# 1. Módulos

**Definición 1.1.** Sea $R$ un anillo (no necesariamente con identidad). Un *$R$-módulo a izquierda* es un grupo abeliano $(M,+)$ junto con una aplicación $R \times M \to M$, denotada por $(r,x) \mapsto rx$ que satisface para todos $r,s \in R$, $x,y \in M$,

(i) $r(sx) = (rs)x$ (asociatividad);

(ii) $(r+s)x = rx + sx$ (distributividad con respecto a la suma en $R$);
$r(x+y) = rx + ry$ (distributividad con respecto a la suma en $M$).

Además, si $R$ tiene identidad, pediremos

(iii) $1x = x$ (también se dice que $M$ es unitario)

Para abreviar diremos simplemente que $M$ es un $R$-módulo (a izquierda). Una notación que usaremos más adelante es ${}_RM$.

**Ejemplo 1.2.** (i) Uno de los ejemplos más sencillos, y del cual la definición de módulo es una generalización inmediata es el siguiente. Si $\mathbb{K}$ es un cuerpo y $V$ un $\mathbb{K}$-espacio vectorial, entonces $V$ es un $\mathbb{K}$-módulo unitario. Si bien estos módulos son importantes, ya han sido estudiado en materias anteriores y no nos proveen nueva intuición. En este curso los ejemplos más interesantes serán módulos sobre anillos que no son cuerpos.

(ii) Todo grupo abeliano $A$ tiene una estructura de $\mathbb{Z}$-módulo definiendo para $n > 0$,

$$nx = \underbrace{x + x + \cdots x}_{n \text{ veces}}$$

y extendiendo esta definición para $n \in \mathbb{Z}$ de la manera obvia. Estos ejemplos también los hemos estudiado anteriormente, pero la teoría de módulos nos ayudará a obtener resultados estructurales no triviales sobre grupos abelianos, como veremos más adelante.

(iii) Otro ejemplo sencillo e importante es el siguiente. Todo anillo $R$ es un $R$-módulo a izquierda. Más generalmente, si $I \subset R$ es un ideal a izquierda, entonces $I$ es un $R$-módulo a izquierda (con la multiplicación de $R$).

**Ejemplo 1.3.** El siguiente ejemplo será muy importante para entender uno de los resultados centrales de este curso. Es conveniente tratar de entenderlo bien, ya que volveremos sobre él muchas veces. Sean $\mathbb{K}$ un cuerpo, $V$ un $\mathbb{K}$-espacio vectorial y $T : V \to V$ una transformación lineal. Entonces $V$ tiene una estructura natural de $\mathbb{K}[x]$-módulo con la multiplicación definida por

$$fv = f(T)v$$

para $f \in \mathbb{K}[x]$ y $v \in V$. Aclaremos un poco la notación: si $f = f_0 + f_1 x + \cdots + f_n x^n$, entonces $p(T) = f_0 I + f_1 T + \cdots + f_n T^n$, y así

$$fv = f_0 v + f_1 Tv + f_2 T^2 v + \cdots + f_n T^n v.$$

Observar que esta estructura depende de la elección de $T$, de hecho otra forma de presentar este ejemplo sería diciendo que *una transformación lineal de $V$ en $V$ es una estructura de $\mathbb{K}[x]$ módulo en $V$*. Analicemos algunos casos particulares.

- Si $T = 0$, entonces $fv = f_0 v$ y en algún sentido (que precisaremos más adelante) la estructura de módulo que obtenemos es la misma que la estructura de espacio vectorial que ya teníamos en $\mathbb{V}$.
- Si $T = I$, entonces

$$fv = f_0 v + f_1 v + \cdots + f_n v = (f_0 + f_1 + \cdots + f_n)v$$

**Ejercicio 1.4.** Probar que si $V$ es un $\mathbb{K}[x]$-módulo, entonces existe una transformación lineal $T : V \to V$ tal que la estructura de $\mathbb{K}[x]$-módulo que vimos en el ejemplo anterior coincide con la dada. Observar que tiene sentido pedir que $T$ sea $\mathbb{K}$ lineal pues $V$ es por hipótesis un $\mathbb{K}[x]$-módulo y $\mathbb{K}$ es un subanillo de $\mathbb{K}[x]$.

A modo de ejercicio verificar las siguientes propiedades elementales (la demostraciones son casi las mismas que las que se dan para espacios vectoriales). Si $M$ es un $R$-módulo entonces:

- $r0 = 0$ para todo $r \in R$ (aquí el 0 denota el elemento nulo de $M$);
- $0x = 0$ para todo $x \in M$ (aquí el 0 denota el elemento nulo de $R$ y de ahora en más no haremos este tipo de aclaraciones si se pueden deducir del contexto);
- $(r - s)x = rx - sx$ para todos $r, s \in R$, $x \in M$;
- $r(x - y) = rx - ry$ para todos $r \in R$, $x, y \in M$;
- si $R$ tiene identidad, entonces $(-1)x = -x$ para todo $x \in M$.

*Observación* 1.5. Sea $A$ un grupo abeliano, recordemos que

$$\mathrm{End}_{\mathbb{Z}}(A) = \{f : A \to A : f(x + y) = f(x) + f(y) \text{ para todos } x, y \in A\}$$

es un anillo con identidad (no necesariamente conmutativo) con las operaciones definidas como

$$(f + g)(x) = f(x) + g(x)$$
$$(fg)(x) = f(g(x))$$

para todos $f, g \in \mathrm{End}_{\mathbb{Z}}(A)$, $x, y \in A$. Este anillo será muy importante en esta materia y se llama el *anillo de endomorfismos de A*.

El siguiente resultado caracteriza las estructuras de módulo en términos de morfimos de otras estructuras conocidas. De hecho nos da una definición categórica, resumida y elegante de $R$-módulo, que es un poco abstracta, pero no requiere de una lista de axiomas sobre las operaciones (como cuando se estudia la definición de espacio vectorial en álgebra lineal).

**Proposición 1.6.** *Sean $A$ un grupo abeliano y $R$ un anillo. Existe una correspondencia biyectiva entre las estructuras de $R$-módulo a izquierda en $A$ y los morfimos de anillos $R \to \mathrm{End}_{\mathbb{Z}}(A)$. Más aún, si $A$ tiene identidad, los $R$-módulos unitarios se corresponden con los morfimos de anillo con identidad.*

*Demostración.* Sea $A$ un $R$-módulo y para cada $r \in R$ sea $\alpha_r(x) = rx$. Sigue que $\alpha_r \in \mathrm{End}_{\mathbb{Z}}(A)$ pues $\alpha_r(x+y) = r(x+y) = rx+ry = \alpha_r(x)+\alpha_r(y)$. Además, $alpha_{rs} = \alpha_r \circ \alpha_s$ pues $\alpha_{rs}(x) = (rs)x = r(sx) = \alpha_r(\alpha_s(x))$. Luego la función $r \mapsto \alpha_r$ es un morfismo de anillos $R \to \mathrm{End}_{\mathbb{Z}}(A)$. Además notar que si $R$ tiene identidad y $A$ es unitario, vale $\alpha_1 = \mathrm{id}_A$.

Recíprocamente, sean $A$ un grupo abeliano y $\alpha : R \to \mathrm{End}_{\mathbb{Z}}(A)$ un morfismo de anillos. Definimos $rx = \alpha(r)(x)$. Entonces se tiene que

$$(rs)x = \alpha(rs)(x) = (\alpha(r) \circ \alpha(s))(x) = \alpha(r)(\alpha(s)(x)) = r(sx)$$

y

$$r(x+y) = \alpha(r)(x+y) = \alpha(r)(x) + \alpha(r)(y) = rx + ry,$$

de donde sigue que $A$ es un $R$-módulo. Además, si $A$ es unitario tenemos que $\alpha(1) = \mathrm{id}_A$. □

**Ejemplo 1.7.** El siguiente ejemplo es muy sencillo y de paso nos muestra que a veces podemos considerar distintas estructuras algebraicas sobre un mismo objeto grupo abeliano). Es importante también aprender a distinguir del contexto que tipo de estructura estamos considerando. $\mathbb{Z}_3$ (grupo abeliano) no admite estructura de $\mathbb{Z}_2$-módulo. En efecto, sabemos que $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}_3) \simeq \mathbb{Z}_3$ (isomorfismo de anillos), pero no existe un morfismo de anillos no trivial $\mathbb{Z}_2 \to \mathbb{Z}_3$ (¿por qué?).

# 2. Módulos a derecha

Observemos que en la Definición 1.1, es arbitrario que los elementos del anillo multipliquen por la izquierda. Uno podría hacer lo mismo trabajando por la derecha.

**Definición 2.1.** Sea $R$ un anillo (no necesariamente con identidad). Un *$R$-módulo a derecha* es un grupo abeliano $(M,+)$ junto con una aplicación $M \times R \to M$, denotada por $(x,r) \mapsto xr$ que satisface para todos $r,s \in R$, $x,y \in M$,

(i) $(xr)s = x(rs)$ (asociatividad);

(ii) $x(r+s) = xr + xs$ (distributividad con respecto a la suma en $R$);
$(x+y)r = xr + yr$ (distributividad con respecto a la suma en $M$).

Además, si $R$ tiene identidad, pediremos

(iii) $x1 = x$ (también se dice que $M$ es unitario)

La notación que usaremos para módulos a derecha es $M_R$.

*Observación* 2.2. Recordemos que si $(R,+,\cdot)$ es un anillo opuesto de $R$ es $(R,+,\cdot_{\mathrm{op}})$ en donde el producto opuesto se define por

$$r \cdot_{\mathrm{op}} s = s \cdot r.$$

En general abusaremos de la notación y denotaremos al anillo opuesto simplemente por $R^{\mathrm{op}}$ (y tampoco usaremos el punto para el producto en $R$).

**Ejercicio* 2.3.** Dar un ejemplo de un anillo $R$ tal que $R^{\mathrm{op}}$ no sea isomorfo a $R$.

El siguiente resultado nos dice que el estudio de los módulos a derecha, se reduce al estudio de los módulos a izquierda (o sea, cada vez que probemos un teorema para módulos a izquierda, automáticamente tendremos un teorema para módulos a derecha).

**Proposición 2.4.** *Todo $R$-módulo (unitario) a derecha es un $R^{\mathrm{op}}$-módulo (unitario) a izquierda y viceversa.*

*Demostración.* Sea $M$ un $R$-módulo a derecha. Definimos una multiplicación a izquierda $R^{\mathrm{op}} \times M \to M$ por

$$rx = xr, \qquad r \in R^{\mathrm{op}},\, x \in M$$

Verificamos fácilmente la asociatividad

$$r(sx) = (sx)r = (xs)r = x(sr) = x(r \cdot_{\mathrm{op}} s) = (r \cdot_{\mathrm{op}} s)x$$

y las dos leyes distributivas

$$(r+s)x = x(r+s) = xr + xs = rx + sx,$$

$$r(x+y) = (x+y)r = xr + yr = rx + ry.$$

Si además $R$ tiene identidad, entonces vale $1x = x1 = x$. □

Observemos que si $R$ es un anillo conmutativo, entonces $R = R^{\mathrm{op}}$.

**Corolario 2.5.** *Si $R$ es conmutativo, entonces todo $R$-módulo a izquierda es un $R$-módulo a derecha y viceversa.*

De ahora en adelante, y salvo que aclaremos lo contrario, $R$-módulo significará $R$-módulo a izquierda.

# 3. Submódulos

**Definición 3.1.** Sea $M$ un $R$-módulo. Un *submódulo* $A$ de $M$ es un subgrupo de $(M, +)$ tal que $rx \in A$ para todos $r \in R$, $x \in A$.

Observemos que si $A$ es un submódulo de $M$, entonces $A$ resulta un $R$-módulo con la restricción de la multiplicación por elementos de $R$.

**Ejemplo 3.2.** (i) Si $M$ es un $R$-módulo, entonces $\{0\}$ y $M$ son submódulos de $M$. En general abusaremos de la notación, denotando el submódulo trivial $\{0\}$ simplemente por 0.

(ii) Los submódulos de un espacio vectorial son sus subespacios.

(iii) Los submódulos de un grupo abeliano (considerado como $\mathbb{Z}$-módulo) son sus subgrupos.

(iv) Los submódulos de ${}_RR$ (resp. $R_R$) son los ideales a izquierda (resp. derecha).

**Proposición 3.3.** (i) *La intersección de una familia arbitraria de submódulos de $M$ es un submódulo de $M$.*

(ii) *La unión de una familia $\{A_i\}_{i\geq 0}$ de submódulos de $M$ tal que $A_i \subset A_{i+1}$ es un submódulo de $M$. Más generalmente, la unión de una familia dirigida[1] de submódulos de $M$, es un submódulo de $M$.*

*Demostración.* Ejercicio. □

**Definición 3.4.** Sean $M$ un $R$-módulo y $S$ un subconjunto de $M$. El *submódulo generado por $S$* se define como la intersección de todos los submódulos de $M$ que contienen a $S$.

Observemos que por la Proposición 3.3, $\langle S\rangle$ es un submódulo de $M$.

**Proposición 3.5.** *Sean $M$ un $R$-módulo unitario y $S$ un subconjunto de $M$. Entonces*

$$\langle S\rangle = \{r_1x_1 + \cdots + r_nx_n : n \in \mathbb{N},\, r_i \in R\, x_i \in S\}$$

*Demostración.* Ejercicio. □

**Ejercicio 3.6.** Dar una versión de la Proposición 3.5 para un anillo sin identidad.

**Ejemplo 3.7.** Sean $\mathbb{K}$ un cuerpo, $V$ un $\mathbb{K}$-espacio vectorial y $T : V \to T$ una transformación lineal. Consideremos en $V$ la estructura de $\mathbb{K}[x]$-módulo dada por $fv = f(T)v$. ¿Cuáles son los submódulos de $V$? En primer lugar, notemos que si $W$ es un submódulo de $V$, entonces es un subespacio, pues si $f = f_0 \in \mathbb{K}$ es un polinomio constante y $w \in W$, entonces $fw = f_0w \in W$ (y además $(W, +)$ es un subgrupo de $(V, +)$). Por otro lado, si $f = x$, entonces $fw = Tw \in W$. O sea $W$ es un subespacio $T$-invariante. Recíprocamente, es fácil ver que cualquier subespacio $T$-invariante de $V$ es un submódulo.

**Definición 3.8.** (i) Un $R$-módulo $M$ se dice *finitamente generado* si existe un subconjunto finito $S \subset M$ tal que $\langle S\rangle = M$.

(ii) El *submódulo cíclico* generado por $x \in M$ es $Rx = \{rx : r \in M\}$. (Ojo: no necesariamente vale $Rx = \langle\{x\}\rangle$.)

(iii) Si $\{A_i\}_{i\in I}$ es una familia de submódulos de $M$, se define la *suma de* $\{A_i\}_{i\in I}$ como

$$\sum_{i\in I} A_i = \left\{\sum_{i\in I} a_i : a_i \in A_i,\, a_i = 0 \text{ p.c.t. } i\right\}.$$

Aclaración: la abreviatura "$a_i = 0$ p.c.t. $i$" se lee "$a_i = 0$ para casi todo $i$" y en este contexto significa que a lo sumo una cantidad finita de $a_i$ son distintos de cero, que es lo lógico si pretendemos sumarlos.

**Proposición 3.9.** *Sea $\{A_i\}_{i\in I}$ una familia de submódulos de $M$, entonces*

$$\sum_{i\in I} A_i = \left\langle \bigcup_{i\in I} A_i \right\rangle.$$

[1] Una familia $\{A_i\}_{i\in I}$ se dice *dirigida* si para todos $i, j \in I$ existe $k \in I$ tal que $A_i \subset A_k$ y $A_j \subset A_k$. En particular, una cadena de submódulos de $M$ es una familia dirigida.

*Demostración.* Observar que $\sum_{i\in I} A_i$ es un submódulo de $M$. En efecto,

$$\sum_{i\in I} a_i + \sum_{i\in I} a_i' = \sum_{i\in I}(a_i + a_i') \in \sum_{i\in I} A_i$$

y

$$r\sum_{i\in I} a_i = \sum_{i\in I} ra_i \in \sum_{i\in I} A_i,$$

en donde $r \in R$ y $a_i, a_i' \in A_i$ son nulos p.c.t. $i$. Además $A_j \subset \sum_{i\in I} A_i$ para todo $j \in I$, luego $\bigcup_{i\in I} A_i \subset \sum_{i\in I} A_i$, de donde sigue que $\langle \bigcup_{i\in I} A_i \rangle \subset \sum_{i\in I} A_i$. A su vez, si $A$ es un submódulo de $M$ que contiene a $\bigcup_{i\in I} A_i$, entonces $\sum_{i\in I} a_i \in A$, y por ende $\sum_{i\in I} A_i \subset A$. Luego $A \subset \langle \bigcup_{i\in I} A_i \rangle$. □

# 4. Morfismos

**Definición 4.1.** Sean $A, B$ dos $R$-módulos. Una función $\varphi : A \to B$ se dice un *morfismo de $R$-módulos* si

$$\varphi(x + yf) = \varphi(x) + \varphi(y)$$

y

$$\varphi(rx) = r\varphi(x)$$

para todos $x, y \in A$, $r \in R$. Como siempre, si además $\varphi$ es inyectiva se dice un *monomorfismo*, si es suryectiva se dice un *epimorfismo* y si es biyectiva se dice un *isomorfismo*. Un morfismo (resp. isomorfismo) de un $R$-módulo en sí mismo también se llama endomorfismo (resp. *automorfismo*).

Las siguientes propiedades se verifican fácilmente:

(i) $\mathrm{id} : M \to M$ es un (iso)morfismo de módulos; $0 : M \to M$ es un morfismo de módulos;

(ii) si $\varphi : A \to B$ y $\psi : B \to C$ son morfismos de $R$-módulos entonces $\psi \circ \varphi : A \to C$ es un morfismo de $R$-módulos;

(iii) si $\varphi, \psi : A \to B$ son dos morfismos de $R$-módulos, entonces $\varphi + \psi$ es un morfismo de $R$-módulos, en donde $(\varphi + \psi)(x) = \varphi(x) + \psi(x)$, luego

$$\mathrm{Hom}_R(A, B) = \{\varphi : A \to B : \varphi \text{ es un morfismo de } R\text{-módulos}\}$$

es un grupo abeliano.

**Proposición 4.2.** *Sea $\varphi : A \to B$ un morfismo de $R$-módulos.*

(i) *Si $C$ es un submódulo de $A$, entonces $\varphi(C)$ es un submódulo de $B$.*

(ii) *Si $D$ es un submódulo de $B$, entonces $\varphi^{-1}(D) = \{x \in A : \varphi(x) \in D$ es un submódulo de $A$.*

*Demostración.* Es estándar y queda como ejercicio. □

**Corolario 4.3.** *Si $\varphi : A \to B$ es un morfismo de $R$-módulos, entonces*

$$\ker \varphi = \{x \in A : \varphi(x) = 0\} = \varphi^{-1}(\{0\})$$

*es un submódulo de $A$.*

**Ejemplo 4.4.** Sean $V$ un $\mathbb{K}$-espacio vectorial y $T, S : V \to V$ dos transformaciones lineales. Denotemos por $V^T$ y $V^S$ los $\mathbb{K}[x]$-módulos con la multiplicación dada por $fv = f(T)v$ y $fv = f(S)v$ respectivamente. ¿Cuándo son $V^T$ y $V^S$ isomorfos como $\mathbb{K}[x]$-módulos. Respuesta: $V^T$ e isomorfo a $V^S$ si y sólo si $T$ es conjugada a $S$. Es decir, cuando existe un isomorfismo de $\mathbb{K}$-espacios vectoriales $Q : V \to V$ tal que $S = Q \circ T \circ Q^{-1}$.

Supongamos primero que existe una tal $Q$ y veamos que $Q : V^T \to V^S$ es isomorfismo de $\mathbb{K}[x]$-módulos. En efecto, ya tenemos que $Q$ preserva la suma. Para ver que preserva la multiplicación por $f \in \mathbb{K}[x]$ notemos que

$$\begin{aligned} Q(fv) &= Q(f(T)v) \\ &= Q(f(T)Q^{-1}Qv) \\ &= Qf(T)Q^{-1}Qv \\ &= f(S)Q(v) \\ &= fQ(v), \end{aligned}$$

en donde, abusando de la notación entendemos que al comienzo de la cadena de igualdades $fv$ se calcula en $V^T$ y al final, $fQ(v)$ se calcula en $V^S$. Para justificar el paso $Qf(T)Q^{-1} = f(S)$ observemos que si $f = f_0 + f_1 x + \cdots + f_n x^n$, entonces $f(T) = f_0 I + f_1 T + \cdots + f_n T^n$ y por consiguiente $Qf(T)Q^{-1} = f_0 QQ^{-1} + f_1 QTQ^{-1} + \cdots + f_n QT^n Q^{-1}$. Ahora bien, como

$$\begin{aligned} QT^k Q^{-1} &= QTQ^{-1}QTQ^{-1}\cdots QTQ^{-1} \\ &= (QTQ^{-1})^k = S^k \end{aligned}$$

sigue que

$$Qf(T)Q^{-1} = f_0 I + f_0 S + \cdots f_n S^n = f(S).$$

Recíprocamente si $\Phi : V^T \to V^S$ es un isomorfismo de $\mathbb{K}[x]$-módulos, entonces $\Phi : V \to V$ es un isomorfismo de $\mathbb{K}$ espacios vectoriales y además (también abusando de la notación) la condición $\Phi(xv) = x\Phi(v)$ significa que $\Phi(Tv) = S\Phi v$ para todo $v \in V$, o equivalentemente, $\Phi \circ T = S \circ \Phi$, es decir $S = \Phi \circ T \circ \Phi^{-1}$.

# 5. Cocientes

Los cocientes (y también los productos y sumas directas que veremos más adelante) de $R$-módulos son muy importantes para tratar de entender la estructura de un $R$-módulo arbitrario.

Sean $M$ un $R$-módulo y $A$ un submódulo de $M$. Como $A$ es un subgrupo normal de $M$ (que es abeliano), ya sabemos que $M/A$ tiene estructura de grupo abeliano. Más precisamente, y fijando un poco de notación, en

$$M/A = \{x + A : x \in M\}$$

la suma está definida por

$$(x + A) + (y + A) = (x + y) + A.$$

Definimos además una multiplicación $R \times M/A \to M/A$ por

$$r(x + A) = rx + A$$

para $r \in R$ y $x \in M$. Para verificar que esta definición es buena, notemos que si $x + A = y + A$, o equivalentemente $x - y \in A$, entonces $r(x - y) = rx - ry \in A$ lo cual significa que $rx + A = ry + A$. Es decir, nuestra definición no depende del representante elegido.

Así, $M/A$ tiene una estructura natural de $R$-módulo. Más aún, observemos que si $M$ es un módulo unitario, entonces $M/A$ también lo es.

**Proposición 5.1.** *Sea $M$ un $R$-módulo y $A$ un submódulo de $M$, entonces la proyección al cociente $\pi : M \to M/A$ es epimorfismo de $R$-módulos con* $\ker \pi = A$.

*Demostración.* Ya sabemos que $\pi$ es un epimorfismo de grupos con $\ker \pi = A$. Solo falta probar que $\pi$ respeta la multiplicación por $r \in R$. En efecto, usando la definición tenemos que $\pi(rx) = rx + A = r(x + A) = r\pi(x)$. □

**Proposición 5.2** (Teorema de factorización)**.** *Sean $M, N$ dos $R$-módulos y sea $A$ un submódulo de $M$. Si $\varphi : M \to N$ es morfismo de $R$-módulos tal que $A \subset \ker \varphi$, entonces existe un único morfismo de $R$-módulos $\bar{\varphi} : M/A \to N$ tal que $\varphi = \bar{\varphi} \circ \pi$. Es decir, $\bar{\varphi}$ es única tal que el siguiente diagrama conmuta.*

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & N \\ {\scriptstyle\pi}\downarrow & \nearrow_{\exists!\bar{\varphi}} & \\ M/A & & \end{array}$$

*Demostración.* Ya sabemos que existe único morfismo de grupos $\bar{\varphi}$ tal que el diagrama anterior conmuta. Verifiquemos que $\bar{\varphi}$ también preserva la multiplicación por $r \in R$. En efecto,

$$\begin{aligned} \bar{\varphi}(r(x + A)) &= \bar{\varphi}(rx + A) = \bar{\varphi}(\pi(rx)) \\ &= \varphi(rx) = r\varphi(x) \\ &= r\bar{\varphi}(\pi(x)) = r\bar{\varphi}(x + A). \end{aligned}$$

□

**Corolario 5.3** (Primer teorema de isomorfismo)**.** *Si $\varphi : A \to B$ es un morfismo de $R$-módulos entonces*

$$A/\ker \varphi \simeq \operatorname{im} \varphi.$$

*Demostración.* Recordemos que un isomorfismo de grupos entre $A/\ker \varphi$ e $\operatorname{im} \varphi$ se construye usando la versión para grupos del teorema de factorización. Pero como acabamos de ver, este isomorfismo de grupos también es isomorfismo de $R$-módulos. □

**Corolario 5.4** (Segundo teorema de isomorfismo)**.** *Sea $A$ un $R$-módulo y consideremos dos submódulos $B, C$ de $A$ tales que $C \subset B \subset A$. Entonces*

$$A/B \simeq \frac{A/C}{B/C}.$$

Observemos que el cociente $B/C$ tiene sentido porque $C$ es también un submódulo de $B$ y el cociente $(A/C)/(B/C)$ tiene sentido porque $B/C = \{x + C : x \in B\}$ es un submódulo de $A/C = \{x + C : x \in A\}$. Completar la demostración como ejercicio.

**Corolario 5.5.** *Si $A, B$ son dos sumbmódulos de un mismo $R$-módulo entonces*

$$(A + B)/B \simeq A/(A \cap B).$$

*Demostración.* Ejercicio. □

**Definición-Ejemplo 5.6.** Sea $M$ un $R$-módulo.

(i) El *anulador de $M$* es

$$\operatorname{Ann}(M) = \{r \in R : rx = 0 \text{ para todo } x \in M\}$$

(ii) El *anulador de $m \in M$* es

$$\operatorname{Ann}(m) = \{r \in R : rm = 0\}$$

Notemos que tanto $\operatorname{Ann}(M)$ como $\operatorname{Ann}(m)$ son ideales a izquierda de $R$. Más aún,

$$\operatorname{Ann}(M) = \bigcap_{m \in M} \operatorname{Ann}(m).$$

**Proposición 5.7.** *Un $R$-módulo unitario es cíclico si y sólo si es isomorfo a $R/L$ (más precisamente ${}_RR/L$) para algún ideal a izquierda $L$ de $R$. Más aún, si $M = Rm$ es cíclico, entonces $M \simeq R/\operatorname{Ann}(m)$.*

*Demostración.* Si $M = Rm$ es cíclico, entonces $\varphi : R \to M$ definida por $\varphi(r) = rm$ es un epimorfismo de $R$-módulos con $\ker \varphi = \{r \in R : rm = 0\} = \operatorname{Ann}(m)$. Luego, por el primer teorema de isomorfismo, tenemos que $M \simeq R/\operatorname{Ann}(m)$.

Recíprocamente, si $M = R/L$, para algún ideal a izquierda $L$, entonces $M = R(1+L)$ es cíclico. □

# 6. Suma directa y producto directo

**Definición 6.1.** El *producto directo (externo)* de una familia de $R$-módulos $\{A_i\}_{i \in I}$ es el producto cartesiano

$$\prod_{i \in I} A_i = \{(x_i)_{i \in I} : x_i \in A_i\}$$

con las operaciones definidas componente a componente

$$(x_i)_{i \in I} + (y_i)_{i \in I} = (x_i + y_i)_{i \in I}$$

y

$$r(x_i)_{i \in I} = (rx_i)_{i \in I}$$

para $r \in R$, $x_i, y_i \in A_i$.

Es inmediato que con esta definición $\prod_{i\in I} A_i$ resulta un $R$-módulo. Utilizaremos la siguiente convención, si $I = \varnothing$ es una familia vacía de índices, entonces $\prod_{i\in I} A_i = \{0\}$ es el $R$-módulo trivial. A modo de ejemplo, mencionamos los siguientes casos particulares

- si $I = \{I_0\}$, entonces $\prod_{i\in I} A_i = A_{i_0}$,
- si $I = \{1, 2, \ldots, n\}$, entonces $\prod_{i\in I} A_i = A_1 \times A_2 \times \cdots \times A_n$.

Dado un producto directo $\prod_{i\in I} A_i$ se tienen asociadas para cada $j \imath I$ las *proyecciones* $\pi_j : \prod_{i\in I} A_i \to A_j$ dadas por $\pi_j((x_i)_{i\in I}) = x_j$. Sigue de las definiciones que $\pi_j$ es un morfismo de módulos para todo $j \in I$. Más aún, probar como ejercicio que el producto directo es la única estructura de $R$-módulo en el conjunto $\prod_{i\in I} A_i$ que hace de $\pi_j$ un morfismo de $R$-módulos para todo $j$.

**Proposición 6.2** (Propiedad universal del producto directo)**.** *Sean $M$ y $(A_i)_{i\in I}$ $R$-módulos. Para cada familia $(\varphi_i)_{i\in I}$ de morfismos de $R$-módulos $\varphi_i : M \to A_i$ existe un único morfismo de $r$-módulos $\varphi : M \to \prod_{i\in I} A_i$ tal que $\pi_j \circ \varphi = \varphi_j$ para todo $j \in I$. Es decir, el siguiente diagrama conmuta.*

$$\begin{array}{ccc} & & M \\ & \overset{\exists!\varphi}{\swarrow} & \downarrow{\scriptstyle \varphi_j} \\ \displaystyle\prod_{i\in I} A_i & \xrightarrow[\pi_j]{} & A_j \end{array}$$

*Demostración.* Ejercicio. □

**Ejemplo 6.3.** Cada familia de morfismos de $R$-módulos $\varphi_i : A_i \to B_i$ induce un (único) morfismo de $R$-módulos $\varphi = \prod_{i\in I} \varphi : \prod_{i\in I} A_i \to \prod_{i\in I} B_i$ tal que el siguiente diagrama conmuta para todo $i \in I$.

$$\begin{array}{ccc} \prod_{i\in I} A_i & \overset{\exists!\varphi}{\dashrightarrow} & \prod_{i\in I} B_i \\ {\scriptstyle \pi_i}\downarrow & & \downarrow{\scriptstyle \tilde{\pi}_i} \\ A_i & \xrightarrow{\varphi_i} & B_i \end{array}$$

En efecto, sigue inmediatamente aplicando la propiedad universal a $\prod_{i\in I} B_i$ y la familia $\varphi_i \circ \pi_i$.

**Definición 6.4.** La *suma directa* o *suma directa interna* de una familia de $R$-módulos $\{A_i\}_{i\in I}$ es el submódulo de $\prod_{i\in I} A_i$ definido por

$$\bigoplus_{i\in I} A_i = \{(x_i)_{i\in I} : x_i = 0 \text{ p.c.t. } i\}.$$

Observemos que cuando $I$ es un conjunto finito, entonces la suma y el producto directo coinciden. En particular, si $I = \{1, 2, \ldots, n\}$,

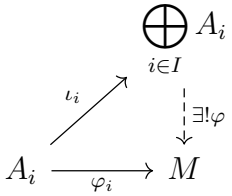
$$A_1 \oplus A_2 \oplus \cdots \oplus A_n = A_1 \times A_2 \times \cdots \times A_n.$$

Asociadas a una suma directa $\bigoplus_{i\in I} A_i$ tenemos las inyecciones $\iota_j : A_j \to \bigoplus_{i\in I} A_i$ definidas, para cada $x \in A_j$, por

$$(\iota(x))_i = \begin{cases} 0, & \text{si } i \neq j \\ x, & \text{si } i = j \end{cases}$$

Observar que $\iota_j$ es un monomorfismo de $R$-módulos para cada $j \in I$.

**Proposición 6.5** (Propiedad universal de la suma directa)**.** *Sean $M$ y $\{A_i\}_{i\in I}$ $R$-módulos. Para cada familia de morfismos de $R$-módulos $\{\varphi_i : A_i \to M\}_{i\in I}$ existe un único morfismo de $R$-módulos $\varphi : \bigoplus_{i\in I} A_i \to M$ tal que $\varphi \circ \iota_i = \varphi_i$ para todo $i \in I$. Es decir, tal que conmuta el siguiente diagrama.*




*Más precisamente, $\varphi((x_i)_{i\in I}) = \sum_{i\in I} \varphi_i(x_i)$.*

A modo de repaso daremos la demostración de la Proposición 6.5

**Lema 6.6.** *Si $x = (x_i)_{i\in I} \in \bigoplus_{i\in I} A_i$, entonces*

$$x = \sum_{i\in I} \iota_i(x_i). \tag{6.1}$$

*Más aún, si $x$ se puede escribir como $x = \sum_{i\in I} \iota_i(y_i)$ con $y_i \in A_i$ e $y_i = 0$ p.c.t. $i$, entonces $y_i = x_i$ para todo $i$. Es decir, la expresión en (6.1) es única.*

*Demostración.* Sea $(x_i)_{i\in I} \in \bigoplus_{i\in I} A_i$ y llamemos $J = \{i \in I : x_i \neq 0\}$. Definimos

$$y = \sum_{i\in J} \iota_i(x_i) = \sum_{i\in I} \iota_i(x_i).$$

Luego

$$y_j = \sum_{i\in J} (\iota_i(x_i))_j = \begin{cases} x_j, & j \in J \\ 0, & j \notin J \end{cases}$$

Así, tenemos que $y = x$ como queríamos probar. Notar que esto además prueba que la expresión en (6.1) es única. □

*Demostración de la Proposición 6.5.* Usando el Lema 6.6, observamos que de existir una tal $\varphi$, debe satisfacer

$$\varphi((x_i)_{i\in I}) = \varphi\left(\sum_{i\in I} \iota_i(x_i)\right) = \sum_{i\in I} \varphi(\iota_i(x_i)) = \sum_{i\in I} \varphi_i(x_i). \tag{6.2}$$

Esto prueba la unicidad de $\varphi$. La existencia sigue notando que el lado derecho en (6.2) define un morfismo de $R$-módulos. □

*Observación* 6.7. Si $I = \{1, 2, \dots, n\}$ es un conjunto finito de índices, entonces $A_1 \oplus A_2 \oplus \cdots \oplus A_n = A_1 \times A_2 \times \cdots \times A_n$ tiene las dos propiedades universales.

**Ejemplo-Ejercicio 6.8.** Toda familia de morfismos de $R$-módulos $\varphi_i : A_i \to B_i$, con $i \in I$, induce un único morfismo de $R$-módulos $\varphi : \bigoplus_{i\in I} A_i \to \bigoplus_{i\in I} B_i$ tal que el siguiente diagrama conmuta.

$$\begin{array}{ccc} \displaystyle\bigoplus_{i\in I} A_i & \overset{\exists!\varphi}{\dashrightarrow} & \displaystyle\bigoplus_{i\in I} B_i \\ {\scriptstyle \iota_i}\uparrow & & \uparrow{\scriptstyle \tilde{\iota}_i} \\ A_i & \xrightarrow[\varphi_i]{} & B_i \end{array}$$

A veces usaremos la notación $\varphi = \bigoplus_{i\in I} \varphi_i$.

El siguiente resultado caracteriza a la suma directa en términos de morfismos de módulos.

**Proposición 6.9.** *Sea $(M_i)_{i\in I}$ una familia de $R$-módulos. Un $R$-módulo $M$ es isomorfo a $\bigoplus_{i\in I} M_i$ si y sólo si existen dos familias de morfismos de $R$-módulos $\mu_i : M_i \to M$ y $\rho_i : M \to M_i$ tales que*

(i) $\rho_i \circ \mu_i = \mathrm{id}_{M_i}$ *para todo $i$;*

(ii) $\rho_i \circ \mu_j = 0$ *para todo $i \neq j$;*

(iii) *para cada $x \in M$, $\rho_i(x) = 0$ p.c.t. $i$*

(iv) $\sum_{i\in I} \mu_i \circ \rho_i = \mathrm{id}_M$.

*Demostración.* Ejercicio. Notar que la parte (iii) implica que la suma en la parte (iv) tiene sentido. □

## 6.1. Suma directa interna

**Proposición 6.10.** *Sean $(M_i)_{i\in I}$ una familia de $R$-módulos y sea $M$ un $R$-módulo. Son equivalentes*

(i) $M \simeq \bigoplus_{i\in I} M_i$ *(isomorfismo de $R$-módulos);*

(ii) *$M$ posee una familia de submódulos $(A_i)_{i\in I}$ tales que $A_i \simeq M_i$ para todo $i$ y cada elemento $x \in M$ se puede escribir de manera única como $x = \sum_{i\in I} a_i$ con $a_i \in A_i$ (y $a_i = 0$ p.c.t. $i$);*

(iii) *$M$ posee una familia de submódulos $(A_i)_{i\in I}$ tales que $A_i \simeq M_i$ para todo $i$, $M = \sum_{i\in I} A_i$ y $A_j \cap \left(\sum_{i\neq j} A_i\right) = \{0\}$.*

*Demostración.* Para ver (i) $\Longrightarrow$ (ii) consideramos los submódulos $M_i' = \iota_i(M_i)$ de $\bigoplus_{i\in I} M_i$. Tenemos que $M_i' \simeq M_i$, pues $\iota_i$ es monomorfismo, y usando el Lema 6.6 tenemos que cada elemento en $\bigoplus_{i\in I} M_i$ se escribe de manera única como $\sum_{i\in I} a_i$ con $a_i \in M_i'$. Si ahora $M \simeq \bigoplus_{i\in I} M_i$ y $\varphi : \bigoplus_{i\in I} M_i \to M$ es un isomorfismo, basta con tomar $A_i = \varphi(M_i')$.

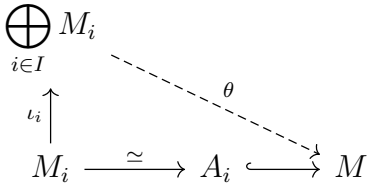
Veamos (ii) $\Longrightarrow$ (iii). Por hipótesis se tiene que $A_i \simeq M_i$ y $M = \sum_{i\in I} A_i$. Además si $x \in A_j \cap \left(\sum_{i\neq j} A_i\right)$, entonces podemos escribir $x = \sum_{i\in I} a_i'$ con $a_j = x$ y $a_i' = 0$ para todo $i \neq j$, y $x = \sum_{i\in I} a_i''$ con $a_j'' = 0$ y $a_i'' \in A_i$ para todo $i \neq j$. Por unicidad de la descomposición concluimos que $x = a_j' = a_j'' = 0$.

Para probar (iii) $\Longrightarrow$ (ii), ya tenemos que $A_i \simeq M_i$. Además el hecho de que $M = \sum_{i\in I} A_i$ nos dice que cualquier elemento $x \in M$ se escribe como $x = \sum_{i\in I} a_i$ con $a_i \in A_i$ (esta suma tiene sólo una cantidad finita de sumandos no nulos). Supongamos que también podemos escribir $x = \sum_{i\in I} a_i'$ con $a_i' \in A_i$. Fijando $j \in I$ tenemos que

$$a_j - a_j' = \sum_{i\neq j}(a_i' - a_i) \in A_j \cap \left(\sum_{i\neq j} A_i\right)$$

de donde sigue que $a_j = a_j'$ para todo $j \in I$.

Finalmente veamos (ii) $\Longrightarrow$ (i) usando la propiedad universal de la suma directa. En efecto, si llamamos $\theta_i$ a la composición del isomorfismo $M_i \to A_i$ con la inclusión de $A_i$ en $M$, tenemos que existe una única $\theta : \bigoplus_{i\in I} M_i \to M$ tal que $\theta\left((x_i)_{i\in I}\right) = \sum_{i\in i} \theta_i(x_i)$.




