Clase 20: Módulos finitamente generados y módulos libres

Sea A un anillo. Recordemos que un A-módulo M es un "A-esv" (i.e., un grupo abeliano junto con multiplicación por "escalares" en A).

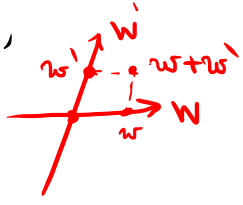
Vimos que en este contexto tiene sentido hablar de morfismos A-lineales, submódulos, cocientes por submódulos (con su respectiva Prop. Universal e Isomorfismo de Noether). Además, podemos considerar la suma e intersección de submódulos.

§35. Operaciones sobre sub-módulos (continuación):

Recuerdo (MAT210): Sea V un k-esv y sean $W, W' \subseteq V$ dos sub-esv. Entonces,

$$V = W \oplus W' \overset{\text{def}}{\iff} \text{vect}_k\langle W, W'\rangle = V \text{ y } W \cap W' = \{0_V\}$$

$$\Rightarrow V \cong W \times W' \text{ espacio vectorial producto}$$



Por lo anterior, si V y V' son k-esv arbitrarios (no nec. subesv de un mismo k-esv!) entonces escribimos $V \oplus V' := V \times V'$.

Def: Sea A un anillo y sea $\{M_\lambda\}_{\lambda\in\Lambda}$ una familia de A-módulos.

a) El **producto** de los M_λ se define como el producto cartesiano $\prod_{\lambda\in\Lambda} M_\lambda$, donde para $a\in A$ y $(m_\lambda)_{\lambda\in\Lambda}, (n_\lambda)_{\lambda\in\Lambda} \in \prod_{\lambda\in\Lambda} M_\lambda$ (con $m_\lambda, n_\lambda \in M_\lambda$) definimos:

$$a\cdot (m_\lambda)_{\lambda\in\Lambda} := (am_\lambda)_{\lambda\in\Lambda} \quad \text{y} \quad (m_\lambda)_{\lambda\in\Lambda} + (n_\lambda)_{\lambda\in\Lambda} := (m_\lambda + n_\lambda)_{\lambda\in\Lambda}$$

b) La **suma directa** de los M_λ es el submódulo de $\prod_{\lambda\in\Lambda} M_\lambda$ dado por

$$\bigoplus_{\lambda\in\Lambda} M_\lambda := \left\{ (m_\lambda)_{\lambda\in\Lambda} \in \prod_{\lambda\in\Lambda} M_\lambda \text{ tal que } m_\lambda = 0 \text{ salvo finitos } \lambda\in\Lambda \right\}$$

Obs: En particular, si el conjunto de índices $\Lambda = \{1,\dots,r\}$ es finito, entonces $\bigoplus_{\lambda\in\Lambda} M_\lambda = \prod_{\lambda\in\Lambda} M_\lambda$. En tal caso, escribimos

$$\bigoplus_{j=1}^{r} M_j = M_1 \oplus \cdots \oplus M_r \quad \text{o bien} \quad \prod_{j=1}^{r} M_j = M_1 \times \cdots \times M_j$$

Ejemplo: $\ell^2(\mathbb{R}) \overset{\text{def}}{=} \{(a_n)_{n\in\mathbb{N}} \text{ sucesión real tq } \sum_{n\geq 0} |a_n|^2 < +\infty\} \subseteq \prod_{n\in\mathbb{N}} \mathbb{R}$, pero $\notin \bigoplus_{n\in\mathbb{N}} \mathbb{R}$

