MA–860: TEORÍA DE MÓDULOS

Joseph C. Várilly

Escuela de Matemática, Universidad de Costa Rica

II Ciclo Lectivo del 2008

Introducción

Uno de los conceptos fundamentales del álgebra es un módulo sobre un anillo. Un módulo sobre un cuerpo $\mathbb{K}$ es un espacio vectorial; un módulo sobre el anillo $\mathbb{Z}$ de números enteros es un grupo abeliano. La teoría de módulos, entonces, incorpora ciertos rasgos del álgebra lineal y de la teoría de grupos abelianos. Sin embargo, el estudio de los módulos tiene un carácter propio que va más allá de las técnicas de esas teorías particulares.

Los módulos sobre un anillo conmutativo aportan información sobre la estructura del anillo subyacente. Se observa en muchas casos un comportamiento similar para la totalidad de módulos sobre ciertos anillos no conmutativos. Cuando las clases de módulos para dos anillos dados son equivalentes, en cierto sentido técnico pero bastante natural, se dice que los dos anillos subyacentes son equivalentes en el sentido de Morita. De este modo, en diversos contextos, la conmutatividad del anillo pasa a segundo plano.

Los módulos sobre un anillo dado A pueden considerarse, entonces, tanto individual como colectivamente. La clase de todos los A-módulos es un ejemplo de una *categoría*, y este ejemplo abre la puerta al estudio de las categorías en general. El tratamiento de las colecciones de A-módulos bajo este punto de vista "natural" se concretiza en diversos protocolos que forman la llamada *álgebra homológica*, que es una herramienta indispensable de las matemáticas modernas.

Uno de los aspectos más llamativos de la teoría de categorías es la *dualidad* obtenida por la "reversión de las flechas". De este modo, la acción de un álgebra (anillo con multiplicación escalar) sobre uno de sus módulos se transforma en la "coacción de una coálgebra sobre un comódulo". Estas estructuras duales resultan ser muy abundantes: hoy en día se emplean para algebraizar muchas ramas de la matemática anteriormente distintas, como el análisis y la geometría diferencial. La subdivisión escolar de las matemáticas en cajones de álgebra, análisis y geometría retrocede ante el panorama unificador de las matemáticas del siglo XXI.

En este curso, se estudiará la teoría de módulos desde diversas perspectivas, siguiendo más o menos el orden de su desarrollo histórico. En primer lugar, se buscará la estructura de un sólo módulo sobre un anillo principal y sus implicaciones para una transformación lineal de espacios vectoriales. Luego se introducen los conceptos fundamentales de categoría y de *funtor*, con énfasis en las llamadas categorías abelianas (que generalizan categorías de módulos sobre un anillo). Luego se consideran las clases principales de módulos: proyectivos, inyectivos y llanos, y sus funtores de homomorfismo y producto tensorial, lo cual con-

duce a las equivalencias de Morita. Al considerar complejos de módulos sobre un anillo fijo, se introducen las herramientas de homología y cohomología, con énfasis en sus propiedades funtoriales.

Indíce de materias

1 Módulos sobre un Anillo

1.1 Anillos enteros y principales

Antes de abordar la teoría de módulos sobre un anillo, conviene recordar ciertos propiedades básicas de anillos.

Definición 1.1. Un **anillo** es un conjunto A, dotado de dos leyes de composición (suma y producto) tales que:

1. $(A,+)$ es un grupo abeliano, con cero $0 \in A$;
2. el producto es asociativo y hay una identidad multiplicativa $1 \in A$;
3. hay distributividad: valen $a(b+c) = ab+ac$, $(a+b)c = ac+bc$ para todo $a,b,c \in A$.

Hay un anillo trivial con un solo elemento, en el cual vale $1 = 0$ (se escribe $A = 0$ en ese caso). En cualquier otro anillo, el cero aditivo 0 y la identidad multiplicativa 1 son distintos.[1]

Ejemplo 1.2. Los ejemplos más familiares de anillos son los siguientes.

- El conjunto $\mathbb{Z}$ de los **números enteros** es un ejemplo de un anillo *conmutativo*.
- Un anillo conmutativo $\mathbb{F}$ en donde cada elemento $a \neq 0$ posee un inverso multiplicativo a^{-1} se llama un **cuerpo**.[2] Los ejemplos más familiares son los números racionales $\mathbb{Q}$; los números reales $\mathbb{R}$; y los números complejos $\mathbb{C}$.
- El anillo finito $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$, cuyos elementos son los residuos de enteros bajo división por n, puede contener "divisores de cero": si $n = rs$ es una factorización no trivial de n en $\mathbb{N}$, entonces $\overline{r}\,\overline{s} = \overline{0}$ en $\mathbb{Z}/n\mathbb{Z}$. En cambio, si $p \in \mathbb{N}$ es un número natural *primo*, entonces $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ es un cuerpo finito.
- Si $\mathbb{F}$ es un cuerpo, los **polinomios** $p(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n$ con coeficientes $a_0, a_1, \ldots, a_n \in \mathbb{F}$ forman un anillo conmutativo $\mathbb{F}[t]$. Si $q(t) = b_0 + b_1 t + \cdots + b_m t^m$ es otro polinomio, entonces

  $$p(t)\,q(t) = a_0 b_0 + (a_0 b_1 + a_1 b_0)t + (a_0 b_2 + a_1 b_1 + a_2 b_0)t^2 + \cdots + a_n b_m t^{n+m},$$

  así que $p(t)q(t) = 0$ en $\mathbb{F}[t]$ si y sólo si $p(t) = 0$ o bien $q(t) = 0$ en $\mathbb{F}[t]$. En otras palabras, el anillo $\mathbb{F}[t]$ no contiene divisores de cero.

[1] Originalmente, la definición de anillo no contemplaba la necesidad de que A tuviera una identidad multiplicativa, y los "anillos sin identidad" aparecen todavía en los libros de texto más viejos. A partir de 1960, los tomos de Bourbaki abogaron por incluir la identidad en la definición de anillo. Hoy en día los textos clásicos como los de Jacobson, Lang, Maclane y Birkhoff, todos postulan la presencia de $1 \in A$.

[2] El nombre viene del alemán *Körper*, un término introducido por Richard Dedekind en 1871; se llama *corps* en francés, *cuerpo* en español, *corp* en rumano, etc., pero en inglés se llama *field*. En español, no debe usarse la traducción secundaria "campo", reservada para campos vectoriales, campos magnéticos, etc.

- Si A es un anillo cualquiera y si $n \in \{1,2,3,\dots\}$, el **anillo de matrices** $M_n(A)$ consta de matrices $n \times n$ con entradas en A, con el producto matricial evidente:

$$c = ab \quad \text{si y solo si todo} \quad c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}.$$

  Para $n \geq 2$, el anillo $M_n(A)$ no es conmutativo, aun cuando el anillo A sea conmutativo.

- Si G es un grupo finito y si $\mathbb{F}$ es un cuerpo, el **anillo grupal** $\mathbb{F}[G]$ consta de sumas formales $\alpha = \sum_{x \in G} a_x x$ con $x \in G$ y $a_x \in \mathbb{F}$, con la operación de suma evidente: si $\beta = \sum_{x \in G} b_x x$, entonces $\alpha + \beta = \sum_{x \in G} (a_x + b_x) x$, mientras

$$\alpha\beta = \left(\sum_{x \in G} a_x x \right) \left(\sum_{y \in G} b_y y \right) = \sum_{x \in G} \sum_{y \in G} a_x b_y xy = \sum_{z \in G} \left(\sum_{xy = z} a_x b_y \right) z.$$

  La identidad de $\mathbb{F}[G]$ es el elemento neutro $1 \in G$, considerado como suma formal con un solo término.

Definición 1.3. Un **homomorfismo de anillos** $\varphi \colon A \to B$ es una aplicación que preserva las operaciones de suma y producto y respeta la identidad multiplicativa:

$$\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2), \qquad \varphi(a_1 a_2) = \varphi(a_1)\,\varphi(a_2), \qquad \varphi(1_A) = 1_B.$$

Un homomorfismo inyectivo se llama un **monomorfismo**, un homomorfismo sobreyectivo es un **epimorfismo**, un homomorfismo biyectivo es un **isomorfismo**.

Definición 1.4. Un **ideal** (bilateral) en un anillo A es un subgrupo aditivo de A tal que

$$x \in B,\ a \in A \implies ax \in B,\ xa \in B.$$

Las coclases aditivos $a + B := \{\, a + x : x \in B \,\}$, elementos del grupo cociente A/B, admiten un producto $(A+B)(b+B) := ab + B$, ya que $(a+x)(b+y) = ab + (ay + bx + xy) \in ab + B$ para todo $x, y \in B$. Luego A/B es un anillo con identidad $1 + B$, llamado el **anillo cociente** de A por el ideal B.

La **aplicación cociente** $\eta \colon A \to A/B : a \mapsto a + B$ es un epimorfismo de anillos, cuyo *núcleo* $\ker \eta$ coincide con el ideal B. Por otro lado, si $\varphi \colon A \to A'$ es un homomorfismo de anillos cualquiera, su núcleo $\ker \varphi := \{\, a \in A : \varphi(a) = 0 \,\}$ es un ideal de A.[3] Obsérvese que $1 \in B$ si y sólo si $B = A$, si y sólo si $A/B = 0$. Si $0 \neq B \neq A$, se dice que B es un **ideal propio** de A.

Definición 1.5. Un *ideal a la izquierda* en un anillo A es un subgrupo aditivo M de A tal que $am \in M$ para todo $a \in A$, $m \in M$. En este caso, las coclases forman un grupo aditivo abeliano A/M que generalmente no es un anillo.

Un *ideal a la derecha* en un anillo A es un subgrupo aditivo N de A tal que $na \in N$ para todo $a \in A$, $n \in N$. Una parte $B \subseteq A$ es simultáneamente un ideal a la izquierda y un ideal a la derecha si y sólo si B es un ideal bilateral.

[3] El cero del anillo A/B es la coclase B. Sin embargo, es costumbre denotar cualquier cero por el dígito 0, y cualquier identidad multiplicativa por el dígito 1. Con algún riesgo de confusión, el anillo trivial $\{0\}$ también se denota simplemente por 0.

Ejemplo 1.6. Si $\mathbb{F}$ es un cuerpo y si $n \in \{2,3,\dots\}$, el anillo de matrices $A = M_n(\mathbb{F})$ es *simple*, es decir, no tiene ideales propios. Sin embargo, A posee varios ideales a la izquierda. Si $J = \{j_1,\dots,j_m\} \subseteq \{1,\dots,n\}$ es un juego de índices, sea B_J la totalidad de matrices en A en donde solamente las columnas $j_1,\dots,j_m$ no son nulas: $b_{ik} = 0$ para $k \notin J$. Entonces cada B_J es un ideal a la izquierda de A.

Definición 1.7. El **ideal generado** por una parte $S \subset A$ es la intersección de todos los ideales de A que incluyen S. Cuando $S = \{b_1,\dots,b_n\}$ es finito, se denota este ideal por $(b_1,\dots,b_n)$. Cuando A es conmutativo, cada elemento de $(b_1,\dots,b_n)$ es de la forma $a_1b_1 + \cdots + a_nb_n$ para algunos elementos $a_1,\dots,a_n \in A$.

Un ideal generado por un solo elemento $b \in A$ es un **ideal principal** de A. En general, $(b) = AbA := \{\sum_{i,j} a_i b c_j : \text{ cada } a_i, c_j \in A\}$ (con sumas finitas). Cuando A es conmutativo, es $(b) = Ab = \{ab : a \in A\}$.

Un anillo *conmutativo* $A \neq 0$ en el cual cada ideal es principal es un **anillo principal**.

Definición 1.8. Un anillo conmutativo A es un **anillo entero** si $ab = 0$ en A implica $a = 0$ o bien $b = 0$; es decir, A no contiene divisores de cero.[4]

Si $a, b \in A$ con $a \neq 0$, se escribe $\underline{a \setminus b}$ y se dice que a **divide** b, si y sólo si hay un elemento $c \in A$ tal que $\underline{b = ca}$. Ese elemento es único, porque $ca = c'a$ sólo si $(c - c')a = 0$, sólo si $c = c'$, ya que A es entero. También se escribe $\underline{c = b/a}$ en este caso. Obsérvese que no hace falta que a sea inversible.

Ejemplo 1.9. El anillo $\mathbb{Z}$ es un *anillo entero principal*.[5] En efecto, si B es un ideal propio de $\mathbb{Z}$, sea b el menor elemento positivo de B. Si $x \in B$, la división con residuo $x = by + r$ con $0 \leq r < b$ conlleva $r \in B$ y por tanto $r = 0$: se concluye que $B = (b)$. Además, el *generador* b de este ideal principal es el máximo común divisor de todos los elementos de B.

Ejemplo 1.10. El ejemplo $\mathbb{Z}$ se puede generalizar. Si $\mathbb{F}$ es un cuerpo, el **anillo de polinomios** $\underline{\mathbb{F}[t]}$ en un "indeterminado" t es un anillo entero principal. En efecto, los polinomios admiten división con residuo: si $f(t), g(t) \in \mathbb{F}[t]$, con $g(t) \neq 0$, entonces hay un único par de polinomios $q(t), r(t)$ tales que $f(t) = q(t)\,g(t) + r(t)$ y además $r(t)$ tiene menor grado que $g(t)$ o bien $r(t) = 0$. (La existencia y unicidad del "cociente" $q(t)$ y el residuo $r(t)$ se verifican con el algoritmo euclidiano.)

Definición 1.11. Más generalmente, un anillo entero A se llama un **anillo euclidiano** si hay una función $\delta\colon A \setminus \{0\} \to \mathbb{N}$ tal que, para cada par de elementos no ceros $a, b \in A$, existen $q, r \in A$ tales que $a = qb + r$, donde o bien $r = 0$, o bien $\delta(r) < \delta(b)$.

En el caso $A = \mathbb{Z}$, se toma $\delta(n) := |n|$, el valor absoluto.

En el caso $A = \mathbb{F}[t]$, $\delta(f(t))$ es el *grado* del polinomio no nulo $f(t)$. Conviene dejar indefinido el grado del polinomio nulo; entonces un polinomio de grado cero es simplemente una constante $c \neq 0$.

[4] En francés, *anneau entier*; pero en inglés, *integral domain*. Serge Lang, *Algebra*, 3a edición (Springer, New York, 2002) usa el término *entire ring*. Kronecker (1881) llamó "dominio de racionalidad" a lo que ahora se llama cuerpo. Huyan de los textos en español que hablan de "dominio íntegro" o "dominio de integridad".

[5] En vez de "anillo entero principal", también se usa la terminología arcaica "dominio entero principal" —en inglés, *principal ideal domain* o bien *PID*.

Lema 1.12. *Un anillo euclidiano es un anillo entero principal.*

Demostración. Si J es un ideal no nulo del anillo euclidiano A, hay un elemento $c \neq 0$ en J tal que $\delta(c)$ es mínimo. Entonces cada $a \in J$ es de la forma $a = qc + r$, con $r = 0$ o bien $\delta(r) < \delta(c)$. Pero $r = a - qc \in J$, así que la posibilidad de que $\delta(r) < \delta(c)$ queda excluida por la minimalidad de $\delta(c)$; por lo tanto, es $r = 0$. La relación $a = qc$ dice que $c \setminus a$ para todo $a \in J$, y por ende $J = (c)$ es un ideal principal. □

Si $A = \mathbb{F}[t_1]$ es un anillo de polinomios con coeficientes en un cuerpo $\mathbb{F}$, se puede formar el anillo $\mathbb{F}[t_1, t_2] := A[t_2]$ de polinomios en dos "indeterminados" t_1, t_2, e inductivamente se definen los anillos $\mathbb{F}[t_1, \ldots, t_m]$ de polinomios en m indeterminados. Estos son anillos enteros, pero no son principales para $m > 1$: el ideal (t_1, t_2) en $\mathbb{F}[t_1, t_2]$, que reúne todos los polinomios en dos variables con coeficiente constante nulo, no admite un solo generador.

Definición 1.13. Un elemento inversible $u \in A$ se llama una *unidad* del anillo A. Dos elementos $a, b \in A$ se dicen **asociados** si hay una unidad $u \in A$ tal que $ua = b$; es fácil ver que esta es una relación de equivalencia.

Si A es un anillo entero, un elemento no nulo $a \in A$ es **irreducible** si a no es inversible y si $a = bc$ es posible sólo si b ó c es una unidad.

Un anillo entero A es un **anillo factorial** si cada elemento no nulo admite una factorización[6] en irreducibles $a = p_1 p_2 \ldots p_r$ que es *única* en el siguiente sentido: si $a = q_1 q_2 \ldots q_s$ es otra factorización en irreducibles, entonces $s = r$ y hay una permutación de índices $\sigma \in S_r$ tal que p_j y $q_{\sigma(j)}$ son asociados, para $j = 1, \ldots, r$.

El número r de factores irreducibles se llama la **longitud** del elemento a, denotado $l(a)$. Si u es una unidad de A, se pone $l(u) = 0$.

Ejemplo 1.14. Sea A un anillo conmutativo. Un elemento $d \in A$ es un **máximo común divisor** de dos elementos $a, b \in A$ si (i) $d \setminus a$ y $d \setminus b$; (ii) para cada $c \in A$ tal que $c \setminus a$ y $c \setminus b$, vale $c \setminus d$. Dos elementos d con esta propiedad son asociados. Si A es un anillo principal, cada par de elementos a, b posee un máximo común divisor: se puede tomar d como un generador del ideal $(a, b) \subseteq A$.

La igualdad $(a, b) = (d)$ da lugar a la **identidad de Bézout**: d es un máximo común divisor de a y b si y sólo si hay elementos $p, q \in A$ tales que $\underline{ap + bq = d}$.

Un teorema clásico de la teoría de anillos[7] dice que cada anillo entero principal es factorial. También puede mostrarse que si A es un anillo factorial, entonces el anillo de polinomios $A[t]$ es también factorial. Por lo tanto, para cualquier cuerpo $\mathbb{F}$, el anillo $\mathbb{F}[t_1, t_2]$ es un ejemplo de un anillo factorial que no es principal.

[6] Terminología arcaica: "dominio de factorización única".

[7] Consúltese uno de los textos básicos:
Isadore N. Herstein, *Topics in Algebra*, Blaisdell, New York, 1964.
Nathan Jacobson, *Basic Algebra I*, W. H. Freeman, New York, 1985.
Serge Lang, *Algebra*, 3ª edición, Springer, New York, 2002.
Saunders MacLane y Garrett Birkhoff, *Algebra*, Macmillan, New York, 1967.

1.2 Módulos sobre un anillo

Definición 1.15. Si A es un anillo, un ***A*-módulo a la izquierda** es un grupo abeliano M, junto con una aplicación $\mu : A \times M \to M$, denotado por $ax := \mu(a,x)$, que cumple las propiedades siguientes:

(a) $a(x+y) = ax+ay$, para todo $a \in A$, $x,y \in M$;

(b) $(a+b)x = ax+bx$, para todo $a,b \in A$, $x \in M$;

(c) $a(bx) = (ab)x$, para todo $a,b \in A$, $x \in M$;

(d) $1x = x$, para todo $x \in M$.

La aplicación μ se llama una **acción** de A sobre M.

Lema 1.16. *Sea M un A-módulo a la izquierda; entonces para $a \in A$ y $x \in M$, valen las igualdades:*

$$a0 = 0, \qquad 0x = 0, \qquad (-1)x = -x.$$

Demostración. La propiedad (a) de la Definición 1.15 implica $a0 = a(0+0) = a0+a0$. La propiedad (b) implica $0x = (0+0)x = 0x+0x$. Además, la propiedad (d) demuestra la relación $0 = (1-1)x = 1x+(-1)x = x+(-1)x$. □

Definición 1.17. Un grupo abeliano N es un ***A*-módulo a la derecha** si existe una aplicación $\nu : N \times A \to N$, denotado por $xa := \nu(x,a)$, que cumple las propiedades:

$$(x+y)a = xa+ya, \qquad x(a+b) = xa+xb, \qquad (xb)a = x(ba), \qquad x1 = x,$$

para todo $a,b \in A$, $x,y \in N$.

La mayoría de los A-módulos considerados en este curso son A-módulos a la izquierda. Cuando el anillo A es *conmutativo*, la asignación $ax := xa$ convierte un A-módulo a la derecha en un A-módulo a la izquierda. Esta correspondencia puede extenderse a anillos no conmutativos, mediante el siguiente artificio.

Definición 1.18. Sea A un anillo cualquiera. Su **anillo opuesto** A° es el anillo tal que $(A^\circ,+)$ coincide con $(A,+)$ como grupo abeliano, pero cuyo producto es el reverso del producto de A. Denótese los elementos de A° por $\{\, a^\circ : a \in A \,\}$; se define

$$a^\circ b^\circ := (ba)^\circ.$$

Evidentemente, la aplicación idéntica $a \mapsto a^\circ$ es un isomorfismo de anillos entre A y A° si y sólo si A es conmutativo.

Obsérvese que cualquier A-módulo a la derecho M puede ser considerado como un A°-módulo a la izquierda, al definir

$$a^\circ x := xa \quad \text{para todo} \quad a \in A,\ x \in M.$$

De ahora en adelante, el término "A-módulo" indicará un A-módulo a la izquierda, salvo indicación expresa de lo contrario.

Ejemplo 1.19. Un módulo V sobre un *cuerpo* $\mathbb{F}$ es simplemente un **espacio vectorial**, en donde la operación $\mu : \mathbb{F} \times V \to V$ es la multiplicación escalar. La teoría de módulos entonces generaliza la teoría de espacios vectoriales (es decir, el álgebra lineal) para que los "escalares" sean elementos de un anillo cualquiera.

Ejemplo 1.20. Un $\mathbb{Z}$-*módulo* M es simplemente un **grupo abeliano** sin más estructura. De hecho, la propiedad $1x = x$ y la propiedad distributiva b implican que

$$nx = (1+1+\cdots+1)x = x+x+\cdots+x \quad (n \text{ veces}),$$

para $n \in \mathbb{N}$; además, $(-n)x = (-1)(nx) = -nx$. De este modo, la acción de $\mathbb{Z}$ sobre M es única y coincide con la acción evidente.

Ejemplo 1.21. Cualquier anillo A es un módulo sobre sí mismo, tanto a la izquierda como a la derecha, al definir $\mu(a,b) = \nu(a,b) := ab$, la operación de multiplicación en A. Las propiedades (a–d) de la definición de A-módulo son las dos leyes distributivas, la asociatividad y la propiedad de identidad de $1 \in A$.

Ejemplo 1.22. Si M es un ideal a la izquierda en un anillo A, entonces M es un A-módulo, ya que $am \in M$ para $a \in A$, $m \in M$, y las propiedades de anillos verifican las propiedades (a–d) de la definición de A-módulo.

El grupo abeliano cociente A/M es también un A-módulo, al definir $a(b+M) := ab+M$.

Ejemplo 1.23. Si A es un anillo y si $n = 1,2,3,\ldots$, sea $\underline{A^n}$ el grupo abeliano de n-tuplas de elementos de A, con suma $(a_1,\ldots,a_n)+(b_1,\ldots,b_n) := (a_1+b_1,\ldots,a_n+b_n)$. Entonces A^n es un A-módulo, al definir la acción $c(a_1,\ldots,a_n) := (ca_1,\ldots,ca_n)$.

Los elementos especiales $e_1 := (1,0,\ldots,0)$, $e_2 := (0,1,\ldots,0)$, $\ldots$, $e_n := (0,0,\ldots,1)$ forman una **base** para A^n, en el siguiente sentido:

- cada elemento de A^n es de la forma $a_1e_1+\cdots+a_ne_n$, con coeficientes $a_1,\ldots,a_n \in A$;
- Si $a_1e_1+\cdots+a_ne_n = 0$ en A^n, entonces $a_1 = \cdots = a_n = 0$ en A.

Cuando A es un cuerpo, cualquier A-módulo (es decir, cualquier espacio vectorial sobre A) posee una base: un conjunto generador, linealmente independiente. Para anillos más generales, esto no ocurre. El A-módulo A^n es *libre*, es decir, posee una base; pero en general hay A-módulos que no son libres.

Ejemplo 1.24. Si A es un anillo, entonces A^n es un módulo a la derecha sobre el anillo de matrices $M_n(A)$: para una matriz $b = [b_{ij}] \in M_n(A)$, se define $(a_1,\ldots,a_n)\,b := (c_1,\ldots,c_n)$ donde $c_j := \sum_{j=1}^{n} a_i b_{ij}$ para $j = 1,\ldots,n$.

Al considerar los elementos de A^n como *columnas* con entradas en A, el grupo abeliano A^n tiene la estructura de $M_n(A)$-módulo a la izquierda, al tomar

$$\begin{pmatrix} b_{11} & \ldots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \ldots & b_{nn} \end{pmatrix} \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} := \begin{pmatrix} b_{11}c_1+\cdots+b_{1n}c_n \\ \vdots \\ b_{n1}c_1+\cdots+b_{nn}c_n \end{pmatrix}.$$

En la práctica, este segundo punto de vista es más útil. En adelante, se tomará A^n como la totalidad de n-columnas con entradas en A, salvo mención explícita de lo contrario. Cuando hay que mirar a A^n como la totalidad de n-filas con entradas en A, se lo denotará por ${}^nA$.

Ejemplo 1.25. Si $T\colon V \to V$ es un operador lineal sobre un espacio vectorial V sobre un cuerpo $\mathbb{F}$, entonces V es un módulo para el anillo de polinomios $\mathbb{F}[t]$, del modo siguiente. Si $f(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n \in \mathbb{F}[t]$, sea $f(T) := a_0 I + a_1 T + a_2 T^2 + \cdots + a_n T^n$ el operador lineal correspondiente. Defínase

$$\underline{f(t)\cdot v} := f(T)(v) \quad \text{para todo} \quad v \in V. \tag{1.1}$$

Es fácil comprobar las propiedades (a–d) de la Definición 1.15 para $A = \mathbb{F}[t]$, $M = V$. Por ejemplo, si $f(t), g(t) \in \mathbb{F}[t]$, $v \in V$, entonces

$$f(t)\cdot\big(g(t)\cdot v\big) = f(t)\cdot g(T)(v) = f(T)\big(g(T)(v)\big) = fg(T)(v) = fg(t)\cdot v,$$

donde $fg(t) := f(t)\,g(t)$ es el producto de los polinomios $f(t)$ y $g(t)$ en $\mathbb{F}[t]$. Las propiedades algebraicas del operador T están reflejadas en las propiedades de este $\mathbb{F}[t]$-módulo.

► Después de pasar revista a estos ejemplos, es oportuno considerar algunos construcciones básicas, que son análogas a lo que se hace con grupos y anillos. El concepto más importante es el de homomorfismo de módulos.

Definición 1.26. Un **submódulo** de un A-módulo M es un subgrupo aditivo N de M tal que $ay \in N$ para todo $a \in A$, $y \in N$.

Si $\mathbb{F}$ es un cuerpo, M un espacio vectorial sobre $\mathbb{F}$, entonces un $\mathbb{F}$-submódulo es un *subespacio vectorial* de M. Por otro lado, si M es un grupo abeliano (es decir, un $\mathbb{Z}$-módulo), un $\mathbb{Z}$-submódulo es simplemente un *subgrupo abeliano* de M.

Si N es un A-submódulo de M, el grupo abeliano cociente M/N es también un A-módulo, al poner $a(x+N) := ax+N$. Este es el **módulo cociente** de M por N.

Definición 1.27. Una aplicación $\varphi\colon M \to N$ entre dos A-módulos es un **homomorfismo de módulos** si

$$\varphi(x+y) = \varphi(x) + \varphi(y), \quad \varphi(ax) = a\,\varphi(x), \quad \text{para todo} \quad x, y \in M,\ a \in A.$$

El **núcleo** de φ es el A-submódulo $\underline{\ker\varphi} := \{\, x \in M : \varphi(x) = 0 \,\} \subseteq M$. La **imagen** de φ es el A-módulo $\underline{\operatorname{im}\varphi} := \{\, \varphi(x) \in N : x \in \overline{M} \,\} \subseteq N$.

Un homomorfismo inyectivo se llama un **monomorfismo**; un homomorfismo sobreyectivo se llama un **epimorfismo**; y un homomorfismo biyectivo se llama un **isomorfismo**.

Definición 1.28. El conjunto de los homomorfismos de A-módulos de M en N se denota por $\underline{\operatorname{Hom}_A(M,N)}$. Este es un grupo abeliano bajo la *suma puntual* de homomorfismos:

$$\underline{(\varphi+\psi)}(x) := \varphi(x) + \psi(x) \in N, \quad \text{para todo} \quad \varphi, \psi \in \operatorname{Hom}_A(M,N),\ \ x \in M. \tag{1.2}$$

Si $N = M$, un homomorfismo $\varphi\colon M \to M$ se llama *endomorfismo* de M. El anillo (bajo composición) de todos los endomorfismos de M se denota por $\underline{\operatorname{End}_A(M)} \equiv \operatorname{Hom}_A(M,M)$.

Cuando N es un A-submódulo de un A-módulo M, se dispone de dos homomorfismos "canónicos": la **inclusión** $\underline{i\colon M \to N}$, el cual es un monomorfismo; y la **aplicación cociente** $\underline{\eta : M \to M/N}$ definido por $\eta(x) := x+N$, el cual es un epimorfismo.

Lema 1.29. *Si $\varphi\colon M \to M'$ es un homomorfismo de A-módulos y si N es un submódulo de M tal que $N \subseteq \ker\varphi$, entonces hay un único homomorfismo $\bar{\varphi}\colon M/N \to M'$ tal que*

$$\bar{\varphi}(x+N) = \varphi(x) \quad \textit{para todo} \quad x \in M. \tag{1.3a}$$

Equivalentemente, si $\eta : M \to M/N$ denota la aplicación cociente, entonces $\underline{\bar{\varphi}\,\eta = \varphi}$, así que se verifica la conmutatividad del diagrama siguiente:

$$\begin{array}{ccc} M & \xrightarrow{\ \varphi\ } & M' \\ {\scriptstyle\eta}\big\downarrow & \nearrow_{\exists!\,\bar{\varphi}} & \\ M/N & & \end{array} \tag{1.3b}$$

Además, $\bar{\varphi}$ es sobreyectiva si y sólo si φ es sobreyectiva; $\bar{\varphi}$ es inyectiva si y sólo si $\ker\varphi = N$; luego, $\bar{\varphi}$ es biyectiva si y sólo si φ es sobreyectiva con $\ker\varphi = N$.

Demostración. La unicidad de $\bar{\varphi}$ es clara, porque la fórmula (1.3a) determina la aplicación $\bar{\varphi}$. Para la existencia, es cuestión de notar que la aplicación dada por esta fórmula está bien definida. En efecto, si $x+N = y+N$, entonces $x-y \in N \subseteq \ker\varphi$, así que $\varphi(x) = \varphi(y)$.

Las propiedades listadas de $\bar{\varphi}$ son evidentes. □

Los tres "teoremas de isomorfismo", que son familiares en los casos de los grupos y anillos, se verifican también para los A-módulos.

Proposición 1.30. *Sea M un A-módulo, sea $\varphi\colon M \to M'$ es un homomorfismo de A-módulos, y sean L,N dos A-submódulos de M. Entonces:*

1. *Hay un isomorfismo de A-módulos $(M/\ker\varphi) \simeq \operatorname{im}\varphi$.*
2. *Los grupos abelianos $L\cap N$ y $L+N$ son A-submódulos de M y hay un isomorfismo $L/(L\cap N) \simeq (L+N)/N$.*
3. *Si $L \subseteq N \subseteq M$, hay un isomorfismo $M/N \simeq (M/L)\big/(N/L)$.*

Demostración. Ad (1): Aplíquese el Lema 1.29 con $N \mapsto \ker\varphi$, $M' \mapsto \operatorname{im}\varphi$. La aplicación $\bar{\varphi}$ dado por (1.3) es el isomorfismo deseado.

Ad (2): Es inmediato verificar que $L\cup N$ y $L+N := \{x+y : x \in L,\ y \in N\}$ son A-submódulos de M. Defínase un homomorfismo $\theta\colon L \to M/N$ por $\theta(x) := x+N$. Fíjese que $\ker\theta = L\cap N$ y que $\operatorname{im}\theta = \{x+N : x \in L\} = (L+N)/N$. La parte anterior proporciona el isomorfismo $\bar{\theta}$ deseado.

Ad (3): Defínase un homomorfismo $\psi\colon M/L \to M/N$ por $\psi(x+L) := x+N$. Fíjese que $\ker\psi = \{x+L : x \in N\} = N/L$ y que $\operatorname{im}\psi = \{x+N : x \in M\} = M/N$. La primera parte proporciona el isomorfismo $\bar{\psi}$ deseado. □

Corolario 1.31. *Cualquier homomorfismo de A-módulos $\varphi\colon M \to N$ admite una factorización canónica*[8] *como composición de un epimorfismo, un isomorfismo y un monomorfismo.*

Demostración. Por la Proposición anterior, el segundo factor en la siguiente composición $\varphi = i\,\bar{\varphi}\,\eta$ es un isomorfismo:

$$\begin{array}{ccc} M & \xrightarrow{\ \varphi\ } & N \\ {\scriptstyle\eta}\downarrow & & \uparrow{\scriptstyle i} \\ M/\ker\varphi & \xrightarrow{\ \bar{\varphi}\ } & \operatorname{im}\varphi \end{array}$$

donde $\eta\colon M \to M/\ker\varphi$ es la aplicación cociente, $i\colon \operatorname{im}\varphi \to N$ es la inclusión. □

1.3 Sumas directas y módulos libres

Dados dos A-módulos M y N cualesquiera, se puede formar su suma directa $M \oplus N$ como grupos abelianos; este puede considerarse como A-módulo de manera evidente. En los textos, se encuentran discusiones de suma directa "externa" y suma directa "interna", lo cual puede crear cierta confusión. Esta distinción es a veces útil en cálculos concretos, pero en todo caso esos dos objetos son isomorfos, aun cuando no coinciden.

Definición 1.32. Si M y N son dos A-módulos, su **suma directa** (externa) es el conjunto $M \oplus N$ de pares ordenados[9] (x,y) con $x \in M$, $y \in N$, con la siguiente suma y acción de A:

$$(x_1,y_1)+(x_2,y_2) := (x_1+x_2, y_1+y_2), \qquad a(x,y) := (ax,ay) \quad \text{para} \quad a \in A.$$

Más generalmente, si $M_1,\dots,M_n$ es un juego finito de A-módulos, su suma directa (externa) $M_1 \oplus M_2 \oplus \cdots \oplus M_n$ es la totalidad de n-tuplas ordenadas $(x_1,\dots,x_n)$ con $x_i \in M_i$ para $i = 1,\dots,n$, donde la suma y la acción de A se define entrada por entrada.

Lema 1.33. *La suma directa de A-módulos $M \oplus N$ determina cuatro homomorfismos:*

$$M \underset{p_1}{\overset{i_1}{\rightleftarrows}} M \oplus N \underset{p_2}{\overset{i_2}{\rightleftarrows}} N \tag{1.4a}$$

que cumplen las siguientes igualdades:

$$p_1\,i_1 = 1_M, \quad p_1\,i_2 = 0, \quad p_2\,i_1 = 0, \quad p_2\,i_2 = 1_N, \quad i_1\,p_1 + i_2\,p_2 = 1_{M\oplus N}. \tag{1.4b}$$

Demostración. Estos homomorfismos se definen así:

$$i_1(x) := (x,0), \quad i_2(y) := (0,y), \quad p_1(x,y) := x, \quad p_2(x,y) := y,$$

[8] La palabra *canónica* tiene un sentido técnico específico, como se verá más adelante. Por ahora, se le usa informalmente, en el sentido de un procedimiento estándar que se aplica de la misma manera en todos los casos.

[9] Es decir, $M \oplus N$ coincide con el producto cartesiano $M \times N$ como conjunto sin operaciones algebraicas.

para $x \in M$, $y \in N$. Las primeras cuatro de las relaciones (1.4b) son evidentes. Para la última relación, obsérvese que tanto $i_1 p_1$ como $i_2 p_2$ pertenecen al anillo $\mathrm{End}_A(M \oplus N)$ y por ende poseen una suma puntual:

$$(i_1 p_1 + i_2 p_2)(x,y) \equiv i_1 p_1(x,y) + i_2 p_2(x,y) = i_1(x) + i_2(y) = (x,0) + (0,y) = (x,y)$$

así que $i_1 p_1 + i_2 p_2$ es el endomorfismo identidad sobre $M \oplus N$. □

Lema 1.34. *Dados dos A-módulos M y N, un tercer A-módulo L es isomorfo a $M \oplus N$ si y sólo si hay cuatro homomorfismos:*

$$M \underset{\pi_1}{\overset{\iota_1}{\rightleftarrows}} L \underset{\pi_2}{\overset{\iota_2}{\rightleftarrows}} N$$

que cumplen las siguientes igualdades:

$$\pi_1 \iota_1 = 1_M, \quad \pi_1 \iota_2 = 0, \quad \pi_2 \iota_1 = 0, \quad \pi_2 \iota_2 = 1_N, \quad \iota_1 \pi_1 + \iota_2 \pi_2 = 1_L. \tag{1.5}$$

Demostración. Si hay un isomorfismo $\theta : M \oplus N \to L$, sean i_1, i_2, p_1, p_2 los homomorfismos definidos en el Lema anterior, que cumplen (1.4). Entonces los homomorfismos $\iota_1 := \theta\, i_1$, $\iota_2 := \theta\, i_2$, $\pi_1 := p_1 \theta^{-1}$, $\pi_2 := p_2 \theta^{-1}$ cumplen las relaciones (1.5).

Por otro lado, dados homomorfismos ι_1, ι_2, π_1, π_2 que cumplen (1.5), defínase

$$\theta := i_1 \pi_1 + i_2 \pi_2 : L \to M \oplus N, \qquad \lambda := \iota_1 p_1 + \iota_2 p_2 : M \oplus N \to L.$$

Sus composiciones son endomorfismos: $\lambda\theta \in \mathrm{End}_A(L)$ mientras $\theta\lambda \in \mathrm{End}_A(M \oplus N)$. De las relaciones (1.4b) y (1.5) se obtiene

$$\begin{aligned} \lambda\theta &= \iota_1 p_1 i_1 \pi_1 + \iota_1 p_1 i_2 \pi_2 + \iota_2 p_2 i_1 \pi_1 + \iota_2 p_2 i_2 \pi_2 = \iota_1 \pi_1 + \iota_2 \pi_2 = 1_L, \\ \theta\lambda &= i_1 \pi_1 \iota_1 p_1 + i_2 \pi_2 \iota_1 p_1 + i_1 \pi_1 \iota_2 p_2 + i_2 \pi_2 \iota_2 p_2 = i_1 p_1 + i_2 p_2 = 1_{M \oplus N}, \end{aligned}$$

lo cual muestra que θ es un isomorfismo con inverso $\theta^{-1} = \lambda$. Luego, es $L \simeq M \oplus N$. □

Corolario 1.35. *Si M y N son A-submódulos de un tercer A-módulo K tales que $M \cap N = 0$, entonces la suma (ordinaria) $\underline{M+N} := \{x+y \in K : x \in M,\ y \in N\}$ es isomorfo a $M \oplus N$.*

Demostración. Sean $\iota_1 : M \to M+N$ y $\iota_2 : N \to M+N$ las inclusiones $\iota_1(x) := x$, $\iota_2(y) := y$.

Para definir unos homomorfismos $\pi_1 : M+N \to M$ y $\pi_2 : M+N \to N$ que cumplen (1.5) en el caso $L = M+N$, fíjese que cada elemento de $M+N$ puede expresar en la forma $x+y$ con $x \in M$, $y \in N$ *de manera única*. En efecto, si $x' \in M$, $y' \in N$ con $x'+y' = x+y$, entonces $x'-x = y-y'$ en K; pero este es un elemento de $M \cap N$, así que $x'-x = y-y' = 0$, luego $x' = x$, $y' = y$.

Entonces las proyecciones $\pi_1(x+y) := x$, $\pi_2(x+y) := y$ son bien definidas y se verifican las primeras cuatro relaciones de (1.5). Además,

$$(\iota_1 \pi_1 + \iota_2 \pi_2)(x+y) = \iota_1(x) + \iota_2(y) = x+y,$$

de modo que $\iota_1 \pi_1 + \iota_2 \pi_2 = 1_{M+N}$. Ahora el Lema 1.34 muestra que $M+N \simeq M \oplus N$. □

Cuando M y N son A-submódulos de otro A-módulo tales que $M \cap N = 0$, como en el enunciado del Corolario anterior, se dice que $M+N$ es la *suma directa interna* de M y N. En vista del isomorfismo ya comprobado, se escribe esta suma como $M \oplus N$ también. En adelante, no se distinguirá entre suma directa "interna" y "externa", sino que el contexto indicará el caso.

Ejemplo 1.36. Si A es un anillo, el módulo A^n es la suma directa $A \oplus A \oplus \cdots \oplus A$ con n sumandos.

Al tratar de formar la suma directa de una familia infinita de A-módulos $\{ M_j : j \in J \}$, los senderos se bifurcan. Por un lado, se puede formar el producto cartesiano $\prod_{j\in J} M_j$ de los M_j e imponer una suma y una acción de A entrada por entrada:

$$(x_j)_j + (y_j)_j := (x_j + y_j)_j, \qquad a(x_j)_j := (ax_j)_j.$$

El A-módulo así obtenido se llama el **producto directo** de los A-módulos individuales M_j. Las proyecciones $p_k \colon \prod_j M_{j\in J} \to M_k$ que acompañan el producto cartesiano, definidas por $p_k\big((x_j)_j\big) := x_k$, son homomorfismos de A-módulos.

Se define la **suma directa** $\bigoplus_{j\in J} M_j$ como el A-submódulo de $\prod_j M_j$ cuyos elementos son las familias $(x_j)_j$ con $x_j = 0$ *salvo por un número finito de índices* $j \in J$. Las inyecciones $i_k \colon M_k \to \bigoplus_{j\in J} M_j$ se definen al declarar que $i_k(y_k)$ es la familia $(x_j)_j$ tal que $x_k := y_k$, $x_j := 0$ para $j \neq k$.

En el caso de que todos los A-módulos M_j son copias de un sólo módulo M, se escribe

$$M^J := \prod_{j\in J} M, \qquad M^{(J)} := \bigoplus_{j\in J} M,$$

habido cuenta de que $M^{(J)} = M^J$ si y sólo si el conjunto J es finito. Si J es un conjunto finito con n elementos, esto es $M^n = M \oplus M \oplus \cdots \oplus M$ (n veces).

Definición 1.37. Sea $S = \{ x_j : j \in J \}$ una familia de elementos de un A-módulo M. Esta familia S **genera** M si todo elemento de M es una *combinación A-lineal* de elementos de S, es decir,

$$x \in M \implies x = a_{j_1}x_{j_1} + a_{j_2}x_{j_2} + \cdots + a_{j_r}x_{j_r}, \quad \text{con} \quad \begin{cases} a_{j_1}, a_{j_2}, \ldots, a_{j_r} \in A, \\ x_{j_1}, x_{j_2}, \ldots, x_{j_r} \in S. \end{cases}$$

Se dice que S es *linealmente independiente* (a veces, "A-linealmente" independiente) si una tal combinación A-lineal de sus elementos es cero sólo si $a_{j_1} = a_{j_2} = \cdots = a_{j_r} = 0$. Si S es linealmente independiente y además genera M, se dice que S es una **base** del A-módulo M.

Definición 1.38. Se dice que un A-módulo M es **libre** *si posee una base*.

Si $S = \{ x_j : j \in J \}$ es un conjunto cualquiera, sea $A\langle S \rangle$ el conjunto de funciones $f \colon S \to A$ tal que $f(x) = 0$ salvo por un número finito de elementos de S. Para $x \in S$, $a \in A$, denótese por ax la función $x \mapsto a$, $y \mapsto 0$ si $y \neq x$. Bajo la suma puntual de funciones, cualquier elemento

de $A\langle S\rangle$ es de la forma $a_{j_1}x_{j_1} + a_{j_2}x_{j_2} + \cdots + a_{j_r}x_{j_r}$, con $a_{j_1}, \ldots, a_{j_r} \in A$ y $x_{j_1}, \ldots, x_{j_r} \in S$. Entonces $A\langle S\rangle$ es un A-módulo libre, del cual S es una base. Se dice que $A\langle S\rangle$ es el A**-módulo libremente generado por** S.

Se adopta el convenio que el elemento nulo $0 \in M$ es una combinación lineal de cero elementos, así que el conjunto vacío $\emptyset$ genera el submódulo trivial $\{0\}$. Bajo este convenio, el A-módulo trivial 0 (es decir, $\{0\}$) es un A-módulo libre con base vacía.

Ejemplo 1.39. Considérese el anillo $\mathbb{Z}/m \equiv \mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$, de residuos de enteros bajo división por un número entero $m \geq 2$. Este es un $\mathbb{Z}$-módulo (es decir, un grupo abeliano) bajo la acción evidente $n\overline{k} := \overline{nk}$ para $n \in \mathbb{Z}$, $\overline{k} \in \mathbb{Z}/m$. Este anillo posee un solo generador, $\overline{1}$ (es decir, es un grupo cíclico) pero $\{\overline{1}\}$ no es una base, porque $m\,\overline{1} = \overline{0}$ en $\mathbb{Z}/m$ aunque $m \neq 0$ en $\mathbb{Z}$. El $\mathbb{Z}$-módulo $\mathbb{Z}/m$ *no es libre*, debido a este fenómeno de "torsión".

La *suma directa* $A^{(J)} = \bigoplus_{j\in J} A$ es un A-módulo libre. En efecto, sea $u_k := i_k(1)$ el elemento de $A^{(J)}$ con 1 en el lugar k y cero en los demás lugares. Entonces cada elemento de $A^{(J)}$ es una combinación lineal de los u_k; la única combinación lineal nula es la trivial, que da el elemento cero de $A^{(J)}$. Luego $\{\, u_j : j \in J \,\}$ es una base para $A^{(J)}$.

Proposición 1.40. *Sea L un A-módulo libre, con base $\{\, x_j : j \in J \,\}$, y sea N un A-módulo cualquiera. Sea $\{\, y_j : j \in J \,\}$ un juego de elementos de N. Entonces hay un único homomorfismo $\varphi\colon L \to N$ tal que $\varphi(x_j) = y_j$ para todo $j \in J$.*

Demostración. Cada elemento de L es una suma finita de la forma $x = a_{j_1}x_{j_1} + \cdots + a_{j_r}x_{j_r}$ donde los coeficientes $a_{j_1}, \ldots, a_{j_r}$ son unívocamente determinados por x. Se define, necesariamente,

$$\varphi(x) = \varphi(a_{j_1}x_{j_1} + \cdots + a_{j_r}x_{j_r}) := a_{j_1}y_{j_1} + \cdots + a_{j_r}y_{j_r} \in N, \tag{1.6}$$

Es fácil que esta receta es un homomorfismo de L en N. □

Corolario 1.41. *Si L y M son A-módulos libres con bases de la misma cardinalidad, entonces L y M son isomorfos. En particular, si $S = \{\, x_j : j \in J \,\}$, entonces $A\langle S\rangle \simeq A^{(J)}$.*

Demostración. Sean $\{\, x_j : j \in J \,\}$, $\{\, y_j : j \in J \,\}$ bases para L y M, respectivamente. La Proposición anterior determina dos homomorfismos $\varphi\colon L \to M$, $\psi\colon M \to L$ tales que $\varphi(x_j) = y_j$ y $\psi(y_j) = x_j$ para todo $j \in J$. Entonces $\psi\varphi \in \mathrm{End}_A(L)$ cumple $\psi\varphi(x_j) = x_j$ para todo $j \in J$, luego $\psi\varphi = 1_L$ por la unicidad de la citada Proposición. De igual manera, se obtiene $\varphi\psi = 1_M$ en $\mathrm{End}_A(M)$. En otras palabras, φ es un isomorfismo con inverso $\varphi^{-1} = \psi$. □

En particular, si L es libre y posee una base de n elementos, entonces $L \simeq A^n$.

La Proposición 1.40 tiene un resultado parejo (a continuación) que resalta la importancia de los módulos libres.

Proposición 1.42. *Sea M un A-módulo cualquiera. Entonces existe un A-módulo libre L que admite un homomorfismo sobreyectivo $\varphi\colon L \to M$. Por lo tanto, M es un cociente de un A-módulo libre.*

Demostración. Sea $\{ y_j : j \in J \}$ un juego de elementos que genera M; por ejemplo, puede tomarse M mismo como conjunto generador. Sea $S := \{ x_j : j \in J \}$ otro conjunto de la misma cardinalidad, y considérese el A-módulo libre $A\langle S\rangle$. La aplicación $S \to M : x_j \mapsto y_j$ se extiende a un homomorfismo $\varphi\colon A\langle S\rangle \to M$, que cumple (1.6) y por ende es sobreyectivo.

Por la Proposición 1.30, se obtiene $A\langle S\rangle / \ker\varphi \simeq \operatorname{im}\varphi = M$, lo cual demuestra que M es un cociente de $A\langle S\rangle$. □

En el caso de que $\mathbb{F}$ sea un cuerpo, cualquier $\mathbb{F}$-módulo es libre: se sabe que cualquier espacio vectorial V sobre $\mathbb{F}$ posee una base, y que $V \simeq \mathbb{F}^n$ si la base de V tiene n elementos.

Además, se sabe que la dimensión de un espacio vectorial está bien definida: si $\mathbb{F}^m \simeq \mathbb{F}^n$, entonces $m = n$. Este resultado extiende a anillos conmutativos.

Proposición 1.43. *Si A es un anillo conmutativo y si un módulo libre L tiene dos bases $\{x_1,\dots,x_n\}$ y $\{y_1,\dots,y_m\}$, entonces $m = n$.*

Demostración. Supóngase que $m \le n$. Hay coeficientes b_{ij}, c_{rs} en A, para $i,s = 1,\dots,m$ y $j,r = 1,\dots,n$, tales que

$$x_j = \sum_{i=1}^{m} b_{ij}\, y_i, \qquad y_s = \sum_{r=1}^{n} c_{rs}\, x_r, \tag{1.7}$$

Por sustitución de cada una de estas fórmulas en la otra, se ve que

$$x_j = \sum_{i=1}^{m}\sum_{k=1}^{n} b_{ij}\, c_{ki}\, x_k, \qquad y_s = \sum_{r=1}^{n}\sum_{t=1}^{m} c_{rs}\, b_{tr}\, y_t,$$

para $j,k = 1,\dots,n$ y $s,t = 1,\dots,m$. Por la unicidad de los coeficientes de combinaciones lineales respecto de una base y la conmutatividad de A, se concluye que

$$\sum_{i=1}^{m} b_{ij}\, c_{ki} = \sum_{i=1}^{m} c_{ki}\, b_{ij} = \delta_{kj}, \qquad \sum_{r=1}^{n} c_{rs}\, b_{tr} = \sum_{r=1}^{n} b_{tr}\, c_{rs} = \delta_{ts}, \tag{1.8}$$

donde aparecen deltas de Kronecker a los lados derechos. De forma más compacta, las b_{ij} son entradas de una matriz $m \times n$ sobre A y las c_{rs} son entradas de otra matriz $n \times m$ sobre A. Para compararlos, es oportuno definir dos matrices in $M_n(A)$ por

$$B := \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \dots & b_{mn} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}, \qquad C := \begin{pmatrix} c_{11} & \dots & c_{1m} & 0 & \dots & 0 \\ c_{21} & \dots & c_{2m} & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ c_{n1} & \dots & c_{nm} & 0 & \dots & 0 \end{pmatrix}.$$

Las relaciones (1.8) se escriben de manera abreviada así:

$$BC = 1_m \oplus 0_{n-m}, \qquad CB = 1_n,$$

donde 1_n es la matriz identidad en $M_n(A)$, mientras $1_m \oplus 0_{n-m}$ es la matriz diagonal con m entradas diagonales iguales a 1 seguidos por $n-m$ entradas diagonales iguales a 0.

Para ver que estas dos igualdades son inconsistentes si $m < n$, recuérdese que para un anillo conmutativo A se puede definir el determinante en $M_n(A)$ por la fórmula usual de Leibniz:

$$\det P := \sum_{\sigma \in S_n} (-1)^{\sigma} p_{1,\sigma(1)} p_{2,\sigma(2)} \cdots p_{n,\sigma(n)}.$$

Es inmediato que $\det(1_n) = 1$ y que $\det(PQ) = \det P \det Q$ para $P, Q \in M_n(A)$ —la multiplicatividad se demuestra por el argumento usual, ya que A es conmutativo. Si fuera $m < n$, los elementos $u = \det B$, $v = \det C$ cumplirían $vu = 1$, $uv = 0$ en A, lo cual es imposible porque $u = u1 = uvu = 0u = 0$ contradice $vu = 1$. Se concluye que $m = n$. □

Corolario 1.44. *Si A es un anillo conmutativo y si $A^m \simeq A^n$, entonces $m = n$.* ⊟

Definición 1.45. Si un A-módulo libre L es finitamente generado, su **rango** es la cardinalidad de cualquiera de sus bases. En particular, el rango de A^n es n.

El rango de un espacio vectorial es su dimensión.

Las expansiones (1.7) definen B y C como *matrices de cambio de base* en un A-módulo libre. Más generalmente, considérese un homomorfismo $\psi\colon L \to M$ entre dos A-módulos libres con las respectivas bases $\{x_1, \ldots, x_n\}$ de L y $\{y_1, \ldots, y_m\}$ de M. Entonces la unicidad de los coeficientes en expansiones muestran que si

$$\psi(x_j) = \sum_{i=1}^{m} c_{ij} y_i,$$

entonces la matriz rectangular $C \in M_{m,n}(A)$ caracteriza el homomorfismo ψ. Además, si $\varphi\colon L \to M$ es otro homomorfismo cuya matriz es B, entonces la *suma* puntual $\varphi + \psi$, definido por

$$\underline{\varphi + \psi}(x) := \varphi(x) + \psi(x), \quad \text{para todo} \quad x \in L,$$

tiene matriz $B + C$. En breves palabras, la correspondencia $\psi \leftrightarrow C$ define un *isomorfismo de grupos abelianos*,

$$\mathrm{Hom}_A(L, M) \simeq M_{m,n}(A), \tag{1.9}$$

donde $M_{m,n}(A)$ denota la totalidad de matrices $m \times n$ con entradas en A. Ahora, el lado derecho es una A-módulo (a la izquierda) de manera obvia: si $a \in A$ y $C = [c_{ij}]$, entonces $aC = [ac_{ij}]$. También se puede definir $a\psi \in \mathrm{Hom}_A(L, M)$ por $(a\psi)(x) := a\,\psi(x)$ para todo $x \in L$. Pero ahora resulta que, para $a, b \in A$:

$$(a\psi)(bx) = a\,\psi(bx) = ab\,\psi(x), \quad \text{mientras} \quad b(a\psi)(x) = ba\,\psi(x).$$

Esto es, la aplicación $a\psi\colon L \to M$ entrelaza la acción del elemento b de A sólo si $ab = ba$, en general. La biyección (1.9) *es un isomorfismo de A-módulos si y sólo si el anillo A es conmutativo*.

En el caso de que $L = M$, se compara el anillo $\mathrm{End}_A(L) = \mathrm{Hom}_A(L,L)$, bajo composición de endomorfismos, con el anillo $M_n(A)$, bajo producto de matrices. Los cálculos de la demostración de la Proposición 1.43 indican que *hay un isomorfismo de anillos*

$$\mathrm{End}_A(L) \simeq M_n(A),$$

si y sólo si el anillo A es conmutativo.

En el caso de un anillo no conmutativo A, se puede notar que las únicas diferencias con el caso conmutativo son unos cambio de orden de multiplicación. Es un ejercicio comprobar que $\mathrm{End}_A(L) \simeq M_n(A^\circ)$ en general, cuando L es un A-módulo libre de rango n.

1.4 Módulos sobre un anillo entero principal

Para poder investigar la estructura de A-módulos en más detalle, es conveniente restringir la mirada a una clase específica de anillos. Recuérdese que un anillo entero principal es un anillo conmutativo A, sin divisores de cero, en la cual cada ideal es generado por un solo elemento de A.

Proposición 1.46. *Sea A un anillo entero principal. Sea L un A-módulo libre de rango n y sea M un submódulo de L. Entonces M también es libre, de rango $m \leq n$.*

Demostración. Por inducción sobre el rango n de L. El caso $n = 0$ es trivial, porque $L = M = 0$. En el caso $n = 1$, es $L = Ax := \{ax : a \in A\}$, donde $\{x\}$ es una base de L. Si $J := \{b \in A : bx \in M\}$, es claro que J es un ideal de A; entonces $J = (c)$ para algún $c \in A$, de donde $M = \{acx : a \in A\}$. Si $M \neq 0$ (fíjese que el submódulo nulo es libre de rango 0), entonces $c \neq 0$ en A. Ahora, si $acx = 0$ en M, entonces $ac = 0$ en A, lo cual implica $a = 0$, por ser A entero. Luego $\{cx\}$ es una base de M así que M es un A-módulo libre de rango 1.

Para $n > 1$, sea $\{x_1, \ldots, x_n\}$ una base de L y sea L_1 el submódulo generado por $\{x_2, \ldots, x_n\}$, el cual es libre, de rango $n-1$. Por la hipótesis inductiva, podemos suponer que cada submódulo de L_1 es libre.

No hay más que hacer si $M \subseteq L_1$; considérese el caso $M \not\subseteq L_1$. Sea J el conjunto de los coeficientes $b \in A$ tal que exista $x \in M$ de la forma

$$x = bx_1 + a_2x_2 + \cdots + a_nx_n \quad \text{con} \quad a_2, \ldots, a_n \in A.$$

Queda claro que J es un ideal (no nulo) de A, así que $J = \{c\}$ para algún $c \neq 0$ en A. Entonces hay un elemento $y \in M$ de la forma $y = cx_1 + a_2'x_2 + \cdots + a_n'x_n$. Al escribir $b \in J$ como $b = dc$, se obtiene

$$x - dy = (a_2 - da_2')x_2 + \cdots + (a_n - da_n'x_n) \in M \cap L_1.$$

En otras palabras, cada $x \in M$ es de la forma $dy + z$ con $d \in A$, $z \in M \cap L_1$; en breve, es $M = Ay + (M \cap L_1)$. Por otro lado, se ve que $Ay \cap L_1 = 0$, debido a la independencia lineal de $\{x_1, \ldots, x_n\}$, así que esta suma es directa: es $M = Ay \oplus (M \cap L_1)$. Como $M \cap L_1$ es libre por hipótesis, con una base $\{z_1, \ldots, z_{m-1}\}$ para algún $m \leq n$, se concluye que M es libre, con base $\{y, z_1, \ldots, z_{m-1}\}$. □

Corolario 1.47. *Sea A un anillo entero principal. Si M es un A-módulo finitamente generado y si N es un submódulo de M, entonces N también es finitamente generado.*

Demostración. Por la Proposición 1.42, si M es generado por $\{y_1,\dots,y_n\}$, hay un A-módulo libre L con base $\{x_1,\dots,x_n\}$ y un homomorfismo sobreyectivo $\varphi\colon L\to M$ determinado por $\varphi(x_i):=y_i$ para $i=1,\dots,n$. Sea $L_1:=\varphi^{-1}(N)=\{x\in L:\varphi(x)\in N\}$ la preimagen de N en L. Entonces L_1 es libre, con una base $\{z_1,\dots,z_m\}$ tal que $m\le n$. Luego N es generado por $\{\varphi(z_1),\dots,\varphi(z_m)\}$. □

¿Cuál es la estructura de un A-módulo finitamente generado, sobre un anillo entero principal? Es posible reducir la cuestión a un procedimiento sobre matrices, que se llama reducción a la *forma normal de Smith*,[10] al aprovechar los resultados anteriores.

Sea A un anillo entero principal y sea M un A-módulo finitamente generado. Si M es generado por n elementos, hay un homomorfismo sobreyectivo $\varphi\colon A^n\to M$ (Proposición 1.42). Si $K:=\ker\varphi$, entonces $M\simeq A^n/K$ y K es un submódulo libre de rango $m\le n$. Denótese por $\{e_1,\dots,e_n\}$ la base estándar de A^n y sea $\{z_1,\dots,z_m\}$ una base de K. Al expresar cada z_i en términos de la base estándar de A^n, se obtiene un sistema de ecuaciones

$$\begin{aligned} z_1 &= c_{11}\,e_1 + c_{12}\,e_2 + \cdots + c_{1n}\,e_n,\\ z_2 &= c_{21}\,e_1 + c_{22}\,e_2 + \cdots + c_{2n}\,e_n,\\ &\vdots \qquad\qquad \vdots\\ z_m &= c_{m1}\,e_1 + c_{m2}\,e_2 + \cdots + c_{mn}\,e_n, \end{aligned} \tag{1.10}$$

donde los coeficientes c_{ij} son elementos de A.

Esta matriz $C\in M_{m,n}(A)$ depende de la elección de bases en K y A^n. De la demostración de la Proposición 1.43 (en su caso $m=n$), se sabe que cualquier cambio de base en un A-módulo libre de rango n utiliza una matriz *inversible* en $M_n(A)$. Concretamente, sea $\{y_1,\dots,y_m\}$ otra base de K y sea $\{u_1,\dots,u_n\}$ otra base de A^n. Entonces hay matrices $Q\in M_m(A)$ y $P\in M_n(A)$ tales que

$$u_s=\sum_{j=1}^{n} p_{sj}\,e_j, \qquad y_t=\sum_{i=1}^{m} q_{ti}\,z_i.$$

Si $R\in M_n(A)$ es la matriz inversa de P, entonces

$$y_t=\sum_{i=1}^{m}\sum_{j=1}^{n} q_{ti}c_{ij}\,e_j=\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{s=1}^{n} q_{ti}c_{ij}r_{js}\,u_s=:\sum_{s=1}^{n} b_{ts}\,u_s,$$

así que $C\mapsto B\in M_{m,n}(A)$, donde

$$B=QCP^{-1}.$$

En otras palabras, C y B son **matrices rectangulares equivalentes**, en el sentido de que se obtiene una de la otra y premultiplicar y postmultiplicar por matrices inversibles.