Ahora bien, como $\theta_i(M_i) = A_i$ y $M = \sum_{i\in I} A_i$ tenemos que $\theta$ es sobre. Además, si $\theta\left((x_i)_{i\in I}\right) = 0$, entonces $\theta_i(x_i) = 0$ para todo $i$. Como $\theta_i$ es un isomorfismo, sigue que $\theta$ es inyectiva. □

**Definición 6.11.** Un $R$-módulo $M$ es la *suma directa interna* de una familia de submódulos $(A_i)_{i\in I}$ si cada elemento de $M$ se puede escribir de manera única como $\sum_{i\in I} A_i$ con $a_i \in A_i$ y $a_i = 0$ p.c.t. $i$. En este caso también utilizaremos la notación $M = \bigoplus_{i\in I} A_i$.

**Corolario 6.12.** *Un $R$-módulo $M$ es una suma directa interna $M = A_1 \oplus A_2 \oplus \cdots \oplus A_n$ si y sólo si $M = A_1 + A_2 + \cdots + A_n$ y $A_j \cap (A_1 + A_2 + \cdots + A_{j-1}) = \{0\}$ para todos $1 \leq j \leq n$*

*Demostración.* ($\Longrightarrow$) es inmediato de la Proposición 6.10.

($\Longleftarrow$) sigue por inducción notando que la condición $A_j \cap (A_1 + \cdots + A_{j-1})$ implica

$$A_1 + \cdots + A_{j-1} + A_j = (A_1 + \cdots + A_{j-1}) \oplus A_j.$$ □

**Corolario 6.13.** *Un $R$-módulo $M$ es una suma directa interna $M = A \oplus B$ si y sólo si $M = A + B$ y $A \cap B = \{0\}$. En tal caso, $M/A \simeq B$ y $M/B \simeq A$.*

*Demostración.* La primera parte es inmediata. La segunda sigue del tercer teorema de isomorfismo. □

**Definición 6.14.** Un *sumando directo* de un $R$-módulo $M$ es un submódulo $A$ tal que $M = A \oplus B$ para algún submódulo $B$ de $M$.

**Proposición 6.15.** *Un submódulo $A$ de un $R$-módulo $M$ es un sumando directo si y sólo si existe un endomorfismo de módulos $\eta : M \to M$ tal que $\operatorname{im}\eta = A$ y $\eta^2 = \eta$.*

*Demostración.* Ejercicio. □

**Ejemplo 6.16.** (i) $\mathbb{Z}_4$ no tiene sumandos directos no triviales. En efecto, el único submódulo no trivial de $\mathbb{Z}_4$ es $\{0, 2\} \simeq \mathbb{Z}_2$, pero no existe ningún morfismo de $\mathbb{Z}$-módulos $\eta : \mathbb{Z}_4 \to \mathbb{Z}_4$ tal que $\eta^2 = \eta$ e $\operatorname{im}\eta = \{0, 2\}$. Si así no fuera, se tendría $\eta(1) = 2$ y consecuentemente $\eta^2 = 0$.

Observemos que este sencillo ejemplo nos dice que, aún cuando podemos obtener un nuevo $\mathbb{Z}$-módulo a partir de $\mathbb{Z}_4$ cocientando por el submódulo isomorfo a $\mathbb{Z}_2$, la estructura de $\mathbb{Z}_4$ no puede descomponerse en partes más sencillas (suma directa). Compara con el siguiente ejemplo.

(ii) Si $V$ es un $\mathbb{K}$-espacio vectorial, entonces todo subespacio de $V$ es un sumando directo (¿por que?).

# 7. Módulos libres

En esta sección los anillos se suponen con identidad y los módulos unitarios.

**Definición 7.1.** Sea $M$ un $R$-módulo. Una familia $(e_i)_{i\in I}$ de elementos de $M$ se dice *linealmente independiente* (sobre $R$) si para cada combinación lineal [2] $\sum_{i\in I} r_i e_i = 0$, con $r_i \in R$, se tiene que $r_i = 0$ para todo $i$

**Definición 7.2.** Una *base* de un $R$-módulo $M$ es una familia linealmente independiente que genera $M$. Un $R$-módulo $M$ se dice libre si admite una base $X$. En tal caso, es frecuente decir que $M$ es un $R$-módulo libre en $X$.

**Proposición 7.3.** *Una familia $(e_i)_{i\in I}$ de elementos de un $R$-módulo $M$ es una base si y sólo si cada elemento $x \in M$ se escribe de manera única como $x = \sum_{i\in I} r_i e_i$ con $r_i \in R$ y $r_i = 0$ p.c.t. $i$.*

*Demostración.* Por un lado, la familia $(e_i)_{i\in I}$ genera $M$ si y sólo si cada elemento $x \in M$ se escribe como una combinación lineal finita $x = \sum_{i\in I} r_i e_i$. Por otro lado, la familia $(e_i)_{i\in I}$ es linealmente independiente si y sólo si todo elemento en $\langle (e_i)_{i\in I}\rangle$ se escribe de manera única como combinación lineal de elementos en $(e_i)_{i\in I}$. En efecto, $\sum_{i\in I} r_i e_i = \sum_{i\in I} s_i e_i$ si y sólo si $\sum_{i\in I}(r_i - s_i)e_i = 0$ si y sólo si $r_i = s_i$ para todo $i \in I$. □

**Proposición 7.4.** *Sea $M$ un $R$-módulo.*

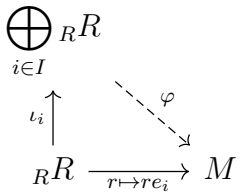
(i) *Si $(e_i)_{i\in I}$ es una base de $M$, entonces existe un isomorfismo $M \simeq \bigoplus_{i\in I} {}_R R$ que asigna a cada elemento $x \in M$ sus coordenadas en la base $(e_i)_{i\in I}$.*

(ii) *Cada suma directa $\bigoplus_{i\in I} {}_R R$ tiene una base canónica $(e_i)_{i\in I}$ dada por $(e_i)_j = \delta_{ij}$.*

(iii) *$M$ es libre si y sólo si $M \simeq \bigoplus_{i\in I} {}_R R$ para algún conjunto $I$.*

[2] Es decir, $r_i = 0$ salvo una cantidad finita de índices $i$.

*Demostración.* Para probar (i) sea $\varphi : \bigoplus_{i\in I} {}_R R \to M$ el morfismo de $R$-módulos inducido por la familia de morfismos de $R$-módulos $\varphi_i : {}_R R \to M$ definidos como $\varphi_i(r) = re_i$.




Tenemos que $\varphi$ es epimorfismo pues $(e_i)_{i\in I}$ genera $M$ y es monomorfismo pues $(e_i)_{i\in I}$ es linealmente independiente. Así $\varphi$ resulta un isomorfismo.

Para la parte (ii) definimos $e_i = \iota_i(1)$, en donde $\iota_i : {}_R R \to \bigoplus_{i\in I}$ son las inyecciones canónicas. Ya vimos en el Lema 6.6 que cualquier elemento en $\bigoplus_{i\in I} {}_R R$ se escribe de manera única como

$$\sum_{i\in I} \iota_i(r_i) = \sum_{i\in I} r_i \iota_i(1) = \sum_{i\in I} r_i e_i.$$

Luego, por la Proposición 7.3 tenemos que $(e_i)_{i\in I}$ es una base.

La parte (iii) es consecuencia de (i) y (ii). □

**Corolario 7.5.** *Dado un conjunto $X$ existe un $R$-módulo libre en $X$ y es único salvo isomorfismo.*

Observar que, sin embargo, el corolario anterior no nos dice que todas las bases de un mismo $R$-módulo libre tengan la misma cardinalidad. Más adelante daremos una discusión sobre este tema.

**Corolario 7.6.** *Todo $R$-módulo libre a izquierda $M$ admite una estructura de $R$-módulo libre a derecha. Dicha estructura depende de la elección de una base $(e_i)_{i\in I}$ de $M$ y está dada por*

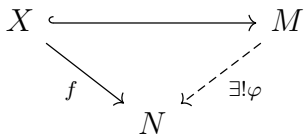
$$\left(\sum_{i\in I} r_i e_i\right) r = \sum_{i\in I} r_i r e_i.$$

**Ejercicio* 7.7** (para pensar un poco más adelante)**.** El corolario anterior muestra una situación un tanto patológica, pues la estructura de módulo a izquierda en $M$, obviamente no depende de la elección de la base. Mostrar dando un ejemplo que, sin embargo, la elección de distintas bases a izquierda en $M$ puede dar lugar para puede dar lugar a distintas estructuras de $R$-módulo a derecha.

**Proposición 7.8** (Propiedad universal para módulos libres)**.** *Sea $X = (e_i)_{i\in I}$ una base de un $R$-módulo libre $M$. Entonces toda función $f : X \to N$, en donde $N$ es un $R$-módulo se extiende a un único morfismo de $R$-módulos $\varphi : M \to N$. Más precisamente,*

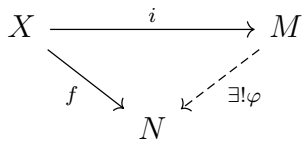
$$\varphi\left(\sum_{i\in I} r_i e_i\right) = \sum_{i\in I} r_i f(e_i). \tag{7.1}$$

*Si además $N = \langle f(X) \rangle$ entonces $\varphi$ es un epimorfismo.*




*Demostración.* Es inmediato que $\varphi$ definida como en (7.1) es un morfismo de $R$-módulos que extiende a $f$. □

**Ejercicio 7.9.** La propiedad universal de la Proposición 7.8 caracteriza a los módulos libres. Más precisamente, probar que si $M$ es un $R$-módulo, $X$ es un conjunto e $i : X \to M$ es una función inyectiva tal que para todo $R$-módulo $N$ y toda función $f : X \to N$ existe un único morfismo de $R$-módulos $\varphi : M \to N$ tal que $\varphi \circ i = f$, entonces $M$ es un $R$-módulo libre en $X$ (es decir, con base $i(X)$).




**Corolario 7.10.** *Cualquier $R$-módulo $M$ es la imagen de un epimorfismo de $R$-módulos $F \to M$, en donde $F$ es un $R$-módulo libre. Más aún, si $M$ está generado por un conjunto $X$, se puede tomar $F$ un $R$-módulo libre en $X$.*

## 7.1. Morfismos de módulos libres

En este apartado nos concentraremos en el caso de módulos libres que tengan bases finitas. Contrariamente a lo que nuestra intuición podría indicar, este caso es más delicado que cuando se tiene una base infinita. Una explicación de esto la daremos en la próxima subsección.

**Proposición 7.11.** *Sean $A, B$ dos $R$-módulos libres a derecha con bases $e_1, \ldots, e_n$ y $f_1, \ldots, f_m$ respectivamente. Entonces existe una correspondencia biyectiva entre los morfimos de $R$-módulos $A \to B$ y las matrices $m \times n$ con coeficientes en $R$.*

*Demostración.* Sea $\varphi : A \to B$ un morfismo de $R$-módulos, entonces para cada $e_j$ tenemos

$$\varphi(e_j) = \sum_{i=1}^{m} f_i r_{ij}, \qquad r_{ij} \in R.$$

Esto define una matriz (¡que depende de la elección de las bases!)

$$M(\varphi) = \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{m1} & r_{m2} & \cdots & r_{mn} \end{pmatrix},$$

en la cual la $j$-ésima columna de $M(\varphi)$ está formada por las coordenadas de $\varphi(e_j)$ en la base $f_1, \ldots, f_m$. Además, la matriz $M(\varphi)$ determina $\varphi$, pues si $x = \sum_{i=1}^{n} e_j x_j$, con $x_j \in R$, entonces

$$\begin{aligned}\varphi(x) &= \varphi\left(\sum_{j=1}^{n} e_j x_j\right) = \sum_{j=1}^{n} \varphi(e_j) x_j \\ &= \sum_{j=1}^{n}\sum_{i=1}^{m} f_i r_{ij} x_j = \sum_{i=1}^{m} f_i \sum_{j=1}^{n} r_{ij} x_j\end{aligned}$$

En particular esto nos dice que las coordenadas de $\varphi(x)$ en la base $f_1, \ldots, f_m$ están dadas por el producto de matrices

$$M(\varphi)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Recíprocamente, si $M = (r_{ij})$ es una matriz $m \times n$ con coeficientes en $R$, entonces la propiedad universal para módulos libres nos dice que existe un único isomorfismo $\varphi : A \to B$ tal que $\varphi(e_j) = \sum_{i=1}^{m} f_j r_{ij}$. Además, la matriz de $\varphi$ en las bases dadas coincide con $M$. □

**Proposición 7.12.** *Sean $\varphi, \psi : A \to B$, $\eta : B \to C$ morfismos de $R$-módulos libres a derecha con bases finitas. Entonces*

(i) $M(\varphi + \psi) = M(\varphi) + M(\psi)$,

(ii) $M(\eta \circ \varphi) = M(\eta)M(\varphi)$.

*Demostración.* En primer lugar notemos que las matrices de los isomorfismos siempre dependen de la elección de las bases, aunque no las hayamos fijado explícitamente en el enunciado de la proposición. Vamos a demostrar (ii), dejando (i) como ejercicio. Sean $e_1, \ldots, e_n$, $f_1, \ldots, f_m$ y $g_1, \ldots, g_\ell$ las bases dadas de $A, B, C$ respecto de las cuales se calculan las matrices de los morfismos del enunciado. Supongamos que para todos $i, j$ tenemos

$$\varphi(e_j) = \sum_{i=1}^{m} f_i r_{ij}, \qquad \text{i.e., } M(\varphi) = (r_{ij})$$

y

$$\eta(f_i) = \sum_{h=1}^{\ell} g_h s_{hi}, \qquad \text{i.e., } M(\eta) = (s_{hi}).$$

Calculamos

$$\begin{aligned}\eta(\varphi(e_j)) &= \eta\left(\sum_{i=1}^{m} f_i r_{ij}\right) \\ &= \sum_{i=1}^{m} \eta(f_i) r_{ij} = \sum_{i=1}^{m}\sum_{h=1}^{\ell} (g_h s_{hi}) r_{ij} \\ &= \sum_{h=1}^{\ell} g_h \sum_{i=1}^{m} s_{ih} r_{ij} = \sum_{h=1}^{\ell} g_h \left(M(\eta)M(\varphi)\right)_{hj}.\end{aligned}$$

Esto nos dice (ver la demostración de la Proposición 7.11) que $M(\eta\circ\varphi)_{hj} = (M(\eta)M(\varphi))_{hj}$ para todos $h, j$, o equivalentemente, $M(\eta \circ \varphi) = M(\eta)M(\varphi)$. □

Usando la proposición anterior, podemos describir de una manera concreta la estructura del anillo de endomorfismos de los $R$-módulos libres que admiten una base finita.

**Corolario 7.13.** *Sea $M$ un $R$-módulo libre a derecha que admite una base finita con $n$ elementos. Entonces* $\mathrm{End}_R(M)$ *es isomorfo (como anillo) a $M_n(R)$, el anillo de matrices $n \times n$ con coeficientes en $R$.*

*Demostración.* Por la Proposiciones 7.11 y 7.12 tenemos que (fijada una base con $n$ elementos) la asignación $\varphi \mapsto M(\varphi)$ es un isomorfismo de anillos (con identidad) entre $\mathrm{End}_R(M)$ y $M_n(R)$. □

**Corolario 7.14.** *Si $M$ es un $R$-módulo libre a izquierda que admite una base finita con $n$ elementos, entonces* $\mathrm{End}_R(M)$ *es isomorfo (como anillo) a $M_n(R^{\mathrm{op}})$.*

*Demostración.* Ejercicio. □

**Ejemplo-Ejercicio 7.15** (Importante)**.** Sea $R = \mathrm{End}_{\mathbb{K}}(V)$ en donde $\mathbb{K}$ es un cuerpo y $V$ es un $\mathbb{K}$-espacio vectorial con una base numerable $e_0, e_1, e_2, \ldots$ Sean $\alpha, \beta : V \to V$ las transformaciones lineales dadas por

$$\begin{aligned} \alpha(e_{2n}) &= e_n, & \alpha(e_{2n+1}) &= 0 \\ \beta(e_{2n}) &= 0, & \beta(e_{2n+1}) &= e_n. \end{aligned}$$

Probar que $\{\alpha, \beta\}$ es base de ${}_RR$ (y observar que $\{1\}$ también es base de ${}_RR$).

**Ejemplo 7.16.** Si $R$ es el anillo del ejemplo anterior entonces $R \simeq M_2(R)$ (isomorfismo de anillos). En efecto, si $M = R_R$, entonces por el Corolario 7.13 tenemos que $\mathrm{End}_R(M) \simeq R = M_1(R)$ tomando la base $\{1\}$ y por otro lado, tomando la base $\{\alpha, \beta\}$ tenemos que $\mathrm{End}_R(M) \simeq M_2(R)$. Más generalmente, para todos $m, n > 0$ se tiene que $M_n(R) \simeq M_m(R)$.

La no conmutatividad de $R$ es en gran parte responsable de este comportamiento tan extraño. Contrastar con el siguiente ejemplo.

**Ejemplo 7.17.** Si $\mathbb{K}$ es un cuerpo, entonces $M_n(\mathbb{K}) \simeq M_m(\mathbb{K})$ (isomorfismo de anillos) si y sólo si $n = m$. En efecto, una forma fácil de probar esto es mirando los elementos nilpotentes. Supongamos que $n > m$ y sea

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

Notar que $A$ es tal que $A^n = 0$ y $A^k \neq 0$ para $k < n$. Si $M_n(\mathbb{K}) \simeq M_m(\mathbb{K})$, entonces existe $B \in M_m(\mathbb{K})$ tal que $B^n = 0$ y $B^k \neq 0$ para $k < n$ (porque sabemos que esto pasa

en $M_n(\mathbb{K})$). Pero esto es absurdo, pues la condición $B^n = 0$ implica que el polinomio característico de $B$ es $x^m$ y por consiguiente $B^m = 0$ con $m < n$.

Si no está familiarizado con este tipo de argumentos de álgebra lineal, puede esperar hasta la clasificación de módulos sobre un dominio de ideales principales, donde recuperaremos como corolario todos estos resultados (y también la forma de Jordan).

## 7.2. Rango

**Definición 7.18.** Sea $M$ un $R$-módulo libre. Si todas las bases de $M$ tienen la misma cardinalidad decimos que $M$ tiene *rango* $\operatorname{rg} M = |X|$, en donde $X$ es alguna base de $M$.

En el apartado anterior vimos con un ejemplo que la noción de rango no está definida para cualquier módulo libre. En lo que que sigue estudiaremos varias situaciones en la que sí tenemos tenemos bien definido el rango.

**Proposición 7.19.** *Sea $M$ un $R$-módulo libre que tiene una base con infinitos elementos. Entonces todas las bases de $M$ tienen la misma cardinalidad.*

*Demostración.* Sean $X, Y$ dos bases de $M$ y supongamos que $X$ tienen infinitos elementos. Como cada $x \in X$ es una combinación lineal finita de un subconjunto finito $Y_x \subset Y$, tenemos que $X \subset \langle \bigcup_{x\in X} Y_x \rangle$ y por consiguiente $\langle \bigcup_{x\in X} Y_x \rangle = \langle X \rangle = M$. Esto nos dice que $Y = \bigcup_{x\in X} Y_x$. En efecto, si así no fuera entonces existe $y \in Y - \bigcup_{x\in X} Y_x$ que es combinación lineal de elementos en $\bigcup_{x\in X} Y_x$, lo cual es absurdo pues $Y$ es linealmente independiente. Usando esto y el hecho de que $X$ tienen una cantidad infinita de elementos concluimos que

$$|Y| \leq |\mathbb{N} \times X| = |X|.$$

Podemos razonar de manera similar, intercambiando los roles para mostrar que $|X| \leq |Y|$, de donde sigue que $|X| = |Y|$. Para esto hay que observar que la hipótesis de que $X$ es un conjunto infinito, implica que $Y$ también lo es. En efecto, supongamos que $Y$ es un conjunto finito. Con el mismo argumento que usamos más arriba, para cada $y \in Y$ existe un subconjunto finito $X_y \subset X$ que genera el elemento $y$. Luego tenemos que $\langle \bigcup_{y\in Y} X_y \rangle = M$, de donde sigue que $X = \bigcup_{y\in Y} X_y$, lo cual es absurdo pues $X$ es un conjunto infinito y la unión del lado derecho de la igualdad es un conjunto finito. □

**Ejercicio 7.20.** Hemos usado en la demostración anterior que si $X$ es un conjunto infinito, entonces $\mathbb{N} \times X$ es biyectivo con $X$. Si esto no resulta lo suficientemente claro, demostrarlo.

**Proposición 7.21.** *Sea $M$ un $R$-módulo libre. Si $R$ es conmutativo, entonces todas las bases de $M$ tienen la misma cardinalidad.*

*Nota* 7.22. En la demostración de la Proposición 7.21 usaremos la siguiente construcción elemental. Si $R$ es un anillo conmutativo y $\mathscr{A}$ es un ideal (bilátero) de $R$, entonces $R/\mathscr{A}$ es un anillo conmutativo, y con identidad si $R \neq \mathscr{A}$. Además

$$\mathscr{A}M = \langle \{rx : x \in M\, r \in \mathscr{A}\} \rangle$$

es un submódulo de $M$. Más aún, $M/\mathscr{A}M$ es un $R/\mathscr{A}$-módulo con la multiplicación definida por

$$(r + \mathscr{A})(x + \mathscr{A}M) = rx + \mathscr{A}M.$$

Si además $M$ es libre y $(e_i)_{i\in I}$ es una $R$-base de $M$, entonces $(e_i + \mathscr{A}M)_{i\in I}$ es una $R/\mathscr{A}$-base de $M/\mathscr{A}M$. En efecto, $(e_i + \mathscr{A}M)_{i\in I}$ pues si $x + \mathscr{A}M \in M/\mathscr{A}M$ y $x = \sum_{i\in I} r_i e_i$, con $r_i \in R$, entonces

$$x + \mathscr{A}M = \sum_{i\in I}(r_i + \mathscr{A})(e_i + \mathscr{A}M).$$

(Notar que no tendría sentido decir que la proyección al cociente es un morfismo de módulos, pues estamos trabajando con distintos anillos.)

Por otro lado, supongamos que

$$\begin{aligned} 0 &= \sum_{i\in I}(r_i + \mathscr{A})(e_i + \mathscr{A}M) \\ &= (r_i e_i + \mathscr{A}M) \\ &= \left(\sum_{i\in I} r_i e_i\right) + \mathscr{A}M. \end{aligned}$$

Luego, $\sum_{i\in I} r_i e_i \in \mathscr{A}M$ y así $r_i \in \mathscr{A}$ para todo $i$ (¿por qué?). Así, tenemos que $(e_i + \mathscr{A}M)_{i\in I}$ es $R/\mathscr{A}$-linealmente independiente y por consiguiente una $R/\mathscr{A}$-base de $M/\mathscr{A}M$.

*Demostración de la Proposición 7.21.* Por la Proposición 7.19 ya sabemos que si $M$ tiene una base infinita, entonces todas sus bases tienen la misma cardinalidad. Luego, podemos suponer sin pérdida de generalidad que todas las bases de $M$ una cantidad finita de elementos. Sean $(e_i)_{i\in I}$ y $(f_j)_{j\in J}$ dos bases de $M$ (o sea, $I, J$ son dos conjuntos finitos). Sean $\mathscr{A}$ un ideal maximal de $R$. Sigue que $R/\mathscr{A}$ es un cuerpo y $M/\mathscr{A}M$ es un $R/\mathscr{A}$-espacio vectorial. Por la Nota 7.22, tenemos que $(e_i + \mathscr{A})_{i\in I}$ y $(f_j)_{j\in J}$ son dos $R/\mathscr{A}$-bases de $M/\mathscr{A}M$. Como ya sabemos, en un espacio vectorial de dimensión finita, dos bases cualesquiera tienen la misma cardinalidad, lo cual dice que $|I| = |J|$. □

### 7.2.1. Espacios vectoriales

Recordemos que un *anillo de división* es un anillo con identidad en el cual todo elemento no nulo tiene inverso. En lo que sigue utilizaremos la siguiente definición.

**Definición 7.23.** Un *espacio vectorial* es un módulo unitario sobre un anillo de división.

*Observación* 7.24. Si $D$ es un anillo de división, entonces $D^{op}$ también es anillo de división. Esto nos dice que es suficiente con estudiar anillos de división a izquierda.

**Ejemplo 7.25.** Recordemos que un ejemplo muy importante de anillo de división no conmutativo está dado por los cuaterniones

$$\mathbb{H} = \{a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} : a, b, c, d \in \mathbb{R}\},$$

en donde la multiplicación se deduce de las identidades de Hamilton

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -\mathbf{1}$$

*Observación* 7.26. En un módulo $V$ sobre un anillo de división $D$, es decir, un $D$-espacio vectorial, la condición

$$r_1x_1 + r_2x_2 + \cdots r_nx_n = 0$$

para $r_i \in D$, $x_i \in V$, con $r_1 \neq 0$ implica que

$$x_1 = -(r_1^{-1}r_2x_2 + \cdots + r_1^{-1}r_nx_n)$$

es combinación lineal de $x_2, \ldots, x_n$. En palabras, si en un espacio vectorial tenemos un conjunto linealmente dependiente, entonces hay un elemento de dicho conjunto que es combinación lineal de los demás. Notar que aunque esto parezca una obviedad (hasta el punto confundir con esta condición la definición de dependencia lineal), no es siempre el caso si $D$ no es un anillo de división.

El siguiente resultado distingue a los espacios vectoriales del resto de los módulos libres.

**Lema 7.27.** *Sea $X$ un subconjunto linealmente independiente de un espacio vectorial $V$ (sobre un anillo de división $D$). Si $y \in V - X$, entonces $X \cup \{y\}$ es linealmente independiente si y sólo si $y$ no es una combinación lineal de elementos en $X$.*

*Demostración.* Si $X \cup \{y\}$ es linealmente dependiente, entonces existen $r_y \in D$ y $r_x \in X$, con $x \in X$, no todos nulos (pero a lo sumo una cantidad finita no nula) tales que

$$r_y y + \sum_{x \in X} r_x x = 0$$

Como $X$ es linealmente independiente, tenemos que $r_y \neq 0$ y usando la Observación 7.26 sigue que $y$ es una combinación lineal de elementos en $X$.

La recíproca es obvia. □

**Teorema 7.28.** *Todo espacio vectorial tiene una base.*

Para la demostración de este teorema usaremos el Lema de Zorn (notar que ya hemos usado implícitamente este resultado en la prueba de la Proposición 7.21). De hecho, uno puede probar que el Teorema 7.28 es equivalente al Lema de Zorn. Para hacer estas notas relativamente autocontenidas, recordemos brevemente qué dice el Lema de Zorn.

Un *conjunto parcialmente ordenado* es un conjunto $\mathscr{X}$ munido de una relación binaria $\leq$ que es

- reflexiva: $x \leq x$ para todo $x \in \mathscr{X}$;
- antisimétrica: si $x \leq y$ e $y \leq x$, entonces $x = y$; y
- transitiva: si $x \leq y$ e $y \leq z$, entonces $x \leq z$.

El orden en $\mathscr{X}$ se dice un *orden total* si para todo par de elementos $x, y \in \mathscr{X}$, se cumple $x \leq y$ o $y \leq x$. También se dice en este caso que $(X, \leq)$ es un *conjunto totalmente ordenado*.

Una *cadena* en un conjunto parcialmente ordenado $(\mathscr{X}, \leq)$ es un subconjunto $\mathscr{C}$ que resulta totalmente ordenado con la restricción del orden en $\mathscr{X}$. Una cota superior (una cadena) $\mathscr{C}$ es un elemento $y \in \mathscr{X}$ tal que $x \leq y$ para todo $x \in \mathscr{C}$. Finalmente, diremos que un elemento $m \in \mathscr{X}$ es *maximal* si no existe $x \in \mathscr{X}$ tal que $m < x$ (es decir, $m \leq x$ y $m \neq x$).

**Lema de Zorn.** *Sea $(\mathscr{X}, \leq)$ un conjunto parcialmente ordenado no vacío tal que toda cadena no vacía de $\mathscr{X}$ tiene una cota superior. Entonces $\mathscr{X}$ tiene un elemento maximal.*

*Demostración del Teorema 7.28.* Sea $V$ un $D$-módulo unitario sobre un anillo de división $D$. Sea $\mathscr{X} = \{X \subset V : X \text{ es linealmente independiente}\}$. Entonces $(X, \subset)$ es un conjunto parcialmente ordenado (no vacío, pues $\varnothing \in \mathscr{X}$). Notemos que si $\mathscr{C}$ es una cadena en $\mathscr{X}$ entonces $Y = \bigcup_{X \in \mathscr{C}} X$ es un conjunto linealmente independiente. En efecto, supongamos que existen para cada $r_y \in D$, no todos nulos tales que $\sum_{y \in Y} r_y y = 0$. Como en esta suma hay a lo sumo una cantidad finita de coeficientes no nulos, digamos $r_{y_1}, \ldots, r_{y_k}$ y $\mathscr{C}$ es una cadena, entonces existe un $X \in \mathscr{C}$ tal que $y_1, \ldots, y_k \in \mathscr{C}$, y como $X$ es linealmente independiente, sigue que $r_y = 0$ para todo $y \in Y$. Así, tenemos una cota superior $Y \in \mathscr{X}$ para cualquier cadena no vacía $\mathscr{C}$. Por el Lema de Zorn, existe un subconjunto linealmente independiente y maximal $\mathscr{S}$ en $M$. Para terminar la prueba veamos que $\mathscr{S}$ genera $V$. En efecto, para cada $x \in V$, se tiene por maximalidad que $\mathscr{S} \cup \{x\}$ es linealmente dependiente. Luego por el Lema 7.27 tenemos que $x$ es combinación lineal de elementos en $\mathscr{S}$. □

**Proposición 7.29.** *Sea $V$ un espacio vectorial y sea $Y$ un subconjunto que genera $V$. Si $X \subset Y$ es linealmente independiente entonces existe una base $\mathscr{B}$ de $V$ tal que $X \subset \mathscr{B} \subset Y$.*

*Demostración.* Ejercicio □

En particular, la proposición anterior dice que cualquier subconjunto linealmente independiente de $V$ se extiende a una base (tomando $Y = V$) y que cualquier conjunto de generadores contiene una base (tomando $X = \varnothing$).

**Lema 7.30.** *Sean $V$ un espacio vectorial y sean $X, Y$ dos bases de $V$. Entonces, para cada $x \in X$ existe $y \in Y$ tal que $(X - \{x\}) \cup \{y\}$ es base de $V$.*

*Demostración.* Si $x \in Y$ no hay nada que probar (tomar $y = x$ sirve). Supongamos que $x \notin Y$ y sea $S = \langle X - \{x\} \rangle$. Si $Y \subset S$, entonces $S = V$ y $x$ sería combinación lineal de elementos en $X - \{x\}$, lo que contradice la independencia lineal de $X$. Así, tenemos que existe un elemento $y \in Y$ tal que $y \notin S$. Dicho de otro modo, $y$ no es combinación lineal de elementos en $X - \{x\}$ y por el Lema 7.27 tenemos que $X' = (X - \{x\}) \cup \{y\}$ es linealmente independiente. Observemos ahora que $x$ es combinación lineal de elementos en $X'$, de lo contrario $X' \cup \{x\} = X \cup \{y\}$ sería linealmente independiente. Así, tenemos que $\langle X' \rangle = \langle X \rangle = V$ y $X'$ resulta una base de $V$. □

**Teorema 7.31.** *Todas las bases de un espacio vectorial tienen la misma cardinalidad.*

*Demostración.* Sean $X, Y$ dos bases de un espacio vectorial $V$. Si alguna de estas dos bases tiene infinitos elementos, ya probamos en la Proposición 7.19 que $|X| = |Y|$. Luego podemos suponer que $X$ e $Y$ son conjuntos finitos. Aplicando el Lema 7.30, podemos construir una base de $V$ en la que cada elemento de $X$ es reemplazado por un elemento de $Y$. Esto no nos dice $|X| \leq |Y|$. Análogamente tenemos que $|Y| \leq |X|$ y por lo tanto $|X| = |Y|$. □

**Definición 7.32.** La *dimensión* $\dim V$ de un espacio vectorial $V$ se define como la cardinalidad de alguna (y por lo tanto todas) de sus bases.

**Proposición 7.33.** *Cada subespacio $S$ de un espacio vectorial $V$ es un sumando directo. Más aún,*

$$\dim S + \dim V/S = \dim V.$$

*Demostración.* Ejercicio. □

**Proposición 7.34.** *Sea $S$ un subespacio de un espacio vectorial $V$. Si $\dim V$ es finita y $\dim S = \dim V$, entonces $S = V$.*

*Demostración.* Ejercicio. □

**Ejercicio 7.35.** Pensar también por qué el resultado análogo a la Proposición 7.34 no es cierto para módulos libres (aun teniendo definido el rango).

# 8. Módulos sobre un DIP

Recordemos que un *dominio de ideales principales*, que en general abreviaremos como DIP, es un anillo conmutativo, sin divisores de cero en donde todo ideal es principal. Entre los ejemplos más destacados tenemos al anillo de enteros $\mathbb{Z}$ y al anillo de polinomios $\mathbb{K}[x]$ de un cuerpo $\mathbb{K}$. Una propiedad muy importante y que usaremos en esta sección es que todo dominio de ideales principales es un dominio de factorización única.

Los módulos sobre un DIP tienen propiedades muy destacadas, como por ejemplo el siguiente teorema (aunque no sea muy fácil de probar).

**Teorema 8.1.** *Sean $R$ un DIP y $F$ un $R$-módulo libre. Entonces todo submódulo de $F$ es libre de rango a lo sumo* $\operatorname{rg} F$.

**Ejemplo 8.2.** Notemos que el enunciado del teorema anterior no es cierto si no suponemos que $R$ es un DIP. En efecto, consideremos $F = \mathbb{Z}_4$ como módulo libre sobre $\mathbb{Z}_4$. Entonces el submódulo $\{0, 2\} \simeq \mathbb{Z}_2$ no es libre (¿por qué?).

A continuación daremos una prueba del Teorema 8.1. En una primera lectura quizás convenga prestar atención a los argumentos principales y técnicas utilizadas para luego prestar atención a los detalles.

*Demostración del Teorema 8.1.* Sea $X$ una base de $F$ y sea $M$ un submódulo de $F$. Para cada subconjunto $Y \subset X$, denotamos por $F_Y$ el submódulo (libre) de $F$ generado por $Y$. La idea de la demostración es usar el Lema de Zorn para hacer "inducción transfinita" en $Y$, en donde el "paso inductivo" sería el siguiente. Supongamos que $Y \neq X$ y que $M_Y = F_Y \cap M$ admite una base $B$. Dado $x \in X - Y$ sea $Z = Y \cup \{x\}$. Notemos que

$$M_Z = \{rx + t \in M : r \in R, t \in F_Y\}$$

y probemos que $B$ se extiende a una base de $M_Z$. En efecto, sea

$$\mathscr{A} = \{r \in R : rx + t \in M_Z \text{ para algún } t \in F_Y\}.$$

Notemos que $\mathscr{A}$ es un ideal de $R$. Si $\mathscr{A} = 0$, entonces $M_Z = M_Y$, luego $B$ es base de $M_Z$ y no hay nada que probar. Si $\mathscr{A} \neq 0$, entonces como $R$ es un DIP, existe $0 \neq a \in R$ tal que

$\mathscr{A} = Ra$. En particular, $c = ax + p \in M_Z$ para algún $p \in F_Y$. Veamos que $C = B \cup \{c\}$ es base de $M_Z$. Supongamos que tenemos una combinación lineal nula

$$r_c c + \sum_{b \in B} r_b b = 0$$

con $r_c, r_b \in R$ (a lo sumo una cantidad finita de coeficientes no nulos). Entonces $r_c c = -\sum_{b \in B} r_b b \in M_Y$, es decir, $r_c c = r_c(ax + p) = r_c ax + r_c p \in M_Y$, de donde sigue que $r_c ax = r_c p - r_c c \in F_Y$, pues $p \in F_Y$ y $r_c c \in M_Y = F_Y \cap M$. Como $Z = Y \cup \{x\}$ es linealmente independiente, sigue que $r_c a = 0$ y por ende $r_c = 0$. Así, tenemos que $\sum_{b \in B} r_b b = 0$ y como $B$ es base de $M_Y$, $r_b = 0$ para todo $b$. Luego $C$ es linealmente independiente (y $c \notin B$). Para ver que $C$ genera, consideremos un elemento genérico $rx + t \in M_Z$ con $r \in R$, $t \in F_Y$. En tal caso se tiene que $r \in \mathscr{A}$ y por ende $r = sa$ para algún $s \in R$. Luego

$$rx + t = sax + t = s(c - p) + t = sc + t - sp.$$

Como $c \in M_Z$ concluimos que $t - sp \in F_Y \cap M = M_Y$, y por ende es combinación lineal de elementos en $B$. Luego, $C$ genera $M_Z$. Observar además que si $|B| \leq |Y|$ entonces $|C| = |B| + 1 \leq |Y| + 1 = |Z|$.

Sea $\mathscr{S}$ el conjunto de todos los pares $(Y, B)$ tales que $Y \subset X$ y $B$ es una base de $M_Y$ con $|B| \leq |Y|$. Observemos que $\mathscr{S}$ está parcialmente ordenado por la inclusión en cada coordenada, es decir, tenemos definido un orden parcial $(Y, B) \leq (C, Z) \iff Y \subset Z$ y $B \subset C$. Notemos también que $\mathscr{S}$ es no vacío, pues $(\varnothing, \varnothing) \in \mathscr{S}$. Además, si $\{(Y_i, B_i)\}_{i \in I}$ es una cadena en $\mathscr{S}$, entonces $(Y, B) = \left(\bigcup_{i \in I} Y_i, \bigcup_{i \in I} B_i\right) \in \mathscr{S}$ es una cota superior. En efecto, $F_Y = \bigcup_{i \in I} F_{Y_i}$ pues una combinación lineal de elementos en $Y$, involucra sólo una cantidad finita de coeficientes no nulos, cuyos correspondientes elementos están tomados de entre los $Y_i$. Así tenemos que $M_Y = \bigcup M_{Y_i}$ está generado por $B$ pues una combinación lineal de elementos en $B$ es una combinación lineal de elementos en algunos $B_i$, y similarmente se prueba que $B$ es linealmente independiente. Además, la condición $|B_i| \leq |Y_i|$ para todo $i$ implica que $|B| \leq |Y|$. Por el Lema de Zorn, existe un elemento maximal $(\tilde{Y}, \tilde{B})$ en $\mathscr{S}$. Ya probamos más arriba que si $\tilde{Y} \neq Y$, entonces $(\tilde{Y}, \tilde{B})$ no es maximal. Luego $\tilde{Y} = X$ y $\tilde{B}$ es una base de $M_X = M$ con $|\tilde{B}| \leq |X|$. □

**10 abr**

El siguiente resultado estudia el caso de rango finito y nos dice esencialmente que elementos de un submódulos de rango $r$ de un módulo libre de rango $n$ pueden pensarse (eligiendo una base adecuada) con las últimas $n - r$ coordenadas nulas y las $r$ primeras en una sucesión de ideales encadenados.

