"Cuadernos de Matemática y Mecánica" comprende dos series de publicaciones. *Ediciones Previas* tiene por objeto facilitar la pronta difusión de trabajos de investigación y desarrollo realizados principalmente en el Instituto de Matemática Aplicada del Litoral (IMAL) y en el Centro Internacional de Métodos Computacionales en Ingeniería (CIMEC). *Serie Cursos y Seminarios* está dedicada a la impresión rápida de material bibliográfico considerado de utilidad para el estudio de temas de interés.

"Cuadernos de Matemática y Mecánica" publishes two series. *Ediciones Previas* aims to provide a rapid way of communicating research and development works, specially those which are carried out within the Instituto de Matemática Aplicada del Litoral (IMAL) and the Centro Internacional de Métodos Computacionales en Ingeniería(CIMEC). *Cursos y Seminarios* publishes lectures notes and educational material which are useful to study currently developing topics.

Encargada de Redacción y Publicación: I. Hernández (IMAL)

ISSN N° 1667-3247
"Cuadernos de Matemática y Mecánica"
IMAL (CONICET - UNL) - CIMEC (INTEC, CONICET - UNL)
Güemes 3450, (3000) Santa Fe, Argentina
Fax: 54 - 42 - 4550944, 54 - 42 - 4556673
E-mail: imal@ceride.gov.ar cimec@ceride.gov.ar
Páginas: http://www.imal.ceride.gov.ar http://www.cimec.org.ar

ANILLOS Y SUS CATEGORÍAS DE REPRESENTACIONES

Andrea Solotar
Marco Farinati
Mariano Suárez Alvarez
Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria, Pabellón 1, (1428) Buenos Aires

Argentina

E-mail address: asolotar@dm.uba.ar

Indice

Introducción

Este libro surgió luego del dictado, en diversas oportunidades, del curso de Algebra II para la licenciatura en Ciencias Matemáticas de la Facultad de Ciencias Exactas y Naturales de la Universidad de Buenos Aires. Se trata de la tercera materia de álgebra que cursan los alumnos. La escasez de bibliografía en castellano sobre los temas abarcados por esta materia fue una de las principales motivaciones para escribirlo.

En el proceso de redacción, varios temas fueron profundizados mas allá de lo que se suele dictar en clase, con la idea de que el alumno interesado cuente no sólo con una guía de los contenidos de la materia, sino también con material de consulta que lo prepare antes de abordar literatura más especializada.

Un curso cuatrimestral de estructuras algebraicas debería incluir los contenidos completos de los primeros cuatro capítulos como esqueleto sobre el cual desarrollar con mayor o menor profundidad los contenidos de los capítulos siguientes.

El capítulo sobre Grupos fue encarado como un capítulo introductorio a estructuras, con los contenidos mínimos sobre grupos que se necesitarán en el resto del libro. La razón de esta minimalidad es por un lado que el punto de vista general del libro es el categórico, y el modelo de categoría elegido por nosotros sobre el cual aprender álgebra es el de categoría abeliana. Esto nos llevó a centrar el curso en categorías de módulos sobre un anillo. Por otra parte, la bibliografía a disposición de los alumnos sobre grupos, o grupos finitos, es mucho mas abundante que sobre módulos, con lo que un nuevo libro detallado sobre este tema no se presenta comparativamente tan necesario.

El capítulo de Teoremas de estructura está formado por dos partes a la vez muy diferentes y análogas. Se trata de los teoremas de

estructura de módulos sobre un anillo semisimple, y sobre un dominio principal. Si bien las categorías semisimples tienen un comportamiento muy diferente del de las categorías de módulos sobre un dominio principal, ambas son ejemplos de categorías en donde se tiene una clasificación "completa" de sus objetos. Mientras que en anillos semisimples el ejemplo que tuvimos en mente fue el de un álgebra de grupo, los ejemplos de dominios principales que tomamos como modelos son $\mathbb{Z}$ (obteniendo el teorema de estructura de grupos abelianos finitamente generados) y el anillo de polinomios con coeficientes en un cuerpo: $k[x]$. Este último ejemplo tiene como aplicación, cuando k es algebraicamente cerrado, la obtención de la forma de Jordan. Dada la importancia de esta aplicación, la hemos descripto separadamente como última sección de este capítulo.

El capítulo sobre Categorías puede considerarse también como un Apéndice. Durante el dictado de la materia, las nociones categóricas no fueron dadas ni todas juntas, ni al final, sino de a poco, cuando las necesidades de lenguaje lo indicaban. Generalmente este tema resulta muy difícil de asimilar si no se cuenta con ejemplos concretos de categorías sobre las cuales se haya trabajado. Por esta razón no recomendamos leer directamente este capítulo si no se está familiarizado con teoremas básicos o definiciones habituales de estructuras algebraicas, como los teoremas de isomorfismo, o las definiciones de suma directa, o de objeto proyectivo.

El capítulo sobre los Teoremas de Morita es un punto ideal hacia donde confluir en un curso de álgebra, pues integra nociones de todos los otros capítulos (equivalencias de categorías, módulos proyectivos, generadores, producto tensorial) y a la vez provee resultados muy concretos, como cálculos de subespacios de conmutadores, o relaciones entre propiedades de un anillo A y del anillo de matrices $M_n(A)$.

Por razones evidentes, varias áreas importantes de la teoría de anillos y de la teoría de módulos no son cubiertas por este texto. Mencionamos por ejemplo las herramientas de homología, la teoría de anillos conmutativos, o aspectos de la teoría de representaciones de grupos como caracteres, fórmulas de inducción, etc.

Los ejercicios destinados a profundizar en el conocimiento de estos temas corresponden en su mayoría a las guías de Trabajos Prác-

ticos del primer cuatrimestre de 2007. Estos fueron redactados en su totalidad por Mariano Suárez Alvarez y enriquecen versiones anteriores de estas notas.

Agradezco infinitamente a Mariano por su ayuda con esta nueva versión.

Quiero agradecer los comentarios, sugerencias y correcciones de los alumnos que cursaron Algebra II en los últimos cuatrimestres y que notaron varios errores en versiones previas de este manuscrito. En especial los alumnos del primer cuatrimestre de 2007 y a Nicolás Botbol, ya que con su interés y dedicación generaron varios cambios. También a Estanislao Herscovich por su ayuda con los últimos capítulos.

Por último agradezco a la Msc. Ilda Hernández y al IMAL por darme la oportunidad de publicar este texto.

Andrea Solotar
Buenos Aires, 30 de julio de 2007.

Capítulo 1

Grupos

1.1 Definición y ejemplos

El concepto de grupo apareció inicialmente al considerar grupos de transformaciones de un conjunto. Sin embargo, al estudiar estos grupos de transformaciones se vio que muchas de sus propiedades eran independientes del hecho de que actuaran sobre un conjunto y resultaban consecuencias de ciertos axiomas básicos.

Definición 1.1.1. Un *grupo* $(G, \cdot)$ es un conjunto G provisto de una operación $\cdot : G \times G \to G$ que satisface las siguientes condiciones:

- *Asociatividad:* para todo $g_1, g_2, g_3 \in G$, es

$$(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3).$$

- *Elemento neutro:* existe $e \in G$ tal que para todo $g \in G$ es

$$e \cdot g = g \cdot e = g.$$

- *Inversos:* para todo $g \in G$, existe $g' \in G$ tal que

$$g \cdot g' = g' \cdot g = e.$$

Si además para todo par $g, h \in G$ es $g \cdot h = h \cdot g$ entonces el grupo se llama *abeliano* o *conmutativo*. El cardinal del conjunto G es el *orden* de G y lo escribiremos $|G|$. Diremos que un grupo G es *finito* si $|G| < \infty$ y que es *infinito* en otro caso.

Observaciones.
1. El elemento neutro de un grupo es único, porque si e y e' son dos neutros, entonces $e = e \cdot e' = e'$. La igualdad de la izquierda es porque e' es neutro "a derecha" y la segunda igualdad es porque e es neutro "a izquierda".

2. Un elemento g posee un único inverso g': si g' y g'' son dos inversos para g entonces

$$g' = g' \cdot e = g' \cdot (g \cdot g'') = (g' \cdot g) \cdot g'' = e \cdot g'' = g''.$$

Al único inverso de un elemento g se lo denotará g^{-1}.

Ejemplos.
1. Sea X un conjunto, sea G el conjunto de las funciones biyectivas de X en X y $\cdot$ la composición. En este caso e es función identidad Id_X y si $g \in G$, g^{-1} es la función inversa.

Si el conjunto $X = \{1, 2, 3, \ldots, n\}$, entonces G se denota $\mathcal{S}_n$ y se llama el *n-ésimo grupo simétrico*.

2. Sea V un k espacio vectorial y sea $G = \mathrm{GL}(V)$ el conjunto de los endomorfismos lineales inversibles de V. G es un grupo con la composición de transformaciones como producto y la identidad como elemento neutro. Si $V = k^n$, $\mathrm{GL}(V)$ se nota $\mathrm{GL}_n(k)$ y se identifica (luego de fijar una base de k^n) con las matrices inversibles de n filas y n columnas a coeficientes en k. El elemento neutro es la matriz identidad.

3. Tomando la suma como operación y el cero como neutro, los conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (los números enteros, racionales, reales y complejos) son todos grupos abelianos.

4. Si $m \in \mathbb{N}$, los "restos módulo m" $(\mathbb{Z}_m, +_m, \overline{0})$ forman un grupo abeliano con exactamente m elementos.

5. Dado $n \in \mathbb{N}$, el conjunto $n\mathbb{Z}$ con la suma usual.

6. Si $m \in \mathbb{N}$, $G_m = \{z \in \mathbb{C} : z^m = 1\}$ con la operación producto (como números complejos) es también un grupo abeliano con m elementos. El neutro es el 1.

7. Si X es un conjunto no vacío y G un grupo, entonces el conjunto $\Gamma = \{f : X \to G\}$ de las funciones de X en G es un grupo con la multiplicación definida por

$$(f \cdot g)(x) := f(x) \cdot g(x), \qquad \forall f, g \in \Gamma,\ x \in X.$$

El neutro es la función constante que a todo $x \in X$ le asigna e, el elemento neutro de G. Es fácil ver que Γ es conmutativo si y sólo si G lo es.

