Clase 19: Módulos sobre un anillo

§33. Módulos, submódulos y morfismos

Los módulos son una generalización natural de los espacios vectoriales:

Def: Sea A un anillo. Un A-módulo (o módulo sobre A) es un grupo abeliano M dotado de una "multiplicación por escalares en A"

$$A \times M \longrightarrow M \,, \quad (a,m) \longmapsto am$$

tal que para todos $a, b \in A$ y $m, n \in M$ se cumple:

1° $a(m+n) = am + an$.

2° $(a+b)m = am + bm$ y $(ab)m = a(bm)$.

3° $1 \cdot m = m$.

Caso particular importante: Si $A = k$ es un cuerpo, entonces un k-módulo es exactamente un k-espacio vectorial.

Sin embargo, la noción de A-módulo es mucho más versátil!

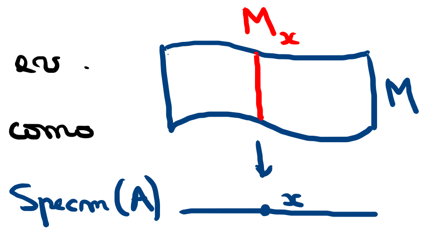
<u>Ejemplos</u>: Sea A un anillo.

1. El conjunto $\{0\}$ es un A-modulo ("trivial"), que denotaremos 0.
2. Un ideal $I \subseteq A$ es un A-módulo. En part, A es un A-módulo.
3. $A[X_1, \ldots, X_n]$ es un A-módulo.
4. $M_n(A)$ es un A-módulo.
5. A/I es un A-módulo (definiendo $a \cdot [b] := [ab]$ en A/I).
6. $A^n := \{(a_1, \ldots, a_n)$ con $a_i \in A\}$ es un A-módulo.
7. Si M y N son A-módulos, entonces $M \times N$ es un A-módulo.
8. Toda A-álgebra B es un A-módulo ("olvidar" que podemos mult. elementos de B).
9. Un $\mathbb{Z}$-módulo es lo mismo que un grupo abeliano:

   Por def, todo $\mathbb{Z}$-módulo es un grupo abeliano. Recíprocamente, si $(G,+)$ es un grupo abeliano definimos $(-1)\cdot g := -g$ y $n \cdot g := \overbrace{g + \cdots + g}^{n \text{ veces}}$ si $n \in \mathbb{N}$ ✓

Cultura general Una consecuencia del Teorema de Freyd-Mitchell (1965) es que MUCHAS situaciones en matemáticas pueden describirse usando módulos!

Interpretación Geométrica: Si $A = k$ cuerpo, un A-módulo es un k-e.v.
Para un anillo arbitrario, una forma de pensar un A-módulo M es como "una familia" de e.v. parametrizados por los puntos de $\operatorname{Specm}(A)$



Def: Un morfismo de A-módulos es $\varphi : M \to N$ morfismo de grupos abelianos que es A-lineal, ie, $\varphi(am) = a\varphi(m)$ para todo $a \in A$ y todo $m \in M$.

Notación: Dados M y N dos A-módulos, escribimos

$$\operatorname{Hom}_A(M,N) := \{\varphi : M \to N \text{ morfismo de } A\text{-módulo}\}.$$

Dicho conjunto está dotado naturalmente de estructura de A-módulo también:
Si $a \in A$ y $\varphi, \psi \in \operatorname{Hom}_A(M,N)$ definimos $a\varphi + \psi$ por $(a\varphi+\psi)(m) := a\varphi(m) + \psi(m)$ $\forall m \in M$

Si $M = N$, escribimos $\operatorname{End}_A(M) := \operatorname{Hom}_A(M,M)$ (A-módulo de endomorfismos de M).

Ejemplo ($A = k$ cuerpo): Si $M = k^n$ y $N = k^m$ entonces $\operatorname{Hom}_A(M,N) \cong M_{m\times n}(k)$
y $\operatorname{End}_A(M) \cong M_n(k)$.