§36. Módulos finitamente generados y Módulos libres

Sea M un A-módulo. Recordemos que si $S \subseteq M$ es un subconjunto arbitrario,

$$\langle S \rangle = \langle S \rangle_A := \{ a_1 m_1 + \ldots + a_n m_n \,,\ n \in \mathbb{N},\ a_i \in A \text{ y } m_i \in S \} = \bigcap_{\substack{S \subseteq N \\ N \text{ submod}}} N$$

es el submódulo generado por S. En part, si $S = \{M_\lambda\}_{\lambda \in \Lambda} \subseteq M$ es una familia de submódulos, entonces $\sum_{\lambda \in M} M_\lambda = \langle \{M_\lambda\}_{\lambda \in \Lambda} \rangle \overset{\text{def}}{=} \langle \bigcup_{\lambda \in \Lambda} M_\lambda \rangle$

Equivalentemente, si consideramos el siguiente morfismo de A-módulos

$$\psi : \bigoplus_{\lambda \in \Lambda} M_\lambda \to M,\ (m_\lambda)_{\lambda \in \Lambda} \mapsto \sum_{\lambda \in \Lambda} m_\lambda \quad \leftarrow \text{bien def!}$$

entonces $\sum_{\lambda \in \Lambda} M_\lambda := \mathrm{Im}(\psi)$. Decimos que $\{M_\lambda\}_{\lambda \in \Lambda}$ está en suma directa si el morfismo ψ es inyectivo, ie,

"$m_{i_1} + \ldots + m_{i_m} = 0 \Rightarrow m_{i_1} = \ldots = m_{i_m} = 0$" para todo subconj. finito $\{i_1, \ldots, i_m\} \subseteq \Lambda$.

En part, en este caso ψ induce un isomorfismo $\bigoplus_{\lambda \in \Lambda} M_\lambda \cong \sum_{\lambda \in \Lambda} M_\lambda$.

⚠ **Obs:** Sabemos de MAT210 que para V k-ev de dimensión finita (i.e., k-módulo fin. generado), para todo $W \subseteq V$ existe $W' \subseteq V$ tal que $V = W \oplus W'$.

Sin embargo, si $A = \mathbb{Z}$, el submódulo fin. generado $N = 2\mathbb{Z}$ de $M = \mathbb{Z}$ **no** posee un complementario en M:
Si $N' = n\mathbb{Z}$ para cierto $n \in \mathbb{N}^{\geq 1}$, entonces $0 \neq 2n \in N \cap N'$.

Caso particular importante: Si $\{M_\lambda\}_{\lambda \in I}$ verifica $M_\lambda = A$ para todo índice $\lambda \in I$.
Entonces escribimos

$$A^I := \prod_{\lambda \in I} A \quad \text{(producto)} \qquad \text{y} \qquad A^{(I)} := \bigoplus_{\lambda \in I} A \quad \text{(suma directa)}$$

Notación: Dado $\lambda \in I$, denotamos por $e_\lambda = (m_\mu)_{\mu \in I}$ con $m_\lambda = 1$ y $m_\mu = 0$ si $\mu \neq \lambda$.
En part, $e_\lambda \in A^{(I)}$ y todo elemento de $A^{(I)}$ se escribe de manera única como $\sum_{\lambda \in I} a_\lambda e_\lambda$, donde $\{a_\lambda\}_{\lambda \in I} \subseteq A$ cumple $a_\lambda \neq 0$ para un nº <u>finito</u> de $\lambda \in I$.

Obs: Sin embargo, $(1, 1, 1, \ldots) \in \mathbb{R}^{\mathbb{N}}$ no pertenece a $\mathbb{R}^{(\mathbb{N})}$.

Propiedad Universal de $A^{(I)}$: Para todo A-módulo M y toda familia de elementos $(m_\lambda)_{\lambda \in I}$ de M indexados por el conjunto I, $\exists!\ \psi : A^{(I)} \to M$ morfismo de A-módulos tal que $\psi(e_\lambda) = m_\lambda$ para todo $\lambda \in I$. Explícitamente, definimos

$$\psi\left(\sum_{\lambda \in I} a_\lambda e_\lambda\right) := \sum_{\lambda \in I} a_\lambda m_\lambda \text{, donde } a_\lambda \neq 0 \text{ para un nº finito de } \lambda \in I \quad \blacksquare$$

