I: MÓDULOS NOETHERIANOS

RELACIONES DE ORDEN

Definición: Dar una relación en un conjunto X es dar una familia de parejas ordenadas $R \subseteq X \times X$, y diremos que $x, y \in X$ están relacionados si la pareja $(x,y) \in R$, en cuyo caso escribiremos xRy.

- Una relación se dice de equivalencia si es reflexiva, simétrica y transitiva.

Definición: Una relación R sobre un conjunto X se dice de orden si es

i) Reflexiva: xRx

ii) Antisimétrica: $xRy,\ yRx \Rightarrow x = y$

iii) Transitiva: $xRy,\ yRz \Rightarrow xRz$.

Al par (X, R) se le llama conjunto ordenado. Si solo se cumple i) y iii) se dice que es un preorden.

Definición: Una relación R sobre X se dice de orden estricto si

i) Asimétrica: $xRy \Rightarrow y \not R x$

ii) Transitiva

- Notar que un orden estricto no es un orden. En lo que sigue hablaremos de un orden (no estricto).
- En lo que sigue pondremos $\leq$ en lugar de R.

Definición: Dos elementos $x, y \in (X, \leq)$ se dicen comparables si $x \leq y$ ó $y \leq x$.

Si no se da ninguna de las dos se dice que x, y son no comparables.

Definición: Un orden $\leq$ en un cjto X se dice total si todos sus elementos son comparables, y se dice que $(X, \leq)$ es un cjto totalmente ordenado. Si no todos sus elemts son comparables, $\leq$ se dice orden parcial y al par $(X, \leq)$ cjto parcialmte ordenado.

Definición: Sea $(X, \leq)$ un cjto ordenado y $S \subseteq X$.

i) Un elemto $m \in S$ se dice maximal (en S) si $\forall m \neq x \in S$ $x \leq m$ ó no son comparables, ie, si $\nexists m \neq x \in S : m \leq x$.

ii) Un elemto $m \in S$ se dice minimal (en S) si $\forall m \neq x \in S$ $m \leq x$ ó no son comparables, ie, si $\nexists m \neq x \in S : x \leq x$.

Definición: Sea $(X, \leq)$ un cjto ordenado y $S \leq X$.

i) Un elemto $x \in X$ se dice cota superior de S si $s \leq x$ $\forall s \in S$.

ii) Un elemto $x \in X$ se dice cota inferior de S si $x \leq s$ $\forall s \in S$.

Llamaremos supremo de S a la menor de las cotas superiores, e ínfimo de S a la mayor de las cotas inferiores.

Proposición: Sea $(X, \leq)$ un conjunto parcialmte ordenado. Son equivalentes:

1) Condición de Cadena Ascendente: Toda cadena (suc. creciente) de elemtos de X estabiliza:
$\forall x_1 \leq x_2 \leq \ldots \ \exists n \in \mathbb{N} : x_n = x_{n+1} = x_{n+2} = \ldots$

2) Condición de Maximalidad: Todo subconjunto no vacío de X contiene algún elemto maximal.

Definición: Un conjunto bien ordenado es un conjunto ordenado $(X, \leq)$ en el que todo subconjunto no vacío tiene mínimo. Se dice que $\leq$ es un buen orden.

• Notar que conj bien ordenado $\Rightarrow$ conjunto totalmente ordenado.

Teorema: Los siguientes enunciados son equivalentes:

1) Axioma de elección: De toda familia de conjuntos no vacíos $\{X_i\}_{i\in I}$ es posible elegir un elemento de cada conjunto, ie, $\prod_{i\in I} X_i \neq \emptyset$.

2) Lema de Zorn: Si $(X, \leq)$ es un conjunto parcialmente ordenado no vacío en el que toda cadena (subconjunto totalmente ordenado) tiene una cota superior, entonces X tiene algún elemento maximal.

3) Principio del Buen Orden: Todo conjunto puede ser bien ordenado, ie, para cualquier conjunto existe una relación de orden que es un buen orden.

NOTA: $\underbrace{\text{C.C.a}}_{\text{toda cadena estabiliza}} \neq \underbrace{\text{Lema de Zorn}}_{\text{toda cadena tiene cota superior}}$.

Definición: Un retículo es un conjunto ordenado $(X, \leq)$ en el que todo par de elementos $x, y \in X$ tiene supremo, que denotaremos $x \vee y$; e ínfimo, que denotaremos $x \wedge y$.

• Todo conjunto totalmente ordenado es un retículo: $x \vee y = \max\{x, y\}$; $x \wedge y = \min\{x, y\}$.

• $(\{\text{sev de un EV}\}, \subseteq)$ es un retículo: $V_1 \vee V_2 = V_1 + V_2$; $V_1 \wedge V_2 = V_1 \cap V_2$.

Definición: Un *morfismo de retículos* es una aplicación entre retículos $f:(X,\preceq)\longrightarrow(X',\preceq')$ que verifica $x\preceq y \Rightarrow f(x)\preceq' f(y)$. Un morfismo de retículos f se dice *isomorfismo de retículos* si $\exists\, g:(X',\preceq')\longrightarrow(X,\preceq)$ morfismo de retículos tal que $g\circ f=Id_X$, $f\circ g=Id_{X'}$.

Proposición: Sea $f:(X,\preceq)\longrightarrow(X',\preceq')$ un morfismo de retículos.

$$f \text{ isomorfismo de retículos} \Longleftrightarrow \begin{cases} 1) & f \text{ biyectiva} \\ 2) & x\preceq y \Longleftrightarrow f(x)\preceq f(y), \quad \forall x,y\in X. \end{cases}$$

Definición: Un *anti-morfismo de retículos* es una aplicación entre retículos $f:(X,\preceq')\to(X',\preceq')$ tal que $x\preceq y \Rightarrow f(y)\preceq' f(x)$. Un morf. de ret. f se dice *anti-isomorfismo de retículos* si $\exists\, g:(X',\preceq')\longrightarrow(X,\preceq)$ anti-morf. de ret. tal que $g\circ f=Id_X$, $f\circ g=Id_{X'}$.

Proposición: Sea $f:(X,\preceq)\longrightarrow(X',\preceq')$ un anti-morfismo de retículos.

$$f \text{ anti-isomorfismo de retículos} \Longleftrightarrow \begin{cases} 1) & f \text{ biyectiva} \\ 2) & x\preceq y \Longleftrightarrow f(y)\preceq' f(x). \end{cases}$$

REPASO DE ANILLOS Y MÓDULOS

<u>Proposición</u>: Sea A un anillo íntegro.

1) $(a) = (b) \iff b = u \cdot a$, $u \in A^*$.

2) $A[x]$ íntegro

3) $(A[x])^* = A^*$.

• El mcd/mcm no siempre existe en anillos. <u>Sí en DIP.</u>

• $\mathbb{Z}$ y $K[x]$ son DIP

• $(0) \in \operatorname{Spec} A \iff A$ es íntegro → (e.g.: 0 no es primo pero en $\mathbb{Z}/4\mathbb{Z}$ pq $\bar{2} \cdot \bar{2} = \bar{0}$)

<u>Proposición</u> (Identidad de Bezout): Sea A DIP, y $d = \operatorname{mcd}(a,b)$. Entonces $\exists r, s \in A$ tal que $d = r \cdot a + s \cdot b$.

• ~~La~~ La identidad de Bezout no se cumple en todos los anillos. Arnde dice que <u>en DIP sí</u>. Igual la división con resto.

<u>Proposición</u> (Algoritmo de Euclides): Si $D = d \cdot c + r$, entonces

$$\operatorname{mcd}(D, d) = \operatorname{mcd}(d, r).$$

<u>Lema</u> (Euclides en DIP): Sea A un DIP, y $\underline{0 \neq a \in A}$. Son equivalentes:

1) a irreducible en A

2) (a) ideal maximal

3) (a) ideal primo

Por tanto, <u>**si A es DIP**</u>

$$\operatorname{Spec} A = \{0, (a)\}_{a \text{ irred}} \quad ; \quad \operatorname{Spec}_{max} A = \{(a)\}_{a \text{ irred}}.$$

Definición: Un dominio de factorización única (DFU) es un anillo íntegro en el que todo elemento es producto de irreducibles del anillo de modo único salvo orden e invertibles.

Proposición: DIP $\Rightarrow$ DFU.

- $\not\Leftarrow$: $(2, x)$ en $\mathbb{Z}[x]$, que es DFU, no es principal. $(x_1, \dots, x_n) \subseteq K[x_1, \dots x_n]$ tampoco.

Proposición: Sea A DFU, $0 \neq a \in A$.

$$a \text{ irreducible} \iff (a) \text{ ideal primo}$$

Por tanto, $\left\{\begin{matrix}\text{ideales} \\ \text{primos} \\ \text{principales}\end{matrix}\right\} = \{0, (a)\}_{a \text{ irred.}}$

Lema (Gauss DFU): Sea A DFU y $\Sigma := A_{A-0}$ su cuerpo de fracciones, y sea $p(x) \in A[x]$ primitivo (ie, no hay ningún elto propio de A que divide a todos sus coef.). Entonces

$$p(x) \text{ irreducible en } A[x] \iff p(x) \text{ irreducible en } \Sigma[x].$$

Teorema (Criterio Eisenstein-Nietsreosie): Sea $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in A[x]$. Si existe $p \in A$ irreducible tal que

1) p no divide a a_n (p no divide a a_0)
2) p divide a $a_{n-1}, \dots, a_0$ (p divide a $a_n, \dots, a_1$)
3) p^2 no divide a a_0 (p^2 no divide a a_n)

$\Rightarrow$ $p(x)$ es irreducible en $A[x]$ y $\Sigma[x]$.

Teorema (Gauss): A DFU $\Rightarrow A[X]$ DFU.

- $\mathbb{Z}[X_1, \dots, X_n]$, $K[X_1, \dots, X_n]$ DFU.

Definición: Sea $\{M_i\}_{i \in I}$ una familia de A-módulos. Su producto directo se denotará como $\prod_{i \in I} M_i$, mientras que llamaremos suma directa y denotaremos $\bigoplus_{i \in I} M_i$ al subgrupo de $\prod M_i$ formado por todos los elementos $(m_i)_{i \in I}$ que tengan todas las componentes nulas salvo finitas. Ambos son A-módulos con $a \cdot (m_i)_{i \in I} := (a m_i)_{i \in I}$.

- $\prod_{i \in I} M_i = \bigoplus_{i \in I} M_i$ si $\# I < \infty$.
- Si $M_i = M \ \forall i \in I$, $\prod_{i \in I} M_i \overset{NOT}{=} M^I$, $\bigoplus_{i \in I} M_i \overset{NOT}{=} M^{(I)}$. Si $\# I = n < \infty$ ambos coinciden y se denota M^n.

Definición: Sea $\{m_i\}_{i \in I}$ una familia de elementos de un A-módulo M. Dicha familia define un morfismo $\phi : A^{(I)} \longrightarrow M$, $\phi\left((a_i)_{i \in I}\right) := \sum_{i \in I} a_i m_i$. Se dice que los $\{m_i\}_{i \in I}$ forman un sistema de generadores de M si $M = \sum_{i \in I} A m_i = \langle m_1, m_2, \dots \rangle$, ie, si ϕ es epiyectivo. Se dice que los $\{m_i\}_{i \in I}$ son A-linealmente independientes si ϕ es inyectivo, y que son base de M si ϕ es isomorfismo, ie, cuando cada elemento de M descomponga, y de modo único, como CL con coef. en A de los $\{m_i\}_{i \in I}$.

