Clase 21: Consecuencias de Cayley-Hamilton y Lema de Nakayama

§37. Teorema de Cayley-Hamilton y Lema de Nakayama (continuación):

La vez pasada probamos el Teorema de Cayley-Hamilton:

Sea M un A-módulo finitamente generado y sea $u : M \to M$ un endomorfismo.
Sean $m_1, \dots, m_n$ generadores de M y escribamos $u(m_i) = \sum_{j=1}^{n} a_{ij} m_j$ para ciertos $a_{ij} \in A$.

Definamos $R := (a_{ij})_{1 \leq i,j \leq n} \in M_n(A)$ y $P(X) := \det(X I_n - R)$
$$= X^n + c_1 X^{n-1} + \dots + c_{n-1} X + c_n \in A[X]$$

$\Rightarrow P(u) = 0$ en $\mathrm{End}_A(M)$.

Obs útil: Si $I \subseteq A$ es un ideal tal que $\mathrm{Im}(u) \subseteq IM$, entonces podemos suponer que $a_{ij} \in I$ (por def. de IM) y luego $c_j \in I^j$ para todo $j \in \{1, \dots, n\}$. $(\star)$

Corolario: Sea M un A-módulo finitamente generado. Entonces, todo endomorfismo $u : M \twoheadrightarrow M$ sobreyectivo es un isomorfismo.

Dem: Como antes, usamos $u: M \to M$ para dotar a M de estructura de $A[X]$-módulo: $X \cdot m \overset{def}{=} u(m) \ \forall m \in M$. Sea $I = \langle X \rangle \subseteq A[X]$ ideal, y notamos que el hecho que u sea sobreyectivo implica que $M = IM \ (= u(M))$.

Consideremos $\varphi = Id_M : M \xrightarrow{\sim} M$ la identidad. Cayley-Hamilton:

$\exists\, P = T^n + c_1(X)T^{n-1} + \dots + c_{n-1}(X)\,T + c_n(X) \in A[X][T] \simeq A[X,T]$ tal que $P(\varphi) = 0$.

$\boxed{\text{Obs útil}}$ $c_j(X) \in I^j \overset{def}{=} \langle X^j \rangle$ y luego podemos escribir $c_j = X d_j$ para cierto $d_j \in A[X]$.

Luego, para todo $m \in M$ calculamos:

$$0 = P(\varphi)(m) = \left(\varphi^n + c_1(X)\varphi^{n-1} + \dots + c_{n-1}(X)\varphi + c_n(X)\,Id\right)(m)$$

$$\overset{\varphi = Id_M}{=} m + c_1(X)\cdot m + \dots + c_{n-1}(X)\cdot m + c_n(X)\cdot m$$

$$\overset{c_j = X d_j}{=} m + X\cdot\left(d_1(X)\cdot m + \dots + d_{n-1}(X)\cdot m + d_n(X)\cdot m\right) = m + X\,Q(X)\cdot m \qquad \underbrace{Q(X)}_{} := d_1(X) + \dots + d_n(X) \in A[X]$$

$$\overset{def}{=} m + u\left(Q(u)(m)\right) = m + Q(u)\left(u(m)\right)$$

Luego, u es inyectivo (pues $u(m) = 0 \Rightarrow m = 0$) y además $0 = Id_M + u \circ Q(u)$ en $End_A(M)$ implica que $u^{-1} = -Q(u)$ ∎

Corolario: Sea $M \cong A^n$ un A-módulo libre de rango n. Entonces, toda familia generadora de n elementos es una base de M.

Dem: Podemos suponer $M = A^n$. Una familia generadora $\mathcal{B} = \{m_1, \dots, m_n\}$ define un endomorfismo sobreyectivo $\varphi : A^n \twoheadrightarrow A^n$, $(a_1, \dots, a_n) \longmapsto a_1 m_1 + \dots + a_n m_n$. El Corolario anterior implica que φ es un isomorfismo y luego $\mathcal{B}$ es una base ∎

Corolario: Sea M un A-módulo finitamente generado y sea $I \subseteq A$ un ideal tal que $IM = M$. Entonces, existe $a \in I$ tal que $(1+a)M = 0$. En part, $b := -a \in I$ cumple $bm = m$ $\forall m \in M$.