La importancia teórica de lo anterior, es que nos permite definir:

Definición 4.2.31. — Sea $(m_i)_{i \in I} \subseteq M$ una familia de elementos de M y sea $\psi : A^{(I)} \to M$ definido como $e_i \mapsto m_i$ el morfismo asociado. Decimos que la familia es:

1. **linealmente independiente** (o **libre**) si ψ es inyectivo, es decir, si $\sum_{\text{finita}} a_i m_i = 0$ implica que $a_i = 0$ para todo i.
2. **generadora** si ψ es sobreyectivo, es decir, si todo $m \in M$ puede ser escrito como $m = \sum_{\text{finita}} a_i m_i$ para ciertos $a_i \in A$.
3. una **base** si ψ es un isomorfismo, es decir, si todo $m \in M$ se escribe de manera única como $m = \sum_{\text{finita}} a_i m_i$ para únicos $a_i \in A$.

Ejemplos: A diferencia de los k-ev, hay varias "patologías" que aparecen al considerar módulos. Sea $A = \mathbb{Z}$ y $M = \mathbb{Z}$, entonces:

1. $\{2,3\}$ es una familia generadora (pues $\mathrm{mcd}(2,3) = 1 \rightsquigarrow$ Bézout!). Pero no es una base de $\mathbb{Z}$: $0 = a_1 2 + a_2 3$ con $a_1 = -3$ y $a_2 = 2$.
2. $\{2\}$ es una familia l.i., pero no es generadora ($\rightsquigarrow$ "~~$\dim_{\mathbb{Z}}(\mathbb{Z}) = 1$~~")
3. **Ejercicio** Probar (eg. Bézout) que $\{1\}$ y $\{-1\}$ son las únicas bases de $M = \mathbb{Z}$.

Definición 4.2.33. — Sea M un A-módulo. Diremos que M es un módulo:

1. **finitamente generado** (o **de tipo finito**) si existe una familia generadora finita. ($i.e.$, $\exists m_1, \dots, m_r \in M$ tq $M = \langle m_1, \dots, m_r \rangle_A$)
2. **libre** si posee una base. En otras palabras, si $M \cong A^{(I)}$ para cierto conjunto I.

Recuerdo (MAT210): Todo k-ev (de dim arbitraria) posee una base

⚠ No todo A-módulo es libre: si $\exists\, I \subsetneq A$ ideal propio no-nulo ($\Leftrightarrow A$ no es cuerpo) y $M := A/I$, entonces todo $a \in I \setminus \{0\}$ cumple $am = 0$ para todo $m \in M$, $i.e.$, ∄ familias li en M.

Del mismo modo, varias propiedades típicas de k-evs de dimensión finita pueden fallar en el caso de A-módulos finitamente generados.

Ejemplos: Sea $A = \mathbb{Z}$ y $M = \mathbb{Z}$, entonces:

1. $\varphi : M \hookrightarrow M$, $m \mapsto 2m$ es inyectiva, pero no es sobreyectiva.
2. $\{2,3\}$ es una familia generadora, pero no se puede extraer una base.
3. $\{2\}$ es una familia lin. indep., pero no se puede completar en una base.

A pesar de esto, los módulos libres finitamente generados sí verifican varias propiedades análogas a los k-evs.

Teorema: Sea M un A-módulo libre finitamente generado. Entonces, todas sus bases tienen el mismo cardinal, llamado el rango (o número de Betti) de M y es denotado $\operatorname{rg}(M)$.