Definición: Un A-módulo M se dice finito-generado o de tipo finito si admite algún sistema finito de generadores, ie, si $M = \langle m_1, \dots, m_r \rangle$. M se dice libre si admite alguna base, ie, si $M \simeq A^n$ para algún $n \in \mathbb{N}$.

Proposición: Todas las bases de un A-módulo libre tienen el mismo número de elementos.

Definición: Llamaremos rango de un A-módulo libre al número de elementos de cualquier base.

MÓDULOS Y ANILLOS NOETHERIANOS

Definición: Sea A un anillo. Se dice que un A-módulo M es noetheriano si el conjunto de sus ideales, ordenados por la inclusión, satisface la condición de cadena ascendente (o la de maximalidad).

Proposición: M noetheriano $\Longleftrightarrow$ todo submódulo es finito-generado.

Corolario: 1) M noeth $\Rightarrow$ M finito-generado
2) M no finito-generado $\Rightarrow$ M no noetheriano.

• Los grupos abelianos finitos (como $\mathbb{Z}$-módulos) y los K-EV de dim $< \infty$ son noeth.

Lema: 1) Submódulo de noeth. es noeth.
2) Cociente de noeth. es noeth.

• $M \xrightarrow{p} M'' \to 0$ suc. exacta $\Longleftrightarrow$ p epi $\Longleftrightarrow$ $M'' \left(= M/\operatorname{Ker} p\right)$ es un cociente de M

$0 \to M' \xrightarrow{i} M$ suc. exacta $\Longleftrightarrow$ i inyectiva $\Longleftrightarrow$ $M' \left(= i(M')\right)$ es un submódulo de M.

$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ suc. exacta $\Longleftrightarrow \left\{\begin{array}{l} p \text{ epi} \\ i \text{ iny.} \\ \operatorname{Im} i = \operatorname{Ker} p \end{array}\right\} \Rightarrow \underline{\underline{M'' = M/M'}}$

Proposición: Sea $0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ una suc. exacta.

M noetheriano $\Longleftrightarrow$ M', M'' noetherianos.

• $K[x_1, x_2, \dots]$ no es noeth : $(x_1, x_2, \dots)$ no es f.g.

Corolario: $M_1, \dots, M_r$ A-módulos noeth $\iff \bigoplus_{i=1}^{r} M_i$ noetherianos.

• Recordar que todo anillo A es un A-módulo, y submódulos de A $=$ ideales de A.

Definición: Un anillo A se dice noetheriano si lo es como A-módulo, i.e, si toda cadena de ideales estabiliza.

Corolario: A noetheriano $\iff$ todos sus ideales son finito-generados.

• A DIP $\Rightarrow$ A noeth.

Teorema: Todo anillo no nulo contiene ideales maximales.

Corolario: Todo ideal $\neq A$ está contenido en algún ideal maximal , i.e,

Corolario: $a \notin A^* \iff$ a está contenido en algún ideal maximal

$$\bigcup_{\mathfrak{m} \in \mathrm{Spec}_{max} A} \mathfrak{m} = A - A^*$$

• Se ha visto que si A anillo, M noeth $\Rightarrow$ M fg . $\not\Leftarrow$ en general. Pero sí si A noeth :

Proposición: Sea A noetheriano, y M un A-módulo.

M noetheriano $\iff$ M finito-generado.

• K, $\mathbb{Z}$ son anillos noeth.

• A anillo noeth $\Rightarrow A/_I$ noeth (I ideal). La dem es análoga a la de los módulos, pero con ideales.

• En Alg Conmt. vimos que

<u>Proposición</u>: A DIP $\Rightarrow$ todo submódulo de un A-módulo fg es fg.

La equivalencia de antes dice que también si A es noeth.

todo submódulo es fg $\Leftrightarrow$ M noeth $\overset{A \text{ noeth}}{\Longleftrightarrow}$ M fg.

Por eso todo SEV = submódulo de un K-EV (K-módulo, K noeth) de dim < ∞

son de dim < ∞.

<u>Teorema</u> (de la base de Hilbert): A noetheriano $\Rightarrow$ A[x] noetheriano.

<u>Corolario</u>: A noeth. $\Rightarrow$ $A[x_1, \dots, x_n]$ noeth.

<u>BASES DE GRÖBNER</u>

<u>Definición</u>: Llamaremos <u>monomio</u> en $K[x_1 \dots x_n]$ a $x_1^{\alpha_1} \cdots x_n^{\alpha_n} \overset{\text{NOT}}{=} \mathbf{x}^{\alpha}$, $\alpha = (\alpha_1 \dots \alpha_n) \in \mathbb{N}^n$,

y diremos que el <u>grado</u> total de $\mathbf{x}$ es $|\alpha| := \alpha_1 + \dots + \alpha_n$.

<u>Definición</u>: Un <u>orden monomial</u> es una relación de orden total $\leq$ sobre $\mathbb{N}^n$ (equivalentemente, sobre el conjunto de los monomios) que cumple

i) $\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma$, $\forall \alpha, \beta, \gamma \in \mathbb{N}^n$

ii) $\mathbf{0} \leq \alpha$ $\forall \alpha \in \mathbb{N}^n - \mathbf{0}$.

• <u>Orden lexicográfico</u>: Se elige un "alfabeto": $x > y > z > \dots$, y se ordenan por el grado de la variable "más importante". En caso de empate se pasa a la sig. var.: $x^2y > xy^5$.

• <u>Orden lexicográfico graduado</u>: Se ordena por grado total. En caso de empate se usa el lexicográfico. $xy^5 > x^2y$, $x^3y^2 > x^2y^3$.

• Notar que dar un orden en $K[x_1, \dots, x_n]$ es dar un orden monomial, i.e, un orden en $\mathbb{N}^n$.

Definición: Sea $(K[x_1, \dots, x_n], <)$ un orden monomial, y consideremos $f = \sum_{\alpha \in \Lambda} \lambda_\alpha X^\alpha$, donde $\Lambda \subseteq \mathbb{N}^n$. Sea $\beta := \max\{\alpha \in \Lambda\}$. Así que $f = \lambda_\beta X^\beta + \dots$. A dicho $\lambda_\beta X^\beta$ ($= LT(f)$) se le llama término líder o principal, a λ_β ($= LC(f)$) coeficiente líder o principal y a X^β ($= LM(f)$) monomio líder o principal. A β se le llama multigrado de f, $\beta = \operatorname{mgr} f$.

• ¿Cómo se divide en $K[x,y]$? f se puede dividir entre 2 pol f_1, f_2:

Se divide primero f entre f_1 según el orden monomial dado. Cuando ya no se puede se pasa a f_2.

$$\begin{array}{c|c|c} f & f_1 & f_2 \\ \hline & c_1(x) & c_2(x) \\ r(x) & & \end{array}$$

En general obtendremos $f = f_1 \cdot c_1 + f_2 \cdot c_2 + r$,

y si $r(x) = 0 \implies f \in (f_1, f_2)$.

NOTA: No hay un teorema de unicidad de cociente y resto ... ¡Porque no son únicos!

Teorema (Algoritmo de División): Dados $f, f_1, \dots, f_s \in (K[x_1, \dots, x_n]$, orden monomial$)$ existen $g_1, \dots, g_s, r \in K[x_1, \dots, x_n]$: $f = \sum_{i=1}^{s} f_i g_i + r$ que cumple:

1) $r \neq 0 \implies$ ninguno de los términos de r es divisible por ninguno de los términos líderes de $f_1, \dots, f_s$.

2) $\operatorname{mgr} f \geq \operatorname{mgr}(f_i g_i)$

¿Cómo saber si un elemento está o no en el ideal que generan unos elementos? Se trata de buscar "buenos generadores":

Definición: Sea $\mathfrak{a} \subseteq K[x_1,\dots,x_n]$. Una **base de Gröbner** de $\mathfrak{a}$ es una colección $G = \{g_1,\dots,g_s\} \subseteq \mathfrak{a}$ que cumple

i) $\mathfrak{a} = (g_1,\dots,g_s)$

ii) $f \in \mathfrak{a} \iff \overline{f}^{G} = 0$ ($\overline{f}^{G}$ es el resto de dividir f entre $g_1,\dots,g_s$)

iii) $\overline{f}^{G}$ no depende del orden de $g_1,\dots,g_s$.

Tener una base de Gröbner es lo mejor que podés tener: sabemos automáticamente si un pol está o no.

¿Cómo obtenerla?

Definición: Sean $f, g \in K[x_1,\dots,x_n]$ no nulos. Llamaremos **S-polinomio** de f y g a

$$S(f,g) := \frac{\operatorname{mcm}(LM(f), LM(g))}{LT(f)} \cdot f - \frac{\operatorname{mcm}(LM(f), LM(g))}{LT(g)} \cdot g$$

. Con esto lo que hacemos es un pol. en el que no aparecen los términos líderes de f y g.

Teorema (Criterio de Buchberger): Sean $f_1,\dots,f_s \in K[x_1,\dots,x_n]$, y consideremos $\mathfrak{a} = (f_1,\dots,f_r)$.

$$G = \{f_1,\dots,f_r\} \text{ es base de Gröbner de } \mathfrak{a} \iff \overline{S(f_i,f_j)}^{G} = 0 \quad \forall i,j.$$

Proposición: Sea ($K[x_1,\dots,x_r,x_{r+1},\dots,x_n]$, orden lex.), G base de Gröbner de un ideal $\mathfrak{a}$. Entonces $G \cap K[x_{r+1},\dots,x_n] \equiv$ polinomios de G que solo dependen de $x_{r+1},\dots,x_n$ es base de Gröbner del ideal $\mathfrak{a} \cap K[x_{r+1},\dots,x_n]$.

II: CONJUNTOS ALGEBRAICOS

• Se trata de estudiar los sistemas de ecuaciones $\left.\begin{array}{l} p_1(x_1 \dots x_n) = 0 \\ \vdots \\ p_r(x_1, \dots x_n) = 0 \end{array}\right\}$. Dichas igualdades,

como polinomios, no son ciertas en $K[x_1, \dots, x_n]$, pero sí en $\dfrac{K[x_1 \dots x_n]}{(p_1, \dots p_r)}$.

Cualquier suma, producto, ... que hagas entre los p_i estará dentro del ideal.

Definición: Dos sistemas de ecuaciones $\left.\begin{array}{l} p_1(x_1 \dots x_n) = 0 \\ \vdots \\ p_r(x_1 \dots x_n) = 0 \end{array}\right\}$, $\left.\begin{array}{l} q_1(x_1 \dots x_n) = 0 \\ \vdots \\ q_s(x_1, \dots x_n) = 0 \end{array}\right\}$; $p_i, q_j \in A[x_1 \dots x_n]$

se dicen equivalentes si tienen las mismas soluciones.

• Veremos que dos sistemas son equivalentes $\iff (p_1, \dots p_r) = (q_1, \dots, q_s)$.