[10] Henry John Stephen Smith (1826–1883), matemático inglés, fue autor de varios trabajos sobre formas cuadráticas y teoría de números.

En el contexto conocido del álgebra lineal, cuando A sea un cuerpo $\mathbb{F}$, esta relación de *equivalencia de matrices* deja invariante el rango de la matriz rectangular C (el número máximo de columnas o filas linealmente independientes). Hay un algoritmo conocido en el cual se transforma C en una *forma escalonada* estándar, mediante ciertas operaciones de filas (construcción de Q) y de columnas (construcción de P^{-1}). Si el rango de la matriz C es k, el resultado final es una matriz B con $b_{11} = b_{22} = \cdots = b_{kk} = 1$ y cuyas demás entradas son ceros. Esto es posible porque cada elemento no nulo de $\mathbb{F}$ tiene un recíproco. Para un anillo entero principal que no sea un cuerpo ($A = \mathbb{Z}$, por ejemplo), la falta de divisibilidad conduce más bien a una matriz B que se llama la **forma normal de Smith** de la matriz original C.

Teorema 1.48 (Forma normal de Smith)**.** *Sea A un anillo entero principal y sea $C \in M_{m,n}(A)$ una matriz con entradas en A. Entonces C es equivalente a una matriz diagonal*[11] *de la forma*

$$D = \begin{pmatrix} d_1 & & \dots & 0 & & & \\ & d_2 & & & 0 & & 0 \\ & & \ddots & & & \ddots & \\ & & & d_r & & 0 & \\ & & & & 0 & & 0 \\ & 0 & & & & \ddots & \\ & & & & & 0 & \dots \quad 0 \end{pmatrix} =: \operatorname{diag}[d_1, d_2, \dots, d_r, 0, \dots, 0], \qquad (1.11)$$

donde $d_1, \dots, d_r \neq 0$ y $\underline{d_i \setminus d_j}$ para $i < j$.

Demostración. Para comprobar esta equivalencia de matrices, hay que recordar las *operaciones de fila* y las *operaciones de columna* del álgebra lineal. Las tres operaciones de fila elementales, con sus efecto sobre las filas $\boldsymbol{c}^1, \dots, \boldsymbol{c}^m$ de una matriz son las siguientes:

- multiplicar una fila por un elemento inversible, $\boldsymbol{c}^i \mapsto u\,\boldsymbol{c}^i$;
- sustraer de una fila un múltiplo de cualquier otra fila, $\boldsymbol{c}^i \mapsto \boldsymbol{c}^i - a\,\boldsymbol{c}^k$;
- intercambiar dos filas de la lista, $\boldsymbol{c}^i \leftrightarrow \boldsymbol{c}^k$.

Cada operación es reversible y se ejecuta al *premultiplicar* la matriz C por una matriz inversible $Q \in M_m(A)$, es decir, $C \mapsto QC$ en $M_{m,n}(A)$. Las operaciones de columna correspondientes son $\boldsymbol{c}_j \mapsto u\,\boldsymbol{c}_j$; $\boldsymbol{c}_j \mapsto \boldsymbol{c}_j - a\,\boldsymbol{c}_l$; y $\boldsymbol{c}_j \leftrightarrow \boldsymbol{c}_l$; cada una de ellas es reversible y se ejecuta al *postmultiplicar* la matriz C por una matriz inversible $P \in M_n(A)$, es decir, $C \mapsto CP$ en $M_{m,n}(A)$.

► Caso 1: si A es un anillo euclidiano.

Si $C = 0$, no hay más que hacer. Si $C \neq 0$, sea c_{ij} la entrada no nula de C tal que $\delta(c_{ij})$ sea mínimo. Después de efectuar las operaciones $\boldsymbol{c}^1 \leftrightarrow \boldsymbol{c}^i$ y $\boldsymbol{c}_1 \leftrightarrow \boldsymbol{c}_j$, se puede suponer que esta entrada es c_{11}.

[11] Se dice que una matriz rectangular B es *diagonal* si $b_{ij} = 0$ para $i \neq j$: las únicas entradas no nulas de B, si las hay, están en la "diagonal principal".

Ahora, para cada $i = 2, \ldots, m$, resulta que $c_{i1} = a_i c_{11} + r_{i1}$ con $r_{i1} = 0$ o bien $\delta(r_{i1}) < \delta(c_{11})$. Ejecútese las operaciones $\boldsymbol{c}^i \mapsto \boldsymbol{c}^i - a_i \boldsymbol{c}^1$ para $i = 2, \ldots, m$. Si cada $r_{i1} = 0$, entonces la primera columna de la matriz queda "limpia", es decir, con ceros debajo del "pivote" c_{11}. En el caso contrario, hay que elegir la fila i con $\delta(r_{i1})$ mínimo, hacer el intercambio $\boldsymbol{c}^1 \leftrightarrow \boldsymbol{c}^i$ que reemplaza c_{11} por r_{11}, y volver a limpiar la primera columna. Después de un número finito de iteraciones, quedan ceros debajo de la diagonal en la primera columna.

De igual modo, se proceda a limpiar la primera fila (para que hayan ceros a la derecha del nuevo pivote c_{11}) con operaciones de columna. Ya se puede suponer que C es de la forma

$$C = \begin{pmatrix} c_{11} & 0 & \ldots & 0 \\ 0 & c_{22} & \ldots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c_{2m} & \ldots & c_{mn} \end{pmatrix}, \tag{1.12}$$

con $\delta(c_{11}) \leq \delta(c_{rs})$ para cada entrada no nula c_{rs}. Si c_{11} no divide c_{rs}, la operación de columna $\boldsymbol{c}_1 \mapsto \boldsymbol{c}_1 + \boldsymbol{c}_s$ produce una primera columna nueva $(c_{11}, c_{2s}, \ldots, c_{ms})^t$. Después de limpiarla con operaciones de fila como antes, se obtiene una nueva entrada $c_{11} \neq 0$ con un menor valor de $\delta(c_{11})$. Al repetir este proceso un número finito de veces, se obtiene una nueva matriz de la forma (1.12) en donde $c_{11} \setminus c_{rs}$ para $r, s \geq 2$. En particular, vale $c_{11} \setminus c_{22}$.

En seguida, se aplica todo el proceso anterior para limpiar la segunda columna y la segunda fila. (Las operaciones apropiadas no afectarán las primeras fila y columna, ya limpias.) Al final de ese paso, se obtiene $c_{11} \setminus c_{22} \setminus c_{33}$ y además $c_{22} \setminus c_{rs}$ para todo $r, s \geq 3$.

Al continuar así, se llega a una matriz D de la forma (1.11). Debido a que todos los pasos del algoritmo son operaciones de fila o columna reversibles, se ve que $D = QCP$ para ciertas matrices inversibles Q, P.

► Caso 2: si A no es un anillo euclidiano.

En este caso, hay que la *longitud* $l(a)$ de una factorización en irreducibles en vez de $\delta(a)$, para $a \neq 0$ en A. (Véase la Definición 1.13.) Elíjase $c_{ij} \neq 0$ con $l(c_{ij})$ mínima y transfiérase c_{ij} a la posición $(1,1)$. Para simplificar la discusión, supóngase que $m = n = 2$ y que c_{11} no divide c_{21}. Sea d un máximo común divisor de c_{11} y c_{21}; fíjese que $l(d) < l(c_{11})$. Existen $p, q \in A$ tales que $c_{11}p + c_{21}q = d$. Sean $r := c_{11}/d$ y $s := c_{21}/d$. Entonces $(pr + qs)d = d$, y por ende $pr + qs = 1$ porque $d \neq 0$ y A es entero. Ahora[12]

$$\begin{pmatrix} p & q \\ s & -r \end{pmatrix} \begin{pmatrix} r & q \\ s & -p \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} p & q \\ s & -r \end{pmatrix} \begin{pmatrix} c_{11} & * \\ c_{21} & * \end{pmatrix} = \begin{pmatrix} d & * \\ 0 & * \end{pmatrix}.$$

En otras palabras, la matriz $Q := \begin{pmatrix} p & q \\ s & -r \end{pmatrix}$ es inversible y la premultiplicación por Q anula la entrada c_{12} y reemplaza c_{11} por un divisor no nulo con una entrada de menor longitud.

Se adapta este argumento al caso general al reemplazar este matriz Q por $Q \oplus 1_{m-2}$. Se limpia la primera columna con un número finito de premultiplicaciones de esta clase, y se limpia la primera fila con un número finito de postmultiplicaciones de matrices del estilo de $Q^t \oplus 1_{n-2}$. El resto del algoritmo procede como en el caso euclidiano. □

[12] Un asterisco en una matriz denota una entrada cuyo valor específico no tiene importancia para el cálculo.

Las entradas diagonales $(d_1,\dots,d_r,0,\dots,0)$ de la forma normal de Smith no quedan determinadas unívocamente, ya que siempre es posible premultiplicar (o postmultiplicar) D por una matriz diagonal con unidades de A en la diagonal, obteniendo así otra matriz equivalente D' de la forma (1.11). Sin embargo, esta falta de unicidad no es muy grave, ya que las nuevas entradas d_i' son *asociados* de los d_i originales. Esta es la misma falta de unicidad que hay en la definición de *un* máximo común divisor de dos o más elementos de A, que impide hablar de *el* máximo común divisor.[13]

Por otro lado, los *ideales* principales (d_1), (d_2), …, (d_r) no son ambiguos, ya que si $d_i' = u_i d_i$ para una unidad u_i si y sólo si $(d_i') = (d_i)$. La condición $d_i \setminus d_j$ para $i < j$ se traduce en $(d_i) \supseteq (d_j)$, así que estos ideales forman *una cadena descendiente*:

$$(d_1) \supseteq (d_2) \supseteq \cdots \supseteq (d_m), \quad \text{con } (d_j) = 0 \text{ para } j > r. \tag{1.13}$$

El próximo resultado dice que esta cadena caracteriza la clase de equivalencia de la matriz C.

Definición 1.49. Si $C \in M_{m,n}(A)$, con $m \le n$, donde A es un anillo entero principal, y si $k = 1,2,\dots,m$, sea $D_k(C) \in A$ un *máximo común divisor de todos los menores* $k \times k$ de la matriz C. Colóquese $D_0(C) := 1 \in A$. Los $D_k(C)$ se llaman **divisores elementales** de C; quedan determinadas hasta multiplicación por unidades de A.

Proposición 1.50. *Si $C \in M_{m,n}(A)$, con $m \le n$, donde A es un anillo entero principal, y sean $\{D_k(C) : k = 0,1,\dots,m\}$ sus divisores elementales.*[14] *Entonces $D_{k-1}(C) \setminus D_k(C)$ para $k = 1,\dots,m$; y la forma normal de Smith de C tiene las entradas diagonales no ceros*

$$d_1 = D_1(C), \quad d_2 = D_2(C)/D_1(C), \dots, \quad d_r = D_r(C)/D_{r-1}(C), \tag{1.14}$$

donde r es el mayor índice tal que $D_r(C) \neq 0$.

Demostración. Si $Q \in M_m(A)$, la fila i de QC es $\sum_{j=1}^m q_{ij}\,\boldsymbol{c}^j$, una combinación A-lineal de las filas $\boldsymbol{c}^j$ de C. Por tanto, los menores $k \times k$ de QC son combinaciones A-lineales de los menores de C. Luego, el máximo común divisor $D_k(QC)$ de estos menores de QC divide $D_k(C)$. Si Q es inversible, este argumento se revierte, de modo que $D_k(QC)$ divide $D_k(C)$; luego $D_k(QC)$ y $D_k(C)$ son asociados.

Si $P \in M_n(A)$, la columna j de CP es $\sum_{i=1}^n \boldsymbol{c}_i\, p_{ij}$, una combinación A-lineal de las columnas $\boldsymbol{c}_i$ de C. Luego, los menores $k \times k$ de CP son combinaciones A-lineales de los menores de C; luego $D_k(CP)$ divide $D_k(C)$, y estos elementos de A son asociados si P es inversible.

Se concluye que $D_k(B) = D_k(C)$ hasta múltiplos por unidades, si B y C son matrices equivalentes.

Es claro que los menores $k \times k$ no ceros de la forma normal de Smith (1.11) son determinantes de submatrices diagonales, $d_{i_1} d_{i_2} \dots d_{i_k}$. La condición $d_i \setminus d_j$ para $i < j$ impone que el máximo común divisor de entre ellos es $d_1 d_2 \dots d_k$ para $k \le r$, o bien 0 para $k > r$. Luego $D_k(C) = D_k(D) = d_1 d_2 \dots d_k$ para $k \le r$ y además $D_k(C) = 0$ para $k > r$, lo cual es equivalente a (1.14). □

[13] Por ejemplo, los enteros $-6, 9, -33 \in \mathbb{Z}$ tienen dos máximos comunes divisores, 3 y -3, que difieren por la unidad -1 de $\mathbb{Z}$. Ahora, en $\mathbb{Z}$ se puede agregar el requisito que el máximo común divisor sea *positivo*, en cuyo caso se puede escribir $\mathrm{mcd}(-6,9,-33) = 3$.

[14] Los $D_k(C)$, y por consiguiente los d_i, están determinadas hasta múltiplos por unidades de A.

Corolario 1.51. *Si A es un anillo entero principal, la cadena de ideales* (1.13) *depende únicamente de la clase de equivalencia de la matriz $C \in M_{m,n}(A)$. Estos ideales (d_j) se llaman los* ***factores invariantes*** *de la matriz C.*

En algunos anillos enteros principales, la ambigüedad en la definición de "máximo común divisor" puede removerse. Tal es el caso de $\mathbb{Z}$, en donde se pide que cualquier máximo común divisor sea positivo. (Las unidades de $\mathbb{Z}$ son 1 y -1.) También es el caso del anillo de *polinomios* $\mathbb{F}[t]$, cuyas unidades son las constantes no ceros. Se dice que

$$f(t) = a_0 + a_1 t + \cdots + a_n t^n \quad \text{es un polinomio } \textbf{mónico} \text{ si} \quad a_n = 1.$$

Al exigir que cada máximo común divisor de un juego de polinomios sea mónico, este queda determinado unívocamente.

Cuando $A = \mathbb{F}[t]$, entonces, se pide que la forma normal de Smith tenga entradas $d_i = d_i(t)$ que sean polinomios mónicos, y se llaman **factores invariantes** a estos polinomios $d_i(t)$, en vez de los ideales que generan.

► Con estos preparativos, se puede develar la estructura de un módulo finitamente generado sobre un anillo entero principal. Conviene introducir un poco más de terminología.

Definición 1.52. Un A-módulo M es **cíclico** si hay un solo elemento $x \in M$ tal que $M = Ax = \{\, ax : a \in A \,\}$.

El **anulador** de un elemento $y \in M$ es el ideal $I_y := \{\, b \in A : by = 0 \,\}$ de A. Si M es cíclico con generador x, la aplicación $a + I_x \mapsto ax$ define un isomorfismo de A-módulos $A/I_x \simeq M$. Un A-módulo cíclico $M = Ax \simeq A/I_x$ es libre, de rango 1, si y sólo si $\{x\}$ es una base de M, si y sólo si $I_x = 0$.

Definición 1.53. Si M es un A-módulo, un elemento $z \in M$ es un **elemento de torsión** si $a \in A$, $a \neq 0$, tal que $az = 0$ en M. Si todos los elementos de M son elementos de torsión, se dice que M es un **módulo de torsión**.

Si A es un anillo entero principal, el conjunto M_{tor} de elementos de torsión en M es un A-submódulo de M (¿por qué?), llamado el **submódulo de torsión** de M.

Teorema 1.54. *Sea A un anillo entero principal y sea M un A-módulo M finitamente generado. Entonces hay una cadena descendiente de ideales principales $(d_1) \supseteq (d_2) \supseteq \cdots \supseteq (d_n)$ [cuyos generadores cumplen $d_1 \setminus d_2 \setminus \cdots \setminus d_n$] tales que M sea isomorfo a una suma directa de A-módulos cíclicos:*

$$M \simeq A/(d_1) \oplus A/(d_2) \oplus \cdots \oplus A/(d_n). \tag{1.15}$$

Si r es el mayor índice tal que $d_r \neq 0$, entonces $M_{\text{tor}} \simeq A/(d_1) \oplus \cdots \oplus A/(d_r)$; además, si $r < n$, entonces $M \simeq M_{\text{tor}} \oplus A^{n-r}$.

Demostración. Por la Proposición 1.42, M es el cociente de un A-módulo libre: hay un $n \in N$ y un submódulo $K \subseteq A^n$ tales que $M \simeq A^n/K$. Por la Proposición 1.46 y el Corolario 1.47, K es un A-módulo libre y finitamente generado, de rango $m \leq n$. Los elementos de una base

de K pueden expresarse como combinaciones lineales de elementos de una base de A^n, como en (1.10). Por cambios de base en K y en A^n, se puede asumir que la matriz de coeficientes tenga la forma normal de Smith (1.11).

Entonces A^n posee una base $y_1,\dots,y_n$ y hay elementos $d_1,\dots,d_r \in A$, con $d_1 \setminus d_2 \setminus \cdots \setminus d_r$, tales que $\{d_1y_1,\dots,d_ry_r\}$ sea una base de K (obsérvese que en este caso, $r=m$ en la forma normal de Smith). Si $r<n$, defínase $d_j := 0$ para $j = r+1,\dots,n$. Entonces

$$M \simeq A^n/K \simeq \frac{Ay_1 \oplus \cdots \oplus Ay_n}{Ad_1y_1 \oplus \cdots \oplus Ad_ny_n}. \tag{1.16a}$$

Considérese el homomorfismo

$$\psi : \bigoplus_{j=1}^{n} Ay_j \longrightarrow \bigoplus_{j=1}^{n} \frac{Ay_j}{Ad_jy_j} : a_1y_1+\cdots+a_ny_n \longmapsto (a_1y_1+Ad_1y_1)+\cdots+(a_ny_n+Ad_ny_n).$$

Este ψ es sobreyectivo y su núcleo es el submódulo $Ad_1y_1 \oplus \cdots \oplus Ad_ny_n$. Al aplicar la Proposición 1.30, el isomorfismo (1.16a) se convierte en otro:

$$M \simeq A^n/K \simeq \frac{Ay_1}{Ad_1y_1} \oplus \cdots \oplus \frac{Ay_n}{Ad_ny_n}. \tag{1.16b}$$

El homomorfismo $\varphi_j\colon A \to Ay_j/Ad_jy_j$ dado por $\varphi_j(a) := ay_j + Ad_jy_j$ tiene núcleo (d_j). Luego φ_j induce un isomorfismo $A/(d_j) \simeq Ay_j/Ad_jy_j$. Al combinar estos isomorfismos con (1.16b), se obtiene la conclusión (1.15).

La cadena descendiente de ideales (d_j) puede terminar con algunos ideales nulos: esto es el caso si hay $r<n$ con $(d_r)\neq 0$ pero $(d_j)=0$ para $j=r+1,\dots,n$. En ese caso, los últimos $n-r$ sumandos de (1.15) forman un submódulo libre: $A\oplus\cdots\oplus A \simeq A^{n-r}$.

Si $x\in M$ es un elemento de torsión, entonces $x = x_1+\cdots+x_n$, donde $x_j \in M_j \simeq A/(d_j)$, así que $d_1\dots d_rx = d_1\dots d_r(x_{r+1}+\cdots+x_n) = 0$ si y sólo si $x_{r+1}\cdots x_n = 0$. Por tanto, el submódulo de torsión de M es $M_{\text{tor}} = M_1\oplus\cdots\oplus M_r \simeq A/(d_1)\oplus\cdots\oplus A/(d_r)$. □

En la demostración anterior, no se excluye que algunos de los d_j sean *unidades* del anillo A, en cuyo caso $(d_j)=A$ y $A/(d_j)=0$. Como los ideales (d_j) forman una cadena descendiente, esto significa que la sucesión $d_1,\dots,d_n$ puede empezar con algunos unidades: sería $(d_j)=A$ para $j=1,\dots,k$ y por tanto $M\simeq A/(d_{k+1})\oplus\cdots\oplus A/(d_n)$. En última instancia, es posible rehacer el argumento al reemplazar A^n por A^{n-k} con base $\{y_{k+1},\dots,y_n\}$, para eliminar redundancias.

Ejemplo 1.55. Sea G un grupo abeliano finitamente generado. Entonces hay $n\in\mathbb{N}$ y enteros positivos $m_1,\dots,m_r\in\mathbb{N}$ para algún $r\leq n$ tales que[15]

$$G \simeq \mathbb{Z}/m_1 \oplus \mathbb{Z}/m_2 \oplus \cdots \oplus \mathbb{Z}/m_r \oplus \cdots \oplus \mathbb{Z}^{n-r}. \tag{1.17}$$

y además vale $m_1 \setminus m_2 \setminus \cdots \setminus m_r$.

[15] Aquí se emplea el convenio de notación $\mathbb{Z}/m := \mathbb{Z}/m\mathbb{Z}$.

En efecto, un grupo abeliano es un $\mathbb{Z}$-módulo y $\mathbb{Z}$ es un anillo entero principal, de modo que el Teorema 1.54 es aplicable al caso. Cada ideal no nulo de $\mathbb{Z}$ es de la forma $(d_j) = m_j\mathbb{Z}$, donde $m_j := |d_j|$ es positivo; entonces $\mathbb{Z}/(d_j) = \mathbb{Z}/m_j$.

Se ve que G es la suma directa de un grupo abeliano libre $\mathbb{Z}^{n-r}$ y su subgrupo de torsión $\mathbb{Z}/m_1 \oplus \cdots \oplus \mathbb{Z}/m_r$.

Un grupo abeliano es cíclico si posee un solo generador. Entonces o bien es $G \simeq \mathbb{Z}$ (grupo cíclico infinito) en el caso libre, o bien $G \simeq \mathbb{Z}/m$ para algún $m \in \mathbb{N}$ con $m \geq 2$.

Ejemplo 1.56. Un grupo abeliano finito es de la forma $G \simeq \mathbb{Z}/m_1 \oplus \mathbb{Z}/m_2 \oplus \cdots \oplus \mathbb{Z}/m_r$, ya que no puede tener sumandos infinitos. El *orden* del grupo es $|G| = m_1 m_2 \ldots m_r$. Dado un grupo abeliano finito de orden n, su clase de isomorfismo es determinado por las factorizaciones $n = m_1 m_2 \ldots m_r$ que cumplen $m_1 \setminus m_2 \setminus \cdots \setminus m_r$.

Si $n = 24$, por ejemplo, las únicas posibilidades son 24 solo, $2 \setminus 12$, ó $2 \setminus 2 \setminus 6$. Luego los grupos abelianos de orden 24 son

$$\mathbb{Z}/24, \qquad \mathbb{Z}/2 \oplus \mathbb{Z}/12, \qquad \mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/6.$$

Obsérvese que $\mathbb{Z}/3 \oplus \mathbb{Z}/8 \simeq \mathbb{Z}/24$, mientras $\mathbb{Z}/4 \oplus \mathbb{Z}/6 \simeq \mathbb{Z}/2 \oplus \mathbb{Z}/12$ (¿por qué?).

1.5 Clasificación de transformaciones lineales

La estructura de los módulos sobre anillos enteros principales tiene una aplicación inmediata en el álgebra lineal tradicional. Hay dos relaciones importantes que pueden usarse para clasificar aplicaciones lineales o matrices: *equivalencia y semejanza*. Dos aplicaciones lineales $S, T \in \mathrm{Hom}_{\mathbb{F}}(V, W)$ de un espacio vectorial en otro son **equivalentes** si poseen una misma matriz A, aunque sea con respecto a bases diferentes de V y de W. Dos matrices rectangulares $A, B \in M_{m,n}(\mathbb{F})$ son equivalentes si $B = QAP$ donde $Q \in M_m(\mathbb{F})$ y $P \in M_n(\mathbb{F})$ son matrices inversibles. Se sabe que dos aplicaciones lineales (o dos matrices) son equivalentes si y sólo si poseen el mismo *rango*.[16] Entonces el rango es un *invariante* que determina las clases de equivalencia, sea en $\mathrm{Hom}_{\mathbb{F}}(V, W)$ o bien en $M_{m,n}(\mathbb{F})$.

Para clasificar *operadores lineales* $T \in \mathrm{End}_{\mathbb{F}}(V)$ de un espacio vectorial V, o bien para clasificar *matrices cuadradas* $A \in M_n(\mathbb{F})$, se dispone de una relación más fina, la de semejanza. Dos operadores lineales $T \in \mathrm{End}_{\mathbb{F}}(V)$ y $S \in \mathrm{End}_{\mathbb{F}}(W)$ son **semejantes** si existe una aplicación inversible $R \in \mathrm{Hom}_{\mathbb{F}}(V, W)$ tal que $S = RTR^{-1}$. Dos matrices cuadradas $A, B \in M_n(\mathbb{F})$ son semejantes si $B = PAP^{-1}$ donde $P \in M_n(\mathbb{F})$ es una matriz inversible. Un invariante bajo semejanza que es bien conocido es el **polinomio característico**,

$$p_T(t) := \det(t\,1_V - T), \qquad p_A(t) := \det(t\,1_n - A).$$

De hecho, es evidente que $p_B(t) = p_A(t)$ si $B = PAP^{-1}$ y luego $p_T(t) = p_A(t)$ si A es la matriz de T con respecto a una base cualquiera de V. Pero este invariante *no es clasificante*:

[16] El rango de una aplicación lineal $T \in \mathrm{Hom}_{\mathbb{F}}(V, W)$ es la dimensión $r(T)$ de su imagen $T(V)$. El rango de una matriz A es el número máximo $r(A)$ de columnas linealmente independientes de A. Si A es la matriz de T con respecto de un par de bases para V y W, se sabe que $r(A) = r(T)$.

es fácil producir ejemplos de dos matrices con el mismo polinomio característico que no son semejantes.

Se busca, entonces, una *familia de invariantes* de un operador lineal, o bien de una matriz cuadrada, que efectúa esta clasificación hasta semejanza. Resulta que se trata de un conjunto finito de polinomios, en vez de uno solo; y que la manera más eficiente de exhibir este conjunto de polinomios emplea la teoría de módulos sobre anillos enteros principales.

Definición 1.57. Sea V un espacio vectorial *finitodimensional* sobre un cuerpo $\mathbb{F}$, y sea $T \in \mathrm{End}_{\mathbb{F}}(V)$ un operador lineal sobre V. Como ya se expuso en el Ejemplo 1.25, V es un módulo para el anillo de polinomios $\mathbb{F}[t]$, mediante (1.1):

$$\underline{f(t)\cdot v} := f(T)(v) \quad \text{para todo} \quad v \in V.$$

Ahora $\mathbb{F}[t]$ es un anillo entero principal, así que le Teorema 1.54 es aplicable: V es la suma directa de un número finito de submódulos cíclicos.

Teorema 1.58. *Sea V un espacio vectorial finitodimensional sobre $\mathbb{F}$. El $\mathbb{F}[t]$-módulo V determinado por un operador lineal $T \in \mathrm{End}_{\mathbb{F}}(V)$ es un módulo de torsión, cuyos **factores invariantes** son polinomios mónicos*

$$d_1(t) \setminus d_2(t) \setminus \cdots \setminus d_n(t),$$

*donde $d_n(t)$ es el **polinomio mínimo** de T; además, el producto $d_1(t)\,d_2(t)\ldots d_n(t)$ es el **polinomio característico** $p_T(t)$ de T.*

Demostración. La dimensión $n := \dim_{\mathbb{F}} V$ es finito, pero $\dim_{\mathbb{F}} \mathbb{F}[t]$ es infinito: luego, esta descomposición no puede contener un sumando libre. Por tanto, V es un $\mathbb{F}[t]$-módulo de torsión.

Sea $\{v_1,\ldots,v_n\}$ una base de V y sea $A = [a_{ij}]$ la matriz de T con respecto a esta base, dada explícitamente por la fórmula

$$T(v_j) =: \sum_{i=1}^{n} a_{ij}\, v_i, \quad \text{para} \quad j = 1,\ldots,n.$$

Para poder aplicar el Teorema 1.54, hay que expresar V como un cociente de $\mathbb{F}[t]$-módulos libres M/K. Tómese $M = \mathbb{F}[t]^n$ y sea $\{e_1,\ldots,e_n\}$ una base estándar de $\mathbb{F}[t]^n$ como módulo libre sobre $\mathbb{F}[t]$. Sea $\eta\colon \mathbb{F}[t]^n \to V$ la aplicación cociente determinado por $\eta(e_j) := v_j$ para $j = 1,\ldots,n$. Ahora η es por definición un $\mathbb{F}[t]$-homomorfismo, así que vale $\eta(f(t)\,e_j) = f(T)(v_j)$ para todo $f(t) \in \mathbb{F}[t]$. Sea $K := \ker\eta$. Fíjese que

$$\eta\left(t\,e_j - \sum_{i=1}^{n} a_{ij}\,e_i\right) = T(v_j) - \sum_{i=1}^{n} a_{ij}\,v_i = 0,$$

y por ende cada combinación $\mathbb{F}[t]$-lineal de la forma

$$z_j := t\,e_j - \sum_{i=1}^{n} a_{ij}\,e_i \tag{1.18}$$

es un elemento de K.

Afirmación:[17] el conjunto $\{z_1,\ldots,z_n\}$ es una base de K. Para comprobarlo, hay que mostrar que los z_j generan K y que son $\mathbb{F}[t]$-linealmente independientes.

Cada $x\in\mathbb{F}[t]^n$ se expresa como $x=\sum_{j=1}^n h_j(t)\,e_j$. Al usar repetidamente las sustituciones $t\,e_j=z_j+\sum_{i=1}^n a_{ij}\,e_i$, se obtiene

$$x=\sum_{i=1}^n b_i\,e_i+\sum_{j=1}^n g_j(t)\,z_j$$

para ciertos polinomios $g_j(t)$ y escalares $b_i\in\mathbb{F}$. Ahora $\eta(x)=\sum_{i=1}^n b_i\,\eta(e_i)=\sum_{i=1}^n b_i\,v_i$. Luego $x\in K$ si y sólo si $\eta(x)=0$, si y sólo si $b_1=\cdots=b_n=0$ en $\mathbb{F}$, si y sólo si $x\in\mathbb{F}[t]\langle z_1,\ldots,z_n\rangle$. En otras palabras, K es generado por $\{z_1,\ldots,z_n\}$.

Por otro lado, si $\sum_{j=1}^n g_j(t)\,z_j=0$, entonces $\sum_{j=1}^n t\,g_j(t)\,e_j=\sum_{i,j=1}^n a_{ij}\,g_j(t)\,e_i$, lo cual implica que

$$t\,g_k(t)=\sum_{j=1}^n a_{kj}\,g_j(t)\quad\text{para cada}\quad k=1,\ldots,n.$$

Si esta relación no es trivial y si $g_k(t)$ es el polinomio de mayor grado en $\{g_1(t),\ldots,g_n(t)\}$, esta relación es absurda porque el lado izquierdo tiene mayor grado que el lado derecho: la única salida es que $g_1(t)=\cdots=g_n(t)=0$ en $\mathbb{F}[t]$. Luego, $\{z_1,\ldots,z_n\}$ es una base de K.

Al comparar las expresiones (1.18) con la fórmula (1.10), se ve que la matriz C que relaciona las bases de K y de $\mathbb{F}[t]^n$ es $C=t\,1_n-A$. (Fíjese que $m=n$ en el caso actual.) Por el Teorema 1.48, hay matrices *inversibles* $P(t),Q(t)\in M_n(\mathbb{F}[t])$ tales que

$$Q(t)\,(t\,1_n-A)\,P(t)^{-1}=\operatorname{diag}[d_1(t),d_2(t),\ldots,d_n(t)],\tag{1.19}$$

donde cada $d_j(t)$ es un polinomio mónico en $\mathbb{F}[t]$, con $d_1(t)\setminus d_2(t)\setminus\cdots\setminus d_n(t)$.

Si los primeros k factores invariantes son de grado cero (es decir, $d_1(t)=\cdots=d_k(t)=1$), entonces la descomposición de V como $\mathbb{F}[t]$-módulo es

$$V\simeq\mathbb{F}[t]/(d_{k+1}(t))\oplus\cdots\oplus\mathbb{F}[t]/(d_n(t)).$$

Cada $v\in V$ es una suma $v=w_{k+1}+\cdots+w_n$, donde $d_j(T)(w_j)=d_j(t)\cdot w_j=0$ para cada j. Además, como $d_j(t)\setminus d_n(t)$, se obtiene $d_n(T)(v)=0$ para v arbitrario, por tanto $d_n(T)=0$ en $\operatorname{End}_{\mathbb{F}}(V)$. Si w_n es un generador para el módulo cíclico $\mathbb{F}[t]/(d_n(t))$, y si $g(t)\in\mathbb{F}[t]$ es un polinomio tal que $g(T)=0$, entonces $g(t)\cdot w_n=0$, lo cual implica que $g(t)\in(d_n(t))$, o lo que es lo mismo, que $d_n(t)\setminus g(t)$. Esto dice que $d_n(t)$ es el polinomio mínimo de T.

Para identificar el polinomio característico, sólo hay que evaluar los determinantes —en el anillo $M_n(\mathbb{F}[t])$— de ambos lados de (1.19). Obsérvese que $(\det Q(t))$ y $(\det P(t))$ son *polinomios inversibles* en $\mathbb{F}[t]$, es decir, constantes no nulos. Luego hay $c_0\neq 0$ en $\mathbb{F}$ tal que

$$p_T(t)=p_A(t):=\det(t\,1_n-A)=c_0\,d_1(t)\,d_2(t)\ldots d_n(t).$$

[17] Obsérvese que $\mathbb{F}[t]$-módulo libre puede tener un submódulo libre propio del mismo rango, en contraste de lo que ocurre con espacios vectoriales, en donde un subespacio propio tiene menor dimensión que un espacio vectorial que lo incluye.

Pero $\det(t\,1_n - A)$ y cada $d_j(t)$ son polinomios mónicos: al comparar los coeficientes de t^n, se ve que $c_0 = 1$ y por ende $p_T(t) = d_1(t)\,d_2(t)\ldots d_n(t)$. □

Corolario 1.59. *Si $T \in \mathrm{End}_{\mathbb{F}}(V)$ es un operador lineal, cada factor irreducible de su polinomio característico $p_T(t)$ es también un factor de su polinomio mínimo $q_T(t)$.* ⊟

Ejemplo 1.60. Para calcular los factores invariantes de una matriz $A \in M_n(\mathbb{F})$, los cuales por definición los factores invariantes del operador $x \mapsto Ax$, $x \in \mathbb{F}^n$, se aprovecha los *divisores elementales* $D_k(t)$ de la matriz $t\,1_n - A \in M_n(\mathbb{F}[t])$; la fórmula (1.14) proporciona los $d_j(t)$. Por ejemplo, considérese las matrices[18]

$$A := \begin{pmatrix} 3 & 1 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 \end{pmatrix}, \qquad t\,1_6 - A = \begin{pmatrix} t-3 & -1 & & & & \\ & t-3 & & & & \\ & & t-3 & & & \\ & & & t-4 & & \\ & & & & t-4 & \\ & & & & & t-5 \end{pmatrix}.$$

Los divisores elementales de la matriz $t\,1_6 - A$ son

$$\begin{aligned} &D_1(t) = D_2(t) = D_3(t) = D_4(t) = 1, \\ &D_5(t) = (t-3)(t-4), \\ &D_6(t) = p_A(t) = (t-3)^3(t-4)^2(t-5). \end{aligned}$$

De ahí se obtiene

$$\begin{aligned} &d_1(t) = d_2(t) = d_3(t) = d_4(t) = 1, \\ &d_5(t) = (t-3)(t-4), \\ &d_6(t) = q_A(t) = (t-3)^2(t-4)(t-5). \end{aligned}$$

Fíjese que A tiene la *forma normal de Jordan*.

Sea B la matriz *diagonal* obtenida al cambiar $a_{12} = 1$ a $b_{12} = 0$, con $b_{ij} = a_{ij}$ para las otras entradas. Los divisores elementales de $t\,1_6 - B$ son

$$\begin{aligned} &D_1(t) = D_2(t) = D_3(t) = 1, \\ &D_4(t) = (t-3), \qquad D_5(t) = (t-3)^2(t-4), \\ &D_6(t) = p_B(t) = (t-3)^3(t-4)^2(t-5). \end{aligned}$$

Los factores invariantes de B son

$$\begin{aligned} &d_1(t) = d_2(t) = d_3(t) = 1, \\ &d_4(t) = (t-3), \qquad d_5(t) = (t-3)(t-4), \\ &d_6(t) = q_B(t) = (t-3)(t-4)(t-5). \end{aligned}$$

El siguiente Teorema comprueba algo que en este ejemplo es evidente, a saber, que las matrices A y B no son semejantes.

[18] En el despliegue de la matriz $t\,1_6 - A$, se usa el convenio de que una entrada en blanco es un cero.

Teorema 1.61. *Dos operadores lineales $T \in \mathrm{End}_{\mathbb{F}}(V)$ y $S \in \mathrm{End}_{\mathbb{F}}(W)$ son semejantes si y sólo si poseen los mismos factores invariantes.*

Demostración. Los operadores S y T son semejantes si y sólo si hay bases $\{v_1, \ldots, v_n\}$ de V y $\{w_1, \ldots, w_n\}$ de W tales que

$$S(w_j) = \sum_{i=1}^{n} a_{ij}\, w_i, \qquad T(v_j) = \sum_{i=1}^{n} a_{ij}\, v_i, \quad \text{para} \quad j = 1, \ldots, n,$$

con la misma matriz $A = [a_{ij}]$. La aplicación lineal $R\colon V \to W$ dado por $R(v_j) =: w_j$ es inversible, con $S = RTR^{-1}$.

Si S y T son semejantes, entonces en la demostración del Teorema 1.58 se puede usar la base $\{w_1, \ldots, w_n\}$ de W y el operador S en vez de la base $\{v_1, \ldots, v_n\}$ de V y el operador T. De este modo, se llega a la misma matriz de relaciones $C = t\,1_n - A$ y por tanto a los mismos factores invariantes $d_1(t), \ldots, d_n(t)$.

Para la dirección inversa, es suficiente tomar $V = \mathbb{F}^n$ y $T = T_A$ donde el operador lineal $T_A \in \mathrm{End}_{\mathbb{F}}(\mathbb{F}^n)$ es definido por $T_A(x) := Ax$, ya que cualquier operador en $\mathrm{End}_{\mathbb{F}}(V)$ es semejante a algún T_A si $n = \dim_{\mathbb{F}} V$. En adelante se comprobará que T_A es semejante a cierto operador que depende únicamente de sus factores invariantes.

Si $d(t) \in \mathbb{F}[t]$ es un polinomio mónico de grado m, el cociente $W_d := \mathbb{F}[t]/(d(t))$ es un espacio vectorial sobre $\mathbb{F}$, cuya dimensión es m. En efecto, si $f(t) \in \mathbb{F}[t]$, entonces $f(t) = q(t)\,d(t) + r(t)$ por división de polinomios, donde $r(t) = 0$ o bien $r(t)$ es un polinomio de grado menor que m. Cada coclase en $\mathbb{F}[t]/(d(t))$ tiene un representante $\overline{r(t)} := r(t) + (d(t))$, con $r(t) = c_0 + c_1 t + \cdots + c_{m-1} t^{m-1}$. Luego $\{\bar{t}^k : k = 0, 1, \ldots, m-1\}$ es una base de W_d. Considérese el operador lineal $S_d \in \mathrm{End}_{\mathbb{F}}(W_d)$ dado por

$$S_d\big(\overline{r(t)}\big) := \overline{t\,r(t)}. \tag{1.20}$$

Más generalmente, si $d_1(t), \ldots, d_n(t)$ son polinomios mónicos en $\mathbb{F}[t]$, sea $S_{d_1,\ldots,d_n}$ el operador lineal sobre $W = W_{d_1} \oplus \cdots \oplus W_{d_n}$ dado por

$$S_{d_1,\ldots,d_n}\big(\overline{r_1(t)}, \ldots, \overline{r_n(t)}\big) := \big(\overline{t\,r_1(t)}, \ldots, \overline{t\,r_n(t)}\big).$$

Dada una matriz $A \in M_n(\mathbb{F})$, sean $d_1(t), \ldots, d_n(t)$ los factores invariantes del operador T_A. Sea $\eta\colon \mathbb{F}[t]^n \to W$ el homomorfismo cociente; su núcleo es $\ker \eta = D(t)\,\mathbb{F}[t]^n$, donde $D(t) := \mathrm{diag}[d_1(t), \ldots, d_n(t)]$ es la matriz diagonal al lado derecho de (1.19). La demostración del Teorema 1.58 muestra que hay matrices inversibles $Q(t), P(t) \in M_n(\mathbb{F}[t])$ que cumplen

$$Q(t)\,(t\,1_n - A) = D(t)\,P(t) \quad \text{y} \quad (t\,1_n - A)\,P(t)^{-1} = Q(t)^{-1}\,D(t). \tag{1.21}$$

Sean $\zeta_A\colon \mathbb{F}[t]^n \to \mathbb{F}^n$ y $R\colon \mathbb{F}^n \to W$ las aplicaciones $\mathbb{F}$-lineales dados por

$$\zeta_A\big(f(t)\,x\big) := f(A)\,x, \qquad R(x) := \eta\big(Q(t)\,x\big), \quad \text{para} \quad x \in \mathbb{F}^n.$$

Entonces $\ker \zeta_A = (t\,1_n - A)\,\mathbb{F}[t]^n$ y las fórmulas (1.21) implican que $Q(t)\big(\ker \zeta_A\big) = \ker \eta$. Esto implica que R es inyectivo, porque

$$R(x) = 0 \implies Q(t)\,x \in \ker \eta \implies x \in \mathbb{F}^n \cap \ker \zeta_A \implies x = 0,$$

y además R es sobreyectivo porque

$$\dim_{\mathbb{F}} W = \dim_{\mathbb{F}}(W_{d_1} \oplus \cdots \oplus W_{d_n}) = \sum_{j=1}^{n} \operatorname{gr} d_j(t) = \operatorname{gr}\big(d_1(t)\ldots d_n(t)\big) = \operatorname{gr}(p_A(t)) = n.$$

Por tanto, $R \in \operatorname{Hom}_{\mathbb{F}}(\mathbb{F}^n, W)$ es un isomorfismo lineal.

Si $x \in \mathbb{F}^n$, entonces $tx - Ax \in \ker \zeta_A$. En vista de que $Q(t)\big(\ker \zeta_A\big) = \ker \eta$, se obtiene

$$R(Ax) = \eta\big(Q(t)Ax\big) = \eta\big(Q(t)tx\big) = \eta\big(t\,Q(t)x\big) = S_{d_1,\ldots,d_n}(R(x)) \quad \text{para todo} \quad x \in \mathbb{F}^n,$$

por la definición de $S_{d_1,\ldots,d_n}$. En otras palabras, $RT_A = S_{d_1,\ldots,d_n} R$, así que $RT_AR^{-1} = S_{d_1,\ldots,d_n}$. Por lo tanto, los operadores T_A y $S_{d_1,\ldots,d_n}$ son semejantes. □

Corolario 1.62. *Dos matrices cuadradas $A, B \in M_n(\mathbb{F})$ son semejantes si y sólo si poseen los mismos factores invariantes.* ⊟

1.6 Ejercicios sobre anillos y módulos

Ejercicio 1.1. (a) Demostrar que $\mathbb{Z}/6$ es un anillo principal que no es entero.

(b) Si $\mathbb{F}$ es un cuerpo, el anillo $\mathbb{F}[t_1,t_2]$ es entero pero no es principal. Comprobar esta última afirmación al verificar en detalle que el ideal (t_1,t_2) de $\mathbb{F}[t_1,t_2]$ no puede ser generado por un sólo polinomio en los dos indeterminados t_1,t_2.

Ejercicio 1.2. Un anillo A se llama **anillo booleano** si $a^2 = a$ para todo elemento $a \in A$. Demostrar que $2a = 0$ para cada $a \in A$; y que A es conmutativo. Dar un ejemplo de un anillo booleano con 8 elementos.

⟦ Indicación: Calcular $(a+a)^2$ y $(a+b)^2$ para $a,b \in A$. ⟧

Ejercicio 1.3. Un A-módulo M se llama **simple** o **irreducible** si no posee A-submódulos salvo M y 0. Un A-módulo se llama **semisimple** si es una suma directa de A-submódulos simples. Si $m \in \mathbb{N}^*$, demostrar que el anillo $\mathbb{Z}/m$ es semisimple (como $\mathbb{Z}/m$-módulo a la izquierda) si y sólo si m es el producto de números primos distintos.

Ejercicio 1.4. (a) Un A-módulo M es **cíclico** si es generado por un solo elemento x, es decir, si $M = Ax = \{\, ax : a \in A \,\}$. Si J es un ideal de A, demostrar que el A-módulo A/J es cíclico.

(b) Mostrar que M es irreducible si y sólo si M es cíclico y cada elemento no cero es un generador de M.

(c) [*Lema de Schur*]: Si M y M' son dos A-módulos irreducibles, mostrar que cada elemento no nulo $\varphi \in \operatorname{Hom}_A(M,M')$ es un isomorfismo. ⟦ Indicación: Usar la descomposición canónica de φ. ⟧ Concluir que $\operatorname{End}_A(M)$ es un *anillo de división*[19] si M es irreducible.

[19] Un *anillo de división* es un anillo D, no necesariamente conmutativo, en donde cada elemento no nulo es inversible. Cualquier cuerpo es un anillo de division. El anillo $\mathbb{H}$ de **cuaterniones** reales es un anillo de división no conmutativo.

Ejercicio 1.5. (a) Una **representación** de un grupo finito G sobre un espacio $\mathbb{F}$-vectorial V es un homomorfismo de grupos $\rho : G \to GL(V)$, donde $GL(V)$ es el grupo de automorfismos lineales de V. Mostrar que esta representación hace de V un módulo sobre el anillo $\mathbb{F}[G]$.

(b) Si H es un subgrupo de G, demostrar que $\mathbb{F}[G]$ es un módulo *libre* sobre el anillo $\mathbb{F}[H]$.

Ejercicio 1.6. Sea M un A-módulo y sean $M_1, M_2, \ldots, M_n$ una colección finita de submódulos de M tales que

(a) $M_1 + M_2 + \cdots + M_n = M$; y

(b) $M_j \cap (M_1 + \cdots + M_{j-1} + M_{j+1} + \cdots + M_n) = 0$ para cada $j = 1, \ldots, n$.

Demostrar que $M \simeq M_1 \oplus M_2 \oplus \cdots \oplus M_n$.

Ejercicio 1.7. Una matriz cuadrada $R \in M_n(\mathbb{Z})$ se llama **unimodular** si $\det R = \pm 1$. Mostrar en detalle que R es inversible en el anillo $M_n(\mathbb{Z})$ si y sólo si R es unimodular.

Ejercicio 1.8. Sea A un anillo, no necesariamente conmutativo, y sea M un A-módulo libre con una base de n elementos. Mostrar que hay un isomorfismo de anillos $\mathrm{End}_A(M) \simeq M_n(A^\circ)$.

Ejercicio 1.9. (a) Transformar la siguiente matriz $C \in M_3(\mathbb{Z})$ a D, su forma normal de Smith:

$$C = \begin{pmatrix} -2 & 3 & 0 \\ -3 & 3 & 0 \\ -12 & 12 & 6 \end{pmatrix}.$$

(b) Obtener matrices inversibles $Q, P \in M_3(\mathbb{Z})$ tales que $D = QCP^{-1}$.

Ejercicio 1.10. Si A es un anillo entero principal y si $C \in M_{m,n}(A)$ es una matriz rectangular con $m \leq n$, demostrar que C y su transpuesta $C^t \in M_{n,m}(A)$ tienen los mismos factores invariantes $d_1, \ldots, d_m$.

Ejercicio 1.11. Para $a \in A$ y $k \geq 2$, sea $J_k(a) \in M_k(A)$ el **bloque de Jordan** con entrada diagonal a, es decir,

$$J_k(a) := \begin{pmatrix} a & 1 & & & \\ & a & 1 & & 0 \\ & & a & \ddots & \\ & & & \ddots & 1 \\ & 0 & & & a & 1 \\ & & & & & a \end{pmatrix}.$$

(a) Calcular los divisores elementales D_k y los factores invariantes d_j de la matriz $J_k(a)$.

(b) Calcular los divisores elementales y los factores invariantes de la matriz $J_k(a) \oplus J_l(b)$, suma directa de dos bloques de Jordan.

Ejercicio 1.12. Comprobar los isomorfismos de grupos abelianos $\mathbb{Z}/3 \oplus \mathbb{Z}/8 \simeq \mathbb{Z}/24$ y además $\mathbb{Z}/4 \oplus \mathbb{Z}/6 \simeq \mathbb{Z}/2 \oplus \mathbb{Z}/12$.

Ejercicio 1.13. Clasificar todos los grupos abelianos de orden 400.

Ejercicio 1.14. Demostrar que las siguientes matrices R y S ("clock and shift"):

$$R = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -i \end{pmatrix}, \qquad S = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

son semejantes en $M_4(\mathbb{Z}[i])$, donde $i = \sqrt{-1}$.

2 Elementos de la Teoría de Categorías

En el primer capítulo, los módulos sobre un anillo fueron introducidos y en un caso particular (módulos finitamente generados sobre un anillo entero principal) fueron clasificados hasta isomorfismo. Sin embargo, la tarea de describir y clasificar módulos individuales no puede ir demasiado lejos. Lo que hace del estudio de los módulos una teoría interesante e útil son las relaciones entre varios módulos, mediados por homomorfismos. Históricamente, la utilidad de los módulos (en especial, los grupos abelianos finitamente generados) fue realizado en ciertos problemas de topología, cuando se logró asociar a los espacios topológicos una serie de grupos y módulos interesantes.

Para esclarecer la esencia de los procedimientos algebraicos empleados en topología en la primera mitad del siglo XX, Eilenberg y MacLane postularon una esquema general de procedimiento, que ha adquirido el nombre de "teoría de categorías".[1] Luego fue percibido que ese enfoque es una clave para simplificar y extender la llamada geometría algebraica, principalmente por medio de los trabajos de Grothendieck en los años sesentas. Hoy en día, se ha convertido en un lenguaje obligatorio para formular y discutir la matemática moderna. En este capítulo se introducirán los conceptos básicos de categoría y funtor, para poder aplicarlos al estudio de los módulos en los capítulos posteriores.

2.1 Definición y ejemplos de categorías

La notación para las categorías no ha sido estandarizada todavía: los textos principales presentan diversos variantes.[2] En este curso, las categorías serán identificadas por una letra sanserif: tales como Ab, An, A-Mod, Top. Todos los ceros serán denotados por el dígito 0 y todas las aplicaciones idénticas por el dígito 1, salvo mención explícito de lo contrario.

Definición 2.1. Una **categoría** C reúne tres cosas:

1. Una clase de **objetos** $\underline{\mathrm{Ob}(\mathsf{C})}$;

2. una familia de conjuntos $\underline{\mathrm{Hom}_{\mathsf{C}}(A,B)}$, uno para cada par de objetos $A,B \in \mathrm{Ob}(\mathsf{C})$; los elementos de $\mathrm{Hom}_{\mathsf{C}}(A,B)$ se llaman **morfismos** de A en B;

3. una familia de aplicaciones

$$\mathrm{Hom}_{\mathsf{C}}(A,B) \times \mathrm{Hom}_{\mathsf{C}}(B,C) \to \mathrm{Hom}_{\mathsf{C}}(A,C),$$

llamada **composición** de morfismos, para cada triplete de objetos $A,B,C \in \mathrm{Ob}(\mathsf{C})$; la composición de $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$ y $g \in \mathrm{Hom}_{\mathsf{C}}(B,C)$ se denota por $\underline{gf} \in \mathrm{Hom}_{\mathsf{C}}(A,C)$.

[1] El trabajo germinal fue el artículo de: Samuel Eilenberg y Saunders MacLane, *General theory of natural equivalences*, Transactions of the American Mathematical Society **58** (1945), 231–294. En este ensayo se introdujo en término "categoría" por primera vez, amén de los conceptos de "funtor" y "transformación natural", con gran cantidad de ejemplos.

[2] Las notaciones y definiciones más comunes están bien resumidos en: Sergey I. Gelfand y Yuri I. Manin, *Homological Algebra*, en el *Encyclopedia of Mathematical Sciences 38* (Algebra V), Springer, Berlin, 1994.

Estos datos deben cumplir tres requisitos:

(a) Los conjuntos de morfismos $\mathrm{Hom}_{\mathsf{C}}(A,B)$ son *disjuntos*: cada morfismo f determina unívocamente dos objetos A, B tales que $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$.

(b) Para cada objeto $A \in \mathrm{Ob}(\mathsf{C})$ existe un único **morfismo idéntico** $1_A \in \mathrm{Hom}_{\mathsf{C}}(A,A)$ tal que $\underline{f\,1_A = f}$ para todo $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$ y $\underline{1_A\, g = g}$ para todo $g \in \mathrm{Hom}_{\mathsf{C}}(C,A)$.

(c) La composición es *asociativa*: si $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$, $g \in \mathrm{Hom}_{\mathsf{C}}(B,C)$ y $h \in \mathrm{Hom}_{\mathsf{C}}(C,D)$, entonces
$$h(gf) = (hg)f \quad \text{en} \quad \mathrm{Hom}_{\mathsf{C}}(A,D).$$

En general, aunque no siempre, la colección de objetos es demasiado amplio para llamarse un conjunto. La palabra *clase* se emplea aquí en el sentido técnico de "la teoría de clases" de Gödel y Bernays, que establece una jerarquía en la teoría de conjuntos. Cualquier conjunto es una clase, pero no al revés: la colección de todos los conjuntos forma una clase que no es un conjunto (este artificio evita la paradoja de Russell). En la teoría de Gödel y Bernays, los conjuntos son precisamente las clases que pueden ser miembros de otras clases.

La totalidad de morfismos, de entre todos los *conjuntos* $\mathrm{Hom}_{\mathsf{C}}(A,B)$, es una clase denotado a veces por $\mathrm{Mor}(\mathsf{C})$. En general, esta clase tampoco es un conjunto. Sin embargo, todos los cálculos con morfismos sólo involucran un número finito de los conjuntos $\mathrm{Hom}_{\mathsf{C}}(A,B)$ a la vez: para los fines de este curso, no hay que preocuparse mucho sobre la axiomática de la teoría de conjuntos.

En muchos de los ejemplos que siguen, aunque no siempre, los morfismos son funciones. En estos casos, se acepta la notación $g \circ f$ como sinónimo de gf. También es cómodo usar la notación "$\underline{f\colon A \to B}$" como abreviatura de "$f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$", aun en los casos en donde f no es una función de A en B, *strictu sensu*.

► El rasgo distintivo del manejo de las categorías es la consideración de *objetos y morfismos* como un paquete inseparable. En los ejemplos que siguen, hay que declarar cuáles son los objetos y cuáles son los morfismos, para describir la categoría con toda precisión.

Ejemplo 2.2. La categoría más sencilla es Set, cuyos objetos son los **conjuntos**.[3] Los morfismos en $\mathrm{Hom}_{\mathsf{Set}}(X,Y)$ son las **funciones** $f\colon X \to Y$.

Ejemplo 2.3. La categoría Gr: sus objetos son los **grupos** y los morfismos en $\mathrm{Hom}_{\mathsf{Gr}}(G,H)$ son los **homomorfismos de grupos** $\varphi\colon G \to H$.

La categoría Ab de los **grupos abelianos** es una **subcategoría** de Gr, es decir, todos los objetos (respectivamente, morfismos) de Ab son objetos (respectivamente, morfismos) de Gr. Esta es una subcategoría **plena**, es decir, $\mathrm{Hom}_{\mathsf{Ab}}(G,H) = \mathrm{Hom}_{\mathsf{Gr}}(G,H)$ cuando G y H son grupos abelianos.

[3] Los objetos de Set se describen con distintas palabras en todos los idiomas: *set* en inglés, *conjunto* en español (ou em portugués), *ensemble* en francés, *insieme* en italiano, *Menge* en alemán, *zbiór* en polaco, *mnózhestvo* en ruso,... En tales casos, se usa la abreviatura inglesa porque, como una vez dijo William de Ockham, *entes non sunt multiplicanda praeter necessitatem*.

Ejemplo 2.4. La categoría Mon: sus objetos son los **monoides** y $\mathrm{Hom}_{\mathsf{Mon}}(M,N)$ consta de los **homomorfismos de monoides** $h\colon M \to N$, es decir, funciones que respetan productos y preservan los elementos neutros.

Esta vez, Gr es una subcategoría plena de Mon, porque todo homomorfismo de monoides entre dos grupos también respeta inversos.

Ejemplo 2.5. La categoría An: sus objetos son los **anillos** y los morfismos en $\mathrm{Hom}_{\mathsf{An}}(A,B)$ son los **homomorfismos de anillos** $\psi\colon A \to B$.

Ejemplo 2.6. Si A es un anillo, los **A-módulos** (a la izquierda) son los objetos de una categoría A-Mod: en este caso se escribe $\mathrm{Hom}_A(M,N)$ en vez de $\mathrm{Hom}_{A\text{-}\mathsf{Mod}}(M,N)$ para denotar los homomorfismos de A-módulos $\varphi\colon M \to N$.

Los **A-módulos a la derecha** son objetos de otra categoría, denombrada Mod-A: si el contexto lo permite, también se escribe $\mathrm{Hom}_A(R,S)$ en vez de $\mathrm{Hom}_{\mathsf{Mod}\text{-}A}(R,S)$ para denotar los homomorfismos de A-módulos a la derecha $\chi\colon R \to S$.

Ejemplo 2.7. La categoría Top: sus objetos son los **espacios topológicos** y los morfismos en $\mathrm{Hom}_{\mathsf{Top}}(X,Y)$ son las **funciones continuas** $f\colon X \to Y$.

Ejemplo 2.8. La categoría Dif: sus objetos son los **variedades diferenciales** (reales, de dimensión finita) y los morfismos en $\mathrm{Hom}_{\mathsf{Dif}}(X,Y)$ son las **funciones suaves** $f\colon X \to Y$.

Ejemplo 2.9. Hay otra categoría Htp cuyos objetos son todos los espacios topológicos, pero los morfismos son diferentes. Dos funciones continuas $f,g\colon X \to Y$ son *homotópicas* si hay una función $h\colon [0,1]\times X \to Y$ tal que $h(0,x) = f(x)$ y $h(1,x) = g(x)$ para todo $x \in X$. La homotopía es una relación de equivalencia[4] entre funciones continuas de X en Y. Ahora los morfismos en $\mathrm{Hom}_{\mathsf{Htp}}(X,Y)$ son las **clases de homotopía** en $\mathrm{Hom}_{\mathsf{Top}}(X,Y)$. Si $[f]$ denota la clase de homotopía de la función f, se define $[g]\,[f] := [g\circ f]$ y es fácil ver que las tres condiciones de la Definición 2.1 quedan satisfechas.

Definición 2.10. Una categoría C es una **categoría pequeña** *si* $\mathrm{Ob}(\mathsf{C})$ *es un conjunto*.

Ejemplo 2.11. Sea J un **conjunto parcialmente ordenado**. Esto es, hay una relación $\leq$ definido sobre J que es reflexivo, transitivo y antisimétrico. Entonces J da lugar a una categoría pequeña J, donde

- $\mathrm{Ob}(\mathsf{J}) := J$;
- $\mathrm{Hom}_{\mathsf{J}}(i,j) := \{f_{ji}\}$ (un solo morfismo) si $i \leq j$, mientras $\mathrm{Hom}_{\mathsf{J}}(i,j) := \emptyset$ si $i \not\leq j$.

Fíjese que para todo $j \in J$, vale $1_k = f_{kk} \in \mathrm{Hom}_{\mathsf{J}}(k,k)$, por reflexividad. Además, vale $f_{kj}f_{ji} = f_{ki}$ si $i \leq j \leq k$, por transitividad. La asociatividad de la composición es consecuencia de la unicidad del morfismo f_{li}, si $i \leq j \leq k \leq l$.

[4] La idea es que $f = h_0$ y $g = h_1$ son extremos de una familia de funciones continuas $h_t(x) := h(t,x)$, parametrizada por $0 \leq t \leq 1$. En los libros de topología algebraica, $\mathrm{Hom}_{\mathsf{Htp}}(X,Y)$ es denotado por $[X,Y]$.

Ejemplo 2.12. Sea X un espacio topológico y sea $\mathcal{T}(X)$ su topología (el conjunto de las partes abiertas de X). Entonces hay una categoría pequeña Top-X definido por $\mathsf{Top}\text{-}X := \mathsf{C}(\mathcal{T}(X))$. En otras palabras, los objetos son las partes abiertas de X; si U y V son partes abiertas de X, entonces $\mathrm{Hom}_{\mathsf{Top}\text{-}X}(U,V) := \{i_{VU}\}$ si $U \subseteq V$, donde $i_{VU} : U \hookrightarrow V$ es la inclusión; y no hay morfismo alguno en $\mathrm{Hom}_{\mathsf{Top}\text{-}X}(U,V)$ si $U \not\subseteq V$.