Ejemplos :

① Un isomorfismo de A-módulos es un morfismo $\varphi: M \xrightarrow{\sim} N$ biyectivo. Decimos que dos A-módulos M y N son isomorfos en caso de existir un tal φ, y escribimos $M \cong N$.

$M = N$

② Sea $f: \mathbb{Z} \to \mathbb{Z}$ morfismo de $\mathbb{Z}$-módulos. Entonces, $f(1) = n$ para cierto $n \in \mathbb{Z}$ (no necesariamente $f(1) = 1$!). Luego, $\forall m \in \mathbb{Z}$ se tiene:

$$f(m) = f(m \cdot 1) \overset{\mathbb{Z}\text{-lineal}}{=} m\, f(1) = mn \quad , \text{ ie }, \quad f = \text{multiplicar por } n.$$

Así, tenemos que $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}$ (cf. $\mathrm{Hom}_{\text{anillo}}(\mathbb{Z}, \mathbb{Z}) = \{\mathrm{Id}_{\mathbb{Z}}\}$).

③ $\boxed{\text{Ejercicio}}$ Sea M un A-módulo. Probar que $\mathrm{Hom}_A(A, M) \cong M$.
Sin embargo, $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z}) = 0$ si $M = \mathbb{Z}/2\mathbb{Z}$.

④ Functorialidad: Sea $\varphi: M \to M'$ un morfismo de A-módulos y N un A-módulo. Definimos el pullback φ^* (resp. pushforward φ_*) de φ mediante:

$$\varphi^*: \mathrm{Hom}_A(M', N) \longrightarrow \mathrm{Hom}_A(M, N), \quad f \longmapsto f \circ \varphi$$

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[dr, "\varphi^*(f)"'] & M' \arrow[d, "f"] \\ & N \end{tikzcd}$$

(resp. $\varphi_*: \mathrm{Hom}_A(N, M) \to \mathrm{Hom}_A(N, M')$, $g \longmapsto \varphi \circ g$

$$\begin{tikzcd} & N \arrow[dl, "g"'] \arrow[d, "\varphi_*(g)"] \\ M \arrow[r, "\varphi"'] & M' \end{tikzcd}$$
)

$\boxed{\text{Ejercicio importante}}$: Probar que φ^* y φ_* son morfismos de A-módulos.

Definiciones: Sea M un A-módulo.

① Un submódulo de M es un subgrupo $N \subseteq M$ tal que $am \in N$ $\forall a \in A$ y $\forall n \in N$.

② Para todo subconjunto $S \subseteq M$ definimos el submódulo generado por S como el submódulo $\langle S \rangle \subseteq M$ más pequeño conteniendo a S. Explícitamente:

$$\langle S \rangle = \langle S \rangle_A := \{ a_1 m_1 + \ldots + a_n m_n \ , \ n \in \mathbb{N} \ , \ a_i \in A \ \text{y} \ m_i \in S \} \ (= \text{"}Vect_A(S)\text{"})$$

③ Decimos que M es un A-módulo finitamente generado si $\exists \, S = \{m_1, \ldots, m_r\} \subseteq M$ conjunto finito tal que $M = \langle m_1, \ldots, m_r \rangle_A$.

Atención: Sea B una A-álgebra. Entonces, decimos que B es una A-álgebra finitamente generada si existen $b_1, \ldots, b_r \in B$ tal que cada elemento de B puede escribirse como polinomio en $b_1, \ldots, b_r$ con coeficientes en A (i.e., $\exists$ morfismo de A-álgebras $A[X_1, \ldots, X_r] \twoheadrightarrow B$, $X_i \mapsto b_i$ sobreyectivo).

$\boxed{\text{Ejercicio}}$ Probar que si B es fin. generado como A-módulo, entonces lo es como A-álgebra.

