Álgebra II

Franco Rufolo

24 de octubre de 2025

Definición. Sea R un anillo. Un R**-módulo a izquierda** es un par (M, ρ), donde M es un grupo abeliano y

$$\begin{aligned} \rho : R &\longrightarrow \mathrm{End}(M) \\ a &\longmapsto \rho_a \end{aligned}$$

es un morfismo de anillos.

Observación. Que ρ sea un morfismo de anillos significa que $\rho_1 = \mathrm{id}_M$ y que $\rho_{ab} = \rho_a \rho_b$, $\rho_{a+b} = \rho_a + \rho_b$ para todos $a, b \in R$. En términos de elementos esto nos dice que, notando $\rho_a(m) = a \cdot m = am$,

$$1m = m, \qquad a(bm) = (ab)m, \qquad (a+b)m = am + bm$$

para todos $m \in M$, $a, b \in R$. Además, como $\rho_a \in \mathrm{End}(M)$ para todo $a \in R$, vale

$$a(m+n) = am + an$$

para todos $a \in R$ y $m, n \in M$. Una definición equivalente de R-módulo a izquierda es un grupo abeliano M con una función $R \times M \to M$, $(a, m) \mapsto am$ que satisface las cuatro condiciones anteriores. Un R-módulo a derecha es un grupo abeliano M con una función $M \times R \to M$ que satisface condiciones simétricas respecto de las anteriores.

Cuando digamos R-módulo, nos estaremos refiriendo a la estructura a izquierda.

Definición. Sea M un R-módulo. Un **submódulo** de M es un subgrupo $N \leq M$ tal que $an \in N$ para todos $a \in R$ y $n \in N$.

Ejemplos.

- R es un R-módulo via $a \cdot b = ab$. Sus submódulos son sus ideales a izquierda.
- El grupo abeliano 0 es un R-módulo para todo anillo R.
- Si K es un cuerpo, un K-módulo es lo mismo que un K-espacio vectorial. Los submódulos son los subespacios vectoriales.
- Para un grupo abeliano M cualquiera, sabemos que $\mathrm{End}(M)$ es un anillo. Luego, existe un único morfismo de anillos $\mathbb{Z} \to \mathrm{End}(M)$, es decir, una única estructura de $\mathbb{Z}$-módulo sobre M. Concretamente, es $k \cdot m = \underbrace{m + \cdots + m}_{k \text{ veces}}$ si $k > 0$, y es análogo para $k < 0$. Los submódulos son los subgrupos de M.
- Todo grupo abeliano M es un R-módulo, con $R = \mathrm{End}(M)$, via $f \cdot m = f(m)$. Esto se corresponde con el morfismo de anillos $\mathrm{id} : R \to \mathrm{End}(M)$.

- Si M es un R-módulo a izquierda, es un R^{op}-módulo a derecha via $m \cdot a = am$. En particular, si R es conmutativo, todo R-módulo a izquierda es un R-módulo a derecha.

- Si R es conmutativo y M es un R-módulo, se define su **torsión** como el conjunto

$$t(M) = \{m \in M : \text{existe } a \in R \setminus \{0\} \text{ tal que } am = 0\}.$$

  Ya sabíamos que es un subgrupo de M. Además, si R es un dominio íntegro, $t(M)$ es un submódulo de M. Se dice que M es **de torsión** si $t(M) = M$ y **sin torsión** o **libre de torsión** si $t(M) = 0$.

- Si K es un cuerpo, V es un K-espacio vectorial y $T \in \mathrm{End}_K(V)$ es un endomorfismo lineal de V, entonces podemos extender la acción de K en V a una acción de $K[x]$ en V via $x \cdot v = T(v)$. Es decir, si $p \in K[x]$, entonces

$$p \cdot v = \left(\sum_{i=0}^{n} a_i x^i \right) \cdot v = \sum_{i=0}^{n} a_i T^i(v),$$

  donde T^i es la composición de T consigo misma i veces. Es directo verificar que esto define una estructura de $K[x]$-módulo en V.