8. Si G_1 y G_2 son dos grupos, entonces el *producto cartesiano* $G_1 \times G_2$ admite una estructura de grupo definiendo la operación

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 \cdot g_1', g_2 \cdot g_2').$$

9. Dado $n \in \mathbb{N}$, el conjunto $\mathbb{R}^n$ con la suma usual de vectores.

10. Tomando la multiplicación como operación y el uno como neutro, los conjuntos $\mathbb{Q} - \{0\}$, $\mathbb{R} - \{0\}$ y $\mathbb{C} - \{0\}$ (los números racionales, reales y complejos no nulos, respectivamente) son todos grupos abeliano.

11. Tomando la multiplicación como operación y el uno como neutro, el conjunto $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ es un grupo abeliano.

Observación. Para un grupo arbitrario $(G, \cdot)$, denotaremos indistintamente el producto de dos elementos g_1 y g_2 por $g_1 \cdot g_2 = g_1.g_2 = g_1g_2$. Los símbolos $\cdot$ y . se utilizarán para cualquier tipo de grupo (abeliano o no), mientras que el símbolo $+$ se utilizará *solamente* para grupos abelianos. Cuando se desprenda del contexto no explicitaremos la operación y hablaremos simplemente de un grupo G.

Antes de seguir con las definiciones básicas de la teoría de grupos, hacemos una pequeña disgresión sobre la estructura de monoide.

1.2 Monoides

La estructura de monoide es una generalización de la estructura de grupo, en donde no se pide la existencia de inverso y, según el contexto, a veces se supone la existencia de elemento neutro y a veces no. Damos pues la definición de monoide:

Definición 1.2.1. Un *monoide* $(M, \cdot)$ es un conjunto M provisto de una operación $\cdot : M \times M \to M$ que es asociativa, es decir, para la cual $m \cdot (n \cdot l) = (m \cdot n) \cdot l$ para toda terna de elementos $m, n, l \in M$. Si además existe $e \in M$ tal que $e \cdot m = m \cdot e$ para todo $m \in M$, entonces M se dirá un *monoide con elemento neutro*.

A partir de la definición, es claro que todo grupo es automáticamente un monoide. El ejemplo clásico de monoide que no es grupo es el de los números naturales $(\mathbb{N}, +)$ o, agregándole el elemento neutro, $(\mathbb{N}_0, +)$.

Ejercicio. Si M es un monoide que admite un elemento neutro, entonces ese elemento neutro es único. En particular, el mismo enunciado es cierto para todos los grupos.

Si M es un monoide con elemento neutro, el subconjunto

$$\mathcal{U}(M) = \{m \in M : \text{existe } m' \in M \text{ con } m' \cdot m = e = m \cdot m'\}$$

se denomina el conjunto de *unidades* de M. Tautológicamente $\mathcal{U}(M)$ es un grupo.

Ejemplos.
1. Si $(k, +, \cdot)$ es un cuerpo entonces $(k, \cdot)$ es un monoide con elemento neutro y $\mathcal{U}(k) = k - \{0\}$.

2. Si V es un k-espacio vectorial, $\mathrm{End}_k(V)$ con la composición como operación es un monoide cuyo elemento neutro es la función identidad. En este caso es $\mathcal{U}(End_k(V)) = \mathrm{GL}(V)$.

3. Si X es un conjunto, $\mathrm{Func}(X, X) = \{f : X \to X\}$ es un monoide con la composición como operación y $\mathcal{U}(\mathrm{Func}(X, X)) = \mathcal{S}(X)$.

4. Existen monoides con elemento neutro que admiten elementos inversibles a izquierda pero no a derecha. Consideremos el conjunto $M = CFM_{\mathbb{N}}(\mathbb{R})$ de las matrices infinitas $(a_{ij})_{i,j\in\mathbb{N}}$ con coeficientes reales tales que para todo $j \in \mathbb{N}$, $a_{ij} = 0$ salvo para finitos valores de i. Con el producto usual de matrices M es un monoide. En M, la matriz $(\delta_{i,2j})_{i,j\in\mathbb{N}}$ es inversible a izquierda pero no a derecha.

5. Terminamos esta disgresión sobre monoides con un ejemplo de tipo general.

Sea X un conjunto arbitrario no vacío. Para cada $n \in \mathbb{N}$, sea $X^n := X \times \cdots \times X$ el producto cartesiano de X consigo mismo n veces. Se define

$$L(X) = \coprod_{n\in\mathbb{N}} X^n,$$

donde $\coprod$ indica unión disjunta. Si $n, m \in \mathbb{N}_0$, $(x_1, \ldots, x_n) \in X^n$ y $(x'_1, \ldots, x'_m) \in X^m$, definimos

$$(x_1, \ldots, x_n) \cdot (x'_1, \ldots, x'_m) = (x_1, \ldots, x_n, x'_1, \ldots, x'_m) \in X^{n+m}.$$

Esta operación da una estructura de monoide (sin elemento neutro) en $L(X)$. Llamamos a $L(X)$ el *monoide libre sobre* X.

Si X es un conjunto unitario, $L(X)$ se identifica con $(\mathbb{N}, +)$. Si X tiene por lo menos dos elementos, pruebe que $L(X)$ no es conmutativo.

1.3 Subgrupos. Subgrupos normales

En general, dado un conjunto G, uno puede obtener toda una familia de otros conjuntos simplemente mirando los subconjuntos de G. Si además G tiene estructura de grupo, uno se puede preguntar cómo obtener "gratis", a partir de G, una familia de grupos de manera análoga a la situación conjuntista.

Definición 1.3.1. Dado un grupo $(G, \cdot)$, un *subgrupo* de G es un subconjunto $H \subseteq G$ tal que $(H, \cdot|_{H\times H})$ es un grupo o, equivalentemente, si

(a) $\cdot$ es cerrado en H, esto es, para todo $h_1, h_2 \in H$, se tiene que $h_1 \cdot h_2 \in H$;
(b) $e \in H$; y
(c) para todo $h \in H$, $h^{-1} \in H$.

Observación. La condición *(b)* implica que $H \neq \varnothing$, a su vez las condiciones *(a)* y *(c)* junto con $H \neq \varnothing$ implican la condición *(b)*, por lo tanto en la definición de subgrupo se puede cambiar *(b)* por $H \neq \varnothing$.

Ejemplos.
1. Si $n \in \mathbb{N}$, sea $G_n = \{w \in \mathbb{C} : w^n = 1\}$. Entonces $(G_n, \cdot)$ es un subgrupo de $(\mathbb{C} - \{0\}, \cdot)$.

2. Si $n \in \mathbb{N}$, el conjunto $n\mathbb{Z} = \{nk \ / \ k \in \mathbb{Z}\}$ de los múltiplos de n es un subgrupo de los enteros $(\mathbb{Z}, +)$.

3. Si $G = \mathbb{Z}_6 = \{\overline{0}, \overline{1}, \cdots, \overline{5}\}$, entonces $H_1 = \{\overline{0}, \overline{2}, \overline{4}\}$ y $H_2 = \{\overline{0}, \overline{3}\}$ son subgrupos de G.

4. Si $(G, \cdot)$ es un grupo, G y $\{e\}$ son siempre subgrupos. Si p es un número primo y $G = \mathbb{Z}_p$ se verá fácilmente luego que estos dos subgrupos triviales son los únicos subgrupos que tiene $\mathbb{Z}_p$.

5. Sea $X = \{1, 2, 3, ..., n\}$ y $G = \mathcal{S}_n$ el conjunto de las permutaciones de X. Si $1 \leq i \leq n$, el conjunto de permutaciones que fijan el elemento i de X, esto es, $H_i = \{g \in G : g(i) = i\}$, es un subgrupo de G. ¿Cuántos elementos tiene G? ¿Cuántos elementos tiene H_i?

6. Sea $G = \mathrm{GL}_n(k)$ y sea $H = \{A \in G : \det A = 1\}$. Entonces H es un subgrupo de G.

7. Si H y K son subgrupos de G entonces $H \cap K$ es un subgrupo de G.

Dado un grupo G y un elemento $x \in G$, consideremos el conjunto $(x) = \{x^n : n \in \mathbb{Z}\}$. Se trata de un subgrupo de G, que puede ser finito o no. Llamaremos *orden de* x, y se notará $o(x)$, al orden de este subgrupo. En caso de ser finito, $o(x) = \min\{n \in \mathbb{N} : x^n = 1\}$.

Ejemplo. Si $G = \mathbb{Z}_6$, $o(\overline{0}) = 1$, $o(\overline{1}) = 6$, $o(\overline{2}) = 3$, $o(\overline{3}) = 2$, $o(\overline{4}) = 3$ y $o(\overline{5}) = 6$.

Observación. Si $x \in G$ es tal que $o(x) = n$ y $t \in \mathbb{Z}$ es tal que $x^t = e_G$, entonces n divide a t. En particular, para todo $x \in G$, se tiene que $o(x) = o(x^{-1})$.

Definición 1.3.2. Dado un grupo G, se llama *exponente* de G al mínimo del siguiente conjunto $A = \{s \in \mathbb{N} : x^s = 1 \text{ si } x \in G\}$.

Ejemplo. Si $G = \mathbb{Z}$ este conjunto es vacío, así que el exponente es, por definición, igual a $+\infty$.

Proposición 1.3.3. *Sea G un grupo finito. Entonces el conjunto A es no vacío. Además, el exponente de G es el mínimo común múltiplo de los órdenes de los elementos de G.*

Demostración. Sea $x \in G$. Si t es tal que $x^t = e$ entonces $o(x) \mid t$. Supongamos que $t = o(g)m$ con $m \in \mathbb{Z}$. Entonces $x^t = x^{o(x)m} = e$. Vemos que $o(x) \mid t \iff x^t = e$. Como G es finito, todo elemento tiene orden finito, y como G tiene una cantidad finita de elementos, tiene sentido considerar al mínimo común múltiplo s de los órdenes $o(x)$ con $x \in G$.