Sea k un cuerpo. Entonces $k[X_1, \ldots, X_r]$ es una k-álgebra fin. generada (por $X_1, \ldots, X_n$) pero NO es un k-módulo ($= k$-ev) fin. generado $\rightsquigarrow$ Hay que especificar!

Ejemplo: Si $M = A$ (visto como A-módulo): Submódulos de A son los ideales de A!

Ejemplo principal: Sea $\varphi: M \to N$ un morfismo de A-módulos. Entonces:

a) Si $M' \subseteq M$ submódulo, entonces $\varphi(M') \subseteq N$ es un submódulo.

b) Si $N' \subseteq N$ submódulo, entonces $\varphi^{-1}(N') \subseteq M$ es un submódulo.

En particular, $\ker(\varphi) := \varphi^{-1}(0_N)$ e $\mathrm{Im}(\varphi) := \varphi(M)$ son submódulos

¿Es cierto que para todo $N \subseteq M$ submódulo existe φ tal que $N = \ker(\varphi)$?

§34. Módulos cocientes

Def: Sea M un A-módulo y $N \subseteq M$ un submódulo. Definimos el A-módulo cociente M/N como el conjunto cociente $M/\sim$ donde $m_1 \sim m_2 \iff m_1 - m_2 \in N$, y donde para $a \in A$ y $[m] \in M/N$ definimos $a \cdot [m] := [am]$. En particular, la proyección canónica $\pi: M \to M/N$, $m \mapsto [m]$ es un morfismo de A-módulos.

con $\ker(\pi) = N$

$\boxed{\text{Ejercicio}}$ Sea $N \subseteq M$ un submódulo. Probar que hay una biyección:

$$\left\{ \begin{array}{c} \text{Submódulos} \\ L \subseteq M/N \end{array} \right\} \overset{1:1}{\underset{\sim}{\longleftrightarrow}} \left\{ \begin{array}{c} \text{Submódulos } P \subseteq M \\ \text{tq } N \subseteq P \end{array} \right\}$$

$$L \longmapsto \pi^{-1}(L)$$

Tal como para grupos y anillos, tenemos

Propiedad Universal del Cociente: Sea $\varphi : M \to M'$ morfismo de A-módulos y sea $N \subseteq M$ submódulo tal que $\varphi(N) = 0$, entonces:

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[dr, "\pi"'] & M' \\ & M/N \arrow[u, "\exists!\, \hat{\varphi}"'] \end{tikzcd}$$

tal que $\varphi = \hat{\varphi} \circ \pi$

(i.e, $\hat{\varphi}([m]) = \varphi(m)$)

En part, $M/\ker(\varphi) \cong \operatorname{Im}(\varphi)$ (Noether).

Equivalentemente, esto último se puede reformular como:

Prop: Todo morfismo de A-módulos $\varphi : M \to M'$ se factoriza de manera única como

$$M \xrightarrow{\pi} M/\ker(\varphi) \xrightarrow[\sim]{\hat{\varphi}} \operatorname{Im}(\varphi) \xhookrightarrow{i} M'$$

Un nuevo ingrediente, muy usado en el contexto de módulos, es:

Def: Sea $\varphi : M \to M'$ un morfismo de A-módulos. El cokernel de φ es:

$$\operatorname{coker}(\varphi) := M' / \operatorname{Im}(\varphi).$$

En particular, φ es sobreyectivo $\Longleftrightarrow \operatorname{coker}(\varphi) = 0$.

§35. Operaciones sobre sub-módulos

A partir de una familia $\{M_\lambda\}_{\lambda\in\Lambda}$ de sub-módulos de M podemos construir lo sgte:

a) La suma $\sum_{\lambda\in\Lambda} M_\lambda$ es el submódulo generado por $\bigcup_{\lambda\in\Lambda} M_\lambda$, ie, cuyos elem. son sumas (finitas!) de la forma $\sum_{\text{finita}} x_\lambda$ con $x_\lambda \in M_\lambda$.

b) La intersección $\bigcap_{\lambda\in\Lambda} M_\lambda$ es un submódulo de M.

