Clase 15 : Anillos reducidos y noetherianos, Teorema de la base de Hilbert

Resumen de la vez pasada : Sea A un anillo.

•) **Ideal** : $(I,+) \subseteq (A,+)$ subgrupo tal que : $\forall a \in A$ y $\forall b \in I$, $ab \in I$.

↳ Eg. $I = \langle a_1, \dots, a_r \rangle = \{ x_1 a_1 + \dots + x_r a_r$ con $x_i \in A \}$ ← finitamente generado

↳ Eg. A es un DIP si es un dominio y todo ideal es principal : $I = \langle a \rangle$ ← eg. $\mathbb{Z}$, $k[X]$ con k cuerpo.

$\boxed{\text{Ejercicio}}$ Probar que para $a \in A$, $\langle a \rangle = A \iff a \in A^\times$ es invertible.

•) **Anillo cociente** : A/I donde $I \subseteq A$ un ideal.

↳ Hay Propiedad Universal y Teo. del isomorfismo de Noether $A/\ker(\varphi) \cong \operatorname{Im}(\varphi)$

•) **Cuerpos** : $A \neq \{0\}$ es cuerpo $\iff \{0\} = \langle 0 \rangle$ y A son sus únicos ideales

•) **Ideal primo** : $\mathfrak{p} \subsetneq A$ es primo $\overset{\text{def}}{\iff}$ $ab \in \mathfrak{p}$ implica que $a \in \mathfrak{p}$ ó $b \in \mathfrak{p}$ $\iff A/\mathfrak{p}$ dominio

·) **Ideal maximal**: $\mathfrak{m} \subsetneq A$ es maximal $\overset{\text{def}}{\iff}$ $\forall \overset{\text{ideal}}{I} \subseteq A$ tq $\mathfrak{m} \subseteq I$ cumple $I = \mathfrak{m}$ ó A $\iff$ $A/\mathfrak{m}$ cuerpo.

$\hookrightarrow$ **Krull**: Todo $I \subseteq A$ ideal está contenido en un ideal maximal.

[**Def**: Sea A un dominio. Decimos que $a \in A$ es irreducible si $a \notin A^\times$ y si: "$a = xy$ entonces $x \in A^\times$ o bien $y \in A^\times$"

Ejemplos:

① En $k[X_1, \ldots, X_n]$ lo anterior coincide con la def de polinomio irreducible.

② Si $a \neq 0$ y $\langle a \rangle \subseteq A$ ideal primo $\Rightarrow$ a es irreducible

(Si $a = xy \Rightarrow x = ax'$ ó $y = ay'$ $\overset{\text{eg. } x = ax'}{\leadsto}$ $a(1 - x'y) = 0 \underset{a \neq 0}{\Rightarrow} x'y = 1 \Rightarrow y \in A^\times$)

③ En general: a irreducible $\cancel{\Rightarrow}$ $\langle a \rangle$ primo.

$\boxed{\text{Ejercicio}}$ En $A = \mathbb{Z}[i\sqrt{5}] \cong \mathbb{Z}[X]/\langle X^2+5 \rangle$, probar que $a = 3$ es irreducible pero $\langle 3 \rangle$ no es primo (pues 3 divide $(1+i\sqrt{5})(1-i\sqrt{5})$).

[Indicación: $N(ab) = N(a)N(b)$, con $N(x + yi\sqrt{5}) = x^2 + 5y^2 \in \mathbb{N}$]

Prop: Sea A un DIP y sea $a \in A$ no-nulo. Son equivalentes:

a) $\langle a \rangle$ es un ideal primo ($\Longleftrightarrow A/\langle a \rangle$ dominio).

b) a es irreducible.

c) $\langle a \rangle$ es un ideal maximal ($\Longleftrightarrow A/\langle a \rangle$ cuerpo).

Dem: Sabemos c) $\Rightarrow$ a) $\Rightarrow$ b). Veamos b) $\Rightarrow$ c): Sup. a irreducible y sea I ideal tq $\langle a \rangle \subseteq I \overset{\text{DIP}}{=} \langle x \rangle$ cierto $x \in A$, i.e., $\exists\, y \in A$ tq $a = xy$

$\underset{a \text{ irred}}{\Longrightarrow}$ $x \in A^\times$ ($\Rightarrow I = A$) ó $y \in A^\times$ ($\Rightarrow I = \langle x \rangle = \langle xy \rangle = \langle a \rangle$).

