Clase 18: Geometría de Ideales y Teorema Chino del Resto

La vez pasada probamos que si $X = V(I) \subseteq \mathbb{A}^n$ variedad algebraica afín, entonces X está completamente determinada por

$$\mathcal{O}(X) = \{ f : X \to \mathbb{C} \ \text{función regular} \} \overset{\text{def}}{=} \mathrm{Im}\left[\mathcal{O}(\mathbb{A}^n) \overset{\text{res}}{\twoheadrightarrow} \mathcal{O}(X),\ F \mapsto f := F|_X \right]$$

$$\cong \mathcal{O}(\mathbb{A}^n) / \mathcal{I}(X),$$

donde $\mathcal{O}(\mathbb{A}^n) = \mathbb{C}[X_1, \dots, X_n]$. Más precisamente, si $Y = V(J) \subseteq \mathbb{A}^m$ es otra variedad algebraica afín, entonces $X \cong Y \iff \mathcal{O}(X) \cong \mathcal{O}(Y)$.

Eslogan: "Las propiedades geométricas de X se traducen en propiedades algebraicas de $\mathcal{O}(X)$, y viceversa". $\rightsquigarrow$ Geometría Algebraica

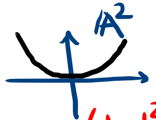
Más aún, hay una correspondencia

$$\left\{ \begin{array}{c} X \subseteq \mathbb{A}^n \ \text{var.} \\ \text{algebraica afín} \end{array} \right\} \overset{\sim}{\longleftrightarrow} \left\{ \begin{array}{c} I \subseteq \mathbb{C}[X_1, \dots, X_n] \\ \text{ideal radical} \end{array} \right\}$$

$$X \longmapsto \mathcal{I}(X)$$

$$V(I) \longleftarrow I$$

Ejemplos:

Sea $X = \{(x,y)\in \mathbb{A}^2$ tal que $y = x^2\} = V(f)$ con $f = y - x^2$  $\xleftarrow[\sim]{\varphi} \mathbb{A}^1$

$(t,t^2) \leftarrow t$

$\Rightarrow I(X) = \sqrt{\langle f\rangle}$. Calculemos $I(X)$:

$\boxed{\text{Método 1}}$: Notar que $\mathbb{C}[x,y]/\langle y-x^2\rangle \cong \mathbb{C}[x]$ dominio $\Rightarrow \langle f\rangle$ ideal primo, y en part $\sqrt{\langle f\rangle} = \langle f\rangle$ ✓ ($\Rightarrow \mathcal{O}(X)\cong \mathcal{O}(\mathbb{A}^1)$, ie, $X\cong \mathbb{A}^1$)

$\boxed{\text{Método 2}}$: Sea $P(x,y)\in I(X)$ y dividamos (en $B[y]$ con $B = A[x]$) por $f = y-x^2$ (resp. a la variable y)

$\Rightarrow P(x,y) = Q(x,y)(y-x^2)+R(x)$ evaluando en $(a,b)\in X \Rightarrow 0 = 0 + R(a)\ \forall a\in\mathbb{C}$

ie, $P\in\langle y-x^2\rangle$ y luego $I(X) = \langle y-x^2\rangle$ ✓

$\boxed{\text{Método 3}}$: Sea $\psi = \varphi^* : \mathbb{C}[x,y]\to\mathbb{C}[T]$, $x\mapsto T$, $y\mapsto T^2$ $\Rightarrow \ker\psi = \langle y-x^2\rangle$ $\boxed{\text{método 2}}$

y luego (Noether): $A = \mathbb{C}[x,y]/\langle y-x^2\rangle \hookrightarrow \mathbb{C}[T]$ ← dominio $\Rightarrow A$ dominio $\Leftrightarrow \langle y-x^2\rangle$ primo ✓

$\boxed{\text{Ejercicio}}$ Sea $X = \{(x,y,z)\in\mathbb{A}^3$ tq $y = x^2,\ z = x^3\}$. Calcular $I(X)$.