Ejemplo 2.13. Una categoría pequeña C con un solo objeto define un *monoide*: si $\mathrm{Ob}(\mathsf{C}) = \{*\}$, entonces $\mathrm{Mor}(\mathsf{C})$ tiene una ley de composición asociativa con una identidad 1_* así que $\mathrm{Mor}(\mathsf{C})$ es un monoide.

En una categoría C cualquiera, un morfismo $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$ es *morfismo inversible* o bien un **isomorfismo** si hay otro morfismo $g \in \mathrm{Hom}_{\mathsf{C}}(B,A)$ tal que

$$gf = 1_A, \qquad fg = 1_B.$$

Este g es el morfismo inverso de f. Fíjese que el inverso g es *único*, porque si $hf = 1_A$ y $fh = 1_B$, entonces $h = 1_A h = (gf)h = g(fh) = g1_B = g$. Si C es una categoría con un sólo objeto en la cual todo morfismo es inversible, entonces $\mathrm{Mor}(\mathsf{C})$ es un **grupo**. De hecho, cualquier grupo G es de esta forma: defínase C_G por $\mathrm{Ob}(\mathsf{C}_G) := \{*\}$ y $\mathrm{Hom}_{\mathsf{C}_G}(*,*) := G$.

Definición 2.14. Un **grupoide** es una categoría pequeña C en la cual todo morfismo es inversible. Si $G_0 = \mathrm{Ob}(\mathsf{C})$ y $G_1 := \mathrm{Mor}(\mathsf{C})$, el grupoide se denota por $\underline{G_1 \rightrightarrows G_0}$. Si $f : x \to y$ es un morfismo y si $g : y \to x$ es su inverso, las fórmulas

$$\begin{aligned} r &: G_1 \to G_0 : f \mapsto y, & i &: G_1 \to G_1 : f \mapsto g, \\ s &: G_1 \to G_0 : f \mapsto x, & u &: G_0 \to G_1 : x \mapsto 1_x \end{aligned}$$

definen cuatro aplicaciones entre conjuntos: la *meta* r, la *fuente* s, la *inversión* i y la *unidad* u. (Las dos flechas en $G_1 \rightrightarrows G_0$ denotan la meta y la fuente.) Las propiedades de grupoides pueden enunciarse en términos de estas cuatro aplicaciones y el "dominio de la multiplicación" $G_2 := \{\, (f,h) \in G_1 \times G_1 : r(h) = s(f) \,\}$.

Definición 2.15. Si C es una categoría cualquiera, C° denota la **categoría opuesta** (o *categoría dual*)[5] definido por

$$\mathrm{Ob}(\mathsf{C}^\circ) := \mathrm{Ob}(\mathsf{C}), \qquad \mathrm{Hom}_{\mathsf{C}^\circ}(A,B) := \mathrm{Hom}_{\mathsf{C}}(B,A). \tag{2.1}$$

Es decir, wC° posee los mismos objetos que C pero "las flechas apunten en la dirección opuesta". Si se denota (por una sola vez) por f° el morfismo $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$ visto como elemento de $\mathrm{Hom}_{\mathsf{C}^\circ}(B,A)$, entonces la ley de composición en C° es $\underline{f^\circ g^\circ := (gf)^\circ}$.

[5]Es evidente de la definición que $(\mathsf{C}^\circ)^\circ = \mathsf{C}$, o mejor dicho, que las categorías $(\mathsf{C}^\circ)^\circ$ y C son *isomorfos* en el sentido de que haya una biyección entre sus objetos (respectivamente, entre sus morfismos) que preserva la ley de composición sin alterar su orden. Esta noción de isomorfismo de categorías resulta bastante banal y será reemplazada más adelante por un poderoso concepto de *equivalencia* de categorías.

2.2 Funtores y transformaciones naturales

Una vez que se haya absorbido el concepto de que los morfismos son tanto o más importantes que los objetos en una categoría, el siguiente paso es inquirir sobre las posibles aplicaciones de una categoría en otra. Hay que hacer dos avisos: uno, que como los objetos no siempre forman conjuntos, estas aplicaciones no siempre serán funciones *strictu sensu*; y dos, que se trata de hacer corresponder no sólo los objetos sino también los morfismos. La formulación de este tipo de correspondencia generalizada fue el gran avance de la obra de Eilenberg y MacLane, quienes introdujeron la siguiente definición.

Definición 2.16. Un **funtor** $\mathcal{F}$ (a veces llamado **funtor covariante**) de una categoría C en otra categoría D consta de:[6]

1. una aplicación $\mathrm{Ob}(\mathsf{C}) \to \mathrm{Ob}(\mathsf{D}) : A \mapsto \mathcal{F}A$;
2. una aplicación $\mathrm{Mor}(\mathsf{C}) \to \mathrm{Mor}(\mathsf{D}) : \varphi \mapsto \mathcal{F}\varphi$, tal que

$$\varphi \in \mathrm{Hom}_{\mathsf{C}}(A,B) \implies \mathcal{F}\varphi \in \mathrm{Hom}_{\mathsf{D}}(\mathcal{F}A, \mathcal{F}B);$$

que cumple las siguientes condiciones:

(a) $\mathcal{F}(\psi\varphi) = (\mathcal{F}\psi)(\mathcal{F}\varphi)$ toda vez que $\varphi \in \mathrm{Hom}_{\mathsf{C}}(A,B)$, $\psi \in \mathrm{Hom}_{\mathsf{C}}(B,C)$;

(b) $\mathcal{F}1_A = 1_{\mathcal{F}A}$ para todo $A \in \mathrm{Ob}(\mathsf{C})$.

Se escribe $\mathcal{F}\colon \mathsf{C} \to \mathsf{D}$ si $\mathcal{F}$ es un funtor de C en D.

Definición 2.17. Un **cofuntor** (a veces, **funtor contravariante**) de una categoría C en otra categoría D es, por definición, un funtor covariante $\mathcal{G}\colon \mathsf{C}^\circ \to \mathsf{D}$.

Ahora, las correspondencias $\mathrm{Ob}(\mathsf{C}) \to \mathrm{Ob}(\mathsf{D}) : A \mapsto \mathcal{G}A$ y $\mathrm{Mor}(\mathsf{C}) \to \mathrm{Mor}(\mathsf{D}) : \varphi \mapsto \mathcal{G}\varphi$ cumplen

$$\varphi \in \mathrm{Hom}_{\mathsf{C}}(A,B) \implies \mathcal{G}\varphi \in \mathrm{Hom}_{\mathsf{D}}(\mathcal{G}B, \mathcal{G}A);$$

que cumple $\mathcal{G}1_A = 1_{\mathcal{G}A}$ para todo $A \in \mathrm{Ob}(\mathsf{C})$ y además

$$\mathcal{G}(\psi\varphi) = (\mathcal{G}\varphi)(\mathcal{G}\psi) \quad \text{toda vez que} \quad \varphi \in \mathrm{Hom}_{\mathsf{C}}(A,B),\ \psi \in \mathrm{Hom}_{\mathsf{C}}(B,C).$$

En otras palabras, un cofuntor "revierte el sentido de las flechas".

Ejemplo 2.18. Si C es una categoría cuyos objetos son conjuntos y cuyos morfismos son aplicaciones entre los conjuntos respectivos, se puede definir un funtor $\mathcal{F}\colon \mathsf{C} \to \mathsf{Set}$ por $\mathcal{F}A := A$ y $\mathcal{F}\varphi := \varphi$ para $A \in \mathrm{Ob}(\mathsf{C})$, $\varphi \in \mathrm{Mor}(\mathsf{C})$. El papel de este funtor es simplemente el de "olvidar" cualquier estructura extra de los objetos y morfismos de C, por tanto se llama un **funtor olvidadizo**. Hay funtores olvidadizos $\mathsf{Gr} \to \mathsf{Set}$, $\mathsf{Ab} \to \mathsf{Set}$, $\mathsf{An} \to \mathsf{Set}$, etcétera, que

[6] Algunos autores escriben $\mathcal{F}(A)$ por $\mathcal{F}A$ y $\mathcal{F}(\varphi)$ por $\mathcal{F}\varphi$, lo cual no hace daño. Sin embargo, es preferible usar la notación sin adornos para evitar selvas de paréntesis —conviene recordar el sabio consejo de Ockham.

suprimen las operaciones de producto o suma y abandonan la mulitplicatividad o aditividad de los homomorfismos.

De igual modo, hay funtores olvidadizos $\mathsf{An} \to \mathsf{Ab}$ (que olvida la operación de producto), A-$\mathsf{Mod} \to \mathsf{Ab}$ (que olvida la acción del anillo A), $\mathsf{Dif} \to \mathsf{Top}$ (que olvida la estructura diferencial), etcétera.

Ejemplo 2.19. Si A es un anillo, $M_n(A)$ denota el anillo de matrices $n \times n$ con entradas en A. Si $f\colon A \to B$ es un homomorfismo de anillos, defínase $M_n f\colon M_n(A) \to M_n(B)$ por $M_n f([a_{ij}]) := [f(a_{ij})]$, aplicando f a una matriz entrada por entrada. En vista de la relación

$$f\left(\sum_{j=1}^{n} a_{ij}\, b_{jk}\right) = \sum_{j=1}^{n} f(a_{ij})\, f(b_{jk}),$$

se ve que $M_n f$ es también un homomorfismo de anillos. La correspondencia $A \mapsto M_n(A)$, $f \mapsto M_n f$ define un funtor $M_n\colon \mathsf{An} \to \mathsf{An}$.

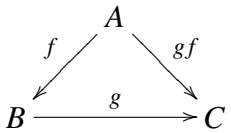
Ejemplo 2.20. Si X es un conjunto, $\mathcal{P}(X)$ denota el conjunto de todas las partes de X. Si $f\colon X \to Y$ es un función entre conjuntos, defínase $\mathcal{P}f\colon A \mapsto f(A) \subseteq Y$ para todo $A \subseteq X$; fíjese que $\mathcal{P}f(\emptyset) = \emptyset$. La correspondencia $X \mapsto \mathcal{P}(X)$, $f \mapsto \mathcal{P}f$ define un funtor $\mathcal{P}\colon \mathsf{Set} \to \mathsf{Set}$.

Ejemplo 2.21. Si G es un grupo, no necesariamente abeliano, se sabe que el subgrupo G' formado por productos finitos de *conmutadores* $ghg^{-1}h^{-1}$ es un subgrupo normal de G y que el cociente $\alpha(G) := G/G'$ es un grupo abeliano. Si $\varphi\colon G \to H$ es un homomorfismo de grupos, es claro que $\varphi(G') \subseteq H'$, lo cual induce un homomorfismo $\alpha(\varphi) = \bar{\varphi} : G/G' \to H/H'$. De este modo, se define un funtor $\alpha\colon \mathsf{Gr} \to \mathsf{Ab}$, llamado **abelianización**.

Definición 2.22. Si C es una categoría y si $A \in \mathrm{Ob}(\mathsf{C})$, considérese la correspondencia

$$\mathrm{Hom}_{\mathsf{C}}(A,-) : \mathsf{C} \to \mathsf{Set} : B \mapsto \mathrm{Hom}_{\mathsf{C}}(A,B). \tag{2.2}$$

Para que esta asignación de objetos defina un funtor, hay que agregar una correspondencia entre morfismos. Dado un morfismo $g \in \mathrm{Hom}_{\mathsf{C}}(B,C)$, el diagrama



sugiere que al morfismo g se le debe asociar la aplicación $f \mapsto gf$:

$$g_* \equiv \mathrm{Hom}_{\mathsf{C}}(A,g) : f \mapsto gf : \mathrm{Hom}_{\mathsf{C}}(A,B) \to \mathrm{Hom}_{\mathsf{C}}(A,C).$$

Si $h \in \mathrm{Hom}_{\mathsf{C}}(C,D)$, entonces $\mathrm{Hom}_{\mathsf{C}}(A,hg) : f \mapsto hgf$ es la composición (en el sentido usual, de funciones) de $f \mapsto gf$ con $gf \mapsto hgf$, de modo que

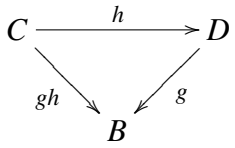
$$(hg)_* = \mathrm{Hom}_{\mathsf{C}}(A,hg) = \mathrm{Hom}_{\mathsf{C}}(A,h) \circ \mathrm{Hom}_{\mathsf{C}}(A,g) = h_* \circ g_*.$$

Luego $\mathrm{Hom}_{\mathsf{C}}(A,-) : \mathsf{C} \to \mathsf{Set}$ es un funtor covariante.

Definición 2.23. Si C es una categoría y si $B \in \mathrm{Ob}(\mathsf{C})$, considérese la correspondencia

$$\mathrm{Hom}_{\mathsf{C}}(-,B) : A \mapsto \mathrm{Hom}_{\mathsf{C}}(A,B). \tag{2.3}$$

Dado un morfismo $h \in \mathrm{Hom}_{\mathsf{C}}(C,D)$, el diagrama



sugiere que al morfismo h se le debe asociar la aplicación $g \mapsto gh$:

$$h^* \equiv \mathrm{Hom}_{\mathsf{C}}(h,B) : g \mapsto gh : \mathrm{Hom}_{\mathsf{C}}(D,B) \to \mathrm{Hom}_{\mathsf{C}}(C,B).$$

Si $k \in \mathrm{Hom}_{\mathsf{C}}(A,C)$, entonces $\mathrm{Hom}_{\mathsf{C}}(hk,B) : g \mapsto ghk$ es la composición (en el sentido usual, de funciones) de $g \mapsto gh$ con $gh \mapsto ghk$, de modo que

$$(hk)^* = \mathrm{Hom}_{\mathsf{C}}(hk,B) = \mathrm{Hom}_{\mathsf{C}}(k,B) \circ \mathrm{Hom}_{\mathsf{C}}(h,B) = k^* \circ h^*.$$

Luego $\mathrm{Hom}_{\mathsf{C}}(-,B) : \mathsf{C}^\circ \to \mathsf{Set}$ es un funtor *contravariante* de C en Set.

En el caso de la categoría A-Mod de A-módulos (a la izquierda), cada conjunto de morfismos $\mathrm{Hom}_A(M,N)$ es un grupo abeliano bajo la suma puntual de A-homomorfismos, dada por $(f+g)(x) := f(x)+g(x)$. Además, esta suma distribuye sobre composición, de manera evidente:

$$(g+h)f = gf + hf, \qquad g(h+k) = gh + gk.$$

Si $M,N \in \mathrm{Ob}(A\text{-}\mathsf{Mod})$, se concluye que los dos funtores anteriores llevan A-Mod en la categoría Ab de grupos abelianos:

$$\mathrm{Hom}_A(M,-) : A\text{-}\mathsf{Mod} \to \mathsf{Ab}, \qquad \mathrm{Hom}_A(-,N) : (A\text{-}\mathsf{Mod})^\circ \to \mathsf{Ab}.$$

Notación. Conviene introducir una abreviatura para denotar que A sea un objeto de la categoría C. En vez de "$A \in \mathrm{Ob}(\mathsf{C})$" se escribirá $\underline{A \in\in \mathsf{C}}$. Esta notación expresa correctamente la jerarquía de pertenencia entre un objeto y su categoría.[7]

Definición 2.24. Si C y D son dos categorías, su **producto directo** es la categoría $\mathsf{C} \times \mathsf{D}$ definido por:

- $\mathrm{Ob}(\mathsf{C} \times \mathsf{D}) := \mathrm{Ob}(\mathsf{C}) \times \mathrm{Ob}(\mathsf{D})$;
- $\mathrm{Hom}_{\mathsf{C}\times\mathsf{D}}\big((A,X),(B,Y)\big) := \mathrm{Hom}_{\mathsf{C}}(A,B) \times \mathrm{Hom}_{\mathsf{D}}(X,Y)$;
- $(g,\psi)(f,\varphi) := (gf, \psi\varphi), \quad 1_{(A,X)} := (1_A, 1_X)$.

[7] Esta notación no se encuentra (todavía) en los libros de texto. Yo lo aprendí de Ralf Meyer, un gran experto contemporario en esta materia. Véase, por ejemplo, el uso de esta simbología en: Ralf Meyer, *Homological algebra in bivariant K-theory and other triangulated categories. II*, preprint arXiv:0801.1344, Göttingen, 2008.

Un funtor $\mathcal{F}\colon \mathsf{C}\times\mathsf{D}\to\mathsf{E}$ también se llama un **bifuntor** de C y D en E. Por ejemplo, debe ser claro cómo definir un bifuntor $\mathrm{Hom}_{\mathsf{C}}\colon \mathsf{C}^{\circ}\times\mathsf{C}\to\mathsf{Set}$.

Definición 2.25. Una categoría C es una **subcategoría** de otra categoría D si

- $\mathrm{Ob}(\mathsf{C})\subseteq\mathrm{Ob}(\mathsf{D})$ y
- $\mathrm{Hom}_{\mathsf{C}}(A,B)\subseteq\mathrm{Hom}_{\mathsf{D}}(A,B)$ para todo $A,B\in\in\mathsf{C}$.

Si $\mathrm{Hom}_{\mathsf{C}}(A,B)=\mathrm{Hom}_{\mathsf{D}}(A,B)$ para todo $A,B\in\in\mathsf{C}$, se dice que C es una **subcategoría plena** de D. Por ejemplo, Ab es una subcategoría plena de Gr.

Definición 2.26. Un **funtor** $\mathcal{F}\colon \mathsf{C}\to\mathsf{D}$ es (a) **fiel**, (b) **pleno**, o (c) **plenamente fiel** si para todo $A,B\in\in\mathsf{C}$, la aplicación

$$\overline{\mathcal{F}}:\mathrm{Hom}_{\mathsf{C}}(A,B)\to\mathrm{Hom}_{\mathsf{D}}(\mathcal{F}A,\mathcal{F}B) \tag{2.4}$$

es respectivamente (a) inyectiva, (b) sobreyectiva, o (c) biyectiva.

Ejemplo 2.27. Los funtores olvidadizos $\mathsf{Gr}\to\mathsf{Set}$, $\mathsf{Ab}\to\mathsf{Set}$, $\mathsf{An}\to\mathsf{Ab}$, A-$\mathsf{Mod}\to\mathsf{Ab}$ y $\mathsf{Dif}\to\mathsf{Top}$ mencionados en el Ejemplo 2.18 son todos fieles pero no son plenos.

La *proyección* $\mathcal{P}_1\colon \mathsf{C}\times\mathsf{D}\to\mathsf{C}$, definido por $\mathcal{P}_1((A,X)):=A$, $\mathcal{P}((f,\varphi)):=f$, es pleno pero no es fiel.

Si C es una subcategoría plena de D, entonces la inclusión de C en D es un funtor plenamente fiel. (Este ejemplo indica que un funtor plenamente fiel no es necesariamente una biyección entre los objetos de C y D.)

► Un funtor relaciona dos categorías, conservando sus estructuras (objetos, morfismos, ley de composición). También hay una manera preferida de relacionar dos funtores $\mathcal{F}\colon \mathsf{C}\to\mathsf{D}$, $\mathcal{G}\colon \mathsf{C}\to\mathsf{D}$ entre dos categorías dadas. Antes de definirla, conviene considerar dos funtores importantes para la teoría de módulos.

Definición 2.28. Sea M un módulo a la izquierda sobre un anillo A. Su **módulo dual**

$$M^*:=\mathrm{Hom}_A(M,A)$$

es un A-módulo *a la derecha*, bajo la suma puntual de A-homomorfismos y la acción de A dado por

$$(fa)(x):=f(x)\,a\quad\text{para todo}\quad f\in M^*,\ a\in A,\ x\in M.$$

Para todo $b\in A$, vale $(fa)(bx)=f(bx)\,a=bf(x)\,a=b(fa)(x)$, así que $fa\in\mathrm{Hom}_A(M,A)$. Si $\varphi\colon M\to N$ es un homomorfismo de A-módulos (a la izquierda), su **transpuesta** es la aplicación

$$\varphi^t:N^*\to M^*:g\mapsto g\circ\varphi.$$

Si $\psi\colon N\to P$ es otro homomorfismo de A-módulos (a la izquierda), entonces $(\psi\circ\varphi)^t=\varphi^t\circ\psi^t:h\mapsto h\circ\psi\circ\varphi$. En otras palabras, $M\mapsto M^*$, $\varphi\mapsto\varphi^t$ es un *funtor contravariante* $\mathcal{D}\colon (A\text{-}\mathsf{Mod})^{\circ}\to\mathsf{Mod}\text{-}A$, llamado **dualidad**.

De la misma manera, si R es un A-módulo a la derecha, entonces $R^* := \mathrm{Hom}_A(R,A)$ es un A-módulo a la izquierda, al definir $(ck)(y) := ck(y)$ para $k \in R^*$, $c \in A$, $y \in R$, ya que $(ck)(yb) = ck(yb) = ck(y)b = (ck)(y)b$ para todo $b \in A$. Luego $R \mapsto R^*$, $\chi \mapsto \chi^t$ es otro funtor de dualidad $\mathcal{D}\colon (\mathsf{Mod}\text{-}A)^\circ \to A\text{-}\mathsf{Mod}$.

Definición 2.29. Sea M un A-módulo a la izquierda. Su **módulo bidual** $M^{**} := \mathrm{Hom}_A(M^*,A)$ es también un A-módulo a la izquierda. Hay un funtor covariante $\mathcal{D}^2\colon A\text{-}\mathsf{Mod} \to A\text{-}\mathsf{Mod}$ dado por $\mathcal{D}^2 M := M^{**}$, $\mathcal{D}^2 f := f^{tt} = (f^t)^t$.

Ejemplo 2.30. Si V es un espacio vectorial finitodimensional sobre un cuerpo $\mathbb{F}$, se puede construir un isomorfismo lineal entre V y $V^* = \mathrm{Hom}_{\mathbb{F}}(V,\mathbb{F})$ al hacer corresponder una base de V con la base dual de V^*. Sin embargo, este isomorfismo lineal $T\colon V \to V^*$ depende de una elección de bases: no hay un isomorfismo preferido que no dependa de las bases.

Denótese por $\mathsf{Vect}\text{-}\mathbb{F}$ la categoría de espacios vectoriales sobre $\mathbb{F}$ y por $\mathsf{FinVect}\text{-}\mathbb{F}$ su subcategoría plena de espacios vectoriales finitodimensionales.

Hay una aplicación *canónica* o *natural* entre un espacio vectorial V y su bidual V^{**}, dada por la **evaluación** $\eta_V : V \to V^{**}$, la cual se define por

$$\eta_V(x) : f \mapsto f(x), \quad \text{para} \quad x \in V,\ f \in V^*. \tag{2.5}$$

Esta definición no requiere elegir bases en V ni en V^{**}. Fíjese que η_V es inyectiva y que es biyectiva si (y sólo si) V es finitodimensional.

Si $S\colon V \to W$ es una transformación lineal, y si $S^{tt}\colon V^{**} \to W^{**}$ es su doble transpuesta, entonces para cada $x \in V$, $\sigma := \eta_V(x) \in V^{**}$, vale

$$\big(S^{tt} \circ \eta_V(x)\big)(g) = \eta_V(x)(S^t(g)) = \eta_V(x)(g \circ S) = g \circ S(x) = g(S(x)) = \eta_W(S(x))(g)$$

para todo $x \in V$, $g \in W^*$, de modo que

$$S^{tt} \circ \eta_V = \eta_W \circ S : V \to W^{**}. \tag{2.6}$$

En otras palabras, la *familia* de evaluaciones $\{\, \eta_V : V \in\in \mathsf{Vect}\text{-}\mathbb{F} \,\}$ *entrelaza* la acción del funtor $\mathcal{D}^2$ sobre $\mathsf{Vect}\text{-}\mathbb{F}$.

Definición 2.31. Si $\mathcal{F}, \mathcal{G}\colon \mathsf{C} \to \mathsf{D}$ son dos funtores, una **transformación natural** entre $\mathcal{F}$ y $\mathcal{G}$ es una familia de morfismos $\theta_A \in \mathrm{Hom}_{\mathsf{D}}(\mathcal{F}A, \mathcal{G}A)$, uno para cada $A \in\in \mathsf{C}$, tal que

$$\mathcal{G}\varphi \circ \theta_A = \theta_B \circ \mathcal{F}\varphi, \quad \text{para cada} \quad \varphi \in \mathrm{Hom}_{\mathsf{C}}(A,B). \tag{2.7}$$

Dicho de otro modo: para cada $\varphi \in \mathrm{Mor}(\mathsf{C})$, *el siguiente diagrama es conmutativo*:[8]

$$\begin{array}{ccc} \mathcal{F}A & \xrightarrow{\theta_A} & \mathcal{G}A \\ {\scriptstyle \mathcal{F}\varphi}\downarrow & & \downarrow{\scriptstyle \mathcal{G}\varphi} \\ \mathcal{F}B & \xrightarrow{\theta_B} & \mathcal{G}B \end{array}$$

[8] Un **diagrama** es **conmutativo** si cada cadena de flechas que une dos vértices dados tiene la misma composición.

Se escribe $\theta\colon \mathcal{F} \to \mathcal{G}$, en forma abreviada. Se dice que θ es un **isomorfismo natural** si cada θ_A es un isomorfismo en la categoría D.

Una transformación natural también se llama **morfismo de funtores**. Hay una categoría[9] $\mathsf{Fun}(\mathsf{C},\mathsf{D})$ cuyos objetos son los funtores $\mathcal{F}\colon \mathsf{C} \to \mathsf{D}$ y cuyos morfismos son las transformaciones naturales $\theta\colon \mathcal{F} \to \mathcal{G}$. Cada funtor conlleva la transformación idéntica $1_{\mathcal{F}} : A \mapsto 1_{\mathcal{F}A}$ y la ley de composición es obvia: $(\theta\eta)_A := \theta_A \circ \eta_A$ para $A \in\in \mathsf{C}$.

Definición 2.32. Para cualquier categoría C hay un **funtor idéntico** $1_{\mathsf{C}}\colon \mathsf{C} \to \mathsf{C}$ dado por $1_{\mathsf{C}}(A) := A$, $1_{\mathsf{C}}(\varphi) := \varphi$ para $A \in\in \mathsf{C}$, $\varphi \in \mathrm{Mor}(\mathsf{C})$.

Se dice que C y D son *categorías isomorfas* si hay funtores $\mathcal{F}\colon \mathsf{C} \to \mathsf{D}$ y $\mathcal{G}\colon \mathsf{D} \to \mathsf{C}$ tales que $\mathcal{G}\mathcal{F} = 1_{\mathsf{C}}$ y $\mathcal{F}\mathcal{G} = 1_{\mathsf{D}}$.

Ejemplo 2.33. Las evaluaciones $\{\, \eta_V : V \in\in \mathsf{Vect}\text{-}\mathbb{F} \,\}$ conforman una transformación natural entre el funtor idéntico $1_{\mathsf{Vect}\text{-}\mathbb{F}}$ el el funtor de bidualidad $\mathcal{D}^2\colon \mathsf{Vect}\text{-}\mathbb{F} \to \mathsf{Vect}\text{-}\mathbb{F}$, en vista de las relaciones (2.6):

$$\begin{array}{ccc} V & \xrightarrow{\eta_V} & V^{**} \\ {\scriptstyle S}\downarrow & & \downarrow{\scriptstyle S^{tt}} \\ W & \xrightarrow{\eta_W} & W^{**} \end{array}$$

Al reemplazar $\mathsf{Vect}\text{-}\mathbb{F}$ por su subcategoría $\mathsf{FinVect}\text{-}\mathbb{F}$ y al considerar la bidualidad $\mathcal{D}^2$ de $\mathsf{FinVect}\text{-}\mathbb{F}$ en sí mismo, las evaluaciones η definen un *isomorfismo natural*, es decir, cada $\eta_V : V \to V^{**}$ es un isomorfismo lineal en $\mathsf{FinVect}\text{-}\mathbb{F}$.

Ahora, las evaluaciones no hacen uso de propiedad alguna de los espacios vectoriales que no sigue válido para A-módulos (a la izquierda, digamos) cualesquiera: la definición (2.5) también determina un morfismo de funtores entre $1_{A\text{-}\mathsf{Mod}}$ y $\mathcal{D}^2\colon A\text{-}\mathsf{Mod} \to A\text{-}\mathsf{Mod}$.

► El concepto de "isomorfismo de categorías" en la Definición 2.32 es de poca utilidad, por ser prácticamente trivial: los casos conocidos no son de mucha interés. El concepto valioso, a continuación, es la *equivalencia* de categorías. La idea maestra es que es suficiente obtener isomorfismo, en lugar de igualdad, entre objetos o entre morfismos.

Definición 2.34. Un funtor $\mathcal{F}\colon \mathsf{C} \to \mathsf{D}$ es una **equivalencia de categorías** si hay otro funtor $\mathcal{G}\colon \mathsf{D} \to \mathsf{C}$ (a veces llamado un *cuasiinverso* de $\mathcal{F}$) tal que exista un par de isomorfismos naturales $\theta\colon \mathcal{G}\mathcal{F} \to 1_{\mathsf{C}}$ y $\eta\colon \mathcal{F}\mathcal{G} \to 1_{\mathsf{D}}$.

Ejemplo 2.35. Sea FinSet la categoría de conjuntos finitos (una subcategoría plena de Set) y sea N la subcategoría plena de FinSet cuyos objetos son $\{1,2,\ldots,n\}$ (vacío en el caso $n = 0$) para $n \in \mathbb{N} = \{0,1,2,\ldots\}$. La inclusión $I\colon \mathsf{N} \to \mathsf{FinSet}$ es una equivalencia de categorías. [10]

[9] Hay que advertir ciertas dificultades de la teoría de conjuntos a la hora de definir $\mathsf{Fun}(\mathsf{C},\mathsf{D})$. Si C es una categoría pequeña, no hay problema, porque la familia de transformaciones naturales entre dos funtores fijos es un conjunto. Si C no es pequeña, hay que extender el contexto de conjuntos. Por ejemplo, las *clases* propias no son elementos de otras clases, pero pertenecen a otros entes más vastos llamados *conglomerados*; y así sucesivamente. En síntesis: se puede proceder como si C fuera pequeña, sin mayor peligro.

[10] De hecho, puede tomarse $\mathrm{Ob}(\mathsf{N}) = \mathbb{N}$, al recordar que un número natural es *por definición* un conjunto con n elementos: $0 := \emptyset$, $1 := \{0\}$, $2 := \{0,1\}$, etc. Véase, por ejemplo: Paul R. Halmos, *Naive Set Theory*, Springer, New York, 1974.

En efecto, para cada conjunto finito X_n de cardinalidad n, elíjase un ordenamiento de sus elementos: $X_n = \{x_1, \ldots, x_n\}$. Defínase $\mathcal{G}\colon \mathsf{FinSet} \to \mathsf{N}$ por $\mathcal{G}X_n = \{1, \ldots, n\}$ (nótese que $\mathcal{G}\emptyset = \emptyset$) y $\mathcal{G}f(j) := k$ toda vez que $f \in \mathrm{Hom}(X_n, Y_m)$ cumple $f(x_j) = y_k$, con $j = 1, \ldots, n$. Entonces $\mathcal{G}\mathcal{F}\{1, \ldots, n\}$ es una permutación $\theta_{\{1,\ldots,n\}}$ de $\{1, \ldots, n\}$ y $\mathcal{F}\mathcal{G}X_n$ es una permutación η_{X_n} de X_n, en cada caso.

Obsérvese, en este ejemplo, que en general no hay unicidad de cuasiinversos.

Definición 2.36. Un funtor $\mathcal{F}\colon \mathsf{C} \to \mathsf{D}$ es **esencialmente sobreyectivo** si para cada $X \in\in \mathsf{D}$ hay un $A \in \mathsf{C}$ tal que $\mathcal{F}A$ es *isomorfo* a X; es decir, $\mathrm{Hom}_{\mathsf{D}}(\mathcal{F}A, X)$ contiene un isomorfismo.[11]

Fíjese que la inclusión $I\colon \mathsf{N} \to \mathsf{FinSet}$ del Ejemplo 2.35 es esencialmente sobreyectivo: para cada conjunto finito X existe un $n \in \mathbb{N}$ tal que haya una biyección entre $\{1, \ldots, n\}$ y X.

Proposición 2.37. *Un funtor $\mathcal{F}\colon \mathsf{C} \to \mathsf{D}$ es una equivalencia de categorías si y sólo si $\mathcal{F}$ es plenamente fiel y esencialmente sobreyectivo.*

Demostración. Ad$(\Rightarrow)$: Sea $\mathcal{F}$ una equivalencia de categorías y sea $\mathcal{G}$ un cuasiinverso de $\mathcal{F}$. Para $X \in\in \mathsf{D}$, el isomorfismo natural $\eta\colon \mathcal{F}\mathcal{G} \to 1_{\mathsf{D}}$ proporciona un isomorfismo $\eta_X \in \mathrm{Hom}_{\mathsf{D}}(\mathcal{F}\mathcal{G}X, X)$. Con $A := \mathcal{G}X \in\in \mathsf{C}$ se concluye que los objetos $\mathcal{F}A$ y X son isomorfos en D, mediante η_X. Luego, $\mathcal{F}$ es esencialmente sobreyectivo.

Tómese $A, B \in\in \mathsf{C}$. Hay que mostrar que $\overline{\mathcal{F}} : \mathrm{Hom}_{\mathsf{C}}(A, B) \to \mathrm{Hom}_{\mathsf{D}}(\mathcal{F}A, \mathcal{F}B)$ de (2.4) es biyectivo. Supóngase que $\overline{\mathcal{F}}(\varphi) = \overline{\mathcal{F}}(\psi)$, es decir, $\mathcal{F}\varphi = \mathcal{F}\psi$ para $\varphi, \psi \in \mathrm{Hom}_{\mathsf{C}}(A, B)$. Entonces $\mathcal{G}\mathcal{F}\varphi = \mathcal{G}\mathcal{F}\psi$. Por hipótesis, se sabe que $\theta\colon \mathcal{G}\mathcal{F} \to 1_{\mathsf{C}}$, lo cual, por (2.7), implica que

$$\varphi \circ \theta_A = \theta_B \circ \mathcal{G}\mathcal{F}\varphi = \theta_B \circ \mathcal{G}\mathcal{F}\psi = \psi \circ \theta_A,$$

y luego $\varphi = \varphi \circ \theta_A \circ \theta_A^{-1} = \psi \circ \theta_A \circ \theta_A^{-1} = \psi$ porque θ_A es un isomorfismo en $\mathrm{Hom}_{\mathsf{D}}(\mathcal{G}\mathcal{F}A, A)$. Por tanto, $\overline{\mathcal{F}}$ es inyectivo. Como esto vale para todo A, B, se concluye que el funtor $\mathcal{F}$ es fiel.

Por la simetría del argumento, el funtor $\mathcal{G}$ también es fiel. Si $\alpha \in \mathrm{Hom}_{\mathsf{D}}(\mathcal{F}A, \mathcal{F}B)$, el diagrama conmutativo

$$\begin{array}{ccc} \mathcal{G}\mathcal{F}A & \xrightarrow{\theta_A} & A \\ {\scriptstyle \mathcal{G}\alpha}\downarrow & & \downarrow{\scriptstyle \varphi} \\ \mathcal{G}\mathcal{F}B & \xrightarrow{\theta_B} & B \end{array}$$

permite *definir* $\varphi := \theta_B \circ \mathcal{G}\alpha \circ \theta_A^{-1} \in \mathrm{Hom}_{\mathsf{C}}(A, B)$. Ahora $\mathcal{G}\mathcal{F}\varphi = \theta_B^{-1} \circ \varphi \circ \theta_A$ (del párrafo anterior), así que $\mathcal{G}\mathcal{F}\varphi = \mathcal{G}\alpha$. La fieldad de $\mathcal{G}$ entonces implica que $\mathcal{F}\varphi = \alpha$; se concluye que $\overline{\mathcal{F}}$ es sobreyectivo. Como esto vale para todo A, B, se concluye que el funtor $\mathcal{F}$ es pleno.

Ad$(\Leftarrow)$: Sea $\mathcal{F}\colon \mathsf{C} \to \mathsf{D}$ un funtor plenamente fiel y esencialmente sobreyectivo. Hay que fabricar un cuasiinverso. Para cada $X \in\in \mathsf{D}$, hay un objeto $X' \in\in \mathsf{C}$ y un isomorfismo $\eta_X \in \mathrm{Hom}_{\mathsf{D}}(\mathcal{F}X', X)$, por la sobreyectividad esencial de $\mathcal{F}$. Además, si $\beta \in \mathrm{Hom}_{\mathsf{D}}(X, Y)$,

[11] En general, se escribe $A \simeq B$ para denotar que dos objetos $A, B \in\in \mathsf{C}$ son isomorfos; es decir, que $\mathrm{Hom}_{\mathsf{C}}(A, B)$ contiene un morfismo inversible.

entonces $\eta_Y^{-1} \circ \beta \circ \eta_X \in \mathrm{Hom}_{\mathsf{D}}(\mathcal{F}X', \mathcal{F}Y')$. Como $\mathcal{F}$ es plenamente fiel, hay un único morfismo $\beta' \in \mathrm{Hom}_{\mathsf{C}}(X', Y')$ tal que $\mathcal{F}\beta' = \eta_Y^{-1} \circ \beta \circ \eta_X$. Las correspondencias $X \mapsto X'$, $\beta \mapsto \beta'$ definen un funtor $\mathcal{G}\colon \mathsf{D} \to \mathsf{C}$. Por su definición, este diagrama conmuta:

$$\begin{array}{ccc} \mathcal{F}\mathcal{G}X & \xrightarrow{\eta_X} & X \\ {\scriptstyle \mathcal{F}\mathcal{G}\beta}\downarrow & & \downarrow{\scriptstyle \beta} \\ \mathcal{F}\mathcal{G}Y & \xrightarrow{\eta_Y} & Y \end{array}$$

así que $\eta : \mathcal{F}\mathcal{G} \to 1_{\mathsf{D}}$ es un isomorfismo natural.

Para cada $A \in\in \mathsf{C}$, hay un isomorfismo $\eta_{\mathcal{F}A} \in \mathrm{Hom}_{\mathsf{D}}(\mathcal{F}\mathcal{G}\mathcal{F}A, \mathcal{F}A)$. Por ser $\mathcal{F}$ plenamente fiel, hay un único morfismo $\theta_A \in \mathrm{Hom}_{\mathsf{C}}(\mathcal{G}\mathcal{F}A, A)$ tal que $\mathcal{F}\theta_A = \eta_{\mathcal{F}A}$. Además, θ_A es un isomorfismo que obedece $\mathcal{F}\theta_A^{-1} = \eta_{\mathcal{F}A}^{-1}$. Si $\varphi \in \mathrm{Hom}_{\mathsf{C}}(A, B)$, sea $\beta := \mathcal{F}\varphi$; entonces

$$\beta \circ \eta_{\mathcal{F}A} = \eta_{\mathcal{F}B} \circ \mathcal{F}\mathcal{G}\beta \implies \mathcal{F}\varphi \circ \mathcal{F}\theta_A = \mathcal{F}\theta_B \circ \mathcal{F}\mathcal{G}\mathcal{F}\varphi \implies \varphi \circ \theta_A = \theta_B \circ \mathcal{G}\mathcal{F}\varphi,$$

porque $\mathcal{F}$ es un funtor fiel. Se concluye que $\theta : \mathcal{G}\mathcal{F} \to 1_{\mathsf{C}}$ es un isomorfismo natural. □

Para la teoría de módulos, algunos de los funtores más importantes son aquéllos que fueron introducidos en las Definiciones 2.22 y 2.23. Un resultado básico de la teoría de categorías es la Proposición que sigue, llamado Lema de Yoneda,[12] que identifica las transformaciones naturales asociados a esos funtores con ciertos *conjuntos*.

Definición 2.38. Si C es una categoría cualquiera, los *funtores contravariantes* $\mathcal{F}\colon \mathsf{C}^\circ \to \mathsf{Set}$ son objetos de una categoría

$$\widehat{\mathsf{C}} := \mathsf{Fun}(\mathsf{C}^\circ, \mathsf{Set}).$$

Si $B \in\in \mathsf{C}$, la notación $\underline{h_B} := \mathrm{Hom}_{\mathsf{C}}(-, B)$ denotará el objeto de $\widehat{\mathsf{C}}$ definido por (2.3). Un funtor contravariante $\mathcal{F} \in\in \widehat{\mathsf{C}}$ se llama **funtor representable** si es isomorfo a h_B (en la categoría $\widehat{\mathsf{C}}$) para algún $B \in\in \mathsf{C}$.

Los funtores *covariantes* $\mathcal{G}\colon \mathsf{C} \to \mathsf{Set}$ son objetos de la categoría $\widehat{\mathsf{C}^\circ}$. Si $A \in\in \mathsf{C}$, la notación $\underline{h^A} := \mathrm{Hom}_{\mathsf{C}}(A, -)$ denotará el funtor covariante definido por (2.2). Un funtor covariante $\mathcal{F} \in\in \widehat{\mathsf{C}}$ se llama *funtor representable* si es isomorfo a h^A para algún $A \in\in \mathsf{C}$.

Si $B \in\in \mathsf{C}$ y si $\mathcal{F}\colon \mathsf{C}^\circ \to \mathsf{Set}$ es un funtor contravariante, una *transformación natural* $\eta \in \mathrm{Hom}_{\widehat{\mathsf{C}}}(h_B, \mathcal{F})$ es una familia de aplicaciones (entre conjuntos) $\{\, \eta_A : A \in\in \mathsf{C} \,\}$ tales que los siguientes diagramas conmutan, para cada $g \in \mathrm{Hom}_{\mathsf{C}}(D, A)$:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathsf{C}}(A, B) & \xrightarrow{\eta_A} & \mathcal{F}A \\ {\scriptstyle g^*}\downarrow & & \downarrow{\scriptstyle \mathcal{F}g} \\ \mathrm{Hom}_{\mathsf{C}}(D, B) & \xrightarrow{\eta_D} & \mathcal{F}D \end{array} \tag{2.8}$$

donde $g^* = h_B g = \mathrm{Hom}_{\mathsf{C}}(g, B) : f \mapsto fg$, para todo $f \in \mathrm{Hom}_{\mathsf{C}}(A, B)$.

[12] Nobuo Yoneda (1930–1996) hizo diversos trabajos en informática, pero su fama se debe principalmente a este Lema.

Proposición 2.39 (Lema de Yoneda)**.** *Si $B \in\in \mathsf{C}$ y si $\mathcal{F}\colon \mathsf{C}^\circ \to \mathsf{Set}$ es un funtor contravariante, hay una* ***biyección*** $\alpha\colon \mathrm{Hom}_{\widehat{\mathsf{C}}}(h_B, \mathcal{F}) \to \mathcal{F}B$ *dada por* $\alpha(\eta) := \eta_B(1_B)$.

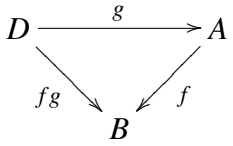
Demostración. Para verificar que α es inyectivo, hay que mostrar que cualquier transformación natural $\eta : h_B \to \mathcal{F}$ queda determinada por $\eta_B(1_B)$. Obsérvese que $1_B \in \mathrm{Hom}_{\mathsf{C}}(B,B)$ implica que $\eta_B(1_B) \in \mathcal{F}B$.

Si $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$, entonces $\mathcal{F}f\colon \mathcal{F}B \to \mathcal{F}A$ como aplicación entre conjuntos. El diagrama (2.8), con $A \mapsto B$, $D \mapsto A$ y $g \mapsto f$, muestra que $\mathcal{F}f \circ \eta_B = \eta_A \circ f^*$. Por lo tanto,

$$\eta_A(f) = \eta_A(f^* 1_B) = \mathcal{F}f(\eta_B(1_B)).$$

Ahora, si $\theta \in \mathrm{Hom}_{\widehat{\mathsf{C}}}(h_B, \mathcal{F})$ cumple $\theta_B(1_B) = \eta_B(1_B)$, entonces $\theta_A(f) = \eta_A(f)$ para todo $A \in\in \mathsf{C}$ y $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$, así que $\theta = \eta$.

Para verificar que α es sobreyectivo, para cada elemento $x \in \mathcal{F}B$ hay que construir una transformación natural $\eta : h_B \to \mathcal{F}$ tal que $\eta_B(1_B) = x$. Defínase $\eta_A(f) := \mathcal{F}f(x)$, para cada $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$. Considérese el diagrama (2.8), para ver si conmuta, para esta familia de aplicaciones $\{\, \eta_A : A \in\in \mathsf{C} \,\}$. Si $g \in \mathrm{Hom}_{\mathsf{C}}(D,A)$, la conmutatividad del diagrama



y la funtorialidad de $\mathcal{F}$ muestran que

$$\eta_D \circ g^*(f) = \eta_D(fg) = \mathcal{F}(fg)(x) = \mathcal{F}g \circ \mathcal{F}f(x) = \mathcal{F}g \circ \eta_A(f),$$

así que $\eta_D \circ g^* = \mathcal{F}g \circ \eta_A$ y el diagrama sí conmuta, para todo g; es decir, η es natural. De su definición, se obtiene

$$\eta_B(1_B) = \mathcal{F}1_B(x) = 1_{\mathcal{F}B}(x) = x. \qquad \square$$

Corolario 2.40. *Si $A \in\in \mathsf{C}$ y si $\mathcal{G}\colon \mathsf{C} \to \mathsf{Set}$ es un funtor* covariante*, las transformaciones naturales $\theta : h^A \to \mathcal{G}$ corresponden biyectivamente con los elementos del conjunto $\mathcal{G}A$, mediante $\theta \leftrightarrow \theta_A(1_A)$.*

Demostración. Repítase la demostración de la Proposición anterior, *mutatis mutandis*; o bien reemplace C por C° en esa Proposición, con atención a la dirección de las flechas. $\square$

Ejemplo 2.41. Al tomar $\mathcal{F} = h_C$ para algún $C \in\in \mathsf{C}$, el Lema de Yoneda dice que hay una biyección

$$\mathrm{Hom}_{\widehat{\mathsf{C}}}(h_B, h_C) \xleftrightarrow{\alpha} h_C B = \mathrm{Hom}_{\mathsf{C}}(B,C) \tag{2.9}$$

para todo $B \in\in \mathsf{C}$. Si $f \in \mathrm{Hom}_{\mathsf{C}}(B,C)$, entonces $f = \alpha(\eta)$ donde $\eta_B(1_B) = f$. La transformación natural $\eta : h_B \to h_C$ satisface

$$\eta_A(g) = \eta_A \circ g^*(1_B) = h_C g \circ \eta_B(1_B) = h_C g(f) \quad \text{para} \quad g \in \mathrm{Hom}_{\mathsf{C}}(A,B),$$

y por ende

$$\eta_A(g) = h_C g(f) = g^* f = fg = f_* g.$$

En otras palabras, se obtiene $\eta_A = f_* : \mathrm{Hom}_{\mathsf{C}}(A,B) \to \mathrm{Hom}_{\mathsf{C}}(A,C)$ cuando $f = \alpha(\eta)$. Se ha comprobado que $B \mapsto h_B$, $f \mapsto f_*$ es un funtor *covariante* de C en $\widehat{\mathsf{C}}$. La biyección (2.9) dice que este funtor es *plenamente fiel*. Además, es *inyectivo sobre objetos*, porque $h_A = h_C$ implica $\mathrm{Hom}_{\mathsf{C}}(B,A) = \mathrm{Hom}_{\mathsf{C}}(B,C)$ para todo $B \in\in \mathsf{C}$, lo cual conlleva $A = C$ porque los conjuntos de morfismos son disjuntos, por definición. Un funtor plenamente fiel que es inyectivo sobre objetos se llama **encaje** de categorías. Este ejemplo es el llamado **encaje de Yoneda** de C en $\widehat{\mathsf{C}}$.

La biyección (2.9) tiene otra consecuencia. Si $\mathcal{F}\colon \mathsf{C}^\circ \to \mathsf{Set}$ es un funtor representable y si hay dos objetos $B,C \in\in \mathsf{C}$ tales que $\mathcal{F} \simeq h_B$ y $\mathcal{F} \simeq h_C$, entonces hay isomorfismos naturales $\eta\colon h_B \to \mathcal{F}$ y $\theta\colon \mathcal{F} \to h_C$ en $\mathrm{Mor}(\widehat{\mathsf{C}})$, cuya composición $\theta\eta$ es un isomorfismo natural en $\mathrm{Hom}_{\widehat{\mathsf{C}}}(h_B,h_C)$. Ahora $\theta\eta = f_*$ para un *isomorfismo único* $f \in \mathrm{Hom}_{\mathsf{C}}(B,C)$. Dicho de otro modo: dos objetos $B,C \in\in \mathsf{C}$ que representan el mismo funtor $\mathcal{F}$ *son isomorfos, mediante un isomorfo único*. Se dice, entonces, que el objeto que representa $\mathcal{F}$ es **esencialmente único**.

▶ El concepto de funtor representable permite reconsiderar ciertas propiedades conocidas de aplicaciones entre conjuntos para que sean aplicables a morfismos de cualquier especie.

Lema 2.42. *Una función $f\colon X \to Y$ es* inyectiva *si y sólo si $f\circ g = f\circ h \implies g = h$ (cancelación de f a la izquierda), toda vez que $g,h\colon W \to X$ son funciones de otro conjunto W en X.*

Una función $f\colon X \to Y$ es sobreyectiva *si y sólo si $k\circ f = l\circ f \implies k = l$ (cancelación de f a la derecha), toda vez que $k,l\colon Y \to Z$ son funciones de Y en otro conjunto Z.*

Demostración. Si f es inyectiva, sean $g,h\colon W \to X$ dos funciones con el mismo dominio y con codominio X. Para todo $w \in W$, vale $f(g(w)) = f(h(w))$ si y sólo si $g(w) = h(w)$; luego $f\circ g = f\circ h$ implica $g = h$.

Inversamente, si f es cancelable a la izquierda, sean $x_1,x_2 \in X$ tales que $f(x_1) = f(x_2)$ en Y. Sea $S := \{*\}$ un conjunto con un solo elemento; defínase $g,h\colon S \to X$ por $g(*) := x_1$, $h(*) := x_2$. Entonces $f\circ g(*) = f\circ h(*)$, así que $f\circ g = f\circ h$, luego $g = h$ por hipótesis y por tanto $x_1 = x_2$.

Si f es sobreyectiva, sean $k,l\colon Y \to Z$ dos funciones con dominio Y y con el mismo codominio. Ahora $Y = \{\, f(x) : x \in X \,\}$; luego $k(f(x)) = l(f(x))$ para todo $x \in X$ si y sólo si $k(y) = l(y)$ para todo $y \in Y$; es decir, $k\circ f = l\circ f$ implica $k = l$.

Inversamente, si f es cancelable a la derecha, defínase $k,l\colon Y \to \{0,1\}$ por $k(y) := 0$ si $y \in f(X)$; $k(y) := 1$ si $y \notin f(X)$; mientras $l(y) := 0$ para todo $y \in Y$. Es claro que $k(f(x)) = l(f(x)) = 0$ para todo $x \in X$, de modo que $k\circ f = l\circ f$; se concluye que $k = l$, lo cual implica que $f(X) = Y$, es decir, f es sobreyectiva. □

Definición 2.43. En una categoría C, un morfismo $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$ es un **monomorfismo** (también se dice que f es **mónico**) si $fg = fh \implies g = h$ toda vez que $g,h \in \mathrm{Hom}_{\mathsf{C}}(D,A)$ para algún $D \in\in \mathsf{C}$.

Por otro lado, un morfismo $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$ es un **epimorfismo** (también se dice que f es **épico**) si $kf = lf \implies k = l$ toda vez que $k,l \in \mathrm{Hom}_{\mathsf{C}}(B,C)$ para algún $C \in\in \mathsf{C}$.

En la terminología de funtores representables:

- f es *mónico* si y sólo si $f_*\colon \mathrm{Hom}_{\mathsf{C}}(D,A) \to \mathrm{Hom}_{\mathsf{C}}(D,B)$ es *inyectivo* para todo D.
- f es *épico* si y sólo si $f^*\colon \mathrm{Hom}_{\mathsf{C}}(B,C) \to \mathrm{Hom}_{\mathsf{C}}(A,C)$ es *inyectivo* para todo C.

Ejemplo 2.44. En las categorías A-Mod y Mod-A, un morfismo $\varphi \in \mathrm{Hom}_A(M,N)$ es un monomorfismo si y sólo si $\varphi\colon M \to N$ es inyectivo como función. También es cierto que φ es un epimorfismo si y sólo si φ es sobreyectivo.[13]

En la categoría An, la inclusión $i\colon \mathbb{Z} \to \mathbb{Q}$ es inyectiva y por tanto es un monomorfismo de anillos. También es un epimorfismo, porque un homomorfismo de anillos $k\colon \mathbb{Q} \to A$ queda determinado por su restricción a $\mathbb{Z}$ (¿por qué?), luego $k \circ i = l \circ i$ implica $k = l$. Este es un ejemplo de un epimorfismo que no es sobreyectivo. También es un ejemplo de un morfismo que es mónico y épico a la vez, pero no es un isomorfismo.[14]

2.3 Categorías aditivas y abelianas

Las estructuras de las dos secciones anteriores son aplicables a categorías cualesquiera. Nuestro interés principal reside en las categorías de A-módulos, que tienen algunas propiedades específicas no compartidas por todas las categorías.

Definición 2.45. En una categoría C, un objeto $X \in\in \mathsf{C}$ es un **objeto inicial** si $\mathrm{Hom}_{\mathsf{C}}(X,A)$ tiene un solo elemento, para todo $A \in\in \mathsf{C}$. Un objeto $Y \in\in \mathsf{C}$ es un **objeto terminal** si $\mathrm{Hom}_{\mathsf{C}}(A,Y)$ tiene un solo elemento, para todo $A \in\in \mathsf{C}$. Un objeto que es a su vez inicial y terminal se llama un **objeto cero** en C.

Ejemplo 2.46. En la categoría Set, el conjunto vacío $\emptyset$ es el único objeto inicial: $\mathrm{Hom}_{\mathsf{Set}}(\emptyset,Z)$ contiene un sólo miembro, el cual es la "aplicación vacía". [Fíjese que estos conjuntos de morfismos siguen disjuntos, ya que $\mathrm{Hom}_{\mathsf{Set}}(\emptyset,Y) \cap \mathrm{Hom}_{\mathsf{Set}}(\emptyset,Z) = \emptyset$ para todo $Y,Z \in\in \mathsf{Set}$.] Cualquier conjunto de un solo elemento, $S = \{*\}$, es un objeto terminal en Set. La categoría Set no contiene un objeto cero.

La categoría pequeña del siguiente diagrama:

$$1_A \circlearrowright A \xrightarrow{f} B \circlearrowleft 1_B$$

con dos objetos y tres morfismos, tiene un único objeto inicial, un único objeto terminal, pero ningún objeto cero.

En las categorías Ab, An, A-Mod y Mod-A, hay un único objeto cero, el cual es, respectivamente: el grupo trivial $\{0\}$, el anillo trivial $\{0\}$, o bien el A-módulo trivial $\{0\}$.

[13] Para la demostración de estas afirmaciones, véase: Nathan Jacobson, *Basic Algebra II*, W. H. Freeman, New York, 1980, pp. 16–17.

[14] Este ejemplo "patológico" no debe tomarse muy a pecho. Una categoría se llama **balanceada** si cada morfismo que es mónico y también épico es un *isomorfismo* (posee un morfismo inverso). Las categorías abelianas de la próxima subsección, en particular A-Mod y Mod-A, son balanceadas.

Definición 2.47. Una **categoría** C es **aditiva** si cumple las siguientes condiciones:

(a) Los conjuntos de morfismos $\mathrm{Hom}_{\mathsf{C}}(A,B)$ son *grupos abelianos* y la composición de morfismos es "bilineal":

$$h(f+g) = hf + hg, \qquad (h+k)f = hf + kf,$$

toda vez que $f,g \in \mathrm{Hom}_{\mathsf{C}}(A,B)$ y $h,k \in \mathrm{Hom}_{\mathsf{C}}(B,C)$.

(b) Existe un *objeto cero*, denotado $0 \in\in \mathsf{C}$. Entonces $\mathrm{Hom}_{\mathsf{C}}(A,0) = \mathrm{Hom}_{\mathsf{C}}(0,B) = 0$ en Ab para todo $A,B \in\in \mathsf{C}$.

(c) Para todo $A,B \in\in \mathsf{C}$, existe una **suma directa** $\underline{A \oplus B} \in\in \mathsf{C}$, dotado de 4 morfismos $i_1 \in \mathrm{Hom}_{\mathsf{C}}(A, A\oplus B)$, $i_2 \in \mathrm{Hom}_{\mathsf{C}}(B, A\oplus B)$, $p_1 \in \mathrm{Hom}_{\mathsf{C}}(A\oplus B, A)$ y también $p_2 \in \mathrm{Hom}_{\mathsf{C}}(A\oplus B, B)$, como sigue:

$$A \underset{p_1}{\overset{i_1}{\rightleftarrows}} A \oplus B \underset{p_2}{\overset{i_2}{\leftrightarrows}} B$$

que cumplen las relaciones (1.4b):

$$p_1 i_1 = 1_A, \quad p_1 i_2 = 0, \quad p_2 i_1 = 0, \quad p_2 i_2 = 1_B, \quad i_1 p_1 + i_2 p_2 = 1_{A\oplus B}.$$

El Lema 1.34 muestra que *la categoría A-Mod es aditiva*, usando la suma directa de A-módulos definido en el capítulo anterior.

El **núcleo** de un A-homomorfismo $f \in \mathrm{Hom}_A(M,N)$ es $K = \underline{\ker f} := \{x \in M : f(x) = 0\}$. En el espíritu de la teoría de categorías, hay que mencionar también la inyección $i\colon K \hookrightarrow M$, que es un monomorfismo en A-Mod.[15] Para ser estricto, el núcleo de f es el par (K,i). (Los puristas dirían que el monomorfismo i es el núcleo de f, ya que K no es más que el dominio de este monomorfismo.[16]

El concepto "dual" al núcleo es el llamado conúcleo. El **conúcleo** de un A-homomorfismo $f \in \mathrm{Hom}_A(M,N)$ es $L = \underline{\mathrm{coker}\, f} := N/f(M)$, el módulo cociente de N por la imagen de f. Si $p\colon M \twoheadrightarrow M/N$ es el A-homomorfismo cociente, el cual es un epimorfismo en A-Mod, también se puede considerar el par (L,p) como el conúcleo de f.

Un A-homomorfismo f es inyectivo si y sólo si su núcleo es 0, y f es sobreyectivo si y sólo si su conúcleo es 0. En general, los A-homomorfismos $i\colon K \to M$ y $p\colon N \to L$ tienen la caracterización siguiente.

Lema 2.48. *Sea $f \in \mathrm{Hom}_A(M,N)$ un homomorfismo de A-módulos, $K := \ker f$. La inyección $i\colon K \hookrightarrow M$ cumple las siguientes propiedades:*

[15] En adelante, se usará las flechas $\hookrightarrow$ ó $\rightarrowtail$ para denotar un *monomorfismo* y la flecha $\twoheadrightarrow$ para denotar un *epimorfismo*.

[16] Quizás este es un buen momento para mencionar *la ideología de las flechas*, según la cual toda discusión categórica puede formularse en términos de morfismos solamente. Un objeto puede representarse por su morfismo idéntico j, que cumple $jf = f$, $gj = g$ toda vez que jf y gj están definidos. Esto no pasa de ser un juego entretenido, pero deja un mensaje: los morfismos son indispensables, los objetos sólo son convenientes.

(a) $f \circ i = 0$*;*

(b) Si $g \in \mathrm{Hom}_A(R,M)$ *es tal que* $f \circ g = 0$*, entonces existe un A-homomorfismo único* $g' \in \mathrm{Hom}(R,K)$ *tal que* $i \circ g' = g$*. (Se dice que* g ***factoriza*** *a través del núcleo de* f*.)*

Sea $L := \operatorname{coker} f$*. La sobreyección* $p\colon N \twoheadrightarrow L$ *cumple las siguientes propiedades:*

(c) $p \circ f = 0$*;*

(d) Si $h \in \mathrm{Hom}_A(N,S)$ *es tal que* $h \circ f = 0$*, entonces existe un A-homomorfismo único* $h' \in \mathrm{Hom}(L,S)$ *tal que* $h' \circ p = h$*. (Se dice que* h ***factoriza*** *a través del conúcleo de* f*.)*

Las factorizaciones (b) y (d) se resumen en las siguientes diagramas, en donde *una flecha quebrada indica un morfismo cuya existencia es consecuencia de una afirmación*:

(2.10)

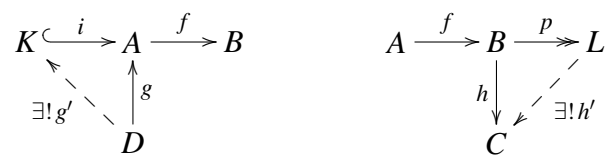
Demostración. Ad (a, c): De la definición de núcleo y conúcleo, es evidente que $f \circ i = 0$ en $\mathrm{Hom}_A(K,N)$ y que $p \circ f = 0$ en $\mathrm{Hom}_A(M,L)$.

Ad (b): Para todo $y \in R$, es $f(g(y)) = 0$, así que $g(y) \in \ker f = K$. Defínase $g'\colon R \to K$ por $g'(y) = g(y)$. Es evidente que $i \circ g' = g$. Si $g''\colon R \to K$ es tal que $i \circ g'' = i \circ g$, entonces $g'' = g'$ porque i es un monomorfismo; esto establece la unicidad de g'.