Es $x^s = e$ para todo $x \in G$, así que A es no vacío y G tiene exponente finito. Además, si m es tal que $x^m = e$ para todo $x \in G$ entonces claramente s divide a m. Luego s es el exponente de G. $\square$

Observemos que si H es un subgrupo de un grupo G, entonces para cada $x \in G$ el conjunto

$$xHx^{-1} = \{xhx^{-1} : h \in H\}$$

es también un subgrupo de G: en efecto, es

$$(xhx^{-1})(xh'x^{-1}) = x(hh')x^{-1}$$

y

$$(xhx^{-1})^{-1} = xh^{-1}x^{-1}.$$

De esta manera, a partir de un subgrupo H obtenemos otros, que llamaremos *conjugados* a H. No hay razón *a priori* para suponer que H coincide con sus subgrupos conjugados, aunque esto sí es cierto si por ejemplo el grupo G es conmutativo o, más generalmente, si los elementos de H conmutan con los de G.

Ejemplo. Sea $G = S_n$ y sea $\sigma \in G$ la permutación cíclica definida por

$$\sigma(i) = \begin{cases} i+1, & \text{si } i < n; \\ 1, & \text{si } i = n. \end{cases}$$

Sea además $H = \{id, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$. H es un subgrupo de G, pero no es cierto, en general, que si $x \in G$ entonces $xHx^{-1} = H$ (¡dé un ejemplo de esto!).

Definición 1.3.4. Un subgrupo H de un grupo G es *invariante* (o también *normal* o *distinguido*) si $xHx^{-1} = H$ para todo $x \in G$. Escribiremos $H \lhd G$.

Observaciones.
1. Sea $\{H_i\}_{i \in I}$ una familia de subgrupos de un grupo G. Entonces $\bigcap_{i \in I} H_i$ es también un subgrupo de G. Si además todos los H_i son invariantes en G, entonces $\bigcap_{i \in I} H_i$ es invariante.

2. Si H es un subgrupo de un grupo G, mostrar que $\bigcap_{x \in G} xHx^{-1}$ es un subgrupo invariante.

3. Si S es un subconjunto de G, sea

$$N_S = \{x \in G : xSx^{-1} = S\}.$$

N_S es un subgrupo de G al que llamamos el *normalizador* de S en G. Por ejemplo, si $a \in G$ y $S = \{a\}$, entonces se tiene que $N_S = \{x \in G : xa = ax\}$.

Si S es un subgrupo de G, se puede ver que S es también un subgrupo de N_S y $S \lhd N_S$. Además N_S es el subgrupo de G más grande con esa propiedad.

4. Sea

$$Z_G = \{x \in G : xg = gx \text{ para tdo } g \in G\}.$$

Z_G es un subgrupo de G. Llamamos a Z_G el *centro* de G. Se tiene $Z_G \lhd G$ y, además, cualquiera sea $S \subseteq G$, es $Z_G \subseteq N_S$.

5. Si G es un grupo cualquiera y $x, y \in G$, el *conmutador de x e y* es el elemento

$$[x, y] = xyx^{-1}y^{-1}.$$

Dejamos como ejercicio verificar que si $z \in G$, entonces

$$z[x, y]z^{-1} = [zxz^{-1}, zyz^{-1}].$$

Llamamos *subgrupo conmutador* o *subgrupo derivado*, y lo escribimos $[G, G]$, al subgrupo de G generado por los conmutadores. Tenemos entonces que $[G, G] \lhd G$.

1.4 Morfismos y cocientes

Así como la noción de conjunto está intrínsecamente ligada al concepto de función, pues una función es una forma de relacionar un conjunto con otro, para el caso de grupos — que son conjuntos provistos de una estructura de producto adicional — serán de importancia central las funciones entre grupos que "respeten" dicha estructura.

Definición 1.4.1. Sean $(G, \cdot_G)$ y $(G', \cdot_{G'})$ dos grupos. Una función $f : G \to G'$ es un *morfismo* (o también un *homomorfismo*) de grupos si para todo $g_1, g_2 \in G$ se tiene que

$$f(g_1 \cdot_G g_2) = f(g_1) \cdot_{G'} f(g_2).$$

Ejercicio. Un subconjunto H de un grupo G es subgrupo si y sólo si H admite una estructura de grupo tal que la función inclusion $i : H \hookrightarrow G$ es un morfismo de grupos.

Definición 1.4.2. Un *monomorfismo* es un morfismo inyectivo. Un *epimorfismo* es un morfismo suryectivo. Un *isomorfismo* es un morfismo biyectivo.

Notemos que el conjunto de morfismos de grupos $f : G \to G'$, que escribiremos $\mathrm{Hom}_{Gr}(G, G')$, es siempre no vacío: la función que a todo elemento de G le asigna el neutro de G' es trivialmente un morfismo de grupos, al que llamamos el "morfismo nulo".

Observaciones.
1. Un morfismo $f : G \to G'$ es un isomorfismo sii es monomorfismo y epimorfismo. En tal caso, la función inversa $f^{-1} : G' \to G$ también es un morfismo de grupos (¡verificarlo!).

2. Si f es un morfismo, entonces $f(e_G) = e_{G'}$: como $e_G = e_G e_G$, es $f(e_G) = f(e_G)f(e_G)$, así que

$$e_{G'} = f(e_G)(f(e_G))^{-1} = f(e_G)f(e_G)(f(e_G))^{-1} = f(e_G).$$

3. Si $f : G \to G'$ es un morfismo, entonces para cada $g \in G$ es $f(g^{-1}) = f(g)^{-1}$.

4. Un morfismo f es un monomorfismo sii

$$f(g) = e_{G'} \implies g = e_G.$$

Definición 1.4.3. Sea $f : G \to G'$ un morfismo de grupos. El *núcleo* de f es el conjunto

$$\mathrm{Ker}(f) = \{g \in G : f(g) = e_{G'}\}$$

y la *imágen* de f es el conjunto

$$\mathrm{Im}(f) = \{g' \in G' : \text{existe } g \in G \text{ tal que } f(g) = g'\}.$$

Se trata de subgrupos de G y de G', respectivamente.

Ejercicios.
1. Verificar que efectivamente $\mathrm{Ker}(f)$ e $\mathrm{Im}(f)$ son subgrupos de G y de G'. Verificar además que $\mathrm{Ker}(f) \lhd G$. Mostrar con un ejemplo que $\mathrm{Im}(f)$ no tiene porque ser invariante.

2. Sea $f : G \to G'$ como antes un morfismo de grupos y H' un subgrupo de G'. Verificar que $f^{-1}(H')$ es un subgrupo de G. Si además $H' \lhd G'$, entonces $f^{-1}(H') \lhd G$. En particular, como es $\{e\} \lhd G'$ resulta $\mathrm{Ker}(f) \lhd G$.

Las definiciones de monomorfismo y epimorfismo pueden ser enunciadas a través de estos subgrupos: un morfismo $f : G \to G'$ es un monomorfismo si y sólo si $\mathrm{Ker}(f) = \{e_G\}$ y es un epimorfismo si y sólo si $\mathrm{Im}(f) = G'$.

Ejemplos.
1. La aplicación exponencial $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$, dada por $\exp(x) = e^x$ para todo $x \in \mathbb{R}$, es un isomorfismo de grupos, cuyo inverso es la función logaritmo.

2. Determinemos los morfismos de $\mathbb{Z}_2$ a $\mathbb{Z}_4$.

Sea $f : \mathbb{Z}_2 \to \mathbb{Z}_4$ un morfismo de grupos. Sabemos que $f(\overline{0}) = \overline{0}$. ¿Cuánto vale $f(\overline{1})$? Como $\overline{0} = \overline{1} + \overline{1}$ entonces $f(\overline{1}) + f(\overline{1}) = \overline{0}$. Esto nos dice que $f(\overline{1})$ debe ser o bien cero o bien la clase de 2 en $\mathbb{Z}_4$. En cualquiera de los dos casos, la función así definida es un morfismo de grupos.

3. Si $f : \mathbb{Z}_2 \to \mathbb{Z}_3$ es un morfismo de grupos, entonces f es el morfismo nulo. (¡Verifíquelo!)

4. La proyección canónica $\pi : \mathbb{Z} \to \mathbb{Z}_n$ es un morfismo de grupos.

5. Dados un cuerpo k y $n \in \mathbb{N}$, la aplicación $f : \mathrm{GL}_n(k) \to k - \{0\}$ tal que $f(A) = \det(A)$ es un morfismo de grupos.

6. Sea $f : G_n \to \mathbb{Z}_n$ dado por $f(e^{\frac{2\pi i k}{n}}) = \overline{k}$. Entonces f es un isomorfismo de grupos.

Ejercicio. Definir un morfismo de grupos $f : S_3 \to S_3$ tal que $\mathrm{Im}(f) \not\lhd S_3$.

Vimos que si $f : G \to G'$ es un morfismo de grupos, entonces $\mathrm{Ker}(f) \lhd G$. Sin embargo, esto no es cierto para $\mathrm{Im}(f)$, como puede verse en el siguiente ejemplo:

Ejemplo. Sean k un cuerpo, $n \in \mathbb{N}$ y $A \in \mathrm{GL}_n(k)$ una matriz no escalar. Sea $f_A : \mathbb{Z} \to \mathrm{GL}_n(k)$ el morfismo de grupos definido por $f_A(r) = A^r$. Entonces la imagen de f_A es el subgrupo de $\mathrm{GL}_n(k)$ generado por A, que no es invariante.

El siguiente lema muestra que todo subgrupo normal de G es el núcleo de algún morfismo de G en algún grupo G'.

Lema 1.4.4. *Sea $H \lhd G$. Entonces existe un grupo G' y un morfismo de grupos $f : G \to G'$ tal que $H = \mathrm{Ker}(f)$.*

Demostración. Definimos una relación de equivalencia $\sim_H$ sobre G.

Si $x, y \in G$, diremos que $x \sim_H y$ sii $y^{-1}x \in H$. Dejamos como ejercicio mostra que, como H es un subgrupo, esto define en efecto una relación de equivalencia; notemos que si $H = \{e\}$ esta relación es simplemente la igualdad.

Consideramos el conjunto cociente $G/\sim_H$ y la aplicación natural

$$\begin{aligned} \pi : G &\to G/\sim_H \\ x &\mapsto \overline{x} \end{aligned}$$

donde $\overline{x} = \{y \in G : x \sim_H y\}$ es la clase de equivalecia de x.