• En particular si dos sistemas son equivalentes, tienen las mismas soluciones. (Lo veremos)

• En lo que sigue se tratará de relacionar las soluciones del sistema con los ideales de $K[x_1 \dots x_n]$.

Definición: Sea $f \in K[x_1, \dots, x_n]$. Llamaremos función regular sobre K^n a

$$\begin{aligned} K^n &\longrightarrow K \\ (a_1 \dots a_n) &\longmapsto f(a_1 \dots a_n) \end{aligned},$$

es decir, es f entendida como función.

• ¿Puede ocurrir que dos polinomios distintos definan la misma función regular? Sí: 0 y $x^2 - x$ en $\mathbb{Z}/2\mathbb{Z}[x]$.

Pero...

Proposición: $\# K = \infty \iff$ El único polinomio que define la función cero en K^n es el pol. cero.

Corolario: Si $\# K = \infty$, entonces dos pol. definen la misma función regular $\iff$ son iguales, i.e. cada función regular viene definida por un único polinomio.

• K alg. cerrado $\Rightarrow \# K = \infty$.

Definición: Si $\#K=\infty$, se dice que $K[x_1,\dots,x_n]$ es el anillo de funciones regulares ó algebraicas sobre K^n; o el anillo de coordenadas de K^n.

Definición: Sea $f\in K[x_1,\dots,x_n]$. Llamaremos ceros de f en K^n a

$$\mathcal{V}(f) := \{(a_1,\dots,a_n)\in K^n : f(a_1,\dots,a_n)=0\}.$$

- La prop. dice que , $\#K=\infty$, entonces $\mathcal{V}(f)=K^n \iff f=0$.
- Es claro que si $f=33 \Rightarrow \mathcal{V}(f)=\emptyset$. ¿Y el inverso? No en general: $x^2+1\in\mathbb{R}[x]$ no tiene raíces. ¿Cuándo sí?

Proposición: Si K es algebraicamente cerrado, et. $\mathcal{V}(f)=\emptyset \iff f=\lambda\in K^*$.

Definición: Sea $S\subseteq K[x_1,\dots,x_n]$. Se llama ceros de S a

$$\mathcal{V}(S) := \bigcap_{f\in S}\mathcal{V}(f) = \{(a_1,\dots,a_n)\in K^n : f(a_1,\dots,a_n)=0 \ \forall f\in S\} = \left.\begin{matrix} f_1=0\\ f_2=0\\ \vdots\end{matrix}\right\}$$

Definición: Un conjunto algebraico afín es un subconjunto $V\subseteq K^n$ que son los ceros de algún subconjunto $S\subseteq K[x_1,\dots,x_n]$, i.e., $V=\mathcal{V}(S)$.

- $S\subseteq S' \Rightarrow \mathcal{V}(S)\supseteq\mathcal{V}(S')$.

Lema: Todo conjunto algebraico son los ceros de un ideal. Más aún, son los ceros de un número finito de polinomios. En particular, si $\mathfrak{a}\subseteq K[x_1,\dots,x_n]$ es ideal generado por $S\subseteq K[x_1,\dots,x_n]$,

1) $\mathcal{V}(S)=\mathcal{V}(\mathfrak{a})$

2) $\exists f_1,\dots,f_m : \mathcal{V}(S)=\mathcal{V}(\mathfrak{a})=\mathcal{V}(\{f_1,\dots,f_m\})$, donde $\mathfrak{a}=(f_1,\dots,f_m)$.

• Por tanto podríamos dar la sgte definición:

<u>Definición</u> (Alternativa): Un <u>conjunto algebraico afín</u> es un subconjunto $V \subseteq K^n$ que son los ceros de un número finito de polinomios, ie, son las soluciones de un sistema de ecuaciones polinómicas $\left.\begin{array}{l} p_1(x_1,\dots,x_n)=0\\ \vdots \\ p_r(x_1,\dots,x_n)=0\end{array}\right\}$

• $\mathcal{V}(\{0\}) = K^n$; $\mathcal{V}(\{3\}) = \emptyset$.

• Los subconjuntos algebraicos de la recta K son $\emptyset$, K y los subconjuntos finitos.

• $\mathcal{V}(f\cdot g) = \mathcal{V}(f) \cup \mathcal{V}(g)$.

<u>Teorema</u>: Sea $a=(a_1,\dots,a_n)\in K^n$, y consideremos $\mathfrak{m}_a := \{p(x_1,\dots,x_n)\in K[x_1,\dots,x_n] : p(a_1,\dots,a_n)=0\}$.

Entonces $\mathfrak{m}_a$ es un ideal maximal y en particular es

$$\mathfrak{m}_a = (x_1-a_1,\dots,x_n-a_n).$$

• $\mathcal{V}(\mathfrak{m}_a) = \{(a_1,\dots,a_n)\}$.

<u>Definición</u>: Llamamos <u>hipersuperficie</u> a los ceros de un polinomio.

• La def alternativa dice que todo conj. algebraico es intersección de un nº finito de hipersuperficies.

<u>Proposición</u>: Si $f,g\in K[X_1,X_2]$ no tienen factores irreducibles comunes, $\Rightarrow \mathcal{V}(f,g)$ es finito ó vacío.

<u>IMPORTANTE</u>: La propiedad 2) del lema es muy importante pues dice que, si $I=(f_1,\dots,f_r)=(g_1,\dots,g_s)$, entonces los sistemas

$$\left.\begin{array}{l} f_1=0\\ \vdots \\ f_r=0\end{array}\right\} \quad , \quad \left.\begin{array}{l} g_1=0\\ \vdots \\ g_s=0\end{array}\right\}$$

tienen las mismas soluciones (pues son el mismo conj. algebraico)

• ¿Se da el recíproco? ¿Si ambos sistemas dan los mismos ptos (ie, conj. alg.) estos dos polinomios dan los mismos ideales? Ya veremos.

Proposición (Propiedades):

1) $\emptyset, K^n$ son conjuntos algebraicos (en particular $\emptyset = \mathcal{V}(\{1\})$, $K^n = \mathcal{V}(\{0\})$)

2) $\bigcap_{i \in I} \mathcal{V}(\mathfrak{a}_i)$ es un conjunto algebraico (en particular, $\boxed{\bigcap_{i \in I} \mathcal{V}(\mathfrak{a}_i) = \mathcal{V}(\sum_{i \in I} \mathfrak{a}_i)}$)

3) $\bigcup_{i=1}^{n} \mathcal{V}(\mathfrak{a}_i)$ es un conjunto algebraico (en particular, $\boxed{\bigcup_{i=1}^{n} \mathcal{V}(\mathfrak{a}_i) = \mathcal{V}(\bigcap_{i=1}^{n} \mathfrak{a}_i)}$)

- Estas son justamente las propiedades que debe cumplir los cerrados de una topología:

Definición: Se llama topología de Zariski en K^n a la que tiene como cerrados a los conjuntos algebraicos.

- Los cerrados $\mathcal{V}(f)$ forman una base de cerrados: son los cerrados básicos, pues $\boxed{\begin{array}{c}\mathcal{V}(f) \cap \mathcal{V}(g) \\ \Downarrow \\ \mathcal{V}(f, g)\end{array}}$
- Los abiertos $D(f) = K^n - \mathcal{V}(f)$ son una base de abiertos. Son abiertos básicos.
- Los puntos son cerrados de la topología: la top Zariski es T_1. En general no es Hausdorff $= T_2$.
- La top Zariski en K es la cofinita.
- Los cerrados en K^2 son: $\emptyset, K^2$, ptos, curvas $f(x,y)=0$ y uniones finitas de ptos y curvas.

• Ya se ha visto que cada polinomio $f \in K[x_1,\dots,x_n]$ define una función regular $(a_1,\dots,a_n) \in K^n \longrightarrow f(a_1,\dots,a_n) \in K$.

De la misma manera si tenemos m polinomios $h_1,\dots,h_m \in K[x_1,\dots,x_n]$ definimos una aplicación

$$K^n \xrightarrow{h^*=(h_1,\dots,h_m)} K^m$$
$$(a_1,\dots,a_n) \longmapsto (h_1(a_1,\dots,a_n),\dots,h_m(a_1,\dots,a_n))$$

<u>Definición</u>: Llamaremos a dichas aplicaciones $h^*: K^n \longrightarrow K^m$ <u>aplicaciones regulares</u>.

• Dar una apl. regular es por tanto dar m polinomios $h_1,\dots,h_m \in K[x_1,\dots,x_n]$, $h^*=(h_1,\dots,h_m)$.

Esto es equivalente también a dar un morfismo de K-álgebras

$$K[y_1,\dots,y_m] \xrightarrow{h} K[x_1,\dots,x_n]$$
$$y_i \longmapsto h_i(x_1,\dots,x_n)$$

Si $\#K=\infty$, sabemos que cada función regular viene de un solo polinomio, i.e.

$$\mathrm{Hom}_{K\text{-alg}}(K[y_1,\dots,y_m], K[x_1,\dots,x_n]) \equiv \left\{ \begin{array}{c} \text{apl. regulares} \\ K^n \longrightarrow K^m \end{array} \right\}$$
$$h \longleftrightarrow h^*=(h_1,\dots,h_m)$$
$$(h(y_i)=h_i(x_1,\dots,x_n))$$

Por tanto,

dar un morfismo de K-álgebras $K[y_1,\dots,y_m] \longrightarrow K[x_1,\dots,x_n]$ $\equiv$ dar una aplicación regular $K^n \xrightarrow{h^*} K^m$ $\equiv$ dar m polinomios $h_1,\dots,h_m \in K[x_1,\dots,x_n]$.

<u>Proposición</u>: Las aplicaciones regulares $h^*: K^n \longrightarrow K^m$ son continuas para la topología de Zariski.

CONJUNTOS ALGEBRAICOS E IDEALES

Teorema (de los ceros de Hilbert, forma débil): Sea K un cuerpo algebraicamente cerrado:

VERSIÓN 1): Todo ideal maximal de $K[x_1, \dots x_n]$ es de la forma $(x_1 - a_1, \dots, x_n - a_n)$ para algún $(a_1, \dots a_n) \in K^n$, i.e.

$$\mathrm{Spec}_{max} K[x_1, \dots, x_n] = K^n$$

$$\mathfrak{m}_{(a_1, \dots, a_n)} \longleftrightarrow (a_1, \dots a_n).$$

VERSIÓN 2): Sea $\mathfrak{a} \subseteq K[x_1, \dots x_n]$ un ideal.

$$\mathcal{V}(\mathfrak{a}) = \emptyset \iff \mathfrak{a} = K[x_1, \dots x_n]$$

VERSIÓN 3):

Un sistema $\left.\begin{array}{l} g_1(x_1, \dots, x_n) = 0 \\ \vdots \\ g_r(x_1, \dots x_n) = 0 \end{array}\right\}$ es incompatible $\iff (g_1, \dots g_r) = K[x_1, \dots x_n]$

- NO es cierto si K no alg cerrado: $(x^2+1) \subseteq \mathbb{R}[x]$ es max pero no tiene raíces[1], es decir, $\mathcal{V}(\mathfrak{a}) = \emptyset$ pero $(x^2+1) \neq \mathbb{R}[x]$.

