenemos $V(X^2 + 1) = \emptyset$. ▲

De hecho, todos los ideales maximales con $\kappa(\mathfrak{m}) = k$ corresponden a los puntos del espacio afín.

3.11. Proposición. *Existe una biyección natural*

$$\begin{aligned} \mathbb{A}^n(k) &\xrightarrow{\cong} \mathrm{Max}_k(k[X_1, \ldots, X_n]) := \{\mathfrak{m} \in \mathrm{Max}(k[X_1, \ldots, X_n]) \mid \kappa(\mathfrak{m}) = k\}, \\ \underline{x} &\mapsto \mathfrak{m}_{\underline{x}}. \end{aligned}$$

En general, para un ideal $\mathfrak{a} \subseteq k[X_1, \ldots, X_n]$ existe una biyección natural

$$V(\mathfrak{a}) \cong \mathrm{Max}_k(k[X_1, \ldots, X_n]/\mathfrak{a}).$$

Demostración. Todo ideal maximal $\mathfrak{m}$ es el núcleo del homomorfismo

$$\phi\colon k[X_1, \ldots, X_n] \twoheadrightarrow k[X_1, \ldots, X_n]/\mathfrak{m} =: \kappa(\mathfrak{m}).$$

Si $\kappa(\mathfrak{m}) = k$, consideremos el punto

$$\underline{x} = (\phi(X_1), \ldots, \phi(X_n)) \in \mathbb{A}^n(k).$$

Ahora se ve que

$$\mathfrak{m}_{\underline{x}} = \ker \phi = \mathfrak{m}$$

y esto nos da la correspondencia inversa a $\underline{x} \mapsto \mathfrak{m}_{\underline{x}}$.

En general, para un ideal $\mathfrak{a} \subseteq k[X_1, \ldots, X_n]$, nótese que tenemos $\underline{x} \in V(\mathfrak{a})$ si y solamente si $\mathfrak{a} \subseteq \mathfrak{m}_{\underline{x}}$. Los ideales maximales que contienen al ideal $\mathfrak{a}$ corresponden a los ideales maximales en el anillo cociente $k[X_1, \ldots, X_n]/\mathfrak{a}$. Esto demuestra que la biyección

$$\mathbb{A}^n(k) \cong \mathrm{Max}_k(k[X_1, \ldots, X_n])$$

induce una biyección

$$V(\mathfrak{a}) \cong \mathrm{Max}_k(k[X_1, \ldots, X_n]/\mathfrak{a}).$$

■

En general, el anillo $k[X_1, \ldots, X_n]$ puede tener ideales maximales con cuerpos residuales distintos de k. Por ejemplo, en el anillo $\mathbb{R}[X]$ hay un ideal maximal $(X^2 + 1)$ con el cuerpo residual

$$\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}.$$

La buena noticia es que $\kappa(\mathfrak{m})$ es siempre una extensión algebraica de k.

3.12. Teorema (Teorema de los ceros, versión básica). *Para todo ideal maximal $\mathfrak{m} \subset k[X_1, \ldots, X_n]$ el cuerpo residual $\kappa(\mathfrak{m})$ es una extensión algebraica de k.*

Vamos a posponer la demostración de este resultado y primero investigar sus numerosas consecuencias. Primero, si el cuerpo k es algebraicamente cerrado, entonces $\kappa(\mathfrak{m}) = k$ para todo ideal maximal $\mathfrak{m} \subset k[X_1, \ldots, X_n]$; es decir,

$$\operatorname{Max}(k[X_1, \ldots, X_n]) = \operatorname{Max}_k(k[X_1, \ldots, X_n]),$$

y 3.11 implica el siguiente resultado.

3.13. Corolario (Teorema de los ceros, segunda versión). *Supongamos que k es un cuerpo algebraicamente cerrado. Entonces hay una biyección natural*

$$\begin{aligned} \mathbb{A}^n(k) &\xrightarrow{\cong} \operatorname{Max}(k[X_1, \ldots, X_n]), \\ \underline{x} &\mapsto \mathfrak{m}_{\underline{x}}. \end{aligned}$$

En general, para un ideal $\mathfrak{a} \subseteq k[X_1, \ldots, X_n]$ hay una biyección natural

$$V(\mathfrak{a}) \cong \operatorname{Max}(k[X_1, \ldots, X_n]/\mathfrak{a}).$$

He aquí otra versión común del teorema que puede ser familiar.

3.14. Corolario (Teorema de los ceros débil). *Sea k un cuerpo algebraicamente cerrado. Entonces para un ideal $\mathfrak{a} \subset k[X_1, \ldots, X_n]$ se tiene $V(\mathfrak{a}) = \emptyset$ si y solamente si $\mathfrak{a} = k[X_1, \ldots, X_n]$.*

Demostración. Supongamos que $\mathfrak{a} \subsetneq k[X_1, \ldots, X_n]$. En este caso existe algún ideal maximal $\mathfrak{m} \supseteq \mathfrak{a}$, y por lo tanto $V(\mathfrak{m}) \subseteq V(\mathfrak{a})$. Puesto que k es algebraicamente cerrado, $V(\mathfrak{m}) = \{\underline{x}\}$, así que $\mathfrak{a} \neq \emptyset$. ■

En cierto sentido, es una generalización del teorema fundamental del álgebra. El último nos dice que todo polinomio no constante en $\mathbb{C}[X]$ tiene una raíz. El teorema de los ceros débil nos dice que para todo ideal propio $\mathfrak{a} \subsetneq k[X_1, \ldots, X_n]$ (es decir, $\mathfrak{a}$ que no contiene los polinomios constantes) los polinomios en $\mathfrak{a}$ tienen un cero común.