Dem: Sup. $M \cong A^r$ y sea $\mathfrak{m} \subsetneq A$ ideal maximal con $k := A/\mathfrak{m}$ cuerpo. Entonces,
$M/\mathfrak{m}M \cong A^r/\mathfrak{m}A^r \cong (A/\mathfrak{m})^r \cong k^r \rightsquigarrow \dim_k(M/\mathfrak{m}M) = r$ únicamente det. por M ■

Ejercicio

En particular, si $M \cong A^n$ y $N \cong A^m$ con bases $\{e_1, \dots, e_n\} \subseteq M$ y $\{f_1, \dots, f_m\} \subseteq N$, entonces todo $\varphi : N \to M$ morfismo de A-módulos está determinado por

$$\varphi(f_j) = \sum_{i=1}^{n} a_{ij} e_i \quad \text{para únicos } a_{ij} \in A$$

ie, $\mathrm{Hom}_A(N, M) \cong M_{n \times m}(A)$.

***Ejercicio* 4.2.36.** — Sean M y N dos A-módulos tales que $N \subseteq M$.

1. Probar que si M es finitamente generado y $N \subseteq M$, entonces M/N es finitamente generado.
2. Probar que si N y M/N son finitamente generados, entonces M es finitamente generado.
3. Sea $A = \mathbb{Z}[x_1, x_2, \dots] = \mathbb{Z}[x_i, i \in \mathbb{N}^{\geq 1}]$ y $M = A$ (finitamente generado por $\{1\}$). Probar que $N = \{\text{polinomios de término constante nulo}\} \subseteq M$ **no** es finitamente generado.

§37. Teorema de Cayley-Hamilton y Lema de Nakayama

Recuerdo (Clase 1, p.7): Si $R \in M_n(A)$ matriz $n \times n$, entonces

$$ {}^t\mathrm{com}(R) \cdot R = R \cdot {}^t\mathrm{com}(R) = \det(R)\, I_n $$

En part, $R \in GL_n(A) \iff \det(R) \in A^\times$

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 $R := (a_{ij})_{1 \le i,j \le n} \in M_n(A)$ y $P(X) := \det(XI_n - R)$

$$ = X^n + c_1 X^{n-1} + \dots + c_{n-1} X + c_n \in A[X] $$

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 $j \in \{1, \dots, n\}$. (★)

Ejercicio* Probar (★) comparando los coeficientes de $B \cdot {}^t\mathrm{com}(B) = P(X) \cdot I_n$, donde $B = XI_n - R$ matriz en $M_n(A[X])$.

Teorema de Cayley-Hamilton generalizado: 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

$$u(m_i) = \sum_{j=1}^{n} a_{ij} m_j \quad \text{para ciertos } a_{ij} \in A.$$

Definamos $R := (a_{ij})_{1 \le i,j \le n} \in M_n(A)$ y $P(X) := \det(XI_n - R) \in A[X]$. Entonces, $P(u) = 0$ en $\mathrm{End}_A(M)$.

Dem: Dotemos a M de estructura de $A[X]$-módulo usando $u : M \to M$ como sigue:

Si $Q \in A[X]$ y $m \in M$, definimos $Q \cdot m := Q(u)(m) \in M$ (eg. $(X^2+1)\cdot m \overset{\text{def}}{=} u^2(m) + m$)

En part, si $Q(X) = X$ entonces $Q \cdot m_i = X \cdot m_i \overset{\text{def}}{=} u(m_i) = \sum_{j=1}^{n} a_{ij} m_j$ para todo $i \in \{1, \dots, n\}$.

$$\Rightarrow \underbrace{(XI_n - R)}_{B \in M_n(A[X])} \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0 \overset{t\,\mathrm{com}(B)\cdot(\cdot)}{\Longrightarrow} \det(XI_n - R)\, I_n \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0 \Rightarrow P(X) \cdot m_i = 0 \ \forall i$$

i.e., $P(u)(m_i) = 0$ para todo $i \overset{M = \langle m_1, \dots, m_n \rangle_A}{\Longrightarrow} P(u) = 0$ en $\mathrm{End}_A(M)$ ■

Obs: Si $A = k$ es un cuerpo, recuperamos el Teorema de Cayley-Hamilton "clásico" de MAT210.