- Si $p \in k^n$, ya vimos que las funciones que se anulaban en p forman un ideal, maximal: $\mathfrak{m}_p$. Vamos a generalizar:

Definición: Sea $F \subseteq K^n$. Llamaremos ideal de F a

$$\mathcal{I}(F) := \{ f \in K[x_1, \dots x_n] : \underset{(f(p) = 0 \ \forall p \in F)}{f(F) = 0} \} = \bigcap_{p \in F} \mathfrak{m}_p$$

$\uparrow$ $\mathcal{I}(F)$ es un ideal.

• $\mathfrak{a} \subseteq \mathcal{I}(\mathcal{V}(\mathfrak{a}))$; $F \subseteq \mathcal{V}(\mathcal{I}(F))$ siempre. Pero las contenciones en general no son igualdades $\forall \mathfrak{a}$ ideal, $\forall F$ subconjunto de k^n.

Proposición:

1) $F \subseteq G \Rightarrow \mathcal{I}(F) \supseteq \mathcal{I}(G)$

2) $\mathcal{I}(\emptyset) = k[x_1, \dots x_n]$; $\mathcal{I}(k^n) = (0)$. (si $\# k = \infty$).

3) $\mathcal{I}\left(\bigcup_{i \in I} W_i\right) = \bigcap_{i \in I} \mathcal{I}(W_i)$

4) $\sum_{i=1}^{n} \mathcal{I}(W_i) \subsetneq \bigcap_{i=1}^{n} \mathcal{I}(W_i)$.

• En principio tenemos una aplicación

$$\begin{array}{ccc} \{\text{ideales de } k[x_1, \dots x_n]\} & & \{\text{subconjuntos de } k^n\} \\ \mathfrak{a} & \longmapsto & \mathcal{V}(\mathfrak{a}) \quad (*) \\ \mathcal{I}(F) & \longleftarrow\!\shortmid & F \end{array}$$

¿Podemos restringir los conjuntos para que nos quede una biyección?

Proposición: Sea $F \subseteq k^n$. La adherencia de F, i.e., el menor cerrado que lo contiene, con la topología de Zariski, es $\overline{F} = \mathcal{V}(\mathcal{I}(F))$.

Corolario: $W = \mathcal{V}(\mathcal{I}(W))$ si W es un conjunto algebraico.

Corolario: $\mathcal{V}(\mathfrak{a}) = \mathcal{V}(\mathfrak{b}) \iff \mathcal{I}(\mathcal{V}(\mathfrak{a})) = \mathcal{I}(\mathcal{V}(\mathfrak{b}))$.

• Esto dice que si en $(*)$ restringimos a $\{\text{conjuntos algebraicos de } k^n\} \subseteq \{\text{subconjuntos de } k^n\}$ entonces tenemos una vuelta: $F \longmapsto \mathcal{I}(F) \longmapsto \mathcal{V}(\mathcal{I}(F)) \overset{F \text{ algebraico}}{=} F$.

• ¿Podemos restringir $\{\text{ideales de } k[x_1, \dots x_n]\}$ para tener la biyección?

<u>Definición</u>: Sea $\mathfrak{a}$ un ideal de un anillo A. Llamaremos <u>radical de $\mathfrak{a}$</u> a

$$\text{rad}\, \mathfrak{a} = \sqrt{\mathfrak{a}} := \{a \in A : a^n \in \mathfrak{a} \text{ para algún } n \in \mathbb{N}\} ,$$

que es un ideal de A.

- <u>rad A</u> $= \{a \in A : a^n = 0 \text{ para algún } n \in \mathbb{N}\} =$ <u>rad(0)</u>.
- $\text{rad}\, \mathfrak{a} = \text{rad}\, A/\mathfrak{a}$ $\quad (a^n \in \mathfrak{a} \Leftrightarrow \overline{a}^n = 0)$.

<u>Definición</u>: Un ideal $\mathfrak{a}$ se dice <u>radical</u> si $\mathfrak{a} = \text{rad}\, \mathfrak{a}$.

<u>Lema</u>: Todo ideal primo es radical: $\mathfrak{p} = \text{rad}\, \mathfrak{p}$.

<u>Lema</u>: Sea $F \subseteq k^n$. Entonces $\mathcal{I}(F)$ es un ideal radical.

<u>Proposición</u> (Propiedades):

1) $\mathfrak{a} \subseteq \text{rad}\, \mathfrak{a}$
2) $A = \text{rad}\, \mathfrak{a} \iff \mathfrak{a} = A$.
3) $\text{rad}\, \mathfrak{a}$ es un ideal radical
4) $\text{rad}\, \mathfrak{a} \subseteq \mathcal{I}(\mathcal{V}(\mathfrak{a}))$, si $\mathfrak{a} \subseteq k[x_1 \dots x_n]$.
5) $\text{rad}\,(p_1^{n_1} \cdots p_r^{n_r}) = (p_1 \cdots p_r)$.

<u>Teorema</u>: Sea k alg. cerrado, y $A = k[x_1 \dots x_n]$, $\mathfrak{a} = (f_1, \dots, f_r)$ ideal de A, $h \in A$.
Son equivalentes:

1) $h \in \text{rad}\, \mathfrak{a}$
2) $h \in \mathcal{I}(\mathcal{V}(\mathfrak{a}))$
3) El sistema $\left.\begin{array}{l} f_1 = 0 \\ \vdots \\ f_r = 0 \\ 1 - hy = 0 \end{array}\right\}$ es incompatible
4) $\mathfrak{a} + (1 - hy) = A[y]$

• La equivalencia 1) $\Longleftrightarrow$ 4) se puede generalizar a A anillo íntegro y tiene sentido:

Teorema (Truco de Rabinovich): Sea $\mathfrak{a} \subseteq A$ ideal de un anillo íntegro.

$$h \in \operatorname{rad} \mathfrak{a} \Longleftrightarrow (\mathfrak{a}, 1-hy) = A[y]$$

• La equivalencia 1) $\Longleftrightarrow$ 2) también:

Teorema (de los Ceros de Hilbert, forma fuerte): Sea $\mathfrak{a} \subseteq K[x_1, \ldots, x_n]$ ideal.

$$\mathcal{I}(\mathcal{V}(\mathfrak{a})) = \operatorname{rad} \mathfrak{a} \quad ,$$

y por tanto $\mathcal{I}(\mathcal{V}(\mathfrak{a})) = \mathfrak{a}$ si $\mathfrak{a}$ es radical.

Lema: Sea $\mathfrak{a}$ un ideal de $K[x_1, \ldots, x_n]$, K alg. cerr. $\displaystyle \mathcal{I}(\mathcal{V}(\mathfrak{a})) = \bigcap_{\substack{\mathfrak{a} \subseteq \mathfrak{m} \\ \mathfrak{m} \text{ maximal}}} \mathfrak{m}$.

Corolario: Si K alg. cerrado, $\displaystyle \operatorname{rad} \mathfrak{a} = \bigcap_{\substack{\mathfrak{a} \subseteq \mathfrak{m} \\ \mathfrak{m} \text{ maximal}}} \mathfrak{m}$.

• Por tanto, ya hemos dado con el subconjunto de {ideales de $K[x_1, \ldots, x_n]$} que teníamos que elegir para tener biyección:

Teorema: Sea K un cuerpo alg. cerrado. Entonces tenemos la correspondencia biunívoca

$$\left\{ \begin{array}{c} \text{ideales radicales} \\ \text{de } K[x_1, \ldots, x_n] \end{array} \right\} = \left\{ \begin{array}{c} \text{subconjuntos} \\ \text{algebraicos} \\ \text{de } K^n \end{array} \right\}$$

$$\mathfrak{a} \longmapsto \mathcal{V}(\mathfrak{a})$$

$$\mathcal{I}(F) \longleftarrow\!\!\shortmid F$$

Definición: Un conjunto algebraico ($\neq \emptyset$) se dice irreducible si no es unión de dos subconjuntos algebraicos propios. ($\neq$ él mismo y el $\emptyset$).

- $\#K = \infty \Rightarrow K$ es irreducible.

Proposición: Sea W conjunto algebraico de K^n.

$$W \text{ irreducible} \Longleftrightarrow \mathcal{I}(W) \text{ es primo}.$$

- ¡Esto dice que puedes dar una correspondencia más exacta aún.

Teorema: Sea K un cuerpo alg cerrado. Se tiene la correspondencia.

$$\operatorname{Spec} K[x_1, \ldots, x_n] \;=\!=\!=\; \left\{ \begin{array}{c} \text{subconjuntos algebraicos} \\ \text{irreducibles de } K[x_1, \ldots x_n] \end{array} \right\}$$

$$\mathfrak{p} \longmapsto \mathcal{V}(\mathfrak{p})$$

$$\mathcal{I}(F) \longleftarrow F$$

- Esto dice que K^n es irreducible, pues $K^n = \mathcal{V}(0)$.

- ¿Qué pasa si K no es alg. cerrado? No tenemos Th Hilbert, así que no todo $\mathfrak{p}$ ideal max será $\mathfrak{m}_{(a_1, \ldots a_n)}$ en $K[x_1, \ldots x_n]$. Sin embargo sí hay una correspondencia.

Teorema: Sea K cuerpo (no nec. alg. cerrado), y consideremos $K[x_1, \ldots, x_n]$.

$$\mathfrak{m} \text{ es un pto racional} \Longleftrightarrow \mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n) \text{ para algún } (a_1, \ldots a_n) \in K.$$

ie,

$$\left\{ \begin{array}{c} \text{ptos racionales} \\ \text{de } K[x_1, \ldots x_n] \end{array} \right\} \;=\!=\!=\; K^n$$

$$\mathfrak{m}_{(a_1, \ldots a_n)} \longleftrightarrow (a_1, \ldots a_n)$$

ANILLOS DE COORDENADAS

• Sea $V \subseteq K^n$ un conjunto algebraico.

Definición: Una función regular sobre V es la restricción de una función regular sobre K^n a V, ie $f = f_{|V} : V \subseteq K^n \longrightarrow K$ (def. por un pol.).

• $f, g \in K[x_1 \ldots x_n]$ definen la misma func. regular sobre $V \Longleftrightarrow f(p) = g(p) \; \forall p \in V \Leftrightarrow f - g \in \mathcal{I}(V)$.

Por tanto cada func. regular en V estará definida por una única func. en $K[x_1 \ldots x_n] / \mathcal{I}(V)$ (donde $\bar{f} = \bar{g}$).

Definición: Se llama anillo de coordenadas de V a $K[V] := K[x_1 \ldots x_n] / \mathcal{I}(V)$.

• $K[V]$ es una K-algebra finita reducida.