Como $a \notin A^\times$, $\langle a \rangle \neq A$ y luego $\langle a \rangle$ es maximal $\blacksquare$

Ejemplo útil: Sea k un cuerpo y consideremos el DIP $k[X]$. Luego, para todo $P \in k[X]$ no-nulo irreducible $\rightsquigarrow K := k[X]/\langle P \rangle$ es un cuerpo.

$\boxed{\text{Ejercicio}}$* Probar que $\dim_k(K) = \deg(P)$.

E.g. $\mathbb{C} := \mathbb{R}[X]/\langle X^2+1 \rangle$, $\mathbb{Q}(i) = \mathbb{Q}[X]/\langle X^2+1 \rangle$, $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[X]/\langle X^3-2 \rangle$

{Cultura general} Esto permite construir el cuerpo finito $\mathbb{F}_q$ con $q = p^n$ (p primo, $n \geq 2$)

§28. Anillos reducidos y anillos noetherianos

Def: Sea A un anillo y $I \subseteq A$ un ideal. El radical de I es

$$\sqrt{I} := \{ a \in A \text{ tal que } \exists\, n \in \mathbb{N}^{\geq 1} \text{ con } a^n \in I \}$$

En part, $I \subseteq \sqrt{I}$. Decimos que I es un ideal radical si $I = \sqrt{I}$.

$\boxed{\text{Ejercicio importante}}$ Probar que $\sqrt{I}$ es un ideal y que $\sqrt{\sqrt{I}} = \sqrt{I}$.
En part, $\sqrt{I}$ es el ideal radical más pequeño que contiene a I!
[Indicación: Si $a^m \in I$ y $b^n \in I$, considerar $(a+b)^{m+n}$ (binomio de Newton!)]

Ejemplos:

① Si $I_n = n\mathbb{Z} \subseteq \mathbb{Z}$ con $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ factorización prima (con $\alpha_1 \leq \alpha_2 \leq \ldots \leq \alpha_r$)
$\Rightarrow \sqrt{I_n} = p_1 \cdots p_r \mathbb{Z}$ (pues $l \in p_1 \cdots p_r \mathbb{Z}$ cumple $l^{\alpha_r} \in I_n$ y $\sqrt{I_{p_1 \cdots p_r}} = I_{p_1 \cdots p_r}$)

② Si $I = \langle X^n \rangle \subseteq k[X]$ con $n \geq 2 \Rightarrow \sqrt{I} = \langle X \rangle$ (división euclideana)

Ejemplo importante: Sea $\mathfrak{p} \subsetneq A$ ideal primo $\Rightarrow$ $\mathfrak{p}$ es un ideal radical.

En efecto, basta ver que $\sqrt{\mathfrak{p}} \subseteq \mathfrak{p}$: Sea $a \in \sqrt{\mathfrak{p}}$, ie, $\exists n \in \mathbb{N}^{\geq 1}$ tq $a^n \in \mathfrak{p}$.

Si $n = 1 \rightsquigarrow$ OK ✓ Si $n \geq 2$: $a \cdot a^{n-1} \in \mathfrak{p} \underset{\mathfrak{p} \text{ primo}}{\Longrightarrow} a \in \mathfrak{p}$ ✓ ó $a^{n-1} \in \mathfrak{p}$ ✓ (Inducción)

Obs: Si $I \subsetneq A$ ideal: I maximal $\Rightarrow$ I primo $\Rightarrow$ I radical.

Def: El nilradical de un anillo A es el ideal de elem. nilpotentes:

$$\mathrm{Nil}(A) := \sqrt{\langle 0 \rangle} \overset{\mathrm{def}}{=} \{a \in A \text{ tal que } \exists n \in \mathbb{N}^{\geq 1} \text{ tal que } a^n = 0\}$$

Decimos que A es un anillo reducido si $\mathrm{Nil}(A) = \langle 0 \rangle$ (ie, $a^n = 0 \Rightarrow a = 0$).