Dem: El Teorema de Cayley-Hamilton aplicado a $u = Id_M : M \xrightarrow{\sim} M$, así como la $\boxed{\text{Obs útil}}$, implica que existen $c_j \in I^j$ tales que $u^n + c_1 u^{n-1} + \dots + c_{n-1} u + c_n Id_M = 0$ en $End_A(M)$. Luego, si definimos $a := c_1 + \dots + c_n \in I$ tenemos que $(1+a) Id_M = 0$, i.e., $(1+a)m = 0$ $\forall m$ ∎

$\boxed{\text{Ejercicio}}$ Sea A un anillo y sea I un ideal finitamente generado tal que $I^2 = I$. Probar que $I = \langle e \rangle$ para cierto $e \in A$ que cumple $e^2 = e$.
(**Obs**: Decimos que e es un elemento idempotente de A).

Recuerdo: Para todo ideal $I \subseteq A$ se tiene que $\sqrt{I} = \bigcap_{\substack{I \subseteq \mathfrak{p} \\ \mathfrak{p} \text{ primo}}} \mathfrak{p}$.

En particular, $\mathrm{Nil}(A) \overset{\text{def}}{=} \sqrt{\langle 0 \rangle} = \bigcap_{\mathfrak{p} \text{ primo}} \mathfrak{p}$

Def (Jacobson, 1945): El radical de Jacobson de un anillo A es la intersección de todos sus ideales maximales:

$$J(A) := \mathrm{rad}(A) :\overset{\text{def}}{=} \bigcap_{\mathfrak{m} \text{ maximal}} \mathfrak{m}$$

$\boxed{\text{Recuerdo: Para } a \in A,\ a \in A^\times \iff \langle a \rangle = A}$

Lema: Sea A un anillo no-nulo. Entonces,

$$J(A) = \{ a \in A \text{ tal que } 1 + ax \text{ es invertible } \forall x \in A \}$$

Dem: $(\supseteq)$ Si $a \notin J(A)$, $\exists\, \mathfrak{m} \subseteq A$ maximal tq $a \notin \mathfrak{m}$. Luego, $\mathfrak{m} + \langle a \rangle \overset{\mathfrak{m} \text{ maximal}}{=} A$

$\rightsquigarrow \exists\, b \in \mathfrak{m}$ y $x \in A$ tal que $b + ax = 1 \iff b = 1 + a(-x)$. Como $\mathfrak{m} \cap A^\times = \emptyset$, $1 + a(-x) \notin A^\times$ ✓

$(\subseteq)$ Si $\exists\, x \in A$ tal que $1 + ax \notin A^\times \Rightarrow \langle 1 + ax \rangle \underset{\text{Krull}}{\subseteq} \exists\, \mathfrak{m} \subsetneq A$. Como $1 \notin \mathfrak{m} \rightsquigarrow a \notin \mathfrak{m}$ ✓ ■

Ejemplos: $J(\mathbb{Z}) = \langle 0 \rangle$ y $J(\mathbb{Z}/12\mathbb{Z}) \overset{\text{def}}{=} 2\mathbb{Z}/12\mathbb{Z} \cap 3\mathbb{Z}/12\mathbb{Z} = 6\mathbb{Z}/12\mathbb{Z}$

Teorema (Lema de Nakayama, 1951): Sea A un anillo no-nulo y sea $I \subseteq J(A)$ un ideal. Para todo A-módulo M finitamente generado se tiene:

1. Si $IM = M$ entonces $M = 0$.
2. Sean $m_1, \dots, m_n \in M$. Si $[m_1], \dots, [m_n] \in M/IM$ generan dicho A-módulo cociente ($\Leftrightarrow$ generan como A/I-módulo), entonces $m_1, \dots, m_n$ generan M.