Ponemos $G' = G/\sim_H$ y definimos una operación sobre G' de manera que

$$\overline{x} * \overline{y} = \overline{xy}.$$

Además, tomamos $f = \pi : G \to G'$. Queremos ver que G' es un grupo, que f es un morfismo de grupos y que $\mathrm{Ker}(f) = H$.

- *La operación $*$ está bien definida.* Sean x, x', y y y' tales que $\overline{x} = \overline{x'}$ y $\overline{y} = \overline{y'}$. Entonces existen $h_1, h_2 \in H$ tales que

  $$(x')^{-1}x = h_1, \qquad (y')^{-1}y = h_2,$$

  o, equivalentemente,

  $$x = x'h_1, \qquad y = y'h_2.$$

  Queremos ver que $\overline{x'y'} = \overline{xy}$ y para eso calculamos xy en términos de x' e y':

  $$\begin{aligned} xy &= x'h_1y'h_2 = x'(y'y'^{-1})h_1y'h_2 = x'y'(y'^{-1}h_1y')h_2 \\ &= x'y'h_3h_2, \end{aligned}$$

donde $h_3 = y'^{-1}h_1y'$, que es un conjugado de h_1. Como H es un subgrupo *invariante*, es $h_3 \in H$ y entonces $h_3h_2 \in H$. Por lo tanto, $xy \sim_H x'y'$ y, finalmente, $\overline{xy} = \overline{x'y'}$.

Notemos que si H no es invariante, el razonamiento anterior no es válido y no hay en general manera de dar al cociente G' una estructura de grupo compatible con la de G.

- *La operación definida en G' da una estructura de grupo*, es decir es asociativa, hay un elemento neutro y todo elemento tiene inverso. Dejamos esto como ejercicio al lector.
- *f es un morfismo de grupos y* $\mathrm{Ker}(f) = H$. Que f es un morfismo de grupos es inmediato a partir de su definición pues

$$f(xy) = \overline{xy} = \overline{x} * \overline{y} = f(x)f(y)$$

Calculamos ahora $\mathrm{Ker}(f)$:

$$\begin{aligned}\mathrm{Ker}(f) &= \{x \in G : f(x) = e_{G'}\}\\ &= \{x \in G : \overline{x} = \overline{e}\}\\ &= \{x \in G : x \sim_H e\}\\ &= \{x \in G : x \in H\}\\ &= H\end{aligned}$$

Esto completa la prueba. □

Definición 1.4.5. Si G es un grupo y $H \lhd G$ un subgrupo invariante, escribiremos G/H al grupo G' construido en la prueba del lema y lo llamaremos el *grupo cociente de G por H* (o G módulo H).

Notemos que la estructura de grupo de G/H proviene del hecho de que $H \lhd G$. Cuando H no es invariante, el conjunto cociente G/H es tan sólo un conjunto.

Ejemplos.
1. Sea $m\mathbb{Z} \subset \mathbb{Z}$. Se trata de un subgrupo de $(\mathbb{Z}, +)$ y $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$.

2. Consideremos el grupo $(\mathbb{R}, +)$ y el subgrupo $\mathbb{Z} \subset \mathbb{R}$. Es $\mathbb{Z} \lhd \mathbb{R}$ porque $\mathbb{R}$ es abeliano. Se obtiene entonces que $\mathbb{R}/\mathbb{Z}$ es un grupo isomorfo a $(S^1, \cdot) = \{z \in \mathbb{C} : |z| = 1\} \subset (\mathbb{C} - \{0\}, \cdot)$ y la proyección canónica es la aplicación

$$\overline{x} \in \mathbb{R}/\mathbb{Z} \mapsto e^{2i\pi x} \in S^1$$

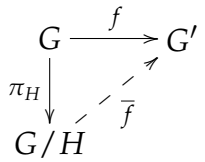
3. Si G es un grupo, entonces $G/\{e\} \cong G$ y $G/G \cong \{e\}$.

4. Sea $n \in \mathbb{N}$ y sea S_n el grupo de permutaciones de $\{1, \ldots, n\}$. Sea $i \in \{1, \ldots, n\}$ y sea H el subgrupo de S_n que consiste de las permutaciones que dejan fijo al elemento i. Entonces $S_n/H \cong S_{n-1}$.

Otra forma de describir al grupo cociente lo da la siguiente proposición, que presenta una propiedad de tipo universal que caracteriza completamente al cociente:

Proposición 1.4.6. *Sean G un grupo, $H \lhd G$ y sea $\pi_H : G \to G/H$ la proyección al cociente. Entonces para todo grupo G' y todo morfismo de grupos $f : G \to G'$ tal que $H \subseteq \mathrm{Ker}(f)$, existe un único morfismo de grupos $\overline{f} : G/H \to G'$ tal que $\overline{f} \circ \pi_H = f$.*

Esta situación se esquematiza con el siguiente diagrama:



Demostración. Mostremos separadamente la existenca y la unicidad.

Existencia. Si $\overline{x} \in G/H$, ponemos $\overline{f}(\overline{x}) = f(x)$. Esta aplicación está bien definida pues si $\overline{x} = \overline{x'}$, entonces ${x'}^{-1}x \in H \subseteq \mathrm{Ker}(f)$ y $f({x'}^{-1}x) = e'_G$. Esto implica que $f(x) = f(x')$.

Resulta claro también que $\overline{f}$ es un morfismo de grupos, pues

$$\overline{f}(\overline{xy}) = f(xy) = f(x)f(y) = \overline{f}(\overline{x})\overline{f}(\overline{y}).$$

Finalmente, la definición misma de $\overline{f}$ implica que $f = \overline{f} \circ \pi_H$.

Unicidad. La unicidad es una consecuencia de la sobreyectividad de π_H. Sean $\overline{f}_1, \overline{f}_2 : G/H \to G'$ morfismos de grupos tales que $\overline{f}_i \circ \pi = f$ para $i = 1, 2$. Entonces, si $\overline{x} \in G/H$, es

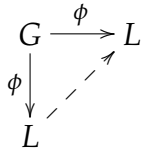
$$\overline{f}_1(\overline{x}) = \overline{f}_1(\pi(x)) = f(x) = \overline{f}_2(\pi(x)) = \overline{f}_2(\overline{x}),$$

así que $\overline{f}_1 = \overline{f}_2$. □

Observaciones.
1. Con las notaciones de la proposición anterior, $\mathrm{Im}(\overline{f}) = \mathrm{Im}(f)$ y $\mathrm{Ker}(\overline{f}) = \pi_H(\mathrm{Ker}(f))$. En particular si f es un epimorfismo, entonces $\overline{f}$ también lo es, y si $H = \mathrm{Ker}(f)$ entonces $\overline{f}$ es un monomorfismo.

2. Sea G un grupo y $H \subset G$ un subgrupo normal. Supongamos que tenemos un grupo L y un morfismo de grupos $\phi : G \to L$ tal que $\mathrm{Ker}(\phi) = H$ y tal que para todo morfismo $f : G \to G'$ con $H \subseteq \mathrm{Ker}(f)$ existe un único morfismo $\hat{f} : L \to G'$ para el cual se tiene que $\hat{f} \circ \phi = f$. Queremos ver que existe un isomorfismo de grupos $L \cong G/H$.

Como $\mathrm{Ker}(\phi) = H$, existe un único $\overline{\phi} : G/H \to L$ tal que $\overline{\phi} \circ \pi_H = \phi$. Sabemos que $\mathrm{Ker}(\overline{\phi}) = \pi_H(\mathrm{Ker}(\phi) = \pi_H(H) = \{e\}$, así que $\overline{\phi}$ es monomorfismo. Para ver que $\overline{\phi}$ es también un epimorfismo, vamos a construir un inverso. Por hipótesis, existe un único morfismo $\hat{\pi}_H : L \to G/H$ tal que $\hat{\pi}_H \circ \phi = \pi_H$. Para verificar que $\hat{\pi}_H$ y $\overline{\phi}$ son inversos, notamos que una un único morfismo que hace conmutar el siguiente diagrama:



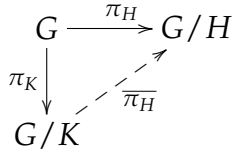
1.5 Teoremas de isomorfismo

Teorema 1.5.1. (Primer teorema de isomorfismo) *Sea $f : G \to G'$ es un morfismo de grupos, sea $H = \mathrm{Ker}(f)$ y consideremos la restricción $f : G \to \mathrm{Im}(f)$. Entonces $\overline{f} : G/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ es un isomorfismo de grupos.*

Demostración. Basta observar que $\overline{f}$ es mono y epi. □

Teorema 1.5.2. (Segundo teorema de isomorfismo) *Sea G un grupo y sean H y K dos subgrupos normales de G tales que $K \subseteq H$. Entonces*

$K \lhd H$ y se tiene el siguiente diagrama conmutativo:



El morfismo $\overline{\pi_H}$ induce un isomorfismo

$$\frac{G/K}{H/K} \cong G/H.$$

Demostración. El morfismo $\overline{\pi_H}$ es claramente sobreyectivo, pues π_H lo es, y el núcleo de $\overline{\pi_H}$ es la imagen de H por π_K en G/K, es decir, $\mathrm{Im}(\overline{\pi_H}) = H/K$. Aaplicando ahora el primer teorema de isomorfismo a π_H se tiene que $\frac{G/K}{H/K} \cong G/H$. □

Ejemplo. Si consideramos los grupos aditivos $\mathbb{Z} \subset \mathbb{R} \subset \mathbb{C}$, entonces

$$\frac{\mathbb{C}/\mathbb{Z}}{\mathbb{R}/\mathbb{Z}} \cong \mathbb{C}/\mathbb{R} \cong \mathbb{R}.$$

Teorema 1.5.3. (Tercer teorema de isomorfismo) *Sea G un grupo y sean H y K subgrupos de G tales que $K \subseteq N_H$, esto es, tales que para todo $k \in J$ es $kHk^{-1} = H$.*

Si $HK = \{hk : h \in H, k \in K\}$, entonces HK es un subgrupo de G y $H \lhd HK$. Además, el morfismo de grupos $k \in K \mapsto \overline{k} \in HK/H$ induce un isomorfismo $K/(H \cap K) \cong HK/H$.

