Clase 16: Hilbert Nullstellensatz y Topología de Zariski

§29. Algunos teoremas de Hilbert (continuación):

La vez pasada: Sea A un anillo y $I \subseteq A$ un ideal.

- Radical de I: $\sqrt{I} = \{ a \in A$ tal que $\exists n \geq 1$ con $a^n \in I \} = \bigcap_{I \subseteq \mathfrak{p} \text{ primo}} \mathfrak{p}$.

- Ideal radical: si $I = \sqrt{I}$. Esto equivale a A/I reducido (i.e., 0 es el único elemento nilpotente)

- Anillo noetheriano: Toda cadena creciente de ideales de A se estabiliza $\Leftrightarrow$ Todo $I \subseteq A$ es finitamente generado.

- Teorema de la base de Hilbert: A noetheriano $\Rightarrow A[X_1, \ldots, X_n]$ noetheriano.

- Espacio afín (complejo): $\mathbb{A}^n = \mathbb{A}^n(\mathbb{C}) = \mathbb{C}^n$ ("olvidamos" que es un e.v.)

Sea $S \subseteq \mathbb{C}[X_1, \dots, X_n]$ un subconjunto arbitrario de polinomios.
$\left(\Rightarrow \langle S \rangle = \langle f_1, \dots, f_r \rangle\right.$ gracias Teorema de la base de Hilbert ! $)$

<u>Def</u>: El conjunto de ceros <u>comunes</u>

$$V(S) := \{ a = (a_1, \dots, a_n) \in \mathbb{A}^n \text{ tq } f(a) = 0 \ \forall f \in S \}$$ ← "vanishing"

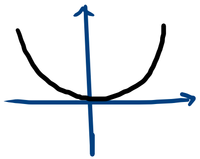
es llamado un conjunto algebraico afín de $\mathbb{A}^n$.

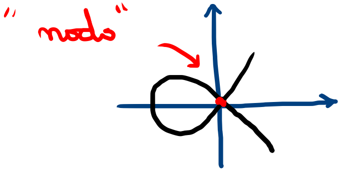
<u>Caso particular importante</u>: Si $S = \{f\}$ es un <u>único</u> polinomio $f \in k[X_1, \dots, X_n]$ no-nulo y no-constante, entonces

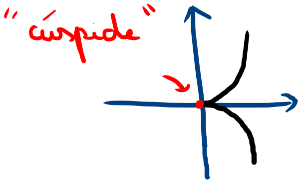
$$V(f) = \{ (a_1, \dots, a_n) \in \mathbb{A}^n \text{ tal que } f(a_1, \dots, a_n) = 0 \}$$

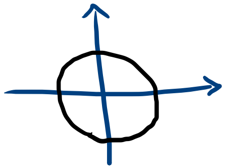
es llamado una hipersuperficie de $\mathbb{A}^n$.

<u>Eg</u>: $V(y - x^2) \subseteq \mathbb{A}^2$ $\quad V(y^2 - x^2(x+1)) \subseteq \mathbb{A}^2$ $\quad V(y^2 - x^3) \subseteq \mathbb{A}^2$ $\quad V(x^2 + y^2 - 1) \subseteq \mathbb{A}^2$









Ejemplos / Propiedades importantes:

① $V(1) = \emptyset$ y $V(\emptyset) = V(0) = \mathbb{A}^n$

② Si $T \subseteq S$ entonces $V(S) \subseteq V(T)$ "más ecuaciones $\rightsquigarrow$ menos puntos"

③ $\boxed{\text{Ejercicio importante}}$ Sea $I = \langle S \rangle$, entonces $V(S) = V(I) = V(\sqrt{I})$.

$\rightsquigarrow$ Basta considerar ideales (radicales)!