Ad (d): La condición $h \circ f = 0$ dice que $h(f(M)) = 0 \subseteq S$. La función $h'\colon L \to S$ dada por $h'(y + f(M)) := h(y)$ es entonces un A-homomorfismo bien definido, Si $h''\colon L \to S$ es tal que $h'' \circ p = h' \circ p$, entonces $h'' = h'$ porque p es un epimorfismo; luego h' es único. □

La dualidad (en el sentido categórico) de las propiedades de núcleo y conúcleo se ve al redibujar (2.10) sin nombrar los objetos ni los morfismos (con una reflexión derecha a izquierda en el segundo diagrama):

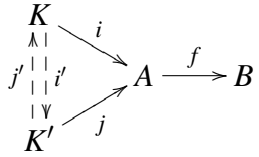
Definición 2.49. En una categoría aditiva C, un **núcleo** de un morfismo $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$ es un par (K,i), donde $K \in\in \mathsf{C}$ y $i \in \mathrm{Hom}_{\mathsf{C}}(K,A)$ es un monomorfismo, tal que $fi = 0$ y cada $g \in \mathrm{Hom}_{\mathsf{C}}(D,A)$ que cumple $fg = 0$ factoriza a través de i. Un *conúcleo* de f es un par (L,p), donde $L \in\in \mathsf{C}$ y $p \in \mathrm{Hom}_{\mathsf{C}}(B,L)$ es un epimorfismo, tal que $pf = 0$ y cada $h \in \mathrm{Hom}_{\mathsf{C}}(B,C)$ que cumple $hf = 0$ factoriza a través de p:



(2.11)

Una categoría aditiva C es **preabeliana** si cada morfismo $f \in \mathrm{Mor}(\mathsf{C})$ posee un núcleo y un conúcleo.

En general, un núcleo de f en este sentido categórico no es único. Pero si (K,i) y (K',j) son dos núcleos de f, hay morfismos únicos $j' : K' \to K$ y $i' : K \to K'$, ofrecidos por (2.11), tales que $j'i = j$, $i'j = i$. En consecuencia, $j'i'j = j$ y también $i'j'i = i$; como i y j son monomorfismos, se concluye que $j'i' = 1_K$ y $i'j' = 1_{K'}$, de modo que $i' \in \mathrm{Hom}_{\mathsf{C}}(K,K')$ es un *isomorfismo*:



Luego, los objetos K y K' son isomorfos, mediante un isomorfismo i' unívocamente determinado por los morfismos i, j. En resumen, un núcleo de f *queda determinado hasta un isomorfismo único*. Dicho de otro modo, *el núcleo de f es esencialmente único*.

De la misma manera, un conúcleo de f, si existe, es esencialmente único.

En las categorías "concretas" Ab, A-Mod, Mod-A, en donde hay una noción "preexistente" de núcleo, cualquier objeto K que es isomorfo a $\ker f$ cumple la definición de núcleo en el sentido de la Definición 2.49: el morfismo i es la composición del isomorfismo $K \to \ker f$ con la inclusión $\ker f \hookrightarrow A$. Ahora, quizá, es posible comprender mejor la noción de la equivalencia de categorías: los objetos isomorfos no pueden distinguirse, ni vale la pena distinguirlos.

Hecha esa advertencia, conviene seguir la costumbre ya arraigada de hablar de *el* núcleo y *el* conúcleo de un morfismo. Así se hará en lo sucesivo.

En particular, si una categoría C posee más de un objeto cero, todos los objetos ceros son isomorfos mediante isomorfismos únicos (¿por qué?). Al identificar estos ceros, se obtiene una categoría C' que es equivalente a C (¿por qué?) pero posee un solo objeto cero. En adelante se asumirá, sin perder generalidad, que en una categoría aditiva el objeto 0 es único.

► La última propiedad deseable de las categorías de módulos requiere una breve explicación. Sea $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$ un morfismo en una categoría preabeliana C. Considérese el diagrama siguiente:

$$\begin{array}{ccccccc} \ker f & \xrightarrow{\ i\ } & A & \xrightarrow{\ f\ } & B & \xrightarrow{\ p\ } & \mathrm{coker}\, f \\ & & \downarrow{\scriptstyle q'} & \searrow^{g} & \uparrow{\scriptstyle j} & & \\ \mathrm{coim}\, f & = & \mathrm{coker}\, i & \xrightarrow{\ \bar{f}\ } & \ker p & = & \mathrm{im}\, f \end{array} \tag{2.12}$$

La primera fila contiene el morfismo $f : A \to B$, su núcleo $(\ker f, i)$ y su conúcleo $(\mathrm{coker}\, f, p)$. El núcleo del conúcleo, $(\ker p, j)$, se llama la **imagen** de f. (En la categoría A-Mod, en donde $\mathrm{coker}\, f = B/f(A)$, es evidente que $\mathrm{coker}\, p$ es isomorfo a $f(A)$: de ahí el nombre "imagen".) Dualmente, el conúcleo del núcleo $(\mathrm{coker}\, i, q')$ se llama la **coimagen** de f.

Ahora bien: como $pf = 0$ y $(\ker p, j)$ es el núcleo de p, hay un único morfismo $g : A \to \ker p$ tal que $jg = f$. Además, $jgi = fi = 0$, luego $gi = 0$ porque j es un monomorfismo.

Como $gi = 0$ y $(\operatorname{coker} i, q')$ es el conúcleo de i, hay un único morfismo $\bar{f}\colon \operatorname{coker} i \to \ker p$ tal que $\bar{f}q' = g$.

En breve: el diagrama (2.12) *conmuta* y muestra la existencia de un *morfismo canónico* $\bar{f}\colon \operatorname{coim} f \to \operatorname{im} f$ tal que $f = j\bar{f}q'$, donde q' es un epimorfismo y j es un monomorfismo. Esta es la **descomposición canónica** del morfismo f.

En la categoría A-Mod, en donde se puede (re)definir $\operatorname{coim} f := A/\ker f$, se puede hacer una afirmación más fuerte: por el Corolario 1.31, el factor central $\bar{f}$ de la descomposición canónica es un *isomorfismo*. Esto conduce a la definición siguiente, cuya importancia ha sido enfatizado por Grothendieck.[17]

Definición 2.50. Una **categoría abeliana** es una categoría aditiva C en donde

- cada morfismo $f \in \operatorname{Hom}_{\mathsf{C}}(A,B)$ posee un núcleo y un conúcleo;
- para cada $f \in \operatorname{Hom}_{\mathsf{C}}(A,B)$, el morfismo canónico $\bar{f}\colon \operatorname{coker}(\ker f) \to \ker(\operatorname{coker} f)$ es un isomorfismo.

El Corolario 1.31 ahora dice que A-Mod es una categoría abeliana. Por razones que deben de ser obvias, las categorías Mod-A y Ab también son abelianas. Sin embargo, en vista del Ejemplo 2.44 y el Lema siguiente, la categoría de anillos An no es abeliana.

Si C es una categoría abeliana, su categoría opuesta C° es también abeliana (se intercambian los núcleos y conúcleos).

Lema 2.51. *Una categoría abeliana es balanceada, es decir, cada morfismo que es simultáneamente mónico y épico es un isomorfismo.*

Demostración. Si C es preabeliana y si $f \in \operatorname{Hom}_{\mathsf{C}}(A,B)$ es a la vez un monomorfismo y un epimorfismo, entonces $\ker f = 0$ y $\operatorname{coker} f = 0$, de modo que $\operatorname{coker} i = (A, 1_A)$ y $\ker p = (B, 1_B)$ en (2.12) y por ende $\bar{f} = f$.

Luego, si C es abeliana, entonces $f = \bar{f}$ donde $\bar{f}$ es un isomorfismo. □

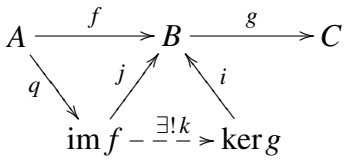
En una categoría abeliana, el isomorfismo $\bar{f}\colon \operatorname{coim} f \to \operatorname{im} f$ permite identificar la coimagen con $\operatorname{im} f$. (Una vez más, hay que recordar que el núcleo y el conúcleo, y también la imagen y la coimagen, están determinados sólo hasta isomorfismo.) Esto permite simplificar el diagrama (2.12) del modo siguiente:

$$\begin{array}{ccccccc} \ker f & \xrightarrow{\ i\ } & A & \xrightarrow{\ f\ } & B & \xrightarrow{\ p\ } & \operatorname{coker} f \\ & & & \searrow^{q} \quad \nearrow_{j} & & & \\ & & & \operatorname{im} f & & & \end{array} \tag{2.13}$$

[17] Alexander Grothendieck (n. 1928), uno de los más grandes matemáticos del siglo XX, revolucionó la geometría algebraica entre 1955 y 1970, mediante la aplicación despiadada de los métodos abstractos. Su obra principal, *Éléments de Géométrie Algebrique*, quedó incompleto cuando abandonó las matemáticas en 1970 (aunque siguió escribiendo manuscritos hasta su desaparición en 1991).

donde $q := \bar{f}q' : A \to \operatorname{im} f$ es un epimorfismo y $j\colon \operatorname{im} f \to B$ es un monomorfismo. En este orden de cosas, $(\operatorname{im} f, j)$ sigue siendo el núcleo de p, pero ahora $(\operatorname{im} f, q)$ es el conúcleo de i. Este diagrama proporciona una factorización de f a través de su imagen, la cual se llama la "factorización mono-epi" del morfismo dado.[18]

Definición 2.52. En una categoría abeliana C, sean $f \in \operatorname{Hom}_{\mathsf{C}}(A,B)$ y $g \in \operatorname{Hom}_{\mathsf{C}}(B,C)$ un par de morfismos que cumplen $gf = 0$. Entonces hay un morfismo canónico $k\colon \operatorname{im} f \to \ker g$ tal que el siguiente diagrama conmuta:



donde $(\ker g, i)$ es el núcleo de g. En efecto, como $gjq = gf = 0$ y q es épico, se obtiene $gj = 0$, por lo tanto j factoriza a través de $\ker g$.

Se dice que el diagrama $A \xrightarrow{f} B \xrightarrow{g} C$ es **exacto en** B si $k\colon \operatorname{im} f \to \ker g$ es un isomorfismo. En términos menos rigurosos (pero inobjetables en la categoría A-Mod) se dice que este diagrama es exacto si $\underline{\operatorname{im} f = \ker g}$.

Definición 2.53. En una categoría abeliana C, una **sucesión exacta** es un juego de morfismos consecutivos:

$$\cdots \longrightarrow A_{i-1} \xrightarrow{f_{i-1}} A_i \xrightarrow{f_i} A_{i+1} \longrightarrow \cdots \tag{2.14}$$

tales que $\underline{\operatorname{im} f_{i-1} = \ker f_i}$ para cada índice i. (El conjunto índice puede ser $\mathbb{Z}$ o cualquier subintervalo de $\mathbb{Z}$: los casos $\mathbb{N}$, $-\mathbb{N}$ y $\{0,1,2,3,4\}$ son de particular importancia.)

Lema 2.54. *En una categoría abeliana:*

(a) La sucesión $0 \longrightarrow A \xrightarrow{f} B$ *es exacta si y sólo si* f *es un monomorfismo.*

(b) La sucesión $B \xrightarrow{g} C \longrightarrow 0$ *es exacta si y sólo si* g *es un epimorfismo.*

(c) La sucesión $0 \longrightarrow A \xrightarrow{h} B \longrightarrow 0$ *es exacta si y sólo si* h *es un isomorfismo.*

(d) La sucesión $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C$ *es exacta si y sólo si* $gf = 0$ *y* $(A,f) \simeq \ker g$.

(e) La sucesión $A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *es exacta si y sólo si* $gf = 0$ *y* $(C,g) \simeq \operatorname{coker} f$.

Demostración. Las afirmaciones (a) y (b) son evidentes. Luego (c) es una consecuencia del Lema 2.51.

Ad (d): Si $gf = 0$ y $(A,f) \simeq (\ker g, i)$ es un núcleo de g, entonces f es un monomorfismo: por tanto, la sucesión es exacta en A. Además, en la factorización mono-epi $A \xrightarrow{q} \operatorname{im} f \xrightarrow{j} B$

[18] Algunos autores definen una categoría abeliana como una preabeliana en donde cada morfismo admite una factorización mono-epi (única hasta isomorfismo único) tal que el diagrama (2.13) conmuta.

de f, el factor q es un isomorfismo porque f ya es un monomorfismo. Esto dice que $(\operatorname{im} f, j) \simeq (\ker g, i)$, así que el morfismo canónico $k\colon \operatorname{im} f \to \ker g$ es un isomorfismo; por ende, la sucesión es exacta en B.

Inversamente, si la sucesión es exacta en A y en B, entonces f es un monomorfismo y $gf = 0$. Además, si $h\colon D \to B$ es un morfismo tal que $gh = 0$, entonces $h = il$ donde $l\colon D \to \ker g$. Luego $h = jm$ donde $(\operatorname{im} f, j) \simeq (\ker g, i)$ y $m\colon D \to \operatorname{im} f$. Finalmente, $f = jq$ donde q es un isomorfismo porque f es mónico, así que $h = fq^{-1}m$ donde $q^{-1}m\colon D \to A$. Esto muestra que $(A, f) \simeq (\ker g, i)$.

Ad(e): Análoga a la demostración de (d), por dualidad categórica. □

Definición 2.55. Una **sucesión exacta corta** (SEC) en una categoría abeliana es una sucesión de la forma:

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0 \tag{2.15}$$

en donde f es un *monomorfismo*, g es un *epimorfismo* y $\underline{\ker g = \operatorname{im} f}$.

Obsérvese que la sucesión

$$0 \longrightarrow \ker f \xrightarrow{i} A \xrightarrow{f} B \xrightarrow{p} \operatorname{coker} f \longrightarrow 0$$

es exacta, pero no es corta (por tener 6 objetos en vez de 5).

Definición 2.56. La categoría SEC-C de *sucesiones exactas cortas en* C tiene como objetos las SEC (2.15). Un morfismo entre dos SEC es un triplete de morfismos (φ, ψ, χ) en $\operatorname{Mor}(\mathsf{C})$ tales que el siguiente diagrama conmuta:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \varphi\downarrow & & \psi\downarrow & & \chi\downarrow & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0, \end{array}$$

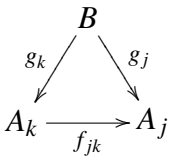
esto es, $\psi f = f'\varphi$ y $\chi g = g'\psi$. Es fácil comprobar que SEC-C es una categoría aditiva.

2.4 Propiedades universales

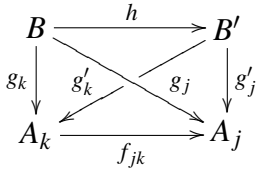
El formalismo de categorías ofrece dos ventajas principales. Primero, permite obviar la distinción entre objetos isomorfos que no son idénticos. Segundo, ofrece un contexto adecuado para el concepto de *universalidad* en matemáticas.

Definición 2.57. Sea J un conjunto parcialmente ordenado y sea J la categoría pequeña asociada, según el Ejemplo 2.11. Sea $\mathcal{F}\colon \mathsf{J}^\circ \to \mathsf{C}$ un *funtor contravariante*. Concretamente, esto es una familia de objetos $\{A_j = \mathcal{F}j : j \in J\}$ en C, junto con una familia de morfismos $\{f_{jk} \in \operatorname{Hom}_{\mathsf{C}}(A_k, A_j) : j \le k\}$ tales que $f_{kk} = 1_{A_k}$ para cada k y $\underline{f_{jk}f_{kl} = f_{jl}}$ toda vez que $j \le k \le l$.

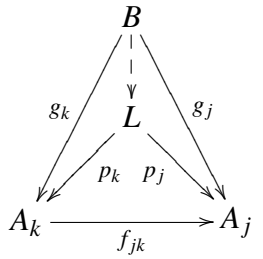
Un **abanico**[19] sobre $\mathcal{F}$ en la categoría C es un objeto $B \in\in \mathsf{C}$ junto con una familia de morfismos $\{\, g_j \in \mathrm{Hom}_{\mathsf{C}}(B, A_j) : j \in J \,\}$ que satisfacen $f_{jk} g_k = g_j$ toda vez que $j \leq k$:



Los abanicos sobre $\mathcal{F}$ en C forman los objetos de una categoría. Un morfismo de abanicos $(B, \{g_k\}) \to (B', \{g'_k\})$ es algún $h \in \mathrm{Hom}_{\mathsf{C}}(B, B')$ tal que los siguientes diagramas conmutan toda vez que $j \leq k$:



Un **límite** de $\mathcal{F}$ en C es un *objeto terminal* $(L, \{p_k\})$, si existe, en esta categoría de abanicos.[20] Se escribe $L = \varprojlim_J A_j$ en ese caso (la flecha quebrada denota el morfismo único en $\mathrm{Hom}_{\mathsf{C}}(B, L)$ que hace conmutativo el diagrama):



(2.16)

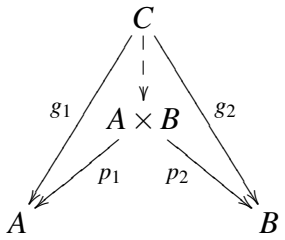
Un límite, si existe, es *esencialmente único*: si $(L', \{p'_k\})$ es otro abanico terminal, entonces hay morfismos únicos $h\colon L' \to L$ y $h'\colon L \to L'$ dados por (2.16), tales que $p_k h = p'_k$ y además $p'_k h' = p_k$ para todo k. Por la unicidad del morfismo $B \to L$ en (2.16), se concluye que h es un isomorfismo con $h^{-1} = h'$.

Antes de explorar la existencia de límites en ciertas categorías, hay que notar una serie de ejemplos que resaltan la gran flexibilidad de esta noción. El primero es concepto fundamental de *producto* en una categoría.

[19] Algunos autores lo llaman **cono** en vez de *abanico*. Pero esto puede confundir con el concepto importante de "cono sobre un morfismo" y además sería inelegante denotar el concepto dual por el vocablo "cocono". MacLane hábilmente evita esa trampa; véase: Saunders MacLane, *Categories for the Working Mathematician*, Springer, New York, 1971. La terminología *abanico* aparece en: Goro Kato, *The Heart of Cohomology*, Springer, Dordrecht, 2006.

[20] Terminología obsoleta: *límite inverso* o bien *límite proyectivo*. También se usa la notación '$\varprojlim$' en lugar de 'lim' simplemente.

Ejemplo 2.58. En el caso $J = \{1,2\}$, un conjunto de dos elementos con un orden trivial (no se impone $1 \leq 2$), entonces $\mathsf{J}^\circ = \mathsf{J}$ y un funtor $\mathcal{F}\colon \mathsf{J} \to \mathsf{C}$, covariante o contravariante, es simplemente un par (ordenado) de objetos $A, B \in\in \mathsf{C}$. En este caso el límite de $\mathcal{F}$ es un **producto** de A y B: este es un objeto $\underline{A \times B} \in\in \mathsf{C}$, junto con dos morfismos $p_1 : A \times B \to A$, $p_2 : A \times B \to B$:



La *propiedad universal* del producto sigue del diagrama: dados dos morfismos $g_1 : C \to A$ y $g_2 : C \to B$, hay un único morfismo $g : C \to A \times B$ tal que $p_1 g = g_1$ y $p_2 g = g_2$.

En la categoría Set, este es el **producto cartesiano** de dos conjuntos: las **proyecciones** $p_1 : X \times Y \to X$, $p_2 : X \times Y \to Y$ son las aplicaciones $p_1(x,y) := x$, $p_2(x,y) := y$; además, dadas dos aplicaciones $g_1 : Z \to X$ y $g_2 : Z \to Y$, se define $g : Z \to X \times Y : z \mapsto (g_1(z), g_2(z))$. Esta es la *única* aplicación tal que $p_1 \circ g = g_1$ y $p_2 \circ g = g_2$, evidentemente.

En la categoría Gr, $G \times H$ es el **producto directo** de los grupos G y H.

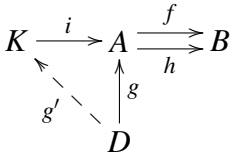
En las categorías Ab, A-Mod y Mod-A (de hecho, en cualquier categoría abeliana) la **suma directa** $A \oplus B$ de dos objetos A y B es un producto, en este sentido categórico.

Ejemplo 2.59. Sea J un conjunto cualquiera con un orden trivial (es decir $j \leq k$ sólo si $j = k$). Entonces un funtor $\mathcal{F}\colon \mathsf{J} \to \mathsf{C}$ es una colección de objetos $\{A_j \in\in \mathsf{C} : j \in J\}$. En este caso el límite de $\mathcal{F}$ define **productos** $\prod_{j\in J} A_j$ con conjunto índice J. Las proyecciones $p_k : \left(\prod_{j\in J} A_j\right) \to A_k$ son las "proyecciones coordenadas" cuando los objetos A_j son conjuntos (con estructura).

Ejemplo 2.60. Hay límites etiquetados por categorías pequeñas J que no son conjuntos parcialmente ordenados (al permitir más de un morfismo entre dos objetos). Un buen ejemplo es la categoría pequeña $\bullet \rightrightarrows *$, en donde $\mathrm{Hom}_{\mathsf{J}}(\bullet, *)$ consta de dos morfismos distintos. Un funtor $\mathcal{F}\colon \mathsf{J}^\circ \to \mathsf{C}$ es un par de morfismos paralelos:

$$A \underset{h}{\overset{f}{\rightrightarrows}} B. \tag{2.17}$$

Un abanico sobre $\mathcal{F}$ es un objeto D con un morfismo $g\colon D \to A$ tal que $fg = hg$. En este caso, el límite de $\mathcal{F}$ es un par (K,i), donde $i \in \mathrm{Hom}_{\mathsf{C}}(K,A)$ tal que: (a) $fi = hi$; y (b) si $g \in \mathrm{Hom}_{\mathsf{C}}(D,A)$ es tal que $fg = hg$, entonces hay un único morfismo $g' \in \mathrm{Hom}_{\mathsf{C}}(D,K)$ tal que $ig' = g$:



Este par (K,i), si existe, se llama el **igualador** de los dos morfismos $f,h\colon A\to B$.

Si C es una categoría aditiva y $h=0$ es el morfismo nulo en $\mathrm{Hom}_{\mathsf{C}}(A,B)$, es evidente que el igualador de f y 0 es el **núcleo** de f. La condición (b) del Lema 2.48 es la *propiedad universal del núcleo*.

Ejemplo 2.61. Un conjunto parcialmente ordenado J es un **conjunto dirigido** si para cada par de elementos $j,k\in J$, hay un elemento $l\in J$ tal que $j\le l$ y $k\le l$. (Por ejemplo, un conjunto totalmente ordenado es dirigido.) Sea $\{X_j : j\in J\}$ una familia dirigida de conjuntos tales que $X_k\subseteq X_j$ si y sólo si $j\le k$; entonces las inclusiones $\{X_k\hookrightarrow X_j : j\le k\}$ definen un funtor contravariante $\mathcal{F}\colon \mathsf{J}^\circ\to\mathsf{Set}$. En este caso, resulta que $\lim_J X_j=\bigcap_{j\in J}X_j$ es la *intersección* de estos conjuntos.

Ejemplo 2.62. Sea J el conjunto $\{a,b,c\}$, parcialmente ordenado por $c\le a$, $c\le b$. Un funtor $\mathcal{F}\colon \mathsf{J}^\circ\to\mathsf{C}$ consta de tres objetos A,B,C y dos morfismos $f\colon A\to C$ y $g\colon B\to C$:

$$\begin{array}{ccc} & & B \\ & & \downarrow{\scriptstyle g} \\ A & \xrightarrow{f} & C \end{array} \tag{2.18a}$$

Un abanico sobre $\mathcal{F}$ es un triplete (Z,h,k) que forma un **cuadrado conmutativo**:

$$\begin{array}{ccc} Z & \xrightarrow{h} & B \\ {\scriptstyle k}\downarrow & & \downarrow{\scriptstyle g} \\ A & \xrightarrow{f} & C \end{array}$$

En este caso, un límite de $\mathcal{F}$ es un triplete (X,p,q):

$$\begin{array}{ccccc} Z & & \xrightarrow{\quad h\quad} & & \\ & \searrow^{l} & & & \\ & & X & \xrightarrow{p} & B \\ {\scriptstyle k}\searrow & & {\scriptstyle q}\downarrow & & \downarrow{\scriptstyle g} \\ & & A & \xrightarrow{f} & C \end{array} \tag{2.18b}$$

tal que: con $X\in\in\mathsf{C}$,

(a) los morfismos $p\colon X\to B$, $q\colon X\to A$ cumplen $gp=fq$; y

(b) dados (Z,h,k) con $Z\in\in\mathsf{C}$, $h\colon Z\to B$, $k\colon Z\to A$ que satisfacen $gh=fk$, hay un único morfismo $l\colon Z\to X$ tal que $pl=h$ y $ql=k$.

Este (X,p,q), si existe, se llama el **pullback**[21] del diagrama (2.18a). Para los morfismos, se dice que p es el pullback de f por g y también que q es el pullback de g por f.

[21] Los franceses hablan de *image inverse* o bien *diagramme cartésien* u otros términos aun menos elegantes. Afortunadamente, el anglicismo *pullback* (una palabra, sin guión) ha sido asimilado al castellano peninsular. Cuenta el escritor Paul Theroux que en su primera visita a Buenos Aires visitó una noche a Jorge Luis Borges, ya viejo y ciego, quien lo rogó que leyera en inglés durante varias horas. A cada rato Borges lo interrumpía con risa, exclamando: *You can't say that in Spanish!*

Lema 2.63. *En la categoría A-Mod, todos los límites existen: es decir, si J es un conjunto parcialmente ordenado y si $\mathcal{F}\colon \mathsf{J}^\circ \to A\text{-}\mathsf{Mod}$ es un funtor con $M_j := \mathcal{F}j$ para $j \in J$, entonces hay un A-módulo L, esencialmente único, tal que $L = \lim_J M_j$.*

Demostración. Sea $\prod_{j\in J} M_j$ el producto directo de todos los A-módulos M_j. Defínase un A-submódulo L de este producto por

$$L := \Big\{ (x_j)_j \in \prod_{j\in J} M_j : f_{kl}(x_l) = x_k \text{ toda vez que } k \le l \Big\}. \tag{2.19}$$

Sean $p_k\colon L \to M_k$, para $k \in J$, las restricciones a L de las proyecciones coordenadas del producto directo, es decir, $p_k\big((x_j)_j\big) := x_k$ para $(x_j)_j \in L$. Entonces

$$f_{kl} \circ p_l\big((x_j)_j\big) = f_{kl}(x_l) = x_k = p_k\big((x_j)_j\big) \quad \text{para todo} \quad (x_j)_j \in L,$$

así que $(L, \{p_k\})$ es un abanico sobre $\mathcal{F}$. Si $(N, \{g_k\})$ es otro abanico y si $y \in N$, entonces $f_{kl}(g_l(y)) = g_k(y)$ toda vez que $k \le l$; luego $(g_j(y))_j \in L$. El A-homomorfismo $h\colon N \to L$ definido por $h(y) := (g_j(y))_j$ es evidentemente el único A-homomorfismo tal que $p_k \circ h = g_k$ para todo $k \in J$. □

La misma demostración establece la existencia de límites cualesquiera en categorías que admiten productos arbitrarias y un concepto análoga al de "submódulo". Por ejemplo, en la categoría Set se puede formar el *producto cartesiano* de una familia de conjuntos $\{X_j : j \in J\}$ y definir $L := \lim_J X_j$ como la *parte* de $\prod_{j\in J} X_j$ cuyos coordenadas cumplen $f_{kl}(x_l) = x_k$ cuando $k \le l$.

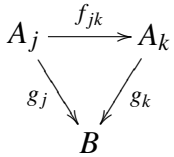
Por ejemplo, dadas dos aplicaciones de conjuntos $f\colon X \to Z$ y $g\colon Y \to Z$, se definido el **producto fibrado** de X, Y sobre Z como un pullback:

$$X \times_Z Y := \{ (x,y) \in X \times Y : f(x) = g(y) \text{ en } Z \}.$$

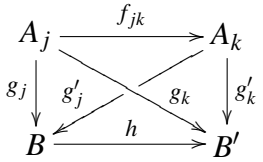
► El concepto dual de un límite es un *colímite*, obtenido de las definiciones anteriores por reversión de flechas.

Definición 2.64. Sea J un conjunto parcialmente ordenado y sea $\mathcal{F}\colon \mathsf{J} \to \mathsf{C}$ un *funtor covariante*. Concretamente, esto es una familia de objetos $\{A_j = \mathcal{F}j : j \in J\}$ en C, junto con una familia de morfismos $\{f_{jk} \in \mathrm{Hom}_{\mathsf{C}}(A_j, A_k) : j \le k\}$ tales que $f_{kk} = 1_{A_k}$ para cada k y $f_{kl}f_{jk} = f_{jl}$ toda vez que $j \le k \le l$.

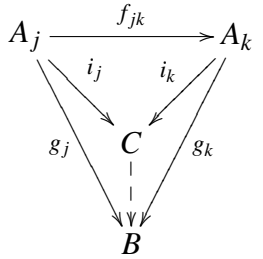
Un **coabanico** sobre $\mathcal{F}$ en la categoría C es un objeto $B \in\in \mathsf{C}$ junto con una familia de morfismos $\{g_j \in \mathrm{Hom}_{\mathsf{C}}(A_j, B) : j \in J\}$ que satisfacen $g_k f_{jk} = g_j$ toda vez que $j \le k$:



Los coabanicos sobre $\mathcal{F}$ en C forman los objetos de una categoría. Un morfismo de coabanicos $(B,\{g_k\}) \to (B',\{g'_k\})$ es algún $h \in \mathrm{Hom}_{\mathsf{C}}(B,B')$ tal que los siguientes diagramas conmutan toda vez que $j \le k$:



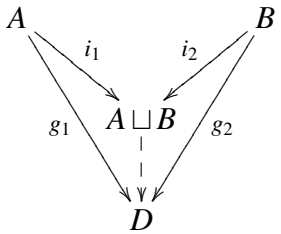
Un **colímite** de $\mathcal{F}$ en C es un *objeto inicial* $(C,\{i_k\})$, si existe, en esta categoría de coabanicos.[22] Se escribe $C = \underline{\mathrm{colim}_J A_j}$ en ese caso (la flecha quebrada denota el morfismo único en $\mathrm{Hom}_{\mathsf{C}}(C,B)$ que hace conmutativo el diagrama):



(2.20)

Un colímite, si existe, es esencialmente único: si $(C',\{i'_k\})$ es otro coabanico inicial, entonces hay morfismos únicos $h\colon C \to C'$ y $h'\colon C' \to C$ dados por (2.20), tales que $hi_k = i'_k$ y además $h'i'_k = i_k$ para todo k. Por la unicidad del morfismo $C \to B$ en (2.20), se concluye que h es un isomorfismo con $h^{-1} = h'$.

Ejemplo 2.65. En el caso $J = \{1,2\}$ con orden trivial, $\mathcal{F}\colon \mathsf{J} \to \mathsf{C}$ un par (ordenado) de objetos $A,B \in\in \mathsf{C}$, el colímite de $\mathcal{F}$ es un **coproducto**[23] de A y B: este es un objeto $\underline{A \sqcup B} \in\in \mathsf{C}$, junto con dos morfismos $i_1 : A \to A \sqcup B$, $i_2\colon B \to A \sqcup B$:



La *propiedad universal* del coproducto sigue del diagrama: dados dos morfismos $g_1 : A \to D$ y $g_2\colon B \to D$, hay un único morfismo $g\colon A \sqcup B \to D$ tal que $gi_1 = g_1$ y $gi_2 = g_2$.

[22] Terminología obsoleta: *límite directo* o bien *límite inyectivo*. También se usa la notación '$\varinjlim$' en lugar de 'colim'.

[23] El término *coproducto*, al igual que *producto*, tiene varias acepciones. En un grupo, un anillo o un álgebra, la operación de multiplicación también se llama "producto" aunque no coincide con la noción de producto en el sentido categórico de esta sección. Dualmente, hay una estructura algebraica llamada coálgebra que posee una operación de "coproducto" en otro sentido; algunos lo llaman "comultiplicación".

En la categoría Set, esta es la **unión disjunta** $X \uplus Y$ de dos conjuntos X, Y. Formalmente, se considera el producto cartesiano $W := (X \cup Y) \times \{0,1\}$ y se define

$$X \uplus Y := (X \times \{0\}) \cup (Y \times \{1\})$$

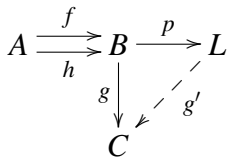
como parte de W. Ahora bien, esta determinación de $X \uplus Y$ es esencialmente único: cualquier otro conjunto que es biyectiva con éste servirá el mismo propósito. Por ejemplo, si $X \cap Y = \emptyset$, se puede identificar $X \uplus Y$ con $X \cup Y$.

Las **inyecciones** $i_1 : X \to X \uplus Y$, $i_2 : Y \to X \uplus Y$ son las aplicaciones $i_1(x) := (x,0)$, $i_2(y) := (y,1)$; además, dadas dos aplicaciones $g_1 : X \to Z$ y $g_2 : Y \to Z$, se define $g : X \uplus Y \to Z$ por $g(x,0) := g_1(x)$, $g(y,1) := g_2(y)$. Esta es la *única* aplicación tal que $g \circ i_1 = g_1$ y $g \circ i_2 = g_2$.

Ejemplo 2.66. Sea J un conjunto cualquiera con un orden trivial. Un funtor $\mathcal{F} : \mathsf{J} \to \mathsf{C}$ es simplemente una colección de objetos $\{A_j \in\in \mathsf{C} : j \in J\}$. Ahora el colímite de $\mathcal{F}$ es un **coproducto** $\bigsqcup_{j\in J} A_j$ con conjunto índice J. En el caso $\mathsf{C} = \mathsf{Set}$, este es la *unión disjunta* $\biguplus_{j\in J} A_j$ de conjuntos.

Ejemplo 2.67. En una categoría *aditiva*, la **suma directa** $A \oplus B$ de dos objetos es un producto y un coproducto, a la vez. Los morfismos p_1, p_2, i_1, i_2 de la definición de suma directa son los morfismos canónicos asociados al producto y al coproducto, respectivamente.[24]

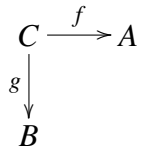
Ejemplo 2.68. Sea J la categoría pequeña $\bullet \rightrightarrows *$, del Ejemplo 2.60. Un funtor covariante $\mathcal{F} : \mathsf{J} \to \mathsf{C}$ es también un par de morfismos paralelos (2.17). Un coabanico sobre $\mathcal{F}$ es un objeto C con un morfismo $g : B \to C$ tal que $gf = gh$. El colímite de $\mathcal{F}$ es un par (L,p), donde $p \in \mathrm{Hom}_{\mathsf{C}}(B,L)$ tal que: (a) $pf = ph$; y (b) si $g \in \mathrm{Hom}_{\mathsf{C}}(B,C)$ es tal que $gf = gh$, entonces hay un único morfismo $g' \in \mathrm{Hom}_{\mathsf{C}}(L,C)$ tal que $g'p = g$:



Este par (L,q), si existe, se llama el **coigualador** de los dos morfismos $f, h : A \to B$.

Si C es una categoría aditiva y $h = 0$ es el morfismo nulo en $\mathrm{Hom}_{\mathsf{C}}(A,B)$, es evidente que el coigualador de f y 0 es el **conúcleo** de f. La condición (d) del Lema 2.48 es la *propiedad universal del conúcleo*.

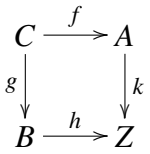
Ejemplo 2.69. Sea J el conjunto $\{a,b,c\}$, parcialmente ordenado por $c \le a$, $c \le b$. Un funtor covariante $\mathcal{F} : \mathsf{J} \to \mathsf{C}$ consta de tres objetos A, B, C y dos morfismos $f : C \to A$ y $g : C \to B$:



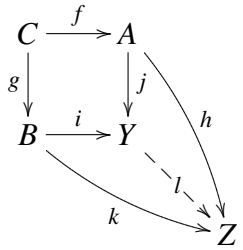
(2.21a)

[24] Algunos autores llaman *biproducto* a un producto que es también un coproducto.

Un coabanico sobre $\mathcal{F}$ es un triplete (Z,h,k) que forma un *cuadrado conmutativo*:



En este caso, un límite de $\mathcal{F}$ es un triplete (Y,i,j):



(2.21b)

tal que: con $Y \in\in \mathsf{C}$,

(a) los morfismos $i\colon B \to Y$, $j\colon A \to Y$ cumplen $jf = ig$; y

(b) dados (Z,h,k) con $Z \in\in \mathsf{C}$, $h\colon A \to Z$, $k\colon B \to Z$ que satisfacen $hf = kg$, hay un único morfismo $l\colon Y \to Z$ tal que $lj = h$ y $li = k$.

Este (Y,i,j), si existe, se llama el **pushout** del diagrama (2.21a). Para los morfismos, se dice que i es el pushout de f por g y también que j es el pushout de g por f.

Lema 2.70. *En la categoría A-Mod, todos los colímites existen: es decir, si J es un conjunto parcialmente ordenado y si $\mathcal{F}\colon \mathsf{J} \to A$-Mod es un funtor con $M_j := \mathcal{F}j$ para $j \in J$, entonces hay un A-módulo N, esencialmente único, tal que $N = \operatorname{colim}_J M_j$.*

Demostración. Sea $\bigoplus_{j\in J} M_j$ la suma directa de todos los A-módulos M_j. Defínase un A-módulo cociente N de esta suma directa por $N := \left(\bigoplus_{j\in J} M_j\right)\big/D$, donde D es el A-submódulo de $\bigoplus_{j\in J} M_j$ generado por $\{\, d_{kl}(x_k) : k < l,\ x_k \in M_k \,\}$, definidos por

$$d_{kl}(x_k) := (y_j)_j \in \bigoplus_{j\in J} M_j, \quad \text{con} \quad \begin{cases} y_j := x_k & \text{si } j = k, \\ y_j := -f_{kl}(x_k) & \text{si } j = l, \\ y_j := 0 & \text{para otros } j. \end{cases}$$

Sea $\eta :\ \bigoplus_{j\in J} M_j \to N$ el A-homomorfismo cociente, sean $i'_k\colon M_k \to \bigoplus_{j\in J} M_j$ las inyecciones canónicas y sean $i_k := \eta \circ i'_k : M_k \to N$, para $k \in J$. Si $x_k \in M_k$ y si $k < l$, entonces

$$i'_k(x_k) - i'_l(f_{kl}(x_k)) = d_{kl}(x_k) \in D,$$

por lo tanto, es $i_k(x_k) = i_l(f_{kl}(x_k))$ en N. Luego $(N, \{i_k\})$ es un coabanico sobre $\mathcal{F}$ en A-Mod. Si $(K, \{g_k\})$ es otro abanico, hay un A-homomorfismo $\psi\colon \bigoplus_{j\in J} M_j \to K$ dado por

$\psi\big((x_j)_j\big) := \sum_{j\in J} g_j(x_j)$. Fíjese que esa es una suma finita, por definición de la suma directa. Ahora

$$\psi(d_{kl}(x_k)) = g_k(x_k) - g_l(f_{kl}(x_k)) = 0 \quad \text{toda vez que} \quad k < l,$$

y en consecuencia ψ se anula sobre el A-submódulo K. Luego hay un único A-homomorfismo $h\colon N \to K$ tal que $h\circ\eta = \psi$. En particular, $h\circ i_k = h\circ\eta\circ i'_k = \psi\circ i'_k = g_k$ para $k\in J$. Luego h es el único A-homomorfismo de N en K tal que $h\circ i_k = g_k$ para todo $k\in J$. □

► Hay un punto de vista alternativa sobre límites y colímites, que aprovecha el Lema de Yoneda.

Definición 2.71. Sea C una categoría cualquiera, sea J una categoría pequeña y escríbase $\widetilde{\mathsf{C}} := \mathsf{Fun}(\mathsf{J},\mathsf{C})$. Para cada objeto $A\in\mathsf{C}$, sea $\Delta A\colon \mathsf{J}\to\mathsf{C}$ el **funtor constante** dado por

$$\begin{aligned} \Delta A(j) &:= A, && \text{para cada } j\in\in \mathsf{J},\\ \Delta A(i\to j) &:= 1_A, && \text{para cada morfismo } (i\to j)\in \mathrm{Mor}(\mathsf{J}). \end{aligned}$$

Si $f\in\mathrm{Hom}_{\mathsf{C}}(A,B)$, defínase la transformación natural $\Delta f\colon \Delta A\to\Delta B$ por $(\Delta f)_j := f$ para cada $j\in\in\mathsf{J}$. Entonces $A\mapsto\Delta A$, $f\mapsto\Delta f$ define un funtor $\Delta\colon\mathsf{C}\to\widetilde{\mathsf{C}}$, llamado el **funtor diagonal** determinado por J.

Si $\mathcal{F}\colon \mathsf{J}^\circ\to\mathsf{C}$ es un funtor contravariante, considérese otro funtor contravariante

$$\widetilde{\mathcal{F}} : \mathsf{C}^\circ \to \mathsf{Set} : A\mapsto \mathrm{Hom}_{\widetilde{\mathsf{C}}}(\Delta A,\mathcal{F}). \tag{2.22a}$$

Este es un *funtor representable* si hay un objeto (esencialmente único, por la discusión después del Lema de Yoneda) $L\in\in\mathsf{C}$ tal que $h_L\simeq\widetilde{\mathcal{F}}$ en $\widetilde{\mathsf{C}}$. En otras palabras, hay una biyección

$$\mathrm{Hom}_{\widetilde{\mathsf{C}}}(\Delta A,\mathcal{F}) \longleftrightarrow h_L(A) = \mathrm{Hom}_{\mathsf{C}}(A,L), \quad \text{para todo} \quad A\in\in\mathsf{C}.$$

En el caso $A=L$, al morfismo $1_L\in\mathrm{Hom}_{\mathsf{C}}(L,L)$ le corresponde una transformación natural $p\colon\Delta L\to\mathcal{F}$ entre funtores de J en C. Esto es, para cada $j\in\in\mathsf{J}$ hay un morfismo $p_j\colon L\to A_j=\mathcal{F}j$ tal que, para cada flecha $j\to k$ en $\mathrm{Mor}_{\mathsf{J}}(j,k)$ con $f_{jk}=\mathcal{F}(j\to k)\in\mathrm{Hom}_{\mathsf{C}}(A_k,A_j)$, vale $f_{jk}p_k = p_j 1_L$, debido a (2.7). En otras palabras, $(L,\{p_k\})$ es un abanico sobre $\mathcal{F}$.

Ahora debe de ser claro que cualquier otro abanico $(B,\{g_k\})$ sobre $\mathcal{F}$ define una transformación natural $g\colon\Delta B\to\mathcal{F}$, a la cual le corresponde un morfismo $h\in\mathrm{Hom}_{\mathsf{C}}(B,L)$. Además, $\Delta h\colon\Delta B\to\Delta L$ es una transformación natural tal que $p\circ\Delta h = (\Delta h)^* p = g$ en $\mathrm{Hom}_{\widetilde{\mathsf{C}}}(\Delta A,\mathcal{F})$; esto significa que $p_j h = g_j$ para cada j, de modo que $(L,\{p_k\})$ es un objeto terminal en la categoría de abanicos sobre $\mathcal{F}$, es decir, el límite de $\mathcal{F}$ en C.

Para resumir: la existencia de un límite para un funtor contravariante $\mathcal{F}\in\mathsf{Fun}(\mathsf{J}^\circ,\mathsf{C})$ es equivalente a la representabilidad del funtor $\widetilde{\mathcal{F}}$ de (2.22a) por un objeto de C; y ese objeto es el límite buscado, hasta un isomorfismo único.

De igual manera, si $\mathcal{G}\in\mathsf{Fun}(\mathsf{J},\mathsf{C})$ es un funtor covariante, $\mathcal{G}$ posee un colímite si y sólo si el funtor covariante

$$\widetilde{\mathcal{G}} : \mathsf{C} \to \mathsf{Set} : A\mapsto \mathrm{Hom}_{\widetilde{\mathsf{C}}}(\mathcal{G},\Delta A) \tag{2.22b}$$

es representable por un objeto $C\in\mathsf{C}$, y este objeto es el colímite de $\mathcal{G}$ en C.

2.5 Ejercicios sobre categorías y funtores

Ejercicio 2.1. Sea G un grupo cualquiera. Una **acción** de G (a la izquierda) sobre un conjunto X es una función $\lambda\colon G\times X\to X$ que cumple $\underline{\lambda(1,x)=x}$ y $\underline{\lambda(g,\lambda(h,x))=\lambda(gh,x)}$ para todo $x\in X$ y $g,h\in G$. ⟦Si se escribe $\lambda(g,x)=:g\triangleright x$, estas propiedades son $1\triangleright x=x$, $g\triangleright(h\triangleright x)=gh\triangleright x$, respectivamente.⟧

Hay una categoría G-Set cuyos objetos son pares (X,λ), donde λ es una acción de G sobre X. Identificar los morfismos de esta categoría y verificar sus propiedades necesarias.

Ejercicio 2.2. Un *grupoide* $G_1\rightrightarrows G_0$ es una categoría pequeña en la cual cada morfismo es un isomorfismo. Mostrar que lo siguiente es una definición equivalente. "Hay dos conjuntos, G_0 y G_1, y cuatro funciones $r,s\colon G_1\to G_0$, $u\colon G_0\to G_1$ y $i\colon G_1\to G_1$; además, al poner $G_2:=\{(g,h)\in G_1\times G_1 : s(g)=r(h)\}$, hay un *producto* $m\colon G_2\to G_1:(g,h)\mapsto gh$; se cumplen estas propiedades:

- $r(gh)=r(g)$ y $s(gh)=s(h)$ para todo $(g,h)\in G_2$;
- $r(u(x))=s(u(x))=x$ para todo $x\in G_0$;
- $u(r(g))\,g=g\,u(s(g))=g$ para todo $g\in G_1$;
- $g\,i(g)=u(r(g))$ y $i(g)\,g=u(s(g))$ para todo $g\in G_1$;
- $(fg)h=f(gh)$ toda vez que $(f,g)\in G_2$ y $(g,h)\in G_2$."

Ejercicio 2.3. Si $\varphi\colon A\to B$ es un homomorfismo de anillos y si $M\in\in B$-Mod, defínase $\mathcal{T}_\varphi M\in\in A$-Mod al colocar $\mathcal{T}_\varphi M:=M$ con la acción $a\cdot x:=\varphi(a)x$ para $a\in A$, $x\in M$. ¿Cómo debe definirse $\mathcal{T}_\varphi f$ para $f\in\mathrm{Hom}_B(M,N)$, para que haya un funtor $\mathcal{T}_\varphi\colon B$-Mod $\to A$-Mod?

Ejercicio 2.4. (a) Comprobar en detalle que la abelianización de grupos $\alpha(G):=G/G'$ es un funtor entre las categorías Gr y Ab.

(b) La abelianización también puede considerarse como un funtor $\alpha\colon\mathsf{Gr}\to\mathsf{Gr}$ (en vez de $\alpha\colon\mathsf{Gr}\to\mathsf{Ab}$). Para cada grupo G, sea $\nu_G\colon G\to G/G'$ la aplicación cociente. Mostrar que la familia $\{\nu_G : G\in\in\mathsf{Gr}\}$ define una transformación natural entre las funtores 1_{Gr} y α.

Ejercicio 2.5. (a) Sea X un espacio topológico. Defínase una categoría Top-X cuyos objetos son las *partes abiertas* $U\subseteq X$ y en donde $\mathrm{Hom}_{\mathsf{Top}\text{-}X}(U,V)$ contiene únicamente la inclusión $i_{UV}\colon U\hookrightarrow V$ si $U\subseteq V$, y este conjunto es vacío si $U\not\subseteq V$. Un **prehaz** de grupos abelianos sobre X es un funtor contravariante $\mathcal{P}\colon(\mathsf{Top}\text{-}X)^\circ\to\mathsf{Ab}$. Describir la definición de un prehaz directamente, sin usar la terminología de categorías y funtores.

(b) Considérese la categoría de prehaces, PreHaz-$X:=\mathsf{Fun}((\mathsf{Top}\text{-}X)^\circ,\mathsf{Ab})$. Describir sus morfismos.

Ejercicio 2.6. Si A es un anillo, defínase la categoría Matr-A por $\mathrm{Ob}(\mathsf{Matr}\text{-}A):=\{1,2,3,\dots\}$ y $\mathrm{Hom}_{\mathsf{Matr}\text{-}A}(n,m):=M_{m,n}(A)$; la ley de composición de morfismos es la multiplicación de matrices.

Si $\mathbb{F}$ es un cuerpo, mostrar que las categorías Matr-$\mathbb{F}$ y FinVect-$\mathbb{F}$ son equivalentes.

Ejercicio 2.7. Sea AnEnt la categoría de anillos enteros, una subcategoría plena de la categoría An de anillos. Si $A \in\in \mathsf{AnEnt}$ y si $\varphi\colon \mathbb{Q} \to A$ es un homomorfismo de anillos, comprobar que φ queda determinado por su restricción $\varphi|_{\mathbb{Z}}$ a $\mathbb{Z}$. Concluir que la inclusión $i\colon \mathbb{Z} \hookrightarrow \mathbb{Q}$ es un epimorfismo en AnEnt. Deducir que la categoría AnEnt no es abeliana.

Ejercicio 2.8. Algunos autores definen una **categoría abeliana** como una categoría preabeliana C que cumple el axioma siguiente: para cada morfismo $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$, hay una sucesión de morfismos

$$K \xrightarrow{\ i\ } A \xrightarrow{\ q\ } X \xrightarrow{\ j\ } B \xrightarrow{\ p\ } L$$

tal que: (a) $f = jq$;

(b) (K,i) es un núcleo de f y (L,p) es un conúcleo de f;

(c) (X,j) es un núcleo de p y (X,q) es un conúcleo de i.

Mostrar que esta definición es equivalente a la otra, que dice: "una categoría abeliana es una categoría preabeliana en donde cada morfismo canónico $\bar{f}\colon \mathrm{coker}(\ker f) \to \ker(\mathrm{coker}\, f)$ es un isomorfismo".

Ejercicio 2.9. Verificar los detalles de la demostración del Lema 2.51, para un morfismo $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$ en una categoría preabeliana, con núcleo $(\ker f, i)$ y conúcleo $(\mathrm{coker}\, f, p)$:

(a) f es un monomorfismo si y sólo si $\ker f = 0$, si y sólo si $\mathrm{coker}\, i = (A, 1_A)$;

(b) f es un epimorfismo si y sólo si $\mathrm{coker}\, f = 0$, si y sólo si $\ker p = (B, 1_B)$.

Ejercicio 2.10. Demostrar el Lema 2.54, inciso (e), que dice que, en una categoría abeliana, una sucesión $A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ es *exacta* si y sólo si $gf = 0$ y $(C,g) \simeq \mathrm{coker}\, f$.

Ejercicio 2.11. En una categoría abeliana, demostrar que la sucesión "corta"

$$0 \longrightarrow A \xrightarrow{\ f\ } B \xrightarrow{\ g\ } C \longrightarrow 0$$

es *exacta* si y sólo si: f es mónico, g es épico, $(A,f) \simeq \ker g$ y $(C,g) \simeq \mathrm{coker}\, f$.

Ejercicio 2.12. Sea $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$ un morfismo en una categoría preabeliana C. Mostar que el núcleo de f es el *pullback* del diagrama $A \xrightarrow{f} B \longleftarrow 0$; y que el conúcleo de f es el *pushout* del diagrama $0 \longleftarrow A \xrightarrow{f} B$.

Ejercicio 2.13. Sea J una categoría pequeña y sea C una categoría abeliana. Demostrar que la categoría $\widetilde{\mathsf{C}} := \mathsf{Fun}(\mathsf{J},\mathsf{C})$ es también abeliana. ⟦ Indicación: Definir los núcleos y conúcleos en $\widetilde{\mathsf{C}}$ "puntualmente". ⟧

3 Módulos Proyectivos e Inyectivos

En este capítulo, A denotara un anillo, no necesariamente conmutativo. Por "A-módulo" se entenderá un A-módulo a la izquierda, salvo indicación de lo contrario.

3.1 Módulos proyectivos

Es útil comenzar con una reformulación del concepto de suma directa de A-módulos, en términos de sucesiones exactas cortas.

Lema 3.1. *Para una determinada sucesión exacta corta de A-módulos,*

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0 \tag{3.1}$$

las siguientes condiciones son equivalentes:

(a) hay una A-homomorfismo $s\colon N \to M$ tal que $g \circ s = 1_N$,

(b) hay una A-homomorfismo $t\colon M \to L$ tal que $t \circ f = 1_L$,

(c) hay un A-submódulo R de M tal que $M = \operatorname{im} f \oplus R$ (suma directa interna).

Demostración. Ad (a) $\Longrightarrow$ (b): Tómese $x \in M$ y sea $y := g(x)$. Entonces $g(x) = g(s(y))$ o bien $g(x - s(y)) = 0$; como $\ker g = \operatorname{im} f$, se concluye que hay $w \in L$ tal que $x - s(y) = f(w)$, es decir, $x = f(w) + s(y)$.

Si $w' \in L$, $y' \in N$ cumplen $x = f(w') + s(y')$, entonces $f(w) + s(y) = f(w') + s(y')$, así que $f(w - w') = s(y' - y)$. Luego $0 = g(f(w - w')) = g(s(y' - y)) = y' - y$ y también $w = w'$ porque $f(w - w') = 0$ y f es inyectivo. Por tanto, cada $x \in M$ se escribe de manera única como una suma $f(w) + s(y)$. Defínase $t\colon M \to L$ por $t(f(w) + s(y)) := w$. Es fácil ver que t es un A-homomorfismo bien definido que cumple $tf = 1_L$.

Ad (b) $\Longrightarrow$ (c): Para $x \in M$, sea $w := t(x) \in L$. Vale $t(x - f(w)) = t(x) - 1_L(t(x)) = 0$, así que $v := x - f(w) \in \ker t$. Luego $x = f(w) + v \in \operatorname{im} f + \ker t$. Si hay $w' \in L$, $v' \in \ker t$ tales que $x = f(w) + v = f(w') + v'$, entonces $w = t(x) = t(f(w')) = w'$ y en consecuencia vale $v = v'$. Por tanto, cada $x \in M$ se escribe de manera única como una suma $f(w) + v$; esto dice que $M = \operatorname{im} f \oplus \ker t$, como suma directa interna.

Ad (c) $\Longrightarrow$ (a): Para cada $y \in N$, hay $x \in N$ tal que $g(x) = y$ porque g es sobreyectivo. Escríbase $x = f(w) + u$ (de manera única) para $w \in L$, $u \in R$. Si $y = g(x')$ para otro $x' = f(w') + u' \in M$, entonces $x - x' \in \ker g = \operatorname{im} f$, así que $u - u' = x - x' - f(w - w') \in R \cap \operatorname{im} f$ y por ende vale $u' = u$. Además vale $y = g(x) = g(u)$. Defínase $s\colon N \to M$ por $s(y) := u$. Es fácil ver que s es un A-homomorfismo bien definido que cumple $gs = 1_N$. □

Definición 3.2. Si una sucesión exacta corta de A-módulos (3.1) cumple una (y por ende todas) de las condiciones del Lema anterior, se dice que esta *sucesión exacta corta* **escinde**. Se escribe

$$0 \longrightarrow L \xrightarrow{f} M \underset{s}{\overset{g}{\rightleftarrows}} N \longrightarrow 0 \tag{3.2}$$

si $s \in \mathrm{Hom}_A(N,M)$ cumple $gs = 1_N$. En este caso, vale $M = f(L) \oplus s(N) \simeq L \oplus N$: una sucesión exacta corta escinde si y sólo si su módulo central es isomorfo a la suma directa de los dos módulos laterales.

Definición 3.3. Un **módulo proyectivo** sobre A es un A-módulo P que cumple la siguiente propiedad: dados dos A-homomorfismos $f\colon P \to N$ y $g\colon M \to N$ con g *sobreyectivo*, existe un A-homomorfismo $h\colon P \to M$ tal que $g \circ h = f$. En otras palabras, el siguiente diagrama, cuya fila inferior es exacta, conmuta:[1]

$$\begin{array}{ccccc} & & & & P \\ & & & \swarrow^{h} & \downarrow{\scriptstyle f} \\ M & \xrightarrow{g} & N & \longrightarrow & 0. \end{array} \tag{3.3}$$

Por ejemplo, *cualquier A-módulo libre L es proyectivo*. En efecto, sea S una base de L; dados $f\colon L \to N$ y $g\colon M \twoheadrightarrow N$, elíjase, para cada $s \in S$, un elemento $x_s \in M$ tal que $g(x_s) = f(s)$. Entonces la asignación $h(s) := x_s$ extiende por A-linealidad a un A-homomorfismo $h\colon L \to M$ tal que $g(h(s)) = f(s)$ para cada $s \in S$, y por tanto $g \circ h = f$.

Proposición 3.4. *Para un A-módulo P, las siguientes condiciones son equivalentes:*

(a) P es un A-módulo proyectivo.

(b) Cada sucesión exacta corta $0 \to M \to N \to P \to 0$ escinde.

(c) P es un sumando directo de un A-módulo libre.

Demostración. Ad (a) $\Longrightarrow$ (b): Dada una sucesión exacta corta $0 \to M \to N \to P \to 0$, hay un diagrama conmutativo

$$\begin{array}{ccccccccc} & & & & & & P & & \\ & & & & & \swarrow^{h} & \downarrow{\scriptstyle 1_P} & & \\ 0 & \longrightarrow & M & \longrightarrow & N & \xrightarrow{g} & P & \longrightarrow & 0, \end{array}$$

y la condición $g \circ h = 1_P$ dice que esta sucesión exacta corta escinde, en vista del Lema 3.1.

Ad (b) $\Longrightarrow$ (c): El A-módulo P es un cociente de un A-módulo libre L. Sea $q\colon L \to P$ la aplicación cociente, sea $K := \ker q$ y sea $j\colon K \hookrightarrow L$ la inclusión. Entonces la sucesión corta

$$0 \longrightarrow K \xrightarrow{j} L \xrightarrow{q} P \longrightarrow 0$$

es exacta. Si $s\colon P \to L$ es un A-homomorfismo tal que $q \circ s = 1_P$, entonces s es inyectivo y la demostración del Lema 3.1 muestra que $L = j(K) \oplus s(P) \simeq K \oplus P$.

[1] Muchas veces se escribe $M \to N \to 0$, bajo la hipótesis de exactitud, en vez de $M \twoheadrightarrow N$, para indicar que un morfismo $g\colon M \to N$ es un epimorfismo.

Ad(c) $\Longrightarrow$ (a): Si L es un A-módulo libre y si K es un A-módulo tales que $L = K \oplus P$, sea $q\colon L \to P$ la aplicación cociente, y considérese el siguiente diagrama:

$$\begin{array}{ccccc} L & \xrightarrow{q} & P & & \\ {\scriptstyle h'}\downarrow & & \downarrow{\scriptstyle f} & & \\ M & \xrightarrow{g} & N & \longrightarrow & 0. \end{array}$$

Como L es libre y por ende proyectivo, hay un A-homomorfismo $h'\colon L \to M$ tal que $g \circ h' = f \circ q$. Ahora sea $h\colon P \to M$ la restricción de h' al submódulo L de P, es decir, $h := h' \circ i$ donde $i\colon P \to L$ es la inclusión. Entonces $g \circ h = g \circ h' \circ i = f \circ q \circ i = f$. □

Corolario 3.5. *Si A es un anillo entero principal, un A-módulo es proyectivo si y sólo es libre.*

Demostración. Un A-módulo libre es proyectivo, para cualquier anillo A. La Proposición anterior muestra que un A-módulo proyectivo es (isomorfo a) un submódulo de un A-módulo libre. Ahora, la Proposición 1.46 muestra que un submódulo de un A-módulo libre es también libre, cuando A es un anillo entero principal. □

Ejemplo 3.6. El isomorfismo $\mathbb{Z}/6 \simeq \mathbb{Z}/2 \oplus \mathbb{Z}/3$, como módulos sobre el anillo $\mathbb{Z}/6$, muestra que $\mathbb{Z}/2$ y $\mathbb{Z}/3$ son módulos proyectivos, pero no libres, sobre $\mathbb{Z}/6$.

Ejemplo 3.7. Sea $B = M_n(A)$, para algún anillo A con $n \geq 2$. Entonces A^n, considerado como la totalidad de columnas formados por n elementos de A, es un B-módulo (a la izquierda). Ahora $B \simeq A^n \oplus \cdots \oplus A^n$ (n veces): cada matriz en $M_n(A)$ es un juego de n columnas, y este isomorfismo es B-lineal (¿por qué?). Luego A^n es un B-módulo proyectivo, pero no libre.

Lema 3.8. *Si $P = \bigoplus_{j\in J} P_j$, entonces P es proyectivo si y sólo si cada P_j es proyectivo.*

Demostración. Si cada P_j es proyectivo, entonces $L_j \simeq M_j \oplus P_j$ donde cada L_j es un A-módulo libre. Si $L := \bigoplus_j L_j$ y $M := \bigoplus_j M_j$, entonces $L \simeq M \oplus P$ donde L es libre: se concluye que P es proyectivo.

Inversamente, si P es proyectivo, hay un A-módulo libre L y otro A-módulo M tal que $L \simeq M \oplus P$. Si $N_j := M \oplus \bigoplus_{k\neq j} P_k$, entonces $L = N_j \oplus P_j$ y por ende P_j es proyectivo. □

► Hay una caracterización importante de módulos proyectivos en términos de funtores representables, que permite transferir el concepto de proyectividad a cualquier categoría abeliana. Comenzamos con un poco más de terminología para funtores.