**Teorema 8.3.** *Sean $R$ un DIP, $F$ un $R$-módulo libre de rango $n \in \mathbb{N}$ y $M$ un submódulo de $F$. Entonces existen una base $e_1, \ldots, e_n$ de $F$, un entero $0 \leq r \leq n$ y elementos no nulos $a_1, \ldots, a_r \in R$ tales que $a_{i+1} \in Ra_i$ (es decir $a_i \mid a_{i+1}$) para todo $i \leq r$ y $a_1 e_1, \ldots, a_r e_r$ es base de $M$.*

**Ejemplo 8.4.** Para $F = \mathbb{Z} \oplus \mathbb{Z}$ y $M = 2\mathbb{Z} \oplus 3\mathbb{Z} = \{(2m, 3n) : m, n \in \mathbb{Z}\}$ una base como la que nos da el Teorema 8.3 es $e_1 = (2, 3)$, $e_2 = (1, 1)$ y tomando $a_1 = 1$, $a_2 = 6$ tenemos que $a_1 e_1 = (2, 3)$ y $a_2 e_2 = (6, 6)$ forma una base de $M$ (verificarlo directamente). En el apartado 8.1 explicamos el procedimiento para encontrar esta base. En una primera lectura quizás convenga pasar directamente a la demostración del teorema y luego volver a este ejemplo.

Recordemos una propiedad importante de los DIPs que necesitaremos para probar el Teorema 8.3.

*Observación* 8.5. Sea $R$ un DIP

(i) $R$ es noetheriano, es decir, toda cadena de ideales $I_1 \subset I_2 \subset I_3 \subset \cdots$ se estabiliza: existe un $n_0$ tal que $I_j = I_{n_0}$ para todo $j \geq n_0$. En efecto, como $R$ es DIP tenemos que $I_1 = Ra_1$, $I_2 = Ra_2$, $I_3 = Ra_3$, ... Si $a_1$ es unidad, entonces $Ra_1 = R$ e $I_j = I_1$ para todo $j$. Si $a_1$ no es unidad, entonces existen elementos irreducibles $p_1, \ldots, p_k$ y números naturales $s_1, \ldots s_k$ tales que $a_1 = p_1^{s_1} \cdots p_k^{s_k}$. Como $a_j \mid a_{j-1}$ tenemos que $a_j = p_1^{r_1} \cdots p_k^{s_k}$ (salvo asociados) para ciertos $0 \leq r_i \leq s_i$. Claramente este proceso se estabiliza en algún $n_0$.

(ii) Si $(I_\alpha)_{\alpha \in A}$ es una familia de ideales, entonces existe un elemento maximal $I_{\alpha_0}$. En efecto, sea $\alpha_1 \in A$, si $I_{\alpha_1}$ es maximal, no hay nada que probar, de lo contrario existe $\alpha_2 \in A$ tal que $I_{\alpha_1} \subsetneq I_{\alpha_2}$. Si $I_{\alpha_2}$ no es maximal, existe $\alpha_3$ tal que $I_{\alpha_2} \subsetneq I_{\alpha_3}$. Por el ítem anterior, este proceso no puede continuar indefinidamente, lo cual nos lleva a un ideal maximal.

*Demostración del Teorema 8.3.* La prueba es por inducción en $n$. El resultado vale para $n \leq 1$ (pues $R$ es un DIP y por lo tanto un submódulo de $R$ es un ideal principal). También es cierto el teorema si $M = 0$. Luego supongamos $n \geq 2$ y $M \neq 0$.

Podemos usar la siguiente idea para encontrar $a_1$: si el teorema es cierto y $\varphi : F \to R$ es un morfismo de módulos, entonces $\varphi(s) \in Ra_1$ para todo $s \in M$, o sea $\varphi(M) \subset Ra_1$. En particular, para $\varphi\left(\sum_{i=1}^n x_i e_i\right) = x_1$ se alcanza igualdad $\varphi(M) = Ra_1$. Luego $Ra_1$ es el ideal más grande de la forma $\varphi(M)$.

Como $R$ es noetheriano, la familia de ideales

$$\{\varphi(M) : \varphi : M \to R \text{ es morfismo de módulos}\}$$

tiene un elemento maximal, digamos $\mu(M)$, en donde $\mu : F \to R$ es algún morfismo de módulos. Como $R$ es DIP, $\mu(M) = Ra$ para algún $a \in R$. Sea $m \in M$ tal que $\mu(m) = a$. Veamos ahora que $\varphi(m) \in Ra$ para todo morfismo de módulos $\varphi : F \to R$. En efecto, $Ra + R\varphi(m) = Rd$ para algún $d = ua + v\varphi(m)$. Consideremos ahora el morfismo $\psi = u\mu + v\varphi : F \to R$. Notar que $\psi$ satisface $\psi(m) = d$. Luego $\mu(M) = Ra \subset Rd \subset \psi(M)$ y por maximalidad sigue que $Ra = Rd$. Así, $\varphi(m) \in Ra$.

Dada una base $e_1, \ldots, e_n$ de $F$ consideremos los morfismos de módulos $\varphi_j : F \to R$ definidos por $\varphi_j\left(\sum_{i=1}^n x_i e_i\right) = x_j$. Como $M \neq 0$, tenemos que $\varphi_j(M) \neq 0$ para algún $j$, luego $\mu(M) \neq 0$ y por ende $a \neq 0$. Además por lo anterior, $\varphi_j(m) \in Ra$ para todo $j$, de donde sigue que todas las coordenadas de $m$ son múltiplos de $a$. Así, $m = ae$ para algún $e \in F$ y por lo tanto $a = \mu(m) = \mu(ae) = a\mu(e)$ de donde sigue que $\mu(e) = 1$. Luego $Re \cap \ker \mu = 0$. Además si $x \in F$, entonces $x = \mu(x)e + x - \mu(x)e$. Como $\mu(x)e \in Re$ y $x - \mu(x)e \in \ker \mu$, tenemos que

$$F = Re \oplus \ker \mu. \tag{8.1}$$

Más aún, si $x \in M$, entonces $\mu(x) \in Ra$, lo cual implica que $\mu(x)e \in Rm$ (pues $m = ae$) y por lo tanto

$$M = Rm \oplus (\ker \mu \cap M). \tag{8.2}$$

Por el Teorema 8.1, $\ker \mu$ es libre de rango a lo sumo $n$. Más aún, $\operatorname{rg}(\ker \mu) = n - 1$ y si $e_2, \ldots, e_n$ es una base de $\ker \mu$, entonces $e, e_2, \ldots, e_n$ es una base de $F$. Por la hipótesis inductiva (aplicada de $\ker \nu \cap M$), podemos suponer que para la base $e_2, \ldots, e_n$ existe un entero $1 \leq r \leq n$ y elementos no nulos $a_2, \ldots, a_r$ tales que $a_{i+1} \in Ra_i$ para todo $i < r$ y $a_2 e_2, \ldots a_r e_r$ es base de $\ker \mu \cap M$. Luego por (8.1) y (8.2) es base de $M$ (¿por qué?). Sólo falta ver que $a_2 \in Ra$. Para esto seguimos un argumento similar al usado más arriba: escribimos $Ra + Ra_2 = Rd$. Por la propiedad universal de los módulos libres existe un morfismo de módulos $\varphi : F \to R$ tal que $\varphi(e) = \varphi(e_2) = 1$ y $\varphi(e_i) = 0$ para $i > 2$. Ahora escribimos $d = ua + va_2 = \varphi(uae + va_2 e_2) \in \varphi(M)$. Como $\mu(M) = Ra \subset Rd \subset \varphi(M)$ tenemos que $Ra = Rd$ y por lo tanto $a_2 \in Ra$. □

**Ejercicio 8.6.** Probar que los elementos $a_1, \ldots, a_r$ del Teorema 8.3 son únicos salvo multiplicación por unidades. Atención: esto no nos dice que haya unicidad en las bases, de hecho, no la hay.

## 8.1. Operaciones elementales sobre matrices con coeficientes en un DIP

Para encontrar la base que nos da el Teorema 8.3 empezamos con una base cualquiera de $u_1, \ldots, u_n$ de $F$ y una base cualquiera $b_1, \ldots b_r$ de $M$. Escribimos cada elemento $b_i$ como combinación lineal de la base $u_1, \ldots, u_n$:

$$b_i = a_{i1}u_1 + \cdots + a_{in}u_n.$$

Dicho de otra forma, las filas de la matriz

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r1} & a_{r2} & \cdots & a_{rn} \end{pmatrix}$$

están formadas por los coeficientes que usamos para escribir los elementos $b_i$ de la base de inicial de $M$ como combinación lineal de los elementos $u_j$ en la base inicial de $F$. Para pasar a una base como la que nos dice que existe el Teorema 8.3 tenemos que tener en cuenta dos cosas:

- si pasamos de la matriz $A$ a una matriz $A'$ aplicando una operación elemental por filas, entonces las combinaciónes lineales de $u_1, \ldots, u_n$ que podemos formar usando los coeficientes de la matriz $A'$ nos dan nuevamente una base de $M$;
- si pasamos de la matriz $A$ a una matriz $A''$ aplicando una operación elemental por columnas, entonces existe una nueva base $\tilde{u}_1, \ldots, \tilde{u}_n$ de $F$ tal que las combinaciones lineales de elementos en esta nueva base que formamos con los coeficientes de $A''$ nos dan la base de $M$ que ya teníamos.

O sea, cuando hacemos operaciones por filas estamos cambiando la base de $M$ y cuando hacemos operaciones por columnas estamos cambiando la base de $F$. A continuación

explicamos en detalle por qué esto funciona en el caso $n = r = 2$ y $R = \mathbb{Z}$. El caso general es completamente análogo, sólo un poco más engorroso de escribir. Fijemos una matriz

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}^{2\times 2}$$

Recordemos que hay tres tipos de operaciones elementales por filas: sumar una fila un mútiplo de otra fila; multiplicar una fila por una unidad e intercambiar dos filas. Las operaciones elementales por filas se pueden obtener multiplicando la matriz $A$ a izquierda por la matriz elemental correspondiente a la operación elemental que queremos aplicar (es decir, la matriz que obtandríamos si aplicáramos nuestra operación elemental a la matriz identidad). En nuestro caso, las matrices elementales son las siguientes

$$E_{1,2,n} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, \qquad E_{2,1,m} = \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix},$$
$$E_{1,-1} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad E_{2,-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$
$$E_{\text{swap}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

en donde $n, m \in \mathbb{Z}$. Llamemos $f_{1,2,n}, f_{2,1,m}, f_{1,-1}, f_{2,-1}, f_{\text{swap}}$ a las operaciones elementales por filas asocidas con las matrices elementales $E_{1,2,n}, E_{2,1,m}, E_{1,-1}, E_{2,-1}, E_{\text{swap}}$ respectivamente. Por ejemplo,

$$f_{1,2,n}(A) = E_{1,2,n}A = \begin{pmatrix} a + nc & b + nd \\ c & d \end{pmatrix}$$

Las operaciones elementales por columna análogas $c_{1,2,m}, c_{2,1,n}, c_{1,-1}, c_{2,-1}, c_{\text{swap}}$ tienen las mismas matrices elementales asociadas $E_{2,1,m}, E_{1,2,n}, E_{1,-1}, E_{2,-1}, E_{\text{swap}}$, respectivamente (notar la permutación en las primeras dos) pero ahora hay que multiplicar por la derecha. Por ejemplo,

$$c_{1,2,m}(A) = AE_{2,1,m} = \begin{pmatrix} a + mb & b \\ c + md & d \end{pmatrix}$$

Supongamos ahora que $u, v$ es una base de $\mathbb{Z} \oplus \mathbb{Z}$ y $au + bv, cu + dv$ es una base de $M$. Para que esto sea posible además tenemos que suponer que $\det A \neq 0$.

*Observación* 8.7. La condición $\det A \neq 0$ no significa que $A$ sea una matriz invertible en $\mathbb{Z}^{2\times 2}$. Las matrices invertibles en $\mathbb{Z}^{2\times 2}$ son aquellas con determinante $\pm 1$ (ejercicio). En particular, todas la matrices elementales son invertibles y como consecuencia sus filas/columnas forman una base de $\mathbb{Z} \oplus \mathbb{Z}$.

**Lema 8.8.** *Sea $f$ una operación elemental por filas y denotemos $f(A) = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$. Entonces $a'u + b'v, c'u + d'v$ es una base de $M$.*

*Demostración.* Ejercicio. □

**Lema 8.9.** *Sea $c$ una operacion elemental por columnas y denotemos $c(A) = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$. Entonces existe una base $\tilde{u}, \tilde{v}$ de $\mathbb{Z} \oplus \mathbb{Z}$ tal que $a'\tilde{u} + b'\tilde{v} = au + bv$ y $c'\tilde{u} + d'\tilde{v} = cu + dv$ (y por lo tanto forman una base de $M$). Más aún,*

(i) *si* $c = c_{1,2,m}$, *podemos tomar* $\tilde{u} = u, \tilde{v} = v - mu$;

(ii) *si* $c = c_{2,1,n}$, *podemos tomar* $\tilde{u} = u - nv, \tilde{v} = v$;

(iii) *si* $c = c_{1,-1}$, *podemos tomar* $\tilde{u} = -u, \tilde{v} = v$;

(iv) *si* $c = c_{2,-1}$, *podemos tomar* $\tilde{u} = u, \tilde{v} = -v$;

(v) *si* $c = c_{\text{swap}}$, *podemos tomar* $\tilde{u} = v, \tilde{v} = u$.

*Demostración.* Ejercicio. □

Con toda esta información podemos volver al Ejemplo 8.4 para encontrar nuestra base. Lo único que faltaría es saber es que aplincando operaciones elementales por filas y columnas siempre podemos llegar a una matriz diagonal. En realidad, el Teorema 8.3 es el que nos dice que esto siempre es posible (¿por qué?). En este caso particular tenemos $u = (1, 0)$, $v = (0, 1)$ la base de $F$ y $2u = (2, 0)$, $3v = (0, 3)$ la base de $M$. Aplicando sucesivamente los Lemas 8.8 y 8.9 (ver Cuadro 8.1) obtenemos que

$$e_1 = 2u + 3v = (2, 3), \qquad e_2 = u + v = (1, 1)$$

es una base de $\mathbb{Z} \oplus \mathbb{Z}$ tal que $e_1 = (2, 3), 6e_2 = (6, 6)$ es base de $M = 2\mathbb{Z} \oplus 3\mathbb{Z}$.

| Coeficientes | Op. Elemental | Base de $F = \mathbb{Z} \oplus \mathbb{Z}$ | Base de $M = 2\mathbb{Z} \oplus 3\mathbb{Z}$ |
|---|---|---|---|
| $\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$ | - | $u, v$ | $2u, 3v$ |
| $\begin{pmatrix} 2 & 0 \\ 2 & 3 \end{pmatrix}$ | $f_{2,1,1}$ | $u, v$ | $2u, 2u + 3v$ |
| $\begin{pmatrix} 2 & -2 \\ 2 & 1 \end{pmatrix}$ | $c_{2,1,-1}$ | $u + v, v$ | $2(u + v) - 2v, 2(u + v) + v$ |
| $\begin{pmatrix} 6 & 0 \\ 2 & 1 \end{pmatrix}$ | $f_{1,2,2}$ | $u + v, v$ | $6(u + v), 2(u + v) + v$ |
| $\begin{pmatrix} 6 & 0 \\ 0 & 1 \end{pmatrix}$ | $c_{1,2,-2}$ | $u + v, 2u + 3v$ | $6(u + v), 2u + 3v$ |
| $\begin{pmatrix} 0 & 1 \\ 6 & 0 \end{pmatrix}$ | $f_{\text{swap}}$ | $u + v, 2u + 3v$ | $2u + 3v, 6(u + v)$ |
| $\begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$ | $c_{\text{swap}}$ | $2u + 3v, u + v$ | $2u + 3v, 6(u + v)$ |

Cuadro 1: Operaciones elementales por filas y columnas en $\mathbb{Z}^{2\times 2}$

**Ejercicio 8.10.** Generalizar.

**Ejercicio 8.11.** Encontrar una base como la del Teorema 8.3 para $F = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ y $M = 2\mathbb{Z} \oplus 3\mathbb{Z} \oplus 5\mathbb{Z}$.

**Ejercicio 8.12.** Encontrar una base como la del Teorema 8.3 para $F = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ y $M$ el subgrupo generado por $(3, 9, 9)$ y $(9, -3, 9)$.

## 8.2. Clasificación de módulos finitamente generados sobre un DIP

16 abr

En este apartado presentamos una clasificación completa de los módulos finitamente generados sobre un DIP. Daremos esencialmente dos versiones de la clasificación las cuales enunciamos a continuación.

**Teorema 8.13** (Descomposición en factores invariantes)**.** *Sea $R$ un DIP. Todo $R$-módulo finitamente generado $M$ es una suma directa*

$$M \simeq F \oplus R/Ra_1 \oplus \cdots \oplus R/Ra_s$$

*de un $R$-módulo libre (de rango finito) $F$ y $R$-módulos cíclicos $R/Ra_1, \ldots, R/Ra_s$ con anuladores $R \supsetneq Ra_1 \supset Ra_2 \supset \cdots \supset Ra_1 \supsetneq 0$. Más aún, $\operatorname{rg} F$ y los ideales $Ra_1, \ldots, Ra_s$ están unívocamente determinados por $M$.*

Los elementos $a_1 \mid a_2 \mid \cdots \mid a_s$ se llaman *factores invariantes* de $M$ y están unívocamente determinados por $M$ (salvo asociados). La segunda versión de la clasificación es la siguiente

**Teorema 8.14** (Descomposición primaria)**.** *Sea $R$ un DIP. Todo $R$-módulo finitamente generado $M$ es una suma directa*

$$M \simeq F \oplus R/Rp_1^{k_1} \oplus \cdots \oplus R/Rp_t^{k_t}$$

*de un $R$-módulo libre (de rango finito) $F$ y $R$-módulos cíclicos $R/Rp_1^{k_1}, \ldots, R/Rp_t^{k_t}$ con anuladores $Rp_1^{k_1}, \ldots, Rp_t^{k_t}$ generados por potencias positivas de elementos primos (que podrían repetirse) de $R$. Más aún, $\operatorname{rg} F$ y los ideales $Rp_1^{k_1}, \ldots, Rp_t^{k_t}$ están unívocamente determinados (salvo el orden) por $M$.*

Los elementos $p_1^{k_1}, \ldots, p_t^{k_t}$, contados con repeticiones se llaman *divisores elementales* de $M$ y están unívocamente determinados (salvo asociados).

La demostración de estos dos teoremas (equivalentes) lleva varios pasos y el desarrollo de algo de teoría que será útil en otras situaciones.

*Demostración de la existencia en Teorema 8.13.* Como $M$ es finitamente generado, existe un $R$-módulo libre de rango finito $F'$ y un epimorfismo $\varphi : F' \to M$. Aplicamos el Teorema 8.3 a $F'$ y $\ker\varphi$: existen una base $e_1, \ldots, e_n$ de $F'$, un entero $0 \leq r \leq n$ y elementos $a_1, \ldots a_r \in R$ tales que $Ra_1 \supset \cdots \supset Ra_r$ y $a_1e_1, \ldots, a_re_r$ es base de $\ker\varphi$. Es decir, tenemos que

$$\begin{aligned} F' &= Re_1 \oplus \cdots \oplus Re_r \oplus Re_{r+1} \oplus \cdots \oplus Re_n, \\ \ker\varphi &= Ra_1e_1 \oplus \cdots \oplus Ra_re_r \end{aligned}$$

y por el primer teorema de isomorfismo, llamando $F = Re_{r+1} \oplus \cdots \oplus Re_n$, tenemos que

$$\begin{aligned} M \simeq F'/\ker\varphi &\simeq \frac{Re_1}{Ra_1e_1} \oplus \cdots \oplus \frac{Re_r}{Ra_re_r} \oplus Re_{r+1} \oplus \cdots \oplus Re_n \\ &\simeq \frac{R}{Ra_1} \oplus \cdots \oplus \frac{R}{Ra_r} \oplus F. \end{aligned}$$

(Observar que para probar que $R/Ra_i \simeq Re_i/Ra_ie_i$ podemos considerar el isomorfismo $R \to Re_i$ definido por $x \mapsto xe_i$, el cual manda $Ra_i$ en $Ra_ie_i$.) Sea $k$ el primer entero tal que $a_k$ no es unidad. Luego para $i < k$, $Ra_i = R$ y por ende $R/Ra_i = 0$. Así, escribimos

$$M \simeq \frac{R}{Ra_k} \oplus \cdots \oplus \frac{R}{Ra_r} \oplus F$$

con $F$ libre de rango $n - r$ y $R \supsetneqq Ra_k \supsetneqq \cdots \supsetneq Ra_r \supsetneqq 0$. □

Para poder demostrar la unicidad necesitamos estudiar la torsión de $M$.

**Definición 8.15.** Un elemento $x$ de un $R$-módulo se dice *de torsión* si $\mathrm{Ann}(x) \neq 0$ (o sea, si existe $r \in R - \{0\}$ tal que $rx = 0$), y $x$ se dice *sin torsión* si $\mathrm{Ann}(x) = 0$ (o sea, si $rx = 0$ implica $r = 0$). Un $R$ módulo se dice *de torsión* si todos sus elementos son elementos de torsión. Un $R$-módulo si dice *sin torsión* si todos sus elementos no nulos son sin torsión.

**Ejemplo 8.16.** (i) $0 \in M$ es de torsión pues $\mathrm{Ann}(0) = R$.

(ii) Si $M$ es un grupo abeliano ($\mathbb{Z}$-módulo) finito, entonces $M$ es de torsión.

(iii) Si $R$ no tiene divisores de cero y $M$ es un $R$-módulo libre, entonces $M$ es sin torsión.

**Definición 8.17.** La *torsión*, o mejor dicho el *submódulo de torsión* de un $R$-módulo $M$ es $T(M) = \{x \in M : \mathrm{Ann}(x) \neq 0\}$, el subconjunto de todos los elementos de torsión de $M$.

**Proposición 8.18.** *Si $R$ es un dominio íntegro y $M$ es un $R$-módulo, entonces $T(M)$ es un submódulo de $M$ y $M/T(M)$ es sin torsión*

*Demostración.* Ejercicio. □

**24 abr**

*Observación* 8.19. Sea $R$ un DIP y sea $\mathscr{P} \subset R$ el conjunto de elementos primos de $R$. La relación de asociados $p_1 \sim p_2 \iff$ existe una unidad $u \in R$ tal que $p_2 = up_1$ es una relación de equivalencia en $\mathscr{P}$. Un *conjunto de representantes* $P$ de $\mathscr{P}$ está formado por un elemento en cada clase de equivalencia de $\mathscr{P}/\sim$. Es decir,

- para cada primo $q \in R$, existe $p \in P$ tal que $q \sim p$;
- si $p, p' \in P$ y $p \sim p'$, entonces $p = p'$.

**Ejercicio 8.20.** Si bien para asegurar la existencia de un conjunto de representantes en general se requiere del axioma de elección, en varios casos de interés esto no es necesario. Dar un conjunto de representantes de elementos primos para $\mathbb{Z}$ y $\mathbb{K}[x]$, con $\mathbb{K}$ un cuerpo.

**Proposición 8.21.** *Sean $R$ un DIP y $P$ un conjunto de representantes de los elementos primos de $R$. Entonces todo $R$-módulo de torsión $M$ es la suma directa $M = \bigoplus_{p \in P} M(p)$, en donde $M(p) = \{x \in M : p^k x = 0$ para algún $k > 0\}$.*

El submódulo $M(p)$ se llama *componente $p$-primaria* de $M$.

*Demostración de la Proposición 8.21.* En primer lugar observemos que $M = \sum_{p\in P} M(p)$. En efecto, sea $x \in M$ y sea $a \in R$ tal que $ax = 0$. Escribimos $a = up_1^{k_1} \cdots p_r^{k_r}$ con $u$ unidad, $p_1, \ldots, p_r \in P$ todos distintos y $k_i > 0$ para todo $i$. Hacemos inducción en $r$. Si $r = 1$, entonces $x \in M(p_1)$ y por ende $x \in \sum_{p\in P} M(p)$. Supongamos que esto vale para $r-1$. Como $p_1^{k_1} \cdots p_{r-1}^{k_{r-1}}$ y $p_r^{k_r}$ son coprimos, existen $s, t \in R$ tales que $1 = sp_1^{k_1} \cdots p_{r-1}^{k_{r-1}} + tp_{k_r}^{k_r}$. Luego,

$$x = sp_1^{k_1} \cdots p_{r-1}^{k_{r-1}} x + tp_r^{k_r} x$$

Claramente el primer sumando del lado derecho de la igualdad está en $M(p_r)$. Además, tenemos que $(p_1^{k_1} \cdots p_{r-1}^{k_{r-1}})tp_r^{k_r} x = tu^{-1}ax = 0$ y por hipótesis inductiva concluimos que $tp_r^{k_r} x \in \sum_{p\in P} M(p)$, lo que implica que $x \in \sum_{p\in P} M(p)$.

Para completar la prueba veamos que $M(p) \cap \sum_{q\in P-\{p\}} M(q) = 0$. En efecto, sea $p \in P$ y $x \in M(p) \cap \sum_{q\in P-\{p\}} M(q)$. Luego existe un $k$ tal que $p^k x = 0$. Como también podemos escribir $x = \sum_{q\in P-\{p\}} x_q$, para cada $q$ existe un $k_q$ tal que $q^{k_q} x_q = 0$. (en realidad, hay a lo sumo una cantidad finita de $x_q$ distintos de cero). Sea $a = \prod_{q\in P-\{p\},\, x_q\neq 0} q^{k_q}$. Claramente tenemos que $ax_q = 0$ para todo $q \neq p$. Como $a$ y $p$ son coprimos, podemos escribir $1 = sa + tb$ para ciertos $s, t \in R$. Luego $x = sax + tp^k x = 0$ como queríamos probar. □

**Proposición 8.22.** *Sean $R$ un DIP y $M \simeq R/Ra$ un $R$-módulo cíclico, en donde $a = up_1^{k_1} \cdots p_\ell^{k_\ell}$ es producto de una unidad $u$ y potencias positivas de representantes distintos de elementos primos en $R$. Entonces $M(p_i) \simeq R/Rp_i^{k_i}$ y $M \simeq R/Rp_1^{k_1} \oplus \cdots \oplus R/Rp_\ell^{k_\ell}$.*

*Demostración.* Se tiene que $ax = 0$ para todo $x \in M = R/Ra$. Sea $x \in M(p)$ con $p \neq p_1, \ldots, p_r$ y supongamos que $p^k x = 0$ para cierto $k > 0$. Como $a$ y $p$ son coprimos, existen $s, t \in R$ tales que $1 = sa + tp^k$, de donde sigue que $x = sax + tp^k x = 0$. Luego $M(p) = 0$.

Ahora sean $1 \leq i \leq \ell$ y $b = \prod_{j\neq i} p_j^{k_j}$. Si $x = r + Ra \in M(p_i)$, entonces $p_i^k x = 0$ para algún $k > 0$ en $M = R/Ra$, por ende $p_i^k r \in Ra$. Luego $b \mid p_i^k r$ y por lo tanto $b \mid r$. Recíprocamente, si $b \mid r$, entonces $r \in Rb$ y por lo tanto $p_i^{k_i} r \in Ra$, lo cual dice que $p_i^{k_i} x = 0$ en $R/Ra$. Hemos probado que $b \mid r$ si y sólo sy $r + Ra \in M(p_i)$. O equivalentemente $M(p_i) = Rb/Ra$. Para completar la demostración sólo necesitamos usar la Proposición 8.21 y el Ejercicio 8.23. □

**Ejercicio 8.23.** Manteniendo la notación de la demostración de la Proposición 8.22 probar que la función $R \to Rb$ definida como $r \mapsto rb$ es un isomorfismo de $R$-módulos que manda $Rp_i^{k_i}$ en $Rp_i^{k_i} b = Ra$. Concluir que $M(p_i) = Rb/Ra \simeq R/Rp_i^{k_i}$.

*Demostración de la Existencia en el Teorema 8.14.* Sigue de la existencia en el Teorema 8.13 y de la Proposición 8.22 aplicada a cada sumando $R/Ra_i$ □

Todavía nos falta demostrar la unicidad para los Teoremas 8.13 y 8.14.

**Lema 8.24.** *Sea $R$ un DIP y sea $p \in R$ un elemento primo. Si*

$$M = M(p) \simeq R/Rp^{k_1} \oplus \cdots \oplus R/Rp^{k_t} \tag{8.3}$$

*con $0 < k_1 \leq \cdots \leq k_t$, entonces $t$ y $k_1, \ldots, k_t$ están unívocamente determinados por $M$.*

Notar que la existencia de la descomposición dada en (8.3) está garantizada por la Proposición 8.22.

*Observación* 8.25. Si $A$ es un $R$-módulo y $p \in R$ es un elemento primo, entonces $A/pA$ es un $R/Rp$-espacio vectorial (notar que $R/Rp$ es un cuerpo y que ya usamos una construcción similar cuando estudiamos módulos libres). Más aún, si $B$ es otro $R$-módulo, entonces $p(A \oplus b) = pA \oplus pB$ y $(A \oplus B)/(pA \oplus pB) \simeq A/pA \oplus B/pB$ (ver la guía de ejercicios).

*Demostración del Lema 8.24.* Como

$$\frac{R/Rp^k}{p(R/Rp^k)} = \frac{R/Rp^k}{Rp/Rp^k} \simeq R/Rp$$

sigue de la descomposición (8.3) que $M/pM \simeq R/Rp \oplus \cdots \oplus R/Rp$ ($t$ veces). Luego $t = \dim_{R/Rp} M/pM$ depende solamente de $M$.

Veamos ahora que $k_1, \ldots, k_t$ están unívocamente determinados por $M$. Hacemos inducción en $k_t$. Si $k_t = 1$, es lo que ya probamos pues $M \simeq R/Rp \oplus \cdots \oplus R/Rp$ ($t$ veces), de donde sigue que $k_1 = \cdots = k_t = 1$ y $t$ está unívocamente determinado por $M$. Supongamos entonces que $k_t > 1$. Observemos también que $\operatorname{Ann}(M) = Rp^{k_t}$, lo cual nos dice que $k_t$ está unívocamente determinado por $M$. Ahora

$$\begin{aligned} pM &\simeq p\left(R/Rp^{k_1} \oplus \cdots \oplus R/Rp^{k_t}\right) \\ &= Rp/Rp^{k_1} \oplus \cdots \oplus Rp/Rp^{k_t} \\ &\simeq R/Rp^{k_1-1} \oplus \cdots \oplus R/Rp^{k_t-1} \end{aligned}$$

en donde el último isomorfismo sigue del Ejercicio 8.23. Sea $s$ el primer entero tal que $k_{s+1} > 1$. Luego

$$pM \simeq R/Rp^{k_{s+1}-1} \oplus \cdots \oplus R/Rp^{k_t-1}$$

con $s > 0$, $k_1 = \cdots k_s = 1$ y $0 < k_{s+1} \leq \cdots \leq k_t$. Por hipótesis inductiva tenemos que $t - s$ y $k_{s+1} - 1, \ldots, k_t - 1$ están unívocamente determinados por $M$. Luego $s$ y $k_1, \ldots, k_t$ están unívocamente determinados por $M$. □

*Demostración de la unicidad en el Teorema 8.14.* Supongamos que

$$M \simeq F \oplus R/Rp_1^{k_1} \oplus \cdots \oplus R/Rp_t^{k_1}.$$

con $F$ libre, $p_i$ primo y $k_i > 0$ para todo $i$. Entonces $T(M) \simeq R/Rp_1^{k_1} \oplus \cdots \oplus R/p_t^{k_t}$. Luego $M/T(M) \simeq F$ y por ende $\operatorname{rg} F = \operatorname{rg} M/T(M)$ queda unívocamente determinado por $M$. Además como $(A \oplus B)(p) = A(p) \oplus B(p)$ (ejercicio) tenemos que $M(p) = \bigoplus_i (R/Rp_i^{k_i}) = \bigoplus_{p_i=p} R/Rp^{k_i}$. y por el Lema 8.24, $p_i = p$ y los correspondientes $k_i$ quedan unívocamente determinados por $M$, salvo el orden. □

*Demostración de la unicidad en el Teorema 8.13.* Supongamos que

$$M \simeq F \oplus R/Ra_1 \oplus \cdots \oplus R/a_s$$

con $F$ libre y $R \supsetneqq Ra_1 \supset \cdots \supset Ra_s \supsetneqq 0$. Como antes tenemos que $T(M) \simeq R/Ra_1 \oplus \cdots \oplus R/Ra_s$ y por ende $F \simeq M/T(M)$. Luego, $\operatorname{rg} F = \operatorname{rg} M/T(M)$ queda unívocamente determinado por $M$. Además como $a_1 \mid a_2 \mid \cdots \mid a_s$. Podemos escribir $a_j = u_j p_1^{k_{1j}} p_2^{k_{2j}} \cdots p_r k_{rj}$,

con $u_j$ unidad, $p_1, p_2, \ldots, p_r$ representantes distintos de elementos primos en $r$ y $k_{i1} \leq k_{i2} \leq \cdots \leq k_{is}$. Por la Proposición 8.22 tenemos que

$$T(M) \simeq \bigoplus_{j=1}^{s} \bigoplus_{i=1}^{r} R/Rp_i^{k_{ij}}$$

y por el Teorema 8.14 los primos $p_1, \ldots, p_j$ y los exponentes $k_{ij}$ están unívocamente determinados salvo el orden. Así los elementos $a_1, \ldots, a_s$ están unívocamente determinados salvo asociados. □

## 8.3. Clasificación de grupos abelianos finitamente generados

Los resultados del apartado anterior tienen como consecuencia inmediata, con $R = \mathbb{Z}$, la clasificación de los grupos abelianos finitamente generados. Estos teoremas usualmente son abordados en un curso de Estructuras Algebraicas I.

**Corolario 8.26.** *Sea $G$ un grupo abeliano finitamente generado, entonces existen $r \geq 0$ y una lista de enteros positivos $1 < a_1 \mid \cdots \mid a_s$ tales que*

$$G \simeq \mathbb{Z}^r \oplus \mathbb{Z}_{a_1} \oplus \cdots \oplus \mathbb{Z}_{a_s}.$$

*Más aún, $r$ y $a_1, \ldots, a_s$ están unívocamente determinados por $G$*

Equivalente a la descomposición en factores invariantes, tenemos la descomposición primaria:

**Corolario 8.27.** *Sea $G$ un grupo abeliano finitamente generado. Entonces existen $r \geq 0$, primos positivos $p_1, \ldots, p_k$ (no necesariamente distintos) y enteros positivos $s_1, \ldots s_k$ tales que*

$$G \simeq \mathbb{Z}^r \oplus \mathbb{Z}_{p_1^{s_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{s_k}}.$$

*Más aún, $r$ y $p_1^{s_1}, \ldots, p_k^{s_k}$ están unívocamente determinados por $G$ (salvo el orden).*

**Ejemplo 8.28.** Clasificar los grupos abelianos de orden 1200. En este caso no hay parte libre pues todo grupo abeliano finito es de torsión. Nos ayudamos de la descomposición en factores primos $1200 = 2^4 \cdot 3 \cdot 5^2$ y los corolarios anteriores para mostrar que todo grupo abeliano de orden 1200 es isomorfo a uno y solo uno de los grupos que aparecen en las filas del Cuadro 2 (y para cada fila, los grupos de las dos columnas son isomorfos).

## 8.4. Forma de Jordan

**26 abr**

A lo largo de esta sección $V$ será un espacio vectorial de dimensión finita sobre un cuerpo $\mathbb{K}$ y $T : V \to V$ una transformación lineal. Recordemos que en esta situación:

- $T$ induce una estructura de $\mathbb{K}[x]$-módulo en $V$ definiendo

  $$(a_0 + a_1 x + \cdots + a_n x^n)v = a_0 v + a_1 Tv + \cdots + a_n T^n,$$

  es decir, para cada $f \in \mathbb{K}[x]$ se define $fv = f(T)v$;

| Descomposición primaria | Descomposición en factores invariantes |
|---|---|
| $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$ | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{30}$ |
| $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$ | $\mathbb{Z}_2 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{60}$ |
| $\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$ | $\mathbb{Z}_{20} \oplus \mathbb{Z}_{60}$ |
| $\mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$ | $\mathbb{Z}_{10} \oplus \mathbb{Z}_{120}$ |
| $\mathbb{Z}_{16} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$ | $\mathbb{Z}_5 \oplus \mathbb{Z}_{240}$ |
| $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25}$ | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{150}$ |
| $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25}$ | $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{300}$ |
| $\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25}$ | $\mathbb{Z}_4 \oplus \mathbb{Z}_{300}$ |
| $\mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25}$ | $\mathbb{Z}_2 \oplus \mathbb{Z}_{600}$ |
| $\mathbb{Z}_{16} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25}$ | $\mathbb{Z}_{1200}$ |

Cuadro 2: Grupos abelianos de orden 1200

- Los $\mathbb{K}[x]$-submódulos de $V$ son exactamente los subespacios $T$-invariante. Es decir, $W$ es un $\mathbb{K}[X]$-submódulo si $W$ es un subespacio de $V$ tal que $TW \subset W$. Más aún, la estructura de $\mathbb{K}[x]$-módulo en $W$ (como submódulo de $V$) coincide con la estructura de $\mathbb{K}[x]$-módulo inducido por la restricción $T|_W : W \to W$ de $T$ a $W$.

**Definición 8.29.** El *polinomio minimal* $m_T$ de $T$ es el generador mónico del ideal $\operatorname{Ann}(V) = \{p \in \mathbb{K}[x] : pv = 0 \text{ para todo } v \in V\}$.

*Observación* 8.30. El polinomio minimal tiene las siguientes propiedades.

- $m_T(T) = 0$.
- Si $f \in \mathbb{K}[x]$, entonces $f(T) = 0$ si y sólo si $m_T \mid f$.
- $m_T \neq 0$. En efecto, $\operatorname{Ann}(V) \neq 0$ pues es el núcleo del morfismo (de anillos) evaluación $\Phi : \mathbb{K}[x] \to \operatorname{End}_{\mathbb{K}}(V)$ definido por $\Phi(f) = f(T)$. En particular, como $\Phi$ es $\mathbb{K}$-lineal, $\mathbb{K}[x]$ es un $\mathbb{K}$-espacio vectorial de dimensión infinita y $\dim_{\mathbb{K}} \operatorname{End}_{\mathbb{K}}(V) = (\dim V)^2 < \infty$, necesariamente se tiene que $\Phi$ no es inyectiva.
- En particular, $V$ es un $\mathbb{K}[x]$-módulo de torsión, pues $m_T v = 0$ para todo $v \in V$.

**Teorema 8.31.** *Sea $V$ un espacio vectorial de dimensión finita sobre un cuerpo $\mathbb{K}$ y sea $T : V \to V$ una transformación lineal. Como $\mathbb{K}[x]$-módulo, con la estructura inducida por $T$, $V$ es una suma directa $V = S_1 \oplus \cdots \oplus S_t$ de submódulos cíclicos tal que el polinomio minimal de $T|_{S_i}$ es una potencia positiva $q_i^{k_i}$ de un polinomio mónico irreducible $q_i \in \mathbb{K}[x]$. La cantidad de sumandos $t$, los polinomios $q_1, \ldots, q_t$ y los exponentes $k_1, \ldots, k_t$ están unívocamente determinados por $T$ (salvo el orden y contando repeticiones). Más aún, el polinomio minimal de $T$ es el mínimo común múltiplo de $q_1^{k_1}, \ldots, q_t^{k_t}$.*

*Demostración.* Aplicamos la descomposición primaria (Teorema 8.14) a

$$\begin{aligned} V &\simeq \mathbb{K}[x]/\operatorname{Ann}(V) \simeq \mathbb{K}[x]/\mathbb{K}[x]m_T \\ &\simeq \mathbb{K}[x]/\mathbb{K}[x]q_1^{k_1} \oplus \cdots \oplus \mathbb{K}[x]/\mathbb{K}[x]q_t^{k_t} \end{aligned}$$

donde $q_i$ es irreducible mónico (observar también que la descomposición primaria nos da la unicidad). Sea $S_i \simeq \mathbb{K}[x]/\mathbb{K}[x]q_i^{k_i}$ el correspondiente submódulo de $V$. Observemos que $S_i$ tiene anulador $q_i^{k_i}$, luego el polinomio minimal de $T|_{S_i}$ es $q_i^{k_i}$. Más aún, como $f(T) = 0$ si y sólo si $f(T)|_{S_i} = 0$ para todo $i$. Esto es equivalente a que $f(T|_{S_i}) = 0$ para $i$, lo cual a su vez equivale a $m_{T|_{S_i}} = q_i^{k_i}$ divida a $f$ para todo $i$. En particular, resulta que $m_T$ es el mínimo común múltiplo de $q_1^{k_1}, \ldots, q_t^{k_t}$. □

Para obtener la forma de Jordan de $T$ necesitamos entender un poco mejor cómo son los submódulos cíclicos de $V$.