④ Sea $\{S_i\}_{i \in I} \subseteq \mathbb{C}[x_1, \ldots, x_n]$ colección arbitraria, entonces

$$\bigcap_{i \in I} V(S_i) \overset{\text{dy?}}{=} V\Big(\bigcup_{i \in I} S_i\Big)$$ $\longrightarrow$ Intersección arbitraria de conj. algebraicos es un conjunto algebraico.

⑤ Unión finita de conj. algebraicos es un conjunto algebraico:

Dados $S, T \subseteq \mathbb{C}[x_1, \ldots, x_n]$ no-vacíos, definimos $ST := \{ fg \, , \, f \in S \text{ y } g \in T \}$.

$$\Longrightarrow V(S) \cup V(T) = V(ST).$$

$(\subseteq)$ Si $a \in V(S) \cup V(T)$ (ie, $f(a) = 0 \ \forall f \in S$ ó $g(a) = 0 \ \forall g \in T$) $\Rightarrow (fg)(a) = 0 \ \forall fg \in ST$

$(\supseteq)$ Si $a \notin V(S) \cup V(T)$, $\exists f_0 \in S$ tq $f_0(a) \neq 0$ y $\exists g_0 \in T$ tq $g_0(a) \neq 0$

$\Rightarrow (f_0 g_0)(a) \neq 0$ y luego $a \notin V(ST)$.

Ejemplo importante: Sea $a = (a_1, \ldots, a_n) \in \mathbb{A}^n$ y sea

$$\mathfrak{m}_a := \langle X_1 - a_1, \ldots, X_n - a_n \rangle \subseteq \mathbb{C}[X_1, \ldots, X_n] \text{ ideal maximal}$$

(pues $\mathbb{C}[X_1, \ldots, X_n]/\mathfrak{m}_a \cong \mathbb{C}$ cuerpo). Entonces, $V(\mathfrak{m}_a) = \{(a_1, \ldots, a_n)\}$.

En efecto, $f \in \mathfrak{m}_a \overset{\text{def}}{\iff} f = (X_1 - a_1)p_1 + \ldots + (X_n - a_n)p_n$ y luego $a \in V(\mathfrak{m}_a)$.
Si $b = (b_1, \ldots, b_n) \in V(\mathfrak{m}_a) \overset{\text{def}}{\iff} f(b) = 0 \ \forall f \in \mathfrak{m}_a$. En part, $f_i = X_i - a_i \in \mathfrak{m}_a$
y luego $f_i(b) = b_i - a_i = 0$, i.e., $b = (a_1, \ldots, a_n)$ ✓

En lo que sigue, admitiremos sin demostración (¿o quizás más adelante?) el siguiente resultado de Hilbert:

↳ Usa que estamos en $\mathbb{C}$.

ceros lugar Teorema

Nullstellensatz débil: Los únicos ideales maximales de $\mathbb{C}[X_1, \ldots, X_n]$ son los

$$\mathfrak{m}_a := \langle X_1 - a_1, \ldots, X_n - a_n \rangle$$

para ciertos $(a_1, \ldots, a_n) \in \mathbb{A}^n(\mathbb{C}) = \mathbb{C}^n$.

Corolario: Sea $S = \{f_i\}_{i\in I}$ una familia (arbitraria) de polinomios en $\mathbb{C}[x_1,\dots,x_n]$ sin ceros comunes (i.e. $V(S)=\emptyset$). Entonces, $\langle S\rangle = \mathbb{C}[x_1,\dots,x_n]$.