Prop: Sea $I \subseteq A$ un ideal. Entonces,

I es radical $\Longleftrightarrow$ A/I es reducido.

Dem: A/I reducido $\overset{\mathrm{def}}{\Longleftrightarrow} \sqrt{\langle [0] \rangle} = \langle [0] \rangle \Longleftrightarrow \forall [a] \in A/I,\ [a^n] = [0] \Rightarrow [a] = [0]$

$\Longleftrightarrow \forall a \in A,\ a^n \in I \Rightarrow a \in I \Longleftrightarrow \sqrt{I} \subseteq I$ $\blacksquare$

Prop: Sea A un anillo y $I \subseteq A$ un ideal. Entonces, $\sqrt{I} = \bigcap_{\substack{I \subseteq \mathfrak{p} \\ \mathfrak{p} \text{ primo}}} \mathfrak{p}$.

Dem: Si $I \subseteq \mathfrak{p}$ con $\mathfrak{p}$ primo $\Rightarrow \sqrt{I} \overset{\text{def de } \sqrt{\cdot}}{\subseteq} \sqrt{\mathfrak{p}} \overset{\text{primo}}{=} \mathfrak{p} \Rightarrow \sqrt{I} \subseteq \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{p}$ ✓

Sup. $a \notin \sqrt{I}$ y veamos que $a \notin \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{p}$: Consideremos el conj. parcialmente ordenado (por $\subseteq$)

$$\mathcal{P} := \{ J \subseteq A \text{ tq } I \subseteq J \text{ pero } a^m \notin J \ \forall m \geq 1 \} \neq \emptyset \quad (\text{pues } I \in \mathcal{P})$$

$\rightsquigarrow$ Toda cadena $\mathcal{C}$ en $\mathcal{P}$ admite una cota superior (su unión)

$\overset{\text{Zorn}}{\Longrightarrow} \exists J = J_{max} \in \mathcal{P}$ elemento maximal resp. a "$\subseteq$". Veamos que J es primo:

Si $x \notin J$ y si $y \notin J$: $\langle x, J \rangle \notin \mathcal{P}$ (pues J maximal) $\Rightarrow \exists m$ tq $a^m \in \langle x, J \rangle$

Similar: $\langle y, J \rangle \notin \mathcal{P} \Rightarrow \exists n$ tq $a^n \in \langle y, J \rangle \rightsquigarrow a^{n+m} \in \langle xy, J \rangle \rightsquigarrow xy \notin J$ ■

$\boxed{\text{Ejercicio útil}}$ Sea A un anillo y $I, J \subseteq A$ ideales. Si definimos

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

Probar que (a) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ $\quad (\Rightarrow \sqrt{I^n} = \sqrt{I} \quad \forall n \in \mathbb{N}^{\geq 1})$.

(b) $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$

[Indicación (b): Si $a^n = b + c$ con $b^r \in I$ y $c^s \in J$, considerar $a^{n(r+s)}$]

Def: Sea A un anillo. Decimos que A es **noetheriano** si:

"Para toda cadena creciente de ideales en A

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_K \subseteq I_{K+1} \subseteq \cdots \qquad (\mathcal{C})$$

$\exists N \geq 1$ tal que $I_N = I_{N+1} = I_{N+2} = \ldots$, i.e., $I_m = I_N \ \forall m \geq N$"

"Ascending Chain Condition" (ACC)

Ejemplos:

1. Si k es un cuerpo, entonces k es noetheriano.

2. $\mathbb{Z}$ es noetheriano: $I_1 = n\mathbb{Z} \subseteq J = m\mathbb{Z} \iff m$ divide n ($\rightsquigarrow$ finitos m!)

3. $\boxed{\text{Ejercicio}}$ Si A noetheriano y $I \subseteq A$ ideal, entonces A/I es noetheriano.