**Lema 8.32.** *Si* $\dim_{\mathbb{K}} V = n$ *y* $V = \mathbb{K}[x]e$ *es un* $\mathbb{K}[x]$*-módulo cíclico, entonces* $\operatorname{gr} m_T = n$ *y* $e, Te, \ldots T^{n-1}e$ *es una base de* $V$ *como* $\mathbb{K}$*-espacio vectorial.*

*Demostración.* Sea $m = \operatorname{gr} m_T$. Notar que cada elemento de $V$ es de la forma $fe = f(T)e$ para algún $f \in \mathbb{K}[x]$. Dividiendo $f$ por el polinomio minimal, podemos escribir $f = m_T q + r$ para ciertos $q, r \in \mathbb{K}[x]$ con $r = 0$ o $\operatorname{gr} r < m$. Luego

$$f(T)e = m_T(T)q(T)e + r(T)e = r(T)e.$$

Luego, cada elemento de $V$ es combinación lineal de $e, Te, \ldots, T^{m-1}e$. Más aun, si tuviéramos $a_0e + a_1Te + \cdots + a_{m-1}T^{m-1}e$, entonces $ge = 0$ con $g = a_0 + a_1x + \cdots + a_{m-1}x^{m-1}$. Esto nos dice que $g(T) = 0$ y por lo tanto $m_T \mid g$. Así resulta $g = 0$ (de lo contrario sería $\operatorname{gr} g < \operatorname{gr} m_T$). De esto resulta que $e, Te, \ldots T^{m-1}e$ es una base de $V$. En particular, $m = n$. □

Recordar que si $\mathbb{K}$ es algebraicamente cerrado entonces todo polinomio mónico irreducible en $\mathbb{K}[x]$ es de la forma $x - \lambda$ para algún $\lambda \in \mathbb{K}$. En este caso, la descripción que dimos en el lema anterior se puede refinar un poco.

**Lema 8.33.** *Si* $\dim_{\mathbb{K}} V = n$ *y* $V$ *es un* $\mathbb{K}[x]$*-módulo cíclico con* $m_T = (x - \lambda)^m$*, entonces* $n = m$ *y* $V$ *tiene una base* $e_1, \ldots, e_n$ *tal que* $Te_1 = \lambda e_1$ *y* $Te_i = \lambda e_i + e_{i-1}$ *para* $i \geq 2$.

*Demostración.* Por el Lema 8.32 tenemos que $m = n$ y que existe $e \in V$ tal que $e, Te, \ldots, T^{n-1}e$ es una $\mathbb{K}$-base de $V$. Además, para $0 \leq k \leq n-1$ tenemos, usando que $T$ conmuta con $\lambda I$, que

$$\begin{aligned} T^k e &= (T - \lambda I + \lambda I)^k e \\ &= \sum_{i=0}^{k} \binom{k}{i} (T - \lambda I)^i (\lambda I)^{k-i} e \\ &= \sum_{i=0}^{k} \binom{k}{i} \lambda^{k-i} (T - \lambda I)^i e \end{aligned}$$

Luego, $T^k e \in \langle e, (T - \lambda I)e, \ldots (T - \lambda I)^k e \rangle$ (subespacio generado sobre $\mathbb{K}$). En particular, como $\dim_{\mathbb{K}} V = n$, tenemos que $e, (T - \lambda I)e, \ldots, (T - \lambda I)^{n-1}e$ es una $\mathbb{K}$-base de $V$. Si definimos (reordenamos) $e_i = (T - \lambda I)^{n-i}e$ para $i = 1, \ldots, n$ obtenemos que

$$(T - \lambda I)e_1 = (T - \lambda I)^n e = m_T e = 0$$

con lo cual $Te_1 = \lambda e_1$; $(T - \lambda I)e_2 = e_1$, de donde sigue que $Te_2 = \lambda e_2 + e_1$ y razonando inductivamente tenemos que $(T - \lambda I)e_k = e_{k-1}$, lo cual implica que $Te_k = \lambda e_k + e_{k-1}$. □

*Observación* 8.34. En la base $e_1, \dots, e_n$ que nos da el Lema 8.33, la matriz de $T$ tiene la forma

$$\begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & \cdots & 0 & 0 \\ 0 & 0 & \lambda & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda \end{pmatrix}.$$

Una matriz que tiene esa forma se llama *bloque de Jordan de autovalor* $\lambda$. Decimos que una matriz está en forma de Jordan si tiene la forma

$$\begin{pmatrix} J_1 & 0 & \cdots & 0 \\ 0 & J_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & J_t \end{pmatrix}$$

con $J_i$ un bloque de Jordan para $1 \leq i \leq t$ (que pueden tener distintos tamaños y estar asociados a distintos autovalores). En particular, toda matriz diagonal está en forma de Jordan.

Supongamos que $\mathbb{K}$ es algebraicamente cerrado, y usando el Teorema 8.31, descompongamos $V = S_1 \oplus \cdots \oplus S_t$ como suma de submódulos cíclicos tales que el polinomio minimal de $T|_{S_i}$ es $(x - \lambda_i)^{k_i}$. Entonces, por el Lema 8.33 sabemos que existe una $\mathbb{K}$-base $B_i$ de $S_i$ tal que la matriz de $T|_{S_i}$ en la base $B_i$ es un bloque de Jordan de autovalor $\lambda_i$. Luego, $B = B_1 \cup \cdots \cup B_t$ es una $\mathbb{K}$-base (ordenada) de $V$ tal que la matriz de $T$ en $B$ está en forma de Jordan.

**Teorema 8.35** (Jordan)**.** *Sea $V$ un espacio vectorial de dimensión finita sobre un cuerpo algebraicamente cerrado $\mathbb{K}$ y sea $T : V \to V$ una transformación lineal. Entonces existe una base $B$ de $V$ tal que la matriz de $T$ en $B$ está en forma de Jordan. Más aún, la forma de Jordan es única, en el sentido de que todas las matrices de $T$ que están en forma de Jordan contienen los mismos bloques de Jordan (contando repeticiones).*

*Demostración.* La existencia la discutimos más arriba. La unicidad se sigue de la descomposición primaria o su variante dada en el Teorema 8.31. □

*Observación* 8.36. En realidad en el Teorema 8.35 no es necesario suponer que $\mathbb{K}$ es algebraicamente cerrado. Es suficiente la hipótesis de que todos los factores irreducibles del polinomio minimal de $T$ sean de grado 1.

La forma de Jordan de una transformación lineal $T$ es muy importante porque a simple vista nos da mucha información relevante sobre $T$.

**Corolario 8.37.** *Si la matriz de $T$ está en forma de Jordan (en alguna base) entonces:*

(i) *Las entradas de la diagonal son los autovalores de $T$ (y para contarlos con repetición contamos cuántos bloques de Jordan aparecen asociados a un mismo autovalor);*

(ii) *El polinomio minimal de $T$ es $(x - \lambda_1)^{\ell_1} \cdots (x - \lambda_r)^{\ell_r}$ en donde $\lambda_1, \dots, \lambda_r$ son los distintos autovalores de $T$ y $\ell_i$ es el tamaño del bloque de Jordan más grande con $\ell_i$ en la diagonal.*

*Demostración.* Claramente los autovalores de $T$ son las entradas de la diagonal de su forma de Jordan (pues la forma de Jordan es una matriz triangular). Para chequer que la multiplicidad de un autovalor dado $\lambda$ es la cantidad de bloques de Jordan de autovalor $\lambda$ que aparecen en la forma de Jordan de $T$, es suficiente probar que si $J$ es un bloque de Jordan de autovalor $\lambda$, entonces el autoespacio de autovalor $\lambda$ de $J$ tiene dimensión 1. En efecto, sea $W = \{v \in V : Jv = \lambda v\}$. Entonces

$$\dim W = \dim \ker(J - \lambda I) = \dim \ker \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} = 1.$$

Esto prueba la parte (i). La parte (ii) queda como ejercicio. □

**Corolario 8.38.** *Si $\mathbb{K}$ es algebraicamente cerrado entones $T : V \to V$ es diagonalizable si y sólo si el polinomio minimal de $T$ es $(x - \lambda_1) \cdots (x - \lambda_r)$ con $\lambda_1, \ldots, \lambda_r \in K$ todos distintos.*

Como un ejemplo (teórico) de aplicación de la forma de Jordan podemos dar una prueba del teorema de Cayley-Hamilton. Recordemos que el *polinomio característico* de $T$ se define como $c_T(x) = \det(T - xI)$ (aquí lo que calculamos es el determinante de la matriz de $T - xI$ en alguna base de $V$, pero puede verse fácilmente que está definición no depende de la base que elijamos).

**Teorema 8.39** (Cayley-Hamilton)**.** *Sea $V$ un espacio vectorial de dimensión finita sobre un cuerpo $\mathbb{K}$ y sea $T : V \to V$ una transformación lineal. Entonces $c_T(T) = 0$.*

*Demostración.* Si $\mathbb{K}$ es algebraicamente cerrado, entonces existe una base de $V$ tal que la matriz de $T$ está en forma de Jordan (en particular es triangular superior). Luego por el Corolario 8.38, tenemos que $c_T(x) = (x - \lambda_1)_1^n \cdots (x - \lambda_r)_r^n$ donde $\lambda_1, \ldots, \lambda_r$ son los distintos autovalores de $T$ y $n_1, \ldots, n_r$ la cantidad de veces que aparecen en la diagonal. Así, también por el Corolario 8.38, tenemos que $m_T \mid c_T$ y consecuentemente $c_T(T) = 0$.

Si $\mathbb{K}$ no es algebraicamente cerrado, podemos tomar la clausura algebraica[3] $\overline{\mathbb{K}}$ de $\mathbb{K}$. Supongamos sin perder generalidad que $V = \mathbb{K}^n$. La prueba se sigue de las siguientes observaciones: el polinomio característico de $T$ pensado como transformación $\mathbb{K}$-lineal es el polinomio característico de una matriz $A \in \mathbb{K}^{n \times n}$ que representa a $T$ en la base canónica de $V$ y la condición $c_T(T) = 0$ es equivalente a $c_A(A) = 0$. Ahora bien, como el polinomio característico de la matriz $A$ calculado sobre $\mathbb{K}$ o $\overline{\mathbb{K}}$ es el mismo, concluimos del párrafo anterior que $c_A(A) = 0$ como queríamos probar. □

**Ejemplo 8.40.** Encontrar la inversa de la matriz

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

[3] Veremos más adelante la existencia de la clausura algebraica para cualquier cuerpo $\mathbb{K}$, por el momento podemos pensar que $\mathbb{K} = \mathbb{R}$ y $\overline{\mathbb{K}} = \mathbb{C}$.

Podemos ayudarnos del teorema de Cayley-Hamilton para decidir si $A$ es invertible y encontrar fácilmente su inversa. Calculamos el polinomio característico

$$c_A(x) = \det(A - xI) = (1-x)^3 + 2 = -x^3 + 3x^2 - 3x + 3$$

y usando que $c_A(A) = 0$ (¡este 0 representa la matriz nula!) concluimos que

$$3I = A^3 - 3A^2 + 3A = A(A^2 - 3A + 3I)$$

y por ende

$$A^{-1} = \frac{1}{3}A^2 - A + I = \begin{pmatrix} \frac{1}{3} & -\frac{2}{3} & \frac{2}{3} \\ \frac{1}{3} & \frac{1}{3} & -\frac{1}{3} \\ -\frac{1}{3} & \frac{2}{3} & \frac{1}{3} \end{pmatrix}.$$

# 9. Categorías

**7 may**

En este apartado presentamos las nociones básicas de la teoría de categorías, que además de ser interesante en sí misma, nos proveerá de un lenguaje muy elegante para continuar nuestro estudio de la teoría de módulos. Incluso muchos de los resultados de la teoría de módulos se generalizan a la teoría de categorías.

## 9.1. Definiciones básicas y ejemplos

**Definición 9.1.** Una *categoría* $\mathscr{C}$ consiste de lo siguiente.

- Una clase de *objetos*, denotada $\operatorname{obj}\mathscr{C}$.
- Una clase de *morfismos* o *flechas*, denotada $\operatorname{mor}\mathscr{C}$, junto con dos funciones de clase $\operatorname{dom} : \operatorname{mor}\mathscr{C} \to \operatorname{obj}\mathscr{C}$ y $\operatorname{codom} : \operatorname{mor}\mathscr{C} \to \operatorname{obj}\mathscr{C}$. O sea, para cada $f \in \operatorname{obj}\mathscr{C}$ se tiene que $A = \operatorname{dom} f \in \operatorname{obj}\mathscr{C}$ y $B = \operatorname{codom} f \in \operatorname{obj}\mathscr{C}$ y en este caso es común denotar $f : A \to B$. También es común la notación, para cada $A, B \in \operatorname{obj}\mathscr{C}$,

  $$\operatorname{Hom}(A, B) = \{f \in \operatorname{mor}\mathscr{C} : \operatorname{dom} f = A,\ \operatorname{codom} f = B\}.$$

- Para cada $A, B, C \in \operatorname{obj}\mathscr{C}$ existe una operación binaria de clases

  $$\operatorname{Hom}(A, B) \times \operatorname{Hom}(B, C) \to \operatorname{Hom}(A, C)$$

  que a cada par $(f, g)$ con $f : A \to B$ y $g : B \to C$ le asigna un morfismo $g \circ f : A \to C$ que satisface las siguientes propiedades.

  - Asociatividad: si $f : A \to B$, $g : B \to C$ y $h : C \to D$ entonces

    $$h \circ (g \circ f) = (h \circ g) \circ f$$

  - Identidad: para cada $A \in \operatorname{obj}\mathscr{C}$ existe $\operatorname{id}_A : A \to A$ tal que $\operatorname{id}_A \circ f = f$ para todos $B \in \operatorname{obj}\mathscr{C}$, $f : B \to A$ y $g \circ \operatorname{id}_A = g$ para todos $C \in \operatorname{obj}\mathscr{C}$, $g : A \to C$.

*Observación* 9.2. En la definición anterior utilizamos la palabra *clase*, un concepto que a veces es más general que el concepto de *conjunto*. Sin entrar en mucho detalle, mencionemos que en la teoría de conjuntos sobre la cual estamos trabajando tenemos las nociones de *clase* y *elemento de una clase*. Los *conjuntos* son las clases que a su vez son elementos de otras clases más grandes. Las *clases propias* son las clases que no son elementos de ninguna clase. Por ejemplo, el ejemplo paradigmático en teoría de categorías, es el de la categoría de todos los conjuntos, denotada **Set**. Los objetos de **Set** son los conjuntos y los morfismos son las funciones entre conjuntos. Es claro de los axiomas de la teoría de conjuntos que $\operatorname{obj}\mathbf{Set}$ y $\operatorname{mor}\mathbf{Set}$ son clases propias (ningún conjunto puede ser elemento de sí mismo). Una categoría $\mathscr{C}$ tal que $\operatorname{obj}\mathscr{C}$ y $\operatorname{mor}\mathscr{C}$ son conjuntos se llama *categoría pequeña*, en tanto que una categoría en la que sólo pedimos que $\operatorname{Hom}(A, B)$ sea un conjunto para todos $A, B \in \operatorname{obj}\mathscr{C}$ se dice *localmente pequeña*. Probar como ejercicio que toda categoría pequeña es localmente pequeña.

**Ejemplo 9.3.** Hay muchísimos ejemplos de categorías con los que ya estamos familiarizados. Resumimos algunos de los más comunes en la siguiente tabla.

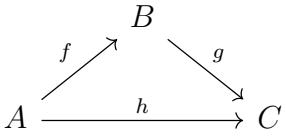
| $\mathscr{C}$ | $\operatorname{obj}\mathscr{C}$ | $\operatorname{mor}\mathscr{C}$ |
|---|---|---|
| **Set** | conjuntos | funciones |
| **Grp** | grupos | morfismos de grupos |
| **Ab** | grupos abelianos | morfismos de grupos (abelianos) |
| $R$-**Mod** | $R$-módulos unitarios a izquierda | morfismos de $R$-módulos (a izquierda) |
| **Mod**-$R$ | $R$-módulos unitarios a derecha | morfismos de $R$-módulos (a derecha) |
| $\mathbf{Vect}_{\mathbb{K}}$ | $\mathbb{K}$-espacios vectoriales | transformaciones lineales |
| **Rng** | anillos (con 1) | morfismos de anillos (con identidad) |
| **CRng** | anillos conmutativos (con 1) | morfismos de anillos (con identidad) |
| **Top** | espacios topológicos | funciones continuas |
| **Diff** | variedades diferenciables | funciones diferenciables |

Observar que en la tabla anterior $R$ es un anillo con identidad y $\mathbb{K}$ es un cuerpo. Notar que en la tabla algunas categorías aparecen dos veces, como por ejemplo $\mathbf{Ab} = \mathbb{Z}$-**Mod** y $\mathbf{Vect}_{\mathbb{K}} = \mathbb{K}$-**Mod**. Además en todos estos ejemplos los morfismos de la categoría son funciones entre los objetos (que preservan la estructura de los mismos). A continuación presentamos ejemplos de categorías que no son de este tipo.

**Ejemplo 9.4.** La categoría **0** es la categoría vacía, no tiene objetos ni morfismos. La categoría **1** consiste de un único objeto y un único morfismo (que debe ser la identidad de dicho objeto). No confundir este ejemplo con otros que veremos en breve, en donde hay un único objeto pero varios morfismos del mismo objeto en sí mismo. La categoría **2** consta de dos objetos y un morfismo entre ellos (además de las identidades). Está categoría se puede representar por el siguiente diagrama

$$A \xrightarrow{f} B$$

en el cual se omiten, como es usual en estos casos, las identidades $\mathrm{id}_A$ e $\mathrm{id}_B$. La categoría **3** puede representarse por el siguiente diagrama.



Notar que necesariamente tenemos que $h = g \circ f$.

**Ejercicio 9.5.** ¿Cómo definiría las categorías $\mathbf{4}, \mathbf{5}, \mathbf{6}, \ldots$?

**Ejemplo 9.6.** Recordemos que un *monoide* $(M, \cdot, e)$ (o simplemente $M$), es un conjunto con una operación binaria $(x, y) \mapsto x \cdot y$ (o simplemente $xy$) que es asociativa y satisface $x \cdot e = e \cdot x = x$ para todo $x \in M$. Es decir, es casi un grupo porque hay elemento neutro pero no se pide que existan los inversos. Un morfismo de monoides $f : M \to N$ es una función tal que $f(e_M) = e_N$ y $f(mm') = f(m)f(m')$ para todos $m, m' \in M$. Un ejemplo destacado de un monoide que no es un grupo es $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ con la operación de suma. Verificar que la clase de todos los monoides junto con la clase de todos los morfismos de monoides forman una categoría, denotada **Mon**.

**Ejemplo 9.7.** (i) Un grupo es, en particular, un monoide. Un morfismo de grupos es un morfismo de monoides.

(ii) Dar un ejemplo de una función entre dos monoides $f : M \to N$ tal que $f(mm') = f(m)f(m')$ para todos $m, m' \in M$ pero que $f$ no sea un morfismo de monoides.

**Ejemplo 9.8.** Si $M$ es un monoide, entonces podemos pensar a $M$ como una categoría con un solo objeto en la cual cada morfismo se corresponde con un elemento de $M$ y la composición de dos morfismos se corresponde con la multiplicación en $M$ (y, en particular, la identidad se corresponde con elemento neutro de $M$). Más aún, cualquier categoría pequeña $\mathscr{C}$ con un solo objeto esta unívocamente determinada por la estructura de monoide en $\operatorname{mor}\mathscr{C}$.

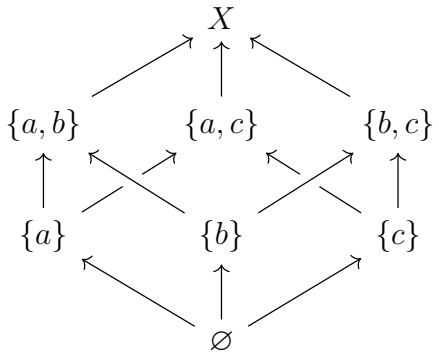
Como un caso particular de lo anterior, un grupo $G$ se identifica con una categoría pequeña $\mathscr{C}$ con un solo objeto $\operatorname{obj}\mathscr{C} = \{*\}$, y tal que todo morfismo tiene un morfismo inverso, es decir, para cada $f \in \operatorname{mor}\mathscr{C}$, existe $f^{-1} \in \operatorname{mor}\mathscr{C}$ tal que $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_*$.

**Ejemplo 9.9.** La categoría **Poset** es la categoría formada por los conjuntos parcialmente ordenados (posets) y las funciones monótonas. Es decir, una función $f : (P, \leq) \to (P', \leq')$ entre dos posets es un morfismo en la categoría **Poset** si y sólo si $x \leq y \implies f(x) \leq' f(y)$.

**Ejemplo 9.10.** Un poset $(P, \leq)$ puede pensarse como categoría categoría $\mathscr{C}$ en la cual $P$ es el conjunto de objetos y decimos que hay (a lo sumo) un morfismo entre $x$ e $y$ en $P$ si y sólo si $x \leq y$. Observar que, en particular, la desigualdad $x \leq x$ se corresponde con el morfismo $\mathrm{id}_x$ y la transitividad de $\leq$ se corresponde con la asociatividad de la composición.

Por ejemplo si consideramos el orden parcial dado por la inclusión en $\mathscr{P}(X)$ para un conjunto con tres elementos $X = \{a, b, c\}$, entonces la categoría que mencionamos en el párrafo anterior puede representarse con el siguiente diagrama, llamado el *diagrama de*

*Hasse* de orden parcial.




Observar que en el diagrama anterior, además de omitir las identidades, sólo dibujamos los morfismos que no son composición de otros dos morfismos.

**Ejemplo 9.11.** Dada una categoría $\mathscr{C}$, se define la categoría opuesta $\mathscr{C}^{\text{op}}$ como sigue. Los objetos de $\mathscr{C}^{\text{op}}$ son los mismos que los objetos de $\mathscr{C}$ y los morfismos de $\mathscr{C}^{\text{op}}$ son los mismos que los de $\mathscr{C}$ pero cambiando el sentido de las flechas. Más precisamente $f : A \to B$ en $\mathscr{C}^{\text{op}}$ si y sólo si $f : B \to A$ en $\mathscr{C}$ (en realidad esto es un abuso de notación y sería mejor escribir $f^{\text{op}}$, pero en la práctica queda todo bien claro a partir del contexto). La composición de morfismos en $\mathscr{C}^{\text{op}}$ se define como

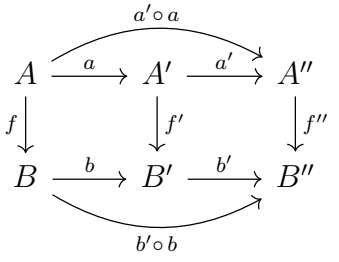
$$f \circ_{\text{op}} g = g \circ f,$$

en donde $\circ$ denota la composición en $\mathscr{C}$. Verificar como ejercicio que esta operación está bien definida y que $\mathscr{C}^{\text{op}}$ es efectivamente una categoría.

**Ejemplo 9.12.** Estudiemos un ejemplo un poco más sofisticado. La categoría $\mathbf{Set}^{\to}$ tiene como objetos a los morfismos de **Set**, es decir, un objeto en $\mathbf{Set}^{\to}$ es simplemente una función $f : A \to B$ entre dos conjuntos $A$ y $B$. Un morfismo entre $f : A \to B$ y $f' : A' \to B'$ consiste de un par ordenado de funciones $(a, b)$ en donde $a : A \to A'$ y $b : B \to B'$ son tales que $f' \circ a = b \circ f$, es decir, son tales que conmuta el siguiente diagrama

$$\begin{array}{ccc} A & \xrightarrow{a} & A' \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f'} \\ B & \xrightarrow{b} & B' \end{array}$$

Si tenemos dos morfismos $(a, b) : f \to f'$ y $(a', b') : f' \to f''$ (en donde $f'' : A'' \to B''$), entonces su composición se define como $(a', b') \circ (a, b) = (a' \circ a, b' \circ b)$, lo cual se visualiza mejor mirando el diagrama conmutativo



Usando diagramas también podemos ver que $\mathrm{id}_f = (\mathrm{id}_A, \mathrm{id}_B)$ puesto que conmuta el diagrama

$$\begin{array}{ccc} A & \xrightarrow{\mathrm{id}_A} & A \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ B & \xrightarrow{\mathrm{id}_B} & B \end{array}$$

y que la composición en $\mathbf{Set}^{\to}$ es asociativa sigue de que el diagrama

$$\begin{array}{ccccccc} A & \xrightarrow{a} & A' & \xrightarrow{a'} & A'' & \xrightarrow{a''} & A''' \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f''} & & \downarrow{\scriptstyle f'''} \\ B & \xrightarrow{b} & B' & \xrightarrow{b'} & B'' & \xrightarrow{b''} & B''' \end{array}$$

conmuta si conmuta cada cuadrado.

## 9.2. Funtores

Rápidamente hablando, los funtores son los morfismos de categorías. La definición formal de funtor es la siguiente.

**Definición 9.13.** Sean $\mathscr{C}, \mathscr{D}$ dos categorías. Un *funtor (covariante)* $F : \mathscr{C} \to \mathscr{D}$ asigna

- a cada objeto $A \in \operatorname{obj}\mathscr{C}$ un objeto $F(A) \in \operatorname{obj}\mathscr{D}$; y
- a cada morfismo $f \in \operatorname{mor}\mathscr{C}$ un morfismo $F(f) \in \operatorname{mor}\mathscr{D}$ tal que $\operatorname{dom} F(f) = F(\operatorname{dom} f)$ y $\operatorname{codom} F(f) = F(\operatorname{codom} f)$, es decir, si $f : A \to B$ entonces $F(f) : F(A) \to F(B)$, con las siguientes propiedades:
  - $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$ para todo $A \in \operatorname{obj}\mathscr{C}$;
  - $F(g \circ f) = F(g) \circ F(f)$ para todos $f : A \to B$, $g : B \to C$.

Sigue de la definición que un funtor $F : \mathscr{C} \to \mathscr{D}$ manda diagramas conmutativos en diagramas conmutativos.

*Observación* 9.14. Un funtor contravariante $F : \mathscr{C} \to \mathscr{D}$ suele definirse de manera similar pero intercambiando el sentido de las flechas, es decir, si $f \in \operatorname{Hom}(A, B)$ se pide que $F(f) \in \operatorname{Hom}(F(B), F(A))$ y que se cumpla $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$ y $F(g \circ f) = F(f) \circ F(g)$ cuando la composición tenga sentido.

Notar, sin embargo, que un funtor contravariante $F : \mathscr{C} \to \mathscr{D}$ no es otra cosa que un funtor covariante $F : \mathscr{C}^{\mathrm{op}} \to \mathscr{D}$.

**Ejemplo 9.15.** Observemos que dados dos funtores $F : \mathscr{C} \to \mathscr{D}$ y $G : \mathscr{D} \to \mathscr{E}$, tiene sentido definir $G \circ F : \mathscr{C} \to \mathscr{E}$ por $(G \circ F)(A) = G(F(A))$ para todo $A \in \operatorname{obj}\mathscr{C}$ y $(G \circ F)(f) = G(F(f))$ para todo $f \in \operatorname{mor}\mathscr{C}$. Verificar como ejercicio que $G \circ F$ es efectivamente un funtor. La categoría $\mathbf{Cat}$ es la categoría en la cual los objetos son las categorías pequeñas y los morfismos son los funtores. Verificar esto también como ejercicio.

Veamos a continuación algunos ejemplos concretos de funtores que ya conocemos.

**Ejemplo 9.16.** El funtor libre free : **Set** $\to$ $R$-**Mod** asigna a cada conjunto $X$ el $R$-módulo libre $F(X)$ en $X$ (que construimos en la Sección 7) y cada función $f : X \to Y$ el único morfismo de $R$-módulos free$(f) : F(X) \to F(Y)$ tal que free$(f)(x) = f(x)$ para todo $x \in X$. Verificar que efectivamente free es un funtor y analizar la situación análoga para free : **Set** $\to$ **Grp**.

**Ejemplo 9.17.** Los funtores de olvido se construyen en categorías concretas en las cuales desestimamos parte de la estructura que llevan los objetos. Por ejemplo tenemos un funtor olvido fgt : **Grp** $\to$ **Set** que asigna a cada grupo su conjunto subyacente y a cada morfismo de grupos la correspondiente función (verificar funtorialidad). Otros ejemplos de funtores de olvido son

- fgt : **Top** $\to$ **Set**
- fgt : **Grp** $\to$ **Mon**
- fgt : **Ab** $\to$ **Grp**
- fgt : $R$-**Mod** $\to$ **Ab**
- fgt : $\mathbf{Vect}_{\mathbb{C}} \to \mathbf{Vect}_{\mathbb{R}}$

**Ejemplo 9.18.** Si $G, H$ son dos grupos (o monoides) y los pensamos como categorías con un único objeto, entonces un funtor de $G$ en $H$ es exactamente un morfismo de grupos (o monoides) de $G$ en $H$.

**Ejemplo 9.19.** El funtor dual : $\mathbf{Vect}_{\mathbb{K}} \to \mathbf{Vect}_{\mathbb{K}}$ asigna a cada espacio vectorial $V$, su dual algebraico $V^* = \mathrm{Hom}_{\mathbb{K}}(V, K)$ y a cada transformación lineal $T : V \to W$ su transpuesta $T^t : W^* \to V^*$, en donde $T^t(\alpha)(v) = \alpha(Tv)$ para todo funcional lineal $\alpha : W \to \mathbb{K}$. El funtor dual es un ejemplo de un funtor contravariante (chequear como ejercicio).

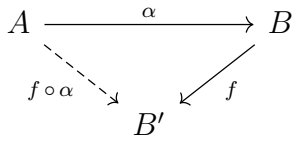
**Ejemplo 9.20.** Si $(P, \leq)$ y $(Q, \leq)$ son dos posets, pensados como categorías entonces un funtor covariante (resp. contravariante) de $(P, \leq)$ en $(Q, \leq)$ es exactamente una función monótona creciente (resp. decreciente) de $P$ en $Q$.

**Ejercicio 9.21.** Si $(P, \leq)$ es un poset, podemos dar a $P$ una topología natural, llamada topología de Alexandrov, en la cual los abiertos de $P$ son los *conjuntos superiores*. Es decir $A \subset P$ es un abierto si y sólo si para todo $x \in P$, $x \in A$ y $x \leq y$ implica $y \in A$. Probar que esta construcción induce un funtor $U$ : **Poset** $\to$ **Top**. *Ayuda*: una función $f : U(P) \to U(Q)$ es continua si y sólo si es monótona (creciente).

**Ejemplo 9.22.** Para cada categoría localmente pequeña $\mathscr{C}$ y cada objeto $A \in \mathrm{obj}\,\mathscr{C}$ se define un funtor

$$\mathrm{Hom}(A, -) : \mathscr{C} \to \mathbf{Set}$$

por $\mathrm{Hom}(A, -)(B) = \mathrm{Hom}(A, B)$ y para cada $f : B \to B'$. $\mathrm{Hom}(A, -)(f) = \mathrm{Hom}(A, f)$ la función que asigna a cada $\alpha \in \mathrm{Hom}(A, B)$ el morfismo $f \circ \alpha \in \mathrm{Hom}(A, B')$.



Análogamente, fijando $B \in \operatorname{obj}\mathscr{C}$ podemos definir un funtor contravariante

$$\operatorname{Hom}(-, B) : \mathscr{C} \to \mathbf{Set}\,.$$

Chequear como ejercicio que $\operatorname{Hom}(A, -)$ y $\operatorname{Hom}(-, B)$ son efectivamente funtores.

## 9.3. Monomorfismos, epimorfismos e isomorfismos

Las nociones de monomorfismo, epimorfismo e isomorfismo tienen sentido en una categoría arbitraria $\mathscr{C}$. Sea $f : A \to B$ un morfismo en $\mathscr{C}$. Decimos que $f$ es un

- *monomorfismo* si para todos $g, h : C \to A$, se tiene que $f \circ g = f \circ h$ implica $g = h$;
- *epimorfismo* si para todos $g, h : A \to C$, se tiene que $g \circ f = h \circ f$ implica $g = h$;
- *isomorfismo* si existe $f^{-1} : B \to A$ tal que $f \circ f^{-1} = \mathrm{id}_B$ y $f^{-1} \circ f = \mathrm{id}_A$.

*Observación* 9.23. (i) Los conceptos de monomorfismo y epimorfismo son conceptos duales. Es decir, la definición de uno se obtiene de la definición del otro dando vuelta el sentido de las flechas. Más precisamente, $f$ es un monomorfismo en $\mathscr{C}$ si y sólo si $f$ es un epimorfismo en $\mathscr{C}^{\mathrm{op}}$.

(ii) Dualizar es un proceso muy importante en teoría de categorías. El *principio de dualidad* esencialmente nos dice que si un teorema es válido para toda categoría, entonces el teorema dual (o coteorema) que se obtienen cambiando las flechas de lugar, también será válido para todas las categorías.

(iii) El concepto de isomorfismo es autodual. Es decir, si $f$ es un isomorfismo, entonces $f^{-1}$ también es un isomorfismo.

**Ejercicio 9.24.** En muchas de las categorías con las cuales estamos familiarizados, por ejemplo **Set**, **Grp**, $R$-**Mod**, **Top**, se tiene la siguiente propiedad: $f$ es un isomorfismo si y sólo si $f$ es monomorfismo y epimorfismo a la vez. Mostrar con un contraejemplo que esta afirmación no es válida en general.

## 9.4. Objetos iniciales, terminales y nulos

Fijemos una categoría $\mathscr{C}$. Decimos que $I \in \operatorname{obj}\mathscr{C}$ es un *objeto inicial* si para cada $A \in \operatorname{obj}\mathscr{C}$ existe exactamente un morfismo $I \to A$. Dualizando esta definición decimos que $T \in \operatorname{obj}\mathscr{C}$ es un *objeto terminal* si para cada $A \in \operatorname{obj}\mathscr{C}$ existe un único morfismo $A \to T$. Un *objeto nulo* (a veces llamado cero) en $\mathscr{C}$ es un objeto que es inicial y terminal a la vez.

Es fácil ver que los objetos iniciales, terminales, nulos son únicos salvo isomorfismo.

**Ejemplo 9.25.** (i) En **Set** el único objeto inicial es el conjunto vacío (¿por qué?), en tanto que los objetos terminales son singuletes o conjuntos que tienen un único elemento. No hay objetos nulos en la categoría **Set**.

(ii) En la categoría $\mathscr{C}$ de los conjuntos no vacíos no hay objeto inicial. En la categoría $\mathscr{C}^{\mathrm{op}}$ no hay objeto terminal.

(iii) **Grp** y $R$-**Mod** tienen objetos nulos (los grupos o $R$-módulos triviales).

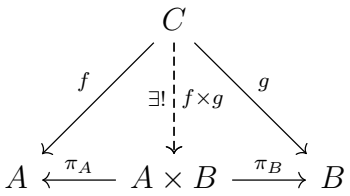
(iv) Si $P$ es un poset y lo pensamos como una categoría entonces los objetos iniciales o terminales se corresponden con mínimos y máximos (si es que existen).

(v) En **Cat** la categoría **0** es el único objeto inicial y la categoría **1** es un objeto terminal (ver Ejemplo 9.4).

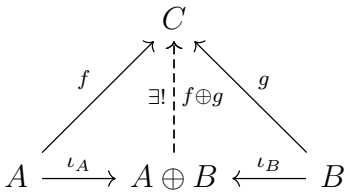
## 9.5. Productos y coproductos

La propiedad universal del producto cartesiano en las categorías que ya hemos estudiado nos dicen cómo deberíamos definir estos conceptos en categorías arbitrarias. Por simplicidad trabajamos con productos binarios, y en el próximo apartado veremos una manera más elegante de definir productos arbitrarios.

Sea $\mathscr{C}$ una categoría. Un *producto* de dos objetos $A$ y $B$ en $\mathscr{C}$ es un objeto $A \times B$ junto con dos morfismos $\pi_A : A \times B \to A$ y $\pi_B : A \times B \to B$ tales que para todo objeto $C$ y para todo par de morfismos $f : C \to A$ y $g : C \to B$ existe un único morfismo $f \times g : C \to A \times B$ tal que el siguiente diagrama conmuta.




El concepto dual de producto es el de coproducto. Un *coproducto* de $A$ y $B$ es un objeto $A \oplus B$ junto con dos morfismos $\iota_A : A \to A \oplus B$ y $\iota_B : B \to A \oplus B$ tal que para todo objeto $C$ y todo par de morfismos $f : A \to C$ y $g : B \to C$ existe un único morfismo $f \oplus g : A \oplus B \to C$ tal que el siguiente diagrama conmuta.




**Ejercicio 9.26.** Los productos (y coproductos) si existen son únicos salvo isomorfismo.

**Ejemplo 9.27.** El coproducto de $A$ y $B$ en **Set** es la unión disjunta $(A \times \{0\}) \cup (B \times \{1\})$ junto con las inclusiones $\iota_A(a) = (a, 0)$ y $\iota_B(b) = (b, 1)$.

**Ejemplo 9.28.** En $R$-**Mod** los productos y coproductos binarios coinciden.

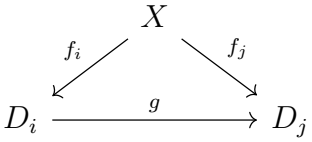
**Ejemplo 9.29.** En la categoría **Grp** el producto de $G$ con $H$ es el grupo producto $G \times H$, pero este grupo no es necesariamente el coproducto de $G$ y $H$. ¿Qué serían los coproductos en **Grp**?

**Ejercicio 9.30.** Sea $P$ un poset (pensado como una categoría). ¿Qué serían los productos y coproductos en $P$?

## 9.6. Límites y colímites

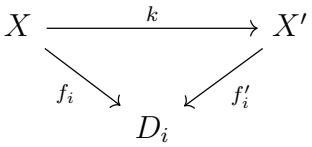
**24 abr**

Para hablar de (co)límites en teoría de categorías necesitamos introducir la noción de (co)conos y diagramas. Informalmente, un diagrama (no necesariamente conmutativo) en una categoría $\mathscr{C}$ puede pensarse como un (multi)grafo dirigido cuyos vértices son objetos de $\mathscr{C}$ y cuyas flechas son morfismos entre los vértices. Un cono sobre un diagrama $D$ con vértices $(D_i)_{i\in I}$ consiste de un objeto $X$ y una familia de morfismos $f_i : X \to D_i$ tales que para cada flecha $g : D_i \to D_j$ en el diagrama vale $g \circ f_i = f_j$, o sea, el siguiente diagrama conmuta




Un poco más formalmente, un *diagrama* de forma $\mathscr{J}$ es un funtor $D : \mathscr{J} \to \mathscr{C}$. En el caso de diagramas modificamos ligeramente la notación y escribimos $D_i$ en lugar de $D(i)$ para $i \in \text{obj}\,\mathscr{J}$. Un *cono* para $D$ consiste entonces de un objeto $X \in \text{obj}\,\mathscr{C}$ y una familia de morfismos $f_i : X \to D_i$, para $i \in \text{obj}\,\mathscr{J}$, tal que para todos $i, j \in \text{obj}\,\mathscr{J}$ y para todo $g \in \text{Hom}(i, j)$, vale $g \circ f_i = f_j$.