Demostración. HK es un subgrupo de G porque, por un lado,

$$(hk)(h'k') = hkh'(k^{-1}k)k' = \big(h(kh'k^{-1})\big)kk' \in HK,$$

ya que $kh'k^{-1} \in H$ y, por otro,

$$(hk)^{-1} = k^{-1}h^{-1} = (k^{-1}h^{-1}k)k^{-1}.$$

Es fácil ver que $H \lhd HK$, así que tiene sentido calcular HK/H. La aplicación $k \in K \mapsto \overline{k} \in HK/H$ es un morfismo de grupos sobreyectivo (¡verificarlo!) y su núcleo es el conjunto de los elementos de K que también están en H. El primer teorema da entonces un isomorfismo $K/(H \cap K) \cong HK/H$. □

1.6 El teorema de Lagrange

Recordamos que el *orden* de un grupo G es el cardinal de G y se lo nota $|G| = \#G$.

Si H es un subgrupo (no necesariamente invariante) de G, podemos construir el conjunto cociente G/H de G por la relación de equivalencia $\sim_H$. Si $H \lhd G$, entonces G/H es un grupo.

Definición 1.6.1. Si G es un grupo y H un subgrupo de G, llamamos *índice de H en G* al cardinal del conjunto G/H y lo escribimos $(G : H) = \#(G/H)$.

Supongamos que tenemos un grupo finito G y un subgrupo H de G. La relación de equivalencia $\sim_H$ es tal que, para $x \in G$, se tiene:

$$\begin{aligned}\overline{x} &= \{y \in G : x \sim_H y\} \\ &= \{y \in G : y^{-1}x \in H\} \\ &= \{y \in G : y = xh \text{ para algún } h \in H\}\end{aligned}$$

Observamos que:

1. Por ser $\sim_H$ una relación de equivalencia, $\overline{x} \cap \overline{y} = \varnothing$ o $\overline{x} = \overline{y}$.
2. Para todo $x \in G$ se tiene que $\#(\overline{x}) = \#(xH) = |H|$.
3. $\#(G/H) = \#\{\overline{x} : x \in G\}$.

En estas condiciones, se tiene el siguiente teorema:

Teorema 1.6.2. (Lagrange) *Sean G un grupo finito y sea H un subgrupo de G, entonces $|G| = (G : H)|H|$.*

Demostración. Del hecho de que $\sim_H$ sea una relación de equivalencia se sigue que G es la unión disjunta de sus clases de equivalencia. Por lo tanto

$$|G| = \sum_{\overline{x} \in G/H} \#(\overline{x}).$$

Usando la observación 2 hecha arriba, vemos que todos los términos de esta suma son iguales a $|H|$ y entonces

$$|G| = \sum_{\overline{x} \in G/H} |H| = \#(G/H)|H| = (G : H)|H|.$$

Esto prueba el teorema. □

Este teorema tiene consecuencias inmediatas importantes:

Corolario 1.6.3. *Sea G un grupo finito:*

(a) El orden de cualquier subgrupo de G divide al orden de G.

(b) Si $H \lhd G$, entonces $|G/H| = \frac{|G|}{|H|}$.

(c) Si $a \in G$, notemos por $\langle a \rangle$ al subgrupo de G dado por el conjunto $\{a^n : n \in \mathbb{Z}\}$ y $|a| = |\langle a \rangle|$. Entonces $|a|$ divide a $|G|$. Observemos que $|a| = \min\{n \in \mathbb{N}_0 : a^n = e_G\}$.

(d) Para todo $x \in G$, $x^{|G|} = e_G$.

(e) (Fermat) *Si $a \in \mathbb{Z}$ y p es un número primo entonces*

$$a^p \equiv a \pmod{p}.$$

(f) Si $f : G \to G'$ es un morfismo de grupos y $a \in G$, entonces $|f(a)|$ divide a $|a|$.

(g) Si $|G|$ es un número primo p (por ejemplo, $G = \mathbb{Z}_p$) entonces los únicos subgrupos de G son los triviales: $\{e_G\}$ y G.

Demostración. Los puntos *(a)*, *(b)*, *(c)* y *(g)* son evidentes. Como

$$x^{|G|} = x^{|x|(G:\langle x \rangle)} = \left(x^{|x|}\right)^{(G:\langle x \rangle)},$$

la afirmación *(d)* se sigue de que $x^{|x|} = e_G$.

Veamos *(e)*. Si $a \equiv 0 \pmod{p}$ el resultado es obvio, así que basta probarlo para $\overline{a} \in (\mathbb{Z}_p - \{0\})$. Consideremos $G = \mathbb{Z}_p - \{0\}$, que es un grupo ara la multiplicación porque p es un número primo (¿por qué?). Usando el punto *(c)*, vemos que $|\overline{a}|$ divide a $|G| = p - 1$. Por lo tanto, $a^{p-1} \equiv 1 \pmod{p}$.

Finalmente, veamos el anteúltimo punto. Consideremos la restricción $f|_{\langle a \rangle} : \langle a \rangle \to G'$. Es claro que $\operatorname{Im}(f|_{\langle a \rangle}) = \langle f(a) \rangle$. El teorema de isomorfismo nos dice entonces que $\langle f(a) \rangle \cong \langle a \rangle / \operatorname{Ker}(f|_{\langle a \rangle})$, así que

$$|f(a)| = \frac{|a|}{|\operatorname{Ker}(f|_{\langle a \rangle})|}.$$

Esto termina la prueba. □

1.7 Grupos cíclicos

Sea G un grupo y $a \in G$ un elemento de G. Si $m \in \mathbb{Z}$, se define inductivamente

$$a^m = \begin{cases} e_G & \text{si } m = 0; \\ a & \text{si } m = 1; \\ a^{m-1}a & \text{si } m > 1; \\ (a^{-1})^{-m} & \text{si } m < 0. \end{cases}$$

Es claro que $a^r a^s = a^s a^r = a^{r+s}$, de manera que que la función $f_a : n \in \mathbb{Z} \mapsto a^n \in G$ es un morfismo de grupos.

Ejercicio. Mostrar que si $a, b \in G$ son tales que $ab = ba$ entonces $(ab)^m = a^m b^m$ para todo $m \in \mathbb{Z}$.

Definición 1.7.1. Un grupo G es *cíclico* si existe un elemento $a \in G$ tal que para todo $b \in G$ existe $m \in \mathbb{Z}$ con $a^m = b$. En otras palabras, G es cíclico si existe un $a \in G$ tal que $\langle a \rangle = G$. Todo tal elemento es un *generador* de G.

Observaciones.
1. Un grupo cíclico no tiene necesariamente un único generador. Por ejemplo, $G = \mathbb{Z}_5$ es un grupo cíclico y

$$\mathbb{Z}_5 = \langle \overline{1} \rangle = \langle \overline{2} \rangle = \langle \overline{3} \rangle = \langle \overline{4} \rangle.$$

2. Si G es un grupo, entonces cualquiera sea $a \in G$ se tiene que $|\langle a \rangle| = |a|$.

Ejercicio. Mostrar que $(\mathbb{Z}, +)$, $(G_n, \cdot)$ y $(\mathbb{Z}_n, +)$, con $n \in \mathbb{N}$ arbitrario, son grupos cíclicos. En cada caso encontrar *todos* los generadores.

Sabemos que G_n y $\mathbb{Z}_n$ son grupos isomorfos y que si $n \neq m$, entonces $\mathbb{Z}_n \ncong \mathbb{Z}_m$ (¿por qué?). Por otro lado, $\mathbb{Z}_n$ no es isomorfo a $\mathbb{Z}$ para ningún $n \in \mathbb{Z}$ (¿por qué?). ¿Puede existir un grupo cíclico no isomorfo a $(\mathbb{Z}, +)$ o a $(\mathbb{Z}_n, +)$? ¿Puede existir un grupo cíclico no conmutativo?

La respuesta a estas preguntas la da el siguiente teorema que caracteriza a todos los grupos cíclicos.

Teorema 1.7.2. *Sea G un grupo cíclico y sea $a \in G$ un generador, de manera que $G = \langle a \rangle$. Entonces:*

(a) Si $|a| = n$, entonces $G \cong (\mathbb{Z}_n, +)$.
(b) Si $|a| = \infty$, entonces $G \cong (\mathbb{Z}, +)$.

Demostración. Consideremos la función $f : m \in \mathbb{Z} \mapsto a^m \in G$. Como $a^{r+s} = a^r a^s$, f es un morfismo de grupos. Además, la imagen de f coincide con $\langle a \rangle = G$. El primer teorema de isomorfismo nos dice entonces que $G \cong \mathbb{Z}/\operatorname{Ker}(f)$.

Supongamos que $|a| = \infty$. Si $m \in \mathbb{Z}$ es tal que $f(m) = a^m = e_G$, debe ser $m = 0$. Esto es, $\operatorname{Ker}(f) = \{0\}$ y $G \cong \mathbb{Z}$.

Por otro lado, si $|a| = n < \infty$, es $\operatorname{Ker}(f) = n\mathbb{Z}$ (¿por qué?) y entonces $G \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. □

Corolario 1.7.3. *(a) Si G y G' son dos grupos cíclicos y $|G| = |G'|$, entonces $G \cong G'$.*
(b) Si $|G| = p$ con $p \in \mathbb{N}$ un número primo, entonces $G \cong \mathbb{Z}_p$.

Demostración. Para demostrar la segunda afirmación, basta ver que G es cíclico. Tomemos $a \in G$ un elemento cualquiera distinto de e_G y consideremos el subgrupo $\langle a \rangle$. El teorema de Lagrange nos dice que el orden de este subgrupo divide al orden de G, que es p, así que es o 1 o p. Pero debe ser $|\langle a \rangle| > 1$, ya que $\langle a \rangle$ contiene por lo menos a los elementos a y e_G. Concluimos que $\langle a \rangle = G$. □

1.8 Acción de un grupo sobre un conjunto

Como vimos en los primeros ejemplos, una de las formas de encontrar grupos es observando transformaciones de algún conjunto. De esta manera, a un grupo abstracto se lo piensa "actuando" sobre el espacio o conjunto en donde operan las transformaciones.