• Es conocido que la proyección π de paso a cociente $\pi : A \longrightarrow A/I$ da la siguiente

$$\left\{ \begin{array}{c} \text{ideales de} \\ A/I \end{array} \right\} \quad = \quad \left\{ \begin{array}{c} \text{ideales de } A \\ \text{que contienen a } I \end{array} \right\}$$

$$\begin{array}{ccc}
\pi(\mathfrak{a}) & \longleftarrow & \mathfrak{a} \\
\bar{\mathfrak{a}} & \longmapsto & \pi^{-1}(\mathfrak{a}) \supset I . \\
\text{primo} & \Longleftrightarrow & \text{primo} \\
\text{maximal} & \Longleftrightarrow & \text{maximal} \\
\text{radical} & \Longleftrightarrow & \text{radical} .
\end{array}$$

¿Qué son los conjuntos algebraicos en V? Vienen definidos por ~~los~~ $K[V]$:

Definición: Sea $\mathfrak{a}' \subseteq K[V]$ ideal. Se llama conjunto algebraico de V a

$$\mathcal{V}(\mathfrak{a}') := \{ p \in V : f(p) = 0 \quad \forall f \in \mathfrak{a}' \}.$$

• En este punto podemos considerar dos topologías: la de subespacio inducida por la Zariski en K^n, y la de los conjuntos algebraicos de V (dada por funciones de $K[V]$).

<u>Proposición</u>: Ambas topologías sobre V <u>coinciden</u>.

<u>Teorema</u>: Sea K alg. cerrado. Se tiene la biyección

$$\left\{\begin{array}{c}\text{ideales radicales}\\ \text{de } K[V]\end{array}\right\} \;=\!=\; \left\{\text{cerrados de } V\right\}$$

$$\begin{array}{ccc}
\pi(\mathcal{I}(F)) & \longleftarrow\!\shortmid & F \\
\mathfrak{a} & \longmapsto & \mathbb{V}(\pi^{-1}(\mathfrak{a})) \\
\mathfrak{m} \text{ maximal} & \longleftrightarrow & \text{ptos} \\
\text{primo} & \longleftrightarrow & \text{irreducible}
\end{array}$$

<u>Definición</u>: Una <u>aplicación regular</u> entre $V \subseteq K^n$ y $W \subseteq K^m$ conj. alg. es una aplicación dada por polinomios $h^* = (h_1, \dots h_m) : V \subseteq K^n \longrightarrow W \subseteq K^m$.

• Dichas aplicaciones regulares las podemos pensar como la restricción a V de una aplic. regular $h^*: K^n \longrightarrow K^m$, y que $h^*(V) \subseteq W$. Pero ya vimos que cada regular $K^n \to K^m$ se corresponde con un morfismo de K-álgebras $K[y_1, \dots y_m] \xrightarrow{h} K[x_1, \dots x_n]$. ¿Cómo se traduce la condición $h^*(V) \subseteq W$ en la h?

<u>Lema</u>: Si $h^*(V) \subseteq W$ como antes $\Rightarrow h(\mathcal{I}(W)) \subseteq \mathcal{I}(V)$.

• Por tanto hace conmutar el diagrama

$$\begin{tikzcd}
K[y_1, \dots y_m] \arrow[r, "h"] \arrow[d, "\pi"] \arrow[dr, "\pi \circ h"] & K[x_1, \dots x_n] \arrow[d, "\pi"] \\
K[y_1, \dots y_m]/\mathcal{I}(W) \arrow[r, dashed, "\exists \bar{h} \text{ (PUAC)}"] \arrow[d, equal] & K[x_1, \dots x_n]/\mathcal{I}(V) \arrow[d, equal] \\
K[W] \arrow[r, "\exists \bar{h} \text{ morf. de } K\text{-alg.}"] & K[V]
\end{tikzcd}$$

• Lo anterior se resume en lo siguiente (análogo al caso $K^n \to K^m$; $K[y_1..y_m] \to K[x_1..x_n]$).

Teorema: Si $V \subseteq K^n$, $W \subseteq K^m$ son conj. algebraicos, tenemos la biyección

$$\mathrm{Hom}_{K\text{-alg}}(K[W], K[V]) \Longleftrightarrow \left\{ \begin{array}{l} \text{aplicaciones regulares} \\ h^*: V \longrightarrow W \end{array} \right\}.$$

Definición: Una aplicación regular $h^*: V \longrightarrow W$ se dice isomorfismo de conjuntos algebraicos si $\exists g^*: W \longrightarrow V$ aplicación regular tal que $g^* \circ h^* = Id_V$; $h^* \circ g^* = Id_W$.

Lema: $(h_2 \circ h_1)^* = h_1^* \circ h_2^*$.

Proposición: $h^*: V \longrightarrow W$ isomorfismo de conjuntos algebraicos $\Longleftrightarrow$ $h: K[W] \longrightarrow K[V]$ es isomorfismo de K-algebras.

Proposición: Sea $h^*: V \longrightarrow W$ la apl. regular definida por $h: K[W] \longrightarrow K[V]$.

1) $h(g) = g \circ h^* \quad \forall g \in K[W]$

2) $h^*(p) = q \Longleftrightarrow \mathfrak{M}_q = h^{-1}(\mathfrak{M}_p)$, $\quad p \in V$, $q \in W$.

Corolario: Sea $h^*: V \to W$ una aplicación entre conj. alg. $V \subseteq K^n$, $W \subseteq K^m$.

$$h^* \text{ aplicación regular} \Longleftrightarrow g \circ h^* \in K[V] \quad \forall g \in K[W].$$

Corolario: Toda aplicación regular $h^*: V \longrightarrow W$ entre conj. alg. es continua con las top. de Zariski.

<u>Proposición</u>: $f, g \in K[x_1 \dots x_n]$; f, g primos entre sí $\Rightarrow V(f,g)$ vacío ó finito

<u>Corolario</u>: f irreducible, $V(f)$ infinito $\Rightarrow I(V(f)) = (f)$.

<u>Proposición</u>: $\mathfrak{a}$ radical $\Longleftrightarrow A/\mathfrak{a}$ reducido.

III: LOCALIZACIÓN

<u>Definición</u>: Un anillo A se dice <u>local</u> si tiene un único ideal maximal.

- $\mathbb{Z}/n\mathbb{Z}$ local $\iff n = p^k$, p primo
- $K[x]/(p(x))$ local $\iff p(x) = r(x)^k$, $r(x)$ irreducible.

<u>Proposición</u>: Sea A un anillo y $\mathfrak{a} \neq A$ un ideal.

$$A \text{ es local de maximal } \mathfrak{a} \iff A^* = A - \mathfrak{a}.$$

<u>Lema</u> (Nakayama, Local): Sea $\mathcal{O}$ un anillo local de maximal $\mathfrak{m}$, y sea M un $\mathcal{O}$-módulo finito-generado.

$$M = 0 \iff \underbrace{M \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m} = M/\mathfrak{m}M}_{\text{es un EV sobre } \mathcal{O}/\mathfrak{m}} = 0 \quad (\iff \mathfrak{m}M = M).$$

ie, un modulo es 0 $\iff$ como EV es 0 $\iff$ un cociente suyo es 0.

<u>Corolario</u>: Sea $N \subseteq M$ submódulo, M $\mathcal{O}$-módulo, $\mathcal{O}$ local, M fg, $\mathfrak{m}$ el id. max.

1) $$N + \mathfrak{m}M = M \implies N = M.$$

2) $$M = \langle m_1, \dots, m_r \rangle \iff M/\mathfrak{m}M = \langle \overline{m_1}, \dots, \overline{m_r} \rangle$$

Definición: Sea $S \subseteq A$ es un sistema multiplicativo si

i) $1 \in S$

ii) $s, s' \in S \Rightarrow s \cdot s' \in S$.

- $S = A - \{0\}$ (A íntegro) ; $S = A - \mathfrak{p}$ ($\mathfrak{p}$ primo) , $S = \{a^n\}_{n \geq 0}$ son sist. multiplicativos.

- Consideramos en $A \times S$ la siguiente relación de equivalencia: $(a,s) \equiv (a',s') \Leftrightarrow \exists t \in S : t(as'-a's)=0$.

Definición: Llamamos localización de A por S a $A_S = S^{-1}A := A \times S / \equiv$,

y para cada par $\overline{(a,s)}$ ponemos $\frac{a}{s}$.

- Definiendo $\frac{a}{s} + \frac{b}{t} := \frac{at+bs}{st}$, $\frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}$, se tiene que $(A_S, +, \cdot)$ es un anillo.

- Los elementos de S se hacen invertibles (el inverso de $\frac{s}{1}$ es $\frac{1}{s} \in A_S$), y en general algunos más de A que no están en S. Si $S = A - \{0\}$, entonces todo elemento no nulo se hace invertible, i.e., A_S es un cuerpo, que se llama cuerpo de fracciones de A.

Definición: Llamamos morfismo de localización a $j : A \longrightarrow A_S$, $a \longmapsto \frac{a}{1}$.

- $\frac{a}{1} = 0 \Leftrightarrow \exists s \in S : as = 0$

- $A_S = 0 \Leftrightarrow 0 \in S$.

Teorema (Propiedad Universal de la Localización de anillos): Sea S un sist. multip. de un anillo A, $j: A \to A_S$ el morf. de loc.. Si $f: A \to B$ es un morf. de anillos tal que $f(s) \in B^* \ \forall s \in S$, entonces $\exists! \ \varphi: A_S \to B$ morf de anillos tal que $f = \varphi \circ j$.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "j"'] & B \\ & A_S \arrow[u, dotted, "\exists! \varphi"'] \end{tikzcd} \quad f = \varphi \circ j.$$

$$\mathrm{Hom}_{\text{anillos}}(A_S, B) = \{ f \in \mathrm{Hom}_{\text{anils}}(A, S) : f(S) \subseteq B^* \}$$

- Dado $\mathfrak{a} \subseteq A$ ideal, $j(\mathfrak{a})$ en general no es un ideal, pero genera un ideal $(j(\mathfrak{a})) \overset{\text{NOT}}{=} \mathfrak{a} A_S \overset{\text{NOT}}{=} \underline{\underline{\mathfrak{a}_S}} = \{ \frac{a}{s} : a \in \mathfrak{a} \}$.

- $\mathfrak{a}_S = A_S \iff S \cap \mathfrak{a} \neq \emptyset$, i.e., si $\mathfrak{a}$ "pilla" a algún invertible (de S), de todos.
- Análogamente, dado $\mathfrak{b} \subseteq A_S$ ideal, $j^{-1}(\mathfrak{b})$ es un ideal de A, que denotamos $\underline{\mathfrak{b} \cap A}$.

- $\mathfrak{b} \neq A_S \Rightarrow S \cap (\mathfrak{b} \cap A) = \emptyset$.

- Estos cuatro últimos puntos establecen un par de aplicaciones

$$\left\{ \begin{array}{c} \text{ideales propios} \\ \text{de } A_S \end{array} \right\} \rightleftarrows \left\{ \begin{array}{c} \text{ideales de } A \\ \text{que no corten a } S \end{array} \right\}$$
$$\mathfrak{b} \longmapsto \mathfrak{b} \cap A$$
$$\mathfrak{a}_S \longleftarrow\!\shortmid \ \mathfrak{a}$$

Proposición: Si $\mathfrak{b} \subsetneq A_S$ ideal propio, entonces $\mathfrak{b} = (\mathfrak{b} \cap A)_S$.