  Recíprocamente, si V es un $K[x]$-módulo, entonces es un K-espacio vectorial (restringiendo la acción) y tenemos un endomorfismo lineal $T \in \mathrm{End}_K(V)$ dado por $v \mapsto x \cdot v$. Es decir, hay una correspondencia biunívoca entre los $K[x]$-módulos con los K-espacios vectoriales junto con un endomorfismo lineal $T \in \mathrm{End}_K(V)$.

  Los submódulos W de un $K[x]$-módulo V son, en primer lugar, subespacios vectoriales. Además, necesitamos que $x \cdot W \subseteq W$, es decir, en términos del endomorfismo lineal T, $T(W) \subseteq W$, o sea que W sea T-invariante. Esta condición asegura que W es T^i-invariante para todo i, y todo subespacio T-invariante de V es un submódulo. Es decir, los submódulos de V son los subespacios T-invariantes de V.

Observación. Intersección de submódulos es nuevamente un submódulo. Luego, dado un subconjunto X de un R-módulo M, podemos definir el submódulo generado por X como el menor submódulo de M que contiene a X. Explícitamente:

$$\langle X \rangle = \left\{ \sum_{i=1}^{n} a_i x_i : a_i \in R, x_i \in X \right\}.$$

Como siempre, si $X = \{x_1, \ldots, x_n\}$ notaremos $\langle X \rangle = \langle x_1, \ldots, x_n \rangle$.

Definición. Un R-módulo M es **finitamente generado (o de tipo finito)** si existen $x_1, \ldots, x_n \in M$ tales que $M = \langle x_1, \ldots, x_n \rangle$. Si se puede tomar $x \in M$ con $M = \langle x \rangle$, M se dice **cíclico**.

Ejemplos.

- R es cíclico como R-módulo: $R = \langle 1 \rangle$.

- Tener un $\mathbb{Z}$-módulo finitamente generado es equivalente a tener un grupo abeliano finitamente generado.

- Si K es un cuerpo, un K-módulo finitamente generado es precisamente un K-espacio vectorial de dimensión finita.

- Un submódulo de un módulo finitamente generado no tiene por qué serlo. Por ejemplo, $R = K[x_n]_{n \in \mathbb{N}}$, donde K es un cuerpo, es finitamente generado como R-módulo pero el submódulo (es decir, el ideal) $\langle x_n : n \in \mathbb{N} \rangle$ no es finitamente generado.

Definición. Dados dos R-módulos M y N, un **morfismo de módulos** de M en N es un morfismo de grupos $f : M \to N$ tal que $f(am) = af(m)$ para todos $a \in R$ y $m \in M$. Decimos que f es un **monomorfismo** si es inyectivo, que es un **epimorfismo** si es sobreyectivo y que es un **isomorfismo** si es biyectivo.

Ejemplos.

- Para todo R-módulo M, id_M es un morfismo.
- Si $f : M \to N$ y $g : N \to T$ son morfismos de R-módulos, entonces $gf : M \to T$ es un morfismo de R-módulos.
- Si M y N son $\mathbb{Z}$-módulos, los morfismos de módulos $f : M \to N$ son exactamente los morfismos de grupos de M en N.
- Si V, W son $K[x]$-módulos, donde K es un cuerpo, consideremos los endomorfismos lineales asociados $T_V \in \mathrm{End}_K(V)$ y $T_W \in \mathrm{End}_K(W)$. Si $f : V \to W$ es un morfismo, entonces $fT_V(v) = f(xv) = xf(v) = T_W f(v)$ para todo $v \in V$. Es decir, conmuta el diagrama
$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ {\scriptstyle T_V}\downarrow & & \downarrow{\scriptstyle T_W} \\ V & \xrightarrow{f} & W. \end{array}$$
Recíprocamente, si $f : V \to W$ es un morfismo de grupos tal que $fT_V = T_W f$, entonces
$$f(xv) = fT_V(v) = T_W f(v) = xf(v)$$
para todo $v \in V$. Usando su aditividad, deducimos que $f(pv) = pf(v)$ para todo $p \in K[x]$, es decir que f es un morfismo de $K[x]$-módulos.