$\boxed{\text{Ejercicio importante}}$ Sea $X\subseteq \mathbb{A}^n$ var. algebraica afín. Probar que hay una biyección

$$\left\{\begin{array}{c}\mathfrak{m}\subseteq\mathcal{O}(X)\\ \text{ideal maximal}\end{array}\right\} \xleftrightarrow{\sim} \left\{\begin{array}{c}\text{Puntos}\\ a\in X\end{array}\right\}$$

Def: Sea A un anillo. Definimos su espectro maximal mediante

$$\mathrm{Specm}(A) := \{ \mathfrak{m} \subseteq A \text{ ideal maximal} \}$$

Ejemplos:

1. $\mathrm{Specm}(\mathbb{Z}) = \{ \langle p \rangle = p\mathbb{Z} , \, p \text{ primo} \} \xleftrightarrow{\sim} \mathbb{P}$ conj. de números primos.

2. Por el ejercicio anterior, si $X \subseteq \mathbb{A}^n$ es una variedad algebraica afín entonces hay una biyección entre $\mathrm{Specm}(\mathcal{O}(X))$ y los puntos de X $\rightsquigarrow$ "$\mathcal{O}(X)$ determina X"
En particular, $\mathrm{Specm}(\mathbb{C}[x_1, \ldots, x_n]) \xleftrightarrow{\sim} \{ \text{Puntos } a \in \mathbb{A}^n \}$ (Nullstellensatz débil!)

3. "$\boxed{\text{Ejercicio}}$" Sea A un DIP. Describir $\mathrm{Specm}(A)$.

Cultura general: No es casualidad que Grothendieck use la palabra "espectro".
Una consecuencia del Teorema de Gelfand - Mazur (análisis funcional $\approx$ 1930) establece un resultado análogo al Nullstellensatz débil en el contexto de álgebras de Banach, que se basa a su vez en estudiar radios espectrales ("valores propios")

§31. Geometría de Ideales

Ya hemos observado que ideales maximales (resp. radicales) de $\mathcal{O}(\mathbb{A}^n)$ están en biyección con puntos (resp. variedades alg. afines) en $\mathbb{A}^n$. ¿Qué sucede con los ideales primos?

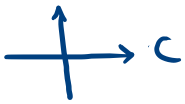
Def: Sea X un espacio topológico no-vacío. Decimos que X es irreducible si no puede ser escrito como $X = X_1 \cup X_2$ con $X_1, X_2 \subsetneq X$ cerrados propios no-vacíos (ie, si $X = X_1 \cup X_2$ con X_1, X_2 cerrados $\Rightarrow X = X_1$ ó $X = X_2$). En caso contrario, decimos que X es reducible.

Ejemplos:

1. Si X es irreducible, entonces todo par de abiertos no-vacíos $\mathcal{U}, V \subseteq X$ se intersectan (ie, $\mathcal{U} \cap V \neq \emptyset$) $\rightsquigarrow$ En caso contrario, $X = X_1 \cup X_2$ con $X_1 = \mathcal{U}^c$, $X_2 = V^c$.

   ($\rightsquigarrow$ Todo abierto $\neq \emptyset$ es denso!)

2. La variedad alg. afín $C = \{(x,y) \in \mathbb{A}^2 \text{ tq } xy = 0\} = \{x=0\} \cup \{y=0\}$ es reducible.

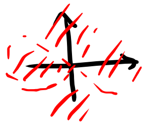


⚠ Notar que: $\mathcal{I}(C) = \langle XY \rangle$ no es primo, pues $X \notin \mathcal{I}(C)$ e $Y \notin \mathcal{I}(C)$.

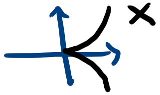
Teorema: Sea $X \subseteq \mathbb{A}^n$ variedad algebraica afín. Entonces,
X irreducible $\iff \mathcal{I}(X) \subseteq \mathbb{C}[X_1,\dots,X_n]$ ideal primo ($\iff \mathcal{O}(X)$ dominio).