- Esto dice que "$\longmapsto$", "$\longleftarrow\!\shortmid$" de la identidad. Desgraciadamente, no se tiene la contraria, i.e.,

$\mathfrak{a} \subsetneq \mathfrak{a}_S \cap A$ en general. Pero sí es verdad para un tipo de ideales: primos:

Teorema: Sea A un anillo y $S \subseteq A$ sistema multiplicativo. Entonces tenemos la siguiente correspondencia biunívoca que conserva inclusiones:

$$\begin{array}{ccc} \operatorname{Spec} A_S & = & \{x \in \operatorname{Spec} A : \mathfrak{p}_x \cap S = \emptyset\} \\ \mathfrak{p}_S & \longleftrightarrow & \mathfrak{p} \end{array}$$

Corolario: Sea A anillo, $\mathfrak{p}_x$ ideal primo, y consideramos la localización $A_{\mathfrak{p}_x} = A_{A-\mathfrak{p}_x}$. Se cumple que el anillo $A_{\mathfrak{p}}$ es local y su ideal maximal es $\mathfrak{p}_S = \mathfrak{p}_x A_{\mathfrak{p}_x}$. En particular,

$$\begin{array}{ccc} \operatorname{Spec} A_{\mathfrak{p}_x} & = & \{y \in \operatorname{Spec} A : \mathfrak{p}_y \subseteq \mathfrak{p}_x\} \\ \mathfrak{p}_y A_{\mathfrak{p}} & \longleftrightarrow & \mathfrak{p}_y \\ \cap & & \cap \\ \mathfrak{p}_x A_{\mathfrak{p}} & \longleftrightarrow & \mathfrak{p}_x \end{array}$$

- ¡Por esto es lo que se le llama localización! Viene de este ejemplo, de hacer un anillo local.
- Surge una pregunta al hacer la localización. Sabemos que los elementos de S se hacen invertibles en A_S, pero en general no solo esos, sino algunos más. ¿Cuándo ocurre que solo los de S?

Proposición (JBG): Sea $S \subseteq A$ un sist. multiplicativo.

$$(A_S)^* = j(S) \iff S = A - \bigcup_i \mathfrak{p}_i \qquad , \mathfrak{p}_i \text{ id. primos}.$$

(ie, $\frac{a}{1} \in A_S^* \Leftrightarrow a \in S$)

Corolario: Sea A DFU, $p \in A$ irreducible, y consideramos el sistema multiplicativo $S = \{p^n\}_{n \geq 0}$.

Entonces $(A_S)^* = \{\frac{p^n}{1}\}$.

TOPOLOGÍA DE ZARISKI

• En el tema 2 estudiamos la top. de Zariski en K^n, que era la que los cerrados eran los conjuntos algebraicos. Vamos a extender esta noción.

<u>Definición</u>: Sea A un anillo y consideremos su espectro primo $\operatorname{Spec} A$. Llamaremos <u>puntos</u> a los elementos de $\operatorname{Spec} A$, y los denotaremos como $x \in \operatorname{Spec} A$, y $\mathfrak{p}_x$ cuando nos refiramos a él como subconjunto de A. Además, llamaremos <u>funciones</u> a los elementos de A, y diremos, por definición, que $f(x) = 0$ cuando $f \in \mathfrak{p}_x$. Con esta terminología, $\mathfrak{p}_x = \{ f \in A : f(x) = 0 \}$.

• Cada punto $(a_1, \dots, a_n) \in K^n$ define un id. maximal $\mathfrak{m}_{(a_1,\dots,a_n)} = (x_1 - a_1, \dots, x_n - a_n)$ en $K[x_1, \dots, x_n]$, que con la terminología anterior denotaremos $(a_1, \dots, a_n) \in \operatorname{Spec} K[x_1, \dots, x_n]$.

<u>Proposición</u> (Propiedades): Sea A un anillo y $x \in \operatorname{Spec} A$.

1) La función 0 se anula en todo pto del $\operatorname{Spec} A$
2) $f(x) \neq 0 \ \forall x \in \operatorname{Spec} A \iff f$ es invertible
3) $f(x) = 0, \ g(x) = 0 \implies (f+g)(x) = 0$
4) $f(x) = 0 \implies (f \cdot g)(x) = 0 \quad \forall g \in A$
5) $(f \cdot g)(x) = 0 \iff f(x) = 0$ ó $g(x) = 0$.

• Las propiedades son iguales que a las del cálculo. Sin embargo, lo único extraño es que el recíproco de 1) no es cierto. Lo que ocurre en realidad es que está en el radical:

<u>Proposición</u>: $$\operatorname{rad} A = \bigcap_{x \in \operatorname{Spec} A} \mathfrak{p}_x$$

• Por tanto, el recíproco de 1) es cierto $\iff$ A es reducido.

Definición: Sea $f \in A$. Se llaman ceros de f a

$$(f)_0 = \{x \in \operatorname{Spec} A : f(x) = 0\} = \{\mathfrak{p}_x \in \operatorname{Spec} A : f \in \mathfrak{p}_x\}$$

y dado $\mathfrak{a} \subseteq A$ un ideal, llamamos ceros de $\mathfrak{a}$ a

$$(\mathfrak{a})_0 = \{x \in \operatorname{Spec} A : f(x) = 0 \ \forall f \in \mathfrak{a}\} = \{x \in \operatorname{Spec} A : \mathfrak{a} \subseteq \mathfrak{p}_x\}.$$

Proposición:

1) Si $\mathfrak{a} = (S)$, entonces $(\mathfrak{a})_0 = \bigcap_{f \in S} (f)_0$.

2) $\mathfrak{a} \subseteq \mathfrak{b} \Rightarrow (\mathfrak{a})_0 \supseteq (\mathfrak{b})_0$

Proposición (Propiedades):

1) $\operatorname{Spec} A = (0)_0$; $\emptyset = (A)_0$

2) $\bigcap_{i \in I} (\mathfrak{a}_i)_0 = \left(\sum_{i \in I} \mathfrak{a}_i\right)_0$

3) $\bigcup_{i=1}^{n} (\mathfrak{a}_i)_0 = \left(\bigcap_{i=1}^{n} \mathfrak{a}_i\right)_0$

- Estas 3 propiedades son justo las que debe cumplir los cerrados de una topología.

Definición: Llamamos topología de Zariski sobre $\operatorname{Spec} A$ a la que tiene como cerrados a los ceros de ideales de A.

- Es claro que los ceros de funciones $(f)_0$ forman una base de cerrados de $(\operatorname{Spec} A, \tau_{\text{Zariski}})$.

Proposición: Sea $x \in \operatorname{Spec} A$. $\boxed{\overline{\{x\}} = (\mathfrak{p}_x)_0}$.

• Si hay un primo no max, éste no es T_1 (por haber puntos que no son cerrados). Por ejemplo, si A es una k-álgebra finita, $\operatorname{Spec} A$ es T_1.

• La aplicación

$$i : k^n \longrightarrow \operatorname{Spec} k[x_1,\dots,x_n]$$
$$(a_1,\dots,a_n) \longmapsto (a_1,\dots,a_n) \equiv \mathfrak{m}_{(a_1,\dots,a_n)}$$

sabemos que es inyectiva. Si dotamos a k^n de la top. de Zariski (del T2, los cerrados son los conjuntos algebraicos) y a $\operatorname{Spec} k[x_1..x_n]$ de la top. de Zariski (del tema 3), tenemos:

Teorema:

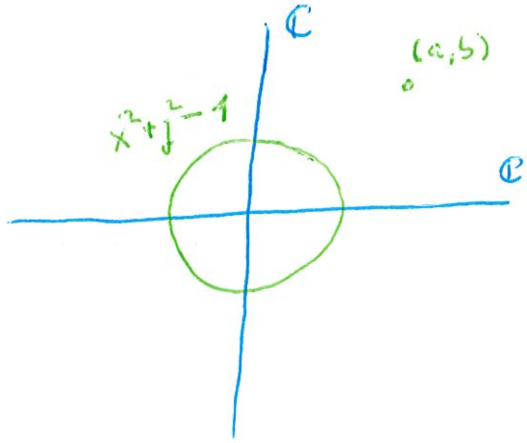
1) Caso k alg. cerrado: $i : (k^n, \tau_{Zariski}) \xrightarrow{\sim} (\operatorname{Spec}_{max} k[x_1,\dots,x_n], \tau_{Zar.\,subesp.})$ es un homeomorfismo.

2) Caso k general: $i : (k^n, \tau_{Zariski}) \xrightarrow{\sim} (\{\text{ptos racionales}\}, \tau_{Zar.\,subesp.})$ es un homeomorfismo.

• Para V un conjunto algebraico, $V \longrightarrow \operatorname{Spec} k[V]$, es idéntico.

• Esta nueva visión del $\operatorname{Spec} k[x_1,\dots,x_n]$ permite dar una visión geométrica del espectro. Por ejemplo, para $\mathbb{C}[x,y]$, sabemos que $\operatorname{Spec} \mathbb{C}[x,y] = \{0, \{(p(x,y))\}_{p \text{ irred}}, \{\mathfrak{m}_{(a,b)}\}_{a,b\in\mathbb{C}}\}$. Éstos puedo representar $\operatorname{Spec} \mathbb{C}[x,y]$ con $\mathbb{R}^2$:

ideales primos		ptos de Spec $\mathbb{C}[x,y]$
0	$\xleftrightarrow{\text{total}}$	pto genérico del plano (es el plano en sí)
$(p(x,y))$	$\xleftrightarrow{\text{curva}}$	pto genérico de la curva $p(x,y)=0$ (es la curva en sí)
$\mathfrak{m}_{(a,b)}$	$\xleftrightarrow{\text{pto}}$	pto (a,b)



<u>Definición</u>: Sea $j: A \to B$ un morfismo de anillos. Puesto que las antiimágenes de ideales son ideales, la j induce un morfismo entre sus espectros que llamaremos <u>aplicación continua inducida</u>

$$\begin{aligned} j^*: \operatorname{Spec} B &\longrightarrow \operatorname{Spec} A \\ \mathfrak{p}_x &\longmapsto j^{-1}(\mathfrak{p}_x) = \mathfrak{p}_{j^*(x)} \\ \parallel\!\!\!\wr \quad & \qquad\qquad \parallel\!\!\!\wr \\ x &\longmapsto j^*(x) \end{aligned}$$

<u>Proposición</u>: En efecto, la aplicación $j^*: \operatorname{Spec} B \to \operatorname{Spec} A$, dotados de las respectivas top. de Zariski, es continua, y $(j^*)^{-1}(f)_0 = (j(f))_0$, y $(j^*)^{-1}(\mathfrak{a})_0 = (\mathfrak{a}B)_0 \left(= (j(\mathfrak{a})\cdot B)_0\right)$.