Observemos que dado un diagrama $D$ en una categoría $\mathscr{C}$ podemos formar la *categoría de conos*, denotada $\mathbf{Cone}(D)$ cuyos objetos son los conos sobre $D$ y los morfismos se definen como sigue. Si $C = \{f_i : X \to D_i\}$ y $C' = \{f'_i : X' \to D_i\}$ son dos conos sobre $D$, entonces un morfismo entre $C$ y $C'$ es un morfismo $k : X \to X'$ tal que para todo $D_i$ en el diagrama $D$, vale $f'_i \circ k = f_i$




**Ejercicio 9.31.** Verificar que $\mathbf{Cone}(D)$ es efectivamente una categoría.

**Definición 9.32.** Un *límite* para un diagrama $D$ en una categoría $\mathscr{C}$ es un objeto terminal en la categoría $\mathbf{Cone}(D)$.

**Ejemplo 9.33.** (i) Un objeto terminal en una categoría $\mathscr{C}$ es un límite para el diagrama vacío (¿por qué?). (Observemos que el diagrama vacío en $\mathscr{C}$ es en funtor $D : \mathbf{0} \to \mathscr{C}$.)

(ii) Un límite para el diagrama

$$A \qquad B$$

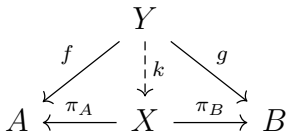
es exactamente un producto entre $A$ y $B$. En efecto, un límite para este diagrama es un cono

$$A \xleftarrow{\pi_A} X \xrightarrow{\pi_B} B$$

con la propiedad de que dado otro cono

$$A \xleftarrow{f} Y \xrightarrow{g} B$$

entonces existe un único morfismo $k : Y \mapsto X$ tal que conmuta el diagrama

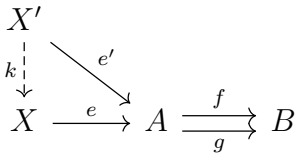



Luego por definición $X$ junto con los morfismos (proyecciones) $\pi_A$, $\pi_B$ constituyen un producto entre $A$ y $B$.

**Ejemplo 9.34.** Un *ecualizador* de dos morfismos $f, g : A \to B$ es un límite para el diagrama

$$A \underset{g}{\overset{f}{\rightrightarrows}} B$$

Es decir, es un morfismo $e : X \to A$ tal que $f \circ e = g \circ e$ con la propiedad de que dado otro morfismo $e' : X' \to A$ tal que $f \circ e' = g \circ e'$, entonces existe un único morfismo $k : X' \to X$ tal que conmuta el diagrama




(9.1)

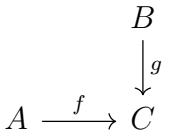
Para entender un poco mejor este concepto mostremos que la categoría **Set** tiene ecualizadores. En efecto, en este caso tanto $f$ como $g$ son funciones de $A$ y $B$, si definimos

$$X = \{a \in A : f(a) = g(a)\}$$

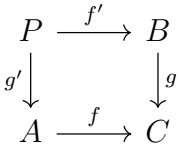
entonces la inclusión $e : X \to A$ es un ecualizador de $f$ y $g$. Para esto, notemos que si $e' : X' \to X$ es una función tal que $f \circ e' = g \circ e'$ entonces $k : X' \to X$ definida como $k(x') = e'(x)$ está bien definida y es tal que el diagrama (9.1) conmuta (completar los detalles como ejercicio).

Observemos que este ejemplo motiva aun más el nombre ecualizador.

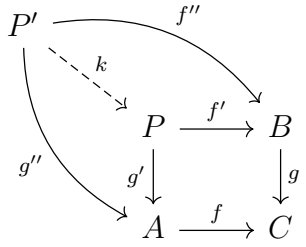
**Ejemplo 9.35.** Un *pullback* de dos morfismos $f : A \to C$ y $g : B \to C$ es un límite para el diagrama




o sea es un objeto $P$ junto con dos morfismos $f' : P \to B$ y $g' : P \to A$ tales que conmuta el diagrama



y con la propiedad de que si $P'$ es otro objeto y $f'' : P' \to B$, $g'' : P' \to A$ es otro par de morfismos tales que $g \circ f'' = f \circ g'$, entonces existe un único morfismo $k : P' \to P$ tal que conmuta el diagrama




**Ejemplo 9.36.** Chequear como ejercicio que los siguientes diagramas son pullbacks.

(i) En una categoría con productos y objeto terminal $T$,

$$\begin{array}{ccc} A \times B & \xrightarrow{\pi_B} & B \\ {\scriptstyle \pi_A}\downarrow & & \downarrow{\scriptstyle !} \\ A & \xrightarrow{!} & T \end{array}$$

(ii) En **Set**,

$$\begin{array}{ccc} A \cap B & \hookrightarrow & B \\ \downarrow & & \downarrow \\ A & \hookrightarrow & C \end{array}$$

en donde $A$ y $B$ son subconjuntos de $C$

(iii) En **Set**,

$$\begin{array}{ccc} f^{-1}(A) & \hookrightarrow & B \\ {\scriptstyle f|_{f^{-1}(A)}}\downarrow & & \downarrow{\scriptstyle f} \\ A & \hookrightarrow & C \end{array}$$

en donde $f : B \to C$ es una función cualquiera y $A$ es un subconjunto de $C$.

**Ejercicio 9.37.** (i) Mostrar que en **Set** el pullback de $A \xrightarrow{f} C \xleftarrow{g} B$ puede construirse como $P = \{(a, b) \in A \times B : f(a) = g(b)\}$ en donde $f' = \pi_B|_P$ y $g' = \pi_A|_P$.

(ii) Mostrar que la construcción anterior también sirve como pullback en **Ab**.

El concepto dual a límite es el de *colímite*. Para definir colímites, definimos primero lo que es un cocono para un diagrama y luego decimos que un colímite para un diagrama $D$ es un objeto inicial en la categoría **coCone**$(D)$. Queda como ejercicio escribir detalladamente esta definición completando todos los detalles y estudiar los ejemplos duales de los límites que ya vimos. Prestar especial atención al dual del pullback, que usualmente se denomina *pushout* (ver la guía de ejercicios).

## 9.7. Transformaciones naturales

Uno de los conceptos más importantes en teoría de categorías es el de transformación natural. Rápidamente hablando, pero en un sentido que precisaremos más adelante, una transformación natural es un morfismo entre dos funtores.

**Definición 9.38.** Dados dos funtores $F, G : \mathscr{C} \to \mathscr{D}$ una *transformación natural*

$$\eta : F \Longrightarrow G$$

es una familia de morfismos $\eta_X : F(X) \to G(X)$, para cada $X \in \operatorname{obj} \mathscr{C}$, tal que para todo morfismo $f : X \to Y$ en $\mathscr{C}$, conmuta el diagrama

$$\begin{array}{ccc} F(X) & \xrightarrow{\eta_X} & G(X) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(Y) & \xrightarrow{\eta_Y} & G(Y) \end{array}$$

Alternativamente suele decirse que el morfismo $\eta_X$ es natural en $X$. Si además se cumple que cada $\eta_X$ es un isomorfismo, entonces $\eta$ se llama un *isomorfismo natural* o se dice que $F$ y $G$ son naturalmente isomorfos.

Veamos algunos ejemplos concretos.

**Ejemplo 9.39.** Fijemos un cuerpo $\mathbb{K}$ y consideremos un $\mathbb{K}$-espacio vectorial $V$ de dimensión finita. En este caso tenemos que $V$ es isomorfo a su dual $V^*$: tienen la misma dimensión y para cada base de $V$ uno se puede construir la correspondiente base dual de $V^*$. Con el mismo argumento vemos que $V$ es isomorfo al doble dual $V^{**}$, pero en este caso suele decirse informalmente que el isomorfismo es natural, porque uno puede darlo sin tener que elegir una base. En efecto, el isomorfismo del que hablamos es el que asigna a cada $v \in V$, la transformación lineal $v^{**} : V^* \to \mathbb{K}$ definida como $v^{**}(\alpha) = \alpha(v)$.

En un sentido categórico lo que tenemos que es una transformación natural

$$\sigma : \mathrm{id}_{\mathbf{Vect}_{\mathbb{K}}} \to \mathrm{dual} \circ \mathrm{dual}$$

entre el funtor identidad y el funtor doble dual definida como sigue: $\sigma_V : V \to V^{**}$ es la transformación lineal $\sigma_V(v) = v^{**}$ (dada por la misma fórmula de más arriba, solo que en el caso de dimensión infinita esto ya no es un isomorfismo). La naturalidad se chequea observando que si $T : V \to W$ es una transformación lineal, entonces conmuta el diagrama

$$\begin{array}{ccc} V & \xrightarrow{\sigma_V} & V^{**} \\ {\scriptstyle T}\downarrow & & \downarrow{\scriptstyle (T^t)^t} \\ W & \xrightarrow{\sigma_W} & W^{**} \end{array} \tag{9.2}$$

Si nos restringimos a la categoría de espacios vectoriales de dimensión finita, entonces $\sigma$ es un isomorfismo natural y la conmutatividad del diagrama (9.2) puede interpretarse diciendo que cuando transponemos dos veces una matriz obtenemos la matriz original.

**Ejemplo 9.40.** La definición de transformación natural también sirve para explicar el hecho de que $V$ y $V^*$ no son naturalmente isomorfos, en donde $V$ es un espacio vectorial de dimensión finita. Con la definición naive de isomorfismo natural deberíamos demostrar que cualquier isomorfismo entre $V$ y $V^*$ supone la elección de una base. Esto resulta tan ambiguo que prácticamente es imposible. Con nuestra nueva definición de isomorfismo natural queda clarísimo que el funtor identidad no puede ser naturalmente isomorfo al funtor dual, pues uno es covariante y el otro contravariante.

**Ejemplo 9.41.** La función determinante es una transformación natural. Más precisamente, si pensamos en el determinante de matrices $n \times n$ con coeficientes en un anillo conmutativo con identidad $R$, obtenemos un morfismo de grupos $\det_R : \mathrm{GL}_n(R) \to R^\times$, en donde $\mathrm{GL}_n(R)$ es el grupo de matrices invertibles de tamaño $n \times n$ con coeficientes en $R$ y $R^\times = \mathrm{GL}_1(R)$ es el grupo multiplicativo de unidades de $R$. Notar además que $\mathrm{GL}_n : \mathbf{CRng} \to \mathbf{Grp}$ es un funtor de la categoría **CRng** de anillos conmutativos con identidad en la categoría de grupos **Grp**. En particular, $(\ )^\times = \mathrm{GL}_1$ es un funtor de **CRng** en **Grp** y el hecho de que $\det : \mathrm{GL}_n \Longrightarrow (\ )^\times$ significa que para todo morfismo de anillos $f : R \to S$, conmuta el diagrama

$$\begin{array}{ccc} \mathrm{GL}_n(R) & \xrightarrow{\det_R} & R^\times \\ {\scriptstyle \mathrm{GL}_n(f)}\downarrow & & \downarrow{\scriptstyle f^\times} \\ \mathrm{GL}_n(S) & \xrightarrow{\det_S} & S^\times \end{array}$$

Completar los detalles como ejercicio.

**Ejercicio 9.42.** Recordemos que si $G$ es un grupo, el *conmutador* de $G$ es el subgrupo $[G, G]$ generado por todos los elementos de la forma $ghg^{-1}h^{-1}$, con $g, h \in G$. Se tiene que $[G, G]$ es un subgrupo normal de $G$ y que $G/[G, G]$ es abeliano. Esto da lugar a un funtor $\mathbf{Grp} \to \mathbf{Ab}$, llamado *abelianizador* (explicar cómo actúa este funtor en un morfismo $G \to H$). Probar que la asignación $G \mapsto G/[G, G]$ es natural en $G$ (explicitando bien qué significa esto).

**Ejemplo 9.43.** (i) Para cada funtor $F : \mathscr{C} \to \mathscr{D}$, podemos definir una transformación natural $\mathrm{id}_F : F \Longrightarrow F$ por $(\mathrm{id}_F)_X = \mathrm{id}_{F(X)} : F(X) \to F(X)$. En efecto, la naturalidad sigue de la conmutatividad del diagrama

$$\begin{array}{ccc} F(X) & \xrightarrow{\mathrm{id}_{F(X)}} & F(X) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle F(f)} \\ F(Y) & \xrightarrow{\mathrm{id}_{F(X)}} & F(Y) \end{array}$$

para todo morfismo $f : X \to Y$.

(ii) Observemos que si $\eta : F \Longrightarrow G$ y $\tau : G \Longrightarrow H$ son dos transformaciones naturales, en donde $F, G, H : \mathscr{C} \to \mathscr{D}$ son tres funtores entre las mismas categorías, entonces para cualquier morfismo $f : X \to Y$, el siguiente diagrama conmuta

$$\begin{array}{ccccc} F(X) & \xrightarrow{\eta_X} & G(Y) & \xrightarrow{\tau_X} & H(Y) \\ \downarrow{\scriptstyle F(f)} & & \downarrow{\scriptstyle G(f)} & & \downarrow{\scriptstyle H(f)} \\ F(Y) & \xrightarrow{\eta_Y} & G(Y) & \xrightarrow{\tau_Y} & H(Y) \end{array}$$

En efecto, el rectángulo exterior conmuta pues los dos cuadrados lo hacen. Esto significa que podemos definir una transformación natural $\tau \circ \eta : F \Longrightarrow H$ por $(\tau \circ \eta)_X = \tau_X \circ \eta_X$

(iii) Los dos ítems anteriores nos permiten construirla categoría $\mathscr{D}^{\mathscr{C}}$ cuyos objetos son los funtores de $\mathscr{C}$ en $\mathscr{D}$ y cuyos morfismos son las transformaciones naturales. Como siempre, chequear los detalles como ejercicio.

**Ejercicio 9.44.** En una categoría localmente pequeña, cada morfismo $g : B \to B'$ induce una transformación natural entre los funtores $\mathrm{Hom}(-, B)$ y $\mathrm{Hom}(-, B')$. Más precisamente, el morfismo correspondiente para cada objeto $A$ es $\mathrm{Hom}(A, g) : \mathrm{Hom}(A, B) \to \mathrm{Hom}(A, B')$. Para chequear la naturalidad hay que verificar que el siguiente diagrama conmuta para cada morfismo $f : A \to A'$.

$$\begin{array}{ccc} \mathrm{Hom}(A, B) & \xrightarrow{\mathrm{Hom}(A,g)} & \mathrm{Hom}(A, B') \\ {\scriptstyle \mathrm{Hom}(f,B)}\uparrow & & \uparrow{\scriptstyle \mathrm{Hom}(f,B')} \\ \mathrm{Hom}(A', B) & \xrightarrow{\mathrm{Hom}(A',g)} & \mathrm{Hom}(A', B') \end{array}$$

Concluir que cada morfismo $f : A \to A'$ induce una transformación natural entre los funtores $\mathrm{Hom}(A', -)$ y $\mathrm{Hom}(A, -)$.

## 9.8. Categorías abelianas

En esta materia estaremos muy interesados en una clase particular de categorías llamadas categorías abelianas. El ejemplo fundamental de este tipo de categorías es la categoría $R$-**Mod**. Para poder definir este concepto, tenemos que precisar en el lenguaje de la teoría de categorías algunas construcciones que sabemos hacer para grupos y módulos.

### 9.8.1. Categorías aditivas

**Definición 9.45.** Una *categoría aditiva* es una categoría localmente pequeña $\mathscr{C}$ en la cual cada $\mathrm{Hom}(A, B)$ tiene una estructura de grupo abeliano tal que para todos $f, g, h \in \mathrm{Hom}(A, B)$ se tiene

$$f \circ (g + h) = f \circ g + f \circ h$$

y

$$(f + g) \circ h = f \circ h + g \circ h.$$

Es decir, la composición se distribuye con respecto a la suma (a izquierda y derecha).

Claramente **Ab** y $R$-**Mod** son categorías aditivas. Veremos más adelante algunos otros ejemplos.

Algunos conceptos que pueden definirse en categorías arbitrarias, tienen una interpretación sencilla en categorías aditivas, en términos de la estructura de grupo en $\mathrm{Hom}(A, B)$. Por ejemplo, un objeto nulo $Z$, tal como lo definimos en el apartado 9.4, es precisamente

un objeto tal que $\mathrm{Hom}(A, Z) = \{0\}$ y $\mathrm{Hom}(Z, B) = \{0\}$ son los grupos triviales cualesquiera sean los objetos $A$ y $B$. Otro ejemplo, un *morfismo nulo* $f : A \to B$ en una categoría con objeto nulo $Z$ es un morfismo tal que los siguientes diagramas conmutan


Para una categoría aditiva, un morfismo nulo $f : A \to B$ es precisamente el elemento neutro de $\mathrm{Hom}(A, B)$ (esto tiene sentido incluso si $\mathscr{C}$ no tiene objeto nulo).

A partir de ahora, a los objetos (y morfismos) nulos trataremos de denotarlos con un 0, indicando con subíndices los dominios o codominios si fuera necesario.

*Observación* 9.46. Observemos que si $\mathscr{C}$ es una categoría aditiva, entonces $\mathscr{C}^{\mathrm{op}}$ también lo es, con la misma estructura de grupo abeliano en $\mathrm{Hom}^{\mathrm{op}}(A, B) = \mathrm{Hom}(B, A)$.

### 9.8.2. Biproductos

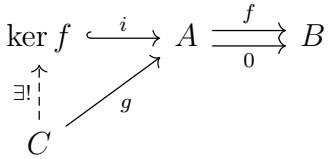
En una categoría aditiva los productos finitos (si existen) "coinciden" con los coproductos. Damos una idea informal para la demostración formal de este hecho. Supongamos que $A \times B$ es un producto de $A$ por $B$ con proyecciones $\pi_A$ y $\pi_B$. Podemos construir las inclusiones $\iota_A : A \to A \times B$ y $\iota_B : B \to A \times B$ como $\iota_A = \mathrm{id}_A \times 0_B$ y $\iota_B = 0_A \times \mathrm{id}_B$ (denotamos por $0_A$ y $0_B$ los morfismos nulos de $A$ en $A$ y $B$ en $B$ respectivamente y usamos la propiedad universal del producto). Queda como ejercicio verificar que $A \times B$ es, junto con $\iota_A$ y $\iota_B$ un coproducto de $A$ y $B$. Observar que se tienen las igualdades $\pi_A \circ \iota_A = \mathrm{id}_A$, $\pi_B \circ \iota_B = \mathrm{id}_B$, $\pi_A \circ \iota B = 0_{B,A}$, $\pi_B \circ \iota_A = 0_{A,B}$ y $\iota_A \circ \pi_A + \iota_B \circ \pi_B = \mathrm{id}_{A \times B}$.

Recíprocamente, a partir de un coproducto $A \oplus B$ con inclusiones $\iota_A$ y $\iota_B$ podemos recuperar el producto $A \times B$ definiendo $\pi_A = \mathrm{id}_A \oplus 0_B$ y $\pi_B = 0_A \oplus \mathrm{id}_B$

En una categoría abeliana un producto (y por ende coproducto) de $A$ y $B$ (o de una familia finita de objetos) se llama un *biproducto* y en general lo denotaremos por $A \oplus B$.

### 9.8.3. Kernels y cokernels

Observemos que la definición de kernel o núcleo de un morfismo, digamos en **Ab**, puede formularse de manera categórica. Más precisamente, si $f : A \to B$ es un morfismo de grupos abelianos, entonces por definición $\ker f = \{a \in A : f(a) = 0\}$ es un subgrupo de $A$, el cual podemos identificar con el morfismo $i : \ker f \hookrightarrow A$, el cual se caracteriza por la siguientes propiedades: $f \circ i = 0$ y todo morfismo $g : C \to A$ tal que $f \circ g = 0$ se factoriza unívocamente a través de $i$, o sea el siguiente diagrama es conmutativo.




Es decir, y esta es la definición para cualquier categoría aditiva, el *kernel* de un morfismo $f : A \to B$ es el ecualizador de $f$ y el morfismo nulo $0 : A \to B$. Notar que esta definición puede pensarse como una versión categórica de los teoremas de isomorfismo.

La definición dual es la de *cokernel* de un morfismo $f : A \to B$, que es el coecualizador de los morfismos $f : A \to B$ y $0 : A \to B$. En el caso de la categoría **Ab**, el cokernel de $f$ se puede construir como $\operatorname{coker} f = B/\operatorname{im} f$, que se identifica con la proyección $p : B \to B/\operatorname{im} f$ caracterizado por las propiedades: $p \circ f = 0$ y que toda $g : B \to C$ tal que $g \circ f = 0$ se factoriza unívocamente a través de $p$, es decir el siguiente diagrama conmuta

$$\begin{array}{ccccc} A & \underset{0}{\overset{f}{\rightrightarrows}} & B & \xrightarrow{p} & B/\operatorname{im} f \\ & & & \searrow^{g} & \downarrow{\scriptstyle \exists!} \\ & & & & C \end{array}$$

*Observación* 9.47. Una propiedad notable de la categoría **Ab**, entre otras, es que dado un grupo abeliano $A$, todo subgrupo de $A$ es el kernel de algún morfismo y dado un grupo abeliano $B$ todo cociente de $B$ es el cokernel de algún morfismo. Otra forma de decir esto es que todo monomorfismo es el kernel de algún morfismo y todo epimorfismo es el cokernel de algún morfismo. Notar que esto no vale en **Grp**.

### 9.8.4. Categorías abelianas

Una categoría aditiva $\mathscr{C}$ se dice una *categoría abeliana* si

- tiene un objeto nulo,
- tiene todos los biproductos binarios,
- todo morfismo tiene kernel y cokernel,
- todos monomorfismo es un kernel y todo epimorfismo es un cokernel.

Las categorías con las que trabajamos en esta materia, siendo la más importante la categoría $R$-**Mod**, son todas ejemplos de categorías abelianas. A modo de ejemplo y para practicar un poco dejamos algunas propiedades elementales de las categorías abelianas (los detalles en las demostraciones quedan como ejercicios), que ya hemos visto para $R$-**Mod**.

**Proposición 9.48.** *Sea $\mathscr{C}$ una categoría abeliana y $f : A \to B$ un morfismo en $\mathscr{C}$. Entonces*

(i) *$f$ es un monomorfismo si y sólo si $i : \ker f \to A$ es un morfismo nulo;*

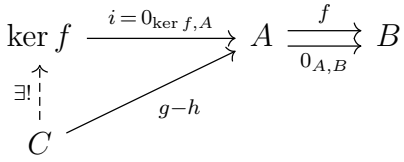
(ii) *$f$ es un epimorfismo si y sólo si $p : B \to \operatorname{coker} f$ es un morfismo nulo;*

(iii) *$f$ es un isomorfismo si y sólo si es monomorfismo y epimorfismo a la vez.*

*Idea de la Demostración.* Los enunciados (iii) y (ii) son duales, por lo que basta probar uno de ellos. Para ver, por ejemplo, (iii) notemos que el siguiente diagrama es conmutativo

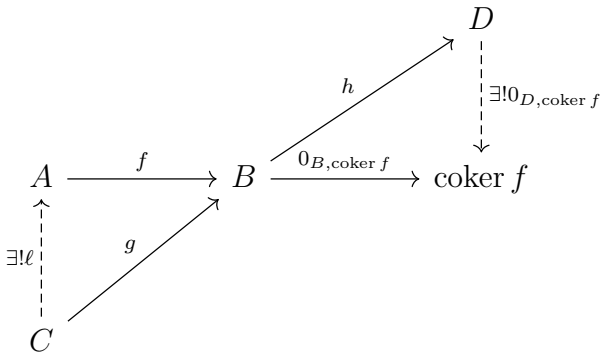
$$\ker f \underset{0_{\ker f, A}}{\overset{i}{\rightrightarrows}} A \xrightarrow{f} B$$

Lo que dice que $f \circ i = f \circ 0_{\ker f,A} = 0_{\ker f,B}$. Luego, si $f$ un monomorfismo se tiene que $i = 0_{\ker f,A}$. Recíprocamente, supongamos que el kernel de $f$ es el morfismo nulo. Debemos probar que dadas $g, h : C \to A$ tales que $f \circ g = f \circ h$, se tiene $g = h$. Notar que esta última condición es equivalente a que $g - h : C \to A$ satisfaga $f \circ (g - h) = 0_{C,B}$ (¡recordar que $\mathrm{Hom}(C, A)$ es un grupo abeliano y la composición se distribuye con la suma!). Con lo cual, $g - h$ se factoriza a través de $i : \ker f \to A$.

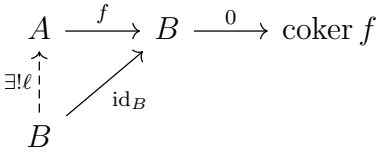



Como $i = 0_{\ker f,A}$ tenemos que $g - h = 0$.

Ya vimos, y esto vale en cualquier categoría, que un isomorfismo es monomorfismo y epimorfismo. Luego para probar la parte (iii) tenemos que ver que si $f$ es monomorfismo y epimorfismo a la vez entonces tiene inversa. La idea que en esta situación $f$ es un kernel de $0 : B \to \mathrm{coker}\, f$ y un cokernel de $0 : \ker f \to A$. Notar que probando una de estas dos propiedades tenemos gratis (por dualidad) la otra. Damos la idea general y los detalles quedan para completar como ejercicio. Para probar que $f$ es un kernel de $0_{B,\mathrm{coker}\, f} : B \to \mathrm{coker}\, f$ tenemos que probar que cualquier morfismo $g : C \to B$ se factoriza a través de $f$ (pues siempre tenemos que $0_{B,\mathrm{coker}\, f} \circ g = 0_{C,\mathrm{coker}\, f}$). Como estamos en una categoría abeliana, sabemos que $f$ es el kernel de algún morfismo $h : B \to D$. Además $h \circ g = 0_{C,D}$ pues el cokernel de $f$ es el morfismo nulo. Esto nos indica cómo construir un único morfismo $\ell : C \to A$ que factoriza a $g$ a través de $f$. Este argumento se puede resumir con el siguiente diagrama conmutativo.




Para construir la inversa de $f$ nos interesa el siguiente caso particular:




De aquí sigue que $f \circ \ell = \mathrm{id}_B$. Para terminar la prueba, hay que mostrar que además vale $\ell \circ f = \mathrm{id}_A$. Aquí usamos que $f$ es un cokernel de $0 : \ker f \to A$ y por unicidad tenemos

que el siguiente diagrama conmuta.

$$\begin{array}{ccccc} \ker f & \xrightarrow{0} & A & \xrightarrow{f} & B \\ & & & \searrow^{\mathrm{id}_A} & \downarrow{\scriptstyle \ell} \\ & & & & A \end{array}$$

□

# 10. Sucesiones exactas

## 10.1. Discusión informal

Para motivar un poco la definición de sucesión exacta, mencionaremos al pasar el concepto de homología de un complejo de cadenas. Un complejo de cadenas $A_\bullet$, digamos en la categoría **Ab**, es una sucesión de grupos abelianos y morfismos

$$\cdots \longrightarrow A_{n+1} \xrightarrow{d_{n+1}} A_n \xrightarrow{d_n} A_{n-1} \longrightarrow \cdots \tag{10.1}$$

tal que $d_n \circ d_{n+1} = 0$ para todo $n$ (a veces se escribe simplemente $d^2 = 0$). Esto es equivalente a que $\operatorname{im} d_{n+1} \subset \ker d_n$. Asociado a un complejo de cadenas se tienen definidos los llamados *grupos de homología*

$$H_n(A_\bullet) = \frac{\ker d_n}{\operatorname{im} d_{n+1}}$$

los cuales constituyen una construcción central en topología algebraica. Digamos rápidamente que dado un espacio topológico $X$ uno tiene asociado un complejo de cadenas $C_\bullet(X)$ y su correspondiente homología $H_\bullet(X)$ (en realidad hay muchas variantes para la construcción del complejo de cadenas). Más aún, lo que obtenemos es un funtor de la categoría de (ciertos) espacios topológicos en la categoría de los complejos de cadenas. A modo de ejemplo, y sin demostración, mencionemos que para la esfera $n$-dimensional $S^n$ se tiene

$$H_i(S^n) = \begin{cases} \mathbb{Z}, & i = 0, n \\ 0, & i \neq 0, n \end{cases}$$

Una aplicación notable de este hecho es la siguiente.

**Corolario 10.1.** *$\mathbb{R}^n$ es homeomorfo a $\mathbb{R}^m$ si y sólo si $n = m$.*

*Demostración.* La idea de la prueba es la siguiente. Si removemos el origen $0 \in \mathbb{R}^n$ la función $f : (\mathbb{R}^n - \{0\}) \times [0, 1] \to S^{n-1}$ definida por

$$f(x, t) = \left(1 - t + \frac{t}{\|x\|}\right) x$$

es un *retracto por deformación*, es decir,

- $f$ es continua,
- $f(x, 0) = x$ para todo $x \in \mathbb{R}^n - \{0\}$, y

- $f(x,t) = x$ para todo $x \in S^{n-1}$ y para todo $t \in [0,1]$

Es un hecho general que si tenemos un retracto por deformación $f : X \to A$ de un espacio topológico $X$ sobre un subespacio $A$, entonces $X$ y $A$ son homotópicamente equivalentes (no importa ahora qué significa esto) y por consiguiente tienen la misma homología. Luego, por funtorialidad, $\mathbb{R}^n$ no puede ser homeomorfo a $\mathbb{R}^m$ si $n \neq m$. □

*Observación* 10.2. Notemos sin embargo que $H_i(\mathbb{R}^n) = H_i(\mathbb{R}^m)$ para todo $i$, pues $\mathbb{R}^n$ se puede retraer por deformación a un punto (¿por qué?).

Nosotros estamos interesados en estudiar sucesiones exactas, que son cadenas como en (10.1) pero en las que además pedimos $\operatorname{im} d_{n+1} = \ker d_n$ (de ahí proviene el adjetivo "exacta"). Obviamente la homología de una sucesión exacta es trivial, pero esto no significa que las sucesiones exactas no sean interesantes e útiles de estudiar, como veremos más adelante.

## 10.2. Propiedades elementales de las sucesiones exactas

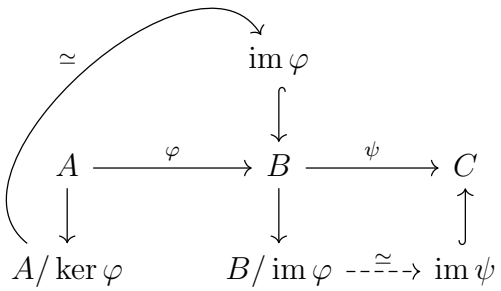
En lo que sigue todos los anillos se asumen con 1 y todos los módulos unitarios.

**Definición 10.3.** Una secuencia (finita o infinita) de morfismos (de módulos, grupos, etc.)

$$\cdots \xrightarrow{\varphi_{i-1}} M_i \xrightarrow{\varphi_i} M_{i+1} \xrightarrow{\varphi_{i+1}} M_{i+2} \xrightarrow{\varphi_{i+2}} \cdots$$

se dice una *sucesión exacta* si $\operatorname{im} \varphi_i = \ker \varphi_{i+1}$ para todo $i$.

Observemos que si $A \xrightarrow{\varphi} B \xrightarrow{\psi} C$ es una sucesión exacta entonces $B$ contiene un submódulo $\operatorname{im} \varphi \simeq A/\ker \varphi$ tal que $B/\operatorname{im} \varphi = B/\ker \psi \simeq \operatorname{im} \psi$:




**Ejemplo 10.4.** (i) $0 \longrightarrow A \xrightarrow{\varphi} B$ es exacta si y sólo si $\varphi$ es un monomorfismo.

(ii) $A \xrightarrow{\varphi} B \longrightarrow 0$ es exacta si y sólo si $\varphi$ es un epimorfismo.

(iii) $0 \longrightarrow A \xrightarrow{\varphi} B \longrightarrow 0$ es exacta si y sólo si $\varphi$ es un isomorfismo.

Notar que estos ejemplos también son válidos en la categoría de grupos, cambiando el módulo trivial 0 por el grupo trivial $\{e\}$.

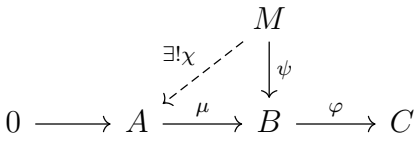
**Definición 10.5.** (i) Una sucesión exata de la forma $0 \longrightarrow A \longrightarrow B \longrightarrow C$ se dice *exacta a izquierda*;

(ii) una sucesión exacta de la forma $A \longrightarrow B \longrightarrow C \longrightarrow 0$ se dice *exacta a derecha*;

(iii) una sucesión exacta de la forma $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ se dice *sucesión exacta corta*.

Observar que si $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ es una sucesión exacta corta, entonces $B$ contiene un subódulo $B' \simeq A$ tal que $B/B' \simeq C$.

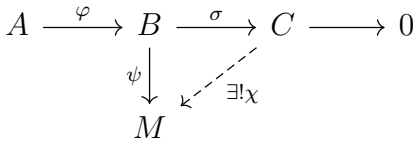
**Lema 10.6.** *Sea* $0 \longrightarrow A \xrightarrow{\mu} B \xrightarrow{\varphi} C$ *una sucesión exacta a izquierda. Entonces todo morfismo* $\psi : M \to B$ *tal que* $\varphi \circ \psi = 0$ *se factoriza unívocamente a través de* $\mu$*. Es decir, existe un único morfismo* $\chi : M \to A$ *tal que* $\mu \circ \chi = \psi$*.*



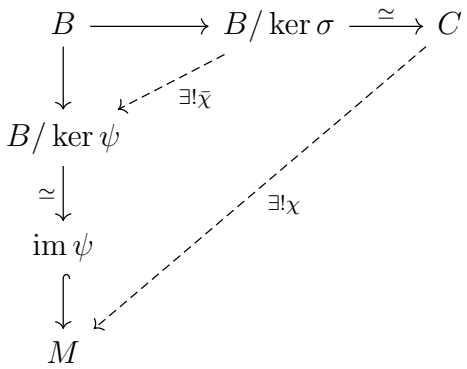

*Demostración.* La condición $\varphi \circ \psi = 0$ implica $\operatorname{im}\psi \subset \ker\varphi = \operatorname{im}\mu$. Como $\mu$ es inyectiva, existe una única $\chi : M \to A$ tal que $\mu \circ \chi = \psi$. Observar que $\chi = \mu^{-1} \circ \psi$ es morfismo de módulos. □

El coteorema del lema anterior también es válido.

**Lema 10.7.** *Sea* $A \xrightarrow{\varphi} B \xrightarrow{\sigma} C \longrightarrow 0$ *una sucesión exacta a derecha. Entonces todo morfismo* $\psi : B \to M$ *tal que* $\psi \circ \varphi = 0$ *se factoriza unívocamente a través de* $\sigma$*. Es decir, existe un único morfismo* $\xi : C \to M$ *tal que* $\chi \circ \sigma = \psi$*.*




*Demostración.* Como $\ker\sigma = \operatorname{im}\varphi \subset \ker\psi$, por los teoremas de isomorfismos, existe un único morfismo $\bar{\chi} : B/\ker\sigma \to B/\ker\psi$ que conmuta con la prouección al cociente $B \to B/\ker\psi$. Además, como $\sigma$ es epimorfismo, $B/\ker\sigma \simeq C$. Luego existe una única $\chi : C \to \operatorname{im}\psi \subset M$ tal que el siguiente diagrama conmuta.




□

**Ejercicio 10.8.** Los Lemas 10.6 y 10.7 son válidos en la categoría de grupos.

**Lema 10.9** (Lema de los cinco)**.** *En un diagrama conmutativo con filas exactas*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\mu} & B & \xrightarrow{\rho} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow{\mu'} & B' & \xrightarrow{\rho'} & C' & \longrightarrow & 0 \end{array}$$

*si $\alpha$ y $\gamma$ son isomorfismos, entonces $\beta$ es isomorfismo.*

*Demostración.* Supongamos que $\beta(b) = 0$, luego $0 = \rho'(\beta(b)) = \gamma(\rho(b))$, de donde $\rho(b) = 0$. Es decir, $b \in \ker \rho = \operatorname{im} \mu$. Así $b = \mu(a)$ para algún $a$ y por ende $0 = \beta(\mu(a)) = \mu'(\alpha(a))$. Esto implica $\alpha(a) = 0$ y por consiguiente $a = 0$. Luego $\beta$ es inyectiva.

Recíprocamente, sea $b' \in B'$. Entonces $\rho'(b') = \gamma(c)$ para algún $c \in C$, el cual es de la forma $c = \rho(b)$ para algún $b \in B$. Luego $\rho'(\beta(b)) = \gamma(\rho(b)) = \gamma(c) = \rho'(b')$. Esto implica que $b' - \beta(b) \in \ker \rho' = \operatorname{im} \mu'$. Así $b' - \beta(b) = \mu'(a')$ para algún $a' \in A'$. Finalmente podemos escribir $a' = \alpha(a)$ para algún $a \in A$ y concluir que

$$\begin{aligned} b' &= \beta(b) + \mu'(\alpha(a)) \\ &= \beta(b) + \beta(\mu(a)) \\ &= \beta(b + \mu(a)). \end{aligned}$$

Esto dice que $\beta$ es sobre. □

**Ejercicio 10.10.** Es cierto el Lema 10.9 en la categoría de grupos.

## 10.3. Sucesiones exactas que se parten

El ejemplo más general de sucesión exacta en el que podemos pensar es básicamente una proyección al cociente: si $A$ es un submódulo de $B$, entonces

$$0 \longrightarrow A \hookrightarrow B \longrightarrow B/A \longrightarrow 0 \tag{10.2}$$

es una sucesión exacta corta. De hecho, toda sucesión exacta corta es de esta forma. Otro ejemplo muy importante de sucesión exacta corta se puede construir usando las proyecciones e inclusiones en una suma directa. En efecto, si $A$ y $C$ son dos módulos, entonces

$$0 \longrightarrow A \xhookrightarrow{\iota} A \oplus C \xrightarrow{\pi} C \longrightarrow 0 \tag{10.3}$$

es una sucesión exacta corta, en donde $\iota$ es la inclusión del primer sumando y $\pi$ es la proyección al segundo. Observar (ejercicio) que no toda sucesión de la forma (10.2) es de la forma (10.3). El siguiente resultado nos da un criterio para decidir cuándo sucede esto.

**Proposición 10.11.** *Dada una sucesión exacta corta*

$$0 \longrightarrow A \xrightarrow{\mu} B \xrightarrow{\rho} C \longrightarrow 0$$

*son equivalentes:*

(i) *$\mu$ se parte (i.e. existe $\sigma : B \to A$ tal que $\sigma \circ \mu = \mathrm{id}_A$);*

(ii) *$\rho$ se parte (i.e. existe $\nu : C \to B$ tal que $\rho \circ \nu = \mathrm{id}_C$);*

(iii) *existe un isomorfismo $\theta : B \to A \oplus C$ tal que el siguiente diagrama conmuta*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\mu} & B & \xrightarrow{\rho} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_A} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \mathrm{id}_C} & & \\ 0 & \longrightarrow & A & \xrightarrow{\iota} & A \oplus C & \xrightarrow{\pi} & C & \longrightarrow & 0 \end{array} \tag{10.4}$$

*Demostración.* (i) $\implies$ (iii): supongamos que $\sigma \circ \mu = \mathrm{id}_A$ y sea $\theta : B \to A \oplus C$ definida por $\theta(b) = (\sigma(b), \rho(b))$. Observemos que

$$\theta(\mu(a)) = (\sigma(\mu(a)), \rho(\mu(a))) = (a, 0) = \iota(a)$$

para todo $a$ y por ende $\theta \circ \mu = \iota$. Por otro lado,

$$\pi(\theta(b)) = \pi(\sigma(b), \rho(b)) = \rho(b).$$

para todo $b$, de donde sigue que $\pi \circ \theta = \rho$. Luego, con $\theta$ así definida, el diagrama (10.4) conmuta y por el Lema 10.9, $\theta$ resulta un isomorfismo.