Definición 1.8.1. Sea G un grupo y X un conjunto. Se dice que G *opera a izquierda* (o que *actúa a izquierda*) sobre X si se tiene dada una función, llamada *acción*,

$$\begin{aligned} \phi : G \times X &\to X \\ (g, x) &\mapsto \phi(g, x) \end{aligned}$$

Habitualmente escribimos $g \cdot x$ o gx en vez de $\phi(g, x)$. Suponemos que ϕ satisface las siguientes condiciones:

- *Asociatividad:* para todo $x \in X$, g, $g' \in$, es

$$(g \cdot g') \cdot x = g \cdot (g' \cdot x).$$

  Nótese que aquí el punto entre g y g' indica la multiplicación en G mientras que el punto entre g' y x es la acción sobre X.
- *Identidad:* para todo $x \in X$, es

$$e_G \cdot x = x.$$

Si A, B y C son conjuntos, hay una biyección

$$\begin{aligned} \mathrm{Func}(A \times B, C) &= \mathrm{Func}(A, \mathrm{Func}(B, C)) \\ f(-,-) &\mapsto (a \mapsto f(a,-)) \end{aligned}$$

En otras palabras, si una función tiene dos variables, fijando una se obtiene una función de la otra.

Esto da otro punto de vista para describir las acciones de un grupo G sobre un conjunto X. Para cada g en G se tiene la función "multiplicación por g",

$$\phi_g = \phi(g,-) : x \in X \mapsto gx \in X$$

Las propiedades de la acción implican que $\phi_g \circ \phi_h = \phi_{gh}$ (¡verificarlo!). En particular, es

$$\phi_{g^{-1}} \circ \phi_g = \phi_g \circ \phi_{g^{-1}} = \phi_{e_G} = \mathsf{Id}_X.$$

Esto nos dice que ϕ_g es una función biyectiva, con inversa $\phi_{g^{-1}}$. Por lo tanto, dar una acción de G sobre X es lo mismo que dar una función $\rho : g \in G \to \phi_g \in S(X)$ de G al grupo de biyecciones de X en X. La propiedad de asociatividad de la acción no dice otra cosa que esta función es un morfismo de grupos, esto es, que

$$\rho(g) \circ \rho(g') = \rho(gg').$$

El par (X, ρ) se llama una *representación* de G en X. A partir del grupo abstracto G, se tiene una imagen de él como un subgrupo del grupo de permutaciones del conjunto X.

Ejemplos.
1. Sea $n \in \mathbb{N}$, $G = G_n$, y $X = \mathbb{R}^2$. Identificamos a $\mathcal{X}$ con $\mathbb{C}$. Definimos una acción de G sobre X poniendo

$$\begin{aligned} G_n \times \mathbb{C} &\to \mathbb{C} \\ (\omega, z) &\mapsto (\omega z) \end{aligned}$$

Notemos que la aplicación $z \in \mathbb{C} \mapsto \omega z \in \mathbb{C}$ es la rotación de $\mathbb{C}$ de ángulo $\arg(\omega)$. Así, en esta representación G_n se representa como rotaciones del plano.

2. Si $G = S_n$ es el grupo simétrico en n elementos y $X = \mathbb{R}^n$, consideramos la acción

$$\begin{aligned} S_n \times \mathbb{R}^n &\to \mathbb{R}^n \\ (\sigma, (x_1, ..., x_n)) &\mapsto (x_{\sigma(1)}, ...x_{\sigma(n)}) \end{aligned}$$

En este caso, cada $\sigma \in S_n$ actúa como una transformación lineal de $\mathbb{R}^n$, así que la acción es un morfismo $S_n \to \mathrm{GL}_n(\mathbb{R}) \subset S(\mathbb{R}^n)$.

3. La acción por *conjugación*, o acción por automorfismos interiores, de un grupo G sobre si mismo está dada por el morfismo de grupos $g \in G \mapsto \phi_g \in S(G)$ tal que

$$\begin{aligned} \phi_g : G &\to G \\ h &\mapsto ghg^{-1} \end{aligned}$$

Dejamos como ejercicio la verificación de que esto es en efecto una acción.

Como en el ejemplo anterior, esta acción respeta la estructura adicional que existe sobre el conjunto $X = G$, pues la acción tiene por imagen automorfismos de grupo de G:

$$\phi_g(hh') = g(hh')g^{-1} = (ghg^{-1})(gh'g^{-1}) = \phi_g(h)\phi_g(h').$$

La imagen de esta acción es un subgrupo del grupo $\mathrm{Aut}(G)$ de los automorfismos de grupo de G, al que llamamos *subgrupo de automorfismos interiores* y escribimos $\mathrm{Aut}_{\mathrm{int}}(G)$.

Si el grupo G es abeliano, el único automorfismo interior es la identidad. De hecho, se puede caracterizar a los automorfismos interiores en términos del grupo G y del centro de G, que de alguna manera mide la "abelianidad" de G:

Por el primer teorema de isomorfismo, se tiene que

$$\mathrm{Aut}_{\mathrm{int}}(G) \cong G/\ \mathrm{Ker}(\text{acción por conjugación}).$$

El núcleo de la acción por conjugación son los elementos de $g \in G$ tales que $\phi_g : h \in G \mapsto ghg^{-1} \in G$ es el automorfismo identidad de G. Pero

$$\phi_g = \mathrm{Id}_G \iff gxg^{-1} = x,\ \forall x \in G \iff gx = xg,\ \forall x \in G,$$

es decir, si y solo si $g \in \mathcal{Z}(G)$. Por lo tanto

$$\mathrm{Aut}_{\mathrm{int}}(G) \cong G/\mathcal{Z}(G).$$

4. G actúa por conjugación en el conjunto $\mathscr{P}(G) = \{X : X \subseteq G\}$ de partes de G. Definimos una acción $g \in G \mapsto \phi_g \in S(\mathscr{P}(G))$: si $A \in \mathscr{P}(G)$ y $g \in G$, ponemos

$$\phi_g(A) = gAg^{-1} = \{gag^{-1} : a \in A\} \in \mathscr{P}(A).$$

Notemos que esta acción puede restringese al subconjunto de $\mathscr{P}(G)$ de los subconjuntos de G que además son subgrupos de G. ¿Quiénes son los "puntos fijos" por la acción de G?

5. *Traslaciones en un grupo.* Sea $X = G$. Si $g \in G$, definimos una aplicación $T_g : G \to G$ por $T_g(h) = gh$; observemos que T_g *no* es un morfismo de grupos (¿por qué?). Esto da una acción de G sobre si mismo, que llamamos la acción por translación.

De manera similar, G actúa por traslaciones sobre $\mathscr{P}(G)$.

6. Sea $G = \mathbb{Z}_2$, $X = \mathbb{C}$, entonces la aplicación

$$\begin{aligned} &\mathbb{Z}_2 \to \mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) \\ &\ \overline{0} \mapsto \mathrm{Id}_{\mathbb{C}} \\ &\ \overline{1} \mapsto \text{conjugación} \end{aligned}$$

es una acción. El conjunto de puntos fijos por la acción de $\mathbb{Z}_2$ es exactamente el subgrupo de números reales.

7. Tener una acción de G sobre X es lo mismo que tener un morfismo $G \to S(X)$. Dados un grupo G y un conjunto X cualesquiera, siempre existe el morfismo nulo

$$\begin{aligned} &G \to \mathcal{S}(X) \\ &g \to \mathrm{Id}_X, \qquad \forall g \in G. \end{aligned}$$

Si G actúa de esta manera, diremos que G actúa trivialmente en X.

1.9 Orbitas, grupos de isotropía y ecuación de clases

Al actuar G sobre un conjunto X, pueden asociarse a esa acción diversos subgrupos de G y subconjuntos de X:

- Si $g \in G$, se puede considerar el subconjunto más grande de X sobre el que el elemento g actúa trivialmente, es decir, el conjunto $X^g = \{x \in X : gx = x\}$. Si, por ejemplo, G actúa sobre sí mismo por conjugación, este subconjunto es el centralizador de g en G; en cambio, si G actúa por traslaciones este conjunto es vacío.
- Inversamente, si $x \in X$, podemos considerar el subgrupo de G formado por los elementos que fijan a x, esto es, el conjunto $\mathcal{E}_x = \{g \in G : gx = x\}$, al que llamamos *estabilizador de x en G*.
- Sado un $x \in X$, también podemos considerar el conjunto de todos los elementos de X que son "accesibles" a través de G, al que llamamos la *órbita* de x. Esto dará el subconjunto de X más pequeño posible que contiene a x sobre el cual se puede definir una acción de G restringiendo la acción que se tenía sobre todo X. Más concretamente:

Definición 1.9.1. Sea G un grupo que actúa en un conjunto X y sea $x \in X$. La *órbita* de x en X es el conjunto

$$\mathcal{O}_x = \{gx : g \in G\} = \{y \in X : \text{existe } g \in G \text{ tal que } y = gx\}.$$

Ejemplos.
1. Sea $G = G_5$ actuando en $\mathbb{R}^2 = \mathbb{C}$ por rotaciones. Si $z = 0$ entonces $\mathcal{O}_z = \{0\}$. Si, en cambio, $z \neq 0$, entonces $\mathcal{O}_z$ contiene 5 elementos, que son los vértices del pentágono regular con centro en el origen y que tiene a z como uno de sus vértices.

2. Consideremos $\mathbb{Z}_2$ actuando en S^1 vía la acción tal que

$$\overline{0}(x) = x,$$
$$\overline{1}(x) = -x.$$

Entonces $\mathcal{O}_x = \{x, -x\}$. para todo $x \in S^1$.

3. Si G actúa sobre sí mismo por conjugación y $x \in G$, entonces $\mathcal{O}_x$ contiene sólo al elemento x sii el elemento x está en el centro de G.

4. Sea $G = G_4$ y consideremos la acción de G sobre el plano por rotaciones — i rota en 90 grados en el sentido contrario al movimiento de las agujas de *casi todos* los relojes. Sea X el conjunto de vértices de un cuadrado centrado en el origen en donde G actúa por rotaciones. La órbita de cualquier elemento de X coincide con X.