Observación. Si $f : M \to N$ es un morfismo, entonces $\ker f$ e $\operatorname{im} f$ son submódulos de M y N, respectivamente. Más aún, para todo submódulo S de M, $f(S)$ es un submódulo de N y para todo submódulo T de N, $f^{-1}(T)$ es un submódulo de M.

Definición. Sea $f : M \to N$ un morfismo de R-módulos.

- f es una **sección** si existe un morfismo $g : N \to M$ tal que $gf = \mathrm{id}_M$.
- f es una **retracción** si existe un morfismo $g : N \to M$ tal que $fg = \mathrm{id}_N$.

Observación. Una sección es necesariamente un monomorfismo y una retracción es necesariamente un epimorfismo. Las vueltas de estas implicaciones no valen. Por ejemplo, la inclusión $2\mathbb{Z} \to \mathbb{Z}$ es un monomorfismo que no es una sección, ya que si $g : \mathbb{Z} \to 2\mathbb{Z}$ es un morfismo, sea $k \in \mathbb{Z}$ tal que $g(1) = 2k$; luego, $g(2l) = 2l2k = 4lk \neq 2l$.

Definición. Dados M y N dos R-módulos, se define
$$\mathrm{Hom}_R(M, N) = \{f : M \to N : f \text{ es morfismo de } R\text{-módulos}\}.$$

Este conjunto es un grupo abeliano con la suma coordenada a coordenada. Para darle más estructura, introducimos primero una definición interesante en sí misma.

Definición. Sean R, S anillos. Un grupo abeliano M es un (R, S)-bimódulo si es un R-módulo a izquierda, un S-módulo a derecha, y dichas estructuras son compatibles, en el sentido de que $r(ms) = (rm)s$ para todos $r \in R$, $m \in M$, $s \in S$.

Observación. Todo R-módulo a izquierda es un $(R, \mathbb{Z})$-bimódulo y todo R-módulo a derecha es un $(\mathbb{Z}, R)$-bimódulo.

Sean R, S, T anillos. Si M es un (R, S)-bimódulo y N es un (R, T)-bimódulo, entonces $\mathrm{Hom}_R(M, N)$ es un (S, T)-bimódulo, con acciones dadas por
$$(sf)(m) = f(ms) \quad \text{y} \quad (ft)(m) = f(m)t.$$
Las acciones son compatibles: $(s(ft))(m) = (ft)(ms) = f(ms)t = (sf)(m)t = ((sf)t)(m)$.

(Co)productos de módulos

Dada una familia de R-módulos $(M_i)_{i\in I}$, se puede considerar su producto cartesiano $\prod_{i\in I} M_i$, que es un grupo abeliano con la operación coordenada a coordenada. Más aún, es un R-módulo con la operación dada por $a(m_i)_{i\in I} = (am_i)_{i\in I}$.

Definición. El **producto directo** de la familia $(M_i)_{i\in I}$ es el R-módulo recién definido.

Tenemos funciones distinguidas, que son las proyecciones a cada coordenada:

$$\begin{aligned} \pi_j : \prod_{i\in I} M_i &\longrightarrow M_j \\ (m_i)_{i\in I} &\longmapsto m_j. \end{aligned}$$

La operación definida es la única que hace de estas morfismos de R-módulos. El producto directo junto con las proyecciones cumplen lo siguiente.