Dem: ($\Rightarrow$) Sup. X irreducible y sean $f, g \in \mathcal{O}(\mathbb{A}^n)$ tales que $fg \in \mathcal{I}(X)$, i.e., $fg = 0$ en X.
$\Rightarrow X \subseteq V(fg) = V(f) \cup V(g)$ y así $X = X_1 \cup X_2$ con $X_1 = V(f) \cap X$ y $X_2 = V(g) \cap X$
X irred $\Rightarrow X_1 = X$ ó $X_2 = X$, i.e., $X \subseteq V(f)$ ó $X \subseteq V(g)$, i.e., $f \in \mathcal{I}(X)$ ó $g \in \mathcal{I}(X)$ ✓
($\Leftarrow$) Sup. $\mathcal{I}(X)$ primo y que $X = X_1 \cup X_2$ con $\emptyset \neq X_i \subsetneq X$ cerrados. Como $X_i \subsetneq X$,
$\exists f_i \in \mathcal{O}(\mathbb{A}^n)$ polinomio tal que $f_i = 0$ en X_i pero $f_i \neq 0$ en X $\Rightarrow f_i \notin \mathcal{I}(X)$.
Sin embargo, $f_1 f_2 = 0$ en $X_1 \cup X_2 = X$, i.e., $f_1 f_2 \in \mathcal{I}(X)$ ↯ ■

Ejemplos:



1. Vimos que $\mathcal{I}(\mathbb{A}^n) = \langle 0 \rangle$ ideal primo $\Rightarrow \mathbb{A}^n$ es irreducible ✓
2. Vimos que si $X = \{(x,y) \in \mathbb{A}^2 \text{ tq } y = x^2\}$ entonces $\mathcal{I}(X) = \langle Y - X^2 \rangle$ ideal primo
   $\Rightarrow X$ irreducible ✓
3. $\boxed{\text{Ejercicio}}$ Probar que $X = \{(x,y) \in \mathbb{A}^2 \text{ tq } y^2 = x^3\}$ es irreducible



4. $\boxed{\text{Ejercicio}}$ Calcular el ideal de $X = \{(0,0), (1,0)\} \subseteq \mathbb{A}^2$

Def: Sea A un anillo y sean $I, J \subseteq A$ ideales. Definimos su suma y producto por:

$$I+J := \{a+b\}_{\substack{a\in I\\ b\in J}} = \langle I\cup J\rangle \quad \text{y} \quad IJ := \langle \{ab\}_{\substack{a\in I\\ b\in J}}\rangle \overset{\text{def}}{=} \Big\{\sum_{\text{finita}} a_i b_i \text{ con } a_i\in I, b_i\in J\Big\}$$

Más generalmente, si $\{I_\lambda\}_{\lambda\in\Lambda} \subseteq A$ colección de ideales $\rightsquigarrow$ $\sum_{\lambda\in\Lambda} I_\lambda := \langle \bigcup_{\lambda\in\Lambda} I_\lambda\rangle$

Caso particular importante: Sup. que $I = \langle a_1,\dots,a_r\rangle$ y $J = \langle b_1,\dots,b_s\rangle$ son fin. generados

$$\Rightarrow I+J = \langle a_1,\dots,a_r, b_1,\dots,b_s\rangle \quad \text{y} \quad IJ = \langle a_1b_1,\dots,a_1b_r, a_2b_1,\dots,a_rb_s\rangle.$$

$\boxed{\text{Ejercicio importante}}$ Probar (eg. usando el Lema de Bézout) que si $I_n := n\mathbb{Z}$ para $n\in\mathbb{N}^{\geq 1}$ entonces: $I_n I_m = nm\mathbb{Z}$, $I_n \cap I_m = \operatorname{mcm}(n,m)\mathbb{Z}$, $I_n + I_m = \operatorname{mcd}(n,m)\mathbb{Z}$

Interpretación geométrica: Si $I, J \subseteq \mathbb{C}[x_1,\dots,x_n]$ son ideales, entonces

$$V(IJ) = V(I)\cup V(J) \quad \text{y} \quad V(I+J) = V(I)\cap V(J)$$

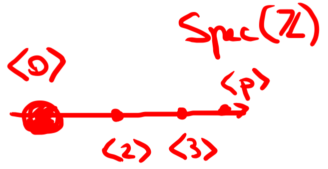
Más generalmente, si $\{I_\lambda\}_{\lambda\in\Lambda} \subseteq \mathbb{C}[x_1,\dots,x_n] \rightsquigarrow V\big(\sum_{\lambda\in\Lambda} I_\lambda\big) = \bigcap_{\lambda\in\Lambda} V(I_\lambda)$.