(ii) $\implies$ (iii): supongamos que $\rho \circ \nu = \mathrm{id}_C$ y sea $\zeta : A \oplus C \to B$ definida por $\zeta(a, c) = \mu(a) + \nu(c)$ (propiedad universal de la suma directa). Entonces

$$\rho(\zeta(a, c)) = \rho(\mu(a) + \nu(c)) = \rho(\nu(c)) = c = \pi(a, c)$$

con lo cual $\rho \circ \zeta = \pi$, y por otro lado

$$\zeta(\iota(a)) = \zeta(a, 0) = \mu(a)$$

de donde sigue que $\zeta \circ \iota = \mu$. Usando nuevamente el Lema de los Cinco, concluimos que $\zeta$ es un isomorfismo.

(iii) $\implies$ (i), (ii): denotemos por $\pi' : A \oplus C \to A$, $\iota' : C \to A \oplus C$ la proyección e inclusión del segundo sumando, respectivamente. Definimos $\sigma = \pi' \circ \theta$ y $\nu = \theta^{-1} \circ \iota'$. Luego,

$$\rho(\mu(a)) = \pi'(\theta(\mu(a))) = \pi'(\iota(a)) = a$$

para todo $a \in A$ y

$$\nu(\rho(c)) = \theta^{-1}(\iota'(\rho(c))) = \theta^{-1}(\theta(c)) = c$$

para todo $c \in C$. El siguiente diagrama conmutativo ilustra esta construcción.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \underset{\sigma}{\overset{\mu}{\rightleftarrows}} & B & \underset{\nu}{\overset{\rho}{\rightleftarrows}} & C & \longrightarrow & 0 \\ & & {\scriptstyle \mathrm{id}_A}\downarrow & & {\scriptstyle \theta^{-1}}\uparrow\downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \mathrm{id}_C} & & \\ 0 & \longrightarrow & A & \underset{\pi'}{\overset{\iota}{\rightleftarrows}} & A \oplus C & \underset{\iota'}{\overset{\pi}{\rightleftarrows}} & C & \longrightarrow & 0 \end{array}$$

□

# 11. Módulos proyectivos

**Definición 11.1.** Un $R$-módulo (a izquierda) $P$ se dice *proyectivo* si todo homomorfismo que sale de $P$ se puede *levantar* o factorizar a través de cualquier epimorfismo sobre el módulo de llegada: es decir, si $\varphi : P \to N$, $\rho : M \to N$ son homomorfismos con $\rho$ sobre, entonces existe $\psi : P \to M$ tal que $\varphi = \rho \circ \psi$. Podemos expresar esto con el siguiente diagrama conmutativo

$$\begin{array}{ccccc} & & P & & \\ & \overset{\exists\psi}{\swarrow} & \downarrow{\scriptstyle \varphi} & & \\ M & \xrightarrow{\rho} & N & \longrightarrow & 0 \end{array}$$

con fila exacta.

Observar que en la definición no se pide que $\psi$ sea única (de hecho, en general no lo es).

**Proposición 11.2.** *Todo módulo libre es proyectivo.*

*Demostración.* Sea $F$ un módulo libre y sea $(e_i)_{i\in I}$ una base de $F$. Sean además $\varphi : F \to N$, $\rho : M \to N$ homomorfismos con $\rho$ sobreyectiva. Luego, para cada $i \in I$ existe $m_i \in M$ tal que $\rho(m_i) = \varphi(e_i)$. Por la propiedad universal de los módulos libres, existe un homomorfismo $\psi : F \to M$ tal que $\psi(e_i) = m_i$. Así $\rho(\psi(e_i)) = \varphi(e_i)$ para todo $i \in I$, y por lo tanto $\rho \circ \psi = \varphi$. □

Una consecuencia inmediata de la proposición anterior es que todo espacio vectorial es proyectivo. Además, se ve claramente en la demostración que no hay una única manera de definir $\psi$ (salvo que $\rho$ sea un isomorfismo).

Observar que si $P$ es proyectivo, entonces cualquier epimorfismo $\rho : M \to P$ se parte (en el sentido de que existe $\mu : P \to M$ tal que $\rho \circ \mu = \mathrm{id}_P$). Esto es evidente considerando el diagrama

$$\begin{array}{ccccc} & & P & & \\ & \overset{\exists\mu}{\swarrow} & \downarrow{\scriptstyle \mathrm{id}_P} & & \\ M & \xrightarrow{\rho} & P & \longrightarrow & 0 \end{array}$$

Más generalmente, se tiene el siguiente resultado.

**Proposición 11.3.** *Sea $P$ un $R$-módulo. Las siguientes afirmaciones son equivalentes.*

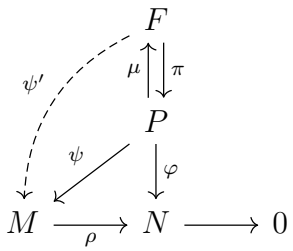
(i) *$P$ es proyectivo.*

(ii) *Todo epimorfismo $M \to P$ se parte.*

(iii) *Toda sucesión exacta corta $0 \to A \to B \to P \to 0$ se parte.*

*Demostración.* Ya observamos que (i) implica (ii). Además, probamos la clase pasada que (ii) es equivalente a (iii). Para completar la prueba basta ver que (ii) implica (i). En efecto, supongamos que todo epimorfismo sobre $P$ se parte y sean $\varphi : P \to N$, $\rho : M \to N$ homomorfismos con $\rho$ sobreyectiva. Sea $\pi : F \to P$ un epimorfismo de un módulo libre $F$ sobre $P$. Como $F$ es proyectivo, entonces existe $\psi' : F \to M$ tal que $\varphi \circ \pi = \rho \circ \psi'$.

Además, por hipótesis existe un homomorfismo $\mu : P \to F$ tal que $\pi \circ \mu = \mathrm{id}_P$. Luego, si $\psi = \psi' \circ \mu$, entonces $\varphi = \rho \circ \psi$, como queríamos probar. El siguiente diagrama conmutativo




ilustra mejor el procedimiento para encontrar $\psi$. □

Queda como ejercicio probar las siguientes propiedades básicas de los módulos proyectivos.

**Proposición 11.4.** *Todo sumando directo de un módulo proyectivo es proyectivo.*

**Proposición 11.5.** *Toda suma directa de $R$-módulos proyectivos es proyectiva.*

*Nota* 11.6. Como consecuencia de la proposición sigue que el producto directo de una familia finita de $R$-módulos proyectivos es proyectivo. Sin embargo, esta propiedad no es cierta para el producto directo de una familia infinita de $R$-módulos proyectivos. (En la guía hay un ejercicio importante que da un contraejemplo.)

El siguiente corolario da una caracterización de módulos proyectivos en términos de módulos libres.

**Corolario 11.7.** *Un módulo es proyectivo si y sólo si es isomorfo a un sumando directo de un módulo libre.*

*Demostración.* Sigue de la Proposición 11.2 y de la Proposición 11.4 que todo sumando directo de un módulo libre es proyectivo. Recíprocamente, si $P$ es proyectivo y $\pi : F \to P$ es un epimorfismo, en donde $F$ es un módulo libre, entonces por la Proposicióm 11.3 la sucesion exacta corta

$$0 \longrightarrow \ker \pi \hookrightarrow F \xrightarrow{\pi} P \longrightarrow 0$$

se parte y por ende $F \simeq \ker \pi \oplus P$. □

**Corolario 11.8.** *Sea $R$ un DIP. Entonces $P$ es un $R$-módulo proyectivo si y sólo si $P$ es libre.*

*Demostración.* La Proposición 11.2 dice que si $P$ es libre, entonces es proyectivo. Recíprocamente, si $P$ es proyectivo entonces $P$ es isomorfo a un sumando directo de un $R$-módulo libre. Pero ya vimos (no trivial), que cuando $R$ es un DIP, todo submódulo de un módulo libre es libre. □

**Ejemplo 11.9.** El corolario anterior nos dice que un grupo abeliano es proyectivo (pensado como $\mathbb{Z}$-módulo) si y sólo si es (isomorfo a) una suma directa de copias de $\mathbb{Z}$.

**Ejemplo 11.10.** El módulo $\mathbb{Z}_2 \hookrightarrow \mathbb{Z}_6 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_3$ es un $\mathbb{Z}_6$-módulo proyectivo que no es libre. ¿Por qué?

**Ejercicio 11.11.** Probar la siguiente generalización del Ejemplo 11.10: $P$ es un $\mathbb{Z}_6$-módulo proyectivo si y sólo si $P$ es libre. (Notar que no se puede aplicar el Corolario 11.8.)

# 12. Módulos inyectivos

La definición de módulo inyectivo es dual a la de módulo proyectivo, es decir, se obtiene invirtiendo el sentido de las flechas en el diagrama que usamos para definir un módulo proyectivo.

**Definición 12.1.** Un $R$-módulo (a izquierda) $J$ se dice *inyectivo* si todo morfismo que llega a $J$ puede ser factorizado o *extendido* a través de cualquier monomorfismo: es decir, si $\varphi : M \to J$ y $\mu : M \to N$ son morfismos de módulos con $\mu$ inyectiva, entonces existe $\psi : N \to J$ tal que $\varphi = \psi \circ \mu$. Podemos expresar esto con el siguiente diagrama conmutativo

$$\begin{array}{ccccc} & & J & & \\ & & \uparrow{\scriptstyle \varphi} & \nwarrow^{\exists \psi} & \\ 0 & \longrightarrow & M & \xrightarrow[\mu]{} & N \end{array}$$

con fila exacta.

Al igual que en el caso de los módulos proyectivos, $\psi$ no necesariamente es única.

Observar que si $J$ es inyectivo, entonces cualquier monomorfismo $\mu : J \to M$ se parte (es decir, existe $\rho : M \to J$ tal que $\rho \circ \mu = \mathrm{id}_J$). Esto sigue inmediatamente de la definición considerando el diagrama

$$\begin{array}{ccccc} & & J & & \\ & & \uparrow{\scriptstyle \mathrm{id}_J} & \nwarrow^{\exists \rho} & \\ 0 & \longrightarrow & J & \xrightarrow{\mu} & M \end{array}$$

**Proposición 12.2.** *Sea $J$ un $R$-módulo. Las siguientes afirmaciones son equivalentes.*

(i) *$J$ es inyectivo.*

(ii) *Todo monomorfismo $J \to M$ se parte.*

(iii) *Toda sucesión exacta corta $0 \to J \to B \to C \to 0$ se parte.*

(iv) *$J$ es un sumando directo de todo $R$-módulo $M$ tal que $J \subset M$.*

*Demostración.* (i) $\Rightarrow$ (ii) fue observado antes de enunciar la proposición. (ii) $\Leftrightarrow$ (iii) ya lo probamos cuando estudiamos sucesiones exactas. (iii) $\Rightarrow$ (iv) y (iv) $\Rightarrow$ (ii) salen considerando la sucesión exacta corta $0 \to J \hookrightarrow M \to M/J \to 0$ (completar los detalles).

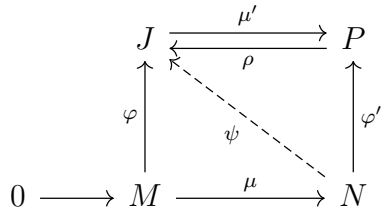
Para probar (ii) $\Rightarrow$ (i) fijamos un monomorfismo $\mu : M \to N$ y un morfismo $\varphi : M \to J$ y consideramos el pushout de $\varphi, \mu$

$$\begin{array}{ccc} J & \xrightarrow{\mu'} & P \\ {\scriptstyle \varphi}\uparrow & & \uparrow{\scriptstyle \varphi'} \\ M & \xrightarrow{\mu} & N \end{array} \tag{12.1}$$

Como $\mu$ es un monomorfismo, $\mu'$ debe ser un monomorfismo. Por hipótesis $\mu' : J \to P$ se parte, luego, existe $\rho : P \to J$ tal que $\rho \circ \mu' = \mathrm{id}_J$. Definiendo $\psi = \rho \circ \varphi'$ tenemos que

$$\begin{aligned}\psi \circ \mu &= (\rho \circ \varphi') \circ \mu = \rho \circ (\varphi \circ \mu) \\ &= \rho \circ (\mu' \circ \varphi) = (\rho \circ \mu') \circ \varphi \\ &= \mathrm{id}_J \circ \varphi = \varphi.\end{aligned}$$

La construcción anterior se ilustra mejor con el siguiente diagrama.




□

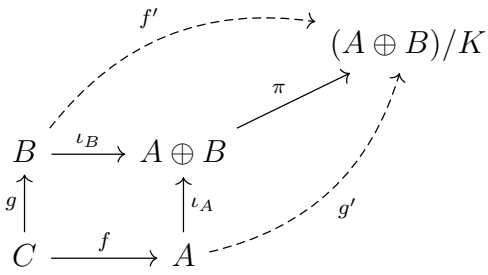
**Ejercicio 12.3.** (i) En la demostración anterior usamos el pushout de dos morfismos en la categoría $R$-**Mod**. La existencia del pushout puede probarse en general para cualquier categoría con colímites y coecualizadores, pero veamos una construcción concreta para $R$-módulos. Dados dos morfismos

$$\begin{array}{ccc} & & B \\ & & {\scriptstyle g}\uparrow \\ C & \xrightarrow{f} & A \end{array} \tag{12.2}$$

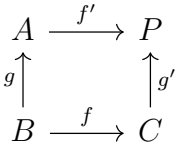
consideramos el submódulo $K$ de $A \oplus B$ definido por

$$K = \{(f(c), -g(c)) : c \in C\}.$$

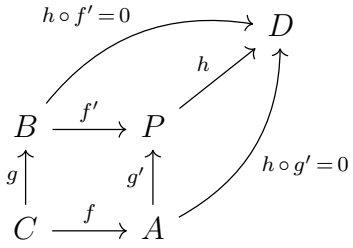
Probar que $(P = (A \oplus B)/K, f', g')$ es un pushout de (12.2), en donde $\pi : A \oplus B \to P$ es la proyección al cociente, y $f' = \pi \circ \iota_B$, $g' = \pi \circ \iota_A$.




(ii) Supongamos que el siguiente diagrama es un pushout.



(a) Probar que si $f$ es un monomorfismo, entonces $f'$ es un monomorfismo. *Ayuda*: supongamos que existe $h : P \to D$ tal que $h \circ f' = 0$. Probar que $h \circ f = 0$, de donde sigue (por unicidad) que $h = 0$.




(b) Probar que si $f$ es un epimorfismo, entonces $f'$ es un epimorfismo.

Quedan como ejercicio las siguientes propiedades básicas de los módulos inyectivos.

**Proposición 12.4.** *Todo sumando directo de un módulo inyectivo es inyectivo.*

**Proposición 12.5.** *Todo producto directo de $R$-módulos inyectivos es inyectivo.*

En particular, una suma directa finita de $R$-módulos inyectivos es inyectiva. Esta propiedad no necesariamente vale para la suma directa de una familia infinita de módulos inyectivos (como veremos más adelante en el Ejemplo 12.20).

Una manera más interesante de encontrar ejemplos de módulos inyectivos es usando el llamado criterio de Baer.

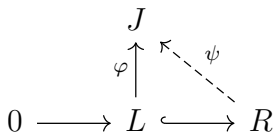
**Proposición 12.6** (Criterio de Baer)**.** *Sea $J$ un $R$-módulo. Las siguientes afirmaciones son equivalentes.*

(i) *$J$ es inyectivo.*

(ii) *Todo morfismo de módulos de un ideal a izquierda de $R$ en $J$ se extiende a ${}_RR$.*

(iii) *Para cada morfismo de módulos $\varphi : L \to J$ con $L$ un ideal a izquierda de $R$, existe $m \in J$ tal que $\varphi(r) = rm$ para todo $r \in L$.*

*Demostración.* (i) $\Rightarrow$ (ii). Sean $L$ un ideal a izquierda de $R$ y $\varphi : L \to J$ un morfismo de $R$-módulos. Como $J$ es inyectivo, existe un morfismo de $R$-módulos $\psi : R \to J$ tal que $\psi(r) = \varphi(r)$ para todo $r \in L$.




(ii) $\Leftrightarrow$ (iii) queda como ejercicio. Veamos (ii) $\Rightarrow$ (i). Debemos probar que cualquier morfismo de módulos $\varphi : M \to J$ se extiende a través de cualquier monomorfismo $\mu : M \to N$. Observar que como $M$ es isomorfo a un submódulo de $N$, se puede asumir que $M \subset N$ y que $\mu$ es el morfismo inclusión. La idea de la prueba es usar el Lema de Zorn para probar que $\varphi$ admite una extensión maximal a un submódulo de $N$.

Sea $\mathscr{S}$ el conjunto de todos los pares ordenados $(A, \alpha)$, en donde $A$ es un submódulo de $N$ que contiene a $M$ y $\alpha : A \to J$ es un morfismo de módulos que extiende a $\varphi$. Claramente $(M, \varphi) \in \mathscr{S}$, con lo cual $\mathscr{S} \neq \varnothing$. Definimos en $\mathscr{S}$ el orden parcial $\leq$ dado por: $(A, \alpha) \leq (B, \beta)$ si y sólo si $A \subset B$ y $\beta$ extiende a $\alpha$. Observemos que cada cadena $(A_i, \alpha_i)_{i \in I}$ en $\mathscr{S}$ tiene una cota superior $(A, \alpha) \in \mathscr{S}$ dada por $A = \bigcup_{i \in I} A_i$ y $\alpha(x) = \alpha_i(x)$ siempre que $x \in A_i$ (verificar esto como ejercicio). Luego, por el Lema de Zorn, existe un elemento maximal $(C, \gamma) \in \mathscr{S}$.

Supongamos que $C \neq N$. Sean $b \in N - C$ y $B = C + Rb$. Entonces

$$L = \{r \in R : rb \in C\}$$

es un ideal a izquierda de $R$ y $r \mapsto \gamma(rb)$ es un morfismo de módulos de $L$ en $J$. Por hipótesis, existe un morfismo de módulos $\psi : R \to J$ tal que $\psi(r) = \gamma(rb)$ para todo $r \in L$. Luego, podemos definir un morfismo de módulos $\beta : B \to J$ por

$$\beta(c + rb) = \gamma(c) + \psi(r)$$

para todo $r \in R$, $c \in C$ En efecto, para ver que $\beta$ está bien definido notemos que si $c + rb = c' + r'b$, para $c' \in C$, $r' \in R$, entonces $(r - r')b = c' - c \in C$ y por tanto $r - r' \in L$. Luego, $\psi(r - r') = \gamma(rb - r'b) = \gamma(c' - c)$, con lo cual $\gamma(c) + \psi(r) = \gamma(c') + \psi(r')$. Esto prueba la buena definición y es fácil ver que $\beta$ es un morfismo de módulos. Así, $\beta : B \to J$ extiende a $\gamma$ con $C \subsetneq B$. Esto implica que $(C, \gamma)$ no es maximal en $\mathscr{S}$, lo cual es absurdo. Como consecuencia, $C = N$ y $\gamma$ extiende a $\varphi$ a todo $N$. □

El criterio de Baer es muy útil en el caso en que $R$ es un DIP.

**Definición 12.7.** Un $R$-módulo $M$ se dice *divisible* si la ecuación $rx = a$ admite una solución $x \in M$ para todo $a \in M$ y para todo $r \in R - \{0\}$.

**Proposición 12.8.** *Si $R$ es un dominio íntegro, entonces todo $R$-módulo inyectivo es divisible.*

*Demostración.* Sea $J$ un $R$-módulo inyectivo. Sean $a \in J$ y $0 \neq r \in R$. Como $R$ es un dominio íntegro, todo elemento de $Rr$ se puede escribir como $tr$ para un único $t \in R$. Luego $\varphi : Rr \to J$, $\varphi(tr) = ta$, define un morfismo de módulos de $Rr$ en $J$. Por la Proposición 12.6, existe $m \in J$ tal que $\varphi(s) = sm$ para todo $s \in Rr$. Luego $a = \varphi(r) = rm$. □

**Proposición 12.9.** *Si $R$ es un DIP, entonces un $R$-módulo es inyectivo si y sólo si es divisible.*

*Demostración.* Por la proposición anterior, sólo debemos probar que todo $R$-módulo divisible es inyectivo. Sean $M$ un $R$-módulo divisible y $Rr$ un ideal (a izquierda) de $R$. (Notar que como $R$ es DIP, todo ideal es de esta forma.) Sea $\varphi : Rr \to M$ un morfismo de módulos. Si $r = 0$, entonces $\varphi(s) = s0$ para todo $s \in Rr$. Si no $\varphi(r) = rm$ para algún $m \in M$, pues $M$ es divisible. Luego $\varphi(tr) = trm$ para todo $tr \in Rr$. Así, $M$ resulta inyectivo por la Proposición 12.6. □

## 12.1. Grupos abelianos divisibles

De acuerdo con la Proposición 12.9 un grupo abeliano es inyectivo (pensado como un $\mathbb{Z}$-módulo) si y sólo si es divisible. A continuación mencionamos los ejemplos más importantes (crf. Teorema 12.14 más abajo).

**Ejemplo 12.10.** $\mathbb{Q}$ es un grupo abeliano divisible. Claramente, si $m \in \mathbb{Q}$ y $r \in \mathbb{Z} - \{0\}$, entonces $x = m/r \in \mathbb{Q}$ satisface $rx = m$.

**Ejemplo 12.11.** Para cada primo $p \in \mathbb{Z}$, tenemos que $\mathbb{Z}_{p^\infty}$ es un grupo abeliano divisible. La prueba de este hecho la veremos en la siguiente proposición, pero antes recordemos (o veamos por primera vez) la definición de $\mathbb{Z}_{p^\infty}$. El grupo abeliano $\mathbb{Z}_{p^\infty}$ puede definirse de manera elegante como la componente $p$-primaria del grupo abeliano $\mathbb{Q}/\mathbb{Z}$. Una forma más concreta de visualizarlo es la siguiente. Sea

$$\mathbb{Z}[1/p] = \{q \in \mathbb{Q} : p^k q \in \mathbb{Z} \text{ para algún } k \in \mathbb{N}\}.$$

Como $\mathbb{Z} \subset \mathbb{Z}[1/p]$, tiene sentido definir $\mathbb{Z}_{p^\infty} = \mathbb{Z}[1/p]/\mathbb{Z}$ el cual es un subgrupo de $\mathbb{Q}/\mathbb{Z}$.

Hay distintas caracterizaciones del grupo $\mathbb{Z}_{p^\infty}$ como puede verse a continuación.

**Ejercicio 12.12.** (i) Probar que efectivamente, $\mathbb{Z}_{p^\infty}$ es la componente $p$-primaria de $\mathbb{Q}/\mathbb{Z}$.

(ii) Probar que $\mathbb{Z}_{p^\infty}$ es el (único) $p$-subgrupo de Sylow de $\mathbb{Q}/\mathbb{Z}$.

(iii) Probar que $\mathbb{Z}_{p^\infty}$ es isomorfo al grupo definido por generadores y relaciones como

$$\langle a_1, a_2, \ldots \mid a_1^p = e,\ a_i^p = a_{i-1} \text{ para todo } i \geq 2\rangle.$$

(iv) Se puede presentar a $\mathbb{Z}_{p^\infty}$ como un subgrupo del círculo de la siguiente forma. Sea $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ el conjunto de números complejos de módulo 1 (¡el cual es un grupo con la multiplicación!). Observemos que cualquier elemento no nulo de $\mathbb{Z}_{p^\infty}$ tiene un representante de la forma $q = m/p^k$ para ciertos $m \in \mathbb{Z}$, $k \in \mathbb{N}$ con $m, p$ coprimos. Se puede definir entonces $\varphi : \mathbb{Z}_{p^\infty} \to S^1$ por $\varphi(\bar{q}) = e^{2im\pi/p^k}$. Probar que $\varphi$ está bien definida y es un monomorfismo de grupos.

**Proposición 12.13.** *$\mathbb{Z}_{p^\infty}$ es unión de una cadena de subgrupos cíclicos*

$$C_1 \subset C_2 \subset C_3 \subset \cdots$$

*de órdenes $p$, $p^2$, $p^3, \ldots$ respectivamente (es decir, $C_i$ es isomorfo a $\mathbb{Z}_{p^i}$) y es un grupo abeliano divisible.*

*Demostración.* Llamemos $\pi : \mathbb{Z}[1/p] \to \mathbb{Z}_{p^\infty}$ a la proyección al cociente y sea $C_k$ el subgrupo cíclico de $\mathbb{Z}_{p^\infty}$ generado por $\pi(1/p^k)$. Observemos que como $p^k\pi(1/p^k) = \pi(1) = 0$ y

$$0 < 1/p^k < 2/p^k < \cdots < (p^k - 1)/p^k < 1,$$

entonces

$$\pi(0),\ \pi(1/p^k),\ \pi(2/p^k) = 2\pi(1/p^k), \ldots,\ \pi((p^k - 1)/p^k) = (p^k - 1)\pi(1/p^k)$$

son elementos distintos en $C_k$. Luego, $C_k$ es cíclico de orden $p^k$ y $C_1 \subset C_2 \subset C_3 \subset \cdots$. Además, como ya observamos más arriba, cualquier elemento no nulo de $\mathbb{Z}_{p^\infty}$ tiene un representante de la forma $m/p^k$ para algún $k \in \mathbb{N}$ y $m \in \mathbb{Z}$. Luego, $\pi(m/p^k) = m\pi(1/p^k) \in C_k$ y por lo tanto $\mathbb{Z}_{p^\infty} = \bigcup_{k\geq 1} C_k$.

Finalmente, sean $0 \neq r \in \mathbb{Z}$ y $\pi(m/p^k)$ un elemento arbitrario de $\mathbb{Z}_{p^\infty}$. Escribamos $r = ap^\ell$ con $a, p$ coprimos. Luego, existen $s, t \in \mathbb{Z}$ tales que $1 = sa + tp^{k+\ell}$ y por lo tanto

$$\frac{m}{p^k} = \frac{msa + mtp^{k+\ell}}{p^k} = \frac{msap^\ell}{p^{k+\ell}} + mtp^\ell = r\frac{ms}{p^{k+\ell}} + mtp^\ell.$$

Así, $\pi(m/p^k) = r\pi(ms/p^{k+\ell})$ lo cual prueba que $\mathbb{Z}_{p^\infty}$ es divisible. □

**Teorema 12.14.** *Un grupo abeliano es divisible si y sólo si es una suma directa de copias de $\mathbb{Q}$ y $\mathbb{Z}_{p^\infty}$ (los primos $p$ pueden variar).*

*Demostración.* Por el Lema 12.15, una suma de copias de $\mathbb{Q}$ y $\mathbb{Z}_{p^\infty}$ es divisible. Recíprocamente, sea $A$ un grupo abeliano divisible. Sea $T = T(A)$ el subgrupo de torsión de $A$, es decir,

$$T = \{x \in A : nx = 0 \text{ para algún } n \neq 0\}.$$

Se tiene que $T$ es divisible, pues para cada $t \in T$ y para cada $n \neq 0$ existe $x \in A$ tal que $nx = t$ (pues $A$ es divisible). Si $m \neq 0$ es tal que $mt = 0$, entonces $(mn)x = 0$, lo cual dice que $x \in T$. Así, por la Proposición 12.9, $T$ es inyectivo. Luego, por la Proposición 12.2, $A = T \oplus D$ en donde $D \simeq A/T$ es sin torsión y además divisible por Lema 12.15. Observemos que en $D$, la ecuación $nx = b$ (con $n \neq 0$) tiene solución única. Esto dice que $D$ tiene una estructura de $\mathbb{Q}$-módulo, definiendo $(m/n)b$ como la única solución de la ecuación $nx = mb$. Luego, $D$ es un $\mathbb{Q}$-espacio vectorial, y por consiguiente es isomorfo a una suma directa de copias de $\mathbb{Q}$.

Por otro lado, ya vimos que $T$ es suma directa de sus componentes $p$-primarias. Es decir, $T = \bigoplus_{p \text{ primo}} T(p)$ (esta suma se toma sobre los primos positivos, por supuesto), en donde

$$T(p) = \{x \in T : p^k x = 0 \text{ para algún } k > 0\}.$$

Cada componente $p$-primaria $T(p)$ es divisible (de nuevo por el Lema 12.15, pues es un cociente del grupo divisible $T$). Para completar la demostración basta con observar que $T(p)$ es una suma directa de copias de $\mathbb{Z}_{p^\infty}$, lo cual sigue del Lema 12.16 más abajo. □

**Lema 12.15.** (i) *Una suma directa de grupos abelianos divisibles es divisible.*

(ii) *Un cociente de un grupo abeliano divisible es divisible.*

*Demostración.* Para probar la primera parte sea $(D_i)_{i\in I}$ una familia de grupos abelianos divisibles y sean $0 \neq r \in \mathbb{Z}$ y $m \in \bigoplus_{i\in I} D_i$. Observar que existe un conjunto finito $J \subset I$ tal que $m = \sum_{i\in J} m_i$ con $m_i \in D_i$. Como cada $D_i$ es divisible, tenemos que existen $x_i \in D_i$ tales que $rx_i = m_i$ para todo $i \in J$. Luego $x = \sum_{i\in J} x_i$ satisface $rx = m$.

Para la segunda parte sean $D$ un grupo abeliano divisible y $C$ un subgrupo de $D$. Sean $0 \neq r \in \mathbb{Z}$ y $m + C \in D/C$. Como $D$ es divisible, existe $x \in D$ tal que $rx = m$. Luego $r(x + C) = m + C$ y por consiguiente $D/C$ es divisible. □

**Lema 12.16.** *Sean $p$ un número primo positivo y $P$ un $p$-grupo abeliano divisible. Entonces $P$ es suma directa de copias de $\mathbb{Z}_{p^\infty}$.*

*Demostración.* Antes que nada observamos que cualquier elemento $0 \neq b \in P$ pertenece a un subgrupo $B \simeq \mathbb{Z}_{p^\infty}$. Sea $p^m$ el orden de $b$. Para $i = 1, \ldots, m$ definimos $b_i = p^{m-i}b$, en particular $b_m = b$. Como $P$ es divisible, podemos elegir $b_{m+1}, b_{m+2}, \ldots$ tales que $b_i = pb_{i+1}$ para todo $i \geq m$. Como $b_m$ tiene orden $p^m$, se concluye que $b_i$ tiene orden $p^i$ para todo $i$. Sea $B$ el subgrupo generado por $b_1, b_2, \ldots$. Notar que $pb_1 = 0$ y que $pb_i = b_{i-1}$ para todo $i \geq 2$. Usando el Ejercicio 12.12 se concluye que $B \simeq \mathbb{Z}_p^\infty$.

Para completar la prueba debemos usar el Lema de Zorn. Sea $\mathscr{S}$ el conjunto formado por todos los conjuntos $\mathscr{D}$ de subgrupos $B \simeq \mathbb{Z}_{p^\infty}$ tales que la suma $\sum_{B \in \mathscr{D}} B$ es directa. Es decir, para cada $B \in \mathscr{D}$ se tiene $B \cap \sum_{C \in \mathscr{D} - \{B\}} C = 0$. Notar que $\mathscr{S} \neq \varnothing$, está parcialmente ordenado por la inclusión y toda cadena no vacía en $\mathscr{S}$ admite una cota superior (completar los detalles como ejercicio). Entonces, por el Lema de Zorn, $\mathscr{S}$ admite un elemento maximal $\mathscr{M}$. Luego, $M = \sum_{B \in \mathscr{M}} B = \bigoplus_{B \in \mathscr{M}} B$ es divisible por Lema 12.15 y por ende inyectivo. Así, $P = M \oplus D$ para algún subgrupo $D$ de $P$. Notemos que $D \simeq P/M$ es un $p$-grupo divisible. Luego, por lo observado en el párrafo anterior, si $D \neq 0$, entonces $D$ contiene un subgrupo $C$ isomorfo a $\mathbb{Z}_{p^\infty}$. Si $\mathscr{M}' = M \cup \{C\}$, entonces la suma $\sum_{B \in \mathscr{M}'} B$ es directa, lo cual contradice que $\mathscr{M}$ es maximal. Por consiguiente $P = M = \bigoplus_{B \in \mathscr{M}} B$ es suma de copias de $\mathbb{Z}_{p^\infty}$. □

Una propiedad notable de los grupos abelianos divisibles es la siguiente.

**Proposición 12.17.** *Todo grupo abeliano puede ser embebido en grupo divisible.*

*Demostración.* Sea $A$ un grupo abeliano y tomemos un epimorfismo $\pi : F \to A$ de un grupo abeliano libre sobre $A$. Como $F$ es suma directa de copias de $\mathbb{Z}$, existe un monomorfismo $\iota : F \to D$, de $F$ en una suma directa $D$ de copias de $\mathbb{Q}$, la cual es divisible por el Lema 12.15. Consideremos el pushout

$$\begin{array}{ccc} D & \xrightarrow{\pi'} & P \\ {\scriptstyle\iota}\uparrow & & \uparrow{\scriptstyle\iota'} \\ F & \xrightarrow{\pi} & A \end{array}$$

de $\iota$ y $\pi$. Por el Ejercicio 12.3 tenemos que $\iota'$ es un monomorfismo $\pi'$ es un epimorfismo, por lo tanto $A$ puede ser embebido en $P \simeq D/\ker \pi'$, el cual es divisible por el Lema 12.15. □

Es importante destacar esta proposición puede generalizarse de la siguiente manera.

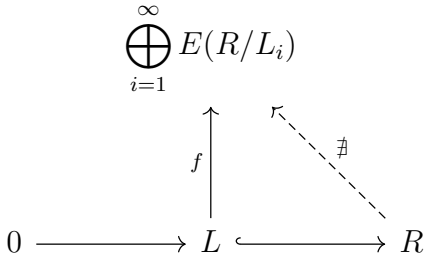
**Teorema 12.18.** *Todo módulo puede ser embebido en un módulo inyectivo.*

Este resultado tiene como consecuencia una importante caracterización de los anillos noetherianos. Recordemos que un anillo $R$ se dice *noetheriano a izquierda* si toda cadena de ideales a izquierda $L_1 \subset L_2 \subset \cdots$ de $R$ se estabiliza, es decir, existe un $i_0$ tal que $L_i = L_{i_0}$ para todo $i \geq i_0$.

**Teorema 12.19.** *Un anillo $R$ es noetheriano a izquierda si y sólo si toda suma directa de $R$-módulos (a izquierda) inyectivos es inyectiva.*

Aunque no cubriremos las pruebas de los Teoremas 12.18 y 12.19, podemos utilizarlos para encontrar importantes ejemplos.

**Ejemplo 12.20.** A continuación damos la idea de cómo se construye en ejemplo de una suma directa de módulos inyectivos que no es inyectiva. Sea $R$ un anillo no-noetheriano y sea $L_1 \subsetneqq L_2 \subsetneqq L_3 \subsetneqq \cdots$ una cadena de ideales que no se estabiliza. Por el Teorema 12.18, cada cociente $R/L_i$ (pensado como módulo cociente de ${}_RR$) puede ser embebido en un módulo inyectivo. Más aún, puede probarse (no lo hacemos) cualquier $R$-módulo admite una extensión inyectiva "minimal" llamada la *cápsula inyectiva*. Denotemos por $E(R/L_i)$ la cápsula inyectiva de $R/L_i$. Entonces $\bigoplus_{i=1}^{\infty} E(R/L_i)$ no es inyectivo. La idea para probar que esta suma no es inyectiva es la siguiente. Sea $L = \bigcup_{i=1}^{\infty} L_i$, el cual es un ideal de $R$. Para cada $i$ tenemos definido un morfismo $f_i : L \to E(R/L_i)$ dado por la composición de los morfismos $L \hookrightarrow R \to R/L_i \hookrightarrow E(R/L_i)$. Por la propiedad universal del producto, la familia $(f_i)_{i=1}^{\infty}$ induce un morfismo $f : L \to \prod_{i=1}^{\infty} E(R/L_i)$, pero en realidad se ve fácilmente que la imagen de $f$ está contenida en $\bigoplus_{i=1}^{\infty} E(R/L_i)$. No es difícil probar que $f : L \to \bigoplus_{i=1}^{\infty} E(R/L_i)$ no se puede extender a todo $R$




lo cual dice que $\bigoplus_{i=1}^{\infty} E(R/L_i)$ no es un $R$-módulo inyectivo.

**Ejemplo 12.21.** Para tener ejemplos concretos de lo anterior, mencionamos algunos anillos no-noetherianos.

(i) Sea $R$ un anillo conmutativo con identidad. El anillo de polinomios $R[x_1, x_2, \ldots]$ en una cantidad numerable de variables $x_1, x_2, \ldots$ no es noetheriano. En efecto, si $L_i$ es el ideal generado por las variables $x_1, x_2, \ldots, x_i$, entonces la cadena de ideales $L_1 \subset L_2 \subset \cdots$ no se estabiliza.

(ii) El anillo $\mathbb{A} \subset \mathbb{C}$ de enteros algebraicos no es noetheriano. Por definición, $z \in \mathbb{C}$ es un entero algebraico si es raíz de un polinomio mónico con coeficientes enteros. Por ejemplo, la cadena de ideales principales

$$2\mathbb{A} \subset 2^{1/2}\mathbb{A} \subset 2^{1/4}\mathbb{A} \subset 2^{1/8}\mathbb{A} \subset \cdot$$

no se estabiliza.

(iii) El anillo $\mathscr{C}[0,1]$ de todas funciones continuas del intervalo $[0,1]$ en $\mathbb{R}$ no es noetheriano. Por ejemplo, si $L_i = \{f \in \mathscr{C}[0,1] : f(x) = 0 \text{ para todo } x \in [0, 1 - \frac{1}{i}]\}$, entonces $L_1 \subset L_2 \subset \cdots$ es una cadena de ideales que no se estabiliza.

# 13. Producto tensorial

## 13.1. Motivación

**Producto tensorial de espacios vectoriales.** Sean $V, W$ dos espacios vectoriales sobre un cuerpo $\mathbb{K}$. Supongamos por simplicidad que $V$ y $W$ son de dimensión finita. El

producto tensorial de $V$ con $W$ es un nuevo espacio vectorial que nos ayuda a entender como son las aplicaciones bilineales de $V \times W$ en cualquier espacio vectorial $U$. Más precisamente, si $e_1, \ldots, e_n$ es una base de $V$ y $f_1, \ldots, f_m$ es una base de $W$, entonces el producto tensorial $V \otimes W$ tiene por base a

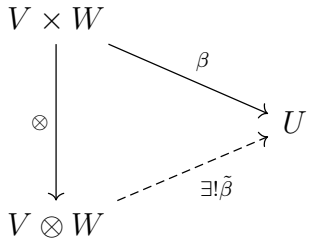
$$\{e_i \otimes f_j : i = 1, \ldots, n,\ j = 1, \ldots, m\},$$

la cual induce una aplicación bilineal $\otimes : V \times W \to V \otimes W$ definida, para $v = \sum v_i e_i$ y $w = \sum w_j f_j$ por

$$v \otimes w = \sum_{i,j} v_i w_j\, e_i \otimes f_j$$

*Observación* 13.1. (i) La construcción anterior no depende de las bases que elijamos para $V$ y $W$ (ejercicio).