Proposición (Propiedad universal del producto directo)**.** Sean $(M_i)_{i\in I}$ una familia de R-módulos, N un R-módulo y para cada $i \in I$ un morfismo de R-módulos $f_i : N \to M_i$. Entonces existe un único morfismo de R-módulos $f : N \to \prod_{i\in I} M_i$ tal que $f_j = \pi_j f$ para todo $j \in I$. Es decir, tal que para cada $j \in I$ conmuta el siguiente diagrama:

$$\begin{tikzcd} & \prod_{i\in I} M_i \arrow[d, "\pi_j"] \\ N \arrow[ur, dashed, "\exists! f"] \arrow[r, "f_j"'] & M_j. \end{tikzcd}$$

Demostración. Definimos f como $f(x) = (f_i(x))_{i\in I}$, la cual es la única que cumple

$$f_j = \pi_j f$$

para todo $j \in I$. Es también un morfismo de R-módulos, pues:

- $f(x+y) = (f_i(x+y))_{i\in I} = (f_i(x)+f_i(y))_{i\in I} = (f_i(x))_{i\in I} + (f_i(y))_{i\in I} = f(x) + f(y)$.
- $f(ax) = (f_i(ax))_{i\in I} = (af_i(x))_{i\in I} = a(f_i(x))_{i\in I} = af(x)$.

■

Corolario. La función

$$\begin{aligned} \varphi : \operatorname{Hom}_R\Big(N, \prod_{i\in I} M_i\Big) &\longrightarrow \prod_{i\in I} \operatorname{Hom}_R(N, M_i) \\ f &\longmapsto (\pi_i f)_{i\in I} \end{aligned}$$

es un isomorfismo de grupos abelianos.

Dado un elemento $(m_i)_{i\in I} \in \prod_{i\in I} M_i$, se define su soporte

$$\operatorname{sop}((m_i)_{i\in I}) = \{i \in I : m_i \neq 0\}.$$

Definición. La **suma directa** de la familia $(M_i)_{i\in I}$ es el submódulo del producto directo dado por

$$\bigoplus_{i\in I} M_i = \{x : |\operatorname{sop}(x)| < \infty\}.$$

Las funciones distinguidas en este caso son las inclusiones de cada coordenada: $\iota_j : M_J \to \bigoplus_{i\in I} M_i$, donde $(\iota_j(m))_i = \delta_{i,j} m$. Son morfismos de R-módulos, y dotan a la suma directa de una propiedad universal:

Proposición (Propiedad universal de la suma directa)**.** Sean $(M_i)_{i\in I}$ una familia de R-módulos, N un R-módulo y para cada $i \in I$ un morfismo de R-módulos $f_i : M_i \to N$. Entonces existe un único morfismo de R-módulos $f : \bigoplus\limits_{i\in I} M_i \to N$ tal que $f_j = f\iota_j$ para todo $j \in I$. Es decir, el siguiente diagrama conmuta para todo $j \in I$:

$$\begin{tikzcd}
M_j \arrow[r, "f_j"] \arrow[d, "\iota_j"] & N \\
\bigoplus\limits_{i\in I} M_i \arrow[ur, dashed, "\exists! f"'] &
\end{tikzcd}$$

Demostración. Dado $m \in \bigoplus\limits_{i\in I} M_i$, se tiene que $m = \sum\limits_{i\in I} \iota_i(\pi_i(m))$, donde la suma tiene sentido porque hay solamente finitos sumandos no nulos. Luego, para que f cumpla lo deseado, debe definirse como $f(m) = \sum\limits_{i\in I} f_i(\pi_i(m))$. Queda como ejercicio ver que esta asignación es un morfismo de R-módulos. ■

Corolario. La función

$$\begin{aligned}
\varphi : \mathrm{Hom}_A\Big(\bigoplus_{i\in I} M_i, N\Big) &\longrightarrow \prod_{i\in I} \mathrm{Hom}_A(M_i, N) \\
f &\longmapsto (f\iota_i)_{i\in I}
\end{aligned}$$

es un isomorfismo de grupos abelianos.