Vamos a ver que la aplicación continua inducida generaliza a las aplicaciones regulares. Sea el morfismo de k-álgebras $h: K[y_1, \dots, y_m] \to K[x_1, \dots, x_n]$, y consideremos $h^*: \operatorname{Spec} K[x_1, \dots, x_n] \to \operatorname{Spec} K[y_1, \dots, y_m]$. Pongamos que $h(y_i) = h_i(x_1, \dots, x_n)$. Entonces tenemos que para cada ideal maximal $(a_1, \dots, a_m) \equiv \mathfrak{m}_{(a_1, \dots, a_m)}$ de $K[x_1, \dots, x_n]$, su imagen es $h^*(a_1, \dots, a_m) = (h_1(a_1, \dots, a_m), \dots, h_m(a_1, \dots, a_m)) = \mathfrak{m}_{(h_1(a_1, \dots, a_m), \dots, h_m(a_1, \dots, a_m))}$ ideal maximal de $K[y_1, \dots, y_m]$. Por tanto, identificando a K^n/K^m con sus imágenes en los espectros (es decir, siendo los id. maximales si K alg. cerrado son los pts racionales), tenemos:

$$\begin{tikzcd} \operatorname{Spec} K[x_1, \dots, x_n] \arrow[r, "h^*\ (T3)"] & \operatorname{Spec} K[y_1, \dots, y_m] \\ K^n \arrow[u, hook, "i"] \arrow[r, "h^*\ (T2)"] & K^m \arrow[u, hook, "i"'] \end{tikzcd}$$

$$(a_1, \dots, a_m) \equiv \mathfrak{m}_{(a_1, \dots, a_m)} \longmapsto (h_1(a_1, \dots), h_\dots) \equiv \mathfrak{m}(h_1(\dots))$$

$$(a_1, \dots, a_n) \longmapsto (h_1(a_1, \dots, a_n), \dots, h_m(a_1, \dots, a_n))$$

Teorema (Espectro del Cociente): Sea $I \subseteq A$ ideal. Entonces

$$\operatorname{Spec} A/I \overset{\pi^*}{=\!=\!=} (I)_0^{\subseteq \operatorname{Spec} A} \quad \text{es un homeomorfismo.}$$
$$\bar{\mathfrak{p}} \longleftarrow\!\shortmid \ \mathfrak{p}$$

• Pongamos k alg. cerrado, $V \subseteq k^n$ conj. algebraico. El homeomorfismo $k^n = \operatorname{Spec}_{max} k[x_1,\dots,x_n]$ induce otro homeomorfismo. Como $\operatorname{Spec}_{max} k[V] = \operatorname{Spec}_{max} k[x_1,\dots,x_n]/\mathcal{I}(V) = (\mathcal{I}(V))_0 \cap \operatorname{Spec}_{max} k[x_1,\dots,x_n]$, y dado $(a_1,\dots,a_n) \in V$ se tiene que $\mathfrak{m}_{(a_1,\dots,a_n)} \supset \mathcal{I}(V)$, entonces el morfismo φ está bien def. Que sea homeomorfismo es porque k alg. cerrado.

$$\begin{tikzcd}
k^n \arrow[r, "\sim"] & \operatorname{Spec}_{max} k[x_1,\dots,x_n] \\
V \arrow[u, hook] \arrow[r, dashed, "\sim"] & \operatorname{Spec}_{max} k[V] \arrow[u, hook]
\end{tikzcd}$$

$(a_1,\dots,a_n)$ $\qquad$ $\mathfrak{m}_{(a_1,\dots,a_n)} \supset \mathcal{I}(V)$

$(a_1,\dots,a_n)$ $\qquad$ $\mathfrak{m}_{(a_1,\dots,a_n)}$

• Para terminar, echamos un vistazo a el morfismo de localización, $j: A \to A_S$. Este induce $j^*: \operatorname{Spec} A_S \to \operatorname{Spec} A$. Si dotamos a los espacios de las respectivas topologías de Zariski, se tiene que la inyección

$$\operatorname{Spec} A_S \xrightarrow{\ \sim\ } \{x \in \operatorname{Spec} A : \mathfrak{p}_x \cap S = \emptyset\} \quad \text{es un homeomorfismo.}$$

LOCALIZACIÓN DE MÓDULOS

• Sea $S \subseteq A$ sist. multip., y A_S su localización. Si M es un A-módulo, ¿cómo crear un A_S-módulo?

• Sobre el conjunto $M \times S$ vamos a crear una relación de equivalencia:

$$(m_1, s_1) \equiv (m_2, s_2) \ :\Longleftrightarrow\ \exists t \in S : t(m_1 s_2 - m_2 s_1) = 0 .$$

Definición: Llamamos localización de M en S a $M_S := M \times S/\equiv$, y para cada pareja (m,s) pondremos $\frac{m}{s}$.

• Las operaciones $\frac{m}{s} + \frac{n}{t} := \frac{tm + sn}{st}$; $\frac{a}{s} \cdot \frac{m}{t} := \frac{am}{st}$ dotan a M_S de estructura de A_S-módulo.

Es claro por tanto que también es A-módulo: $a \cdot \frac{m}{s} := \frac{a}{1} \cdot \frac{m}{s}$.

• Al morfismo de A-módulos $\begin{array}{ccc} M & \xrightarrow{j} & M_S \\ m & \longmapsto & \frac{m}{1} \end{array}$ le llamaremos morfismo de localización.

Teorema (Propiedad Universal de la Localización de Módulos): Sea $S \subseteq A$ sist. multipl., M un A-módulo y N un A_S-módulo, y consideremos $f: M \longrightarrow N$ un morfismo de A-módulos. Entonces existe un único morfismo de A_S-módulos $\phi: M_S \longrightarrow N$: $f = \phi \circ j$:

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "j"'] & N \\ M_S \arrow[ur, dashed, "\exists \phi"'] & \end{tikzcd}$$

$$\mathrm{Hom}_{A_S\text{-mod}}(M_S, N) = \mathrm{Hom}_{A\text{-mod}}(M, N)$$

• Lo que hemos hecho entonces es convertir un A-módulo en un A_S-módulo. ¿Esto lo hemos hecho antes? Sí: CAMBIO DE ANILLO BASE (Alg I). Como M es un A-mod, $M \otimes_A A_S$ es un A_S-módulo. Y además

$$\mathrm{Hom}_{A_S\text{-mod}}(\underline{M_S}, N) \overset{\text{PU Loc}}{=} \mathrm{Hom}_{A\text{-mod}}(M, N) \overset{\text{PU}}{=} \mathrm{Hom}_{A_S\text{-mod}}(\underline{M \otimes_A A_S}, N)$$

("dime cómo te relacionas y te diré quién eres")

Proposición: $M_S = M \otimes_A A_S \; (= M_{A_S})$.

Teorema: Sea $S \subseteq A$ sist. mult., y M, N A-mod. Dado $f: M \to N$ mf. de A-mod, $\exists! f_S : M_S \to N_S$ que hace conmutativo el diagrama

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "j"'] & N \arrow[d] \\ M_S \arrow[r, dashed, "\exists! f_S"] & N_S \end{tikzcd}$$

$$\frac{m}{s} \longmapsto \boxed{f_S\left(\frac{m}{s}\right) := \frac{f(m)}{s}}$$

Luego tenemos $\mathrm{Hom}_{A\text{-mod}}(M,N) \longrightarrow \mathrm{Hom}_{A_S\text{-mod}}(M_S, N_S)$.

Proposición (Propiedades):

1) $0_S = 0$

2) $Id_S = Id_{M_S}$

3) $(f \circ g)_S = f_S \circ g_S$

4) $(f+g)_S = f_S + g_S$

Teorema: La localización de módulos conserva sucesiones exactas.

Corolario:

1) N A-submódulo de M $\Longrightarrow$ N_S A_S-submódulo de M_S.

2) N A-submod de M $\Longrightarrow$ $\left(M/N\right)_S = M_S/N_S$.

Proposición: Sean N, N' A-submods de M

1) $(N+N')_S = N_S + N'_S$

2) $(N \cap N')_S = N_S \cap N'_S$.

3) $\left(\bigoplus_{i\in I} M_i\right)_S = \bigoplus_{i\in I} (M_i)_S$.

Proposición:

1) $(\mathrm{Ker}\, f)_S = \mathrm{Ker}\, f_S$

2) $(\mathrm{Im}\, f)_S = \mathrm{Im}\, f_S$

3) $(\mathrm{Coker}\, f)_S = \mathrm{Coker}\, f_S$.

IV: MORFISMOS FINITOS

• Dados $f: A \to B$ mf de anillos, f dota a B de estructura de A-álgebra: $a \cdot b := f(a) \cdot b$. A f se le llama <u>morfismo estructural</u> de B. En particular B es un A-módulo.

<u>Definición</u>: Sea $f: A \to B$ un mf. de anillos. Se dice que f es un <u>morfismo finito</u>, o que B es una <u>A-álgebra finita</u>, si B es finito-generado como A-módulo, ie, si $\exists b_1, \dots, b_n \in B$:

$B = Ab_1 + \dots + Ab_n = \langle b_1, \dots, b_n \rangle$.

• $f: A \to B$ epi, $Id: A \to A$, $\mathbb{Z} \to \mathbb{Z}[i]$ son mf. finitos.

• $K \hookrightarrow A$ K-álgebra finita (Alg $\mathbb{F}$). En este caso es que $A = K^n = K \oplus \overset{n}{\dots} \oplus K$, como EV $\equiv$ $\equiv K$-EV $\equiv K$-módulo. Es un mfismo finito.

<u>Lema</u>: Sea $f: A \to B$ finito. A anillo noeth $\Rightarrow$ B anillo noeth.

<u>Proposición</u>: Sea $f: A \to B$ un mfismo de anillos, $b \in B$. Entonces $\exists\, p(x) \in A[x]$ mónico : $p(b) = 0$, ie, b satisface una relación del tipo $b^n + a_{n-1}b^{n-1} + \dots + a_1 b + a_0 = 0$ $\Leftrightarrow$ $A \hookrightarrow A[b]$ es un mf. finito.

• Si A noeth $\Rightarrow$ toda sub-álgebra de una A-álgebra finita es finita. Si no pasa no necesariamente.

<u>Proposición (Propiedades)</u>:

1) La composición de mfismos finitos es finito.

2) Sea $f: A \to B$ finito, $\mathfrak{a} \subseteq A$ un ideal y $\mathfrak{a}B = (f(\mathfrak{a}))$ $\equiv$ ideal que genera $f(\mathfrak{a})$. Entonces el mfismo $A/\mathfrak{a} \to B/\mathfrak{a}B$ es finito.

3) Sea $S \subseteq A$ sist. mlp. $f: A \to B$ finito $\Rightarrow$ $f_S: A_S \to B_S$ finito.

Lema: Sea $f:A\to B$ finito e inyectivo, y $\mathfrak{m}\in \operatorname{Spec}_{max} A$. Entonces $B/\mathfrak{m}B \neq 0$.

Proposición: Sea $f:A\to B$ finito e inyectivo. $f(a)\in B^* \Longrightarrow a\in A^*$

Corolario: Sea $f:A\to B$ inyectivo. Si $\exists\, a\in A,\ a\notin A^* : f(a)\in B^* \Longrightarrow f$ no es finito.

Corolario: $j: A\to A_S$ morf. finito $\iff A\simeq A_S$.

- $\mathbb{Z}\hookrightarrow\mathbb{Q}$ no es finito.

Corolario: $f:A\to B$ finito e inyectivo. B cuerpo $\Rightarrow A$ cuerpo.

Definición: Sea $f:A\to B$ un morfismo de anillos. Se dice que f es de tipo finito o que B es una A-álgebra de tipo finito si B es finito-generada como A-álgebra, i.e., si $\exists\, b_1,\dots,b_n\in B$: $B=A[b_1,\dots,b_n]$ (i.e., si B es un cociente del anillo de pol.).

Lema: Sea B una A-álgebra de tipo finito. A anillo noeth $\Rightarrow B$ anillo noeth.