En part, $\bigcap_{\lambda\in\lambda} M_\lambda \subseteq \sum_{\lambda\in\Lambda} M_\lambda$. **Ejercicio** Dar un ejemplo donde $\bigcap_{\lambda\in\Lambda} M_\lambda \neq \sum_{\lambda\in\Lambda} M_\lambda$.

Tal como para anillos (cf. §32) tenemos que:

1. Si $N \subseteq P \subseteq M$ son A-módulos, entonces

$$(M/N)/(P/N) \cong M/P$$

2. Si $N_1, N_2 \subseteq M$ son A-modulos, entonces la composición

$$N_2 \hookrightarrow N_1 + N_2 \twoheadrightarrow (N_1+N_2)/N_1$$ es sobreyectiva con kernel $N_1 \cap N_2$

Noether $\Rightarrow$ $$(N_1+N_2)/N_1 \cong N_2/(N_1\cap N_2) \quad \blacksquare$$

Los conceptos discutidos hasta ahora son análogos al caso de espacios vectoriales. Veamos algunos nuevos, que aprovechan la existencia de ideales no-triviales en A:

Def: Sea M un A-módulo, sean $N, P \subseteq M$ submódulos y sea $I \subseteq A$ un ideal:

a) Definimos el submódulo $IM \subseteq M$ mediante

$$IM := \langle \{am\}_{a\in I,\, m\in M} \rangle \overset{\text{def}}{=} \Big\{ \sum_{\text{finita}} a_i m_i \text{ con } a_i \in I \text{ y } m_i \in M \Big\}.$$

b) Definimos el ideal $(N:P) \subseteq A$ mediante

$$(N:P) := \{ a \in A \text{ tal que } am \in N \text{ para todo } m \in P \}.$$

c) Definimos el anulador (o aniquilador) de $N \subseteq M$ como $\operatorname{ann}(N) := (0:N) \subseteq A$.
Explícitamente, $\operatorname{ann}(N) = \{ a \in A \text{ tal que } am = 0 \text{ para todo } m \in N \}$.

Obs: Notamos que el A-módulo cociente M/IM puede ser dotado de estructura de A/I-módulo: si $[a] \in A/I$ y $[m] \in M/IM$, definimos $[a]\cdot[m] := [am]$ (bien definido, pues si $a - a' = b \in I$ y $m - m' = n \in IM \Rightarrow am - a'm' = a'n + bm' + bn \in IM$).

$\rightsquigarrow$ En part, si $\mathfrak{m} \subseteq A$ ideal maximal entonces $M/\mathfrak{m}M$ es un $(A/\mathfrak{m})$-e.v.

Ejemplos:

1. Si $A = k$ cuerpo, $M = V$ k-ev no-nulo y $N = W \neq 0$ sub-ev $\Rightarrow$ $\operatorname{ann}(N) = \langle 0 \rangle \subseteq k$.
2. El A-módulo $M = A/I$ cumple $\operatorname{ann}(A/I) = I$.
3. Sean I, J submódulos del A-módulo $M = A$ (i.e., ideales). Entonces

$$(I : J) \overset{\text{def}}{=} \{ a \in A \text{ tal que } ab \in I \text{ para todo } b \in J \}$$

$\boxed{\text{Ejercicio}}$ Sea $A = \mathbb{Z}$ y sean $I = n\mathbb{Z}$, $J = m\mathbb{Z}$ con $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ y $m = p_1^{\beta_1} \cdots p_r^{\beta_r}$ para p_i primo y $\alpha_i, \beta_i \in \mathbb{N}$. Probar que

$$(I : J) = \langle p_1^{\gamma_1} \cdots p_r^{\gamma_r} \rangle \subseteq \mathbb{Z}, \quad \text{con } \gamma_i := \max\{\alpha_i - \beta_i, 0\}.$$