Definición 3.9. Si C y D son categorías aditivas, un funtor $\mathcal{F}\colon \mathsf{C} \to \mathsf{D}$ se llama **funtor aditivo** si $\mathcal{F}(\varphi + \psi) = \mathcal{F}\varphi + \mathcal{F}\psi$ toda vez que $\varphi, \psi \in \mathrm{Hom}_{\mathsf{C}}(A, B)$. En otras palabras, cada aplicación $\overline{\mathcal{F}} : \mathrm{Hom}_{\mathsf{C}}(A,B) \to \mathrm{Hom}_{\mathsf{D}}(\mathcal{F}A, \mathcal{F}B)$ es un homomorfismo de grupos abelianos.

Por ejemplo, si C es una categoría aditiva, los funtores representables $h^A = \mathrm{Hom}_{\mathsf{C}}(A, -) : \mathsf{C} \to \mathsf{Ab}$ son funtores aditivos.

Definición 3.10. Si C y D son categorías abelianas, sea $\mathcal{F}\colon \mathsf{C} \to \mathsf{D}$ un funtor aditivo (covariante). Se dice que $\mathcal{F}$ es un **funtor exacto** si para cada sucesión exacta corta en C,

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0 \tag{3.4}$$

la sucesión corta correspondiente en D *es también exacta*:

$$0 \longrightarrow \mathcal{F}A \xrightarrow{\mathcal{F}f} \mathcal{F}B \xrightarrow{\mathcal{F}g} \mathcal{F}C \longrightarrow 0.$$

Si, para toda sucesión exacta corta (3.4), sólo se obtiene exactitud de la sucesión

$$0 \longrightarrow \mathcal{F}A \xrightarrow{\mathcal{F}f} \mathcal{F}B \xrightarrow{\mathcal{F}g} \mathcal{F}C,$$

se dice que $\mathcal{F}$ es **exacto a la izquierda**. En cambio, si sólo se puede concluir exactitud de la sucesión

$$\mathcal{F}A \xrightarrow{\mathcal{F}f} \mathcal{F}B \xrightarrow{\mathcal{F}g} \mathcal{F}C \longrightarrow 0,$$

se dice que $\mathcal{F}$ es **exacto a la derecha**. Finalmente, si se obtiene únicamente la exactitud de la sucesión

$$\mathcal{F}A \xrightarrow{\mathcal{F}f} \mathcal{F}B \xrightarrow{\mathcal{F}g} \mathcal{F}C,$$

se dice que $\mathcal{F}$ es **semiexacto**.

Lema 3.11. *Si R es un A-módulo, el funtor representable $h^R = \mathrm{Hom}_A(R,-) : A\text{-}\mathsf{Mod} \to \mathsf{Ab}$ es exacto a la izquierda.*

Demostración. Sea $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ una sucesión exacta corta en A-Mod. Hay que mostrar que la sucesión

$$0 \longrightarrow \mathrm{Hom}_A(R,L) \xrightarrow{f_*} \mathrm{Hom}_A(R,M) \xrightarrow{g_*} \mathrm{Hom}_A(R,N)$$

es también exacta: es decir, que f_* es inyectivo, que $g_* \circ f_* = 0$ y que $\mathrm{im}\, f_* = \ker g_*$.

Si $h \in \mathrm{Hom}_A(R,L)$ cumple $f_*(h) = 0$, entonces $f \circ h = 0$, luego $h = 0$ porque f es un monomorfismo. Por tanto, f_* es inyectivo.

Es $g_* \circ f_* = (g \circ f)_* = 0$ por la funtorialidad de h^R; en consecuencia, se obtiene $\mathrm{im}\, f_* \subseteq \ker g_*$. Además, si $k \in \mathrm{Hom}_A(R,M)$ cumple $g_*(k) = g \circ k = 0$ y si $x \in R$, entonces $g(k(x)) = 0$, así que $k(x) \in \ker g = \mathrm{im}\, f$, y por ende $k(x) = f(y)$ para algún $y \in L$. Este y es único porque f es un monomorfismo; al escribir $y =: l(x)$, se obtiene $l \in \mathrm{Hom}_A(R,L)$ tal que $k = f \circ l = f_*(l)$. Se concluye que $\ker g_* \subseteq \mathrm{im}\, f_*$. □

El funtor representable *contravariante* $h_R = \mathrm{Hom}_A(-,R) : A\text{-}\mathsf{Mod} \to \mathsf{Ab}$ es también exacto a la izquierda, en el sentido de llevar una sucesión exacta corta $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ de A-módulos en una sucesión exacta

$$0 \longrightarrow \mathrm{Hom}_A(N,R) \xrightarrow{g^*} \mathrm{Hom}_A(M,R) \xrightarrow{f^*} \mathrm{Hom}_A(L,R). \tag{3.5}$$

Se demuestra esta exactitud (siniestra) por argumentos análogas a las del Lema 3.11.

Lema 3.12. *Un A-módulo P es proyectivo si y sólo si el funtor covariante $h^P = \mathrm{Hom}_A(P,-)$ es exacto.*

Demostración. Sea P un A-módulo proyectivo. Si $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ es una sucesión exacta corta en A-Mod, hay que mostrar que la sucesión corta de grupos abelianos

$$0 \longrightarrow \mathrm{Hom}_A(P,L) \xrightarrow{f_*} \mathrm{Hom}_A(P,M) \xrightarrow{g_*} \mathrm{Hom}_A(P,N) \longrightarrow 0$$

es exacta. Por el Lema 3.11, basta mostrar que g_* es sobreyectivo si g es un epimorfismo de A-módulos. Pero la sobreyectividad de g implica que cada $f \in \mathrm{Hom}_A(P,N)$ es de la forma $f = g \circ h$ para algún $h \in \mathrm{Hom}_A(P,M)$, según el diagrama (3.3). Esto dice que $f = g_*(h)$; luego g_* es sobreyectivo.

Inversamente, si h^P es exacto a la izquierda, dados $f \in \mathrm{Hom}_A(P,N)$ y $g \in \mathrm{Hom}_A(M,N)$ con g sobreyectivo, se concluye que g_* es sobreyectivo, de modo que $f = g \circ h$ para algún $h \in \mathrm{Hom}_A(P,M)$: en otras palabras, P es proyectivo. □

Hay una generalización del Lema anterior a cualquier categoría abeliana C. Brevemente, se dice que $P \in\in \mathsf{C}$ es un **objeto proyectivo** si se reproduce el cuadro (3.3): dado un epimorfismo $g \in \mathrm{Hom}_{\mathsf{C}}(A,B)$, cada morfismo $f \in \mathrm{Hom}_{\mathsf{C}}(P,B)$ puede "levantarse" a un morfismo $h \in \mathrm{Hom}_{\mathsf{C}}(P,A)$ tal que $gh = f$. Resulta que un objeto P es proyectivo si y sólo si el funtor covariante $h^P \colon \mathsf{C} \to \mathsf{Ab}$ es exacto.

► Una construcción algebraica importante utiliza los módulos proyectivos sobre un anillo determinado A. Se aprovecha la circunstancia que la suma directa $P \oplus Q$ de dos A-módulos proyectivos es también proyectivo. Si se reemplaza el A-módulo P por su *clase de isomorfismo* $[P]$, es posible definir una operación de *suma*:

$$[P] + [Q] := [P \oplus Q]. \tag{3.6}$$

Como $(P \oplus Q) \oplus R \simeq P \oplus (Q \oplus R)$ y también $Q \oplus P \simeq P \oplus Q$ por isomorfismos obvios, estas clases de isomorfismo forman un *monoide conmutativo*, cuyo elemento nulo es $[0]$. Para promover este monoide a un *grupo abeliano*, se usa una "construcción universal", introducido por Grothendieck.

Proposición 3.13. *Sea S un monoide conmutativo cualquiera. Hay un grupo abeliano $K(S)$, junto con un homomorfismo de monoides $\iota \colon S \to K(S)$, que posee la siguiente propiedad universal:*

$$\begin{array}{ccc} K(S) & & \\ {\scriptstyle\iota}\uparrow & \searrow^{\tilde\sigma} & \\ S & \xrightarrow{\sigma} & G \end{array} \tag{3.7}$$

cualquier homomorfismo $\sigma \colon S \to A$ de S en un grupo abeliano G determina un único homomorfismo de grupos $\tilde\sigma \colon K(S) \to G$ tal que $\tilde\sigma \circ \iota = \sigma$.

Demostración. Se adapta la construcción conocida del grupo $\mathbb{Z}$ a partir del monoide $\mathbb{N}$. El único detalle que merece notar es que $\mathbb{N}$ posee una propiedad de *cancelación* que no es compartido por todos los monoides: si $r+n=s+n$ para $r,s,n\in\mathbb{N}$, entonces $r=s$.

Defínase $K(S)$ como el cociente de conjuntos $(S\times S)/\!\sim$ bajo la siguiente relación de equivalencia:

$$(x,y)\sim(x',y') \quad \text{si y sólo si} \quad x+y'+z=x'+y+z \quad \text{para algún} \quad z\in S.$$

Defínase $\iota(x):=[(x,0)]$ para $x\in S$. La suma en $K(s)$ es $[(x,y)]+[(x',y')]:=[(x+x',y+y')]$, la cual es obviamente asociativa y conmutativa, con elemento nulo $[(0,0)]$. El negativo de $[(x,y)]$ es $[(y,x)]$, ya que $(x+y,x+y)\sim(0,0)$.

Si $\sigma\colon S\to G$ es un homomorfismo de S en un grupo abeliano G, defínase

$$\tilde{\sigma}[(x,y)]:=\sigma(x)-\sigma(y).$$

Esto es un homomorfismo, evidentemente único y bien definido, tal que $\tilde{\sigma}\circ\iota=\sigma$. □

Debe de ser evidente que el grupo $K(S)$ es esencialmente único; este grupo se llama el **grupo de Grothendieck** del monoide S.

Ejemplo 3.14. Fíjese que el homomorfismo canónico $\iota\colon S\to K(S)$ es inyectivo si y sólo si el monoide S tiene la propiedad de cancelación.

Si $S=(\mathbb{N},\cdot)$ es el monoide *multiplicativo* de enteros (con elemento identidad 1), la presencia del elemento $0\in\mathbb{N}$ destruye cancelación: $r\cdot 0=s\cdot 0=0$ no implica $r=s$. En este caso, se obtiene $K((\mathbb{N},\cdot))=0$.

Lema 3.15. *Si P y Q son A-módulos proyectivos finitamente generados, entonces $P\oplus Q$ también es finitamente generado.*

Demostración. Si P es proyectivo y si P es generado por $\{x_1,\ldots,x_n\}$, entonces hay un epimorfismo $q\colon A^n\twoheadrightarrow P$. Al tomar $L=A^n$ en la demostración de la Proposición 3.4, la sucesión exacta corta $0\longrightarrow\ker q\xrightarrow{j}A^n\xrightarrow{q}P\longrightarrow 0$ escinde, luego hay un A-módulo R tal que $A^n\simeq P\oplus R$. En resumen: P es proyectivo y finitamente generado si y sólo si P es isomorfo a un sumando directo de A^n para algún n.

Ahora, si $Q\oplus S\simeq A^m$ para algún m y algún A-módulo S, entonces

$$(P\oplus Q)\oplus(R\oplus S)\simeq(P\oplus R)\oplus(Q\oplus S)\simeq A^n\oplus A^m\simeq A^{n+m},$$

y por tanto $P\oplus Q$ es proyectivo y finitamente generado. □

Definición 3.16. Sea A un anillo y sea $P(A)$ el monoide conmutativo cuyos elementos son las clases de isomorfismo de A-módulos proyectivos finitamente generados, con la suma (3.6). El grupo abeliano $K_0(A):=K(P(A))$ se llama el **K-grupo algebraico**[2] del anillo A.

[2]Es evidente que si $A\simeq B$ como anillos, entonces $K_0(A)\simeq K_0(B)$ como grupos abelianos. De hecho, $K_0\colon \mathsf{An}\to\mathsf{Ab}$ es un *funtor semiexacto*. La notación K_0 indica que existen otros grupos abelianos $K_1(A)$, $K_2(A)$, etc., cuyo estudio se llama la "K-teoría algebraica". Véase, por ejemplo: Jonathan Rosenberg, *Algebraic K-theory and its Applications*, Graduate Texts in Mathematics 147, Springer, Berlin, 1994.

3.2 Módulos inyectivos

Es dual categórico de un módulo proyectivo es un módulo inyectivo, que se define a continuación.

Definición 3.17. Un **módulo inyectivo** sobre A es un A-módulo Q que cumple la siguiente propiedad: dados dos A-homomorfismos $f\colon M \to Q$ y $j\colon M \to N$ con j *inyectivo*, existe un A-homomorfismo $h\colon N \to Q$ tal que $h \circ j = f$. En otras palabras, el siguiente diagrama, cuya fila inferior es exacta, conmuta:

$$\begin{array}{ccccc} 0 & \longrightarrow & M & \xrightarrow{j} & N \\ & & {\scriptstyle f}\downarrow & \swarrow_{h} & \\ & & Q & & \end{array} \tag{3.8}$$

Proposición 3.18. *Para un A-módulo Q, las siguientes condiciones son equivalentes:*

(a) Q es un A-módulo inyectivo.

(b) El funtor contravariante $h_Q = \mathrm{Hom}_A(-, Q)$ es exacto.

(c) Cada sucesión exacta corta $0 \to Q \to M \to N \to 0$ escinde.

Demostración. Ad (a) $\Longrightarrow$ (b): El funtor h_Q es exacto a la izquierda; para que éste sea un funtor exacto, cada sucesión exacta corta $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ de A-módulos debe dar lugar a una sucesión exacta corta

$$0 \longrightarrow \mathrm{Hom}_A(N, Q) \xrightarrow{g^*} \mathrm{Hom}_A(M, Q) \xrightarrow{f^*} \mathrm{Hom}_A(L, Q) \longrightarrow 0.$$

Al comparar esta con la sucesión exacta (3.5), lo que hace falta es que f^* sea sobreyectivo. En otras palabras, dado $k \in \mathrm{Hom}_A(L, Q)$ y el monomorfismo $f \in \mathrm{Hom}_A(L, M)$,

$$\begin{array}{ccccc} 0 & \longrightarrow & L & \xrightarrow{f} & M \\ & & {\scriptstyle k}\downarrow & \swarrow_{h} & \\ & & Q & & \end{array}$$

hay un A-homomorfismo $h \in \mathrm{Hom}_A(M, Q)$ tal que $f^*(h) = hf = k$; luego f^* es sobreyectivo.

Ad (b) $\Longrightarrow$ (c): Dada una sucesión exacta corta $0 \longrightarrow Q \xrightarrow{j} M \xrightarrow{g} N \longrightarrow 0$, hay un diagrama conmutativo

$$\begin{array}{ccccccc} 0 & \longrightarrow & Q & \xrightarrow{j} & M & \xrightarrow{g} & N \longrightarrow 0 \\ & & {\scriptstyle 1_Q}\downarrow & \swarrow_{t} & & & \\ & & Q & & & & \end{array}$$

y la condición $t \circ j = 1_Q$ dice que esta sucesión exacta corta escinde, en vista del Lema 3.1.

Ad(c) $\Longrightarrow$ (a): Dados dos A-homomorfismos $f\colon M \to Q$ y $j\colon M \to N$ con j inyectivo, sea (R,i,h) el *pushout* correspondiente:

$$\begin{array}{ccc} M & \xrightarrow{j} & N \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle h} \\ Q & \xrightarrow[i]{} & R \end{array}$$

No es difícil verificar que i es inyectivo, ya que j es inyectivo.[3] Sea $q\colon R \to R/i(Q)$ el homomorfismo cociente; entonces hay una sucesión exacta corta

$$0 \longrightarrow Q \xrightarrow{i} R \xrightarrow{q} R/i(Q) \longrightarrow 0$$

la cual escinde, por hipótesis. En consecuencia, hay un A-homomorfismo $t\colon R \to Q$ tal que $t \circ i = 1_Q$. Las propiedades de pushouts implican que $t \circ h \in \mathrm{Hom}_A(M,Q)$ cumple

$$(t \circ h) \circ j = t \circ (h \circ j) = t \circ (i \circ f) = (t \circ i) \circ f = 1_Q \circ f = f.$$

Luego Q es un A-módulo inyectivo. □

Lema 3.19. *Si $Q = \prod_{j\in J} Q_j$, entonces Q es inyectivo si y sólo si cada Q_j es inyectivo. En particular, una suma directa finita $\bigoplus_{k=1}^{n} Q_k$ es inyectivo si y sólo si cada sumando directo Q_k es inyectivo.*

Demostración. Sean $p_j\colon Q \to Q_j$, para $j \in J$, los homomorfismos que definen el producto directo $Q = \prod_{j\in J} Q_j$. Dados un monomorfismo $u\colon M \rightarrowtail N$ y un homomorfismo $f\colon M \to Q$, sea $f_j := p_j \circ f : M \to Q_j$ para $j \in J$. Si cada Q_j es inyectivo, entonces hay un homomorfismo $h_j\colon N \to Q_j$ tal que $h_j \circ u = f_j$. Por la propiedad universal del producto directo, hay un (único) homomorfismo $h\colon N \to Q$ tal que $p_j \circ h = h_j$. Ahora, vale $p_j \circ (h \circ u) = h_j \circ u = f_j = p_j \circ f$ en $\mathrm{Hom}_A(M,Q_j)$ para cada j; por lo tanto, vale $h \circ u = f$ en $\mathrm{Hom}_A(M,Q)$.

$$\begin{array}{ccccc} 0 & \longrightarrow & M & \xrightarrow{u} & N \\ & & {\scriptstyle f}\downarrow & \overset{h}{\swarrow} & \downarrow{\scriptstyle h_j} \\ & & Q & \xrightarrow[p_j]{} & Q_j \end{array}$$

Inversamente, una familia de homomorfismos $\{ f_j \in \mathrm{Hom}_A(M,Q_j) : j \in J \}$ determina un homomorfismo $f\colon M \to Q$ tal que $p_j \circ f = f_j$ para cada j. Si Q es inyectivo, hay un homomorfismo $h\colon N \to Q$ tal que $h \circ u = f$. Al definir $h_j := p_j \circ h : N \to Q_j$, se ve que $h_j \circ u = p_j \circ h \circ u = p_j \circ f = f_j$ para cada j. En consecuencia, cada Q_j es un A-módulo inyectivo. □

Hay un criterio sencillo para ver si un A-módulo determinado es inyectivo o no.

[3] Véase el Ejercicio 3.8 al final de este capítulo.

Lema 3.20 (El criterio de Baer)**.** *Un A-módulo Q es inyectivo*[4] *si y sólo si cada A-homomorfismo $\varphi\colon J \to Q$ desde un ideal a la izquierda $J \subseteq A$ puede extenderse en un A-homomorfismo $\psi\colon A \to Q$.*

Demostración. Ad $(\Rightarrow)$: Si Q es inyectivo, es cuestión de reemplazar $j\colon M \rightarrowtail N$ en el diagrama (3.8) por la inclusión $i\colon J \hookrightarrow A$ para obtener la extensión deseada. (Se dice que ψ **extiende** φ si $\psi(x) = \varphi(x)$ para todo $x \in J$; esto es, si $\psi \circ i = \varphi$ donde i es la inclusión.)

Ad $(\Leftarrow)$: Sean dados dos A-homomorfismos $f\colon M \to Q$ y $j\colon N \rightarrowtail M$ con j inyectivo. Considérese el conjunto $\mathcal{N}$ de pares (N', g), donde $N' \subseteq N$ es un A-submódulo con $j(M) \subseteq N'$ y $g \in \mathrm{Hom}_A(N', Q)$ cumple $g(j(x)) = f(x)$ para $x \in M$. El conjunto $\mathcal{N}$ es parcialmente ordenado, al declarar que $(N_1', g_1) \leq (N_2', g_2)$ toda vez que $N_1' \subseteq N_2'$ y la restricción de g_2 a N_1' coincide con g_1. Es claro que una cadena $\{(N_i', g_i)\}_{i\in I}$ de tales pares posee una cota superior en $\mathcal{N}$, pues la unión $\bigcup_{i\in I} N_i'$ es también un A-submódulo de N. Se obtiene un elemento máximo (L, h) de $\mathcal{N}$ por una Zornicación.[5]

Si $L \neq N$, tómese $x \in N \setminus L$ y sea $J := \{\, a \in A : ax \in L \,\}$, el cual es un ideal a la izquierda en A. Defínase $\varphi\colon J \to Q$ por $\varphi(a) := h(ax)$. Por la hipótesis, φ se extiende a $\psi\colon A \to Q$. Sea $L' := L + Ax$ y defínase $h'\colon L' \to Q$ por

$$h'(z + ax) := h(z) + \psi(a), \quad \text{para todo} \quad z \in L.$$

Supóngase que $z + ax = y + bx$, con $y \in L$, $b \in A$. Entonces $(a-b)x = y - z \in L$, así que $a - b \in J$. Luego

$$h(y - z) = h((a-b)x) = \varphi(a-b) = \psi(a-b),$$

de modo que $h(z) + \psi(a) = h(y) + \psi(b)$; se ve que h' está bien definido. Si $z \in L$, se puede entonces tomar $a = 0$ para obtener $h'(z) = h(z)$; pero esto implica que $(L, h) < (L', h')$ en $\mathcal{N}$, contrario a la maximalidad de (L, h). En consecuencia, es $L = N$ y $h\colon N \to Q$ cumple $h \circ j = f$; por tanto, Q es un A-módulo inyectivo. □

Una clase importante de ejemplos de A-módulos inyectivos son los grupos abelianos divisibles (en el caso $A = \mathbb{Z}$).

Definición 3.21. Un grupo abeliano $(G, +)$ es **divisible** si para todo entero positivo $m \in \mathbb{N}^*$, el endomorfismo $x \mapsto mx$ es sobreyectivo; esto es, para cada $y \in G$ hay $x \in G$ tal que $mx = y$.

Ejemplo 3.22. Los grupos aditivos $\mathbb{Q}$ y $\mathbb{Q}/\mathbb{Z}$ son divisibles; pero $\mathbb{Z}$ no es divisible.

Un grupo abeliano finito G no es divisible: si $n = |G|$ es la cardinalidad de G, entonces $nx = 0$ para todo $x \in G$.

Si G es divisible, cualquier grupo cociente G/H es también divisible.

Lema 3.23. *Un $\mathbb{Z}$-módulo Q es inyectivo si y sólo si Q es un grupo abeliano divisible.*

[4] Este criterio se debe a Reinhold Baer, quien introdujo el concepto de módulo inyectivo en 1940, mucho antes de la consideración de los módulos proyectivos, en: Reinhold Baer, *Abelian groups that are direct summands of every containing abelian group*, Bulletin of the American Mathematical Society **46** (1940), 800–806.

[5] El *Lema de Zorn*, que es equivalente al axioma de elección, asegura que un conjunto parcialmente ordenado, en el cual cada cadena (parte totalmente ordenada) posee una cota superior, contiene un elemento máximo.

Demostración. Ad $(\Rightarrow)$: Si Q es inyectivo, tómese $m \in \{1,2,3,\dots\}$ y sea $y \in Q$. Entonces $m\mathbb{Z}$ es un ideal de $\mathbb{Z}$ y la aplicación aditiva $f\colon m\mathbb{Z} \to Q : km \mapsto ky$ está bien definido. Por el Lema anterior, f se extiende a un homomorfismo $h\colon \mathbb{Z} \to Q$. Ahora vale

$$y = f(m) = h(m) = mh(1),$$

de modo que $x := h(1)$ cumple $mx = y$. Luego Q es divisible.

Ad $(\Leftarrow)$: Si Q es divisible como grupo abeliano, sea J un ideal no nulo de $\mathbb{Z}$. Entonces $J = m\mathbb{Z}$ para algún $m \in \mathbb{N}^*$. Si $f\colon J \to Q$ es aditivo, existe $x \in Q$ tal que $mx = f(m)$. Defínase $h\colon \mathbb{Z} \to Q$ por $h(r) := rx$. Entonces h es aditivo y vale $h(rm) = rmx = rf(m) = f(rm)$ para $rm \in \mathbb{Z}$, así que h es una extensión de f a todo $\mathbb{Z}$. Por el Lema 3.20, Q es inyectivo. □

Lema 3.24. *Cualquier grupo abeliano puede ser encajado en un grupo abeliano divisible.*[6]

Demostración. Si G es un grupo abeliano y sea $\{g_j : j \in J\}$ una colección de generadores de G. Entonces G es un cociente de un grupo abeliano libre $F = \mathbb{Z}^{(J)}$, de modo que $G \simeq F/K$, donde K es el núcleo de la aplicación cociente $\eta\colon F \to G$. Considérese el producto directo $\mathbb{Q}^J$; por los Lemas 3.19 y 3.23, este es un grupo abeliano divisible. Hay inclusiones obvias $\mathbb{Z}^{(J)} \hookrightarrow \mathbb{Q}^{(J)} \hookrightarrow \mathbb{Q}^J$. Luego hay una cadena de subgrupos

$$G \simeq \mathbb{Z}^{(J)}/K \leq \mathbb{Q}^{(J)}/K \leq \mathbb{Q}^J/K$$

y el último grupo $\mathbb{Q}^J/K$ es divisible. □

► Si A es un anillo y G es un grupo abeliano cualquiera, el grupo abeliano $\mathrm{Hom}_{\mathbb{Z}}(A,G)$ es un A-módulo a la izquierda, al definir

$$(af)(b) := f(ba) \in G, \quad \text{para todo} \quad a,b \in A,\ f \in \mathrm{Hom}_{\mathbb{Z}}(A,G).$$

Este A-módulo es una pieza auxiliar en los dos resultados que siguen.

Proposición 3.25. *Si Q es un grupo abeliano divisible, entonces el A-módulo* $\mathrm{Hom}_{\mathbb{Z}}(A,Q)$ *es inyectivo.*

Demostración. Se aplica el criterio de Baer. Sea $J \subseteq A$ un ideal a la izquierda y sea $\varphi\colon J \to \mathrm{Hom}_{\mathbb{Z}}(A,Q)$ un A-homomorfismo. Defínase una aplicación aditiva (homomorfismo de grupos abelianos) $\sigma\colon J \to Q$ por $\sigma(a) := \varphi(a)(1)$. Ahora Q es inyectivo como $\mathbb{Z}$-módulo, así que σ se extiende a una aplicación aditiva $\tilde{\sigma}\colon A \to Q$,

$$\begin{array}{ccccc} 0 & \longrightarrow & J & \xrightarrow{\ i\ } & A \\ & & {\scriptstyle\sigma}\downarrow & \swarrow_{\tilde{\sigma}} & \\ & & Q & & \end{array}$$

[6]Un **encaje** es un homomorfismo inyectivo. Luego, una redacción alternativa de este enunciado sería: "cualquier grupo abeliano es isomorfo a un subgrupo de un grupo abeliano divisible".

Fíjese que $\tilde{\sigma} \in \mathrm{Hom}_{\mathbb{Z}}(A,Q)$. Ahora, si $a \in J$ y $b \in A$, entonces $ba \in J$ y vale

$$(a\tilde{\sigma})(b) = \tilde{\sigma}(ba) = \sigma(ba) = \varphi(ba)(1) = (b\varphi(a))(1) = \varphi(a)(b),$$

porque $\tilde{\sigma}$ coincide con σ sobre J y φ es A-lineal. Luego $\varphi(a) = a\tilde{\sigma}$ para $a \in J$. La definición $\widetilde{\varphi}(c) := c\tilde{\sigma}$, para todo $c \in A$, extiende φ a un A-homomorfismo $\widetilde{\varphi}\colon A \to \mathrm{Hom}_{\mathbb{Z}}(A,Q)$. Por tanto, el Lema 3.20 muestra que $\mathrm{Hom}_{\mathbb{Z}}(A,Q)$ es inyectivo. □

Proposición 3.26. *Cualquier A-módulo M puede ser encajado en un A-módulo inyectivo.*

Demostración. Por el Lema 3.24, el grupo abeliano $(M,+)$ puede ser encajado en un grupo abeliano divisible Q. Por otro lado, el A-módulo M puede ser identificado con el A-módulo $\mathrm{Hom}_A(A,M)$, pues $x \in M$ corresponde al A-homomorfismo $f_x\colon a \mapsto ax$; esta identificación es a su vez A-lineal, porque $f_{bx}(a) = abx = f_x(ab) = (bf_x)(a)$ conlleva $f_{bx} = bf_x$ para todo $b \in A$. Esto da lugar a una cadena de A-submódulos

$$M \simeq \mathrm{Hom}_A(A,M) \leq \mathrm{Hom}_{\mathbb{Z}}(A,M) \leq \mathrm{Hom}_{\mathbb{Z}}(A,Q)$$

y por el Lema anterior, el último A-módulo es inyectivo. □

Evidentemente, el A-módulo inyectivo que incluye (una copia isomorfa de) M, a partir de esta construcción, es bastante "grande". Resulta que hay un A-módulo inyectivo Q, junto con un monomorfismo $i\colon M \to Q$, que es *mínimo* en el siguiente sentido: si hay un monomorfismo $j\colon M \to Q'$ con Q' inyectivo, entonces hay un monomorfismo $u\colon Q \to Q'$ tal que $u \circ i = j$. Es claro que un tal Q es único hasta un isomorfismo de A-módulos, y recibe el nombre de **cascarón inyectivo**[7] del A-módulo M. Por ejemplo, el cascarón inyectivo de $\mathbb{Z}$, como grupo abeliano, es $\mathbb{Q}$, el grupo aditivo de números racionales.

Para un A-módulo determinado M, la construcción de un A-módulo inyectivo que lo incluye como submódulo (en la Proposición 3.26) es mucho más concreto —y más difícil— que la construcción de un A-módulo proyectivo del cual M es un cociente. Entonces, no queda claro si hay un resultado similar para otras categorías abelianas. De hecho, se dice que una categoría abeliana C **tiene suficientes inyectivos** si cada objeto de C puede ser encajada (con un monomorfismo adecuado) en un objeto inyectivo $Q \in\in \mathsf{C}$, es decir, un objeto Q para el cual el funtor $h_Q\colon \mathsf{C}^\circ \to \mathsf{Ab}$ es exacto. La construcción subsiguiente de las resoluciones inyectivas de A-módulos puede llevarse a cabo en cualquier categoría abeliana que tiene suficientes inyectivos.

► El concepto de *divisibilidad* puede plantearse en la categoría de A-módulos cuando A es un *anillo entero*. Se dice que un A-módulo M es divisible si para cada $a \neq 0$ en A y cada $y \in M$, hay $x \in M$ tal que $ax = y$. Al examinar la demostración del Lema 3.23, se ve que cualquier A-módulo inyectivo Q es divisible en este sentido; pero para que un A-módulo divisible sea inyectivo, se requiere que A sea un anillo entero *principal*.

[7] Este resultado no será demostrado en este curso, pero está probado en muchos textos. Véase, por ejemplo: Saunders MacLane, *Homology*, Springer, Berlin, 1975; § III.11.

3.3 El producto tensorial

Hasta ahora, se ha considerado los A-módulos a la izquierda casi exclusivamente. Por ejemplo, en la expresión $\varphi \in \mathrm{Hom}_A(M,N)$ los dos módulos M, N son A-módulos a la izquierda y φ es A-lineal en el sentido de respetar la acción a la izquierda de A, pues $\varphi(ax) = a\varphi(x)$ para $a \in A$. Igualmente, se podría considerar A-módulos a la derecha exclusivamente, en cuyo caso la A-linealidad de φ sería la condición de que $\varphi(xa) = \varphi(x)a$ para $a \in A$. En adelante será necesario combinar objetos de A-Mod y Mod-A, mediante el llamado producto tensorial.

Definición 3.27. Sea A un anillo (no necesariamente conmutativo), sea M un *A-módulo a la derecha* y sea N un *A-módulo a la izquierda*. Sea F el grupo abeliano libre generado por todos los pares ordenados (x,y) con $x \in M$, $y \in N$; y sea K el subgrupo generado por todos los elementos de una de estas tres tipos:

$$(x+x',y)-(x,y)-(x',y), \qquad (x,y+y')-(x,y)-(x,y'),$$
$$(xa,y)-(x,ay),$$

para $x,x' \in M$, $y,y' \in N$, $a \in A$. Denótese el grupo abeliano F/K por $\underline{M \otimes_A N}$: este *grupo abeliano* es el **producto tensorial** de M y N (sobre el anillo A).

Escríbase $\underline{x \otimes y}$ para denotar la coclase $(x,y)+K$. Entonces $M \otimes_A N$ es un grupo abeliano generado por los elementos $\{\, x \otimes y : x \in M,\ y \in N \,\}$, sujeto (solamente) a las relaciones

$$(x+x') \otimes y = x \otimes y + x' \otimes y, \qquad x \otimes (y+y') = x \otimes y + x \otimes y', \tag{3.9a}$$
$$xa \otimes y = x \otimes ay. \tag{3.9b}$$

Un elemento $z \in M \otimes_A N$ es una suma finita de estos "tensores simples": $z = \sum_{j=1}^{m} x_j \otimes y_j$.

Ejemplo 3.28. Aun en el caso $A = \mathbb{Z}$, el producto tensorial $M \otimes_{\mathbb{Z}} N$ de dos grupos abelianos M y N puede ser *nulo*, debido a la presencia de *torsión*. Por ejemplo, tómese $M = \mathbb{Z}/2$ y $N = \mathbb{Z}/3$. Entonces, para $x \in \mathbb{Z}/2$, $y \in \mathbb{Z}/3$, vale

$$x \otimes y = 3(x \otimes y) - 2(x \otimes y) = x \otimes 3y - 2x \otimes y = 0,$$

así que $\mathbb{Z}/2 \otimes_{\mathbb{Z}} \mathbb{Z}/3 = 0$.

Si G, H son dos grupos abelianos, $G \times H$ denota su *producto directo*, es decir, el producto cartesiano con su estructura usual de grupo abeliano.

Definición 3.29. Sea M un A-módulo a la derecha y N un A-módulo a la izquierda. Una **aplicación A-equilibrada** de $M \times N$ en un grupo abeliano R es una función $f : M \times N \to R$ que cumple

$$f(x+x',y) = f(x,y) + f(x',y), \qquad f(x,y+y') = f(x,y) + f(x,y'),$$
$$f(xa,y) = f(x,ay), \tag{3.10}$$

para $x,x' \in M$, $y,y' \in N$, $a \in A$.

Ejemplo 3.30. Si $M \in\in \mathsf{Mod}\text{-}A$ y $N \in\in A\text{-}\mathsf{Mod}$, el homomorfismo de grupos abelianos $\eta : M \times N \to M \otimes_A N$ definido por $\eta(x,y) := x \otimes y$ es una aplicación A-equilibrada, por (3.9).

Proposición 3.31. *Si $f : M \times N \to R$ es una aplicación A-equilibrada, entonces hay un único homomorfismo de grupos abelianos $\varphi : M \otimes_A N \to R$ tal que $\varphi \circ \eta = f$:*

$$\begin{array}{ccc} M \times N & & \\ \downarrow{\scriptstyle \eta} & \searrow^{f} & \\ M \otimes_A N & \overset{\varphi}{\dashrightarrow} & R \end{array} \tag{3.11}$$

Demostración. Para que el diagrama conmute, hay que definir $\varphi(x \otimes y) := f(x,y)$ para todo $x \in M$, $y \in N$; lo cual demuestra la unicidad de φ. Para su existencia, sólo falta observar las propiedades (3.10) de f implican que φ es un homomorfismo bien definido, en vista de (3.9). □

Es posible reformular la definición de producto tensorial en términos categóricos. Para cada $M \in\in \mathsf{Mod}\text{-}A$ y $N \in\in A\text{-}\mathsf{Mod}$, sea $\mathsf{C}(M,N)$ la categoría cuyos *objetos* son aplicaciones A-equilibradas de $M \times N$ en algún grupo abeliano. Un *morfismo* entre $g : M \times N \to R$ y $h : M \times N \to S$ es un homomorfismo de grupos abelianos $\theta : R \to S$ tal que $\theta \circ g = h$:

$$\begin{array}{ccc} & \overset{g}{\nearrow} & R \\ M \times N & & \downarrow{\scriptstyle \theta} \\ & \underset{h}{\searrow} & S \end{array}$$

Entonces un producto tensorial de M y N sobre A es un *objeto inicial* $\rho : M \times N \to T$ en la categoría $\mathsf{C}(M,N)$; el cual, si existe, es esencialmente único. La Proposición 3.31 demuestra esa existencia y dice que la *aplicación canónica* $\eta : M \times N \to M \otimes_A N$ es el objeto inicial deseado.

Si N es un A-módulo a la izquierda, el grupo abeliano $A \otimes_A N$ es también un A-módulo a la izquierda, al definir $a(b \otimes y) := ab \otimes y$ para $a, b \in A$, $y \in N$. Si M es un A-módulo a la derecha, el grupo abeliano $M \otimes_A A$ es también un A-módulo a la derecha, al colocar $(x \otimes a)b := x \otimes ab$ para $a, b \in A$, $x \in M$.

Lema 3.32. *Si $N \in\in A\text{-}\mathsf{Mod}$, entonces $A \otimes_A N \simeq N$ en $A\text{-}\mathsf{Mod}$. También, si $M \in\in \mathsf{Mod}\text{-}A$, entonces $M \otimes_A A \simeq M$ en $\mathsf{Mod}\text{-}A$.*

Demostración. Defínase $\alpha : N \to A \otimes_A N$ y $\beta : A \otimes_A N \to N$ por

$$\alpha(y) := 1 \otimes y, \qquad \beta\left(\textstyle\sum_j a_j \otimes y_j\right) := \sum_j a_j y_j.$$

Es fácil ver que α y β son A-homomorfismos y que $\beta \circ \alpha = 1_N$, $\alpha \circ \beta = 1_{A \otimes_A N}$.

Además, $\alpha'(x) := x \otimes 1$, $\beta'\left(\sum_k x_k \otimes a_k\right) := \sum_k x_k a_k$ son morfismos inversos en $\mathsf{Mod}\text{-}A$. □

Lema 3.33. *$g \in \mathrm{Hom}_A(N,N')$, entonces hay un único homomorfismo de grupos abelianos $f \otimes g : M \otimes_A N \to M' \otimes_A N'$ que cumple*

$$(f \otimes g)(x \otimes y) := f(x) \otimes g(y), \quad \textit{para todo} \quad x \in M,\ y \in N.$$

Demostración. Defínase $h\colon M \times N \to M' \otimes_A N'$ por $h(x,y) := f(x) \otimes g(y)$. Es claro que h es aditiva en ambos variables porque f, g son aditivos. Además, si $a \in A$, entonces

$$h(xa,y) = f(xa) \otimes g(y) = f(x)a \otimes g(y) = f(x) \otimes ag(y) = f(x) \otimes g(ay) = h(x,ay),$$

así que h es A-equilibrada. La Proposición 3.31 ahora proporciona el homomorfismo deseado $f \otimes g$ tal que $(f \otimes g)(x \otimes y) = (f \otimes g)(\eta(x,y)) = h(x,y) = f(x) \otimes g(y)$. □

Es importante notar que la expresión $z = \sum_j x_j \otimes y_j$ de un elemento $z \in M \otimes_A N$ como suma finita de tensores simples *no es única, en general*. Sin embargo, cuando N es un A-módulo *libre*, se puede tomar los y_j de entre una base fija de N (¿por qué?). En ese caso, si $\sum_{j=1}^n x_j \otimes y_j = \sum_{j=1}^n x'_j \otimes y_j$, entonces $\sum_{j=1}^n (x_j - x'_j) \otimes y_j = 0$. Sea $g_k\colon N \to A$ el morfismo (bien definido, porque los y_j forman una base de N) dado por $g_k\big(\sum_j a_j y_j\big) := a_k$. Entonces el homomorfismo $1_M \otimes g_k\colon M \otimes_A N \to M$ queda definido por los dos Lemas anteriores y se obtiene

$$x_k - x'_k = (1_M \otimes g_k)\big(\textstyle\sum_{j=1}^n (x_j - x'_j) \otimes y_j\big) = (1_M \otimes g_k)(0) = 0,$$

de modo que los componentes x_j de la expresión $z = \sum_j x_j \otimes y_j$ son únicos.

De igual modo, si M es libre y si se toma los x_j de entre una base de M, entonces los $y_j \in N$ en la expresión $z = \sum_j x_j \otimes y_j$ quedan determinados.

Proposición 3.34. *Si M es un A-módulo a la derecha, si $\{N_j : j \in J\}$ es una familia de A-módulos a la izquierda, entonces hay un isomorfismo*

$$M \otimes_A \left(\bigoplus_{j\in J} N_j\right) \simeq \bigoplus_{j\in J} (M \otimes_A N_j).$$

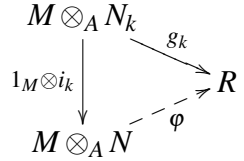
Demostración. Escríbase $N := \bigoplus_{j\in J} N_j$ y sean $i_k\colon N_k \to N$, para $k \in J$, las inyecciones canónicas. Estas definen homomorfismos de grupos $1_M \otimes i_k\colon M \otimes_A N_k \to M \otimes_A N$. Si R es un grupo abeliano y si $g_k \in \mathrm{Hom}_{\mathbb{Z}}(M \otimes_A N_k, R)$ para cada k, sean $\eta_k\colon M \times N_k \to M \otimes_A N_k$ las aplicaciones canónicas. Luego cada $g_k \circ \eta_k\colon M \times N_k \to R$ es A-equilibrada, de modo que

$$\big(x, \textstyle\sum_j y_j\big) \longmapsto \sum_j g_j(\eta_j(x,y_j)) = \sum_j g_j(x \otimes y_j), \quad \text{con sumas finitas,}$$

define una aplicación A-equilibrada $g\colon M \times N \to R$. Por la Proposición 3.31, hay un único homomorfismo $\varphi\colon M \otimes_A N \to R$ tal que

$$\varphi\big(x \otimes \textstyle\sum_j y_j\big) = g\big(x, \sum_j y_j\big) = \sum_j g_j(x \otimes y_j),$$

para $x \in M$, $\sum_j y_j \in N$. En particular, es $\varphi \circ (1_M \otimes i_k) = g_k$ para cada $k \in J$:



Se concluye que $M \otimes_A N$ es el coproducto categórico en Ab (es decir, la suma directa) de los grupos $M \otimes_A N_k$ y que los homomorfismos $1_M \otimes i_k$ son las inyecciones canónicas que definen la suma directa. □

Del mismo modo, se demuestra que $\left(\bigoplus_{i\in I} M_i\right) \otimes_A N \simeq \bigoplus_{i\in I}(M_i \otimes_A N)$ cuando N es un A-módulo a la izquierda y $\{M_i : i \in I\}$ es una familia de A-módulos a la derecha.

Definición 3.35. Sea R un A-módulo a la derecha. Si $f \in \mathrm{Hom}_A(M,N)$ es un homomorfismo entere dos A-módulos a la izquierda, entonces $f_\sharp \equiv 1_R \otimes f : R \otimes_A M \to R \otimes_A N$ es un homomorfismo de grupos abelianos. Las correspondencias $M \mapsto R \otimes_A M$ y $f \mapsto 1_R \otimes f$ definen un *funtor* covariante $t_R \equiv \underline{(R \otimes_A -)} : A\text{-Mod} \to \mathsf{Ab}$.

Proposición 3.36. *Si R es un A-módulo a la derecha, el funtor $t_R : A\text{-Mod} \to \mathsf{Ab}$ es exacto a la derecha.*

Demostración. Sea $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ una sucesión exacta corta en A-Mod. Hay que mostrar que la sucesión siguiente es exacta:

$$R \otimes_A L \xrightarrow{f_\sharp} R \otimes_A M \xrightarrow{g_\sharp} R \otimes_A N \longrightarrow 0,$$

es decir, que $g_\sharp$ es sobreyectivo, que $g_\sharp \circ f_\sharp = 0$ y que $\operatorname{im} f_\sharp = \ker g_\sharp$.

Como $g : M \to N$ es sobreyectivo, cada elemento de $R \otimes_A N$ es una suma finita de la forma $z = \sum_j r_j \otimes g(x_j) = g_\sharp\left(\sum_j r_j \otimes x_j\right)$. Luego $g_\sharp$ es sobreyectivo.

La hipótesis $g \circ f = 0$ implica que

$$g_\sharp(f_\sharp(r \otimes w)) = g_\sharp(r \otimes f(w)) = r \otimes g(f(w)) = 0$$

para cada tensor simple $r \otimes w$ en $R \otimes_A L$; como dichos tensores simples generan el grupo $R \otimes_A L$, se concluye que $g_\sharp \circ f_\sharp = 0$. En particular, se obtiene $\operatorname{im} f_\sharp \subseteq \ker g_\sharp$.

Entonces hay un homomorfismo $\theta : (R \otimes_A M)/\operatorname{im} f_\sharp \to R \otimes_A N$ determinado por

$$\theta(r \otimes x + \operatorname{im} f_\sharp) := g_\sharp(r \otimes x) = r \otimes g(x).$$

Escríbase $[r \otimes x] \equiv r \otimes x + \operatorname{im} f_\sharp$ para denotar la coclase del tensor simple $r \otimes x$. Resulta que esta coclase depende solamente de r y $g(x)$. En efecto, si $r \in R$, $y \in N$, sean $x, x' \in M$ dos elementos tales que $y = g(x) = g(x')$. Entonces $g(x - x') = 0$, así que $x - x' = f(w)$ para algún $w \in L$. Luego $r \otimes x = r \otimes x' + f_\sharp(r \otimes w)$; por ende, vale $[r \otimes x] = [r \otimes x']$.

Luego hay una aplicación bien definida $h : R \times N \to (R \otimes_A M)/\operatorname{im} f_\sharp$ dada por $h(r,y) := [r \otimes x]$ cuando $y = g(x)$. Es claro que h es aditiva en sus dos argumentos y además

$$h(ra, y) = [ra \otimes x] = [r \otimes ax] = h(r, ay),$$

porque $g(ax) = a\,g(x) = ay$ cuando $g(x) = y$. Luego h es A-equilibrada. La Proposición 3.31 produce un homomorfismo de grupos $\varphi : R \otimes_A N \to (R \otimes_A M)/\operatorname{im} f_\sharp$ tal que $\varphi \circ \eta = h$, es decir, $\varphi(r \otimes y) = [r \otimes x]$ cuando $y = g(x)$. Se concluye que φ es un inverso para θ; en particular, θ es un isomorfismo.

Si $\pi\colon R\otimes_A M \to (R\otimes_A M)/\operatorname{im} f_\sharp$ es el homomorfismo cociente, entonces

$$\theta(\pi(r\otimes x)) = \theta[r\otimes x] = r\otimes g(x) = g_\sharp(r\otimes x)$$

para $r\in R$, $x\in M$. Luego $\theta\circ\pi = g_\sharp$. Como θ es un isomorfismo, es $\ker(\theta\circ\pi) = \ker\pi$, de donde se obtiene $\ker g_\sharp = \ker\pi = \operatorname{im} f_\sharp$. □

Lema 3.37. *Si H es un grupo abeliano de torsión (es decir, cada elemento es de orden finito) y si Q es un grupo abeliano divisible, entonces $H\otimes_{\mathbb{Z}} Q = 0$.*

Demostración. Sea $h\otimes y$ un tensor simple en $H\otimes_{\mathbb{Z}} Q$ y sea $m\in\mathbb{N}^*$ tal que $mh = 0$. Existe $x\in Q$ tal que $mx = y$. Entonces,

$$h\otimes y = h\otimes mx = mh\otimes x = 0\otimes x = 0.$$

Pero los tensores simples generan el grupo $H\otimes_{\mathbb{Z}} Q$; por lo tanto, es $H\otimes_{\mathbb{Z}} Q = 0$. □

Ejemplo 3.38. El funtor $(R\otimes_A -)$ no es exacto en general. Tómese $A = \mathbb{Z}$ y $R = \mathbb{Z}/m$ para $m\in\{2,3,\dots\}$. La sucesión exacta de grupos abelianos

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\ i\ } \mathbb{Q} \xrightarrow{\ p\ } \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

donde $i\colon \mathbb{Z}\hookrightarrow\mathbb{Q}$ es la inclusión y $p\colon \mathbb{Q}\hookrightarrow\mathbb{Q}/\mathbb{Z}$ es la aplicación cociente, tiene la siguiente imagen bajo el funtor $(\mathbb{Z}/m\otimes_{\mathbb{Z}} -)$:

$$0 \longrightarrow \mathbb{Z}/m\otimes_{\mathbb{Z}}\mathbb{Z} \xrightarrow{\ i_\sharp\ } \mathbb{Z}/m\otimes_{\mathbb{Z}}\mathbb{Q} \xrightarrow{\ p_\sharp\ } \mathbb{Z}/m\otimes_{\mathbb{Z}}\mathbb{Q}/\mathbb{Z} \longrightarrow 0\,.$$

Ahora $\mathbb{Q}$ y $\mathbb{Q}/\mathbb{Z}$ son divisibles, así que el segundo y el tercer grupo se anulan. El Lema 3.32 muestra que $\mathbb{Z}/m\otimes_{\mathbb{Z}}\mathbb{Z}\simeq\mathbb{Z}/m$. Por tanto, la última sucesión corta se simplifica en

$$0 \longrightarrow \mathbb{Z}/m \longrightarrow 0 \longrightarrow 0 \longrightarrow 0,$$

la cual evidentemente no es exacta en $\mathbb{Z}/m$.

Si M es un A-módulo a la izquierda, hay un funtor $t'_M \equiv (-\otimes_A M)\colon \mathsf{Mod}\text{-}A \to \mathsf{Ab}$ dado por $R\mapsto R\otimes_A M$ y $h\mapsto h\otimes 1_M$. Este funtor (covariante) es también exacto a la derecha: si $0\longrightarrow R\xrightarrow{h} S\xrightarrow{k} T\longrightarrow 0$ una sucesión exacta corta en Mod-A, la sucesión siguiente es exacta:

$$R\otimes_A M \xrightarrow{h\otimes 1_M} S\otimes_A M \xrightarrow{k\otimes 1_M} T\otimes_A M \longrightarrow 0.$$

La demostración de la Proposición 3.36 se repite, *mutatis mutandis*.

► Si A es un anillo *conmutativo*, un A-módulo M es simultáneamente un objeto de A-Mod y de Mod-A, al convenir en que

$$ax \equiv xa, \quad \text{para todo} \quad x\in M,\ a\in A.$$

Si M y N son A-módulos, entonces $M \otimes_A N$ es también un A-módulo, bajo la acción

$$a(x \otimes y) := ax \otimes y = x \otimes ay, \quad \text{para} \quad x \in M,\ y \in N,\ a \in A.$$

En este caso, una función $f\colon M \times N \to R$ en un tercer A-módulo R que cumple (3.10) ahora se llama una **aplicación A-bilineal**. Por la Proposición 3.31, esta función da lugar a un único homomorfismo de A-módulos $\varphi\colon M \otimes_A N \to R$ tal que $\varphi \circ \eta = f$, etcétera. En este caso, los funtores $(R \otimes_A -)$ y $(- \otimes_A M)$ llevan A-Mod en A-Mod y siempre son exactos a la derecha.

► Para poder hablar de *bilinealidad* en el contexto de anillos no conmutativos, se introduce el concepto de *bimódulo* con respecto a dos anillos.

Definición 3.39. Sean A y B dos anillos cualesquiera. Un ***A*-*B*-bimódulo** es un grupo abeliano M que es simultáneamente un *A-módulo a la izquierda* y un *B-módulo a la derecha*, tal que las dos acciones de anillos sean compatibles, es decir, tal que

$$(ax)b = a(xb) \quad \text{para todo} \quad x \in M,\ a \in A,\ b \in B. \tag{3.12}$$

Luego se puede escribir $axb := (ax)b = a(xb)$, sin ambigüedad.

Un *morfismo* de A-B-bimódulos es una aplicación aditiva $f\colon M \to N$ que es un A-homomorfismo y un B-homomorfismo a la vez:

$$f(axb) = a\,f(x)\,b \quad \text{para} \quad x \in M,\ a \in A,\ b \in B.$$

De este modo, los A-B-bimódulos forman una categoría, A-B-Bimod.

Para indicar que $M \in\in A$-B-Bimod, a veces se escribe ${}_AM_B$.

Ejemplo 3.40. Cualquier anillo A es naturalmente un A-A-bimódulo, mediante el producto de A por ambos lados: la condición (3.12) es simplemente la asociatividad del producto.

Ejemplo 3.41. Sea $B = M_n(A)$ y considérese $\underline{A^n} = A \oplus A \oplus \cdots \oplus A$ (n veces) como la colección de *vectores de columna* con n entradas en A. Entonces A^n es un $M_n(A)$-A-bimódulo.

Por otro lado (literalmente), sea ${}^n\underline{A} := A \oplus A \oplus \cdots \oplus A$ (n veces), considerado como la colección de *vectores de fila* con n entradas en A. Entonces ${}^nA$ es un A-$M_n(A)$-bimódulo.

Ejemplo 3.42. Si M es un A-módulo *a la derecha*, sea $B := \mathrm{End}_A(M)$ el anillo de A-endomorfismos $\beta : M \to M$. Entonces M es también un B-módulo *a la izquierda*, al definir $\underline{\beta \cdot x \equiv \beta(x)}$ para $x \in M$, $\beta \in B$. La condición $\beta(xa) = \beta(x)a$ muestra que M es un B-A-bimódulo.

Proposición 3.43. *Si A y B son dos anillos y si L es un A-módulo a la derecha, M es un A-B-bimódulo y N es un B-módulo a la izquierda, entonces hay un isomorfismo de grupos abelianos*

$$\begin{aligned} \psi : (L \otimes_A M) \otimes_B N &\xrightarrow{\simeq} L \otimes_A (M \otimes_B N) \\ (w \otimes x) \otimes y &\longmapsto w \otimes (x \otimes y). \end{aligned} \tag{3.13}$$

Demostración. Fíjese que $L \otimes_A M$ es un B-módulo a la derecha y que $M \otimes_B N$ es un A-módulo a la izquierda, al definir

$$(w \otimes x)b := w \otimes xb, \qquad a(x \otimes y) := ax \otimes y,$$

para $b \in B$, $a \in A$, $w \in L$, $x \in M$, $y \in N$. Entonces $(L \otimes_A M) \otimes_B N$ y también $L \otimes_A (M \otimes_B N)$ son grupos abelianos bien definidos.

Los tensores simples $(w \otimes x) \otimes y$ generan el grupo abeliano $(L \otimes_A M) \otimes_B N$, así que la receta $\psi((w \otimes x) \otimes y) := w \otimes (x \otimes y)$ determina el homomorfismo ψ unívocamente, una vez establecida su existencia.

Para todo $a \in A$, vale

$$wa \otimes (x \otimes y) = w \otimes a(x \otimes y) = w \otimes (ax \otimes y)$$

en $L \otimes_A (M \otimes_B N)$. Luego, para $y \in N$ fijo, la fórmula $f_y(w,x) := w \otimes (x \otimes y)$ define una aplicación A-equilibrada $f_y \colon L \times M \to L \otimes_A (M \otimes_B N)$. Por tanto, hay un homomorfismo $\varphi_y \colon L \otimes_A M \to L \otimes_A (M \otimes_B N)$ dado por $\varphi_y(w \otimes x) := w \otimes (x \otimes y)$. En seguida, la fórmula $g(w \otimes x, y) := \varphi_y(w \otimes x)$ define una aplicación de $(L \otimes_A M) \otimes_B N$ en $L \otimes_A (M \otimes_B N)$ que es aditiva en ambos variables. Además, para todo $b \in B$, vale

$$g((w \otimes x)b, y) = g(w \otimes xb, y) = w \otimes (xb \otimes y) = w \otimes (x \otimes by) = g(w \otimes x, by),$$

o sea, g es B-equilibrado. Luego hay un homomorfismo $\psi \colon (L \otimes_A M) \otimes_B N \to L \otimes_A (M \otimes_B N)$ tal que

$$\psi((w \otimes x) \otimes y) = g(w \otimes x, y) = w \otimes (x \otimes y).$$

En otras palabras, ψ cumple (3.13).

El mismo procedimiento, *mutatis mutandis*, muestra que hay un homomorfismo

$$\chi : L \otimes_A (M \otimes_B N) \longrightarrow (L \otimes_A M) \otimes_B N : w \otimes (x \otimes y) \longmapsto (w \otimes x) \otimes y.$$

Es claro que ψ, χ son inversos uno del otro; en particular, ψ es un isomorfismo de grupos. □

Corolario 3.44. *Si A, B, C, D son cuatro anillos y sean ${}_DL_A$, ${}_AM_B$ y ${}_BN_C$ tres bimódulos para los pares de anillos indicados. Entonces los dos lados de* (3.13) *son D-C-bimódulos y la aplicación $\psi \colon (L \otimes_A M) \otimes_B N \to L \otimes_A (M \otimes_B N)$ es un isomorfismo de D-C-bimódulos.* ⊟

La condición de *asociatividad hasta isomorfismo* del producto tensorial, manifestado en (3.13), requiere que L sea un A-módulo a la derecha y que N sea un B-módulo a la izquierda. En cambio, si N es un B-módulo a la derecha, la fórmula (3.13) puede perder sentido, pero se abre la puerta a otra fórmula no menos importante, que se verá a continuación.

Proposición 3.45. *Si A y B son dos anillos y si L es un A-módulo a la derecha, M es un A-B-bimódulo y N es un B-módulo a la derecha, entonces hay un isomorfismo de grupos abelianos*

$$\mathrm{Hom}_B(L \otimes_A M, N) \simeq \mathrm{Hom}_A(L, \mathrm{Hom}_B(M, N)). \tag{3.14}$$

Demostración. En ambos lados de la relación (3.14), las expresiones Hom_B y Hom_A denotan aplicaciones B-lineales [respectivamente, A-lineales] *a la derecha*. Hay que constatar que el grupo abeliano $\mathrm{Hom}_B(M,N)$ es un A-módulo a la derecha. En efecto, si $\varphi \in \mathrm{Hom}_B(M,N)$, $a \in A$, se define

$$(\varphi a)(x) := \varphi(ax) \quad \text{para todo} \quad x \in M.$$

Si $a,c \in A$, el cálculo $(\varphi a)c : x \mapsto (\varphi a)(cx) = \varphi(acx)$ muestra que $(\varphi a)c = \varphi(ac)$; luego, $\varphi \mapsto \varphi a$ es una acción de A a la derecha sobre el grupo abeliano $\mathrm{Hom}_B(M,N)$. De esta forma, se obtiene $\mathrm{Hom}_B(M,N) \in\in \mathsf{Mod}\text{-}A$ y el lado derecho de (3.14) adquiere sentido.

Si $f\colon L \otimes_A M \to N$ es B-lineal, defínase $\hat{f}\colon L \to \mathrm{Hom}_B(M,N)$ por $\hat{f}(w)\colon x \mapsto f(w \otimes x)$. Para verificar que $\hat{f}(w)$ es B-lineal, nótese que

$$\hat{f}(w)(xb) = f(w \otimes xb) = f((w \otimes x)b) = f(w \otimes x)b = \hat{f}(w)(x)b$$

para $w \in L$, $x \in M$, $b \in B$; la tercera igualdad usa la B-linealidad de f. Para ver que $\hat{f}$ es A-lineal, fíjese que

$$\hat{f}(wa) : x \mapsto f(wa \otimes x) = f(w \otimes ax) = \hat{f}(w)(ax) = [\hat{f}(w)a](x),$$

o bien $\hat{f}(wa) = \hat{f}(w)a$ para $w \in L$, $a \in A$. Entonces $\alpha\colon f \mapsto \hat{f}$ es un homomorfismo de $\mathrm{Hom}_B(L \otimes_A M,N)$ en $\mathrm{Hom}_A(L,\mathrm{Hom}_B(M,N))$.

Inversamente, si $g\colon L \to \mathrm{Hom}_B(M,N)$ es A-lineal, defínase $h\colon L \times M \to N$ por $h(w,x) := g(w)(x)$. Esta función h es evidentemente aditiva en sus dos variables; además, vale

$$h(wa,x) = g(wa)(x) = [g(w)a](x) = g(w)(ax) = h(w,ax)$$

para $w \in L$, $x \in M$, $a \in A$; la segunda igualdad usa la A-linealidad de g. Entonces h es una aplicación A-equilibrada y por lo tanto existe un homomorfismo $\tilde{g}\colon L \otimes_A M \to N$ tal que $\tilde{g}(w \otimes x) = h(w,x) = g(w)(x)$ para cada tensor simple $w \otimes x$ en $L \otimes_A M$. Para ver que $\tilde{g}$ es B-lineal, fíjese que

$$\tilde{g}((w \otimes x)b) = \tilde{g}(w \otimes xb) = g(w)(xb) = g(w)(x)b = \tilde{g}(w \otimes x)b$$

cuando $w \in L$, $x \in M$, $b \in B$; la tercera igualdad usa la B-linealidad de $g(w)$. Luego $\beta\colon g \mapsto \tilde{g}$ es un homomorfismo de $\mathrm{Hom}_A(L,\mathrm{Hom}_B(M,N))$ en $\mathrm{Hom}_B(L \otimes_A M,N)$.