(ii) Existe una propiedad universal: para toda aplicación bilineal $\beta : V \times W \to U$ existe una única aplicación lineal $\tilde{\beta} : V \times W \to U$ tal que conmuta el diagrama




En efecto, $\tilde{B}$ es la única aplicación lineal tal que $\tilde{\beta}(e_i \otimes f_j) = \beta(e_i, f_j)$

**Ejemplo 13.2.** El producto tensorial es una herramienta que nos permite pensar las aplicaciones bilineales como transformaciones lineales (que salen de $V \otimes W$)

(i) La multiplicación en $\mathbb{K}$ puede pensarse como una aplicación lineal $m : \mathbb{K} \otimes \mathbb{K} \to \mathbb{K}$ tal que $m(x \otimes y) = xy$.

(ii) Si $\mathbb{K} = \mathbb{R}$, un producto interno $g$ en $V$ puede pensarse como una aplicación lineal $g : V \otimes V \to \mathbb{R}$ tal que $g(v \otimes w) = g(w \otimes v)$ (simetría) y $g(v \otimes v) > 0$ para todo $v \neq 0$ (no degenerado). Verificar esto como ejercicio.

**Producto tensorial de módulos sobre un anillo conmutativo.** Si $R$ es un anillo conmutativo también podemos definir el producto tensorial de dos $R$-módulos $A$ y $B$ (no necesariamente libres). La construcción $A \otimes B$ la daremos un poco más adelante, pero lo que queremos enfatizar ahora es que nuevamente el producto tensorial es una herramienta que nos permite interpretar las aplicaciones *bilineales* $\beta : A \times B \to C$ como morfismos de $R$-módulos $\tilde{\beta} : A \otimes B \to C$ que satisfacen $\tilde{\beta}(a \otimes b) = \beta(a, b)$.

Recordemos que $\beta : A \times B \to C$ es bilineal si satisface, para todos $a, a' \in A$, $b, b' \in B$, $r \in R$, las siguientes identidades

$$\begin{aligned} \beta(a + a', b) &= \beta(a, b) + \beta(a', b) \\ \beta(a, b + b') &= \beta(a, b) + \beta(a, b') \\ \beta(ra, b) &= r\beta(a, b) = \beta(a, rb) \end{aligned}$$

Por ejemplo, la multiplicación $R \times R \to R$ es una aplicación bilineal (porque $R$ es conmutativo) y por lo tanto induce un morfismo de $R$-módulos $m : R \otimes R \to R$ tal que $m(r \otimes r') = rr'$.

Las aplicaciones bilineales en $A \times B$ pueden caracterizarse de la siguiente manera.

**Proposición 13.3.** *Sean $R$ un anillo conmutativo, $A, B, C$ tres $R$-módulos y $\beta : A \times B \to C$ una función. Son equivalentes.*

(i) *$\beta$ es bilineal;*

(ii) *$a \mapsto \beta(a, -)$ es un morfismo de $R$-módulos de $A$ en $\mathrm{Hom}_R(B, C)$;*

(iii) *$b \mapsto \beta(-, b)$ es un morfismo de $R$-módulos de $B$ en $\mathrm{Hom}_R(A, C)$.*

En palabras: $\beta$ es bilineal si y sólo si fijando una variable tenemos un morfismo de $R$-módulos en la otra.

*Demostración.* Ejercicio. Para que el enunciado de la proposición tenga sentido, hará falta entender cuál es la estructura de $R$-módulo en $\mathrm{Hom}_R(A, C)$ y $\mathrm{Hom}_R(B, C)$, ver apartado 13.4 más adelante. □

**¿Qué pasa con anillos no-conmutativos?** Las aplicaciones bilineales entre $R$-módulos son un objeto engañoso cuando $R$ no es conmutativo. De hecho, la multiplicación en $R$ ni siquiera es bilineal. En efecto, si $\beta : R \times R \to R$ denota el producto $\beta(x, y) = xy$ en $R$, entonces ya no podemos asegurar que $\beta(rx, y) = rxy = r\beta(x, y)$ sea igual a $\beta(x, ry)$. También tendremos dificultades con la linealidad de $\beta(x, y)$ en una variable una vez fijada la otra. Sin embargo, una propiedad que si satisface $\beta$ es que para todos $x, y, r$ se tiene

$$\beta(xr, y) = (xr)y = x(ry) = \beta(x, ry)$$

Es decir, si pensamos al producto $R \times R$ con el primer factor como el $R$-módulo a derecha $R_R$ y al segundo como el $R$-módulo a izquierda ${}_RR$, entonces la acción (como módulos) de $R$ en cada uno factor pasa de una variable a la otra en $\beta(x, y)$, aunque no sale afuera.

Estas sutilezas son las que se tienen en cuenta en la definición formal del producto tensorial, la que para trabajar con los objetos más generales posibles ($R$-módulos) tenemos que debilitar un poco las definiciones (ya no sirve trabajar con aplicaciones bilineales).

## 13.2. Definición del producto tensorial

**5 jun**

**Definición 13.4.** Sean $R$ un anillo (no necesariamente conmutativo), $A$ un $R$-módulo a derecha, $B$ un $R$-modulo a izquierda y $C$ un grupo abeliano. Una función $\beta : A \times B \to C$ se dice un *bihomomorfismo* si

$$\begin{aligned} \beta(a + a', b) &= \beta(a, b) + \beta(a', b) \\ \beta(a, b + b') &= \beta(a, b) + \beta(a, b') \\ \beta(ar, b) &= \beta(a, rb) \end{aligned}$$

para todos $a, a' \in A$, $b, b' \in B$, $r \in R$.

**Lema 13.5.** *Si $A$ es un $R$-módulo a derecha, $B$ un $R$-modulo a izquierda y $C$ un grupo abeliano, entonces*

(i) $\mathrm{Hom}_{\mathbb{Z}}(A, C)$ *es un $R$-módulo a izquierda definiendo para $f \in \mathrm{Hom}_{\mathbb{Z}}(A, C)$ y $r \in R$,*

$$(rf)(x) = f(xr), \qquad x \in A;$$

(ii) $\mathrm{Hom}_{\mathbb{Z}}(B, C)$ *es un $R$-módulo a derecha definiendo para $g \in \mathrm{Hom}_{\mathbb{Z}}(B, C)$ y $r \in R$,*

$$(gr)(x) = g(rx), \qquad x \in B$$

*Demostración.* Veamos (i) y dejamos (ii) como ejercicio. Sean $f, f' \in \mathrm{Hom}(A, C)$, $r, r' \in R$ y $x \in A$. Es fácil ver que $rf$ es un morfismo de grupos abelianos. Por otro lado, claramente $\mathrm{Hom}_{\mathbb{Z}}(A, C)$ es un grupo abeliano y además

$$\begin{aligned}(r(f + f'))(x) &= (f + f')(xr) = f(xr) + f'(xr)\\ &= (rf)(x) + (rf')(x) = (rf + rf')(x),\end{aligned}$$

con lo cual $r(f + f') = rf + rf'$,

$$\begin{aligned}((r + r')f)(x) &= f(x(r + r')) = f(xr + xr')\\ &= f(xr) + f(xr') = (rf)(x) + (r'f)(x)\\ &= (rf + r'f)(x),\end{aligned}$$

de donde sigue que $(r + r')f = rf + r'f$, y finalmente

$$(r(r'f))(x) = (r'f)(xr) = f((xr)r') = f(x(rr')) = ((rr')f)(x)$$

lo que nos dice que $r(r'f) = (rr')f$ como queríamos probar □

El resultado del Lema 13.5 será generalizado un poco más adelante cuando estudiemos bimódulos[4], pero por lo pronto esto nos permite dar una caracterización categórica de los bihomomorfismos similar a la que vimos en la Proposición 13.3.

**Proposición 13.6.** *Sean $R$ un anillo conmutativo, $A$ un $R$-módulo a derecha, $B$ un $R$-módulo a izquierda, $C$ un grupo abeliano $\beta : A \times B \to C$ una función. Son equivalentes.*

(i) *$\beta$ es un bihomomorfismo;*

(ii) *$a \mapsto \beta(a, -)$ es un morfismo de $R$-módulos a derecha de $A$ en $\mathrm{Hom}_{\mathbb{Z}}(B, C)$;*

(iii) *$b \mapsto \beta(-, b)$ es un morfismo de $R$-módulos a izquierda de $B$ en $\mathrm{Hom}_{\mathbb{Z}}(A, C)$.*

[4]Un *$R$-$S$-bimódulo* es un grupo abeliano que tiene a la vez una estructura de $R$-módulo a izquierda y una de $S$-módulo a derecha compatibles entre si: es decir se satisface la igualdad $(rx)s = r(xs)$. Notar que en Lema 13.5 $A$ es un $\mathbb{Z}$-$R$-bimódulo, $B$ es un $R$-$\mathbb{Z}$-bimódulo y $C$ es un $\mathbb{Z}$-$\mathbb{Z}$-bimódulo.

*Demostración.* Veamos (i) $\iff$ (ii), (i) $\iff$ (iii) es similar y queda como ejercicio. Supongamos primero que $\beta$ es un bihomomorfismo, entonces claramente se tiene que $\beta(a,-) \in \mathrm{Hom}(B,C)$ y $\beta(a+a',-) = \beta(a,-) + \beta(a',-)$, además $\beta(ar,-) = \beta(a,-)r$. En efecto, para todo $b$ tenemos que

$$\beta(ar,-)(b) = \beta(ar,b) = \beta(a,rb) = \beta(a,-)(rb) = (\beta(a,-)r)(b).$$

Recíprocamente, si suponemos (ii), entonces para todos $a, a' \in A$, $b, b' \in B$ y $r \in R$, tenemos

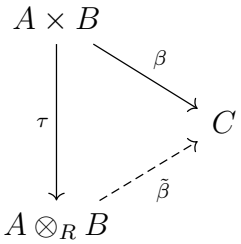
$$\begin{aligned}\beta(a+a',b) &= \beta(a+a',-)(b) = (\beta(a,-) + \beta(a',-))(b)\\ &= \beta(a,-)(b) + \beta(a',-)(b) = \beta(a,b) + \beta(a',b),\end{aligned}$$

$$\begin{aligned}\beta(a,b+b') &= \beta(a,-)(b+b') = \beta(a,-)(b) + \beta(a,-)(b')\\ &= \beta(a,b) + \beta(a,b')\end{aligned}$$

y finalmente

$$\beta(ar,b) = \beta(ar,-)(b) = (\beta(a,-)r)(b) = \beta(a,-)(rb) = \beta(a,rb). \qquad \square$$

**Definición 13.7.** Sean $A$ un $R$-módulo a derecha y $B$ un $R$-módulo a izquierda. Un *producto tensorial* entre $A$ y $B$ es un grupo abeliano $A \otimes_R B$ junto con un bihomomorfismo $\tau : A \times B \to A \otimes_R B$, $\tau(a,b) = a \otimes b$ tal que para cualquier grupo abeliano $C$ y cualquier bihomomorfismo $\beta : A \times B \to C$ existe un único morfismo de grupos abelianos $\tilde{\beta} : A \otimes_R B \to C$ tal que $\beta = \tilde{\beta} \circ \tau$, es decir, el siguiente diagrama conmuta.



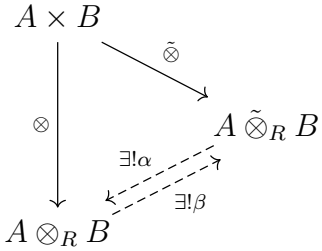

Es común denotar el bihomomorfismo $\tau$ con el mismo símbolo $\otimes$.

**Teorema 13.8.** *El producto tensorial $A \otimes_R B$ entre un $R$-módulo a derecha $A$ y un $R$-módulo a izquierda $B$ existe y es único salvo isomorfismo.*

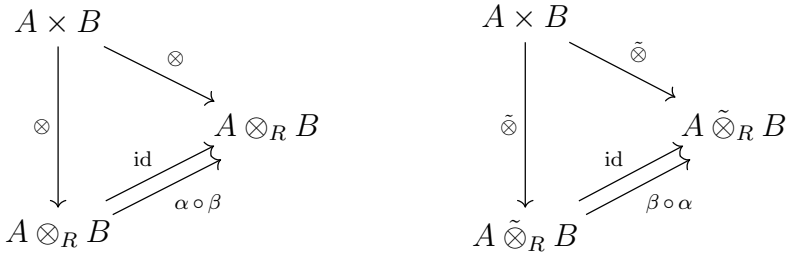
*Demostración.* Veamos primero la unicidad. Supongamos que tenemos dos productos tensoriales $A \otimes_R B$ y $A \tilde{\otimes}_R B$. Por las propiedades universales que tiene cada producto tensorial podemos construir dos morfismos de grupos abelianos

$$\beta : A \otimes_R B \to A \tilde{\otimes}_R B \qquad\qquad \alpha : A \tilde{\otimes}_R B \to A \otimes_R B$$

tales que $\beta(a \otimes b) = a \tilde{\otimes} b$ y $\alpha(a \tilde{\otimes} b) = a \otimes b$.



Para chequear que $\beta$ y $\alpha$ son inversas una de la otra, usamos la unicidad de factorización aplicada a los siguientes diagramas conmutativos.




De donde sigue que $\alpha \circ \beta = \mathrm{id}_{A \otimes_R B}$ y $\beta \circ \alpha = \mathrm{id}_{A \tilde{\otimes}_R B}$.

Para probar la existencia consideramos el grupo abeliano libre $F$ en $A \times B$. Sea $K$ el subgrupo de $F$ generado por los elementos de la forma

$$\begin{aligned} &(a + a', b) - (a, b) - (a', b), \\ &(a, b + b') - (a, b) - (a', b), \\ &(ar, b) - (a, rb), \end{aligned} \tag{13.1}$$

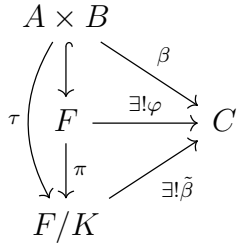
en donde $a, a' \in A$, $b, b' \in B$, $r \in R$, y sea

$$\tau : A \times B \hookrightarrow F \longrightarrow F/K$$

la inclusión compuesta con la proyección al cociente. Por definición tenemos que $\tau$ es un bihomomorfismo. Sea $C$ un grupo abeliano y $\beta : A \times B \to C$ un bihomomorfismo. Notemos que $\beta$ se extiende a un morfismo de grupos abelianos $\varphi : F \to C$. Además $K \subset \ker \varphi$. En efecto, chequeando en los generadores de $K$ tenemos

$$\begin{aligned} \varphi((a + a', b) - (a, b) - (a, b')) &= \varphi((a + a', b)) - \varphi((a, b)) - \varphi((a', b)) \\ &= \beta(a + a', b) - \beta(a, b) - \beta(a', b) \\ &= 0 \end{aligned}$$

(análogamente con los otros generados). Luego existe un único morfismo de grupos abelianos $\tilde{\beta} : F/K \to C$ tal que $\beta = \tilde{\beta} \circ \tau$. Luego $F/K$ es un producto tensorial entre $A$ y $B$.




□

**Corolario 13.9.** (i) *Todo elemento en $A \otimes_R B$ es una suma finita $\sum_i a_i \otimes b_i$ con $a_i \in A$, $b_i \in B$.*

(ii) *Si $\sum_i a_i \otimes b_i = 0$ en $A \otimes_R B$ entonces $\sum_i a_i \otimes b_i = 0$ en $A' \otimes_R B'$ para ciertos submódulos finitamente generados $A' \subset A$, $B' \subset B$.*

*Demostración.* (i) Sea $A \otimes_R B = F/K$ como en la demostración del Teorema 13.8. Por definición, todo elemento en $F$ es una combinación lineal finita $\sum_i n_i(a_i, b_i)$ con $n_i \in \mathbb{Z}$, $a_i \in A$ y $b_i \in B$. Luego, todo elemento en $F/K$ es una combinación lineal finita de la forma $\sum_i n_i(a_i \otimes b_i) = \sum_i (n_i a_i) \otimes b_i$, en donde $n_i a_i \in A$ y $b_i \in B$.

(ii) Si $\sum_i a_i \otimes b_i = 0$, en $A \otimes_R B$, entonces $\sum_i (a_i, b_i) \in K$, y por consiguiente usando (13.1) podemos escribir

$$\begin{aligned}\sum_i (a_i, b_i) = &\sum_j m_j[(a'_j + a''_j, b'_j) - (a'_j, b'_j) - (a''_j, b'_j)] \\ &+ \sum_k n_k[(a'''_k, b''_k + b'''_k) - (a'''_k, b''_k) - (a'''_k, b'''_k)] \\ &+ \sum_\ell q_\ell[(a''''_\ell r_\ell, b''''_\ell) - (a''''_\ell, r_\ell b''''_\ell)]\end{aligned}$$

en donde las todas las sumas son finitas, $m_j, n_k, q_\ell \in \mathbb{Z}$, $a'_j, a''_j, a'''_k, a''''_\ell \in A$, $b'_j, b''_k, b'''_k, b''''_\ell \in B$ y $r_\ell \in R$. Sean $A'$ el submódulo de $A$ generado por $a_i, a'_j, a''_j, a'''_k, a''''_\ell$ y $B'$ el submódulo de $B$ generado por $b_i, b'_j, b''_k, b'''_k, b''''_\ell$. Construimos el producto tensorial $A' \otimes_R B' = F'/K'$, de donde sigue que $\sum_i (a_i, b_i) \in K'$ y por ende $\sum_i a_i \otimes b_i = 0$ en $A' \otimes_R B'$. □

**Ejercicio 13.10.** Mostrar con un ejemplo que en $A \otimes_R B$ no todo elemento es de la forma $a \otimes b$ para ciertos $a \in A$, $b \in B$.

## 13.3. Morfismos

**Proposición 13.11.** *Sean $\varphi : A \to A'$ un morfismo de $R$-módulos a derecha y $\psi : B \to B'$ un morfismo de $R$-módulos a izquierda, entonces existe un único morfismo de grupos abelianos $\varphi \otimes \psi : A \otimes_R B \to A' \otimes_R B'$ tal que $\varphi \otimes \psi(a \otimes b) = \varphi(a) \otimes \psi(b)$ para todos $a \in A$, $b \in B$. Es decir, el siguiente diagrama conmuta*

$$\begin{array}{ccc} A \times B & \xrightarrow{\varphi \times \psi} & A' \times B' \\ {\scriptstyle \tau}\downarrow & & \downarrow{\scriptstyle \tau'} \\ A \otimes_R B & \xrightarrow{\varphi \otimes \psi} & A' \otimes_R B' \end{array}$$

*Más aún*

- $\mathrm{id}_A \otimes_R \mathrm{id}_B = \mathrm{id}_{A \otimes_R B}$,
- $(\varphi \circ \varphi') \otimes (\psi \circ \psi') = (\varphi \otimes \psi) \circ (\varphi' \otimes \psi')$,
- $(\varphi + \varphi') \otimes \psi = \varphi \otimes \psi + \varphi' \otimes \psi$,
- $\varphi \otimes (\psi + \psi') = \varphi \otimes \psi + \varphi \otimes \psi'$.

*Es decir, fijando un $R$-módulo a derecha $A$, tenemos un funtor aditivo*[5]

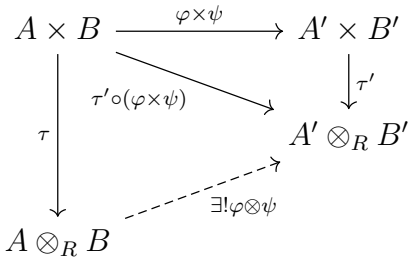
$$A \otimes_R - : R\text{-}\mathbf{Mod} \to \mathbf{Ab}$$

[5]Un funtor $F : \mathscr{C} \to \mathscr{D}$ entre dos categorías abelianas se dice *aditivo* si para cada par de objetos $A, B$ en $\mathscr{C}$, la asignación $F : \mathrm{Hom}(A, B) \to \mathrm{Hom}(F(A), F(B))$ es un morfismo de grupos abelianos.

*y fijando un $R$-módulo a izquierda $B$, tenemos un funtor aditivo*

$$- \otimes_R B : \mathbf{Mod}\text{-}R \to \mathbf{Ab}\,.$$

*Demostración.* El siguiente diagrama muestra cómo construir $\varphi \otimes \psi$




Observar que la existencia del morfismo de grupos abelianos $\varphi \otimes \psi$ está garantizada porque $\tau' \circ (\varphi \times \psi)$ es un bihomomorfismo (ejercicio).

Las propiedades listadas salen por unicidad usando la propiedad universal. Probarlas como ejercicio (por el Corolario 13.9 basta evaluar en tensores simples). Para la definir los funtores indicados en la última parte ponemos

$$(A \otimes_R -)(\psi) = A \otimes_R \psi := \mathrm{id}_A \otimes \psi,$$
$$(- \otimes_R B)(\varphi) = \varphi \otimes_R B := \varphi \otimes \mathrm{id}_B\,.$$

Completar los detalles como ejercicio. □

*Observación* 13.12. Observemos que, con la notación de la proposición anterior, tenemos que

$$(\varphi \otimes \mathrm{id}'_B) \circ (\mathrm{id}_A \otimes \psi) = \varphi \otimes \psi = (\mathrm{id}'_A \otimes \psi) \circ (\varphi \otimes \mathrm{id}_B),$$

es decir, conmuta el diagrama

$$\begin{array}{ccc} A \otimes_R B & \xrightarrow{A \otimes_R \psi} & A \otimes_R B' \\ {\scriptstyle \varphi \otimes_R B}\downarrow & & \downarrow{\scriptstyle \varphi \otimes_R B'} \\ A' \otimes_R B & \xrightarrow{A' \otimes_R \psi} & A' \otimes_R B' \end{array}$$

Esto significa que el morfismo $A \otimes_R \psi$ es natural en $A$ y el morfismo $\varphi \otimes_R B$ es natural en $B$.

## 13.4. Bimódulos

**6 jun**

**Definición 13.13.** Un *$R$-$S$-bimódulo* es un grupo abeliano $M$ que tiene una estructura de $R$-módulo a izquierda y una estructura de $S$-módulo a derecha tales que $r(xs) = (rx)s$ para todos $x \in M$, $r \in R$ y $s \in S$. Si $M, N$ son dos $R$-$S$-bimódulos, un *morfismo de $R$-$S$-bimódulos* $f : M \to N$ es una función que es a la vez un morfismo de $R$-módulos a izquierda y un morfismo de $S$-módulos a derecha. Esto permite formar la categoría $R$-**Mod**-$S$ de todos los $R$-$S$-bimódulos.

A veces utilizaremos la notación ${}_RM_S$ para indicar que $M$ es un $R$-$S$-bimódulo.

**Ejemplo 13.14.** (i) $R$ es un $R$-$R$-bimódulo.

(ii) Todo $R$-módulo a izquierda es un $R$-$\mathbb{Z}$-bimódulo. Todo $R$-módulo a derecha es un $\mathbb{Z}$-$R$-bimódulo.

(iii) Todo $R$-módulo a izquierda es un $R$-$\mathrm{End}_R^{\mathrm{op}}(M)$-bimódulo. ¿Por qué?

(iv) Una estructura de $R$-módulo libre a derecha en un $R$-módulo libre a izquierda (la cual depende de la elección de una base, ver Corolario 7.6) induce una estructura de $R$-$R$-bimódulo.

(v) Si $R$ es conmutativo, todo $R$-módulo es un $R$-$R$-bimódulo.

Cuando uno trabaja con bimódulos es posible dar estructura adicional al grupo de morfismos.

**Proposición 13.15.** *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 las operaciones definidas por*

$$(sf)(x) = f(xs) \qquad\qquad (ft)(x) = f(x)t, \tag{13.2}$$

*en donde $f \in \mathrm{Hom}_R(M,N)$, $x \in M$, $s \in S$ y $t \in T$.*

*Demostración.* En primer lugar observemos que $sf$ y $ft$ definidas como (13.2) resultan morfismo de $R$-módulos. En efecto, ambos son morfismos de grupos abelianos. Además, si $r \in R$, entonces

$$(sf)(rx) = f(rxs) = rf(xs) = r(sf)(x).$$

Análogamente $(ft)(rx) = r(ft)(x)$. Notemos también que $s(f+g) = sf + sg$ para todos $f, g \in \mathrm{Hom}_R(M,N)$ y que

$$(s(s'f))(x) = (s'f)(xs) = f((xs)s') = f(x(ss')) = ((ss')f)(x),$$

con lo cual $\mathrm{Hom}_R(M,N)$ es un $S$-módulo a izquierda. Similarmente $\mathrm{Hom}_R(M,N)$ es un $T$-módulo a derecha. Por último, observemos que

$$(s(ft))(x) = (ft)(xs) = f(t(xs)) = f((tx)s) = (sf)(tx) = ((sf)t)(x),$$

o sea $s(ft) = (sf)t$, de donde sigue que $\mathrm{Hom}_R(M,N)$ es un $S$-$T$-bimódulo. □

**Ejercicio 13.16.** Sigue de la Proposición 13.15 que si $A$ es un $R$-módulo a izquierda, entonces $\mathrm{Hom}_R({}_RR, A)$ es un $R$-módulo. En efecto, como ${}_RR$ es un $R$-$R$-bimódulo y $A$ es un $R$-$\mathbb{Z}$-bimódulo, tenemos que $\mathrm{Hom}({}_RR, A)$ es un $R$-$\mathbb{Z}$-bimódulo. Probar que $\mathrm{Hom}_R({}_RR, A) \simeq A$.

**Corolario 13.17.** *Si $R$ es conmutativo, entonces $\mathrm{Hom}_R(M,N)$ es un $R$-módulo para todo par de $R$-módulos $M, N$.*

**Proposición 13.18.** *Sean $M$ un $R$-$S$-bimódulo y $N$ un $R$-$T$-bimódulo. Entonces*

(i) $\mathrm{Hom}_R(M,-) : R\text{-}\mathbf{Mod}\text{-}T \to S\text{-}\mathbf{Mod}\text{-}T$ *es un funtor covariante;*

(ii) $\mathrm{Hom}_R(-,N) : R\text{-}\mathbf{Mod}\text{-}S \to S\text{-}\mathbf{Mod}\text{-}T$ *es un funtor contravariante.*

*Demostración.* Ejercicio. □

### 13.4.1. Producto tensorial de bimódulos

Es posible extender la definición de producto tensorial para trabajar con bimódulos. Para ello, primero que nada tenemos que extender la definición de bihomomorfismo.

**Definición 13.19.** Consideremos tres bimódulos ${}_SA_R$, ${}_RB_T$ y ${}_SC_T$. Una función $\beta : A \times B \to C$ se dice un *bihomomorfismo de bimódulos* si

$$\begin{aligned}\beta(a+a',b) &= \beta(a,b)+\beta(a',b),\\ \beta(a,b+b') &= \beta(a,b)+\beta(a,b'),\\ \beta(sa,b) &= s\beta(a,b),\\ \beta(a,bt) &= \beta(a,b)t,\\ \beta(ar,b) &= \beta(a,rb)\end{aligned}$$

para todos $a, a' \in A$, $b, b' \in B$, $s \in S$, $t \in T$, $r \in R$.

Los bihomomorfismos de bimódulos tienen una caracterización análoga a la de los bihomomorfismos a secas.

**Proposición 13.20.** *Sean ${}_SA_R$, ${}_RB_T$ y ${}_SC_T$ tres bimódulos y $\beta : A\times B \to C$ una función. Las siguientes afirmaciones son equivalentes.*

(i) *$\beta$ es un bihomomorfismo de bimódulos.*

(ii) *$a \mapsto \beta(a,-)$ es un morfismo de $S$-$R$-bimódulos de $A$ en $\mathrm{Hom}_T(B,C)$.*

(iii) *$b \mapsto \beta(-,b)$ es un morfismo de $R$-$T$-bimódulos de $B$ en $\mathrm{Hom}_S(A,C)$.*

*Demostración.* Ejercicio. Tener la siguiente precaución: claramente por la Proposición 13.15 tenemos que $\mathrm{Hom}_S(A,C)$ es un $R$-$T$-bimódulo, para pensar a $\mathrm{Hom}_T(B,C)$ como un $S$-$R$-bimódulo razonamos como sigue. Tener una estructura de $R$-$T$-bimódulo en $B$ es equivalente a tener una estructura de $T^{\mathrm{op}}$-$R^{\mathrm{op}}$-bimódulo en $B$. Similarmente $C$ puede pensarse como un $T^{\mathrm{op}}$-$S^{\mathrm{op}}$-bimódulo. Luego, nuevamente por la Proposición 13.15, tenemos que $\mathrm{Hom}_{T^{\mathrm{op}}}(B,C) = \mathrm{Hom}_T(B,C)$ es un $R^{\mathrm{op}}$-$S^{\mathrm{op}}$-bimódulo. Equivalentemente $\mathrm{Hom}_T(B,C)$ es un $S$-$R$-bimódulo. □

**Proposición 13.21.** *Sean $A$ un $R$-módulo a derecha y $B$ un $R$-módulo a izquierda.*

(i) *Si $A$ es un $S$-$R$-bimódulo, entonces $A \otimes_R B$ es un $S$-módulo a izquierda tal que $s(a\otimes b) = (sa)\otimes b$ para todos $a \in A$, $b \in B$, $s \in S$.*

(ii) *Si $B$ es un $R$-$T$-bimódulo, entonces $A \otimes_R B$ es un $T$-módulo a derecha tal que $(a\otimes b)t = a\otimes(bt)$ para todos $a \in A$, $b \in B$, $t \in T$.*

*Si $A$ es un $S$-$R$-bimódulo y $B$ es un $R$-$T$-bimódulo entonces:*

(iii) *$A \otimes_R B$ es un $S$-$T$-bimódulo.*

(iv) *$\otimes : A \times B \to A \otimes_R B$ es un bihomomorfismo de bimódulos.*

(v) *Para cada $S$-$T$-bimódulo $C$ y cada bihomomorfismo de bimódulos $\beta : A \times B \to C$ existe un único morfismo de bimódulos $\tilde{\beta} : A \otimes_R B \to C$ tal que $\tilde{\beta}(a \otimes b) = \beta(a, b)$ para todos $a \in A$, $b \in B$.*

(vi) *Si $\varphi : A \to A'$, $\psi : B \to B'$ son morfismos de bimódulos, entonces $\varphi \otimes \psi$ es un morfismo de bimódulos.*

(vii) *$A \otimes_R - : R$-**Mod**-$S \to S$-**Mod**-$T$ y $- \otimes_R B : S$-**Mod**-$R \to S$-**Mod**-$T$ son funtores aditivos.*

*Demostración.* (i). Tenemos que definir el producto a izquierda en $A \otimes_R B$ por elementos de $S$. Dado $s \in S$, sea $\alpha_s : A \to A$ definida por $\alpha_s(a) = sa$. Notemos que $\alpha_s$ es un morfismo de $R$-módulos a derecha, la cual induce un morfismo de grupos abelianos $\bar{\alpha}_s = \alpha_s \otimes \mathrm{id}_B : A \otimes_R B \to A \otimes_R B$ que satisface $\bar{\alpha}_s(a \otimes b) = (sa) \otimes b$.

$$\begin{array}{ccc} A \times B & \xrightarrow{\alpha_S \times \mathrm{id}_B} & A \times B \\ {\scriptstyle \otimes}\downarrow & & \downarrow{\scriptstyle \otimes} \\ A \otimes_R B & \xrightarrow{\alpha_s \otimes \mathrm{id}_B} & A \otimes_R B \end{array}$$

Notemos que $\alpha : S \to \mathrm{End}_R(A)$ definida por $\alpha(s) = \alpha_s$ es un morfismo de anillos (con identidad) y consecuentemente, por Proposición 13.11, $\bar{\alpha} : S \to \mathrm{End}_{\mathbb{Z}}(A \otimes_R B)$ es un morfismo de anillos. Esto último significa que $A \otimes_R B$ es un $S$-módulo a izquierda (ver Proposición 1.6)

(ii). Es similar (hacerla como ejercicio).

(iii). Ya tenemos que $A \otimes_R B$ es un $S$-módulo a izquierda y un $T$-módulo a derecha. Además, en tensores simples vale

$$s((a \otimes b)t) = s(a \otimes (bt)) = (sa) \otimes (bt) = ((sa) \otimes b)t = (s(a \otimes b))t.$$

Como cualquier elemento en $A \otimes_R B$ es un suma finita de tensores simples, tenemos que $s(xt) = (sx)t$ para todo $x \in A \otimes_R B$. Por lo tanto $A \otimes_R B$ es un $S$-$T$-bimódulo.

Probar (iv), (v), (vi) y (vii) como ejercicio. □

## 13.5. Aplicaciones

**8 jun**

### 13.5.1. Producto tensorial de módulos libres

Recordemos que si $F$ es un $R$-módulo libre a derecha con base $(e_i)_{i \in I}$, entonces $F$ tiene estructura de $R$-módulo a izquierda definiendo $r(\sum_{i \in I} e_i x_i) = \sum_{i \in I} e_i (r x_i)$. Análogamente si $F$ es un $R$-módulo libre a izquierda con base $(e_i)_{i \in I}$, entonces $F$ tiene una estructura de $R$-módulo a derecha definiendo $(\sum_{i \in I} x_i e_i)r = \sum_{i \in I} (x_i r) e_i$. En cualquiera de los dos casos obtenemos un $R$-$R$-bimódulo.

**Proposición 13.22.** (i) *Si $F$ es un $R$-módulo libre a derecha con base $(e_i)_{i \in I}$ y $B$ es un $R$-módulo libre a izquierda, entonces*

$$F \otimes_R B \simeq_{R\text{-}\mathbf{Mod}} \bigoplus_{i \in I} B$$

*vía un isomorfismo de $R$-módulos a izquierda que manda $\sum_{i \in I} e_i \otimes b_i$ en $(b_i)_{i \in I}$. En particular $R_R \otimes_R B \simeq_{R\text{-}\mathbf{Mod}} B$.*

(ii) *Si $F$ es un $R$-módulo libre a izquierda con base $(e_i)_{i\in I}$ y $A$ es un $R$-módulo a derecha, entonces*

$$A \otimes_R F \simeq_{\mathbf{Mod}\text{-}R} \bigoplus_{i\in I} A$$

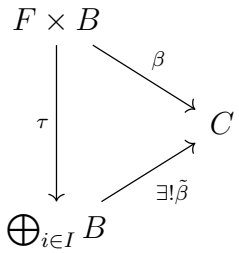
*vía un isomorfismo de $R$-módulos a derecha que manda $\sum_{i\in I} a_i \otimes e_i$ en $(a_i)_{i\in I}$. En particular, $A \otimes_R {}_R R \simeq_{\mathbf{Mod}\text{-}R} A$.*

Por si hace falta alguna aclaración, las notaciones $\simeq_{R\text{-}\mathbf{Mod}}$ y $\simeq_{\mathbf{Mod}\text{-}R}$ significan isomorfismo en la categoría $R$-**Mod** y **Mod**-$R$ respectivamente.

*Demostración.* Probaremos (i) dejando (ii) como ejercicio. Primero veamos que $F \otimes_R B \simeq \bigoplus_{i\in I} B$ como grupos abelianos. Sea $\tau : F \times B \to \bigoplus_{i\in I} B$ definida por $\tau(\sum_{i\in I} e_i x_i, b) = (x_i b_i)_{i\in I}$. Es sencillo verificar que $\tau$ es un bihomomorfismo. Además, cada bihomomorfismo $\beta : F \times B \to C$ se factoriza unívocamente a través de $\tau$. En efecto, $\beta$ induce un único morfismo de grupos abelianos $\tilde{\beta} : \bigoplus_{i\in I} B \to C$ tal que $\tilde{\beta}((b_i)_{i\in I}) = \sum_{i\in I} \beta(e_i, b_i)$ (verificar esto usando la propiedad universal de la suma directa), el cual satisface

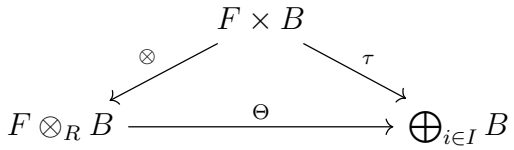
$$\begin{aligned}\beta\left(\sum_{i\in I} e_i x_i, b\right) &= \sum_{i\in I} \beta(e_i x_i, b) = \sum_{i\in I} \beta(e_i, x_i b) \\ &= \tilde{\beta}((x_i b)_{i\in I}) = \tilde{\beta}\left(\tau\left(\sum_{i\in I} e_i x_i, b\right)\right),\end{aligned}$$

de donde sigue que $\beta = \tilde{\beta} \circ \tau$.




Por la unicidad del producto tensorial existe un isomorfismo de grupos abelianos $\Theta : F \otimes_R B \to \bigoplus_{i\in I} B$ tal que

$$\Theta\left(\left(\sum_{i\in I} e_i x_i\right) \otimes b\right) = \tau\left(\sum_{i\in I} e_i x_i, b\right) = (x_i b)_{i\in I}.$$




Además como observamos al principio de este apartado, $F \otimes_R B$ es un $R$-módulo a

izquierda y vale

$$\begin{aligned}\Theta\left(r\left(\left(\sum_{i\in I} e_i x_i\right)\otimes b\right)\right) &= \Theta\left(\left(\sum_{i\in I} e_i(rx_i)\right)\otimes b\right)\\ &= ((rx_i)b)_{i\in I} = r(x_i b)_{i\in I}\\ &= r\Theta\left(\left(\sum_{i\in I} e_i x_i\right)\right).\end{aligned}$$

Esto muestra que $\Theta(r(f\otimes b)) = r\Theta(f\otimes b)$ para todo $f\in F$, $b\in B$ y consecuentemente, $\Theta$ es un morfismo de $R$-módulos a izquierda. □

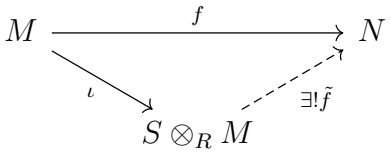
### 13.5.2. Extensión de escalares

Recordemos que si $\rho : R\to S$ es un morfismo de anillos, entonces todo $S$-módulo $M$ tiene asociada una estructura natural de $R$-módulo, definiendo $rx = \rho(r)x$ para todos $x\in M$, $r\in R$. Por ejemplo, todo $\mathbb{C}$-espacio vectorial es un $\mathbb{R}$-espacio vectorial de manera natural, y esta construcción se corresponde con la inclusión $\mathbb{R}\hookrightarrow\mathbb{C}$). Con la ayuda del producto tensorial, podemos dar una construcción recíproca que convierte cualquier $R$-módulo en un $S$-módulo.

**Proposición 13.23.** *Sean $M$ un $R$-módulo a izquierda y $\rho : R\to S$ un morfismo de anillos con identidad.*

(i) *$S\otimes_R M$ es un $S$-módulo a izquierda y la función $\iota : M\to S\otimes_R M$ definida por $\iota(x) = 1\otimes x$ es un morfismo de $R$-módulos (con respecto a la estructura de $R$-módulo en $S\otimes_R M$ inducida por $\rho$).*

(ii) *Si $N$ es un $S$-módulo y $f : M\to N$ es un morfismo de $R$-módulos, entonces existe un único morfismo de $S$-módulos $\tilde{f} : S\otimes_R M\to M$ tal que $f = \tilde{f}\circ\iota$. Es decir, el siguiente diagrama conmuta.*




(iii) *Si $M$ es un $R$-módulo libre y $(e_i)_{i\in I}$ es una base de $M$, entonces $S\otimes_R M$ es un $S$-módulo libre y $(\iota(e_i))_{i\in I}$ es una base de $S\otimes_R M$.*

*Demostración.* Claramente $S$ es un $S$-$R$-bimódulo con la multiplicación a derecha por elementos de $R$ definida como $s\cdot r = s\rho(r)$. Luego por la Proposición 13.21, $S\otimes_R M$ es un $S$-módulo a izquierda. Notar que la estructura de $R$-módulo a izquierda en $S\otimes_R M$ está dada determinada por $r\cdot(s\otimes x) = \rho(r)(s\otimes x)$. Luego, para todo $r\in R$, $x\in M$ tenemos

$$\begin{aligned}\iota(rx) &= 1\otimes(rx) = (1\cdot r)\otimes x\\ &= (1\rho(r))\otimes x = \rho(r)\otimes x\\ &= \rho(r)(1\otimes x) = r\cdot\iota(x)\end{aligned}$$

de donde sigue que $\iota$ es un morfismo de $R$-módulos, lo cual prueba (i).