Dem: Sea $I=\langle S\rangle$. Si $I \subsetneq \mathbb{C}[x_1,\dots,x_n] \overset{\text{Krull}}{\Longrightarrow} I \subseteq \exists\, \mathfrak{m} = \mathfrak{m}_a$ (Nullstellensatz débil) $= \langle x_1-a_1,\dots,x_n-a_n\rangle$

$$\Rightarrow \underbrace{V(\mathfrak{m}_a)}_{=\{a\}} \subseteq V(I) = \emptyset \quad ↯ \qquad \blacksquare$$

$$\left\{\begin{array}{l} f_1 = 0 \\ \vdots \\ f_r = 0 \end{array}\right\} \text{ no tiene sol. en } \mathbb{A}^n \iff \langle f_1,\dots,f_r\rangle = \mathbb{C}[x_1,\dots,x_n]$$

Consecuencia práctica:

Si $V(S)=\emptyset$, entonces existen $f_1,\dots,f_r \in S$ y $g_1,\dots,g_r \in \mathbb{C}[x_1,\dots,x_n]$ tales que

$$f_1g_1 + \dots + f_rg_r = 1 \quad (\text{"Partición de la unidad"}).$$

Cultura general: Sea $\Omega \subseteq \mathbb{R}^n$ abierto $\neq \emptyset$ y $\Omega = \bigcup_{i\in I} \mathcal{U}_i$ cubrimiento abierto.

Una partición de la unidad de Ω es un conj. de funciones continuas

$$R = \{\rho_i : \Omega \to [0,1]\}_{i\in I}$$

con $\operatorname{supp}(\rho_i) \subseteq \mathcal{U}_i$, $\forall x\in\Omega\ \exists\, \mathcal{U}\ni x$ vecindad tq $\rho_i(x)\neq 0$ para finitos $i\in I$, $\sum_{i\in I} \rho_i(x) = 1$.

Ya podemos enunciar el Teorema de los ceros de Hilbert (fuerte), que usualmente se enuncia con su nombre en alemán:

Hilbert Nullstellensatz (1893): Sea $g \in \mathbb{C}[X_1, \dots, X_n]$ y sea $I \subseteq \mathbb{C}[X_1, \dots, X_n]$ un ideal. Si g se anula en $V(I) \subseteq \mathbb{A}^n$ (ie, para todo $a \in V(I)$ se tiene que $g(a) = 0$), entonces $\exists N \in \mathbb{N}^{\geq 1}$ tal que $g^N \in I$ (ie, $g \in \sqrt{I}$).

En part,

"Si I es radical: $g|_{V(I)} = 0 \Rightarrow g \in I$"

Dem: $I = \langle f_1, \dots, f_r \rangle$ (base de Hilbert). "Truco de Rabinowitch": Agregar una variable X_{n+1}:

$\Rightarrow$ Los pol. $f_1, \dots, f_r$ y $f_{r+1} := X_{n+1} g - 1$ no tienen ceros comunes (por hipótesis) en $\mathbb{A}^{n+1}$ $\overset{\text{cor.}}{\Rightarrow}$ $\langle f_1, \dots, f_r, X_{n+1} g - 1 \rangle = \mathbb{C}[X_1, \dots, X_{n+1}] = \langle 1 \rangle$

$\rightsquigarrow \exists$ pol. $p_1, \dots, p_{r+1} \in \mathbb{C}[X_1, \dots, X_{n+1}]$ tq $f_1 p_1 + \dots + f_r p_r + (X_{n+1} g - 1) \cdot p_{r+1} = 1$ $(\star)$

Consideremos el siguiente morfismo de $\mathbb{C}$-algebras:

$$\varphi : \mathbb{C}[X_1, \dots, X_{n+1}] \longrightarrow \mathbb{C}(X_1, \dots, X_n)\,;\quad X_1 \mapsto X_1, \dots, X_n \mapsto X_n,\; X_{n+1} \longmapsto \frac{1}{g}$$

$$\varphi(\star): \quad 1 = p_1\left(X_1, \dots, X_n, \frac{1}{g}\right) f_1 + \dots + p_r\left(X_1, \dots, X_n, \frac{1}{g}\right) f_r + 0$$

$\rightsquigarrow$ Mult. por el denominador común g^N $\rightsquigarrow$ $g^N = \tilde{p}_1 f_1 + \dots + \tilde{p}_r f_r \in \langle f_1, \dots, f_r \rangle = I$ $\blacksquare$