- $f:A\to B$ morfismo finito $\Longrightarrow$ morfismo de tipo finito
  $\not\Longleftarrow$ ($A\to A[x]$)

***Lema** (de normalización de Noether): Si $K\hookrightarrow A=K[a_1,\dots,a_n]$ es una K-álgebra de tipo finito, existe un morfismo finito e inyectivo $K[x_1,\dots,x_r]\hookrightarrow A$, con $r\le n$. En particular, si $\exists\, p(x_1,\dots,x_n)\in K[x_1,\dots,x_n]$: $p(a_1,\dots,a_n)=0 \Rightarrow r<n$.

$$\begin{tikzcd} K \arrow[r, hook] \arrow[d] & A=K[a_1,\dots,a_n] \\ K[x_1,\dots,x_r] \arrow[ur, bend right, "\exists \text{ finito e inyectivo}"'] & \end{tikzcd}$$

Lema (Zariski): Sea $k\hookrightarrow K$ una extensión de cuerpos. Si K es una k-álgebra de tipo finito, $\Rightarrow$ la extensión es finita. En particular, si k es alg. cerrado $\Rightarrow k=K$.

• Ahora podemos probar el Th fundamental del curso (que estaba sin plantear):

<u>Teorema</u> (de los ceros de Hilbert, versión débil): Sea $K \hookrightarrow A$ una K-álgebra de tipo finito, y sea $\mathfrak{m}$ un id. maximal de A. Entonces el cuerpo residual $A/\mathfrak{m}$ es una extensión finita de cuerpos, $K \hookrightarrow A/\mathfrak{m}$. En consecuencia, si K es alg cerrado, $K = A/\mathfrak{m}$ $\forall \mathfrak{m}$ maximal.

V : DIMENSIÓN DE KRULL

__Definición__: Se llama __dimensión de Krull__ de un anillo A a la máxima de las longitudes de las cadenas estrictamente crecientes de ideales primos de A,

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n .$$

(i.e., es el nº de "$\subsetneq$", ó el número de ideales -1).

- Notar que $\mathfrak{p}_n$ debe ser maximal.
- $\dim_{kll} A = \sup\{\dim_{kll} A_{\mathfrak{p}} (A_m) : \mathfrak{p} \in \operatorname{Spec} A \ (m \in \operatorname{Spec}_{max} A)\} = \sup\{\dim_{kll} A/\mathfrak{p} : \mathfrak{p} \in \operatorname{Spec} A\}$.

__Lema__: $\dim_{krll} A = \dim_{krll} A/\operatorname{rad} A$.

- $\dim_{krll} A_{\mathfrak{p}} = 0 \iff \mathfrak{p}$ primo minimal
- $\dim_{krll} K = 0$; $\dim_{kll} A = 1$, A DIP. ; $\dim_{kll} A = 0$, A K-algebra finita.
- $\dim_{Krull} \mathbb{C}[x,y] = 2$; $\dim_{Krull} \mathbb{C}[x,y]/(p(x,y)) = 1$, $p(x,y)$ ni nulo ni invertible.

__Proposición__: Sea A un anillo de dim finita, $S \subseteq A$ sist. mult. e I ideal

1) $\dim_{krll} A_S \leq \dim_{kll} A$
2) $\dim_{krll} A/I \leq \dim_{krll} A$.

__Proposición__: A local + noetheriano $\implies \dim_{krll} A < +\infty$.

- __OJO__! Existen anillos noeth de dim ∞.

Teorema (del ascenso): Sea $A \xhookrightarrow{f} B$ **finito** e **inyectivo**. Entonces $\forall \mathfrak{p} \in \operatorname{Spec} A \ \exists \mathfrak{q} \in \operatorname{Spec} B$ tal que $\mathfrak{p} = \mathfrak{q} \cap A$, es decir, la aplicación $f^*: \operatorname{Spec} B \to \operatorname{Spec} A$ es epiyectiva.

$$\begin{tikzcd}
A \arrow[r, hook] & B \\
\mathfrak{p} = \mathfrak{q}\cap A \arrow[d, phantom, "\cap"] & \exists \mathfrak{q} \arrow[l, mapsto] \arrow[d, phantom, "\cap"] \\
\mathfrak{p}' = \mathfrak{q}'\cap A & \exists \mathfrak{q}' \arrow[l, mapsto]
\end{tikzcd}$$

Lema: Sea $f: A \hookrightarrow B$ un morfismo finito, $\mathfrak{q} \in \operatorname{Spec} B$ y $\mathfrak{q} \cap A \in \operatorname{Spec} A$ su antiimagen. Entonces

$$\mathfrak{q} \text{ maximal} \iff \mathfrak{q} \cap A \text{ maximal}.$$

Proposición: Sea $f: A \hookrightarrow B$ un morfismo finito. Si $\mathfrak{q}_1, \mathfrak{q}_2$ son dos ideales primos de B tales que $\mathfrak{q}_1 \subsetneq \mathfrak{q}_2 \Longrightarrow$
$\Rightarrow \mathfrak{q}_1 \cap A \subsetneq \mathfrak{q}_2 \cap A$.

$$\begin{tikzcd}
A \arrow[r, hook] & B \\
\mathfrak{q}_1 \cap A \arrow[d, phantom, "\cap\neq"] & \mathfrak{q}_1 \arrow[l, mapsto] \arrow[d, phantom, "\cap\neq"] \arrow[l, phantom, shift right=4, "\Longleftarrow"] \\
\mathfrak{q}_2 \cap A & \mathfrak{q}_2 \arrow[l, mapsto]
\end{tikzcd}$$

• Coloquialmente: "hacer antiimagen por morf. finito no aplasta las inclusiones".

Teorema. Si $f: A \hookrightarrow B$ es un morfismo finito, entonces $\dim B \leq \dim A$. En particular, si f es **finito** e **inyectivo**, entonces $\underline{\dim A = \dim B}$.

NOCIÓN DE DIM EN UN ET

Definición: Sea X un esp. top. Un cerrado $V \neq \emptyset$ se dice **irreducible** si no es unión de dos cerrados propios, i.e, $V = F \cup G \Rightarrow V = F$ ó $V = G$ (F, G cerrados).

• En $(K^n, \tau_{Zariski})$, V cerrado irreducible $\iff$ V conj. alg. irreducible (pues cerrados = conj. alg., y la noción de irreducible es análoga).

• Recordar del T2: $\underline{V \text{ irreducible} \iff \mathcal{I}(V) \text{ primo}}$, y por tanto

$$\left\{\begin{matrix} \text{ideales primos} \\ \text{de } K[x_1, \ldots, x_n] \end{matrix}\right\} \; = \; \left\{\begin{matrix} \text{subconj. algebraicos} \\ \text{(cerrados) irreducibles} \\ \text{de } K^n \end{matrix}\right\}$$

$$\mathfrak{p} \longmapsto \mathbb{V}(\mathfrak{p})$$
$$\mathcal{I}(V) \longleftarrow\!\!\shortmid\ V$$

o bien $\left\{ \begin{array}{c} \text{ideales primos} \\ \text{de } K[V] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{cerrados irreducibles} \\ \text{de } V \end{array} \right\}$.

__Definición__: Se llama __dimensión de Krull__ o __combinatoria__ de un espacio topológico X al supremo de las longitudes de las cadenas de cerrados irreducibles de X

$$V_0 \supsetneq V_1 \supsetneq \dots \supsetneq V_n$$

__Proposición__: Sea $V \subseteq K^n$ un conj. algebraico. Entonces $\underline{\dim_{Krull} V = \dim_{Krull} K[V]}$.

- $\dim_{Krull} K = \dim_{Krull} K[x] = 1$; $\dim_{Krull} \mathbb{C}^2 = \dim_{Krull} \mathbb{C}[x,y] = 2$;
- $\dim_{Krull} \mathcal{V}((p(x,y))) = \dim_{Krull} \mathbb{C}[x,y]/(p(x,y)) = 1$, $p(x,y)$ ni nulo ni invertible.
- $\dim_{Krull} A = \dim_{Krull} \operatorname{Spec} A$; $\dim_{Krull} K[x_1, \dots x_n]/I = \dim_{Krull} \mathcal{V}(I)$.,

__Definición__: Sea X ET. Llamaremos __componentes irreducibles__ de X a los subespacios irreducibles maximales, i.e., a los que no están contenidos en otro subespacio irreducible

- La correspondencia de antes dice que $(\text{si } V = \mathcal{V}(I))$

$\left\{ \begin{array}{c} \text{ideales primos} \\ \text{minimales de} \\ K[x_1,..x_n]/I \end{array} \right\} = \left\{ \begin{array}{c} \text{ideales primos} \\ \text{minimales de } K[V] \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{componentes irreducibles} \\ \text{de } V \end{array} \right\} = \left\{ \begin{array}{c} \text{primos minimales de} \\ K[x_1,..x_n] \text{ que contienen} \\ \text{a } I \end{array} \right\}$

__Proposición__: Todo conjunto algebraico es la unión de sus componentes irreducibles. En particular, dicha unión siempre es finita.

__Teorema__: $\dim_{Krull} K[x_1, \dots x_n] = n$.

__Corolario__: $\dim_{Krull} K^n = n$ (con la top Zariski)

__Corolario__: Toda K-álgebra de tipo finito tiene $\dim_{Krull} < \infty$. Es decir, todo conjunto algebraico es de dimensión finita.

__Corolario__: Sea V un conj. alg. sobre K alg. cerrado. Entonces $\dim_{Krull} V = \dim_{Krull} K[V] =$
$= \max \{ \dim_{Krull} K[V]/\mathfrak{p} : \mathfrak{p} \text{ primo minimal de } K[V] \} = \max \{ \dim_{Krull} W : W \text{ comp. irreducible} \}$.

o En espacios vectoriales, donde se anula una forma lineal tiene dim "total − 1", en las variedades diferenciables donde se anula 1 función dif tiene dim "total − 1". ¿Cuál es el análogo a las variedades algebraicas?

<u>Teorema</u>: Sea $f \in k[x_1, \dots x_n]$ irreducible.

$$\dim_{Krull} k[x_1, \dots x_n]/(f) = n-1 \quad ; \text{ i.e., } \quad \dim_{Krull} \mathbb{V}(f) = n-1 .$$

<u>Corolario</u>: Sea $f \in k[x_1, \dots x_n]$ ni nulo ni invertible.

$$\dim_{Krull} k[x_1, \dots x_n]/(f) = n-1 \quad ; \text{ i.e., } \quad \dim \mathbb{V}(f) = n-1$$

Además, cualquier factor p_i irreducible de f cumple que $\dim_{Krull} k[x_1, \dots x_n]/(p_i) = n-1$, es decir, <u>todas las componentes irreducibles de $\mathbb{V}(f)$ tienen la misma dimensión</u>

<u>Teorema</u> (del Ideal Principal de Krull): Sea A una k-álgebra de tipo finito íntegra y $f \in A$ ni nulo ni invertible, entonces

$$\dim_{Krull} A/(f) = \dim_{Krull} A - 1$$

Además, para todo primo minimal $\mathfrak{p}$ de (f) se cumple

$$\dim_{Krull} A/\mathfrak{p} = \dim A - 1.$$