En general, cuando un grupo G actúa sobre un conjunto X de manera tal que existe un x con $\mathcal{O}_x = X$, la acción se llama *transitiva*. Observar que en ese caso $\mathcal{O}_y = X$ para todo $y \in X$.

Observación. Si G actúa sobre un conjunto X, las órbitas dan una partición de X. Más precisamente:

- $\mathcal{O}_x \cap \mathcal{O}_y = \varnothing$ o bien $\mathcal{O}_x = \mathcal{O}_y$.
- $\bigcup_{x \in X} \mathcal{O}_x = X$ (pues $x \in \mathcal{O}_x \ \forall x \in X$).

Esto nos dice que si definimos una relación $\sim$ en X poniendo

$$x \sim y \iff x \in \mathcal{O}_y$$

entonces $\sim$ resulta una relación de equivalencia.

Si un grupo G opera en X y $x \in X$, se llama *subgrupo estabilizador* o *grupo de isotropía* de x al subgrupo

$$\mathcal{E}_x = \{g \in G : gx = x\}$$

(¡verifique que se trata de un subgrupo!). Notemos que el "tamaño" de este subgrupo $\mathcal{E}_x$ de alguna manera se contrapone al "tamaño" de la órbita del elemento x: si hay muchos elementos que actúan trivialmente sobre x, entonces la órbita de este elemento es pequeña y su grupo de isotropía es grande. Recíprocamente, si la órbita de un elemento x es enorme, eso significa que hay "pocos" elementos que fijan a x.

La siguiente proposición formaliza esta idea intuitiva:

Proposición 1.9.2. *Sea G un grupo que opera sobre un conjunto X y sea $x \in X$. Entonces $\#\mathcal{O}_x = (G : \mathcal{E}_x)$.*

Demostración. Si $g\mathcal{E}_x = g'\mathcal{E}_x$, entonces $g = g'h$ para algún $h \in \mathcal{E}_x$, así que $gx = g'hx = g'x$. Esto nos dice que la función

$$g\mathcal{E}_x \in G/\mathcal{E}_x \mapsto gx \in \mathcal{O}_x$$

esta bien definida. Claramente es suryectiva. Por otro lado, si es $gx = g'x$, entonces $(g')^{-1}gx = x$ y $(g')^{-1}g \in \mathcal{E}_x$. Esto implica que $g\mathcal{E}_x = g'\mathcal{E}_x$ y hemos mostrado que nuestra aplicación es inyectiva. Luego $G/\mathcal{E}_x$ y $\mathcal{O}_x$ tienen la misma cantidad de elementos. □

Corolario 1.9.3. *Sea G un grupo finito que actúa sobre un conjunto X. Entonces $\#\mathcal{O}_x = \frac{|G|}{|\mathcal{E}_x|}$. En particular $\#\mathcal{O}_x$ es finito y divide al orden de G.*

Ejemplos.
1. Un grupo G actúa por conjugación sobre el conjunto de subgrupos de G. Si $H \subset G$ es un subgrupo, entonces la órbita de H está formada por los subgrupos conjugados a H y el estabilizador de H es el *normalizador* N_H de H en G, esto es, el mayor subgrupo de G tal que $H \lhd N_H$

2. Si G actúa sobre si mismo por conjugación y $x \in G$, entonces el estabilizador $\mathcal{E}_x = N_{\langle x \rangle}$ es el subgrupo de los elementos que conmutan con x. Se suele llamar a este grupo el *centralizador* de x y se lo nota $\mathcal{Z}(x)$.

3. Sea V un k-espacio vectorial. Sea $G = k - \{0\}$ es el grupo multiplicativo de k y $X = V - \{0\}$. Entonces G actúa en X vía la acción

$$\begin{aligned} G \times X &\to X \\ (\lambda, v) &\mapsto \lambda v \end{aligned}$$

Entonces $\mathcal{O}_v = \langle v \rangle - \{0\}$.

4. Sea X un conjunto y $G = \mathcal{S}(X)$ el grupo de las funciones biyectivas de X en X. Entonces G opera naturalmente sobre X por la fórmula

$$\begin{aligned} G \times X &\to X \\ (f, x) &\mapsto f(x) \end{aligned}$$

En este caso, es fácil ver que G opera transitivamente sobre X (¡hágalo!). Si $x \in X$, entonces $\mathcal{E}_x = \{f \in S(X) : f(x) = x\}$ se identifica con $\mathcal{S}(X - \{x\})$.

5. Si G actúa sobre si mismo por conjugación y s, $t \in G$, entonces $\mathcal{O}_s = \mathcal{O}_t$ si y sólo si s y t son conjugados. En ese caso, $\mathcal{E}_s$ es un subgrupo conjugado a $\mathcal{E}_t$ (¡verificarlo!) y, por lo tanto, isomorfo. En particular, se tiene que $|\mathcal{E}_s| = |\mathcal{E}_t|$

Aplicando la proposición anterior a un caso particular obtenemos el siguiente resultado:

Proposición 1.9.4. *Sea G un grupo y consideremos la acción de G sobre si mismo por conjugación. Sea $s \in G$. Entonces existe una biyección*

$$\begin{aligned} f : G/\mathcal{E}_s &\to \mathcal{O}_s \\ \overline{x} &\mapsto x.s.x^{-1} \end{aligned}$$

En particular, $\#(\mathcal{O}_s) = (G : \mathcal{E}_s)$.

Corolario 1.9.5. *El cardinal de toda órbita de G actuando sobre si mismo por conjugación, esto es, de cada clase de conjugación, divide al orden del grupo.*

Terminamos este capítulo con un resultado de demostración trivial a partir de la noción de acción, pero que es de gran ayuda en la teoría de grupos finitos: la llamada "ecuación de clases". Esta ecuación proviene esencialmente de partir a un grupo en órbitas bajo la acción por conjugación y contar los cardinales de cada parte:

Teorema 1.9.6. (Ecuación de clases) *Sea G un grupo finito actuando por conjugación sobre sí mismo. Entonces existe $\{a_1, ..., a_k\} \subset G$ tal que ningun a_i está en el centro de G y*

$$G = \mathcal{Z}(G) \coprod (\coprod_{i=1}^{k} \mathcal{O}_{a_i})$$

Luego

$$|G| = |\mathcal{Z}(G)| + \sum_{i=1}^{k} (G : \mathcal{Z}(a_i))$$

En particular, $\mathcal{Z}(a_i) \neq G$ cualquiera sea i y por lo tanto $(G : \mathcal{Z}(a_i)) \neq 1$.

Demostración. Como la acción define una relación de equivalencia sobre G, G es la unión disjunta de las clases de equivalencia, que en este caso son las órbitas. Las órbitas que tienen un único elemento corresponden a los elementos del centro de G. Eligiendo un a_i por cada órbita con más de un elemento, vemos que vale la primera ecuación del enunciado. Tomando ahora cardinales, porque la unión es disjunta y porque los ordenes de las órbitas coinciden con los índices de los estabilizadores de los a_i, obtenemos la segunda ecuación. □

Corolario 1.9.7. (Cauchy) *Sea G un grupo finito y sea p un número primo que divide al orden de G. Entonces existe un elemento en G de orden p.*

Demostración. La demostración se obtiene considerando primero el caso abeliano y después el caso no abeliano. En el primer caso no se usa la ecuación de clases y el segundo es una consecuencia del anterior más la ecuación de clases.

- *Primer caso: G abeliano.* Procedemos por inducción en el orden de G. Sea $a \in G$ un elemento cualquiera distinto del neutro. Si $|a|$ es un múltiplo de p, digamos $|a| = kp$, entonces el elemento a^k tiene orden p.

  Si, por el contrario, $|a|$ no es múltiplo de p, entonces consideramos el grupo $G/\langle a\rangle$; como G es abeliano, el subgrupo $\langle a\rangle$ es invariante, así que esto tiene sentido. Como $|a|$ no es un múltiplo de p, p divide a $|G/\langle a\rangle|$, que es un grupo de orden estrictamente menor que $|G|$ (porque $a \neq e_G$) y podemos aplicar la hipótesis inductiva al grupo cociente. Existe entonces $\overline{z} \in G/\langle a\rangle$ tal que $|\overline{z}| = p$. Pero esto implica que $|z|$ es un múltiplo de p y se procede como al principio.
- *Segundo caso: G no abeliano.* Si p divide al orden del centro de G, consideramos el subgrupo $\mathcal{Z}(G)$, que es conmutativo y que está, por lo tanto, en el caso anterior. Podemos suponer entonces que p no divide al orden de $\mathcal{Z}(G)$.

  Utilizando la ecuación de clases, vemos que existen elementos no centrales $a_1, \ldots, a_k \in G$ tales que:

$$|G| = |\mathcal{Z}(G)| + \sum_{i=1}^{k} (G : \mathcal{Z}(a_i)).$$

  El hecho de que p no divida a $|\mathcal{Z}(G)|$ y sí a $|G|$ implica que debe existir por lo menos alguno de los a_i tal que p no divide a $(G : \mathcal{Z}(a_i))$. Como $(G : \mathcal{Z}(a_i)) = |G|/|\mathcal{Z}(a_i)|$, $|\mathcal{Z}(a_i)|$ es un múltiplo de p. Considerando ahora el grupo $\mathcal{Z}(a_i)$, que, como es un subgrupo propio, tiene orden estrictamente menor al de G, y la hipótesis inductiva, vemos que $\mathcal{Z}(a_i)$ contiene un elemento de orden p. Esto prueba el corolario en este caso. □

Corolario 1.9.8. *Sea G un grupo finito de orden n. Entonces $n = p^r$ para algún número primo p si y sólo si todo elemento de G tiene orden igual a una potencia de p.*

La estructura de los grupos finitos conmutativos está completamente estudiada y clasificada, como se verá más adelante dentro del marco de la teoría de módulos sobre un tipo particular de anillos. Lo mismo vale para grupos conmutativos infinitos pero con una cantidad finita de generadores. Si no hay finitos generadores el problema no está completamente resuelto.