Para probar la parte (ii), dado un morfismo de $R$-módulos $f : M \to N$ en el $S$-módulo $N$, construimos el bihomomorfismo de bimódulos $\beta : S \times M \to N$ definido por $\beta(s, x) = sf(x)$. Por la propiedad universal del producto tensorial, existe un único morfismo de $S$-módulos $\tilde{f} : S \otimes_R M \to N$ tal que $\tilde{f}(s \otimes x) = sf(x)$. En particular, tomando $s = 1$, obtenemos que $\tilde{f}(\iota(x)) = \tilde{f}(1 \otimes x) = f(x)$.

Finalmente, si $M$ tiene una base $(e_i)_{i\in I}$, entonces por la Proposición 13.22, existe un isomorfismo de $S$-módulos $\Theta : S \otimes_R M \to \bigoplus_{i\in I} S$ cuya inversa manda la base canónica de $\bigoplus_{i\in I} S$ en $(1 \otimes e_i)_{i\in I} = (\iota(e_1))_{i\in I}$. Esto prueba (iii). □

**Ejemplo 13.24.** Para el monomorfismo de anillos $\mathbb{R} \hookrightarrow \mathbb{C}$, la construcción de la proposición anterior es llamada *complexificación*. Por ejemplo

(i) $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n \simeq \mathbb{C}^n$,

(ii) $\mathbb{C} \otimes_{\mathbb{R}} M_n(\mathbb{R}) \simeq M_n(\mathbb{C})$. Probar como ejercicio que en este último caso el isomorfismo es también un isomorfismo de anillos (comparar con los ejercicios de la guía para entender bien cuál es la estructura de anillo en $\mathbb{C} \otimes_{\mathbb{R}} M_n(\mathbb{R})$).

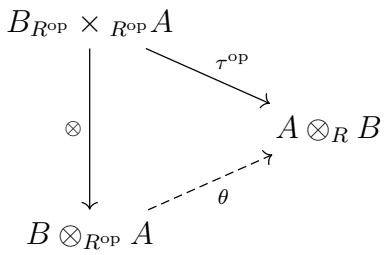
## 13.6. Conmutatividad del producto tensorial

**Proposición 13.25.** *Sean $A$ un $R$-módulo a derecha y $B$ un $R$-módulo a izquierda. Entonces existe un isomorfismo natural*

$$A \otimes_R B \simeq B \otimes_{R^{\mathrm{op}}} A$$

*que manda $a \otimes b$ en $b \otimes a$.*

*Demostración.* Antes que nada, observemos que como $A$ es un $R$-módulo a derecha y $B$ es un $R$-módulo a izquierda, podemos pensarlos naturalmente como $R^{\mathrm{op}}$-módulos izquierda y derecha respectivamente (ver Proposición 2.4). Luego, el isomorfismo que tenemos que probar tiene perfecto sentido. Sea $C$ un grupo abeliano. Observemos que una función $\beta : A_R \times {}_R B \to C$ un bihomomorfismo (con respecto a $R$) si y sólo si $\beta^{\mathrm{op}} : B_{R^{\mathrm{op}}} \times {}_{R^{\mathrm{op}}} A \to C$ definida como $\beta^{\mathrm{op}}(b, a) = \beta(a, b)$ es un bihomomorfismo (con respecto a $R^{\mathrm{op}}$). En particular, $\tau^{\mathrm{op}} : B_{R^{\mathrm{op}}} \times {}_{R^{\mathrm{op}}} A \to A \otimes_R B$ definida como $\tau^{\mathrm{op}}(b, a) = a \otimes b$ es un bihomomorfismo. Luego existe un único morfismo de grupos abelianos $\theta : B \otimes_{R^{\mathrm{op}}} A \to A \otimes_R B$ tal que $\theta(b \otimes a) = a \otimes b$ para todos $a \in A$, $b \in B$. Análogamente, existe un morfismo de grupos abelianos $\zeta : A \otimes_R B \to B \otimes_{R^{\mathrm{op}}} A$ tal que $\zeta(a \otimes b) = b \otimes a$ para todos $a \in A$, $b \in B$. Como $\theta \circ \zeta$ y $\zeta \circ \theta$ coinciden con la identidad en tensores simples, se tiene que $\theta = \zeta^{-1}$ es un isomorfismo de grupos abelianos.



Para chequear la naturalidad, sean $\varphi : A \to A'$ y $\psi : B \to B'$ dos morfismos de $R$-módulos a derecha e izquierda respectivamente. Debemos ver que el siguiente diagrama conmuta

$$\begin{array}{ccc} A \otimes_R B & \xrightarrow{\varphi \otimes \psi} & A' \otimes_R B' \\ \zeta \downarrow & & \downarrow \zeta' \\ B \otimes_{R^{\mathrm{op}}} A & \xrightarrow{\psi \otimes \varphi} & B' \otimes_{R^{\mathrm{op}}} A' \end{array}$$

en donde $\zeta$ y $\zeta'$ son los isomorfismos que construimos en el párrafo anterior. (Notar también que el morfismo $\psi \otimes \varphi$ tiene sentido porque $\psi$ y $\varphi$ son morfismos de $R^{\mathrm{op}}$-módulos a derecha e izquierda respectivamente.)

Es suficiente con chequear la conmutatividad en tensores simples. En efecto, para todos $a \in A$, $b \in B$ se tiene

$$\begin{aligned} (\psi \otimes \varphi)(\zeta(a \otimes b)) &= (\psi \otimes \varphi)(b \otimes a) \\ &= \psi(b) \otimes \varphi(a) = \zeta'(\varphi(a) \otimes \psi(b)) \\ &= \zeta'((\varphi \otimes \psi)(a \otimes b)) \end{aligned}$$

como queríamos probar. □

**Proposición 13.26.** *Sean ${}_SA_R$, ${}_RB_T$ dos bimódulos. Entonces existe un isomorfismo de bimódulos*

$$A \otimes_R B \simeq B \otimes_{R^{\mathrm{op}}} A$$

*que es natural en $A$ y $B$.*

*Demostración.* Ejercicio. Observemos que por un lado $A \otimes_R B$ es un $S$-$T$-bimódulo y $B \otimes_{R^{\mathrm{o}}} A$ es un $T^{\mathrm{op}}$-$S^{\mathrm{op}}$-bimódulo. Luego $B \otimes_{R^{\mathrm{op}}} A$ tiene una estructura natural de $S$-$T$-bimódulo y el isomorfismo de bimódulos del enunciado tiene perfecto sentido. □

**Corolario 13.27.** *Si $R$ es conmutativo entonces $A \otimes_R B \simeq B \otimes_R A$ (isomorfismo de $R$-módulos).*

*Demostración.* Ejercicio. □

## 13.7. Asociatividad del producto tensorial

**13 jun**

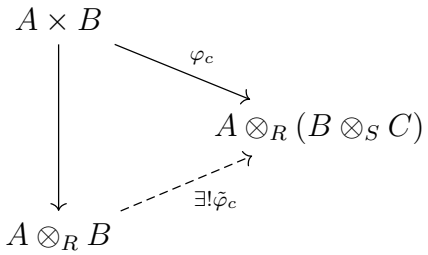
**Proposición 13.28.** *Sean ${}_RA$, ${}_RB_S$, ${}_SR$ (bi)módulos. Entonces existe un isomorfismo natural*

$$(A \otimes_R B) \otimes_S C \simeq A \otimes_R (B \otimes_S C)$$

*el cual manda $(a \otimes b) \otimes c$ en $a \otimes (b \otimes c)$. Si además $A$ y $C$ son bimódulos, entonces este isomorfismo es un isomorfismo de bimódulos.*

*Demostración.* Antes que nada observemos que $A \otimes_R B$ es un $S$-módulo a derecha y $A \otimes_R B$ es un $S$-módulo a izquierda, por lo cual tienen sentido ambos productos tensoriales triples. Para cada $c \in C$, definimos $\varphi_c : A \times B \to A \otimes_R (B \otimes_S C)$ por $\varphi_c(a, b) = a \otimes (b \otimes c)$. Como

$\varphi_c$ es un bihomomorfismo (ejercicio), se factoriza unívocamente a través de un morfismo de grupos abelianos $\tilde{\varphi}_c : A \otimes_R B \to A \otimes_R (B \otimes_S C)$.




Luego, podemos definir $\varphi : (A \otimes_R B) \times C \to A \otimes_R (B \otimes_S C)$ por $\varphi(t, c) = \tilde{\varphi}_c(t)$. Notemos que $\varphi$ es un bihomomorfismo. En efecto,

$$\begin{aligned} \varphi(t + t', c) &= \tilde{\varphi}_c(t + t') = \tilde{\varphi}_c(t) + \tilde{\varphi}_c(t') \\ &= \varphi(t, c) + \varphi(t', c), \end{aligned}$$

y haciendo las cuentas en tensores simples tenemos que

$$\begin{aligned} \varphi(a \otimes b, c + c') &= \tilde{\varphi}_c(a \otimes b) = \varphi_{c+c'}(a, b) \\ &= a \otimes (b \otimes (c + c')) \\ &= a \otimes (b \otimes c + b \otimes c') \\ &= a \otimes (b \otimes c) + a \otimes (b \otimes c') \\ &= \varphi_c(a, b) + \varphi_{c'}(a, b) \\ &= \tilde{\varphi}_c(a \otimes b) + \tilde{\varphi}_{c'}(a \otimes b) \\ &= \varphi(a \otimes b, c) + \varphi(a \otimes b, c'), \end{aligned}$$

y por lo tanto vale $\varphi(t, c + c') = \varphi(t, c) + \varphi(t, c')$ para todo $t \in A \otimes_R B$. Similarmente tenemos, para todo $s \in S$,

$$\begin{aligned} \varphi((a \otimes b)s, c) &= \varphi(a \otimes (bs), c) = \tilde{\varphi}_c(a \otimes (bs)) \\ &= a \otimes ((bs) \otimes c) = a \otimes (b \otimes (sc)) \\ &= \tilde{\varphi}_{sc}(a \otimes b) = \varphi(a \otimes b, sc), \end{aligned}$$

de donde sigue que $\varphi(ts, c) = \varphi(t, sc)$ para todo $t \in A \otimes_R B$. Luego existe un único morfismo de grupos abelianos $\tilde{\varphi} : (A \otimes_R B) \otimes_S C \to A \otimes_R (B \otimes_S C)$ tal que $\tilde{\varphi}((a \otimes b) \otimes c) = a \otimes (b \otimes c)$. Análogamente, existe $\tilde{\psi} : A \otimes_R (B \otimes_S C) \to (A \otimes_R B) \otimes_S C$ tal que $\tilde{\psi}(a \otimes (b \otimes c)) = (a \otimes b) \otimes c$. Luego $\tilde{\varphi} = \tilde{\psi}^{-1}$ (¿por qué?).

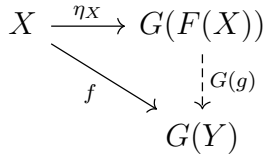
Queda como ejercicio la naturalidad y el caso de bimódulos. □

## 13.8. Adjunción ⊗-Hom

### 13.8.1. Funtores adjuntos

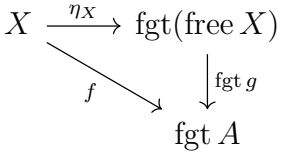
Un concepto muy importante en teoría de categorías es el de adjunción. Dados dos funtores $F : \mathscr{C} \to \mathscr{D}$ y $G : \mathscr{D} \to \mathscr{C}$ una *adjunción* entre $F$ y $G$ es una transformación

natural $\eta : \mathrm{id}_{\mathscr{C}} \Longrightarrow G \circ F$ tal que para cada morfismo $f : X \to G(Y)$ existe un único morfismo $g : F(X) \to Y$ tal que el siguiente diagrama conmuta



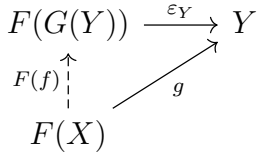

También se dice que $F$ y $G$ son *funtores adjuntos* y que $F$ es *adjunto a izquierda* y $G$ es *adjunto a derecha*.

**Ejemplo 13.29.** La definición anterior puede parecer un poco abstracta al principio, pero hay numerosos ejemplos de funtores adjuntos y tienen importantes propiedades. Un ejemplo sencillo pero importante es el de la adjunción entre el funtor libre free : **Set** $\to$ **Ab** y el funtor olvido fgt : **Ab** $\to$ **Set**. Observar que por definición dado un conjunto $X$ y grupo abeliano $A$, para cada función $f : X \to A$, o mejor dicho $f : X \to \mathrm{fgt}\, A$ existe un único morfismo de grupos $g : \mathrm{free}\, X \to A$ del grupo abeliano libre en $X$ en $A$ que extiende a $f$. Más precisamente, si $\eta_X : X \to \mathrm{fgt}(\mathrm{free}\, X)$ es la inclusión, entonces conmuta el diagrama




**Definición alternativa de adjunción.** Por definición, una $\eta$ es una adjunción entre $F$ y $G$ determina una biyección entre $\mathrm{Hom}(F(X), Y)$ y $\mathrm{Hom}(X, G(Y))$ que es natural en $X$ e $Y$. De aquí viene la terminología "adjunto a izquierda" para $F$ y "adjunto a derecha" para $G$. Recíprocamente, una biyección natural entre $\mathrm{Hom}(X, G(Y))$ y $\mathrm{Hom}(F(X), Y)$ determina una adjunción entre $F$ y $G$. En efecto, $\eta_X : X \to G(F(X))$ es elemento en $\mathrm{Hom}(X, G(F(X)))$ que se corresponde con el morfismo identidad en $\mathrm{Hom}(F(X), F(X))$ vía la biyección dada. Chequear como ejercicio que $\eta$ es una transformación natural.

**Counidad de adjunción.** En una adjunción $\eta$ entre $F$ y $G$, la transformación natural $\eta : \mathrm{id}_{\mathscr{C}} \Longrightarrow G \circ F$ es a veces llamada (por motivos que explicaremos en breve) la *unidad de adjunción*. Asociada a una adjunción también tenemos una *counidad de adjunción* que es una transformación natural $\varepsilon : F \circ G \to \mathrm{id}_{\mathscr{D}}$ que tiene la siguiente propiedad: para cada morfismo $g : F(X) \to Y$ existe un único morfismo $f : X \to G(Y)$ tal que el siguiente diagrama conmuta.

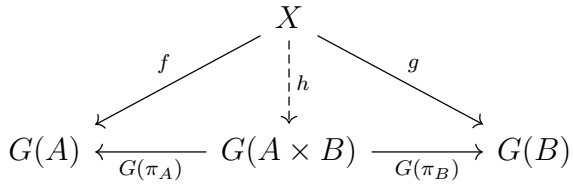



En otras palabras, $\varepsilon$ induce la inversa del isomorfismo $\mathrm{Hom}(X, G(Y)) \to \mathrm{Hom}(F(X), Y)$.

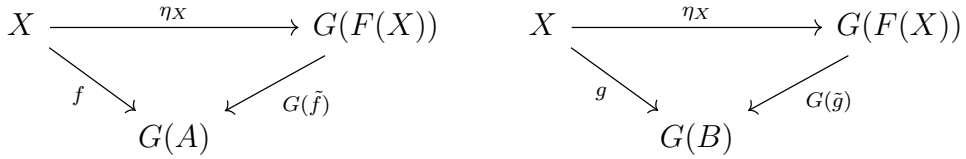
Una propiedad muy importante de las adjunciones y que usaremos más adelante:

**Proposición 13.30.** *Todo funtor adjunto a izquierda manda coproductos en coproductos. Todo funtor adjunto a derecha manda productos en productos.*

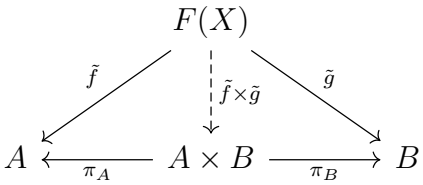
*Demostración.* Dejamos la prueba como ejercicio, pero precisamos un poco más el enunciado. Consideremos por simplicidad el caso de productos binarios, pero la misma prueba debería valer para productos arbitrarios. Sea $\mathscr{C} \underset{G}{\overset{F}{\rightleftarrows}} \mathscr{D}$ una adjunción. Habría que probar que si $(A \times B, \pi_A : A \times B \to A, \pi_B : A \times B \to B)$ es un producto en $\mathscr{D}$, entonces $(G(A \times B), G(\pi_A), G(\pi_B))$ es un producto en $\mathscr{D}$. O sea, para cada $X \in \operatorname{obj} \mathscr{C}$ y cada par de morfismos $f : X \to A$, $g : X \to B$, existe un único morfismo $h : X \to F(A \times B)$ tal que el siguiente diagrama conmuta.



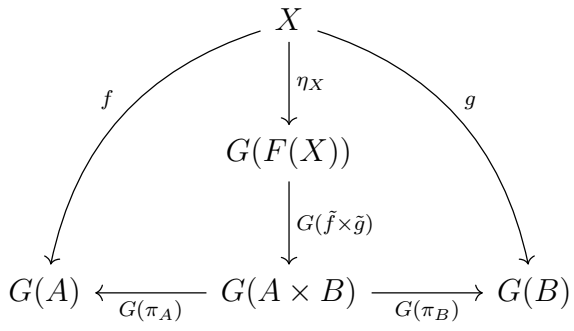

Usando la unidad de adjunción $\eta_X : X \to G(F(X))$ podemos construir dos morfismos $\tilde{f} : F(X) \to A$ y $\tilde{g} : F(X) \to B$ como sigue:




Usando que $A \times B$ es un producto en $\mathscr{D}$ construimos el (único) morfismo $\tilde{f} \times \tilde{g} : F(X) \to A \times B$ tal que conmuta el diagrama




Verificar que $h = G(\tilde{f} \times \tilde{g}) \circ \eta_X$ es el morfismo deseado




Para probar la afirmación acerca de los coproductos se puede utilizar un argumento similar (usando la counidad de adjunción) o razonar por dualidad. □

Finalmente dejamos como ejercicio el siguiente resultado.

**Proposición 13.31.** *Dos funtores adjuntos a izquierda (resp. derecha) de un mismo funtor son naturalmente isomorfos.*

## 13.9. El teorema de adjunción $\otimes$-Hom

Volvamos nuevamente a la categoría de $R$-módulos. Recordemos que si $A$ es un $R$-módulo a derecha y $B$ es un $R$-módulo a derecha, entonces tenemos asociados los siguientes funtores covariantes (ver Proposición 13.11 y Proposición 13.15):

$$R\text{-}\mathbf{Mod} \xrightarrow{A\otimes_R -} \mathbf{Ab} \xrightarrow{\mathrm{Hom}_{\mathbb{Z}}(A,-)} R\text{-}\mathbf{Mod}$$

y

$$\mathbf{Mod}\text{-}R \xrightarrow{-\otimes_R B} \mathbf{Ab} \xrightarrow{\mathrm{Hom}_{\mathbb{Z}}(B,-)} \mathbf{Mod}\text{-}R$$

El siguiente resultado demuestra que efectivamente el funtor $A \otimes -$ es un adjunto a izquierda para $\mathrm{Hom}_{\mathbb{Z}}(B,-)$ y $-\otimes B$ es un adjunto a izquierda para $\mathrm{Hom}_{\mathbb{Z}}(A,-)$.

**Teorema 13.32.** *Sean $A$ un $R$-módulo a derecha, $B$ un $R$-módulo a izquierda y $C$ un grupo abeliano. Existen isomorfismos*

$$\Theta : \mathrm{Hom}_{\mathbb{Z}}(A \otimes_R B, C) \longrightarrow \mathrm{Hom}_R(A, \mathrm{Hom}_{\mathbb{Z}}(B,C))$$

*y*

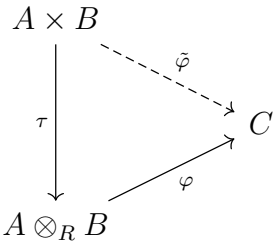
$$\Xi : \mathrm{Hom}_Z(A \otimes_R B, C) \longrightarrow \mathrm{Hom}_R(B, \mathrm{Hom}_{\mathbb{Z}}(A,C))$$

*los cuales son naturales en $A, B, C$. Más aún, para cada $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(A \otimes_R B, C)$, vale*

$$(\Theta(\varphi)(a))(b) = \varphi(a \otimes b) = (\Xi(\varphi)(b))(a)$$

*para todos $a \in A$, $b \in B$.*

*Demostración.* Denotemos por $\mathrm{Bihom}(A \times B, C)$ el conjunto de todos los bihomomorfismos de $A \times B$ en $C$. Observar que $\mathrm{Bihom}(A \times B, C)$ es un grupo abeliano (con la suma punto a punto). La función que asigna a cada $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(A \otimes_R B, C)$ el bihomomorfismo $\tilde{\varphi} = \varphi \circ \tau$ es un isomorfismo de grupos de $\mathrm{Hom}_{\mathbb{Z}}(A \otimes_R)$ en $\mathrm{Bihom}(A \times B, C)$, por propiedad universal del producto tensorial, en donde $\tau : A \times B \to A \otimes_R B$ está dado por $\tau(a,b) = a \otimes b$.




Por otro lado, usando la Proposición 13.4 la función que asigna a cada $\beta \in \mathrm{Bihom}(A \times B, C)$ el morfismo de $R$-módulos a derecha $\hat{\beta} \in \mathrm{Hom}_R(A, \mathrm{Hom}_{\mathbb{Z}}(B,C))$ definido por $\hat{\beta}(a) = \beta(a,-)$ es también un isomorfismo de grupos. Luego, definiendo

$$\Theta(\varphi) = \hat{\tilde{\varphi}}$$

tenemos un isomorfismo de grupos de $\mathrm{Hom}_{\mathbb{Z}}(A \otimes_R B, C)$ en $\mathrm{Hom}_R(A, \mathrm{Hom}_{\mathbb{Z}}(B,C))$ el cual satisface

$$\begin{aligned}(\Theta(\varphi)(a))(b) &= (\tilde{\varphi}(a,-))(b)\\ &= \tilde{\varphi}(a,b)\\ &= \varphi(a \otimes b)\end{aligned}$$

La definición de $\Xi$ y la naturalidad quedan como ejercicio. $\square$

**Corolario 13.33.** *Si $R$ es conmutativo y $A$ es un $R$-módulo, entonces $A \otimes -$ es naturalmente isomorfo a $- \otimes A$.*

*Demostración.* Sigue de la Proposición 13.31. □

**Corolario 13.34.** *Existen isomorfismos*

$$M \otimes_R \left( \bigoplus_{i \in I} B_i \right) \simeq \bigoplus_{i \in I} (M \otimes_R B_i) \tag{13.3}$$

*y*

$$\left( \bigoplus_{i \in I} A_i \right) \otimes_R N \simeq \bigoplus_{i \in I} (A_i \otimes_R N) \tag{13.4}$$

*en donde $M, A_i$ son $R$-módulos a derecha y $N, B_i$ son $R$-módulos a izquierda. Los isomorfismos anteriores son naturales en $M, A_i$ y $N, B_i$.*

*Demostración.* Sigue del Teorema 13.32 y de la Proposición 13.30 que los funtores $M \otimes_R -$ y $- \otimes_R N$ mandan coproductos en coproductos. Para la naturalidad, observar dichos isomorfismos mandan $m \otimes (b_i)_{i \in I}$ en $(m \otimes b_i)_{i \in I}$ en el caso (13.3) y $(a_i)_{i \in I} \otimes n$ en $(a_i \otimes n)_{i \in I}$ en el caso (13.4). Completar los detalles como ejercicio. □

**Corolario 13.35.** *Dados $R$-módulos a izquierda (o derecha) $M$, $N_i$ $(i \in I)$ existe un isomorfismo de grupos abelianos*

$$\mathrm{Hom}_R \left( M, \prod_{i \in I} A_i \right) \simeq \prod_{i \in I} \mathrm{Hom}_R(M, A_i)$$

*el cual es natural en $M$ y $N_i$.*

*Demostración.* Por el Teorema 13.32 sabemos que

$$\mathrm{Hom}_{\mathbb{Z}} \left( M, \prod_{i \in I} A_i \right) \simeq \prod_{i \in I} \mathrm{Hom}_{\mathbb{Z}}(M, A_i).$$

Notar que $\mathrm{Hom}_R(M, \prod_{i \in I} A_i)$ es un submódulo de $\mathrm{Hom}_{\mathbb{Z}}(M, \prod_{i \in I} A_i)$ cuya imagen vía la proyección al factor $\mathrm{Hom}_{\mathbb{Z}}(M, A_i)$ es exactamente $\mathrm{Hom}_R(M, A_i)$. Completar los detalles como ejercicio. □

**Proposición 13.36.** *Dados $R$-módulos a izquierda (o derecha) $M_i$ $(i \in I)$, $N$, existe un isomorfismo de grupos abelianos*

$$\mathrm{Hom}_R \left( \bigoplus_{i \in I} M_i, N \right) \simeq \prod_{i \in I} \mathrm{Hom}_R(M_i, N). \tag{13.5}$$

*Demostración.* Ejercicio. Ayuda: verificar que el lado izquierdo en (13.5) tiene la propiedad universal del producto directo de los $\mathrm{Hom}_R(M_i, N)$. □

**Ejemplo 13.37.** La Proposición 13.36 no es cierta si cambiamos $\prod$ por $\bigoplus$ en el lado derecho de (13.5). Por ejemplo, probar que $\mathrm{Hom}_{\mathbb{Z}} \left( \bigoplus_{i=1}^{\infty} \mathbb{Z}, \mathbb{Z} \right) \simeq \prod_{i=1}^{\infty} \mathbb{Z}$ no es libre, en tanto que $\bigoplus_{i=1}^{\infty} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \simeq \bigoplus_{i=1}^{\infty} \mathbb{Z}$ sí lo es.

# 14. Módulo dual

En este apartado estudiamos con un poco más de detalle los morfismos de módulos de un módulo dado en el anillo.

**Definición 14.1.** Sean $M$ un $R$-módulo a izquierda y $N$ un $R$-módulo a derecha. Definimos

(i) el módulo dual de $M$ como $M^* = \mathrm{Hom}_R(M, {}_RR)$ y

(ii) el módulo dual de $N$ como $N^* = \mathrm{Hom}_R(N, R_R)$

Observar que de la Proposición 13.15 sigue que $M^*$ es un $R$-módulo a derecha y $N^*$ es un $R$-módulo a izquierda con las multiplicaciones definidas para $\alpha \in M^*$, $r \in R$, $m \in M$,

$$(\alpha r)(m) = \alpha(rm)$$

y para $\beta \in N^*$, $r \in R$, $n \in N$,

$$(r\beta)(n) = \beta(nr)$$

Más aún, la Definición 14.1 determina dos funtores

$$(-)^* : R\text{-}\mathbf{Mod} \longrightarrow \mathbf{Mod}\text{-}R$$

y

$$(-)^* : \mathbf{Mod}\text{-}R \longrightarrow R\text{-}\mathbf{Mod}$$

los cuales abusando de la notación estamos denotando de la misma manera.

*Observación* 14.2. (i) Si $A \to B \to C \to 0$ es exacta entonces $0 \to C^* \to B^* \to A^*$. Esto sigue del hecho de que los funtores $\mathrm{Hom}_R(-, R_R)$ y $\mathrm{Hom}_R(-, {}_RR)$ son exactos a izquierda. Ver Ejercicio 14.3 más abajo.

(ii) Por la Proposición 13.36 tenemos que $\left(\bigoplus_{i\in I} A_i\right)^* \simeq \prod_{i\in I} A_i^*$. En particular,

$$(A_1 \oplus \cdots \oplus A_n)^* \simeq A_1^* \oplus \cdots \oplus A_n^*.$$

**Ejercicio 14.3.** Un funtor covariante entre categorías abelianas (o entre categorías donde tenga sentido hablar de sucesiones exactas) se dice *exacto a izquierda* si manda sucesiones exactas a izquierda en sucesiones exactas a izquierda. Recordar que una sucesión exacta a izquierda es una sucesión exacta de la forma $0 \to A \to B \to C$. Luego si $F$ es exacto a izquierda tendremos que $0 \to F(A) \to F(B) \to F(C)$ es exacta.

Un funtor contravariante se dice *exacto a izquierda* si manda sucesiones exactas a derecha en sucesiones exactas a izquierda. Esto tiene sentido porque un funtor contravariante puede interpretarse como un funtor covariante en la categoría opuesta, y las sucesiones exactas a derecha se convierten en sucesiones exactas a izquierda en la categoría opuesta. Es decir si $A \to B \to C \to 0$ es exacta y $F$ es un funtor contravariante, entonces $0 \to F(C) \to F(B) \to F(A)$ es exacta.

Sean $A$, $B$ dos $R$-módulos (a izquierda o derecha). Probar que los funtores $\mathrm{Hom}_R(A, -)$ y $\mathrm{Hom}_R(-, B)$ son exactos a izquierda.

El siguiente resultado sigue de la Observación 14.2.

**Proposición 14.4.** *Si $F$ es un $R$-módulo libre con una base finita $(e_i)_{i\in I}$ entonces $F^*$ es libre con base $(e_i^*)_{i\in I}$, en donde $e_i^*$ es el único elemento de $F^*$ tal que $e_i^*(e_j) = \delta_{ij}$.*

**Corolario 14.5.** *Si $M$ es un módulo proyectivo finitamente generado entonces, $M^*$ también lo es.*

*Demostración.* Ejercicio. □

Observemos que al ser el funtor dual un funtor contravariante, si lo "aplicamos dos veces" obtenemos un funtor covariante, llamado doble dual. Más precisamente, tenemos dos endofuntores

$$(-)^{**} : R\text{-}\mathbf{Mod} \longrightarrow R\text{-}\mathbf{Mod}$$

y

$$(-)^{**} : \mathbf{Mod}\text{-}R \longrightarrow \mathbf{Mod}\text{-}R.$$

**Proposición 14.6.** *Para cada $R$-módulo $M$ existe un morfismo canónico $\varepsilon_M : M \to M^{**}$ el cual es natural en $M$ y está dado por*

$$(\varepsilon_M(m))(\alpha) = \alpha(m)$$

*para todos $m \in M$, $\alpha \in M^*$*

El morfismo $\varepsilon_M$ suele llamarse morfismo evaluación.

*Demostración.* Verificar como ejercicio que $\varepsilon_M$ es un morfismo de $R$-módulos. La naturalidad significa que para cada morfismo de $R$-módulos $\varphi : M \to M'$ el siguiente diagrama conmuta.

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & M' \\ {\scriptstyle \varepsilon_M}\downarrow & & \downarrow{\scriptstyle \varepsilon_{M'}} \\ M^{**} & \xrightarrow{\varphi^{**}} & (M')^{**} \end{array}$$

En efecto, para cada $m \in M$ y cada $\beta \in (M')^{**}$ tenemos

$$(\varepsilon_{M'}(\varphi(m))) = \beta(\varphi(m)).$$

Por otro lado, por definición tenemos que $\varphi^{**}(\varepsilon_M(m)) = \varepsilon_M(m) \circ \varphi^*$, con lo cual

$$\begin{aligned} (\varphi^{**}(\varepsilon_M(m)))(\beta) &= (\varepsilon_M(m))(\varphi^*(\beta)) \\ &= (\varepsilon_M(m))(\beta \circ \varphi) \\ &= \beta(\varphi(m)), \end{aligned}$$

como queríamos probar. □

Sabemos que si $V$ es un espacio vectorial de dimensión finita, entonces $\varepsilon_V$ es un isomorfismo, pero esto no vale en general. Más aún, por la Proposición 14.4 sabemos que la evaluación es un isomorfismo para cualquier módulo libre con una base finita. La siguiente proposición extiende este resultado a módulos proyectivos.

**Proposición 14.7.** *Si $P$ es un módulo proyectivo finitamente generado entonces $\varepsilon_P : P \to P^{**}$ es un isomorfismo.*

*Demostración.* Si $F$ es libre (finitamente generado), mencionamos más arriba que este resultado se puede probar usando bases duales, por la Proposición 14.4. En efecto, si $e_1, \dots e_n$ es una base de $P$ y $e_1^{**}, \dots, e_n^{**}$ es la base dual de $e_1^*, \dots, e_n^*$, es fácil ver que $\varepsilon_P(e_i) = e_i^{**}$, de donde sigue que $\varepsilon_P$ es un isomorfismo.

Si $P$ es proyectivo finitamente generado, entonces $P$ es un sumando directo de un módulo libre finitamente generado $F$. Es decir, existen un epimorfismo $\pi : F \to P$ y un monomorfismo $\iota : P \to F$ tales que $\pi \circ \iota = \mathrm{id}_P$. Por funtorialidad sigue que $\pi^{**} \circ \iota^{**} = \mathrm{id}_{P^{**}}$. Esto implica que $\pi^{**}$ es un epimorfismo e $\iota^{**}$ es un monomorfismo. Por naturalidad, sabemos que el siguiente diagrama conmuta.

$$\begin{array}{ccc} F & \xrightarrow{\varphi} & F^{**} \\ {\scriptstyle\iota}\uparrow \downarrow{\scriptstyle\pi} & & {\scriptstyle\iota^{**}}\uparrow \downarrow{\scriptstyle\pi^{**}} \\ P & \xrightarrow[\varphi^{**}]{} & P^{**} \end{array}$$

Como $\varepsilon_P \circ \pi = \pi^{**} \circ \varepsilon_F$ y sabemos que $\pi^{**}$ es epimorfismo y $\varepsilon_F$ es isomorfismo concluimos que $\varepsilon_P$ es epimorfismo. Análogamente, $\iota^{**} \circ \varepsilon_P = \varepsilon_F \circ \iota$, y como $\iota^{**}$ es monomorfismo concluimos que $\varepsilon_P$ también es un monomorfismo. Luego $\varepsilon_P$ es un isomorfismo. □

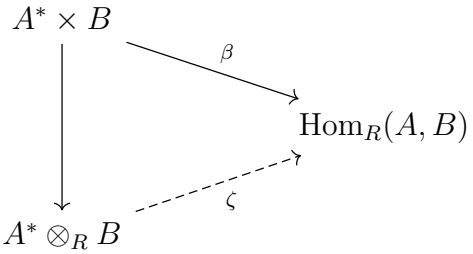
El siguiente resultado es muy útil y nos da una interpretación muy elegante del grupo de morfismos de dos módulos usando producto tensorial y módulo dual.

**Proposición 14.8.** *Sean $A, B$ dos $R$-módulos a izquierda. Entonces existe un morfismo de grupos abelianos*

$$\zeta : A^* \otimes_R B \longrightarrow \mathrm{Hom}_R(A, B)$$

*el cual es natural en $A, B$ y satisface $\zeta(\alpha \otimes b)(a) = \alpha(a)b$. Si además $A$ es proyectivo finitamente generado, entonces $\zeta$ es un isomorfismo.*

*Demostración.* Consideremos la aplicación $\beta : A^* \times B \to \mathrm{Hom}_R(AmB)$ definida por $\beta(a, b) = \alpha(a)b$. Verificar como ejercicio que $\beta$ es un bihomomorfismo. En particular, notar que hay que chequear que $\beta(a, b) \in \mathrm{Hom}_R(A, B)$. Luego por propiedad universal del producto tensorial, existe un único morfismo de grupos $\zeta : A^* \otimes_R B \to \mathrm{Hom}_R(A, B)$ tal que $\zeta(a \otimes b) = \alpha(a)b$.




Verificar la naturalidad como ejercicio.

Para la segunda parte supongamos primero que $A$ es libre con una base finita $(e_i)_{i \in I}$. Entonces $A^*$ es libre con base $(e_i^*)_{i \in I}$, por Proposición 14.4. Y por ende, usando la Proposición 13.22, cada elemento en $A^* \otimes_R B$ se escribe de manera única como

$$\sum_{i \in I} e_i^* \otimes b_i.$$

Luego,

$$\zeta\left(\sum_{i\in I} e_i^*\otimes b_i\right)=\sum_{i\in I} e_i^*(e_j)b_i=b_j.$$

Sigue que $\zeta\left(\sum_{i\in I} e_i^*\otimes b_i\right) : A\to B$ es el único morfismo que manda $e_j$ en $b_j$. Por propiedad universal de los módulos libres, $\zeta$ es biyectiva.

Supongamos ahora que $A$ es proyectivo finitamente generado. Razonando como en la prueba de la Proposición 14.8, sean $F$ un módulo libre finitamente generado, $\pi : F\to A$ un epimorfismo y $\iota : A\to F$ un monomorfismo tales que $\pi\circ\iota=\mathrm{id}_A$. Para simplificar la notación denotamos $\iota'=i^*\otimes \mathrm{id}_B$, $\iota''=\mathrm{Hom}_R(\iota,B)$ y $\pi'=\pi^*\otimes\mathrm{id}_B, \pi''=\mathrm{Hom}_R(\pi,B)$. Observemos que por funtorialidad, la condición $\pi\circ\iota=\mathrm{id}_P$ implica $\iota^*\circ\pi^*=\mathrm{id}_{P^*}$ y por ende $\iota'\circ\pi'=\mathrm{id}_{F^*\otimes_R B}$ y $\iota''\circ\pi''=\mathrm{id}_{\mathrm{Hom}_R(F,B)}$. En particular, $\iota',\iota'$ son monomorfismos y $\pi',\pi''$ son epimorfismos (notar que los funtores son contravariantes). Por naturalidad, el siguiente diagrama conmuta.

$$\begin{array}{ccc} A^*\otimes_R B & \xrightarrow{\zeta_A} & \mathrm{Hom}_R(A,B) \\ \uparrow{\scriptstyle \iota'} & & \uparrow{\scriptstyle \iota''} \\ F^*\otimes_R B & \xrightarrow{\zeta_F} & \mathrm{Hom}_R(F,B) \end{array}$$

En donde $\zeta_A,\zeta_F$ están definidas como en el enunciado de la proposición. De aquí sigue que $\iota''\circ\zeta=\zeta_A\circ\iota'$. Como $\eta_F$ es un isomorfismo, concluimos que $\zeta_A$ es un epimorfismo.

Similarmente, usando que el siguiente diagrama conmuta

$$\begin{array}{ccc} A^*\otimes_R B & \xrightarrow{\zeta_A} & \mathrm{Hom}_R(A,B) \\ \downarrow{\scriptstyle \pi'} & & \downarrow{\scriptstyle \pi''} \\ F^*\otimes_R B & \xrightarrow{\zeta_F} & \mathrm{Hom}_R(F,B) \end{array}$$

concluimos que $\pi''\circ\eta_A=\eta_F\circ\pi'$, de donde sigue que $\zeta_A$ es un monomorfismo. Esto prueba que $\zeta_A$ es un isomorfismo. □

**Corolario 14.9.** *Si $A$ es un $R$-módulo proyectivo finitamente generado y $B$ es un $R$-módulo a izquierda entonces existe un isomorfismo*

$$A\otimes_R B\simeq \mathrm{Hom}_R(A^*,B)$$

*el cual es natural en $A,B$*

*Demostración.* Ejercicio □

**Corolario 14.10.** *Si $R$ es conmutativo y $A,B$ son dos $R$-módulos proyectivos finitamente generados entonces existe un isomorfismo*

$$A^*\otimes_R B^*\simeq (A\otimes_R B)^*$$

*el cual es natural en $A,B$*