Es evidente que α y β son inversos uno del otro; en particular, α es el isomorfismo deseado. □

El isomorfismo (3.14) es un ejemplo importante de una construcción categórica. El A-B-bimódulo M determina dos funtores covariantes, $t^M \equiv (- \otimes_A M) : \mathsf{Mod}\text{-}A \to \mathsf{Mod}\text{-}B$ y también $h^M \equiv \mathrm{Hom}_B(M,-) : \mathsf{Mod}\text{-}B \to \mathsf{Mod}\text{-}A$. Entonces el isomorfismo (3.14) se escribe como

$$\alpha_{L,N} : \mathrm{Hom}_B(t^M L,N) \xrightarrow{\simeq} \mathrm{Hom}_A(L,h^M N),$$

para todo $L \in\in \mathsf{Mod}\text{-}A$, $N \in\in \mathsf{Mod}\text{-}B$. Los funtores t^M y h^M son ejemplos de la definición siguiente.

Definición 3.46. Sean C y D dos categorías y sean $\mathcal{F}\colon \mathsf{C} \to \mathsf{D}$ y $\mathcal{G}\colon \mathsf{D} \to \mathsf{C}$ dos funtores. Se dice que $\mathcal{G}$ es un **adjunto a la derecha** de $\mathcal{F}$, y que $\mathcal{F}$ es un **adjunto a la izquierda** de $\mathcal{G}$, si hay *isomorfismos naturales*

$$\eta_{A,B} : \mathrm{Hom}_{\mathsf{D}}(\mathcal{F}A, B) \xrightarrow{\simeq} \mathrm{Hom}_{\mathsf{C}}(A, \mathcal{G}B), \quad \text{para todo} \quad A \in\in \mathsf{C},\ B \in\in \mathsf{D}.$$

La naturalidad de los $\eta_{A,B}$ en A y B quiere decir que: (i) para cada B fijo, $A \mapsto \eta_{A,B}$ es una transformación natural de $h_B \circ \mathcal{F}$ en $h_{\mathcal{G}B}$; y (ii) para cada A fijo, $B \mapsto \eta_{A,B}$ es una transformación natural de $h^{\mathcal{F}A}$ en $h^A \circ \mathcal{G}$.

Ejemplo 3.47. Si M es un A-B-bimódulo, los funtores $t^M\colon \mathsf{Mod}\text{-}A \to \mathsf{Mod}\text{-}B$ y $h^M\colon \mathsf{Mod}\text{-}B \to \mathsf{Mod}\text{-}A$ son adjuntos. Por la Proposición 3.45, sólo hay que verificar la naturalidad de los isomorfismos $\alpha_{L,N}$. Si $\varphi \in \mathrm{Hom}_A(L, L')$, se requiere que el siguiente diagrama conmuta:

$$\begin{array}{ccc} \mathrm{Hom}_B(t^M L, N) & \xrightarrow{\alpha_{L,N}} & \mathrm{Hom}_A(L, h^M N) \\ {\scriptstyle (\varphi\otimes 1_M)^*}\uparrow & & \uparrow{\scriptstyle \varphi^*} \\ \mathrm{Hom}_B(t^M L', N) & \xrightarrow{\alpha_{L',N}} & \mathrm{Hom}_A(L', h^M N) \end{array}$$

Además, si $\psi \in \mathrm{Hom}_B(N, N')$, se requiere la conmutatividad del diagrama

$$\begin{array}{ccc} \mathrm{Hom}_B(t^M L, N) & \xrightarrow{\alpha_{L,N}} & \mathrm{Hom}_A(L, h^M N) \\ {\scriptstyle \psi_*}\downarrow & & \downarrow{\scriptstyle (\psi_*)_*} \\ \mathrm{Hom}_B(t^M L, N') & \xrightarrow{\alpha_{L,N'}} & \mathrm{Hom}_A(L, h^M N') \end{array}$$

Es fácil chequear que estos dos diagramas conmutan.

Definición 3.48. Un A-módulo a la izquierda M es **llano** si para cada morfismo inyectivo $g\colon R \to S$ en $\mathsf{Mod}\text{-}A$, el homomorfismo $g^\sharp \equiv g \otimes 1_M : R \otimes_A M \to S \otimes_A M$ es también inyectivo.

Un A-módulo a la derecha R es **llano** si para cada morfismo inyectivo $f\colon M \to N$ en A-Mod, el homomorfismo $f_\sharp \equiv 1_M \otimes f : R \otimes_A M \to R \otimes_A N$ es también inyectivo.

Lema 3.49. *Un A-módulo $M \in\in A$-Mod es llano si y sólo si el funtor $t^M = (- \otimes_A M)$ es exacto. Un A-módulo $R \in\in \mathsf{Mod}$-A es llano si y sólo si el funtor $t_R = (R \otimes_A -)$ es exacto.*

Demostración. Basta probar la segunda afirmación; la primera se demuestra de modo similar. Sea, entonces, $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ una sucesión exacta corta en A-Mod. Para la sucesión corta siguiente,

$$0 \longrightarrow R \otimes_A L \xrightarrow{f_\sharp} R \otimes_A M \xrightarrow{g_\sharp} R \otimes_A N \longrightarrow 0,$$

la Proposición 3.36 muestra que $g_\sharp$ es sobreyectivo y que $\mathrm{im}\, f_\sharp = \ker g_\sharp$. Como f es un monomorfismo, esta sucesión corta de grupos abelianos es exacta si y sólo si $f_\sharp$ es también inyectivo, lo cual queda garantizado si y sólo si R es llano. □

Lema 3.50. *El anillo A es un A-módulo llano, tanto en A-*Mod *como en* Mod-A.

Demostración. Basta mostrar que A sea llano en Mod-A. Si $N \in\in A$-Mod, entonces hay un isomorfismo $\beta_N \colon A \otimes_A N \to N$ dado por $\beta_N(a \otimes y) := ay$. Si $f \in \mathrm{Hom}_A(M,N)$ es inyectivo, entonces el siguiente diagrama:

$$\begin{array}{ccc} A \otimes_A M & \xrightarrow{\beta_M} & M \\ {\scriptstyle f_\sharp}\downarrow & & \downarrow{\scriptstyle f} \\ A \otimes_A N & \xrightarrow{\beta_N} & N \end{array}$$

conmuta, porque si $a \in A$, $x \in M$, vale

$$\beta_N(f_\sharp(a \otimes x)) = \beta_N(a \otimes f(x)) = a\,f(x) = f(ax) = f(\beta_M(a \otimes x)).$$

Luego $f_\sharp = \beta_N^{-1} \circ f \circ \beta_M$ es inyectivo cuando f es inyectivo. □

Proposición 3.51. *Si $N = \bigoplus_{j\in J} N_j$ en A-*Mod*, entonces N es un A-módulo llano si y sólo si cada sumando directo N_j es un A-módulo llano.*

Demostración. La Proposición 3.34 construye, para cada A-módulo a la derecha R, un isomorfismo

$$\theta_R : R \otimes_A N \xrightarrow{\simeq} \bigoplus_{j\in J} (R \otimes_A N_j) \quad \text{dado por} \quad \theta_R\big(r \otimes (y_j)_j\big) := (r \otimes y_j)_j\,.$$

Estos isomorfismos son naturales: si S es otro A-módulo a la derecha y si $g \in \mathrm{Hom}_A(R,S)$, entonces hay un homomorfismo de grupos abelianos

$$\tilde{g} : \bigoplus_{j\in J} (R \otimes_A N_j) \longrightarrow \bigoplus_{j\in J} (S \otimes_A N_j) : (r \otimes y_j)_j \longmapsto (g(r) \otimes y_j)_j$$

que hace conmutar el siguiente diagrama:

$$\begin{array}{ccc} R \otimes_A N & \xrightarrow{\theta_R} & \bigoplus_{j\in J} (R \otimes_A N_j) \\ {\scriptstyle g\otimes 1_N}\downarrow & & \downarrow{\scriptstyle \tilde{g}} \\ S \otimes_A N & \xrightarrow{\theta_S} & \bigoplus_{j\in J} (S \otimes_A N_j). \end{array}$$

Supóngase que $g \colon R \to S$ es un monomorfismo en Mod-A. Como θ_R y θ_S son isomorfismos, $g \otimes 1_N$ es inyectivo si y sólo si $\tilde{g}$ es inyectivo, si y sólo si cada $g \otimes 1_{N_j}$ es inyectivo. □

Corolario 3.52. *Cada A-módulo proyectivo es un A-módulo llano.*

Demostración. Si L es una A-módulo *libre*, entonces $L \simeq A^{(J)}$ para algún J. El Lema 3.50 y la Proposición 3.51 muestran que $A^{(J)}$ es un A-módulo llano.

Si P es un A-módulo proyectivo, entonces hay otro A-módulo (también proyectivo) R y un A-módulo libre L tal que $L \simeq P \oplus R$. La Proposición anterior muestra que P y R son llanos porque L es llano. □

Ejemplo 3.53. Hay A-módulos llanos que no son proyectivos, aun cuando $A = \mathbb{Z}$. Se dice que un grupo abeliano H es **libre de torsión** si 0 es el único elemento de orden finito en H. Resulta que $H \in\in \mathsf{Ab}$ es un $\mathbb{Z}$-módulo llano si y sólo si H es libre de torsión. En particular, el grupo aditivo $\mathbb{Q}$ de números racionales es un $\mathbb{Z}$-módulo llano.

Por otro lado, $\mathbb{Q}$ no admite una base como $\mathbb{Z}$-módulo (¿por qué no?), así que $\mathbb{Q}$ no es un $\mathbb{Z}$-módulo libre, así que tampoco es un $\mathbb{Z}$-módulo proyectivo, por el Corolario 3.5.

3.4 Equivalencia de Morita para anillos

Si A y B son anillos isomorfos, entonces las categorías A-Mod y B-Mod son también isomorfos. (Si $\varphi\colon A \to B$ es un isomorfismo, se puede considerar cada $M \in\in B$-Mod como un A-módulo a la izquierda, al definir $a \cdot x := \varphi(a)x$ para $a \in A$, $x \in M$. De este modo se obtiene un funtor $\mathcal{T}_\varphi\colon B\text{-Mod} \to A\text{-Mod}$ tal que $\mathcal{T}_\varphi M = M$ y $\mathcal{T}_\varphi f = f$ para $f \in \mathrm{Mor}(B\text{-Mod})$, el cual es un isomorfismo de categorías.) Como ya se ha observado, esta noción de isomorfismo categórico es muy restrictivo. Sería más interesante establecer condiciones sobre un par de anillos A y B que garantice que las categorías A-Mod y B-Mod sean *equivalentes*.

Lo ideal sería obtener dos funtores $\mathcal{F}\colon A\text{-Mod} \to B\text{-Mod}$ y $\mathcal{G}\colon B\text{-Mod} \to A\text{-Mod}$, bajo condiciones apropiadas, que son cuasiinversos uno del otro. De este modo, a cada A-módulo se le hace corresponder un B-módulo mediante una receta explícita. Un importante trabajo de Morita identifica esas condiciones y permite exhibir esas correspondencias.[8]

Definición 3.54. Sea M un A-módulo *a la derecha*. El **dual** de M es el A-módulo *a la izquierda*

$$\underline{M^*} := \mathrm{Hom}_A(M, A)$$

donde la acción a la izquierda de A sobre M^* es dado por

$$(\underline{af})(x) := a\,f(x), \quad \text{para} \quad a \in A,\ f \in M^*,\ x \in M.$$

Sea $B := \mathrm{End}_A(M) = \mathrm{Hom}_A(M, M)$. Al escribir $\underline{bx} := b(x)$ para $b \in B$, $x \in M$, resulta que M es un B-A-*bimódulo*, ya que

$$b(xa) = b(x)\,a = (bx)a \quad \text{para} \quad a \in A,\ b \in B,\ x \in M,$$

por la A-linealidad de cada $b \in \mathrm{End}_A(M)$.

Lema 3.55. *Si $M \in\in$ Mod-A y si $B = \mathrm{End}_A(M)$, entonces M^* es un A-B-*bimódulo*, al definir*

$$(\underline{af})(x) := a\,f(x), \qquad (\underline{fb})(x) := f(bx), \tag{3.15}$$

para $a \in A$, $b \in B$, $f \in M^*$, $x \in M$.

[8] El artículo básico fue: Kiiti Morita, *Duality for modules and its applications to the theory of rings with minimum condition*, Scientific Reports of the Tokyo Kyoiku Daigaku **6** (1958), 83–142. Hoy en día existen varias versiones de sus teoremas para anillos y hay teoremas análogos en otros contextos, tales como los grupoides simplécticos y las C^*-álgebras. Aquí se sigue el enfoque de Jacobson en su libro *Basic Algebra II*.

Demostración. El primero de las fórmulas (3.15) repite la definición de af, el segundo dice que $fb := f \circ b$ en $\mathrm{Hom}_A(M,A)$.

Evidentemente $(a(f_1+f_2)) : x \mapsto a(f_1+f_2)(x) = af_1(x) + af_2(x) = (af_1 + af_2)(x)$ y también $(f_1+f_2)\circ b = f_1 \circ b + f_2 \circ b$ para $f_1, f_2 \in M^*$. Además, si $a_1, a_2 \in A$ y si $b_1, b_2 \in A$, entonces

$$(a_1a_2)f : x \mapsto a_1a_2\, f(x) = a_1(a_2f)(x), \qquad f \circ b_1b_2 = f \circ b_1 \circ b_2 = (f \circ b_1) \circ b_2.$$

Luego $f \mapsto af$ y $f \mapsto fb$ definen acciones de A a la izquierda y de B a la derecha sobre M^*. Para ver que estas acciones son compatibles, fíjese que

$$a(fb) = (af)b \ : \ x \mapsto a\, f(b(x)),$$

todo vez que $a \in A$, $b \in B$, $f \in M^*$. □

Definición 3.56. Sea M un A-módulo a la derecha. Si $x \in M$, $f \in M^*$, la notación

$$\underline{(f,x)} := f(x) \in A$$

define un *apareamiento* $M^* \times M \to A$ que es aditivo en ambos variables, absorbe las acciones de A a cada lado, y además es B-equilibrado:

$$\begin{aligned} (f, x_1+x_2) &= (f,x_1) + (f,x_2), \\ (f_1+f_2, x) &= (f_1,x) + (f_2,x), \\ (f, xa) &= (f,x)a, \\ (af, x) &= a(f,x), \\ (fb, x) &= (f, bx). \end{aligned} \tag{3.16}$$

Estas propiedades son, respectivamente, la aditividad de cada $f \in M^*$; la definición de suma de homomorfismos; la A-linealidad de f; la definición de af; y la definición de fb. La primera, segunda y quinta propiedades establecen la existencia de un homomorfismo

$$e : M^* \otimes_B M \to A \quad \text{dado por} \quad e(f \otimes x) := (f,x),$$

llamada **evaluación**. Las otras propiedades dicen que e es un morfismo de A-A-bimódulos.

Definición 3.57. Sea M un A-módulo a la derecha. Si $x \in M$, $f \in M^*$, se define $\underline{[x,f]} \in B = \mathrm{End}_A(M)$ por[9]

$$[x,f] : z \mapsto x\, f(z).$$

[9]En la física cuántica, la *notación de Dirac* introduce unas expresiones análogas, pero no idénticas, a estos apareamientos de módulos. Dirac denota por $|\lambda\rangle$ el autovector de cierto operador lineal que corresponde al autovalor $\lambda \in \mathbb{C}$. Se escribe $\langle\mu|$ para denotar un forma lineal sobre vectores (un elemento del espacio de Hilbert dual), y la evaluación de $\langle\mu|$ sobre el vector $|\lambda\rangle$ por $\langle\mu\,|\,\lambda\rangle$, el llamado "bra-ket" (del vocablo inglés *bracket*, corchete). El operador de rango uno $|\nu\rangle \mapsto |\lambda\rangle\,\langle\mu\,|\,\nu\rangle$ se denota por $|\lambda\rangle\langle\mu|$, el llamado "ket-bra". Por analogía, las expresiones $[x,f]$ del contexto actual son llamados ket-bras por algunos autores.

Este es un apareamiento $M \times M^* \to B$ que es aditivo en ambos variables, absorbe las acciones de B a cada lado, y además es A-equilibrado:

$$\begin{aligned} [x_1 + x_2, f] &= [x_1, f] + [x_2, f], \\ [x, f_1 + f_2] &= [x, f_1] + [x, f_2], \\ [x, fb] &= [x, f]b, \\ [bx, f] &= b[x, f], \\ [xa, f] &= [x, af]. \end{aligned} \tag{3.17}$$

Estas propiedades se verifican al evaluar ambos lados de cada ecuación sobre un elemento $z \in M$. Ellas establecen la existencia de un morfismo de B-B-bimódulos

$$v : M \otimes_A M^* \to B \quad \text{dado por} \quad v(x \otimes f) := [x, f].$$

Lema 3.58. *La dos apareamientos* $(\cdot,\cdot) : M^* \times M \to A$ *y* $[\cdot,\cdot] : M \times M^* \to B$ *son* compatibles *en el sentido de que*

$$[x, f]\, z = x\,(f, z), \qquad g\,[x, f] = (g, x)\, f$$

para $x, z \in M$ *y* $f, g \in M^*$.

Demostración. La primera igualdad es la definición de $[x, f]$ en B. Para la segunda, obsérvese que para todo $z \in M$, vale

$$\big(g\,[x, f], z\big) = g\big([x, f], z\big) = g([x, f]\, z) = g(x\,(f, z)) = g(x)\,(f, z) = (g, x)\,(f, z) = \big((g, x)\, f, z\big),$$

así que $g\,[x, f]$ y $(g, x)\, f$ son homomorfismos de M en A que tiene el mismo valor en cada elemento de M. □

Definición 3.59. Un **contexto de Morita** es un sexteto (A, B, M, N, e, v), donde

- A y B son anillos;
- M es un B-A-bimódulo y N es un A-B-bimódulo;
- $e : M^* \otimes_B M \to A$ es un morfismo de A-A-bimódulos;
- $v : M \otimes_A M^* \to B$ es un morfismo de B-B-bimódulos; y
- al escribir $(y, x) := e(y \otimes x)$ y también $[x, y] := v(x \otimes y)$ para $x \in M$, $y \in N$, valen

$$[x, y]\, z = x\,(y, z), \quad w\,[x, y] = (w, x)\, y \quad \text{para todo} \quad x, z \in M,\ y, w \in N.$$

Ejemplo 3.60. Si M es un A-módulo a la derecha, las definiciones y los lemas anteriores dicen que $(A, \mathrm{End}_A(M), M, M^*, e, v)$ es un contexto de Morita.

Por la simetría de las fórmulas anteriores, $(\mathrm{End}_A(M), A, M^*, M, v, e)$ es otro contexto de Morita.

Ejemplo 3.61. Sea A un anillo y sea $n \in \mathbb{N}^*$. Sea A^n y ${}^nA$ dos copias del A-módulo libre de rango n, cuyos elementos son organizados como columnas y filas, respectivamente (véase el Ejemplo 3.41). A cada columna $x \in A^n$ le corresponde su transpuesta $x^t \in {}^nA$. Defínase dos homomorfismos e, v por

$$e(y^t \otimes x) := y^t x \in A, \qquad v(x \otimes y^t) := xy^t \in M_n(A),$$

para $x, y \in A^n$. Entonces $(A, M_n(A), A^n, {}^nA, e, v)$ es un contexto de Morita.

Es evidente que e es sobreyectiva. Cualquier matriz $C \in M_n(A)$ es una suma finita $C = \sum_{i,j} c_{ij}\, e_i e_j^t$ donde $\{e_1, \ldots, e_n\}$ es la base estándar de A^n; por tanto, v es sobreyectivo. De hecho, e y v son biyectivos, en vista del teorema que sigue.

Definición 3.62. Sea M un A-módulo a la derecha. Denótese por $T(M)$ el subgrupo aditivo de A generado por $\{\, (f,x) : f \in M^*,\ x \in M \,\}$. Como $(\cdot,\cdot)$ absorbe las multiplicaciones por elementos de A, véase (3.16), $T(M)$ es un ideal (bilateral) de A, llamado el **ideal de traza** del módulo M. Se dice que M es un **generador** de Mod-A si $T(M) = A$ o, lo que es lo mismo, si $1 \in T(M)$.

De igual manera se define $T(N)$ para un A-módulo a la izquierda N; se dice que N es un generador de A-Mod si $T(N) = A$.

Un A-módulo a la derecha M es un **progenerador** si[10] (i) M es un *generador* de Mod-A; y (ii) M es *proyectivo* y *finitamente generado* en Mod-A.

Teorema 3.63 (Morita I)**.** *Sea (A, B, M, N, e, v) un contexto de Morita en donde los homomorfismos e, v son* sobreyectivos*. Entonces:*[11]

(a) M es un progenerador en Mod-A *y en* B-Mod*; también, N es un progenerador en* A-Mod *y en* Mod-B.

(b) Las aplicaciones $\underline{e} : M^* \otimes_B M \to A$, $\underline{v} : M \otimes_A M^* \to B$ son isomorfismos.

(c) Al poner $\langle y| : x \mapsto (y,x)$, la correspondencia $y \mapsto \langle y| : N \to M^* = \mathrm{Hom}_A(M,A)$ es un isomorfismo de A-B-bimódulos. También, al poner $|x\rangle : y \mapsto (y,x)$, la correspondencia $x \mapsto |x\rangle : M \to N^* = \mathrm{Hom}_B(N,B)$ es un isomorfismo de B-A-bimódulos.

(d) Al poner $\lambda(b) : x \mapsto bx$, se obtiene un isomorfismo de anillos $\lambda : B \to \mathrm{End}_A(M)$. También, al poner $\lambda'(a) : y \mapsto ay$, se obtiene un isomorfismo de anillos $\lambda' : A \to \mathrm{End}_B(N)$.

(e) Los funtores $t^N = (- \otimes_A N)$ y $t^M = (- \otimes_B M)$ definen una equivalencia de categorías entre Mod-A *y* Mod-B*. También, los funtores $t_M = (M \otimes_A -)$ y $t_N = (N \otimes_B -)$ definen una equivalencia de categorías entre* A-Mod *y* B-Mod.

[10] El lamentable vocablo *progenerador* indica simplemente un generador proyectivo; la generación finita se da por sentado.

[11] Hay una convención que reparte los resultados de Morita en tres teoremas, denombrados I, II, III.

Demostración. Por la simetría del enunciado bajo $A \leftrightarrow B$, $M \leftrightarrow N$, $e \leftrightarrow v$, basta mostrar una afirmación en cada inciso.

Ad (a): La sobreyectividad de v implica que $\sum_{j=1}^{m}[e_j,u_j]=1$ en B para unos elementos $\{e_1,\ldots,e_m\}\subset M$ y $\{u_1,\ldots,u_m\}\subset N$. Luego, si $x\in M$, vale

$$x=\sum_{j=1}^{m}[e_j,u_j]x=\sum_{j=1}^{m}e_j\,(u_j,x). \tag{3.18}$$

Entonces, al definir $f_j\in M^*$ por $f_j(x):=(u_j,x)$, se ve que los conjuntos $\{e_1,\ldots,e_m\}\subset M$ y $\{f_1,\ldots,f_m\}\subset M^*$ definen una *base proyectiva* de M como A-módulo a la derecha. (Véase el Ejercicio 3.4.) Luego M es proyectivo en Mod-A. Además, la fórmula (3.18) muestra que M es generado por el conjunto finito $\{e_1,\ldots,e_m\}$.

La sobreyectividad de e implica que cada $a\in A$ es de la forma $a=\sum_{i=1}^{r}[y_i,x_i]$ para algunos elementos $x_i\in M$, $y_i\in N$. Por tanto $A=T(M)$, así que M es un generador en Mod-A.

Ad (b): Como e es sobreyectivo, hay elementos $\{c_1,\ldots,c_n\}\subset M$ y $\{v_1,\ldots,v_n\}\subset N$ tales que $\sum_{k=1}^{n}(v_k,c_k)=1$ en A. Si $\sum_{i=1}^{r}y_i\otimes x_i\in\ker e$, de modo que $\sum_{i=1}^{r}(y_i,x_i)=0$ en A, entonces

$$\begin{aligned}\sum_{i=1}^{r}y_i\otimes x_i&=\sum_{i,k}y_i\otimes x_i\,(v_k,c_k)=\sum_{i,k}y_i\otimes[x_i,v_k]\,c_k\\&=\sum_{i,k}y_i\,[x_i,v_k]\otimes c_k=\sum_{i,k}(y_i,x_i)\,v_k\otimes c_k=\sum_{k=1}^{n}0\otimes c_k=0.\end{aligned}$$

Luego e es inyectivo. Se comprueba que v es inyectivo de igual manera.

Ad (c): Si $a\in A$, $b\in B$, $x\in M$, $y\in N$, entonces

$$\begin{aligned}\langle ay|(x)&=(ay,x)=a\,(y,x)=a\,\langle y|(x),\\\langle yb|(x)&=(yb,x)=(y,bx)=\langle y|(bx)=\langle y|b(x),\end{aligned}$$

así que $y\mapsto\langle y|:N\to M^*$ es un homomorfismo de A-B-bimódulos. Si $\langle y|=0$ en M^*, entonces $(y,x)=0$ para todo $x\in M$, luego $y=\sum_{j=1}^{m}y\,[e_j,u_j]=\sum_{j=1}^{m}(y,e_j)\,u_j=0$ en N; por ende, $y\mapsto\langle y|$ es inyectivo.

Si $f\in M^*$, sea $w:=\sum_{j=1}^{m}f(e_j)\,u_j\in N$. Entonces, para cada $x\in M$ vale

$$\langle w|(x)=(w,x)=\sum_{j=1}^{m}f(e_j)\,(u_j,x)=f\left(\sum_{j=1}^{m}e_j\,(u_j,x)\right)=f\left(\sum_{j=1}^{m}[e_j,u_j]x\right)=f(x),$$

por tanto $\langle w|=f$. Luego, $y\mapsto\langle y|$ es sobreyectivo.

Ad (d): La igualdad $(bx)a=b(xa)$ muestra que la correspondencia $x\mapsto bx$ es A-lineal a la derecha; luego, $\lambda(b)\in\mathrm{End}_A(M)$ para cada $b\in B$. Las identidades $(b_1+b_2)x=b_1x+b_2x$, $(b_1b_2)x=b_1(b_2x)$ muestran que $\lambda:B\to\mathrm{End}_A(M)$ es un homomorfismo de anillos.

Si $\lambda(b)=0$, entonces $bx=0$ para $x\in M$, así que $b=\sum_{j=1}^{m}b\,[e_j,u_j]=\sum_{j=1}^{m}[be_j,u_j]=0$. Por tanto, λ es inyectivo.

Si $\beta \in \mathrm{End}_A(M)$, sea $d := \sum_{j=1}^m [\beta(e_j), u_j] \in B$. Para cada $x \in M$, vale

$$dx = \sum_{j=1}^m [\beta(e_j), u_j]x = \sum_{j=1}^m \beta(e_j)\,(u_j, x) = \beta\left(\sum_{j=1}^m e_j\,(u_j, x)\right) = \beta\left(\sum_{j=1}^m [e_j, u_j]\,x\right) = \beta(x),$$

así que $\beta = \lambda(d)$. Luego, λ es sobreyectivo.

Ad (e): El funtor compuesto $t^M t^N \colon \mathsf{Mod}\text{-}A \to \mathsf{Mod}\text{-}A$ cumple $t^M t^N R = (R \otimes_A N) \otimes_B M$ para $R \in\in \mathsf{Mod}\text{-}A$. Ahora hay una cadena de isomorfismos

$$(R \otimes_A N) \otimes_B M \xrightarrow{\psi_R} R \otimes_A (N \otimes_B M) \xrightarrow{1_R \otimes e} R \otimes_A A \xrightarrow{\beta_R} R$$

obtenidos de la Proposición 3.43, la parte (b) de este mismo Teorema y del Lema 3.32. Su composición $\theta_R := \beta_R \circ (1_R \otimes e) \circ \psi_R$ define un isomorfismo natural $\theta \colon t^M t^N \to 1_{\mathsf{Mod}\text{-}A}$. Además, el funtor compuesto $t^N t^M \colon \mathsf{Mod}\text{-}B \to \mathsf{Mod}\text{-}B$ cumple $t^N t^M S = (S \otimes_B M) \otimes_A N$ para $S \in\in \mathsf{Mod}\text{-}B$. Hay otra cadena de isomorfismos

$$(S \otimes_B M) \otimes_A N \xrightarrow{\psi'_S} S \otimes_B (M \otimes_A N) \xrightarrow{1_S \otimes v} S \otimes_B B \xrightarrow{\beta'_S} S$$

cuya composición $\eta_S := \beta'_S \circ (1_S \otimes v) \circ \psi'_S$ define un isomorfismo natural $\eta \colon t^N t^M \to 1_{\mathsf{Mod}\text{-}B}$. De esta manera se ha construido una equivalencia de categorías entre $\mathsf{Mod}\text{-}A$ y $\mathsf{Mod}\text{-}B$. □

Proposición 3.64. *Si (A, B, M, N, e, v) es un contexto de Morita con $\underline{e}$ y $\underline{v}$ sobreyectivos, entonces los* centros *de los anillos A y B son* isomorfos*: $Z(A) \simeq Z(B)$.*

Demostración. La parte (d) del Teorema 3.63 construye un isomorfismo de anillos $\lambda \colon B \to \mathrm{End}_A(M)$ con los operadores de multiplicación a la izquierda $\lambda(b) \colon x \mapsto bx$. De modo similar, las operadores de multiplicación a la derecha $\rho(a) \colon x \mapsto xa$ conforman un *antiisomorfismo*[12] $\rho \colon A \to \mathrm{End}_B(M)$; fíjese que

$$\rho(a_1 a_2)(x) = x(a_1 a_2) = (xa_1)a_2 = \rho(a_2)\rho(a_1)(x) \quad \text{para todo} \quad a_1, a_2 \in A,\ x \in M.$$

Denótese por $\mathrm{End}(M)$ el anillo de endomorfismos de M como grupo abeliano. Entonces $\mathrm{End}_A(M)$ y $\mathrm{End}_B(M)$ son subanillos de $\mathrm{End}(M)$, a saber,

$$\mathrm{End}_A(M) = \{\, \beta \in \mathrm{End}(M) : \beta(xa) \equiv \beta(x)a \text{ si } a \in A \,\},$$
$$\mathrm{End}_B(M) = \{\, \alpha \in \mathrm{End}(M) : \alpha(bx) \equiv b\alpha(x) \text{ si } b \in B \,\}.$$

La condición $(bx)a = b(xa)$ y la sobreyectividad de λ y ρ muestran que cada uno de estos subanillos centraliza el otro. Luego

$$Z(\mathrm{End}_A(M)) = \mathrm{End}_A(M) \cap \mathrm{End}_B(M) = Z(\mathrm{End}_B(M)).$$

El isomorfismo $\lambda : B \to \mathrm{End}_A(M)$ y el antiisomorfismo $\rho : A \to \mathrm{End}_B(M)$ inducen, por restricción a los centros en cada caso, dos isomorfismos $\lambda : Z(B) \to Z(\mathrm{End}_A(M))$ y $\rho : Z(A) \to Z(\mathrm{End}_B(M))$. Luego $Z(A) \simeq Z(B)$ mediante el isomorfismo $\lambda^{-1} \circ \rho$. □

[12] Un *antiisomorfismo* entre dos anillos es una biyección aditiva que revierte el orden de la multiplicación.

Definición 3.65. Dos anillos son **Morita-equivalentes**, escrito $A \overset{\text{M}}{\sim} B$, si existen bimódulos M y N e *isomorfismos* $\underline{e}$, $\underline{v}$ tales que (A,B,M,N,e,v) sea un contexto de Morita.

Ejemplo 3.66. Si P es un progenerador para Mod-A, entonces los anillos A y $\mathrm{End}_A(P)$ son Morita-equivalentes. De hecho, con $B := \mathrm{End}_A(P)$ se puede formar el contexto de Morita (A,B,P,P^*,e,v) del Ejemplo 3.60. Al leer la parte (a) de la demostración del Teorema 3.63 *contrario sensu*, se observa que P es un progenerador *si y sólo si* e y v son sobreyectivos.

Nótese el corolario de que $A \simeq \mathrm{End}_B(P^*)$ en este caso.

Ejemplo 3.67. Si A es un anillo y $n \in \mathbb{N}^*$, entonces A y $M_n(A)$ son Morita-equivalentes. Esto es una consecuencia directa del Ejemplo 3.61; o bien, se puede observar que A^n es un progenerador para Mod-A.

Nótese el corolario de que $Z(M_n(A)) \simeq Z(A)$; en particular, vale $Z(M_n(A)) \simeq A$ cuando A es conmutativo.

El segundo teorema de Morita, apodado "Morita II", establece que las categorías Mod-A y Mod-B son equivalentes si y sólo si A y B son anillos Morita-equivalentes. En más detalle: dados dos funtores $\mathcal{F}\colon$ Mod-$A \to$ Mod-B y $\mathcal{G}\colon$ Mod-$B \to$ Mod-A que son cuasiinversos, se puede construir progeneradores P para Mod-A y Q para Mod-B tales que $\mathcal{F} \simeq t^Q$ y $\mathcal{G} \simeq t^P$ mediante isomorfismos naturales.[13]

3.5 Ejercicios sobre módulos proyectivos e inyectivos

Ejercicio 3.1. Encontrar dos funciones $f\colon \mathbb{Z}/2 \to \mathbb{Z}/4$ y $g\colon \mathbb{Z}/4 \to \mathbb{Z}/2$ tales que el diagrama

$$0 \longrightarrow \mathbb{Z}/2 \xrightarrow{f} \mathbb{Z}/4 \xrightarrow{g} \mathbb{Z}/2 \longrightarrow 0$$

sea una sucesión exacta corta (SEC) de $\mathbb{Z}/4$-módulos. Mostrar que esta SEC no escinde. Concluir que un submódulo de un módulo proyectivo no es necesariamente proyectivo.

Ejercicio 3.2. (a) Si $e \in A$ es un elemento idempotente (es decir, $e^2 = e$) del anillo A, mostrar que el A-módulo cíclico $\underline{Ae}$ es proyectivo.

(b) Si $p = [p_{ij}] \in M_n(A)$ es una matriz idempotente, sea $\underline{A^n p}$ el A-módulo (a la izquierda) con elementos $\boldsymbol{c}p$, donde cada $\boldsymbol{c} \in A^n$ se considera como "vector de fila" con n entradas. Mostrar que $A^n p$ es un A-módulo proyectivo.

Ejercicio 3.3. Si A es un anillo conmutativo y si $M,N \in\in A$-Mod, mostrar que $\mathrm{Hom}_A(M,N)$ es también un A-módulo, al definir $(a\varphi)(x) := \varphi(ax)$ para $a \in A$, $\varphi \in \mathrm{Hom}_A(M,N)$, $x \in M$. Si P y R son A-módulos proyectivos, mostrar que $\mathrm{Hom}_A(P,R)$ es un A-módulo proyectivo.

[13] Un tercer teorema, "Morita III", es aplicable cuando dos anillos A y B son Morita-equivalentes: clasifica las diversas equivalencias entre Mod-A y Mod-B en términos de clases de isomorfismos de progeneradores P que cumplen $P \otimes_A P^* \simeq B$ y $P^* \otimes_B P \simeq A$. Véase, por ejemplo, el libro: Carl Faith, *Rings, Modules and Categories I*, Springer, New York, 1973.

Ejercicio 3.4. Si M es un A-módulo a la izquierda, su dual $M^* := \mathrm{Hom}_A(M,A)$ es un A-módulo a la derecha. Una parte $\{ x_j : j \in J \} \subset M$ se llama una **base proyectiva** de M si hay $\{ \varphi_j : j \in J \} \subset M^*$ tal que, para cada $x \in M$, $\{ \varphi_j : f_j(x) \neq 0 \}$ es finito y vale

$$x = \sum_{j \in J} \varphi_j(x)\, x_j.$$

Mostrar que un A-módulo P es proyectivo si y sólo si P posee una base proyectiva.

Ejercicio 3.5. Sea P un A-módulo (a la izquierda) proyectivo y finitamente generado. Mostrar que $P^* = \mathrm{Hom}(P,A)$ es un A-módulo (a la derecha) proyectivo y finitamente generado.

Concluir que el homomorfismo natural $\eta_P \colon P \to P^{**}$ es biyectivo.

Ejercicio 3.6. En la categoría A-Mod, mostrar que el *pullback* del diagrama $L \xrightarrow{f} N \xleftarrow{g} M$ se obtiene como sigue:

$$\begin{array}{ccc} R & \xrightarrow{p} & M \\ {\scriptstyle q}\downarrow & & \downarrow{\scriptstyle g} \\ L & \xrightarrow{f} & N \end{array}$$

Sea $R := \{ (x,y) \in L \oplus M : f(x) = g(y) \}$; defínase $p(x,y) := y$, $q(x,y) := x$ para $(x,y) \in R$.
⟦ Indicación: Es cuestión de mostrar que este cuadrado es conmutativo y que es un objeto terminal de entre todos los cuadrados conmutativos que incluyen el diagrama original. ⟧

Comprobar que si f es sobreyectivo, entonces p es también sobreyectivo.

Ejercicio 3.7 (*Lema de Schanuel*)**.** Si $0 \longrightarrow L \xrightarrow{f} P \xrightarrow{g} N \longrightarrow 0$ y $0 \longrightarrow M \xrightarrow{j} Q \xrightarrow{k} N \longrightarrow 0$ son dos SEC de A-módulos con P y Q proyectivos, mostrar que $L \oplus Q \simeq M \oplus P$.

⟦ Indicación: Considérese el pullback del diagrama $P \xrightarrow{g} N \xleftarrow{k} Q$. ⟧

Ejercicio 3.8. En la categoría A-Mod, mostrar que el *pushout* del diagrama $M \xleftarrow{g} N \xrightarrow{f} L$ se obtiene como sigue:

$$\begin{array}{ccc} N & \xrightarrow{f} & L \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle j} \\ M & \xrightarrow{i} & S \end{array}$$

Sea $S := (L \oplus M)/K$, donde $K := \{ (f(z), -g(z)) : z \in N \}$; defínase $j(x) := (x,0) + K$ para $x \in L$ y además $i(y) := (0,y) + K$ para $y \in M$.
⟦ Indicación: Es cuestión de mostrar que este cuadrado es conmutativo y que es un objeto inicial de entre todos los cuadrados conmutativos que incluyen el diagrama original. ⟧

Comprobar que si f es inyectivo, entonces i es también inyectivo.

Ejercicio 3.9. Sea $m \in \mathbb{N}$ con $m \geq 2$.

(a) Mostrar que $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m, \mathbb{Z}) = 0$ pero $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m, \mathbb{Q}/\mathbb{Z}) \neq 0$. Concluir que el funtor $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m, -)$ no es exacto.

(b) Mostrar que $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) = 0$. Concluir que el funtor $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Z})$ no es exacto.

Ejercicio 3.10. Si A es un anillo entero, sea $\mathbb{F} = \{a/b : a,b \in A,\ b \neq 0\}$ su *cuerpo de fracciones*. Si J es un ideal de A y si $f\colon J \to \mathbb{F}$ es un A-homomorfismo, mostrar que la función $x \mapsto f(x)/x$ es constante, para $x \in J \setminus \{0\}$. Deducir que $\mathbb{F}$ es un A-módulo inyectivo.

Ejercicio 3.11. Sea R un A-módulo a la izquierda y sea S un A-módulo a la derecha. Demostrar que los tres funtores

$$\text{(a)}\quad h^R = \mathrm{Hom}_A(R,-); \qquad \text{(b)}\quad h_R = \mathrm{Hom}_A(-,R); \qquad \text{(c)}\quad t_S = (S \otimes_A -);$$

llevan sucesiones exactas cortas *escindidas* de A-módulos (a la izquierda) en sucesiones exactas cortas *escindidas* de grupos abelianos.

Ejercicio 3.12. (a) Si $m,n \in \mathbb{N}^*$ y si $d = \mathrm{mcd}(m,n) > 1$, demostrar que $\mathbb{Z}/m \otimes_{\mathbb{Z}} \mathbb{Z}/n \simeq \mathbb{Z}/d$.
(b) Demostrar que $\mathbb{Z}/m \otimes_{\mathbb{Z}} m\mathbb{Z} \simeq \mathbb{Z}/m$.

Ejercicio 3.13. Demostrar que $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}$, con un isomorfismo explícito.

Ejercicio 3.14. Si A es un anillo conmutativo y si M y N son A-módulos, construir y verificar un isomorfismo de A-módulos $\tau\colon M \otimes_A N \xrightarrow{\simeq} N \otimes_A M$.

Ejercicio 3.15. Si M es un A-módulo a la izquierda, si N es un B-módulo a la izquierda y si L es un B-A-bimódulo, construir y verificar un isomorfismo de grupos abelianos:

$$\mathrm{Hom}_B(L \otimes_A M, N) \simeq \mathrm{Hom}_A(M, \mathrm{Hom}_B(L,N)).$$

Ejercicio 3.16. Sea M un A-módulo a la derecha llano y sea N un A-B-bimódulo que es llano como B-módulo a la derecha. Demostrar que $M \otimes_A N$ es llano en Mod-B.

Ejercicio 3.17. Si A y B son dos anillos Morita-equivalentes, comprobar que la categoría de A-A-bimódulos y la categoría de B-B-bimódulos son equivalentes.
⟦ Indicación: Para el contexto de Morita (A,B,M,N,e,v), considerar el funtor $M \otimes_A - \otimes_A N$. ⟧

Ejercicio 3.18. Si M es una A-módulo a la derecha, sea $T(M)$ su ideal de traza en A (las sumas finitas de elementos $f(x)$, con $x \in M$, $f \in M^*$). Se dice que $R \in\in$ Mod-A es un **generador** de Mod-A si cualquier $M \in\in$ Mod-A es una suma (no necesariamente directa) de submódulos $M = \sum_{j\in J} g_j(R)$ donde cada $g_j \in \mathrm{Hom}_A(R,M)$. ⟦ Nota: el A-módulo trivial A es un generador porque hay una aplicación cociente $\eta : A^{(J)} \to M$; además, R es un generador si algún R^n es un generador. ⟧ Demostrar que las siguientes condiciones sobre $R \in\in$ Mod-A son equivalentes:

(a) R es un generador de Mod-A.

(b) El funtor $h^R = \mathrm{Hom}_A(R,-)$ es fiel.

(c) $T(R) = A$.

(d) El A-módulo trivial A es un cociente de R^n, para algún $n \in \mathbb{N}^*$.

⟦ Indicación: Para (b) ⇒ (c), considerar la aplicación cociente $p\colon A \to A/T(R)$. ⟧

Ejercicio 3.19. Dos anillos A y B son **Morita-equivalentes**, escrito $A \overset{\text{M}}{\sim} B$, si hay un contexto de Morita (A,B,M,N,e,v) con $\underline{e}$, $\underline{v}$ isomorfismos. Demostrar que esta es una relación de equivalencia (en particular, que esta relación es transitiva.)

Ejercicio 3.20. Sea (A,B,M,N,e,v) un contexto de Morita. El **anillo vinculador** C se define como sigue. Los elementos de C son las matrices

$$\begin{pmatrix} a & y \\ x & b \end{pmatrix}, \quad \text{con} \quad a \in A,\ b \in B,\ x \in M,\ y \in N.$$

La sumas se define entrada por entrada; el producto es dado por

$$\begin{pmatrix} a_1 & y_1 \\ x_1 & b_1 \end{pmatrix} \begin{pmatrix} a_2 & y_2 \\ x_2 & b_2 \end{pmatrix} := \begin{pmatrix} a_1a_2 + (y_1,x_2) & a_1y_2 + y_1b_2 \\ x_1a_2 + b_1x_2 & [x_1,y_2] + b_1b_2 \end{pmatrix},$$

donde se escribe $(y_1,x_2) := e(y_1 \otimes x_2)$ y también $[x_1,y_2] := v(x_1 \otimes y_2)$.

(a) Verificar en detalle que C es un anillo.

(b) Comprobar que $N \oplus B$ es un C-B-bimódulo y que $A \oplus N$ es un A-C-bimódulo.

(c) Si e, v son isomorfismos, mostrar que $C \simeq \text{End}_B(N \oplus B)$. ¿Es válida la implicación inversa?

4 Elementos de Algebra Homológica

Quizás el concepto más importante de la teoría de módulos es el concepto de *homología*. En muchas aplicaciones se presentan sucesiones exactas de grupos abelianos, espacios vectoriales, o módulos sobre un anillo fijo A; acompañadas con otras sucesiones que no son exactas, pero que tienen la propiedad más débil de que la composición de dos morfismos consecutivos es cero. La homología se presenta como una familia de grupos abelianos [o espacios vectoriales, o A-módulos] que mide la *falta de exactitud* de la sucesión de marras.

4.1 Complejos de módulos

La noción principal en homología es un *complejo* de módulos sobre un anillo. Como el nombre indica, se trata de varios módulos, ligados por ciertos homomorfismos. Hay dos maneras de presentar complejos; en el fondo los dos puntos de vista son equivalentes, pero las aplicaciones enfatizan una alternativa sobre la otra. Aquí serán presentados en paralelo.

Definición 4.1. Sea A un anillo cualquiera. Un **complejo (de cadenas**) de A-módulos es una familia $\{C_n : n \in \mathbb{Z}\}$ de A-módulos, junto con un A-homomorfismo $\delta_n : C_n \to C_{n-1}$ para cada n, tales que $\underline{\delta_{n-1} \circ \delta_n = 0}$ en $\mathrm{Hom}_A(C_n, C_{n-2})$ para todo n. Un complejo de cadenas queda ilustrado así:

$$\cdots \longrightarrow C_{n+1} \xrightarrow{\delta_{n+1}} C_n \xrightarrow{\delta_n} C_{n-1} \xrightarrow{\delta_{n-1}} C_{n-2} \longrightarrow \cdots$$

Se denota por $C_\bullet := \bigoplus_n C_n$ la suma directa de todos estos A-módulos.[1] Entonces los δ_n son componentes de un A-homomorfismo $\delta : C_\bullet \to C_\bullet$, llamado la **diferencial** del complejo, tal que $\delta(C_n) \subseteq C_{n-1}$ para cada n y además $\underline{\delta^2 = 0}$. Este complejo será denotado por $(C_\bullet, \delta)$. Los elementos de C_n se llaman ***n*-cadenas**.

Si $C_n = 0$ para $n < 0$, se dice que el complejo de cadenas $(C_\bullet, \delta)$ es *positivo*. Si hay enteros $r \leq s$ tales que $C_n \neq 0$ sólo si $r \leq n \leq s$, se dice que $(C_\bullet, \delta)$ es un complejo *acotado*.

El segundo punto de vista resulta de colocar $C^n := C_{-n}$ y $d_n := \delta_{-n}$ en un complejo de cadenas.

Definición 4.2. Un **complejo (de cocadenas)** de A-módulos es una familia $\{C^n : n \in \mathbb{Z}\}$ de A-módulos, junto con un A-homomorfismo $d_n : C^n \to C^{n+1}$ para cada n, tales que $\underline{d_{n+1} \circ d_n = 0}$ en $\mathrm{Hom}_A(C^n, C^{n+2})$ para todo n. Un complejo de cocadenas queda ilustrado así:

$$\cdots \longrightarrow C^{n-1} \xrightarrow{d_{n-1}} C^n \xrightarrow{d_n} C^{n+1} \xrightarrow{d_{n+1}} C^{n+2} \longrightarrow \cdots$$

Se denota por $C^\bullet := \bigoplus_n C^n$ la suma directa de todos estos A-módulos. Los d_n son componentes de un A-homomorfismo $d : C^\bullet \to C^\bullet$, llamado la **diferencial** del complejo, tal que $d(C^n) \subseteq C^{n+1}$ para cada n y además $\underline{d^2 = 0}$. Este complejo será denotado por $(C^\bullet, d)$. Los elementos de C^n se llaman ***n*-cocadenas**.

Si $C^n = 0$ para $n < 0$, se dice que el complejo de cocadenas $(C^\bullet, d)$ es positivo.

[1] El símbolo $\bullet$ denota un "índice anónimo".

Definición 4.3. Considérese la categoría pequeña S cuyos objetos son todos los conjuntos $[m] := \{0, 1, \ldots, m\}$ para $m \in \mathbb{N}$, y en la cual los morfismos en $\mathrm{Hom}_{\mathsf{S}}([m],[n])$ son las *funciones no decrecientes* $f\colon [m] \to [n]$; es decir, $0 \le j \le k \le m$ implica $0 \le f(j) \le f(k) \le n$.

Denótese por Δ^n el ***n*-símplice estándar**,

$$\Delta^n := \{\, (t_0, \ldots, t_n) \in \mathbb{R}^{n+1} : \text{cada } t_i \ge 0;\ t_0 + t_1 + \cdots + t_n = 1 \,\}.$$

Si $(e_0, \ldots, e_n)$ denota la base estándar de $\mathbb{R}^{n+1}$, entonces los elementos de Δ^n son *combinaciones convexas* de los **vértices** e_j. Una *aplicación afín*[2] $h\colon \Delta^m \to \Delta^n$ queda determinada por los vectores $\{h(e_j) : j = 0, 1, \ldots, m\}$. En particular, cada morfismo $f\colon [m] \to [n]$ de S determina una aplicación afín $\tilde{f}\colon \Delta^m \to \Delta^n$ por $\tilde{f}(e_j) := e_{f(j)}$.

En particular, la k-ésima **faceta** de Δ^n es $\partial_n^k(\Delta^{n-1})$, con $\partial_n^k \equiv \tilde{d}_n^k$, donde $d_n^k\colon [n-1] \to [n]$ es el (único) morfismo que omite k:

$$d_n^k(j) := \begin{cases} j, & \text{si } j < k, \\ j+1, & \text{si } j \ge k. \end{cases}$$

El conjunto $\partial_n^k(\Delta^{n-1})$ es la envoltura convexa de los vértices $\{e_0, \ldots, e_{k-1}, e_{k+1}, \ldots, e_n\}$, es decir, la faceta de Δ^n opuesta al vértice e_k.

Ejemplo 4.4. Sea X un espacio topológico. Una ***n*-símplice singular** en X es una función continua $\sigma\colon \Delta^n \to X$. Sea $C_n(X, \mathbb{Z})$ el grupo abeliano libre generado por todos los n-símplices singulares en X. Sus elementos, llamados n-**cadenas** en X, son "sumas formales" finitas $\sum_{i=1}^{r} m_i \sigma_i$ con coeficientes $m_i \in \mathbb{Z}$.

Para cada $f \in \mathrm{Hom}_{\mathsf{S}}([m],[n])$ hay un homomorfismo de grupos $F^*\colon C_n(X,\mathbb{Z}) \to C_m(X,\mathbb{Z})$ determinado por $F^*\sigma := \sigma \circ f$. En otras palabras, la correspondencia $[n] \mapsto C_n(X,\mathbb{Z})$ determina un *funtor contravariante* $\mathcal{F}\colon \mathsf{S}^\circ \to \mathsf{Ab}$.

Defínase el *homomorfismo de borde* $\delta_n\colon C_n(X,\mathbb{Z}) \to C_{n-1}(X,\mathbb{Z})$ por

$$\delta_n \sigma := \sum_{k=0}^{n} (-1)^k (\sigma \circ \partial_n^k).$$

(Geométricamente, δ_n reemplaza la función $\sigma\colon \Delta^n \to X$ por una suma alternada de las restricciones de σ a cada una de sus facetas. Esta suma alternada es una $(n-1)$-cadena singular.) Debe notarse que

$$\begin{aligned} \delta_{n-1}(\delta_n \sigma) &= \sum_{k=0}^{n} \sum_{l=0}^{n-1} (-1)^{k+l} \sigma \circ (\partial_n^k \circ \partial_{n-1}^l) \\ &= \sum_{k \le l} (-1)^{k+l} \sigma \circ (\partial_n^k \circ \partial_{n-1}^l) + \sum_{k > l} (-1)^{k+l} \sigma \circ (\partial_n^l \circ \partial_{n-1}^{k-1}), \end{aligned} \tag{4.1}$$

[2]Una **aplicación afín** $g\colon X \to Z$ entre dos conjuntos convexos $X \subseteq \mathbb{R}^{m+1}$ y $Z \subseteq \mathbb{R}^{n+1}$ es una función que cumple $g((1-t)x + ty) = (1-t)\,g(x) + t\,g(y)$ para $x, y \in X$, $0 \le t \le 1$. En otras palabras, g es la restricción de una aplicación lineal de $\mathbb{R}^{m+1}$ en $\mathbb{R}^{n+1}$.

al notar que $d_n^k \circ d_{n-1}^l = d_n^l \circ d_{n-1}^{k-1}$ si $k > l$. De hecho, los dos lados de esta igualdad llevan

$$j \mapsto j \text{ para } j < l, \qquad j \mapsto j+1 \text{ para } l \le j < k-1, \qquad j \mapsto j+2 \text{ para } k-1 \le j.$$

Al cambiar $(l, k-1) \mapsto (k, l)$ en la última sumatoria de (4.1), que también cambia la condición $k > l$ en $l \ge k$ y el signo $(-1)^{k+l}$ en $(-1)^{l+k+1}$, así que $\delta_{n-1}(\delta_n \sigma) = 0$ por cancelación de signos.

Luego, $(C_\bullet(X, \mathbb{Z}), \delta)$ es un complejo de cadenas, llamado el **complejo singular** del espacio topológico X.

Ejemplo 4.5. Sea M una variedad diferencial real, compacta y sin borde, de dimensión n. (Como ejemplos, puede mencionarse la esfera $\mathbb{S}^n$, el toro $\mathbb{T}^n$ —el producto cartesiano de n círculos— el plano proyectivo $\mathbb{R}P^n$, entre otros.) Las funciones suaves $f : M \to \mathbb{R}$ forman un anillo $A = C^\infty(M, \mathbb{R})$ que en general admite muchos divisores de cero.[3]

Las **formas diferenciales** sobre M de grado k son elementos de un espacio vectorial real $\mathcal{A}^k(M, \mathbb{R})$. En coordenadas locales definidas sobre una carta local $U \subset M$, una tal *k-forma* se escribe así:

$$\omega = \sum_{|I|=k} \omega_I \, dx^{i_1} \wedge dx^{i_2} \wedge \cdots \wedge dx^{i_k},$$

donde cada ω_I es una función suave de U en $\mathbb{R}$; los índices $I = \{i_1, \ldots, i_k\}$ se escriben en orden creciente, $i_1 < I_2 < \cdots < i_k$, ya que el "producto cuña" de diferenciales dx^i es anticonmutativa. Para $k = 0, 1, \ldots, n$, cada $\mathcal{A}^k(M, \mathbb{R})$ es un A-módulo proyectivo.[4]

La **derivada exterior** $d = d_k : \mathcal{A}^k(M, \mathbb{R}) \to \mathcal{A}^{k+1}(M, \mathbb{R})$ se define por la fórmula local

$$d\omega = \sum_{|I|=k} \sum_{j \notin I} \frac{\partial \omega_I}{\partial x^j} \, dx^j \wedge dx^{i_1} \wedge \cdots \wedge dx^{i_k}.$$

Es un ejercicio clásico de cálculo diferencial (basado en la igualdad de derivadas parciales mixtas de segundo orden) comprobar que $d(d\omega) = 0$. Luego $(\mathcal{A}^\bullet(M, \mathbb{R}), d)$ es un complejo acotado de cocadenas, llamado el **complejo de de Rham**[5] de la variedad diferencial M.

Definición 4.6. Sea $\mathbb{F}$ un cuerpo cualquiera. Un **álgebra (asociativa)** sobre $\mathbb{F}$ es un anillo A que es a la vez un espacio vectorial sobre $\mathbb{F}$, tal que $\lambda(ac) = (\lambda a)c = a(\lambda c)$ para $a, c \in A$ y $\lambda \in \mathbb{F}$; es decir, la multiplicación escalar y el producto del anillo A son compatibles.

[3] La compacidad de M implica que todas estas funciones suaves son acotadas y que $1 \in A$. Para considerar variedades no acotadas, se recomienda usar $C_0^\infty(M, \mathbb{R})$, el conjunto de funciones suaves que "se anulan en el infinito", el cual excluye la función constante 1. Para obtener un anillo, se agregan las funciones constantes; el anillo resultante es isomorfo a $C^\infty(M^+, \mathbb{R})$ donde M^+ es la *compactificación de un punto* de la variedad localmente compacta M.

[4] Una variedad diferencial compacta admite una **partición de la unidad** finita: esta es una familia de funciones $f_1, \ldots, f_m \in C^\infty(M, \mathbb{R})$, cada f_r con soporte en el dominio de una carta local U_r de M, con valores no negativos, tales que $\sum_{r=1}^m f_r(x) = 1$ para cada $x \in M$. Si $\omega \in \mathcal{A}^k(M, \mathbb{R})$, entonces $\omega = \sum_{r=1}^m f_r \omega$ y cada $f_r \omega$ tiene una expansión como producto cuña de diferenciales sobre la carta U_r. Los $(f_r \, dx^{i_1} \wedge \cdots \wedge dx^{i_k})|_{U_r}$ forman una base proyectiva de $\mathcal{A}^k(M, \mathbb{R})$ como módulo sobre $C^\infty(M, \mathbb{R})$.

[5] En 1933, *Georges de Rham* demostró que la cohomología de este complejo es finitodimensional y depende solamente de la topología (en vez de la estructura diferencial) de la variedad M.

Fíjese que $(a,c) \mapsto ac$ es una aplicación $\mathbb{F}$-bilineal de $A \times A$ en A. Por tanto, da lugar a una aplicación $\mathbb{F}$-*lineal* $m\colon A \otimes_{\mathbb{F}} A \to A$ definido por $m(a \otimes c) := ac$.

En lo sucesivo, cuando A y B son $\mathbb{F}$-álgebras, se escribirá $\underline{A \otimes B}$ simplemente, en vez de $A \otimes_{\mathbb{F}} B$ para denotar su producto tensorial sobre $\mathbb{F}$.

Ejemplo 4.7. Sea A un álgebra asociativa sobre un cuerpo $\mathbb{F}$ y sea M un A-A-bimódulo. Defínase otros A-A-bimódulos $C_n(A,M)$, para $n \in \mathbb{N}$, por

$$C_n(A,M) := M \otimes \underbrace{A \otimes \cdots \otimes A}_{n \text{ veces}} \equiv M \otimes A^{\otimes n},$$

donde $C_0(A,M) := M$ y se toman productos tensoriales sobre $\mathbb{F}$.

Defínase el *homomorfismo de borde* $\beta = \beta_n\colon C_n(A,M) \to C_{n-1}(A,M)$ —el cual es un homomorfismo de A-A-bimódulos— por

$$\beta(x \otimes a_1 \otimes \cdots \otimes a_n) := xa_1 \otimes a_2 \otimes \cdots \otimes a_n + \sum_{j=1}^{n-1} (-1)^j x \otimes a_1 \otimes \cdots \otimes a_j a_{j+1} \otimes \cdots \otimes a_n + (-1)^n a_n x \otimes a_1 \otimes \cdots \otimes a_{n-1}, \tag{4.2}$$

para $x \in M$, $a_1, \ldots, a_n \in A$. Es fácil verificar que $\beta_{n-1} \circ \beta_n = 0$. El complejo $(C_\bullet(A,M), \beta)$ se llama el **complejo de Hochschild** de A *con coeficientes en* M.

En particular, al tomar $M = A$ se obtiene $C_n(A,A) = A^{\otimes(n+1)}$; suele escribirse $x = a_0$ en la fórmula anterior.

Ejemplo 4.8. Sea A una $\mathbb{F}$-álgebra asociativa, de nuevo, y sea M un A-A-bimódulo. Cada aplicación n-lineal $\varphi\colon A^n \to M$ da lugar a una aplicación lineal $\widetilde{\varphi}\colon A^{\otimes n} \to M$ por la fórmula $\widetilde{\varphi}(a_1 \otimes \cdots \otimes a_n) := \varphi(a_1, \ldots, a_n)$. La totalidad de estas aplicaciones n-lineales de A^n en M es un A-A-bimódulos $C^n(A,M)$, donde $C^0(A,M) := M$ y $C^1(A,M) = \mathrm{Hom}_{\mathbb{F}}(A,M)$. Defínase un *homomorfismo de coborde* $b = b_n\colon C^n(A,M) \to C^{n+1}(A,M)$ por

$$b\varphi(a_0,a_1,\ldots,a_n) := a_0\,\varphi(a_1,\ldots,a_n) + \sum_{j=1}^{n-1} (-1)^j \varphi(a_0,a_1,\ldots,a_j a_{j+1},\ldots,a_n) + (-1)^n \varphi(a_0,a_1,\ldots,a_{n-1})\,a_n. \tag{4.3}$$

Es fácil verificar que $b_{n+1} \circ b_n = 0$. Luego $(C^\bullet(A,M), b)$ es un complejo de cocadenas.

En particular, al tomar $M = A^* = \mathrm{Hom}_{\mathbb{F}}(A,\mathbb{F})$ se puede identificar $C^n(A,A^*)$ con las formas $(n+1)$-lineales sobre A o bien con el espacio $\mathbb{F}$-vectorial dual de $A^{\otimes(n+1)} = C_n(A,A)$.