Dem: (1) Vimos antes que si $IM = M$ entonces existe $a \in I$ tal que $(1+a)m = 0$ para todo $m \in M$. Como $I \subseteq J(A)$, tenemos que $1 + ax \overset{x=1}{=} 1+a \in A^\times$ y luego $M = 0$ ✓

(2) Sup. que $[m_1], \dots, [m_n] \in M/IM$ generan M/IM y definamos

$$N_0 := \langle m_1, \dots, m_n \rangle_A \subseteq M \quad \text{y} \quad N := M/N_0 .$$

Veamos que $N = 0$ ($\Rightarrow$ (2) ✓):

Sea $m \in M$ y escribamos $[m] = \sum_{j=1}^{n} a_i [m_i]$ (generadores) en M/IM para ciertos $a_i \in A$.

En otras palabras, módulo N_0, tenemos que $m \in IM$. De lo anterior, se deduce que $IN = N$ ($\boxed{\text{Ejercicio}}$: Convencerse). Como N es fin. generado, $N = 0$ gracias a (1) ■

↳ Obs: Otra forma es notar que $M = IM + N_0 \Rightarrow M/N_0 = (IM + N_0)/N_0 \cong I(M/N_0)$

Un caso particular importante es el caso de "anillos locales":

***Definición 4.2.45* (anillo local).** — Un anillo A no nulo es un **anillo local** si existe un único ideal maximal $\mathfrak{m} \subseteq A$. El cuerpo $\kappa = A/\mathfrak{m}$ se llama **cuerpo residual** del anillo local $(A, \mathfrak{m})$.

$\to J(A) = \mathfrak{m}$

$(\Rightarrow I \subseteq J(A)$ equivale a $I \neq A)$

***Corolario 4.2.46* (Nakayama).** — *Sea $(A, \mathfrak{m})$ un anillo local con cuerpo residual $\kappa = A/\mathfrak{m}$. Sea M un A-módulo finitamente generado, entonces:*

1. *Si $\mathfrak{m}M = M$ entonces $M = 0$.*
2. *Si las imagenes de $m_1, \ldots, m_n$ generan el κ-espacio vectorial* de dim finita *$M/\mathfrak{m}M$, entonces $M = \langle m_1, \ldots, m_n \rangle_{A-\mathrm{mod}}$.*

Una de las formas más usadas!

$\boxed{\text{Ejercicio}}$ Sea $(A, \mathfrak{m})$ un anillo local y sean M, N dos A-módulos finitamente generados. Sea $\varphi : M \longrightarrow N$ morfismo A-lineal.

① Probar que $\varphi_{\mathfrak{m}} : M/\mathfrak{m}M \longrightarrow N/\mathfrak{m}N$, $[m] \mapsto [\varphi(m)]$ está bien definido y es κ-lineal.

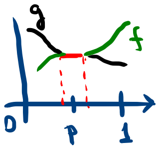
② Probar que si $\varphi_{\mathfrak{m}}$ es sobreyectivo, entonces φ es sobreyectivo.

Ejemplo principal de anillo local:

Sea $A := \mathcal{C}^0([0,1],\mathbb{R}) = \{f : [0,1]\to\mathbb{R} \text{ continua}\}$ la $\mathbb{R}$-álgebra de funciones reales continuas en $[0,1]$, y sea $p\in[0,1]$ un punto arbitrario (que fijaremos). Sea:

$$I := \{f\in A \text{ tal que } \exists\, \mathcal{U}\subseteq[0,1] \text{ vecindad abierta de } p \text{ tal que } f(x)=0\ \forall x\in\mathcal{U}\}$$

Definimos $A_p := A/I$ es anillo de gérmenes de funciones continuas en p, i.e., $[f]=[g]$ en A_p si f y g coinciden en una vecindad abierta de p.



Veamos que A_p es un anillo <u>local</u>: $\{\mathfrak{m}\subseteq A_p \text{ maximal}\} \overset{1:1}{\longleftrightarrow} \{I\subseteq\mathfrak{m}\subseteq A \text{ maximal}\}$.