{Cultura general} En 1960, Grothendieck generaliza el concepto de variedad alg afín:
Sea A un anillo, definimos su **espectro** como

$$\mathrm{Spec}(A) := \{\mathfrak{p} \subseteq A \text{ ideal primo}\}$$

y decimos que los conjuntos de la forma $V(S) := \{\mathfrak{p} \in \mathrm{Spec}(A) \text{ tal que } \mathfrak{p} \supseteq S\}$, donde $S \subseteq A$ subconjunto arbitrario, son **cerrados de Zariski**.

$\rightsquigarrow$ $\mathrm{Spec}(A)$ junto a su topología de Zariski es llamado un **esquema afín**.



§32. Morfismos entre cocientes y Teorema chino del resto

Consideremos un anillo A y sean $I, J \subseteq A$ ideales tal que $I \subseteq J$. Entonces:

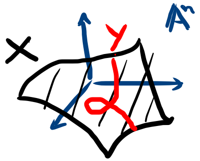
$$\begin{tikzcd} A \arrow[r, two heads, "\pi_J"] \arrow[d, "\pi_I"'] & A/J \\ A/I \arrow[ur, "\exists!\, \hat{\pi}_I"'] & \end{tikzcd}$$

$\exists!\ \hat{\pi}_I$ (pues $\pi_J(I) = 0$ en A/J $\rightsquigarrow$ Prop. Universal del Cociente)

Además, $\ker(\hat{\pi}_I) = \ker(\pi_J)/I = J/I \overset{\text{def}}{=} \pi_I(J)$ ideal de A/I. Por Noether:

Prop: Sean $I \subseteq J$ ideales de A. Entonces J/I es un ideal de A/I y además

$$(A/I)/(J/I) \cong A/J$$



Interpretación geométrica: Sean $Y \subseteq X \subseteq \mathbb{A}^n$ variedades algebraicas afines

Entonces, $\mathcal{O}(X) \cong \mathcal{O}(\mathbb{A}^n)/\mathcal{I}(X)$ y $\mathcal{O}(Y) \cong \mathcal{O}(\mathbb{A}^n)/\mathcal{I}(Y)$

con $\mathcal{I}(X) \subseteq \mathcal{I}(Y) \subseteq \mathcal{O}(\mathbb{A}^n) \Rightarrow \mathcal{O}(Y) \cong \mathcal{O}(X)/(\mathcal{I}(Y)/\mathcal{I}(X))$

Ejemplo: Sean $I, J \subseteq A$ ideales arbitrarios y sea $K := I + J$, con $I \subseteq K$.

Luego, $(A/I)/(K/I) \cong A/K$, i.e., $(A/I)/((I+J)/I) \cong A/(I+J)$

Observación: Sea A un anillo y sean $I, J \subseteq A$ ideales. Consideremos

$$\pi_I : A \twoheadrightarrow A/I \qquad \text{y} \qquad \pi_J : A \twoheadrightarrow A/J$$

$$a \mapsto \pi_I(a) =: a \pmod{I} \qquad\qquad a \mapsto \pi_J(a) =: a \pmod{J}$$

Definamos entonces $\Phi : A \to A/I \times A/J$, $a \mapsto \Phi(a) := (a \pmod{I}, a \pmod{J})$.

Por definición, $\ker(\Phi) = I \cap J$. Luego, la Propiedad Universal del Cociente nos da

$\exists!\ \varphi : A/(I \cap J) \hookrightarrow A/I \times A/J$ morfismo inyectivo tal que $\varphi(a \pmod{I \cap J}) = \Phi(a)$

¿Bajo qué condiciones φ es un isomorfismo?