Definición 4.9. Sea A un anillo. Los complejos (de cadenas) de A-módulos (a la izquierda) forman una categoría A-Compl. Un morfismo de complejos $f\colon (C_\bullet, \delta) \to (D_\bullet, \delta')$, también llamado una **aplicación de cadenas**, es una familia de A-homomorfismos $f_n\colon C_n \to D_n$ tales que $\underline{f_{n-1} \circ \delta_n = \delta'_n \circ f_n}\colon C_n \to D_{n-1}$ para todo $n \in \mathbb{Z}$. En otras palabras, el siguiente diagrama es conmutativo:

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & C_{n+1} & \xrightarrow{\delta_{n+1}} & C_n & \xrightarrow{\delta_n} & C_{n-1} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle f_{n+1}} & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \\
\cdots & \longrightarrow & D_{n+1} & \xrightarrow{\delta'_{n+1}} & D_n & \xrightarrow{\delta'_n} & D_{n-1} & \longrightarrow & \cdots
\end{array}$$

De modo similar, un morfismo de complejos de cocadenas $g\colon (C^\bullet, d) \to (D^\bullet, d')$, también llamado una **aplicación de cocadenas**, es una familia de A-homomorfismos $g_n\colon C^n \to D^n$ tales que $g_{n+1} \circ d_n = d'_n \circ g_n : C^n \to D^{n+1}$ para todo $n \in \mathbb{Z}$. En otras palabras, el siguiente diagrama es conmutativo:

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & C^{n-1} & \xrightarrow{d_{n-1}} & C^n & \xrightarrow{d_n} & C^{n+1} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle g_{n-1}} & & \downarrow{\scriptstyle g_n} & & \downarrow{\scriptstyle g_{n+1}} & & \\
\cdots & \longrightarrow & D^{n-1} & \xrightarrow{d'_{n-1}} & D^n & \xrightarrow{d'_n} & D^{n+1} & \longrightarrow & \cdots
\end{array}$$

Definición 4.10. Sea $(C_\bullet, \delta)$ un complejo de cadenas de A-módulos. Una n-cadena $x \in C_n$ es un n**-ciclo** si $\delta_n x = 0$; además, x es un n**-borde** si $x = \delta_{n+1} y$ para algún $y \in C_{n+1}$.

La totalidad de los n-ciclos es $Z_n := \ker \delta_n$, un A-submódulo de C_n. La totalidad de los n-bordes es $B_n := \operatorname{im} \delta_{n+1}$, otro A-submódulo de C_n.

La condición $\delta_n \circ \delta_{n+1} = 0$ garantiza que $B_n \subseteq Z_n$. El A-módulo cociente

$$H_n := Z_n / B_n = \ker \delta_n / \operatorname{im} \delta_{n+1}$$

es el n-ésimo **módulo de homología** del complejo $(C_\bullet, \delta)$. El A-módulo $H_\bullet := \bigoplus_{n\in\mathbb{Z}} H_n$ es la *homología* (a secas) del complejo de marras. Fíjese que $H_\bullet = 0$ si y sólo si el complejo es una sucesión exacta.

Definición 4.11. Sea $(C^\bullet, d)$ un complejo de cocadenas de A-módulos. Una n-cocadena $\varphi \in C^n$ es un n**-cociclo** si $d_n \varphi = 0$; además, φ es un n**-coborde** si $\varphi = d_{n-1} \psi$ para algún $\psi \in C^{n-1}$.

La totalidad de los n-cociclos es $Z^n := \ker d_n$, un A-submódulo de C^n. La totalidad de los n-cobordes es $B^n := \operatorname{im} d_{n-1}$, otro A-submódulo de C^n.

La condición $d_n \circ d_{n-1} = 0$ garantiza que $B^n \subseteq Z^n$. El A-módulo cociente

$$H^n := Z^n / B^n = \ker d_n / \operatorname{im} d_{n-1}$$

es el n-ésimo **módulo de cohomología** del complejo $(C^\bullet, d)$. El A-módulo $H^\bullet := \bigoplus_{n\in\mathbb{Z}} H^n$ es la *cohomología* (a secas) del complejo de marras. Fíjese que $H^\bullet = 0$ si y sólo si el complejo es una sucesión exacta.

Ejemplo 4.12. La homología del complejo singular $(C_\bullet(X, \mathbb{Z}), \delta)$ se llama la **homología singular** $H_\bullet(X, \mathbb{Z})$ del espacio topológico X. Este es un grupo abeliano, es decir, un $\mathbb{Z}$-módulo.

Ejemplo 4.13. Si M es una variedad diferencial real (compacta y sin borde), la cohomología del complejo $(\mathcal{A}^\bullet(M, \mathbb{R}), d)$ se llama la **cohomología de de Rham** $H^\bullet_{\mathrm{dR}}(M)$ de la variedad diferencial M. Este es un módulo sobre el anillo conmutativo $C^\infty(M, \mathbb{R})$.

En este caso, los k-cociclos son las *k-formas cerradas*: $\omega \in Z^k(M, \mathbb{R})$ si $d\omega = 0$. Los k-cobordes son las *k-formas exactas*: $\omega \in B^k(M, \mathbb{R})$ si $\omega = d\eta$ para alguna $(k-1)$-forma η. Entonces $H^k_{\mathrm{dR}}(M)$ consta de clases de k-formas cerradas, módulo las k-formas exactas.

Cada espacio vectorial real $C_k(M,\mathbb{R}) := C_k(M,\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{R}$ tiene dimensión finita (ya que M es compacta), igual al rango del sumando libre de torsión de $C_k(M,\mathbb{Z})$. Sus espacios vectoriales duales $C^k(M,\mathbb{R}) := C_k(M,\mathbb{R})^*$, junto con las aplicaciones lineales $d_k := \delta^t_{k+1}$, forman el complejo de *cocadenas singulares* de la variedad M. La integración sobre símplices,[6]

$$I(\omega) : \sigma \mapsto \int_{\Delta^k} \sigma^* \omega \in \mathbb{R},$$

define una aplicación de cocadenas $I\colon \mathcal{A}^\bullet(M,\mathbb{R}) \to C^\bullet(M,\mathbb{R})$. El teorema de de Rham muestra que este morfismo induce un *isomorfismo* $H^\bullet_{\mathrm{dR}}(M) \simeq H^\bullet(M,\mathbb{R})$ entre las cohomologías de de Rham y singular.[7] Este es el ejemplo paradigmático de un fenómeno interesante: la misma cohomología puede calcularse mediante complejos distintos de diversa naturaleza.

Ejemplo 4.14. Si A es un álgebra asociativa y M es un A-A-bimódulo, la homología del complejo $(C_\bullet(A,M),\beta)$ se llama la **homología de Hochschild** de A *con coeficientes en* M. En el caso particular $M = A$, se escribe $HH_n(A) := H_n(A,A)$.

La cohomología del complejo $(C^\bullet(A,M),b)$ se llama la **cohomología de Hochschild** de A *con coeficientes en* M. En el caso particular $M = A^*$, se escribe $HH^n(A) := H^n(A,A^*)$.

4.2 Sucesiones exactas cortas y largas

Muchas cálculos en álgebra homológica dependen de dos lemas principales, llamados *Lema de Cinco* y el *Lema de la Culebra*.

Lema 4.15 (Lema de Cinco)**.** *Si el siguiente diagrama de A-módulos conmuta y tiene filas exactas:*

$$\begin{array}{ccccccccc} K & \xrightarrow{e} & L & \xrightarrow{f} & M & \xrightarrow{g} & N & \xrightarrow{h} & R \\ \downarrow{\scriptstyle s} & & \downarrow{\scriptstyle t} & & \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle w} \\ K' & \xrightarrow{e'} & L' & \xrightarrow{f'} & M' & \xrightarrow{g'} & N' & \xrightarrow{h'} & R' \end{array} \tag{4.4}$$

entonces:

(a) si $\underline{t},\underline{v}$ son epimorfismos y si $\underline{w}$ es un monomorfismo, entonces $\underline{u}$ es un epimorfismo;

(b) si $\underline{t},\underline{v}$ son monomorfismos y si $\underline{s}$ es un epimorfismo, entonces $\underline{u}$ es un monomorfismo;

(c) si $\underline{t},\underline{v}$ son isomorfismos, si $\underline{s}$ es épico y $\underline{w}$ es mónico, entonces $\underline{u}$ es un isomorfismo.

Demostración. Como el inciso (c) es simplemente la unión de los incisos (a) y (b), sólo hay que verificar los dos primeros.

Ad (a): Sea $x' \in M'$; se busca un elemento de $x_0 \in M$ tal que $u(x_0) = x'$.

[6] La notación $\sigma^*\omega \in \mathcal{A}^k(\Delta^k,\mathbb{R})$ denota el pullback (o preimagen) de $\omega \in \mathcal{A}^k(M,\mathbb{R})$ bajo un n-símplice singular $\sigma\colon \Delta^k \to M$, cuando σ es una función suave. Un detalle técnico del teorema de de Rham garantiza que puede asumirse que σ es suave.

[7] Para una exposición asequible del teorema de de Rham, véase, por ejemplo: Shigeyuki Morita, *Geometry of Differential Forms*, American Mathematical Society, Providence, RI, 2001.

Como v es sobreyectivo, hay $y \in N$ tal que $v(y) = g'(x')$. Ahora $w(h(y)) = h'(v(y)) = h'(g'(x)) = 0$ porque $h' \circ g' = 0$. Como w es inyectivo, se obtiene $h(y) = 0$ en R.

Luego $y \in \ker h = \operatorname{im} g$, así que $y = g(x)$ con $x \in M$. Además, $g'(x') = v(y) = v(g(x)) = g'(u(x))$. Por tanto, $x' - u(x) \in \ker g' = \operatorname{im} f'$, así que hay $q' \in L'$ tal que $x' - u(x) = f'(q')$.

Como t es sobreyectivo, hay $q \in L$ con $q' = t(q)$; por ende, $x' - u(x) = f'(t(q)) = u(f(q))$. Entonces $x' = u(x + f(q)) \in \operatorname{im} u$. Se concluye que u es sobreyectivo.

Ad (b): Sea $x \in \ker u$; entonces $v(g(x)) = g'(u(x)) = g'(0) = 0$, así que $g(x) = 0$ porque v es inyectivo. Luego $x \in \ker g = \operatorname{im} f$, así que $x = f(q)$ con $q \in L$.

Ahora $0 = u(x) = u(f(q)) = f'(t(q))$. Por tanto, $t(q) \in \ker f' = \operatorname{im} e'$, así que hay $p' \in K'$ tal que $t(q) = e'(p')$. Como s es sobreyectivo, hay $p \in K$ tal que $s(p) = p'$. Entonces vale $t(q) = e'(s(p)) = t(e(p))$.

Como t es inyectivo, se obtiene $q = e(p)$ en L. Por tanto, es $x = f(q) = f(e(p)) = 0$ porque $f \circ e = 0$. Se concluye que u es inyectivo. □

Corolario 4.16 (Lema de Cinco Corto)**.** *Si los homomorfismos (t, u, v) forman una aplicación de cadena*[8] *entre dos sucesiones exactas cortas de A-módulos:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{f} & M & \xrightarrow{g} & N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle t} & & \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle v} & & \\ 0 & \longrightarrow & L' & \xrightarrow{f'} & M' & \xrightarrow{g'} & N' & \longrightarrow & 0 \end{array}$$

entonces $\underline{u}$ es un isomorfismo si $\underline{t}, \underline{v}$ son isomorfismos. ⊟

Lema 4.17. *Dado un diagrama conmutativo de A-módulos,*

$$\begin{array}{ccc} L & \xrightarrow{f} & M \\ {\scriptstyle t}\downarrow & & \downarrow{\scriptstyle u} \\ R & \xrightarrow{h} & S \end{array}$$

Hay A-homomorfismos $\tilde{t}\colon \ker f \to \ker h$, $\bar{u}\colon \operatorname{coker} f \to \operatorname{coker} h$ que hace conmutar el siguiente diagrama ampliado (cuyas filas son exactas):

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & \ker f & \xrightarrow{i} & L & \xrightarrow{f} & M & \xrightarrow{p} & \operatorname{coker} f & \longrightarrow & 0 \\ & & {\scriptstyle \tilde{t}}\downarrow & & {\scriptstyle t}\downarrow & & {\scriptstyle u}\downarrow & & {\scriptstyle \bar{u}}\downarrow & & \\ 0 & \longrightarrow & \ker h & \xrightarrow{j} & R & \xrightarrow{h} & S & \xrightarrow{q} & \operatorname{coker} h & \longrightarrow & 0. \end{array} \tag{4.5}$$

Demostración. En el diagrama (4.5), los morfismos i, j son inclusiones y $p\colon M \to M/f(L)$, $q\colon S \to S/h(R)$ son las aplicaciones cocientes.

Si $x \in L$ con $f(x) = 0$, entonces $h(t(x)) = u(f(x) = u(0) = 0$. Luego, $t(\ker f) \subseteq \ker h$. Entonces $\tilde{t}$ es simplemente la restricción de t al dominio $\ker f$. Es evidente que $j \circ \tilde{t} = t \circ i$.

[8] No se dibuja los morfismos verticales $0 \to 0$, que son necesariamente homomorfismos nulos.

Si $[y] \equiv p(y) = y + f(L)$ es una coclase en $\operatorname{coker} f$, con $y \in M$, entonces $[u(y)] \equiv q(u(y)) = u(y) + h(R)$ es una coclase en $\operatorname{coker} h$. Si hay otro elemento $y' \in M$ con $[y'] = [y]$, entonces $y' - y = f(x)$ para algún $x \in L$, luego

$$u(y') - u(y) = u(y' - y) = u(f(x)) = h(t(x)) \in h(R),$$

así que $\bar{u}([y]) := [u(y)]$ bien define un homomorfismo $\bar{u}\colon \operatorname{coker} f \to \operatorname{coker} h$. Es evidente que $\bar{u} \circ p = q \circ u$. □

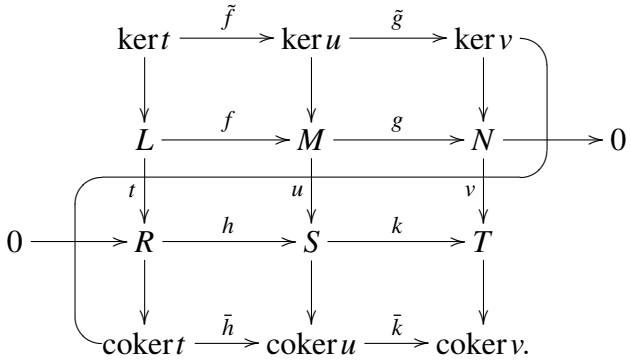
Lema 4.18 (Lema de la Culebra)**.** *Dado un diagrama conmutativo de A-módulos, con filas exactas:*

$$\begin{array}{ccccccccc} & & L & \xrightarrow{f} & M & \xrightarrow{g} & N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle t} & & \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle v} & & \\ 0 & \longrightarrow & R & \xrightarrow{h} & S & \xrightarrow{k} & T & & \end{array}$$

hay una sucesión exacta de 6 *términos:*

$$\ker t \xrightarrow{\tilde{f}} \ker u \xrightarrow{\tilde{g}} \ker v \xrightarrow{\partial} \operatorname{coker} t \xrightarrow{\bar{h}} \operatorname{coker} u \xrightarrow{\bar{k}} \operatorname{coker} v, \tag{4.6}$$

donde el ***morfismo conector*** $\partial\colon \ker v \to \operatorname{coker} t$ *sigue la "culebra" de abajo:*



Demostración. Los morfismos $\tilde{f}$, $\tilde{g}$, $\bar{h}$, $\bar{k}$ se definen por el Lema anterior.

Para definir $\partial\colon \ker v \to \operatorname{coker} t$, tómese $z \in \ker v$. Entonces $z \in N$; como g es sobreyectivo, es $z = g(y)$ para algún $y \in M$. Por tanto, vale $0 = v(z) = v(g(y)) = k(u(y))$; esto implica que $u(y) \in \ker k = \operatorname{im} h$, de manera que hay $x \in R$ tal que $u(y) = h(x)$. Ahora colóquese $\partial(z) := [x] \equiv x + t(L) \in \operatorname{coker} t$.

Hay que comprobar que las tres fórmulas subrayadas del párrafo anterior conducen a una buena definición de un morfismo ∂. El problema es que la elección de $y \in g^{-1}(z)$ es arbitrario. Si $y' \in M$ obedece $g(y') = z = g(y)$, entonces $g(y' - y) = 0$, así que $y' - y \in \ker g = \operatorname{im} f$, luego $y' = y + f(w)$ para algún $w \in L$.

Entonces $u(y') = u(y) + u(f(w)) = u(y) + h(t(w))$. Si $x' \in R$ cumple $u(y') = h(x')$, entonces $h(x') = h(x) + h(t(w))$. Por hipótesis, h es inyectivo, lo cual implica que $x' = x + t(w)$. Pero entonces $[x'] = [x]$ en $\operatorname{coker} t = R/t(L)$. Se concluye que la coclase $[x]$ depende sólo de

z y no de y; por ende, $\partial\colon z \mapsto [x]$ está bien definido. (Es fácil comprobar ahora que ∂ es un A-homomorfismo.)

Para ver que (4.6) es exacta en $\ker u$, fíjese que $\tilde{g}(\tilde{f}(x)) = g(f(x)) = 0$ para todo $x \in \ker t$; luego, vale $\operatorname{im}\tilde{f} \subseteq \ker\tilde{g}$. Por otro lado, si $y \in \ker u$ cumple $\tilde{g}(y) = g(y) = 0$, entonces $y = f(w)$ para algún $w \in L$. Como $h(t(w)) = u(f(w)) = u(y) = 0$ y h es inyectivo, se obtiene $t(w) = 0$ así que $w \in \ker t$, con $\tilde{f}(w) = f(w) = y$. Se ha comprobado que $\ker\tilde{g} \subseteq \operatorname{im}\tilde{f}$.

Para ver que (4.6) es exacta en $\operatorname{coker} u$, fíjese que $\bar{k}(\bar{h}([w])) = [k(h(w))] = 0$ para todo $[w] = w + t(L) \in \operatorname{coker} t$; luego, vale $\operatorname{im}\bar{h} \subseteq \ker\bar{k}$. Por otro lado, si $[s] = s + u(M) \in \operatorname{coker} u$ cumple $\bar{k}([s]) = [k(s)] = 0$, entonces $k(s) \in v(N)$, es decir, $k(s) = v(z)$ para algún $z \in N$. Como g es sobreyectivo, es $z = g(y)$ para algún $y \in M$. Ahora $k(s) = v(g(y)) = k(u(y))$ y se obtiene $s - u(y) \in \ker k = \operatorname{im} h$ así que $s = u(y) + h(x)$ para algún $x \in R$. Luego $[s] = [h(x)] = \bar{h}([x])$. Se ha comprobado que $\ker\bar{k} \subseteq \operatorname{im}\bar{h}$.

Para ver que (4.6) es exacta en $\ker v$, fíjese que para todo $y \in \ker u$ vale $\partial(\tilde{g}(y)) = \partial(g(y)) = [x]$ donde $x \in R$ cumple $h(x) = u(y) = 0$; como h es inyectivo, esto implica que $x = 0$ y por ende $[x] = 0$ en $\operatorname{coker} t$; luego, vale $\operatorname{im}\tilde{g} \subseteq \ker\partial$. Por otro lado, si $z \in \ker v$ cumple $\partial(z) = 0$, entonces hay elementos $y \in M$, $x = t(w) \in t(L)$ tales que $z = g(y)$, $u(y) = h(x)$; entonces, $u(y) = h(x) = h(t(w)) = u(f(w))$. Luego $y - f(w) \in \ker u$, por tanto $\tilde{g}(y - f(w)) = g(y) - g(f(w)) = z - 0 = z$. Se ha comprobado que $\ker\partial \subseteq \operatorname{im}\tilde{g}$.

Para ver que (4.6) es exacta en $\operatorname{coker} t$, fíjese que para todo $z \in \ker v$ y $y \in M$ tal que $g(y) = z$, hay $x \in M$ tal que $u(y) = h(x)$; luego vale $\bar{h}(\partial(z)) = \bar{h}([x]) = [h(x)] = [u(y)] = 0$ en $\operatorname{coker} u = S/u(M)$; luego, vale $\operatorname{im}\partial \subseteq \ker\bar{h}$. Por otro lado, si $[x] = x + t(L) \in \operatorname{coker} t$ cumple $\bar{h}([x]) = [h(x)] = 0$, entonces $h(x) \in u(M)$, es decir, $h(x) = u(y)$ para algún $y \in M$. Sea $z := g(y)$; obsérvese que $v(z) = v(g(y)) = k(u(y)) = k(h(x)) = 0$, así que $x \in \ker v$. Entonces $\partial(z) = [x]$ por la definición de ∂. Se ha comprobado que $\ker\bar{h} \subseteq \operatorname{im}\partial$. □

Si $(C_\bullet, \delta) \in\in A\text{-}\mathsf{Compl}$ es un complejo de cadenas de A-módulos, sus módulos de homología se denotarán por $\{H_n(C) : n \in \mathbb{Z}\}$ cuando es necesario distinguirlos de los módulos de homología de algún otro complejo.

Lema 4.19. *Si $(C_\bullet, \delta)$ y $(D_\bullet, \delta')$ son dos complejos de cadenas de A-módulos, entonces para cada aplicación de cadenas $f_\bullet\colon C_\bullet \to D_\bullet$ hay A-homomorfismos $H_n f\colon H_n(C) \to H_n(D)$, para $n \in \mathbb{Z}$, los cuales conforman un funtor covariante $H_n\colon A\text{-}\mathsf{Compl} \to A\text{-}\mathsf{Mod}$.*

Demostración. La aplicación de cadena $f_\bullet$ da lugar a un diagrama conmutativa

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & C_{n+1} & \xrightarrow{\delta_{n+1}} & C_n & \xrightarrow{\delta_n} & C_{n-1} & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle f_{n+1}} & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \\ \cdots & \longrightarrow & D_{n+1} & \xrightarrow{\delta'_{n+1}} & D_n & \xrightarrow{\delta'_n} & D_{n-1} & \longrightarrow & \cdots \end{array} \tag{4.7}$$

En particular, vale $f_{n-1} \circ \delta_n = \delta'_n \circ f_n$; y $f_n \circ \delta_{n+1} = \delta'_{n+1} \circ f_{n+1}$ para cada n. El Lema 4.17, aplicado al cuadrado conmutativo a la derecha, dice que $f_n(Z_n(C)) \subseteq Z_n(D)$ y que la restricción de f_n a los n-ciclos es un A-homomorfismo $\tilde{f}_n\colon Z_n(C) \to Z_n(D)$. Por otro lado, del mismo Lema aplicado al otro cuadrado, se obtiene $\bar{f}_n\colon C_n/B_n(C) \to D_n/B_n(D)$ tal que

$\bar{f}_n([x]) = [f_n(x)]$ para $x \in C_n$. De ahí resulta el siguiente diagrama conmutativo, con filas exactas:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Z_n(C) & \xrightarrow{i_n} & C_n & \xrightarrow{\delta_n} & C_{n-1} & \xrightarrow{p_n} & C_{n-1}/B_{n-1}(C) \longrightarrow 0 \\ & & \downarrow{\scriptstyle \tilde{f}_n} & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \downarrow{\scriptstyle \bar{f}_{n-1}} \\ 0 & \longrightarrow & Z_n(D) & \xrightarrow{i'_n} & D_n & \xrightarrow{\delta'_n} & D_{n-1} & \xrightarrow{p'_n} & D_{n-1}/B_{n-1}(D) \longrightarrow 0 \end{array}$$

con inclusiones i_n, i'_n y aplicaciones cocientes p_n, p'_n. Como $H_n(C) = Z_n(C)/B_n(C)$, del primer o del tercer cuadrado del diagrama anterior se obtiene dos diagramas nuevos:

$$\begin{array}{ccccc} 0 & \longrightarrow & H_n(C) & \longrightarrow & C_n/B_n(C) \\ & & \downarrow{\scriptstyle H_nf} & & \downarrow{\scriptstyle \bar{f}_n} \\ 0 & \longrightarrow & H_n(D) & \longrightarrow & D_n/B_n(D) \end{array} \qquad \begin{array}{ccccc} Z_{n-1}(C) & \longrightarrow & H_{n-1}(C) & \longrightarrow & 0 \\ \downarrow{\scriptstyle \tilde{f}_{n-1}} & & \downarrow{\scriptstyle H_{n-1}f} & & \\ Z_{n-1}(D) & \longrightarrow & H_{n-1}(D) & \longrightarrow & 0 \end{array} \tag{4.8}$$

al definir $H_nf(x + B_n(C)) := f_n(x) + B_n(D)$ si $x \in Z_n(C)$, para cada $n \in \mathbb{Z}$.

Es evidente de esta definición que si $g_\bullet \colon D_\bullet \to E_\bullet$ es otra aplicación de cadena, entonces $H_n(g \circ f) = H_ng \circ H_nf$; y que $H_n(1_{C_\bullet}) = 1_{H_n(C)}$. Luego H_n es un funtor covariante. □

Proposición 4.20. *Dada una* sucesión exacta corta *en* A-Compl,[9]

$$0 \longrightarrow C_\bullet \xrightarrow{f_\bullet} D_\bullet \xrightarrow{g_\bullet} E_\bullet \longrightarrow 0, \tag{4.9}$$

hay una ***sucesión exacta larga*** *en* A-Mod*, con infinitos términos, dado por*

$$\cdots \xrightarrow{\partial_{n+1}} H_n(C) \xrightarrow{H_nf} H_n(D) \xrightarrow{H_ng} H_n(E) \xrightarrow{\partial_n} H_{n-1}(C) \xrightarrow{H_{n-1}f} H_{n-1}(D) \xrightarrow{H_{n-1}g} H_{n-1}(E) \xrightarrow{\partial_{n-1}} \cdots \tag{4.10}$$

donde cada $\partial_n \colon H_n(E) \to H_{n-1}(C)$ *es un morfismo conector.*

Demostración. De la sucesión exacta corta (4.9), se obtiene el siguiente diagrama conmutativo en A-Mod con filas exactas:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C_{n+1} & \xrightarrow{f_{n+1}} & D_{n+1} & \xrightarrow{g_{n+1}} & E_{n+1} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \delta_{n+1}} & & \downarrow{\scriptstyle \delta'_{n+1}} & & \downarrow{\scriptstyle \delta''_{n+1}} & & \\ 0 & \longrightarrow & C_n & \xrightarrow{f_n} & D_n & \xrightarrow{g_n} & E_n & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \delta'_n} & & \downarrow{\scriptstyle \delta'_n} & & \downarrow{\scriptstyle \delta''_n} & & \\ 0 & \longrightarrow & C_{n-1} & \xrightarrow{f_{n-1}} & D_{n-1} & \xrightarrow{g_{n-1}} & E_{n-1} & \longrightarrow & 0 \end{array}$$

Al aplicar el Lema 4.18 a las dos filas inferiores, se obtiene una sucesión exacta de 6 términos:

$$Z_n(C) \xrightarrow{\tilde{f}_n} Z_n(D) \xrightarrow{\tilde{g}_n} Z_n(E) \xrightarrow{\check{\partial}} C_{n-1}/B_{n-1}(C) \xrightarrow{\bar{f}_{n-1}} D_{n-1}/B_{n-1}(D) \xrightarrow{\bar{g}_{n-1}} E_{n-1}/B_{n-1}(E). \tag{4.11}$$

[9]No es difícil comprobar que A-Compl es una categoría abeliana. Por tanto, admite sucesiones exactas.

Tomando en cuenta la conmutatividad de los diagramas (4.8), los primeros tres y también los últimos tres términos de estos seis dan lugar a dos sucesiones exactas de A-módulos:

$$H_n(C) \xrightarrow{H_nf} H_n(D) \xrightarrow{H_ng} H_n(E), \qquad H_{n-1}(C) \xrightarrow{H_{n-1}f} H_{n-1}(D) \xrightarrow{H_{n-1}g} H_{n-1}(E),$$

que son idénticos, salvo cambio de índice. Falta comprobar que $\check{\partial}\colon Z_n(E) \to C_{n-1}/B_{n-1}(C)$ induce un homomorfismo $\partial_n\colon H_n(E) \to H_{n-1}(C)$ tal que (4.10) es exacta en $H_n(E)$ y en $H_{n-1}(C)$.

Para $z \in Z_n(E)$, las fórmulas $z = g_n(y)$ con $y \in D_n$, $\delta'_n(y) = f_{n-1}(x)$ con $x \in C_{n-1}$ determinan $\check{\partial}(z) := x + B_{n-1}(C)$. Si $z' \in Z_n(E)$ es tal que $z' - z = \delta''_{n+1}(w)$ con $w \in E_{n+1}$, entonces hay $v \in D_{n+1}$ con $g_{n+1}(v) = w$. Las fórmulas $z' = g_n(y')$, $\delta'_n(y') = f_{n-1}(x')$ conducen a las siguientes relaciones. Primero,

$$g_n(y' - y) = z' - z = \delta''_{n+1}(g_{n+1}(v)) = g_n(\delta'_{n+1}(v)),$$

así que $y' - y - \delta'_{n+1}(v) \in \ker g_n = \operatorname{im} f_n$, luego hay $u \in C_n$ tal que $y' - y = \delta'_{n+1}(v) + f_n(u)$. Entonces

$$f_{n-1}(x' - x) = \delta'_n(y' - y) = \delta'_n(f_n(u)) = f_{n-1}(\delta_n(u)),$$

lo cual implica que $x' - x = \delta_n(u) \in B_{n-1}(C)$ porque f_{n-1} es inyectivo. En otras palabras, hay un homomorfismo bien definido

$$\partial_n\colon H_n(E) \to H_{n-1}(C) \quad \text{dado por} \quad \partial_n(z + B_n(E)) := x + B_{n-1}(C).$$

La exactitud de (4.10) en $H_n(E)$ y en $H_{n-1}(C)$ ahora es una consecuencia fácil de la exactitud de (4.11) en $Z_n(E)$ y en $C_{n-1}/B_{n-1}(C)$. □

► Resulta que la correspondencia functorial $f_\bullet \mapsto H_\bullet f$ que lleva $\mathrm{Hom}_{A\text{-}\mathsf{Compl}}(C_\bullet, D_\bullet)$ en $\mathrm{Hom}_{A\text{-}\mathsf{Mod}}(H_\bullet(C), H_\bullet(D))$ no es inyectiva. Hay una relación de equivalencia entre aplicaciones de cadena que produce igualdad en homología. Por su origen en la topología algebraica, esta relación se llama *homotopía*; pero tiene una expresión puramente algebraica y en el contexto actual se habla de "homotopía de cadenas".

Definición 4.21. Dadas dos aplicaciones de cadenas $f_\bullet, g_\bullet\colon C_\bullet \to D_\bullet$ entre un par de complejos de A-módulos, una **homotopía de cadenas** entre ellas es una familia de A-homomorfismos $s_n\colon C_n \to D_{n+1}$, para $n \in \mathbb{Z}$, tales que

$$\delta'_{n+1} \circ s_n + s_{n-1} \circ \delta_n = f_n - g_n \tag{4.12}$$

en $\mathrm{Hom}_A(C_n, D_n)$, para todo $n \in \mathbb{Z}$. Se dice que $f_\bullet$, $g_\bullet$ son **homotópicos** y se escribe $f_\bullet \sim g_\bullet$ si existe una homotopía de cadenas entre $f_\bullet$ y $g_\bullet$. (Debe de ser evidente que esta es una relación de equivalencia.)

Lema 4.22. *Si $f_\bullet, g_\bullet\colon C_\bullet \to D_\bullet$ son homotópicas, entonces $H_nf = H_ng$ para todo $n \in \mathbb{Z}$.*

Demostración. Sea $s_\bullet : f_\bullet \to g_\bullet$ una homotopía de cadenas. Si $x \in Z_n(C)$, la fórmula (4.12) implica que

$$f_n(x) - g_n(x) = \delta'_{n+1}(s_n(x)) + s_{n-1}(\delta_n(x)) = \delta'_{n+1}(s_n(x)) \in B_n(D)$$

así que $[f_n(x)] = [g_n(x)]$ en $H_n(D)$. Por lo tanto, $H_nf = H_ng$ en $\mathrm{Hom}_A(H_n(C), H_n(D))$. □

Definición 4.23. Dos complejos de A-módulos $C_\bullet$ y $D_\bullet$ son **equivalentes en homotopía**, escrito $C_\bullet \sim D_\bullet$, si hay un par de aplicaciones de cadenas $f_\bullet : C_\bullet \to D_\bullet$ y $g_\bullet : D_\bullet \to C_\bullet$ tales que $g_\bullet \circ f_\bullet \sim 1_{C_\bullet}$ y $f_\bullet \circ g_\bullet \sim 1_{D_\bullet}$.

En tal caso, los A-homomorfismos $H_n f : H_n(C) \to H_n(D)$ son isomorfismos para cada n, en vista de la funtorialidad de H_n. Más generalmente, dos complejos $C_\bullet$ y $D_\bullet$ se llaman **cuasiisomorfos** si $H_n(C) \simeq H_n(D)$ para todo n.

4.3 Resoluciones proyectivas e inyectivas

Cualquier A-módulo (a la izquierda) M es el cociente de un A-módulo proyectivo. Esto es, hay un A-módulo proyectivo P_0 y un A-homomorfismo sobreyectivo $\varepsilon : P_0 \twoheadrightarrow M$. (Si M ya es proyectivo, se puede tomar $P_0 = M$ y $\varepsilon = 1_M$.) En todo caso, ε sería un isomorfismo sólo si M ya es proyectivo.

Si $M \in\in A\text{-}\mathsf{Mod}$ no es proyectivo, entonces $\ker \varepsilon \neq 0$; escríbase $K_0 := \ker \varepsilon$. Por tanto, hay otro A-módulo proyectivo P_1 que admite un epimorfismo $\varepsilon_1 : P_1 \twoheadrightarrow K_0$. Si $i_1 : K_0 \hookrightarrow P_0$ es la inclusión, sea $\delta_1 := i_1 \circ \varepsilon_1 : P_1 \to P_0$. De esta manera, se obtiene el siguiente diagrama conmutativo con fila superior exacta:

$$\begin{array}{ccccccccc} P_1 & & \xrightarrow{\delta_1} & & P_0 & \xrightarrow{\varepsilon} & M & \longrightarrow & 0 \\ & \searrow^{\varepsilon_1} & & \nearrow_{i_1} & & & & & \\ & & K_0 & & & & & & \end{array}$$

Ahora sea $K_1 := \ker \delta_1$. Si $K_1 \neq 0$, hay un A-módulo proyectivo P_2 que admite un epimorfismo $\varepsilon_2 : P_2 \twoheadrightarrow K_1$. Si $i_2 : K_1 \hookrightarrow P_1$ es la inclusión, sea $\delta_2 := i_2 \circ \varepsilon_2 : P_2 \to P_1$. Se obtiene un nuevo diagrama conmutativo con fila superior exacta:

$$\begin{array}{ccccccccccc} P_2 & & \xrightarrow{\delta_2} & & P_1 & & \xrightarrow{\delta_1} & & P_0 & \xrightarrow{\varepsilon} & M & \longrightarrow & 0 \\ & \searrow^{\varepsilon_2} & & \nearrow_{i_2} & & \searrow^{\varepsilon_1} & & \nearrow_{i_1} & & & & & \\ & & K_1 & & & & K_0 & & & & & & \end{array}$$

(Si $K_1 = 0$, tómese $P_2 := 0$ también.) Al repetir este proceso, se obtiene por inducción (con $K_n := \ker \delta_n$; $\varepsilon_{n+1} : P_{n+1} \twoheadrightarrow K_n$ si $K_n \neq 0$; $i_{n+1} : K_n \hookrightarrow P_n$; $\delta_{n+1} := i_{n+1} \circ \varepsilon_{n+1} : P_{n+1} \to P_n$) una sucesión exacta larga de la siguiente forma:

$$\cdots \longrightarrow P_n \xrightarrow{\delta_n} P_{n-1} \longrightarrow \cdots \longrightarrow P_2 \xrightarrow{\delta_2} P_1 \xrightarrow{\delta_1} P_0 \xrightarrow{\varepsilon} M \longrightarrow 0 \tag{4.13}$$

donde cada P_n es un A-módulo proyectivo. (Si $\ker \delta_n = 0$ para algún n, se define $P_m := 0$ para todo $m > n$.)

Definición 4.24. Sea M un A-módulo. Una **resolución** (a la izquierda) de M es una sucesión exacta de la forma (4.13), escrito brevemente $P_\bullet \twoheadrightarrow M$. El epimorfismo $\varepsilon : P_0 \to M$ se llama una **aumentación** del complejo $(P_\bullet, \delta)$. Si cada P_n es un A-módulo proyectivo, se habla de

una **resolución proyectiva**; si cada P_n es un A-módulo libre, se habla de una **resolución libre**. Si hay $n \in \mathbb{N}$ tal que $P_m = 0$ para $m > n$, se habla de una **resolución finita**.

La Proposición 1.42 y la discusión anterior garantizan que cada A-módulo M posee una resolución libre (la cual es, *ipso facto*, una resolución proyectiva).

Si $P_\bullet \twoheadrightarrow M$ es una resolución de M, obsérvese que $P_\bullet$ solo, con M reemplazado por 0, es un complejo tal que $H_n(P) = \ker \delta_n / \operatorname{im} \delta_{n+1} = 0$ para $n > 0$; mientras $H_0(P) = P_0 / \operatorname{im} \delta_1 = P_0 / \ker \varepsilon \simeq \operatorname{im} \varepsilon = M$. Un complejo de este tipo, cuya homología es trivial salvo para $n = 0$, se llama un **complejo acíclico**.

Proposición 4.25. *Si $P_\bullet \twoheadrightarrow M$ es una resolución proyectiva en A-Mod y si $R_\bullet \twoheadrightarrow N$ es otra resolución, con aumentaciones respectivas $\varepsilon\colon P_0 \to M$ y $\varepsilon'\colon R_0 \to N$, cada A-homomorfismo $\varphi\colon M \to N$ da lugar a una aplicación de cadenas $f_\bullet\colon P_\bullet \to Q_\bullet$ tal que $\varepsilon' \circ f_0 = \varphi \circ \varepsilon$:*

$$\begin{array}{ccccccccccccc}
\cdots & \longrightarrow & P_n & \xrightarrow{\delta_n} & P_{n-1} & \longrightarrow \cdots \longrightarrow & P_2 & \xrightarrow{\delta_2} & P_1 & \xrightarrow{\delta_1} & P_0 & \xrightarrow{\varepsilon} & M \longrightarrow 0 \\
 & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle \varphi} \\
\cdots & \longrightarrow & R_n & \xrightarrow{\delta'_n} & R_{n-1} & \longrightarrow \cdots \longrightarrow & R_2 & \xrightarrow{\delta'_2} & R_1 & \xrightarrow{\delta'_1} & R_0 & \xrightarrow{\varepsilon'} & N \longrightarrow 0
\end{array} \tag{4.14}$$

Además, si $g_\bullet\colon P_\bullet \to R_\bullet$ es otra aplicación de cadenas tal que $\varepsilon' \circ g_0 = \varphi \circ \varepsilon$, entonces $f_\bullet \sim g_\bullet$.

Demostración. Como P_0 es proyectivo y $\varepsilon'\colon R_0 \to N$ es un epimorfismo, la aplicación $\varphi \circ \varepsilon\colon P_0 \to N$ se levanta a un A-homomorfismo $f_0\colon P_0 \to R_0$ tal que $\varepsilon' \circ f_0 = \varphi \circ \varepsilon$:

$$\begin{array}{ccccc}
P_0 & & & & \\
\downarrow{\scriptstyle f_0} & \searrow^{\varphi\circ\varepsilon} & & & \\
R_0 & \xrightarrow{\varepsilon'} & N & \longrightarrow & 0.
\end{array}$$

Ahora $\varepsilon' \circ f_0 \circ \delta_1 = \varphi \circ \varepsilon \circ \delta_1 = 0$, por tanto $\operatorname{im}(f_0 \circ \delta_1) \subseteq \ker \varepsilon' = \operatorname{im} \delta'_1$. Como P_1 es proyectivo, hay un A-homomorfismo $f_1\colon P_1 \to R_1$ tal que $\delta'_1 \circ f_1 = f_0 \circ \delta_1$:

$$\begin{array}{ccccc}
P_1 & & & & \\
\downarrow{\scriptstyle f_1} & \searrow^{f_0\circ\delta_1} & & & \\
R_1 & \xrightarrow{\delta'_1} & \operatorname{im}\delta'_1 & \longrightarrow & 0.
\end{array}$$

Se procede por inducción sobre n; una vez construido $f_n\colon P_n \to R_n$ tal que $\delta'_n \circ f_n = f_{n-1} \circ \delta_n$, se concluye que $\delta'_n \circ f_n \circ \delta_{n+1} = 0$, por ende $\operatorname{im}(f_n \circ \delta_{n+1}) \subseteq \ker \delta'_n = \operatorname{im} \delta'_{n+1}$. Como P_{n+1} es proyectivo, hay un A-homomorfismo $f_{n+1}\colon P_{n+1} \to R_{n+1}$ tal que $\delta'_{n+1} \circ f_{n+1} = f_n \circ \delta_{n+1}$. Esta última igualdad, válida por todo n, dice que $f_\bullet\colon P_\bullet \to R_\bullet$ es una aplicación de cadena.

Ahora sea $g_\bullet\colon P_\bullet \to R_\bullet$ otra aplicación de cadena tal que $\varepsilon' \circ g_0 = \varphi \circ \varepsilon$. Considérese las aplicaciones $h_n := f_n - g_n \in \operatorname{Hom}_A(P_n, R_n)$ para $n \in \mathbb{N}$, que son componentes de una

aplicación de cadena $h_\bullet = f_\bullet - g_\bullet \colon P_\bullet \to R_\bullet$. Fíjese que $\varepsilon' \circ h_0 = 0$, así que $\operatorname{im} h_0 \subseteq \ker \varepsilon = \operatorname{im} \delta_1'$. Entonces hay un A-homomorfismo $s_0 \colon P_0 \to R_1$ tal que $\delta_1' \circ s_0 = h_0$:

$$\begin{array}{ccccc} & & P_0 & & \\ & \swarrow^{s_0} & \downarrow{\scriptstyle h_0} & & \\ R_1 & \xrightarrow{\delta_1'} & \ker\varepsilon & \longrightarrow & 0. \end{array}$$

En seguida, se definen $s_n \colon P_n \to R_{n+1}$, para $n \geq 1$, por inducción sobre n; una vez construido $s_{n-1} \colon P_{n-1} \to R_n$ tal que $\delta_n' \circ s_{n-1} + s_{n-2} \circ \delta_{n-1} = h_{n-1}$, se puede notar que

$$\delta_n' \circ (h_n - s_{n-1} \circ \delta_n) = \delta_n' \circ h_n - \delta_n' \circ s_{n-1} \circ \delta_n = \delta_n' \circ h_n - h_{n-1} \circ \delta_n = 0,$$

por lo tanto $\operatorname{im}(h_n - s_{n-1} \circ \delta_n) \subseteq \ker \delta_n' = \operatorname{im} \delta_{n+1}'$. Como P_n es proyectivo, hay un A-homomorfismo $s_n \colon P_n \to R_{n+1}$ tal que $\delta_{n+1}' \circ s_n = h_n - s_{n-1} \circ \delta_n$:

$$\begin{array}{ccccccc} & & P_n & \xrightarrow{\delta_n} & P_{n-1} & & \\ & \swarrow^{s_n} & \downarrow{\scriptstyle h_n} & \swarrow_{s_{n-1}} & & & \\ R_{n+1} & \xrightarrow{\delta_{n+1}'} & R_n & \xrightarrow{\delta_n'} & R_{n-1}. & & \end{array}$$

La última igualdad, válida por todo n, dice que $s_\bullet \colon f_\bullet \to g_\bullet$ es una homotopía de cadenas. □

Ejemplo 4.26. El grupo abeliano $\mathbb{Z}/m$ no es proyectivo como $\mathbb{Z}$-módulo, si $m \geq 2$. La aplicación cociente $\varepsilon \colon \mathbb{Z} \to \mathbb{Z}/m$ tiene núcleo $\ker \varepsilon = m\mathbb{Z}$. Si $i_1 \colon m\mathbb{Z} \hookrightarrow \mathbb{Z}$ es la inclusión y si $\varepsilon_1 \colon \mathbb{Z} \twoheadrightarrow m\mathbb{Z}$ es el epimorfismo $k \mapsto mk$, entonces $i_1 \circ \varepsilon_1 : \mathbb{Z} \to \mathbb{Z}$ es la multiplicación por m en $\mathbb{Z}$, comúnmente denotado por $(\times m)$. Este operador de multiplicación es inyectiva; luego, $\mathbb{Z}/m$ posee la resolución finita

$$\mathbb{Z} \xrightarrow{\times m} \mathbb{Z} \xrightarrow{\varepsilon} \mathbb{Z}/m \longrightarrow 0,$$

la cual es una resolución libre de $\mathbb{Z}/m$.

Definición 4.27. Sea M un A-módulo. Una **coresolución** (o resolución a la derecha) de M es una sucesión exacta de la siguiente forma:

$$0 \longrightarrow M \xrightarrow{j} Q^0 \xrightarrow{d_0} Q^1 \xrightarrow{d_1} Q^2 \xrightarrow{d_2} \cdots \longrightarrow Q^n \xrightarrow{d_n} Q^{n+1} \longrightarrow \cdots \tag{4.15}$$

escrito brevemente $M \rightarrowtail Q^\bullet$. Si cada Q^n es un A-módulo inyectivo, se habla de una **coresolución inyectiva**.[10] Si hay $n \in \mathbb{N}$ tal que $Q^m = 0$ para $m > n$, se habla de una **coresolución finita**.

[10] Muchos autores hablan de una **resolución inyectiva**, sin el prefijo 'co-', dejando que el contexto indique si se trata de un complejo de cadenas o de cocadenas.

Lema 4.28. *Cada A-módulo M posee una coresolución inyectiva.*

Demostración. La Proposición 3.26 garantizan que hay un A-módulo inyectivo Q^0 y un monomorfismo $j\colon M \hookrightarrow Q^0$. Si M no es inyectivo, este j no es un isomorfismo y $\operatorname{coker} j \neq 0$; sea $q_0\colon Q^0 \twoheadrightarrow R_0 := \operatorname{coker} j$ la aplicación cociente. Ahora hay un A-módulo inyectivo Q^1 y un monomorfismo $j_0\colon R_0 \hookrightarrow Q^1$; sea $d_0 := j_0 \circ q_0\colon Q^0 \to Q^1$. Entonces $\ker d_0 = \ker q_0 = \ker(\operatorname{coker} j) = \operatorname{im} j$, de modo que el siguiente diagrama conmutativo tiene fila superior exacta:

$$\begin{array}{ccccccc} 0 & \longrightarrow & M & \xrightarrow{j} & Q^0 & \xrightarrow{\quad d_0 \quad} & Q^1 \\ & & & & & {\scriptstyle q_0}\searrow \quad \nearrow{\scriptstyle j_0} & \\ & & & & & R_0 & \end{array}$$

Ahora sea $R_1 := \operatorname{coker} d_0$. Si $R_1 \neq 0$, hay un A-módulo inyectivo Q^2 que admite un monomorfismo $j_1\colon R_1 \hookrightarrow Q^2$. Si $q_1\colon Q^1 \twoheadrightarrow R_1$ es la aplicación cociente, sea $d_1 := j_1 \circ q_1 : Q^1 \to Q^2$. La sucesión $Q^0 \xrightarrow{d_0} Q^1 \xrightarrow{d_1} Q^2$ es exacta en Q^1. Al continuar por inducción, se obtiene una coresolución inyectiva de la forma (4.15). □

Proposición 4.29. *Si $M \rightarrowtail R^\bullet$ es una coresolución y si $N \rightarrowtail Q^\bullet$ es una coresolución inyectiva, con monomorfismos respectivos $j'\colon M \hookrightarrow R^0$ y $j\colon N \hookrightarrow Q^0$, cada A-homomorfismo $\varphi\colon M \to N$ induce una aplicación de cocadenas $f_\bullet\colon R^\bullet \to Q^\bullet$ tal que $f_0 \circ j' = j \circ \varphi$:*

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & M & \xrightarrow{j'} & R^0 & \xrightarrow{d_0'} & R^1 & \xrightarrow{d_1'} & R^2 & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \\ 0 & \longrightarrow & N & \xrightarrow{j} & Q^0 & \xrightarrow{d_0} & Q^1 & \xrightarrow{d_1} & Q^2 & \longrightarrow & \cdots \end{array}$$

Si $g_\bullet\colon R^\bullet \to Q^\bullet$ es otra aplicación de cocadenas tal que $g_0 \circ j' = j \circ \varphi$, entonces $f_\bullet \sim g_\bullet$.

Demostración. Es exactamente análoga a la demostración de la Proposición 4.25, usando la propiedad (3.8) de módulos inyectivos para fabricar los homomorfismos necesarios. Los detalles se dejan como ejercicio. □

4.4 Funtores derivados, Ext y Tor

Los funtores más importantes de la teoría de módulos no son exactos: los funtores representables $\operatorname{Hom}_A(M,-)$ y $\operatorname{Hom}_A(-,N)$ son exactos a la izquierda, mientras $(R \otimes_A -)$ y $(- \otimes_A S)$ son exactos a la derecha. En algunos casos (módulos proyectivos, inyectivos, llanos) uno de estos funtores se vuelve exacto; pero es deseable *medir la falta de exactitud* en el caso general. Las nuevas herramientas de resoluciones proyectivas (y coresoluciones inyectivas), junto con la sucesión exacta larga en homología, permiten la construcción de nuevos funtores a partir de los funtores ya conocidos, que se anulan justamente cuando los funtores originales son exactos.

Es conveniente empezar con una construcción categórica general, para luego ejemplificarla con los funtores representables y tensoriales.

Definición 4.30. Sea $\mathcal{F}\colon A\text{-Mod} \to \mathsf{Ab}$ un funtor aditivo covariante. Para un determinado A-módulo M, sea $P_\bullet \twoheadrightarrow M$ una resolución proyectiva. Al aplicar $\mathcal{F}$ a esta resolución, se obtiene una sucesión larga de grupos abelianos:

$$\cdots \longrightarrow \mathcal{F}P_n \xrightarrow{\mathcal{F}\delta_n} \mathcal{F}P_{n-1} \longrightarrow \cdots \longrightarrow \mathcal{F}P_2 \xrightarrow{\mathcal{F}\delta_2} \mathcal{F}P_1 \xrightarrow{\mathcal{F}\delta_1} \mathcal{F}P_0 \xrightarrow{\mathcal{F}\varepsilon} \mathcal{F}M \longrightarrow 0. \tag{4.16}$$

Como $\mathcal{F}$ es covariante y aditiva, se obtiene

$$\mathcal{F}\delta_n \circ \mathcal{F}\delta_{n+1} = \mathcal{F}(\delta_n \circ \delta_{n+1}) = \mathcal{F}0 = 0 \quad \text{para todo} \quad n \geq 1$$

y además $\mathcal{F}\varepsilon \circ \mathcal{F}\delta_1 = \mathcal{F}(\varepsilon \circ \delta_1) = \mathcal{F}0 = 0$. Luego, la sucesión (4.16) es un complejo en Ab. Al sustituir la cabeza $\mathcal{F}P_0 \xrightarrow{\mathcal{F}\varepsilon} \mathcal{F}M \to 0$ por $\mathcal{F}P_0 \to 0$, se obtiene un *complejo truncado* de cadenas $(\mathcal{F}P_\bullet, \mathcal{F}\delta)$.

Si $\varphi \in \mathrm{Hom}_A(M,N)$, sea $R_\bullet \twoheadrightarrow N$ una resolución proyectiva de N. Sea $f_\bullet\colon P_\bullet \to R_\bullet$ una aplicación de cadena que hace conmutar el diagrama (4.14); entonces $\mathcal{F}f_\bullet\colon \mathcal{F}P_\bullet \to \mathcal{F}R_\bullet$ es también una aplicación de cadenas.

Para cada $n \in \mathbb{N}$, la homología del complejo truncado define un funtor $L_n\mathcal{F} : A\text{-Mod} \to \mathsf{Ab}$ por

$$L_n\mathcal{F}(M) := H_n(\mathcal{F}P), \qquad L_n\mathcal{F}(\varphi) := H_n(\mathcal{F}f). \tag{4.17}$$

Este funtor $L_n\mathcal{F}$ se llama el n-ésimo **funtor derivado izquierdo** del funtor covariante $\mathcal{F}$.

Obsérvese que la definición de los $L_n\mathcal{F}$ depende de la elección de una resolución proyectiva particular para $M \in\in A\text{-Mod}$, y además de una aplicación de cadenas particular $f_\bullet$ para cada $\varphi \in \mathrm{Hom}_A(M,N)$. Sin embargo, el efecto de estas elecciones no es importante. En primera instancia, si $g_\bullet\colon P_\bullet \to R_\bullet$ es otra aplicación de cadena que hace conmutar (4.14), la Proposición 4.25 muestra que hay una homotopía de cadenas $s_\bullet\colon f_\bullet \to g_\bullet$. Cada fórmula $\delta'_{n+1} \circ s_n + s_{n-1} \circ \delta_n = f_n - g_n$ se convierte en $\mathcal{F}\delta'_{n+1} \circ \mathcal{F}s_n + \mathcal{F}s_{n-1} \circ \mathcal{F}\delta_n = \mathcal{F}f_n - \mathcal{F}g_n$ al aplicar el funtor $\mathcal{F}$, así que $\mathcal{F}f_\bullet \sim \mathcal{F}g_\bullet$ mediante la homotopía de cadenas $\mathcal{F}s_\bullet$. Del Lema 4.23 se obtiene la igualdad $H_n(\mathcal{F}f) = H_n(\mathcal{F}g)$, así que la definición de $L_n\mathcal{F}(\varphi)$ es independiente de la aplicación de cadenas $f_\bullet$.

En segundo lugar, supóngase que $P'_\bullet \twoheadrightarrow M$ es otra resolución proyectiva en A-Mod. De la Proposición 4.25, aplicada a $\varphi = 1_M$ con $P'_\bullet \twoheadrightarrow M$ en lugar de $R_\bullet \twoheadrightarrow N$, se obtiene una aplicación de cadenas $h_\bullet\colon P_\bullet \to P'_\bullet$; y viceversa, cambiando los papeles de las resoluciones proyectivas $P_\bullet \twoheadrightarrow M$ y $P'_\bullet \twoheadrightarrow M$, se obtiene de 1_M una aplicación de cadenas $k_\bullet\colon P'_\bullet \to P_\bullet$. Una vez más, la Proposición 4.25 produce homotopías de cadenas $k_\bullet \circ h_\bullet \sim 1_{P_\bullet}$ y $h_\bullet \circ k_\bullet \sim 1_{P'_\bullet}$; esto es, los complejos $P_\bullet$ y $P'_\bullet$ son *equivalentes en homotopía*. Por lo tanto, hay isomorfismos de grupos $\eta_M \equiv H_n h\colon H_n(\mathcal{F}P) \to H_n(\mathcal{F}P')$ para cada $n \in \mathbb{N}$ (que dependen sólo del A-homomorfismo 1_M y no de la $h_\bullet$ elegida).

En otros términos: si $L'_n\mathcal{F}(M) := H_n(\mathcal{F}P')$ es el n-ésimo funtor derivado de $\mathcal{F}$ definido por otra elección de una resolución proyectiva para cada $M \in\in A\text{-Mod}$, hay un isomorfismo natural $\eta : L_n\mathcal{F} \to L'_n\mathcal{F}$. En consecuencia, *el funtor $L_n\mathcal{F}$ es esencialmente único*.

Lema 4.31. *Los funtores derivados izquierdos tienen las siguientes propiedades, para un A-módulo M con resolución proyectiva $P_\bullet \twoheadrightarrow M$:*

(a) $L_0\mathcal{F}(M) \simeq \mathcal{F}P_0/\operatorname{im}(\mathcal{F}\delta_1)$.

(b) Si $\mathcal{F}$ es un funtor exacto, entonces $L_n\mathcal{F}(M) = 0$ para $n \geq 1$.

(c) Si $\mathcal{F}$ es un funtor exacto a la derecha, entonces $L_0\mathcal{F} = \mathcal{F}$.

Demostración. Ad (a): Para definir $L_0\mathcal{F}$, se usa la homología del complejo truncado $P_\bullet$. En grado cero, cada 0-cadena es un 0-ciclo y cada 0-borde es $\delta_1(x)$ para alguna 1-cadena $x \in P_1$. Luego $Z_0(P) = P_0$ y $B_0(P) = \operatorname{im}\delta_1$.

Ad (b): Si $\mathcal{F}$ es exacto, entonces el complejo $(\mathcal{F}P_\bullet, \mathcal{F}\delta)$ es exacto en $\mathcal{F}P_n$ para cada $n > 0$; luego $H_n(\mathcal{F}P) = 0$ para $n \geq 1$.

Ad (c): La hipótesis implica que la sucesión $\mathcal{F}P_1 \xrightarrow{\mathcal{F}\delta_1} \mathcal{F}P_0 \xrightarrow{\mathcal{F}\varepsilon} \mathcal{F}M \longrightarrow 0$ es exacta. En consecuencia, vale

$$\mathcal{F}M = \operatorname{coker}(\mathcal{F}\delta_1) = \mathcal{F}P_0/\operatorname{im}(\mathcal{F}\delta_1) = H_0(\mathcal{F}P) = L_0\mathcal{F}(M).$$

Si $\varphi \in \operatorname{Hom}_A(M,N)$, es fácil verificar que el homomorfismo $L_0\mathcal{F}(\varphi)\colon H_0(\mathcal{F}P) \to H_0(\mathcal{F}R)$ coincide con $\mathcal{F}\varphi\colon \mathcal{F}M \to \mathcal{F}N$. □

Hay definiciones similares para el caso contravariante. Los detalles se dejan como ejercicio.

Definición 4.32. Sea $\mathcal{G}\colon (A\text{-Mod})^\circ \to \mathsf{Ab}$ un funtor aditivo *contravariante*. Para un A-módulo M, sea $P_\bullet \twoheadrightarrow M$ una resolución proyectiva. Al aplicar $\mathcal{G}$ a esta resolución, se obtiene una *complejo de cocadenas* (de grupos abelianos):

$$0 \longrightarrow \mathcal{G}M \xrightarrow{\mathcal{G}j} \mathcal{G}P_0 \xrightarrow{\mathcal{G}\delta_1} \mathcal{G}P_1 \xrightarrow{\mathcal{G}\delta_2} \cdots \longrightarrow \mathcal{G}P_n \longrightarrow \cdots$$

La cohomología del complejo truncado $(\mathcal{G}P_\bullet, \mathcal{G}\delta)$ no depende (hasta isomorfismo único) de la resolución proyectiva elegida.

Si $\varphi \in \operatorname{Hom}_A(M,N)$, si $R_\bullet \twoheadrightarrow N$ es una resolución proyectiva de N y si $f_\bullet\colon P_\bullet \to R_\bullet$ una aplicación de cadena que hace conmutar el diagrama (4.14), entonces $\mathcal{G}f_\bullet\colon \mathcal{G}R_\bullet \to \mathcal{G}P_\bullet$ es una aplicación de cocadenas.

Para cada $n \in \mathbb{N}$, la cohomología del complejo truncado $(\mathcal{G}P_\bullet, \mathcal{G}\delta)$ define un funtor contravariante $R^n\mathcal{G} : A\text{-Mod} \to \mathsf{Ab}$, esencialmente único, por

$$R^n\mathcal{G}(M) := H^n(\mathcal{G}P), \qquad R^n\mathcal{G}(\varphi) := H^n(\mathcal{G}f). \tag{4.18}$$

Este funtor $R^n\mathcal{G}$ se llama el n-ésimo **funtor derivado derecho** del funtor contravariante $\mathcal{G}$.

Lema 4.33. *Los funtores derivados derechos tienen las siguientes propiedades, para un A-módulo M con resolución proyectiva $P_\bullet \twoheadrightarrow M$:*

(a) $R^0\mathcal{G}(M) \simeq \ker(\mathcal{G}\delta_1)$.

(b) Si $\mathcal{G}$ es un funtor exacto, entonces $R^n\mathcal{G}(M) = 0$ para $n \geq 1$.

(c) Si $\mathcal{G}$ es un funtor exacto a la izquierda, entonces $R^0\mathcal{G} = \mathcal{G}$. ⊟

► Si R es un A-módulo *a la derecha* fijo, ya se sabe que $t_R = (R \otimes_A -)$ es un funtor covariante de A-Mod en Ab que es exacto a la derecha. Por otro lado, si N es un A-módulo (a la izquierda) fijo, se sabe también que $h_N = \mathrm{Hom}_A(-,N)$ es un funtor contravariante de A-Mod en Ab que es exacto a la izquierda. Al particularizar las consideraciones anteriores a estos dos funtores, se obtiene dos familias importantes de funtores derivados.

Definición 4.34. Sea R un A-módulo a la derecha. Entonces $t_R = (R \otimes_A -) : A\text{-Mod} \to \mathsf{Ab}$ es un funtor covariante, exacto a la derecha. Sus funtores derivados izquierdos son

$$\mathrm{Tor}_n^A(R,-) := L_n t_R = L_n(R \otimes_A -), \quad \text{para} \quad n \in \mathbb{N}.$$

Concretamente, si $P_\bullet \twoheadrightarrow M$ es una resolución proyectiva, hay un complejo de cadenas

$$\cdots \longrightarrow R \otimes_A P_n \longrightarrow \cdots \longrightarrow R \otimes_A P_1 \xrightarrow{1_R \otimes \delta_1} R \otimes_A P_0 \xrightarrow{1_R \otimes \varepsilon} R \otimes_A M \longrightarrow 0,$$

y la homología del complejo truncado es $\mathrm{Tor}_n^A(R,M) := H_n(R \otimes_A P_\bullet)$. Este grupo abeliano se llama el n-ésimo **producto de torsión** de R por M.

Por el Lema 4.31, vale $\mathrm{Tor}_0^A(R,M) = R \otimes_A M$. Además, si R es llano en Mod-A, entonces $\mathrm{Tor}_n^A(R,M) = 0$ para $n \geq 1$.