La siguiente definición permite reformular convenientemente el Hilbert Nullstellensatz:

Def: Sea $X \subseteq \mathbb{A}^n$ un subconjunto (arbitrario). Definimos el ideal de X por:

$$\mathcal{I}(X) := \{ f \in \mathbb{C}[x_1, \ldots, x_n] \text{ tal que } f(a) = 0 \text{ para todo } a \in X \}$$

Ejemplos y Propiedades:

1. Si $X \subseteq Y \subseteq \mathbb{A}^n$, entonces $\mathcal{I}(Y) \subseteq \mathcal{I}(X)$. "más puntos ⇝ menos ecuaciones"

2. Si $X, Y \subseteq \mathbb{A}^n$, entonces $\mathcal{I}(X \cup Y) = \mathcal{I}(X) \cap \mathcal{I}(Y)$.

3. $\mathcal{I}(\phi) = \mathbb{C}[x_1, \ldots, x_n]$ y $\mathcal{I}(\mathbb{A}^n) = \langle 0 \rangle$ $\boxed{\text{Ejercicio}}$ (Fijar $n-1$ variables y usar $\mathbb{C}$ infinito).

4. Hilbert Nullstellensatz (reformulación): Para todo ideal $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$

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

En part, I es un ideal radical $\iff$ $\mathcal{I}(V(I)) = I$.

§ 30 Topología de Zariski y funciones regulares

La noción de topología (Poincaré 1895) y de espacio topológico (Hausdorff 1914) son centrales en prácticamente todas las áreas de las matemáticas:

Def: Sea X un conjunto y sea $\tau = \{\mathcal{U}_i\}_{i \in I}$ familia de subconjuntos de X. Decimos que τ es una topología (y que (X,τ) es un espacio topológico) si:

① $\emptyset \in \tau$ y $X \in \tau$.

② Para cada $J \subseteq I$, la unión arbitraria $\bigcup_{j \in J} \mathcal{U}_j \in \tau$.

③ Para $\mathcal{U}, V \in \tau$, la intersección finita $\mathcal{U} \cap V \in \tau$.

Terminología: Los elementos $\mathcal{U} \in \tau$ son llamados abiertos, y sus complementos $F := X \setminus \mathcal{U}$ son llamados cerrados.

Obs: Considerando complementos en ①, ② y ③, notamos que τ también se define a partir de sus cerrados: ① $\emptyset$ y X son cerrados; ② Intersección arbitraria de cerrados es cerrado; ③ Unión finita de cerrados es cerrado.

Def: Sea (X,τ) un espacio topológico. Un subconjunto de abiertos $\mathcal{B}\subseteq\tau$ es una **base** si:

1. $X=\bigcup_{U\in\mathcal{B}} U$, i.e., los elementos de $\mathcal{B}$ cubren X.
2. Para cada intersección (no-vacía) $U\cap V$ con $U,V\in\mathcal{B}$ se tiene que: $\forall x\in U\cap V$ existe $W\in\mathcal{B}$ tal que $x\in W\subseteq U\cap V$.

Ejemplo: En $X=\mathbb{R}^n$ con la topología euclideana (i.e., definida a partir de la distancia $d_{eucl}(x,y)=\sqrt{(x_1-y_1)^2+\dots+(x_n-y_n)^2}$), una base está dada por las bolas:

$$\mathcal{B}=\{B_r(a),\ r\in\mathbb{R}^{>0} \text{ y } a\in\mathbb{R}^n\}$$

Def: Sea $f: X\to Y$ una función entre dos espacios topológicos (X,τ_X) e (Y,τ_Y). Decimos que f es una **función continua** si:

"Para todo abierto $V\subseteq Y$, la preimagen $f^{-1}(V)\subseteq X$ es un abierto"

Terminología: Decimos que $f: X\xrightarrow{\sim} Y$ es un **homeomorfismo** si f es biyectiva y si tanto f como f^{-1} son funciones continuas.