En A hay muchos ideales maximales: si $x\in[0,1]$, definimos

$ev_x : A \twoheadrightarrow \mathbb{R}$, $f\mapsto f(x)$ con $\mathfrak{m}_x := \ker(ev_x) = \{f\in A \text{ tq } f(x)=0\}$ maximal. $A/\mathfrak{m}_x\cong\mathbb{R}$ cuerpo

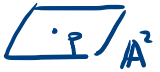
$\boxed{\text{Ejercicio}}$ Todo ideal maximal de A es de la forma $\mathfrak{m}_x$ para algún $x\in[0,1]$.

$\Rightarrow I\subseteq\mathfrak{m}_x$ si y sólo si $x=p$. Así,

$$\mathfrak{m}_{A_p} := \mathfrak{m}_p/I = \{\text{gérmenes de } f:[0,1]\to\mathbb{R} \text{ tq } f(p)=0\}$$

es el <u>único</u> ideal maximal de A_p, con $K = A_p/\mathfrak{m}_{A_p}\cong A/\mathfrak{m}_p\cong\mathbb{R}$.

Ejemplo algebro-geométrico: Sea $p \in \mathbb{A}^2$ un punto. El anillo local de $\mathbb{A}^2$ en p es



$$\mathcal{O}_p := \mathcal{O}_{\mathbb{A}^2,p} := \left\{ \frac{f}{g} \text{ tales que } f,g \in \mathbb{C}[X,Y] \text{ con } g(p) \neq 0 \right\} \subseteq \mathbb{C}(X,Y)$$

Como antes, definimos $ev_p : \mathcal{O}_p \twoheadrightarrow \mathbb{C}$, $\frac{f}{g} \longmapsto \frac{f(p)}{g(p)}$ cuyo kernel es un ideal maximal:

$$\mathfrak{m}_p := \mathfrak{m}_{\mathbb{A}^2,p} := \left\{ \frac{f}{g} \text{ tales que } f,g \in \mathbb{C}[X,Y] \text{ con } f(p) = 0 \text{ y } g(p) \neq 0 \right\}$$

En este caso es más sencillo ver que $(\mathcal{O}_p, \mathfrak{m}_p)$ es un anillo local: si $I \subseteq \mathcal{O}_p$ ideal tal que $I \not\subseteq \mathfrak{m}_p \Rightarrow \exists\, f/g \in I$ con $f(p) \neq 0$ y luego $g/f \in \mathcal{O}_p \Rightarrow 1 = (f/g)\cdot(g/f) \in I$ ie, $I = \mathcal{O}_p$.

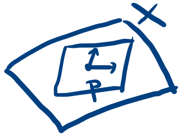
⚠ El Lema de Nakayama es un análogo algebraico del Teorema de la Función Inversa!

En el primer ejemplo: $(A_p, \mathfrak{m}_{A_p})$ anillo local y sea $M = \mathfrak{m}_{A_p}$ ← Estoy haciendo trampa (Para que sea fin. generado hay que mirar f analítica ↓ Malgrange (1962) u holomorfa!) ↳ Weierstrass

Nakayama: "Generadores de $M/\mathfrak{m}M = \mathfrak{m}_{A_p}/\mathfrak{m}_{A_p}^2$ se levantan a generadores de $\mathfrak{m}_{A_p}$"

$\rightsquigarrow$ si $f(t) = \sum_{n=0}^{\infty} a_n (t-p)^n$ analítica en p, con $a_n = \frac{f^{(n)}(p)}{n!}$

$\Rightarrow f \in \mathfrak{m}_{A_p} \Leftrightarrow f(p) = 0$ y $[f] = [f'(p)\underbrace{(t-p)}_{\in\, \mathfrak{m}_{A_p}}]$ en $\mathfrak{m}_{A_p}/\mathfrak{m}_{A_p}^2$



Base de $T_{X,p} \rightsquigarrow$ Coord locales!