Teorema chino del resto: Sea A un anillo y sean $I, J \subseteq A$ ideales. Consideremos

$$\varphi : A/(I \cap J) \hookrightarrow A/I \times A/J$$

el morfismo inyectivo definido anteriormente. Entonces, φ es un isomorfismo si y sólo si $I + J = A$. Más aún, en tal caso se cumple que $IJ = I \cap J$ y en particular

$$A/(IJ) \cong A/(I \cap J) \cong A/I \times A/J$$

Dem: $(\Leftarrow)$ Si $I+J = A$, $\exists\, a \in I$ y $\exists\, b \in J$ tq $a+b=1$. Dados $x, y \in A$ arbitrarios, buscamos $[c] \in A/(I\cap J)$ tq $c \equiv x \pmod I$ y $c \equiv y \pmod J$ (ie, φ sobreyectivo).

Sea $c := ay + bx$ y calculamos:

$$c - x = ay + bx - x = ay + x(b-1) \overset{a+b=1}{=} ay + x(-a) = a(y-x) \overset{a \in I}{\in} I \Rightarrow c \equiv x \pmod I$$

Similar, $c \equiv y \pmod J$ y luego φ es sobreyectivo ✓

$(\Rightarrow)$ Si φ sobreyectivo, $\exists\, b \in A$ tq $\varphi(b) = ([1],[0]) \in A/I \times A/J$, ie, $b - 1 \in I$ y $b \in J$.

Sea $a := 1 - b \in I$ y notar que $a + b = 1 \Rightarrow I + J = A$ ✓

Finalmente, observamos que siempre se cumple $IJ \subseteq I \cap J$. Para probar que $I \cap J \subseteq IJ$, consideramos $a \in I$ y $b \in J$ tq $a+b=1$ y consideramos $x \in I \cap J$ y notamos:

$ax \in IJ$ (pues $a \in I$, $x \in J$) y $bx \in IJ$ (pues $b \in J$, $x \in I$) $\Rightarrow x = ax + bx \in IJ$ ■

Caso particular importante: si $A = \mathbb{Z}$ y $I = I_n \overset{\text{def}}{=} n\mathbb{Z}$, $J = I_m \overset{\text{def}}{=} m\mathbb{Z}$ con $n, m \in \mathbb{N}^{\geq 1}$

$\Rightarrow I_n + I_m = \text{mcd}(n,m)\mathbb{Z}$ y luego: $I_n + I_m = \mathbb{Z} \iff$ n y m primos entre sí.

En tal caso, $nm\mathbb{Z} = I_n I_m = I_n \cap I_m = \text{mcm}(n,m)\mathbb{Z}$ y luego:

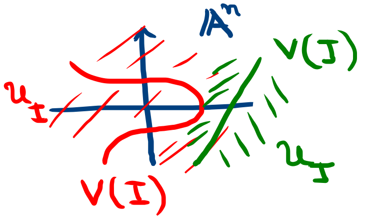
$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

Interpretación geométrica: si $I, J \subseteq \mathbb{C}[x_1, \dots, x_n] = \mathcal{O}(\mathbb{A}^n)$ son ideales radicales, entonces

$$V(IJ) = V(I) \cup V(J) \quad \text{y} \quad V(I+J) = V(I) \cap V(J)$$

Además, sabemos que $I + J = \mathcal{O}(\mathbb{A}^n) \iff V(I+J) = \emptyset$.

Luego, si escribimos $\mathcal{U}_I = \mathbb{A}^n - V(I)$ y $\mathcal{U}_J = \mathbb{A}^n - V(J)$ abiertos de Zariski, entonces $I + J = \mathcal{O}(\mathbb{A}^n) \iff \mathbb{A}^n = \mathcal{U}_I \cup \mathcal{U}_J$



$$\mathcal{O}(\mathbb{A}^n)/IJ \cong \mathcal{O}(\mathbb{A}^n)/I \times \mathcal{O}(\mathbb{A}^n)/J$$

$$\iff \mathcal{O}(V(I) \cup V(J)) \cong \mathcal{O}(V(I)) \times \mathcal{O}(V(J)) \ni (f,g) \rightsquigarrow$$

$\exists!$ extensión a $V(I) \cup V(J)$