Prop: A es noetheriano $\iff$ Todo ideal $I \subseteq A$ es finitamente generado (cf. $2\mathbb{Z} \cup 5\mathbb{Z} \not\ni 5-2$)

Dem: ($\Leftarrow$) Sea $(\mathcal{C}) = (I_n)_{n\geq 1}$ como antes y sea $I = \bigcup_{n\geq 1} I_n \subseteq A$ ideal (por hipótesis)

$\rightsquigarrow I = \langle x_1, \ldots, x_r \rangle$ con $x_i \in {}^{\exists} I_{n(i)} \Rightarrow I = I_N$ con $N = \max\{n(i),\ i = 1, \ldots, r\}$ ✓

($\Rightarrow$) Si I <u>no</u> es fin. gen, construimos $I_1 = \langle x_1 \rangle \subsetneq I_2 = \langle x_1, x_2 \rangle \subsetneq I_3 = \langle x_1, x_2, x_3 \rangle \subsetneq \cdots$

que no se estabiliza $\Rightarrow A$ <u>no</u> es noetheriano ■

§29. Algunos teoremas de Hilbert

Una de las piedras angulares del álgebra conmutativa es el siguiente resultado de David Hilbert:

Teorema de la base de Hilbert (1890): Sea A un anillo noetheriano, entonces $A[X]$ es noetheriano también.

Dem: Sup. $\exists\, J \subseteq A[X]$ no fin. gen $(\Rightarrow J \neq \langle 0 \rangle)$. Sea $J_0 := \langle 0 \rangle$ y $\forall\, i \geq 1$ sea $f_i \in J - J_i$ de grado d_i minimal, donde $J_i := \langle f_1, \dots, f_i \rangle$.

$(\rightsquigarrow J_0 = \langle 0 \rangle \subsetneq J_1 = \langle f_1 \rangle \subsetneq J_2 = \langle f_1, f_2 \rangle \subsetneq \dots \subseteq J$ y $d_i \leq d_{i+1})$

Sea c_i el coef. principal de f_i y sea $\mathfrak{a} := \langle \{c_i\}_{i \geq 1} \rangle \subseteq A \underset{A \text{ noeth.}}{\Longrightarrow} \mathfrak{a} = \langle c_1, \dots, c_m \rangle$ cierto $m \geq 1$.

Luego: $c_{m+1} = a_1 c_1 + \dots + a_m c_m$ ciertos $a_i \in A$.

Sea $f := f_{m+1} - (a_1 f_1 x^{d_{m+1}-d_1} + \dots + a_m f_m x^{d_{m+1}-d_m}) \overset{\text{dg}}{\in} J_{m+1}$

$$= (\cancel{c_{m+1} x^{d_{m+1}}} + \dots) - ((\cancel{a_1 c_1 + \dots + a_m c_m) x^{d_{m+1}}} + \dots) \rightsquigarrow \deg(f) < d_{m+1}$$

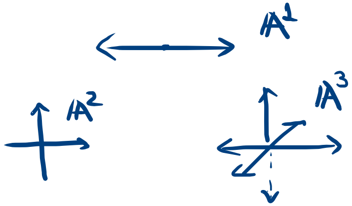
$\Rightarrow f \in J_m$ y $f = f_{m+1} - g$ con $g \in J_m \Rightarrow f_{m+1} \in J_m$ ↯ ■

Consecuencia: Para todo cuerpo k, el anillo $k[X_1,\dots,X_n]$ es noetheriano.
En part, **todo** ideal $I \subseteq k[X_1,\dots,X_n]$ es finitamente generado, i.e., $\exists f_1,\dots,f_r$ polinomios tales que $I = \langle f_1,\dots,f_r \rangle$.

Para enunciar otro importante resultado de Hilbert, así como para reinterpretar geométricamente varias de las nociones ya estudiadas, necesitamos introducirnos al mundo de la geometría algebraica clásica:

Def: Sea k un cuerpo y $n \in \mathbb{N}$. Definimos el espacio afín de dimensión n sobre k como:

$$\mathbb{A}^n = \mathbb{A}^n(k) = \{ (x_1,\dots,x_n) \text{ con } x_i \in k \} = k^n$$



Obs: Concretamente, en $\mathbb{A}^n$ **no** nos restringimos a sub-ev de k^n.

Convención: En todo lo que sigue, asumiremos $k = \mathbb{C}$ y luego $\mathbb{A}^n = \mathbb{A}^n(\mathbb{C}) = \mathbb{C}^n$.
(Sin embargo, bastaría considerar k algebraicamente cerrado).