Ejemplo 4.35. Considérese el grupo abeliano $\mathbb{Z}/m$, donde $m \in \mathbb{N}$ con $m > 1$. Una resolución proyectiva de $\mathbb{Z}/m$ en $\mathsf{Ab} = \mathbb{Z}$-Mod es

$$\cdots \longrightarrow 0 \longrightarrow \mathbb{Z} \xrightarrow{\times m} \mathbb{Z} \xrightarrow{\varepsilon} \mathbb{Z}/m \longrightarrow 0,$$

según el Ejemplo 4.26. Si H es un grupo abeliano, el complejo $H \otimes_{\mathbb{Z}} P_\bullet$ es

$$\cdots \longrightarrow 0 \longrightarrow H \xrightarrow{\times m} H \longrightarrow 0,$$

donde se ha empleado el isomorfismo $H \otimes_{\mathbb{Z}} \mathbb{Z} \simeq H$ y $(\times m)$ denota el endomorfismo $x \mapsto mx$ de H. La homología de este complejo da $\mathrm{Tor}_0^{\mathbb{Z}}(H, \mathbb{Z}/m) = H/mH$ mientras $\mathrm{Tor}_1^{\mathbb{Z}}(H, \mathbb{Z}/m) = \{\, x \in H : mx = 0 \,\}$; además, $\mathrm{Tor}_n^{\mathbb{Z}}(H, \mathbb{Z}/m) = 0$ para $n \geq 2$.

Definición 4.36. Sea N un A-módulo a la izquierda. Entonces $h_N = \mathrm{Hom}_A(-,N) : A\text{-Mod} \to \mathsf{Ab}$ es un funtor contravariante, exacto a la izquierda. Sus funtores derivados derechos son

$$\mathrm{Ext}_A^n(-,N) := R^n h_N = R^n(\mathrm{Hom}_A(-,N)), \quad \text{para} \quad n \in \mathbb{N}.$$

Concretamente, si $P_\bullet \twoheadrightarrow M$ es una resolución proyectiva, hay un complejo de cocadenas

$$0 \longrightarrow \mathrm{Hom}_A(M,N) \xrightarrow{j^*} \mathrm{Hom}_A(P_0,N) \xrightarrow{\delta_1^*} \mathrm{Hom}_A(P_1,N) \xrightarrow{\delta_2^*} \cdots$$

y la cohomología del complejo truncado es $\mathrm{Ext}_A^n(M,N) := H^n(\mathrm{Hom}_A(P_\bullet,N))$.

Por el Lema 4.33, vale $\mathrm{Ext}_A^0(M,N) = \mathrm{Hom}_A(M,N)$. Además, si N es inyectivo en A-Mod, entonces $\mathrm{Ext}_A^n(M,N) = 0$ para todo $n \geq 1$.

Ejemplo 4.37. Considérese el grupo abeliano $\mathbb{Z}/m$, donde $m \in \mathbb{N}$ con $m > 1$. Si H es un grupo abeliano, hay un isomorfismo obvio $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, H) \simeq \mathbb{Z}$ que lleva el homomorfismo $(1 \mapsto k)$ al elemento $k \in \mathbb{Z}$. Al aplicar $\mathrm{Hom}_{\mathbb{Z}}(-, H)$ a la resolución proyectiva del Ejemplo 4.35, se obtiene el complejo

$$0 \longrightarrow H \xrightarrow{\times m} H \longrightarrow \cdots$$

donde $(\times m)$ denota el endomorfismo $x \mapsto mx$ de H. Entonces $\mathrm{Ext}^0_{\mathbb{Z}}(\mathbb{Z}/m, H) = \{x \in H : mx = 0\}$ mientras $\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/m, H) = H/mH$; además, $\mathrm{Ext}^n_{\mathbb{Z}}(\mathbb{Z}/m, H) = 0$ para $n \geq 2$.

Lema 4.38. *Sea* $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ *una sucesión exacta corta en* A-Mod. *Si* $P_\bullet \twoheadrightarrow L$ *y* $R_\bullet \twoheadrightarrow N$ *son resoluciones proyectivas, hay una resolución proyectiva* $Q_\bullet \twoheadrightarrow M$ *y aplicaciones de cadena* $f_\bullet \colon P_\bullet \to Q_\bullet$ *y* $g_\bullet \colon Q_\bullet \to R_\bullet$ *tales que* $0 \to P_\bullet \xrightarrow{f_\bullet} Q_\bullet \xrightarrow{g_\bullet} R_\bullet \to 0$ *sea una sucesión exacta corta en* A-Compl.

Demostración. Si $\varepsilon' \colon P_0 \twoheadrightarrow L$ y $\varepsilon'' \colon R_0 \twoheadrightarrow N$ son las aumentaciones de las dos resoluciones dadas, se busca un A-módulo proyectivo Q_0 y un epimorfismo $\varepsilon \colon Q_0 \to M$ tal que el siguiente diagrama sea conmutativa, con filas exactas:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & P_0 & \xrightarrow{f_0} & Q_0 & \xrightarrow{g_0} & R_0 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \varepsilon'} & & \downarrow{\scriptstyle \varepsilon} & & \downarrow{\scriptstyle \varepsilon''} & & \\
0 & \longrightarrow & L & \xrightarrow{f} & M & \xrightarrow{g} & N & \longrightarrow & 0
\end{array}$$

Defínase $Q_0 := P_0 \oplus R_0$, el cual es proyectivo por el Lema 3.8. Sea $f_0 \equiv i_1 \colon P_0 \to Q_0$ la inyección canónica y sea $g_0 \equiv p_2 \colon Q_0 \to R_0$ la proyección canónica. Como R_0 es proyectivo, hay un A-homomorfismo $h \colon R_0 \to M$ tal que $g \circ h = \varepsilon''$. Entonces la aplicación $\varepsilon := (f \circ \varepsilon', h) \colon Q_0 \to M$ cumple todos los requisitos.

El Lema de la Culebra, junto con las observaciones de que f_0 es mónico y g es épico, muestra que hay una sucesión exacta corta

$$0 \longrightarrow \ker \varepsilon' \longrightarrow \ker \varepsilon \longrightarrow \ker \varepsilon'' \longrightarrow 0$$

y además hay epimorfismos $\varepsilon'_1 \colon P_1 \twoheadrightarrow \ker \varepsilon$ y $\varepsilon''_1 \colon R_1 \twoheadrightarrow \ker \varepsilon''$ obtenidas de la construcción de resoluciones proyectivas. Luego, al tomar $Q_1 := P_1 \oplus R_1$, el mismo algoritmo produce una sucesión exacta corta

$$0 \longrightarrow P_1 \xrightarrow{f_1} Q_1 \xrightarrow{g_1} R_1 \longrightarrow 0$$

junto con un epimorfismo sobre la sucesión exacta corta anterior. Al continuar por inducción, se obtiene el complejo $Q_\bullet := P_\bullet \oplus R_\bullet$ junto con las aplicaciones de cadena deseadas. □

Proposición 4.39. *Sea* $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ *una sucesión exacta corta en* A-Mod. *Si* $\mathcal{F} \colon$ Mod-$A \to$ Ab *es un funtor covariante, exacto a la derecha, hay una sucesión exacta larga de la forma siguiente:*

$$\cdots \longrightarrow L_2\mathcal{F}N \longrightarrow L_1\mathcal{F}L \longrightarrow L_1\mathcal{F}M \longrightarrow L_1\mathcal{F}N \longrightarrow \mathcal{F}L \xrightarrow{\mathcal{F}f} \mathcal{F}M \xrightarrow{\mathcal{F}g} \mathcal{F}N \longrightarrow 0$$

Además, si $\mathcal{G}\colon (\mathsf{Mod}\text{-}A)^\circ \to \mathsf{Ab}$ *es un funtor contravariante, exacto a la izquierda, hay una sucesión exacta larga de la forma siguiente:*

$$0 \longrightarrow \mathcal{G}L \xrightarrow{\mathcal{G}g} \mathcal{G}M \xrightarrow{\mathcal{G}f} \mathcal{G}N \longrightarrow R^1\mathcal{G}L \longrightarrow R^1\mathcal{G}M \longrightarrow R^1\mathcal{G}N \longrightarrow R^2\mathcal{G}L \longrightarrow \cdots$$

Demostración. Sean $P_\bullet \twoheadrightarrow L$ y $R_\bullet \twoheadrightarrow N$ dos resoluciones proyectivas, y sea $Q_\bullet \twoheadrightarrow M$ la resolución proyectiva proporcionada por el Lema 4.38, que además produce una sucesión exacta corta de complejos de cadena, $0 \to P_\bullet \xrightarrow{f_\bullet} Q_\bullet \xrightarrow{g_\bullet} R_\bullet \to 0$.

Por la construcción de $Q_\bullet$ como suma directa $P_\bullet \oplus R_\bullet$, esta SEC de complejos *escinde*.[11] Al aplicar el funtor $\mathcal{F}$, la siguiente sucesión exacta corta de complejos de grupos abelianos también escinde:

$$0 \longrightarrow \mathcal{F}P_\bullet \xrightarrow{\mathcal{F}f_\bullet} \mathcal{F}Q_\bullet \xrightarrow{\mathcal{F}g_\bullet} \mathcal{F}R_\bullet \longrightarrow 0.$$

Ahora bien: al aplicar la Proposición 4.20 a esta SEC de complejos, se obtiene una sucesión exacta larga en homología, la cual es exactamente la primera sucesión del enunciado.

En el caso contravariante, se obtiene una SEC de complejos de cocadenas en Ab:

$$0 \longrightarrow \mathcal{G}R_\bullet \xrightarrow{\mathcal{G}g_\bullet} \mathcal{G}Q_\bullet \xrightarrow{\mathcal{G}f_\bullet} \mathcal{G}P_\bullet \longrightarrow 0,$$

que conlleva una sucesión exacta larga en cohomología, por la Proposición 4.25 (*mutatis mutandis*), que es exactamente la segunda sucesión del enunciado. □

Corolario 4.40. *Sea* $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ *una sucesión exacta corta en* A-Mod.

(a) Si $R \in\in \mathsf{Mod}\text{-}A$*, hay una* ***sucesión exacta larga*** *para* Tor*:*

$$\begin{aligned} \cdots &\longrightarrow \operatorname{Tor}_2^A(R,L) \longrightarrow \operatorname{Tor}_2^A(R,M) \longrightarrow \operatorname{Tor}_2^A(R,N) \\ &\longrightarrow \operatorname{Tor}_1^A(R,L) \longrightarrow \operatorname{Tor}_1^A(R,M) \longrightarrow \operatorname{Tor}_1^A(R,N) \\ &\longrightarrow R\otimes_A L \xrightarrow{f_\sharp} R\otimes_A M \xrightarrow{g_\sharp} R\otimes_A N \longrightarrow 0 \end{aligned} \tag{4.19a}$$

(b) Si $S \in\in A$-Mod*, hay una* ***sucesión exacta larga*** *para* Ext*:*

$$\begin{aligned} 0 &\longrightarrow \operatorname{Hom}_A(L,S) \xrightarrow{g^*} \operatorname{Hom}_A(M,S) \xrightarrow{f^*} \operatorname{Hom}_A(N,S) \\ &\longrightarrow \operatorname{Ext}_A^1(L,S) \longrightarrow \operatorname{Ext}_A^1(M,S) \longrightarrow \operatorname{Ext}_A^1(N,S) \\ &\longrightarrow \operatorname{Ext}_A^2(L,S) \longrightarrow \operatorname{Ext}_A^2(M,S) \longrightarrow \operatorname{Ext}_A^2(N,S) \longrightarrow \cdots \end{aligned} \tag{4.19b}$$

Demostración. Son los casos particulares $\mathcal{F} = (R\otimes_A -)$ y $\mathcal{G} = \operatorname{Hom}_A(-,S)$ de la Proposición anterior. □

[11] La SEC original $0 \to L \to M \to N \to 0$ no escinde en general, pero esto es irrelevante porque se trabaja con los complejos truncados $P_\bullet$, $Q_\bullet$, $R_\bullet$ a la hora de calcular su homología.

Proposición 4.41. *Las siguientes condiciones son equivalentes, para $M \in\in A$-Mod:*

(a) M es un A-módulo proyectivo.

(b) $\operatorname{Ext}^n_A(M,N) = 0$ para todo A-módulo N y todo $n \geq 1$.

(c) $\operatorname{Ext}^1_A(M,N) = 0$ para todo A-módulo N.

Demostración. Ad (a) $\Longrightarrow$ (b): Si M es proyectivo, la sucesión exacta $0 \to M \xrightarrow{1_M} M \to 0$ es una resolución proyectiva finita de M. Al aplicar el funtor h_N, se obtiene el complejo truncado $\operatorname{Hom}_A(M,N) \to 0 \to 0 \to \cdots$ que es obviamente acíclico.

Ad (b) $\Longrightarrow$ (c): Evidente.

Ad (c) $\Longrightarrow$ (a): Elíjase un epimorfismo $\varepsilon\colon P \to M$ donde P es un A-módulo proyectivo y sea $K := \ker\varepsilon$. Entonces hay una sucesión exacta corta de A-módulos:

$$0 \longrightarrow K \xrightarrow{j} P \xrightarrow{\varepsilon} M \longrightarrow 0. \tag{4.20}$$

Debido a que $\operatorname{Ext}^1_A(P,N) = 0$ por la implicación (a) $\Longrightarrow$ (b) para el A-módulo proyectivo P, la sucesión exacta larga (4.19b) para Ext se reduce a una sucesión exacta de 6 términos:

$$0 \longrightarrow \operatorname{Hom}_A(M,N) \xrightarrow{\varepsilon^*} \operatorname{Hom}_A(P,N) \xrightarrow{j^*} \operatorname{Hom}_A(K,N) \longrightarrow \operatorname{Ext}^1_A(M,N) \longrightarrow 0. \tag{4.21}$$

Se concluye que $\operatorname{Ext}^1_A(M,N) = \operatorname{coker} j^*$.

En el caso de que $\operatorname{Ext}^1_A(M,N) = 0$, el homomorfismo j^* es sobreyectivo. Si esto es así para cualquier N, puede tomarse $N = K$ y por ende $j^*\colon \operatorname{Hom}_A(P,K) \to \operatorname{End}_A(K)$ es sobreyectivo. En particular, la identidad $1_K \in \operatorname{End}_A(K)$ tiene un preimagen $f \in \operatorname{Hom}_A(P,K)$ tal que $f \circ j = j^*(f) = 1_K$. Pero la existencia de tal f dice que la SEC (4.20) escinde; luego, M es proyectivo por la Proposición 3.4. □

► El resultado de la Proposición anterior conduce a una interpretación importante del grupo abeliano $\operatorname{Ext}^1_A(M,N)$, que entre otras cosas motiva el nombre Ext. Es necesario hacer una excursión lateral al concepto de extensiones de A-módulos.

Definición 4.42. Una **extensión** de un A-módulo M por otro A-módulo N es una sucesión exacta en A-Mod:

$$\mathcal{E}: \qquad 0 \longrightarrow N \xrightarrow{i} R \xrightarrow{p} M \longrightarrow 0. \tag{4.22}$$

Fíjese que $N \simeq i(N) \subseteq R$ y que $R/i(N) \simeq M$. Cabe mencionar la **extensión escindida** como caso particular:

$$\mathcal{E}_0: \qquad 0 \longrightarrow N \xrightarrow{i_2} M \oplus N \xrightarrow{p_1} M \longrightarrow 0. \tag{4.23}$$

Un **morfismo de extensiones** es una aplicación de cadena de la siguiente forma:

$$\begin{array}{ccccccccc} \mathcal{E}: & & 0 & \longrightarrow & N & \xrightarrow{i} & R & \xrightarrow{p} & M & \longrightarrow & 0 \\ \downarrow & & & & \downarrow{\scriptstyle 1_N} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_M} & & \\ \mathcal{E}': & & 0 & \longrightarrow & N & \xrightarrow{i'} & R' & \xrightarrow{p'} & M & \longrightarrow & 0 \end{array}$$

determinado por un A-homomorfismo $\varphi\colon R \to R'$ que cumple $\underline{\varphi \circ i = i'}$ y $\underline{p' \circ \varphi = p}$.

Por el Lema de Cinco (corto), tal φ es automáticamente un *isomorfismo*. Dos extensiones de M por N se llaman **equivalentes** si hay un morfismo entre ellas. (Es evidente que esta relación es transitiva.) Denótese por $\underline{E(M,N)}$ el conjunto de clases de equivalencia de extensiones de M por N.

Proposición 4.43. *Dadas dos A-módulos M y N, hay una correspondencia biyectiva entre clases de extensiones en $E(M,N)$ y elementos del grupo abeliano* $\operatorname{Ext}^1_A(M,N)$.

Demostración. Hay un A-módulo proyectivo P tal que M sea un cociente de P. Sea $\varepsilon\colon P \to M$ la aplicación cociente y sea $K := \ker \varepsilon$. Es posible definir una aplicación de cadena desde la sucesión exacta corta (4.20) y la extensión (4.22) de la siguiente manera. En el diagrama que sigue:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{j} & P & \xrightarrow{\varepsilon} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \tilde f} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle 1_M} & & \\ 0 & \longrightarrow & N & \xrightarrow{i} & R & \xrightarrow{p} & M & \longrightarrow & 0 \end{array} \tag{4.24}$$

sea 1_M el homomorfismo vertical a la derecha. Por ser P proyectivo y $p\colon R \to M$ sobreyectivo, hay $f \in \operatorname{Hom}_A(P,R)$ tal que $p \circ f = \varepsilon$. Como (K,j) es un núcleo para ε y (N,i) es un núcleo para p, el Lema 4.17 produce $\tilde f \in \operatorname{Hom}_A(K,N)$ tal que $i \circ \tilde f = f \circ j$.

Estos f y $\tilde f$ no son únicos, en general. Si $g \in \operatorname{Hom}_A(P,R)$ cumple $p \circ g = \varepsilon$, entonces hay $\tilde g \in \operatorname{Hom}_A(K,N)$ tal que $i \circ \tilde g = g \circ j$. Por tanto, vale $p \circ (f-g) = 0$. Como (R,i) es un núcleo para p, hay un único $h \in \operatorname{Hom}_A(P,N)$ tal que $f - g = i \circ h$. Entonces

$$i \circ (\tilde f - \tilde g) = (f-g) \circ j = i \circ h \circ j,$$

y como i es un monomorfismo, se concluye que $\tilde f - \tilde g = h \circ j = j^*(h)$ en $\operatorname{Hom}_A(K,N)$.

Como P es proyectivo, la sucesión exacta (4.21) termina con un A-módulo nulo $0 = \operatorname{Hom}_A(P,N)$, así que $\operatorname{coker} j^* = \operatorname{Ext}^1_A(M,N)$. Ahora, $\tilde f$ y $\tilde g$ pertenecen a la misma coclase con respecto a $\operatorname{im} j^*$; por ende,

$$[\tilde f] = [\tilde g] \in \operatorname{Hom}_A(K,N)/(\operatorname{im} j^*) = \operatorname{coker} j^* = \operatorname{Ext}^1_A(M,N).$$

Este elemento de $\operatorname{Ext}^1_A(M,N)$ depende sólo de la extensión (4.22) y no de la elección de $\tilde f$.

Si $0 \to N \xrightarrow{i'} R' \xrightarrow{p'} M \to 0$ es otra extensión equivalente a (4.22) mediante un isomorfismo $\varphi\colon \mathcal{E} \to \mathcal{E}'$, la aplicación de cadena compuesta

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{j} & P & \xrightarrow{\varepsilon} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \tilde f} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle 1_M} & & \\ 0 & \longrightarrow & N & \xrightarrow{i} & R & \xrightarrow{p} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 1_N} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_M} & & \\ 0 & \longrightarrow & N & \xrightarrow{i'} & R' & \xrightarrow{p'} & M & \longrightarrow & 0 \end{array}$$

indica que $\tilde{f} \in \mathrm{Hom}_A(K,N)$ no cambia al mudar $f \in \mathrm{Hom}_A(P,R)$ en $\varphi \circ f \in \mathrm{Hom}_A(P,R')$. Luego la coclase $[\tilde{f}] \in \mathrm{Ext}^1_A(M,N)$ depende solamente de la clase de equivalencia $[\mathcal{E}]$de la extensión (4.22). Esto define una función $\Psi\colon E(M,N) \to \mathrm{Ext}^1_A(M,N)$.

Para ver que Ψ es sobreyectiva, sea dada un elemento $\tilde{f} \in \mathrm{Hom}_A(K,N)$. Considérese el pushout de $N \xleftarrow{\tilde{f}} K \xrightarrow{j} P$:

$$\begin{array}{ccccc} 0 & \longrightarrow & K & \xrightarrow{j} & P \\ & & \downarrow{\scriptstyle \tilde{f}} & & \downarrow{\scriptstyle f} \\ 0 & \longrightarrow & N & \xrightarrow{i} & R \end{array}$$

Fíjese que i es un monomorfismo porque j es un monomorfismo, por las propiedades de pushouts. Concretamente, tómese $R := (N \oplus P)/J$, donde $J = \{\, (-\tilde{f}(z), j(z)) : z \in K \,\}$. Si $x \in N$, $y \in P$, conviene denotar por $[x,y]$ la coclase en R de $(x,y) \in N \oplus P$. El A-homomorfismo $N \oplus P \to M : (x,y) \mapsto \varepsilon(y)$ se anula en J, luego hay un A-homomorfismo sobreyectivo $p\colon R \to M$ dado por $p[x,y] := \varepsilon(y)$. Además,

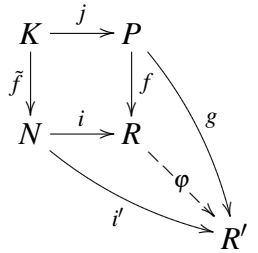
$$\begin{aligned} \ker p &= \{\, [x,y] : y \in \ker \varepsilon = \mathrm{im}\, j \,\} = \{\, [x, j(z)] : x \in N,\ z \in K \,\} \\ &= \{\, [x + \tilde{f}(z), 0] : x \in N,\ z \in K \,\} = \mathrm{im}\, i. \end{aligned}$$

De este modo se obtiene un diagrama conmutativo con filas exactas:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{j} & P & \xrightarrow{\varepsilon} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \tilde{f}} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle 1_M} & & \\ 0 & \longrightarrow & N & \xrightarrow{i} & R & \xrightarrow{p} & M & \longrightarrow & 0 \end{array}$$

y la fila inferior es una extensión $\mathcal{E}$ de M por N tal que $\Psi([\mathcal{E}]) = [\tilde{f}] \in \mathrm{Ext}^1_A(M,N)$. Luego Ψ es sobreyectiva.

La función Ψ es también inyectiva: sea $\mathcal{E}'\colon\ 0 \to N \xrightarrow{i'} R' \xrightarrow{p'} M \to 0$ otra extensión que induce $g \in \mathrm{Hom}_A(P,R)$ y $\tilde{g} \in \mathrm{Hom}_A(K,N)$ como antes, tal que $\tilde{g} = \tilde{f}$. Entonces, como (R,i,f) es un pushout, hay un único $\varphi \in \mathrm{Hom}_A(R,R')$ tal que $\varphi \circ i = i'$ y $\varphi \circ f = g$:



Además, $p' \circ \varphi \circ f = p' \circ g = \varepsilon = p \circ f$ y también $p' \circ \varphi \circ i = p' \circ i' = 0 = p \circ i$, de modo que $p' \circ \varphi$ y p coinciden sobre $i(N) + f(P) = R$; luego, $p' \circ \varphi = p$ en $\mathrm{Hom}_A(R,M)$. Esto dice que $\varphi\colon \mathcal{E} \to \mathcal{E}'$ es una equivalencia de extensiones. En otras palabras, la coclase $[\tilde{f}]$ determina la clase $[\mathcal{E}]$ de la extensión; por tanto, Ψ es inyectiva. $\square$

Es posible combinar dos extensiones de manera directa, para definir una operación asociativa y conmutativa en clases de extensiones. De esta manera, $E(M,N)$ queda dotado de una estructura de grupo abeliano y resulta que $\Psi\colon E(M,N) \to \operatorname{Ext}^1_A(M,N)$ es un isomorfismo de grupos.

Definición 4.44. Sean $\mathcal{E}'\colon\ 0 \to N \xrightarrow{i'} R' \xrightarrow{p'} M \to 0$ y $\mathcal{E}''\colon\ 0 \to N \xrightarrow{i''} R'' \xrightarrow{p''} M \to 0$ dos extensiones de M por N en A-Mod. Su **suma de Baer** es la extensión definida como sigue. Sea (T,h',h'') el pullback del diagrama $R' \xrightarrow{p'} M \xleftarrow{p''} R''$. Concretamente, se define

$$T := \{\, (x,y) \in R' \oplus R'' : p'(x) = p''(y) \,\}, \quad \text{con} \quad h'(x,y) := x,\ h''(x,y) := y.$$

El submódulo "antidiagonal" $S := \{\, (i'(z), -i''(z)) : z \in N \,\} \subseteq R' \oplus R''$ cumple $S \subseteq T$, ya que $p'(i'(z)) = 0 = p''(i''(-z))$ para $z \in N$. Sea $\underline{R := T/S}$. Con la notación $[x,y] \equiv (x,y) + S$, defínase $i\colon N \to R$ y $p\colon R \to M$ por

$$i(z) := [i'(z), 0] = [0, i''(z)], \qquad p([x,y]) := p'(x) = p''(y).$$

Entonces i es inyectiva, p es sobreyectiva y además

$$\begin{aligned} \ker p &= \{\, [x,y] \in R : p'(x) = p''(y) = 0 \,\} = \{\, [i'(z), i''(w)] : z, w \in N \,\} \\ &= \{\, [i'(z+w), 0] : z, w \in N \,\} = \operatorname{im} i. \end{aligned}$$

Luego $\mathcal{E}\colon\ 0 \to N \xrightarrow{i} R \xrightarrow{p} M \to 0$ es una extensión de M por N: esta extensión es la suma de Baer $\underline{\mathcal{E}' + \mathcal{E}''} := \mathcal{E}$.

Lema 4.45. *Cuando $\mathcal{E}'$ y $\mathcal{E}''$ son dos extensiones de M por N en A-Mod, resulta entonces que $\Psi([\mathcal{E}' + \mathcal{E}'']) = \Psi([\mathcal{E}']) + \Psi([\mathcal{E}''])$ en $\operatorname{Ext}^1_A(M,N)$.*

Demostración. Sea $0 \to K \xrightarrow{j} P \xrightarrow{\varepsilon} M \longrightarrow 0$ una sucesión exacta corta en A-Mod, con P proyectivo. Entonces $\Psi([\mathcal{E}']) = [\tilde{f}']$ y $\Psi([\mathcal{E}'']) = [\tilde{f}'']$ donde $f', f'' \in \operatorname{Hom}_A(P,N)$ y $\tilde{f}', \tilde{f}'' \in \operatorname{Hom}_A(K,N)$ se definen por diagramas análogas a (4.24). Con $R = T/S$ de la Definición anterior de $\mathcal{E} := \mathcal{E}' + \mathcal{E}''$, sea $f\colon P \to R$ el A-homomorfismo dado por $f(u) := [f'(u), f''(u)]$ para $u \in P$. Si $v \in K$, entonces

$$f(j(v)) = \big[f'(j(v)), f''(j(v))\big] = \big[i'(\tilde{f}'(v)), i''(\tilde{f}''(v))\big] = i\big(\tilde{f}'(v) + \tilde{f}''(v)\big) \in R.$$

Por tanto, la definición $\tilde{f} := \tilde{f}' + \tilde{f}'' \in \operatorname{Hom}_A(K,N)$ es consistente con el diagrama (4.24). En otras palabras, $\Psi([\mathcal{E}]) = [\tilde{f}] = [\tilde{f}'] + [\tilde{f}'']$. □

Lema 4.46. *El cero del grupo abeliano $E(M,N)$ es la extensión escindida* (4.23).

Demostración. Obsérvese que la aditividad de Ψ, del Lema anterior, junto con la notación $[\mathcal{E}'] + [\mathcal{E}''] := [\mathcal{E}' + \mathcal{E}'']$, define una operación binaria sobre $E(M,N)$ que corresponde bajo Ψ con la suma del grupo abeliano $\operatorname{Ext}^1_A(M,N)$. Por tanto, esta operación de grupo en $E(M,N)$ es asociativa y conmutativa.

Para mostrar que $[\mathcal{E}_0] = 0$ en este grupo, basta encontrar un A-homomorfismo $g\colon P \to M \oplus N$ tal que $\tilde{g} = 0$ en $\mathrm{Hom}_A(K,N)$; en otras palabras, se requiere un diagrama conmutativo con filas exactas, de la forma

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{j} & P & \xrightarrow{\varepsilon} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 0} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle 1_M} & & \\ 0 & \longrightarrow & N & \xrightarrow{i_2} & M \oplus N & \xrightarrow{p_1} & M & \longrightarrow & 0. \end{array}$$

Los requisitos $p_1 \circ g = \varepsilon$ y $g \circ j = 0$ son satisfechos por $g(u) := (\varepsilon(u), 0)$, para $u \in P$. □

► Para dar una interpretación concreta a los elementos de los grupos abelianos $\mathrm{Ext}^n_A(M,N)$ para $n > 1$, se introduce el concepto de *extensión de orden superior*. Hay una operación de "empalme", introducida por Yoneda, que combina tales extensiones.

Definición 4.47. Una extensión $\mathcal{E}_1\colon\ 0 \to L \xrightarrow{j} R_2 \xrightarrow{p} M \to 0$ del M por L y otra extensión $\mathcal{E}_2\colon\ 0 \to N \xrightarrow{i} R_2 \xrightarrow{q} L \to 0$ de L por N dan lugar a una sucesión exacta de 6 términos por el siguiente **empalme**:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xrightarrow{i} & R_2 & \xrightarrow{h} & R_1 & \xrightarrow{p} & M \longrightarrow 0 \\ & & & & & {\scriptstyle q}\searrow & \uparrow{\scriptstyle j} & & \\ & & & & & & L & & \end{array} \tag{4.25}$$

donde $h := j \circ q \in \mathrm{Hom}_A(R_2, R_1)$. Fíjese que $h \circ i = j \circ q \circ i = 0$ y que $p \circ h = p \circ j \circ q = 0$; además, $\ker h = \ker q = \mathrm{im}\, i$ porque j es mónico, mientras $\mathrm{im}\, h = \mathrm{im}\, j = \ker p$ porque q es épico. Una tal sucesión exacta de 6 términos $\mathcal{E}\colon\ 0 \to N \xrightarrow{i} R_2 \xrightarrow{h} R_1 \xrightarrow{p} M \to 0$ se llama una **2-extensión** de M por N.

Un **morfismo de 2-extensiones** de M por N, $\Phi\colon \mathcal{E} \to \mathcal{E}'$, es una aplicación de cadena de la forma

$$\begin{array}{ccccccccccc} \mathcal{E}: & & 0 & \longrightarrow & N & \xrightarrow{i} & R_2 & \xrightarrow{h} & R_1 & \xrightarrow{p} & M \longrightarrow 0 \\ {\scriptstyle\Phi}\downarrow & & & & \downarrow{\scriptstyle 1_N} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle 1_M} \\ \mathcal{E}': & & 0 & \longrightarrow & N & \xrightarrow{i'} & R_2' & \xrightarrow{h'} & R_1' & \xrightarrow{p'} & M \longrightarrow 0 \end{array}$$

determinado por dos aplicaciones $\Phi = (\varphi_1, \varphi_2)$ con $\varphi_i \in \mathrm{Hom}_A(R_i, R_i')$ para $i = 1,2$, tales que $p' \circ \varphi_1 = p$; $h' \circ \varphi_2 = \varphi_1 \circ h$; $i' = \varphi_2 \circ i$. En este caso, los homomorfismos φ_1, φ_2 no son isomorfismos en general.

Un par de 2-extensiones se declaran equivalentes, $\mathcal{E} \sim \mathcal{E}'$, si hay un número par finito de 2-extensiones intermedios $\mathcal{E} = \mathcal{E}_0, \mathcal{E}_1, \ldots, \mathcal{E}_{2m-1}, \mathcal{E}_{2m} = \mathcal{E}'$ que admiten morfismos según el patrón siguiente

$$\mathcal{E} = \mathcal{E}_0 \xrightarrow{\Phi_1} \mathcal{E}_1 \xleftarrow{\Psi_m} \mathcal{E}_2 \xrightarrow{\Phi_2} \cdots \xleftarrow{\Psi_2} \mathcal{E}_{2m-2} \xrightarrow{\Phi_m} \mathcal{E}_{2m-1} \xleftarrow{\Psi_1} \mathcal{E}_{2m} = \mathcal{E}'.$$

Las clases de equivalencia bajo esta relación forman un conjunto $E_2(M,N)$. El empalme (4.25) determina una operación binaria $\mathrm{Ext}^1_A(M,L) \times \mathrm{Ext}^1_A(L,N) \to \mathrm{Ext}^2_A(M,N)$, llamado el **producto de Yoneda**.

Hay una biyección entre $E_2(M,N)$ y el grupo abeliano $\mathrm{Ext}^2_A(M,N)$, definido por el procedimiento de la Proposición 4.43. En este caso se compara una 2-extensión dada con una resolución parcial de M que incluye dos módulos proyectivos:

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & K & \xrightarrow{j} & P_1 & \xrightarrow{\delta_1} & P_0 & \xrightarrow{\varepsilon} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \tilde{f}} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle 1_M} & & \\ 0 & \longrightarrow & N & \xrightarrow{i} & R_2 & \xrightarrow{h} & R_1 & \xrightarrow{p} & M & \longrightarrow & 0 \end{array}$$

La fila superior es una sucesión exacta, donde los A-módulos P_0 y P_1 son proyectivos. Los primeros dos pasos de la construcción de una resolución proyectiva de M muestran su existencia. Los A-homomorfismos f_0 y f_1 son consecuencias de la proyectividad de P_0 y P_1, y $\tilde{f}\colon K \to N$ sigue por el Lema 4.17. De este modo, se define una clase $[\tilde{f}] \in \mathrm{Ext}^2_A(M,N) = H^2(\mathrm{Hom}_A(P_\bullet, N))$, independiente de la elección de f_0 y f_1, tal que $[\mathcal{E}] \mapsto [\tilde{f}]$ sea la biyección deseada.[12]

► La sucesión exacta larga (4.19b) para los funtores *contravariantes* $\mathrm{Ext}^n_A(-,S)$ no es la única sucesión exacta larga asociada con Ext. Para introducir la otra, sea M un A-módulo fijo y considérese un A-homomorfismo $g\colon N \to N'$. Recuérdese que $h \mapsto g \circ h = g_*(h)$ es un homomorfismo de $\mathrm{Hom}_A(M,N)$ en $\mathrm{Hom}_A(M,N')$. Si $P_\bullet \twoheadrightarrow M$ es una resolución proyectiva de M, los homomorfismos $g_*\colon \mathrm{Hom}_A(P_n,N) \to \mathrm{Hom}_A(P_n,N')$ forman una aplicación de cocadenas entre dos complejos de grupos abelianos:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}_A(M,N) & \xrightarrow{\varepsilon^*} & \mathrm{Hom}_A(P_0,N) & \xrightarrow{\delta_1^*} & \mathrm{Hom}_A(P_1,N) & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle g_*} & & \downarrow{\scriptstyle g_*} & & \downarrow{\scriptstyle g_*} & & \\ 0 & \longrightarrow & \mathrm{Hom}_A(M,N') & \xrightarrow{\varepsilon^*} & \mathrm{Hom}_A(P_0,N') & \xrightarrow{\delta_1^*} & \mathrm{Hom}_A(P_1,N') & \longrightarrow & \cdots \end{array} \tag{4.26}$$

Hay una familia de homomorfismos en cohomología, $\hat{g}_n \equiv H^n g_* : \mathrm{Ext}^n_A(M,N) \to \mathrm{Ext}^n_A(M,N')$ para $n \in \mathbb{N}$.

Es fácil comprobar ahora que las correspondencias $N \mapsto \mathrm{Ext}^n_A(M,N)$, $g \mapsto \hat{g}_n$ definen funtores *covariantes* $\mathrm{Ext}^n_A(M,-)\colon A\text{-}\mathsf{Mod} \to \mathsf{Ab}$ para cada $n \in \mathbb{N}$; y que $\mathrm{Ext}^0_A(M,-)$ coincide con $\mathrm{Hom}_A(M,-)$.

Si $f \in \mathrm{Hom}_A(M',M)$, hay un homomorfismo $f^*\colon \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(M',N)$ para cualquier A-módulo N. Al aplicar la Proposición 4.25 a dos resoluciones proyectivas $P_\bullet \twoheadrightarrow M$, $P'_\bullet \twoheadrightarrow M'$, se obtienen homomorfismos $f^*_n\colon \mathrm{Hom}_A(P_n,N) \to \mathrm{Hom}_A(P'_n,N)$, los cuales inducen homomorfismos $\hat{f}^n \equiv H^n(f^*) : \mathrm{Ext}^n_A(M,N) \to \mathrm{Ext}^n_A(M',N)$ para $n \in \mathbb{N}$. Hay cuadrados conmutativos:

$$\begin{array}{ccc} \mathrm{Hom}_A(M,N) & \xrightarrow{f^*} & \mathrm{Hom}_A(M',N) \\ \downarrow{\scriptstyle g_*} & & \downarrow{\scriptstyle g_*} \\ \mathrm{Hom}_A(M,N') & \xrightarrow{f^*} & \mathrm{Hom}_A(M',N') \end{array} \qquad \begin{array}{ccc} \mathrm{Ext}^n_A(M,N) & \xrightarrow{\hat{f}^n} & \mathrm{Ext}^n_A(M',N) \\ \downarrow{\scriptstyle \hat{g}_n} & & \downarrow{\scriptstyle \hat{g}_n} \\ \mathrm{Ext}^n_A(M,N') & \xrightarrow{\hat{f}^n} & \mathrm{Ext}^n_A(M',N') \end{array}$$

[12] Para los detalles de esta construcción, consúltese el Capítulo 3 del libro: Saunders MacLane, *Homology*, *op. cit.*

En efecto, si $h \in \mathrm{Hom}_A(M,N)$, entonces

$$f^*(g_*(h)) = f^*(g \circ h) = (g \circ h) \circ f = g \circ (h \circ f) = g_*(h \circ f) = g_*(f^*(h)),$$

lo cual establece la conmutatividad del primer diagrama y, de rebote, el caso $n = 0$ del segundo diagrama. Para $n > 0$, hay igualdades análogas en cohomología. La conmutatividad de estos digramas dice que cada $\mathrm{Ext}^n : A\text{-}\mathsf{Mod} \times (A\text{-}\mathsf{Mod})^\circ \to \mathsf{Ab}$ es un *bifuntor*.

Proposición 4.48. *Sea* $0 \to R \xrightarrow{h} S \xrightarrow{k} T \to 0$ *una sucesión exacta corta en* A-Mod. *Para cada* A*-módulo* M*, hay una* ***sucesión exacta larga*** *para* Ext*:*

$$\begin{aligned} 0 &\longrightarrow \mathrm{Hom}_A(M,R) \xrightarrow{h_*} \mathrm{Hom}_A(M,S) \xrightarrow{k_*} \mathrm{Hom}_A(M,T) \\ &\longrightarrow \mathrm{Ext}^1_A(M,R) \longrightarrow \mathrm{Ext}^1_A(M,S) \longrightarrow \mathrm{Ext}^1_A(M,T) \\ &\longrightarrow \mathrm{Ext}^2_A(M,R) \longrightarrow \mathrm{Ext}^2_A(M,S) \longrightarrow \mathrm{Ext}^2_A(M,T) \longrightarrow \cdots \end{aligned}$$

Demostración. Sea $P_\bullet \twoheadrightarrow M$ una resolución proyectiva de M. Por el Lema 3.12, la siguiente sucesión corta es exacta, para cada $n \in \mathbb{N}$:

$$0 \longrightarrow \mathrm{Hom}_A(P_n,R) \xrightarrow{h_*} \mathrm{Hom}_A(P_n,S) \xrightarrow{k_*} \mathrm{Hom}_A(P_n,T) \longrightarrow 0.$$

Además, la conmutatividad del diagrama (4.26), con $g \in \mathrm{Hom}_A(N,N')$ reemplazado por $h \in \mathrm{Hom}_A(R,S)$ y por $k \in \mathrm{Hom}_A(S,T)$ respectivamente, muestra que hay una sucesión exacta corta de complejos de cocadenas:

$$0 \longrightarrow \mathrm{Hom}_A(P_\bullet,R) \xrightarrow{h_{*,\bullet}} \mathrm{Hom}_A(P_\bullet,S) \xrightarrow{k_{*,\bullet}} \mathrm{Hom}_A(P_\bullet,T) \longrightarrow 0.$$

Al aplicar la Proposición 4.20, *mutatis mutandis*, a su cohomología, se obtiene la sucesión exacta larga deseada. □

Hay una manera alternativa de obtener los bifuntores Ext^n, al reemplazar todas las resoluciones proyectivas por *coresoluciones inyectivas*. Brevemente, si $N \rightarrowtail Q^\bullet$ es una coresolución inyectiva y si $\mathcal{F}$: A-Mod $\to$ Ab es un funtor covariante, se puede definir sus funtores derivados derechos (hasta isomorfismos naturales) por $R^n\mathcal{F}(N) := H^n(\mathcal{F}Q)$. Para el caso $\mathcal{F} = \mathrm{Hom}_A(M,-)$, resulta que $R^n\mathcal{F}$ es igual (o mejor dicho, naturalmente isomorfo) a $\mathrm{Ext}^n_A(M,-)$. Los procedimientos anteriores pueden repetirse por analogía, para obtener las dos sucesiones exactas para Ext, aunque en el orden inverso. Para las eventuales aplicaciones en geometría algebraica, algunos autores prefieren desarrollar la teoría de Ext (y Tor) con coresoluciones inyectivas solamente.[13]

[13] Véase, por ejemplo, el Capítulo 20 del libro: Serge Lang, *Algebra*, 3a edición, *op. cit*.

4.5 Ejercicios de álgebra homológica

Ejercicio 4.1. Sea A un álgebra sobre un cuerpo $\mathbb{F}$ y sea M un A-A-bimódulo. Defínase $\beta_n\colon C_n(A,M) \to C_{n-1}(A,M)$ y $b_n\colon C^n(A,M) \to C^{n+1}(A,M)$ por las fórmulas (4.2) y (4.3) respectivamente.

(a) Verificar que $\beta_{n-1} \circ \beta_n = 0$ y que $b_{n+1} \circ b_n = 0$.

(b) Si se define $\beta'_n\colon C_n(A,M) \to C_{n-1}(A,M)$ y $b'_n\colon C^n(A,M) \to C^{n+1}(A,M)$ por las mismas fórmulas pero con el último término a la derecha suprimido en cada caso, comprobar que $\beta'_{n-1} \circ \beta'_n = 0$ y que $b'_{n+1} \circ b'_n = 0$ también.

(c) Defínase $s_n\colon C_n(A,M) \to C_{n+1}(A,M)$ por

$$s_n(x \otimes a_1 \otimes \cdots \otimes a_n) := (-1)^n x \otimes a_1 \otimes \cdots \otimes a_n \otimes 1.$$

Mostrar que $\beta'_{n+1} \circ s_n + s_{n-1} \circ \beta'_n = 1_{C_n(A,M)}$. Concluir que el complejo $(C_\bullet(A,M), \beta')$ tiene homología trivial.

Ejercicio 4.2. Sea A un álgebra sobre un cuerpo $\mathbb{F}$ y sea M un A-A-bimódulo. Sea $\mathrm{Der}(A,M)$ el espacio $\mathbb{F}$-vectorial de las **derivaciones** de A en M: ellas son las aplicaciones lineales $\partial\colon A \to M$ tales que $\partial(ac) = \partial(a)\,c + a\,\partial(c)$ para $a, c \in A$. El subespacio $\mathrm{Der}'(A,M)$ de derivaciones *internas* consta de las $\partial_x\colon a \mapsto (ax - xa)$, para $x \in M$. Demostrar que los primeros dos grupos de cohomología de Hochschild son

$$H^0(A,M) = \{\, x \in M : ax = xa \text{ para todo } a \in A \,\},$$
$$H^1(A,M) = \mathrm{Der}(A,M)/\,\mathrm{Der}'(A,M).$$

Ejercicio 4.3. Sea $f_\bullet\colon (C_\bullet, \delta) \to (D_\bullet, \delta')$ una aplicación de cadenas. Para cada $n \in \mathbb{Z}$, sea $E_n := C_{n-1} \oplus D_n$ y defínase $\delta''_n := E_n \to E_{n-1}$ por

$$\delta''_n(x,y) := \big(-\delta_{n-1}(x), f_{n-1}(x) + \delta'_n(y)\big).$$

(a) Mostrar que $(E_\bullet, \delta'')$ es un complejo de cadenas.[14]

(b) Si $(C^+_\bullet, \delta^+)$ es el complejo "corrido" definido por $C^+_n := C_{n-1}$ y $\delta^+_n := -\delta_{n-1}$, encontrar una aplicación de cadena $p_\bullet\colon E_\bullet \to C^+_\bullet$ tal que haya una sucesión exacta de complejos

$$0 \longrightarrow D_\bullet \xrightarrow{j_\bullet} E_\bullet \xrightarrow{p_\bullet} C^+_\bullet \longrightarrow 0,$$

donde $j_n\colon D_n \to E_n$ es la inclusión $y \mapsto (0,y)$.

(c) Concluir que hay una sucesión exacta larga en homología de la siguiente forma (es cuestión de identificar el homomorfismo conector):

$$\cdots \longrightarrow H_n(D) \xrightarrow{H_n j} H_n(E) \xrightarrow{H_n p} H_{n-1}(C) \xrightarrow{H_{n-1} f} H_{n-1}(D) \xrightarrow{H_{n-1} j} H_{n-1}(E) \longrightarrow \cdots.$$

[14] Este complejo se llama el **cono** de la aplicación de cadenas $f_\bullet$.

Ejercicio 4.4. Un **álgebra de Lie** sobre un cuerpo $\mathbb{F}$ es un espacio $\mathbb{F}$-vectorial $\mathfrak{g}$ (de dimensión finita) con una operación bilineal $[\cdot,\cdot]:\mathfrak{g}\times\mathfrak{g}\to\mathfrak{g}$ (el **corchete**) que cumple[15]

- $[X,Y]=-[Y,X]$ para todo $X,Y\in\mathfrak{g}$ (antisimetría);
- $[[X,Y],Z]+[[Y,Z],X]+[[Z,X],Y]=0$ para todo $X,Y,Z\in\mathfrak{g}$ (identidad de Jacobi).

Un $\mathfrak{g}$**-módulo** es un espacio $\mathbb{F}$-vectorial V con una aplicación lineal $\mathfrak{g}\to\mathrm{End}_{\mathbb{F}}(V)$, escrito $v\mapsto X(v)$ para $v\in V$, $X\in\mathfrak{g}$, que cumple $\underline{[X,Y](v)=X(Y(v))-Y(X(v))}$ para $X,Y\in\mathfrak{g}$.

(a) Mostrar que el propio $\mathfrak{g}$ es un $\mathfrak{g}$-módulo, con $X(Z):=[X,Z]$ para $X,Z\in\mathfrak{g}$.

(b) Una *n-cocadena* en $C^n(\mathfrak{g},V)$ es una aplicación n-lineal *alternante* $\alpha:\mathfrak{g}^n\to V$. ⟦En particular, se toma $C^0(\mathfrak{g},V):=V$.⟧ Defínase $d=d_n:C^n(\mathfrak{g},V)\to C^{n+1}(\mathfrak{g},V)$ por

$$d\alpha(X_0,\dots,X_n):=\sum_{j=0}^{n}(-1)^j X_j\big(\alpha(X_0,\dots,\widehat{X_j},\dots,X_n)\big)\\ +\sum_{1\le j<k\le n}(-1)^{j+k}\,\alpha\big([X_j,X_k],X_0,\dots,\widehat{X_j},\dots,\widehat{X_k},\dots,X_n\big),$$

donde $\widehat{X_j}$ significa la *ausencia* del término X_j en el lugar indicado. Mostrar que $d_{n+1}\circ d_n=0$ para todo $n\in\mathbb{N}$, y verificar que $H^0(\mathfrak{g},V)=V^{\mathfrak{g}}\equiv\{\,v\in V: X(v)=0 \text{ para todo } X\in\mathfrak{g}\,\}$.

Ejercicio 4.5. Sea $C_n:=\{1,\lambda,\lambda^2,\dots,\lambda^{n-1}\}$, con $\lambda^n=1$, el grupo cíclico de orden n; y sea $\mathbb{Z}C_n$ el anillo de grupo (entero) correspondiente. Sea $\underline{N:=1+\lambda+\lambda^2+\cdots+\lambda^{n-1}}\in\mathbb{Z}C_n$. Considérese $\mathbb{Z}$ como $\mathbb{Z}C_n$-módulo trivial, al definir $\lambda m:=m$ para todo $m\in\mathbb{Z}$. Defínase el $\mathbb{Z}C_n$-homomorfismo $\varepsilon:\mathbb{Z}C_n\to\mathbb{Z}$ por $\varepsilon(m_0+m_1\lambda+\cdots+m_{n-1}\lambda^{n-1}):=m_0+\cdots+m_{n-1}$.

Mostrar que hay una resolución proyectiva $P_\bullet\twoheadrightarrow\mathbb{Z}$ de $\mathbb{Z}C_n$-módulos con $P_m=\mathbb{Z}C_n$ para todo m, donde $\delta_{2m}:=N$ y $\delta_{2m-1}:=\lambda-1$ (como operadores de multiplicación) para $m\ge1$:

$$\cdots\longrightarrow P_m\longrightarrow\cdots\longrightarrow P_4\xrightarrow{N}P_3\xrightarrow{\lambda-1}P_2\xrightarrow{N}P_1\xrightarrow{\lambda-1}P_0\xrightarrow{\varepsilon}\mathbb{Z}\longrightarrow0.$$

⟦Para comprobar que esta sucesión es exacta, considérese los homomorfismos de grupos abelianos $s,s':\mathbb{Z}C_n\to\mathbb{Z}C_n$ definidos por

$$s(1):=0,\quad s(\lambda^k):=1+\lambda+\cdots+\lambda^{k-1}\text{ para }k=1,\dots,n-1,\\ s'(\lambda^{n-1}):=1,\quad s'(\lambda^k):=0\text{ para }k=0,\dots,n-2.$$

Comprobar que $(\lambda-1)\circ s+s'\circ N=1$ y también que $N\circ s'+s\circ(\lambda-1)=1$.⟧

Ejercicio 4.6. Sea A un anillo entero y sea $\mathbb{F}$ su cuerpo de fracciones (véase el Ejercicio 3.10.) Demostrar que la siguiente sucesión es una resolución inyectiva de A:

$$0\longrightarrow A\xrightarrow{i}\mathbb{F}\xrightarrow{p}\mathbb{F}/A\longrightarrow0\longrightarrow\cdots\longrightarrow0\longrightarrow\cdots$$

donde $i:A\hookrightarrow\mathbb{F}$ es la inclusión y $p:\mathbb{F}\to\mathbb{F}/A$ es la aplicación cociente.

[15] Por ejemplo, $\mathfrak{gl}(n,\mathbb{F})$ denota el espacio vectorial de matrices $M_n(\mathbb{F})$ con corchete $[X,Y]:=\underline{XY-YX}$. Un álgebra de Lie se llama *matricial* si es un subálgebra (de Lie) de algún $\mathfrak{gl}(n,\mathbb{F})$.

Ejercicio 4.7. Si $\mathcal{F}\colon A\text{-Mod} \to \mathsf{Ab}$ es un funtor aditivo covariante y $0 \to L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ es una SEC escindida de A-módulos, demostrar que $0 \to \mathcal{F}L \xrightarrow{\mathcal{F}f} \mathcal{F}M \xrightarrow{\mathcal{F}g} \mathcal{F}N \longrightarrow 0$ es una SEC escindida de grupos abelianos.[16]

Ejercicio 4.8. Si $\mathcal{F}\colon A\text{-Mod} \to \mathsf{Ab}$ es un funtor aditivo covariante y $0 \to K \xrightarrow{j} P \xrightarrow{\varepsilon} M \longrightarrow 0$ es una SEC de A-módulos con P proyectivo, mostrar que $L_1\mathcal{F}M \simeq \ker(\mathcal{F}j)$ y que hay isomorfismos $L_{n+1}\mathcal{F}M \simeq L_n\mathcal{F}K$ para $n \geq 1$.

Ejercicio 4.9. Dado un diagrama conmutativo de A-módulos, cuyas filas son sucesiones exactas cortas:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{f} & M & \xrightarrow{g} & N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle t} & & \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle v} & & \\ 0 & \longrightarrow & R & \xrightarrow{h} & S & \xrightarrow{k} & T & \longrightarrow & 0, \end{array}$$

(a) si t, v son sobreyectivos, mostrar que u es también sobreyectivo y que hay una sucesión exacta corta:[17]

$$0 \longrightarrow \ker t \xrightarrow{\tilde{f}} \ker u \xrightarrow{\tilde{g}} \ker v \longrightarrow 0\,;$$

(b) si t, v son inyectivos, mostrar que u es también inyectivo y que hay otra SEC:

$$0 \longrightarrow \operatorname{coker} t \xrightarrow{\bar{h}} \operatorname{coker} u \xrightarrow{\bar{k}} \operatorname{coker} v \longrightarrow 0\,.$$

Ejercicio 4.10. Sea R un A-módulo a la derecha.

(a) Demostrar que $\operatorname{Tor}_1^A(R,P) = 0$ si P es un A-módulo proyectivo.

(b) Mostrar que R es llano en Mod-A si y sólo si $\operatorname{Tor}_1^A(R,M) = 0$ para todo $M \in\in A\text{-Mod}$.

⟦ Indicación: Considerar una SEC $0 \to K \xrightarrow{j} P \xrightarrow{\varepsilon} M \longrightarrow 0$, con P proyectivo. ⟧

Ejercicio 4.11. (a) Si M,N son A-módulos a la izquierda y si R,S son A-módulos a la derecha, demostrar que $\operatorname{Tor}_n^A(R, M\oplus N) \simeq \operatorname{Tor}_n^A(R,M) \oplus \operatorname{Tor}_n^A(R,N)$ y que $\operatorname{Tor}_n^A(R\oplus S, M) \simeq \operatorname{Tor}_n^A(R,M) \oplus \operatorname{Tor}_n^A(S,M)$.

(b) Si A es un anillo entero principal y si M_{tor} denota el submódulo de torsión de M, demostrar que $\operatorname{Tor}_n^A(R,M) \simeq \operatorname{Tor}_n^A(R_{\text{tor}}, M_{\text{tor}})$.

Ejercicio 4.12. (a) Encontrar una resolución proyectiva de $\mathbb{Z}/4$ en A-Mod para el anillo $A = \mathbb{Z}/8$.

(b) Calcular los grupos abelianos $\operatorname{Tor}_n^{\mathbb{Z}/8}(\mathbb{Z}/4, \mathbb{Z}/4)$, para todo $n \in \mathbb{N}$.

Ejercicio 4.13. Si A es un anillo entero principal con $b \in A$ y si M es un A-módulo, escríbase $bM := \{\, bx : x \in M \,\}$. Demostrar que $\operatorname{Ext}_A^1(A/bA, M) \simeq M/bM$.

[16] El resultado de este Ejercicio fue usado en la demostración de la Proposición 4.39.

[17] El resultado de este Ejercicio fue usado en la demostración del Lema 4.38.

Ejercicio 4.14. (a) Si $p \in \mathbb{N}$, demostrar que $\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/p, \mathbb{Z}/p) \simeq \mathbb{Z}/p$.

(b) Si $p \in \mathbb{N}$ es primo, mostrar que las extensiones

$$\mathcal{E}_k: \qquad 0 \longrightarrow \mathbb{Z}/p \xrightarrow{\ i\ } \mathbb{Z}/p^2 \xrightarrow{\ \hat{k}\ } \mathbb{Z}/p \longrightarrow 0,$$

donde $i(m \bmod p) := (pm \bmod p^2)$ y $\hat{k}(r \bmod p^2) := (kr \bmod p)$, para $k = 1, 2, \ldots, p-1$, son inequivalentes y que no son escindidas.

Ejercicio 4.15. (a) Si $\mathcal{E}: \ 0 \to N \xrightarrow{\ i\ } R \xrightarrow{\ p\ } M \longrightarrow 0$ es una extensión de M por N y si $f \in \mathrm{Hom}_A(N, N')$, construir una extensión $f_*\mathcal{E}$ de M por N', tal que haya un diagrama conmutativo

$$\begin{array}{lccccccc}
\mathcal{E}: & 0 \longrightarrow & N & \xrightarrow{\ i\ } & R & \xrightarrow{\ p\ } & M & \longrightarrow 0 \\
 & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_M} & \\
f_*\mathcal{E}: & 0 \longrightarrow & N' & \xrightarrow{\ i'\ } & R' & \xrightarrow{\ p'\ } & M & \longrightarrow 0
\end{array}$$

para un A-homomorfismo conveniente $\varphi: R \to R'$. Mostrar que dos extensiones de este tipo son equivalentes.

(b) Si además $g \in \mathrm{Hom}_A(M'', M)$, construir una extensión $g^*\mathcal{E}$ de M'' por N, tal que haya un diagrama conmutativo

$$\begin{array}{lccccccc}
g^*\mathcal{E}: & 0 \longrightarrow & N & \xrightarrow{\ i''\ } & R'' & \xrightarrow{\ p''\ } & M'' & \longrightarrow 0 \\
 & & \downarrow{\scriptstyle 1_N} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle g} & \\
\mathcal{E}: & 0 \longrightarrow & N & \xrightarrow{\ i\ } & R & \xrightarrow{\ p\ } & M & \longrightarrow 0
\end{array}$$

para un A-homomorfismo conveniente $\psi: R'' \to R$. Mostrar que dos extensiones de este tipo son equivalentes.

⟦ Indicación: Sea R' un pushout y R'' un pullback de ciertos diagramas. ⟧

(c) (Opcional). Mostrar que las extensiones $g^*(f_*\mathcal{E})$ y $f_*(g^*\mathcal{E})$, de M'' por N', son equivalentes.

Nota bibliográfica

Los siguientes libros amplifican y profundizan los tópicos vistos en este curso.

1. Frank W. Anderson y Kent R. Fuller, *Rings and Categories of Modules*, Graduate Texts in Mathematics **13**, Springer, New York, 1974.
2. Nicholas Bourbaki, *Éléments de Mathématique VI: Algèbre II*, Hermann, Paris, 1962.
3. Paul M. Cohn, *Algebra 1*, Wiley, Chichester, 1982.
4. John Dauns, *Modules and Rings*, Cambridge University Press, Cambridge, 1994.
5. Carl Faith, *Rings, Modules and Categories I*, Springer, New York, 1973.
6. Sergey I. Gelfand y Yuri I. Manin, *Homological Algebra*, en el Encyclopedia of Mathematical Sciences *38* (Algebra V), Springer, Berlin, 1994.
7. Isadore N. Herstein, *Topics in Algebra*, Blaisdell, New York, 1964.
8. Nathan Jacobson, *Basic Algebra I*, W. H. Freeman, New York, 1985.
9. Nathan Jacobson, *Basic Algebra II*, W. H. Freeman, New York, 1980.
10. Jean-Pierre Lafon, *Les Formalismes Fondamentaux de l'Algèbre Commutative*, Hermann, Paris, 1974.
11. Serge Lang, *Algebra*, 3ª edición, Springer, New York, 2002.
12. Saunders MacLane, *Categories for the Working Mathematician*, Springer, New York, 1971.
13. Saunders MacLane, *Homology*, Springer, Berlin, 1975.
14. Saunders MacLane y Garrett Birkhoff, *Algebra*, Macmillan, New York, 1967.
15. M. Scott Osborne, *Basic Homological Algebra*, Graduate Texts in Mathematics **196**, Springer, New York, 2000.
16. Bodo Pareigis, *Categories and Functors*, Academic Press, Orlando, FL, 1970.
17. Lekh R. Vermani, *An Elementary Approach to Homological Algebra*, Chapman & Hall/CRC Press, Boca Raton, FL, 2003.

Algunos otros libros y artículos mencionados en el texto, en las notas al pie de la página, son los siguientes.

18. Reinhold Baer, *Abelian groups that are direct summands of every containing abelian group*, Bulletin of the American Mathematical Society **46** (1940), 800–806.

19. Samuel Eilenberg y Saunders MacLane, *General theory of natural equivalences*, Transactions of the American Mathematical Society **58** (1945), 231–294.

20. Paul R. Halmos, *Naive Set Theory*, Springer, New York, 1974.

21. Goro Kato, *The Heart of Cohomology*, Springer, Dordrecht, 2006.

22. Ralf Meyer, *Homological algebra in bivariant K-theory and other triangulated categories. II*, preprint arXiv:0801.1344, Göttingen, 2008.

23. Kiiti Morita, *Duality for modules and its applications to the theory of rings with minimum condition*, Scientific Reports of the Tokyo Kyoiku Daigaku **6** (1958), 83–142.

24. Shigeyuki Morita, *Geometry of Differential Forms*, Translations of Mathematical Monographs **201**, American Mathematical Society, Providence, RI, 2001.

25. Jonathan Rosenberg, *Algebraic K-theory and its Applications*, Graduate Texts in Mathematics **147**, Springer, Berlin, 1994.

26. Paul Theroux, *The Old Patagonian Express: By Train Through the Americas*, Mariner Books, New York, 1979.