Si el grupo no es necesariamente conmutativo, diversos resultados relacionan propiedades aritméticas del orden con la estructura del grupo. Entre esos resultados cabe destacar los teoremas de Sylow (que usan exclusivamente la ecuación de clases), resultados de Burnside, Frobenius, Feit–Thompson, etc. Para los teoremas de Sylow, se propone al lector interesado que los demuestre por su cuenta guiándose por los ejercicios al final de la lista.

1.10 Ejercicios

Definiciones

1.10.1. *Exponentes pequeños.* El *exponente* de un grupo G es el menor número e tal que para todo $g \in G$ se tiene $g^e = 1$.

(a) Mostrar que un grupo G tal que $g^2 = 1$ para todo $g \in G$ es abeliano.

†*(b)* ¿Qué puede decir si se tiene en cambio que $g^3 = 1$?

1.10.2. Encontrar todos los grupos de orden a lo sumo 6.

†**1.10.3.** Mostrar que los tres axiomas de grupo—la asociatividad, la existencia de elemento neutro y la existencia de inversos—son independientes.

Ejemplos

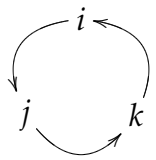
1.10.4. *(a)* Sea $n \in \mathbb{N}$ y sea $\mathbb{G}_n = \{z \in \mathbb{C} : z^n = 1\}$. Mostrar que $\mathbb{G}_n$, con respecto al producto de $\mathbb{C}$ es un grupo abeliano cíclico.

(b) Sea $S^1 = \{z \in \mathbb{C} : |z| = 1\}$. Mostrar que S^1, con respecto al producto de $\mathbb{C}$, es un grupo abeliano. ¿Es cíclico?

1.10.5. Sea $\mathbb{H}$ el conjunto de 8 elementos $\{\pm 1, \pm i, \pm j, \pm k\}$ dotado del producto dado por la siguiente ecuaciones:

$$\begin{aligned} &i \cdot j = k, \quad j \cdot k = i, \quad k \cdot i = j, \\ &j \cdot i = -k, \quad k \cdot j = -i, \quad i \cdot k = -j, \\ &i \cdot i = j \cdot j = k \cdot k = -1, \end{aligned}$$

y la regla usual de los signos. Mostrar que $(\mathbb{H}, \cdot)$ es un grupo no abeliano. Llamamos a $\mathbb{H}$ el *grupo de cuaterniones*. El siguiente diagrama permite recordar la tabla de multiplicación de $\mathbb{H}$.



1.10.6. Sea k un cuerpo y $n \in \mathbb{N}$. Ponemos

$$\mathrm{GL}_n(k) = \{A \in M_n(k) : \det A \neq 0\}$$

y

$$\mathrm{SL}_n(k) = \{A \in M_n(k) : \det A = 1\}.$$

Mostrar que, dotados de la multiplicación usual de matrices, estos dos conjuntos resultan ser grupos. Descríbalos para $n = 1$. ¿Cuándo son abelianos?

1.10.7. *Grupo opuesto.* Sea G un grupo. Sea $(G^{\mathrm{op}}, \cdot)$ tal que $G^{\mathrm{op}} = G$ como conjunto, y el producto es

$$\cdot : (g, h) \in G^{\mathrm{op}} \times G^{\mathrm{op}} \mapsto hg \in G^{\mathrm{op}}.$$

Mostrar que $(G^{\mathrm{op}}, \cdot)$ es un grupo.

1.10.8. Sea G uno grupo y X un conjunto.

(a) Consideremos el conjunto $G^X = \{f : X \to G\}$ dotado del producto $\cdot : G^X \times G^X \to G^X$ dado por

$$(f \cdot g)(x) = f(x)g(x), \qquad \forall f, g \in G^X, \forall x \in X.$$

Mostrar que G^X es un grupo. ¿Cuándo es abeliano?

(b) Sea $x_0 \in X$ y sea $H_{x_0} = \{f \in G^X : f(x_0) = 1\}$. Mostrar que H_{x_0} es un subgrupo de G. ¿Es normal?

1.10.9. *Producto directo.* Sean G y H dos grupos. Consideremos la operación $\cdot$ sobre el conjunto $K = G \times H$ dada por

$$\cdot : \big((g_1, h_1), (g_2, h_2)\big) \in K \times K \mapsto (g_1 g_2, h_1 h_2) \in K.$$

Mostrar que K es un grupo. Llamamos a K el *producto directo de G y H* y lo notamos $G \times H$.

1.10.10. *$\mathbb{F}_p$-espacios vectoriales.*

(a) Sea G un grupo abeliano y sea p un número primo. Supongamos que todo elemento de G tiene order p. Mostrar que es posible definir una multiplicación $\cdot : \mathbb{F}_p \times G \to G$ por escalares de $\mathbb{F}_p$ de manera que $(G, +, \cdot)$ resulte un $\mathbb{F}_p$-espacio vectorial.

(b) Supongamos además que G es finito. Mostrar que existe $n \in \mathbb{N}_0$ tal que

$$G \cong \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n \text{ veces}}.$$

Subgrupos

1.10.11. Sea G un grupo y $H \subset G$ un subconjunto. Mostrar que las siguientes afirmaciones son equivalentes:

(i) H es un subgrupo de G.

(ii) H es no vacío y cualesquiera sean $x, y \in H$, es $xy^{-1} \in H$.

Si además G es finito, estas afirmaciones son equivalentes a:

(iii) H es no vacío y cualesquiera sean $x, y \in H$, es $xy \in H$.

Dar un contraejemplo para esta última equivalencia cuando G es infinito.

1.10.12. Sea G un grupo y H_1 y H_2 subgrupos de G.

(a) $H_1 \cap H_2$ es un subgrupo de G.

(b) $H_1 \cup H_2$ es un subgrupo de G sii $H_1 \subset H_2$ o $H_2 \subset H_1$.

1.10.13. Dado un grupo G, ¿el subconjunto de elementos de orden finito es un subgrupo de G?

1.10.14. Sea G un grupo.

(a) Sea $\mathcal{H}$ una familia de subgrupos de G. Mostrar que $\bigcap_{H \in \mathcal{H}} H$ es un subgrupo de G.

(b) Sea ahora $X \subset G$ un subconjunto arbitrario. Mostrar que existe un menor subgrupo de G que contiene a X. Describirlo en término de los elementos de X.

El subgrupo cuya existencia se afirma en la segunda parte de este ejercicio se denomina el *subgrupo de G generado por X* y se denota $\langle X \rangle$. Si $X = \{x_1, \ldots, x_r\}$, escribimos $\langle x_1, \ldots, x_r \rangle$ en lugar de $\langle \{x_1, \ldots, x_n\} \rangle$.

1.10.15. Sea G un grupo, $X \subset X$ un subconjunto tal que $G = \langle X \rangle$. Mostrar que un subgrupo N de G es normal en G sii $xNx^{-1} \subset N$ para todo $x \in X$.

1.10.16. Sea $n \in \mathbb{N}$ y sea $\omega \in \mathbb{G}_{2^n}$ una raíz primitiva 2^n-ésima. Consideremos las matrices

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

y sea $\mathbb{H}_n = \langle R, S \rangle$ el subgrupo generado por R y S en $\mathrm{GL}_2(\mathbb{C})$. Llamamos a $\mathbb{H}_n$ el *n-ésimo grupo de cuaterniones generalizados*.

Determinar el orden de $\mathbb{H}_n$ y listar sus elementos.

1.10.17. *(a)* Sea $G = \mathrm{GL}_2(\mathbb{Z})$ y sean $\alpha, \beta \in G$ dados por

$$\alpha = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad \beta = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Muestre que $\alpha^4 = \beta^3$, pero que $\alpha\beta$ tiene orden infinito. En particular, el subgrupo $\langle \alpha, \beta \rangle$ es infinito.

Este ejemplo muestra que finitos elementos de orden finito pueden generar un subgrupo infinito.

(b) Determine $\langle \alpha, \beta \rangle$.

1.10.18. *Generación de S_n.*

(a) Mostrar que

(i) $S_n = \langle \{(i\,j) : 1 \leq i < j \leq n\} \rangle$;

(ii) $S_n = \langle \{(1\,i) : 1 \leq i \leq n\} \rangle$;

(iii) $S_n = \langle \{(i \;\; i+1) : 1 \leq i < n\} \rangle$;

(iv) $S_n = \langle (1\,2),\ (1\,2\,3\ldots n) \rangle$;

†*(b)* Sea $\mathcal{T} = \{(i\,j) : 1 \leq i < j \leq n\}$ el conjunto de todas las transposiciones. Encuentre una condición necesaria y suficiente para que un subconjunto $T \subset \mathcal{T}$ para que $S_n = \langle T \rangle$.

1.10.19. Sea G un grupo.

(a) Sea $\mathcal{H}$ una familia de subgrupos normales de G. Mostrar que $\bigcap_{H\in\mathcal{H}} H$ es un subgrupo normal de G.

(b) Sea $X \subset G$ un subconjunto arbitrario. Mostrar que existe un menor subgrupo normal de G que contiene a X. Describirlo en término de los elementos de X.

El subgrupo cuya existencia se afirma en la segunda parte de este ejercicio se denomina el *subgrupo normal de G generado por X*. En general, este subgrupo no coincide con el subgrupo generado por X, construido en **1.10.14**.

(d) Supongamos que $X \subset G$ es un conjunto tal que, cualquiera sea $g \in G$, es $gXg^{-1} \subset X$. Mostrar que entonces el subgrupo normal generado por X coincide con el subgrupo generado por X.

1.10.20. *(a)* Sea G un grupo y sea $N \subset G$ un subgrupo tal que $gNg^{-1} \subset N$ para todo $g \in G$. Muestre que N es normal.

(b) Sea $G = \mathrm{GL}_2(\mathbb{Q})$ y $H = \{\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) : n \in \mathbb{Z}\} \subset G$. Entonces H es un subgrupo de G. Sea ahora $g = \left(\begin{smallmatrix} 5 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in G$. Muestre que $gHg^{-1} \subsetneq H$.

1.10.21. Si G es un grupo y $A, B \subset G$ son subconjuntos, definimos

$$AB = \{ab : a \in A, b \in B\}.$$

Consideremos un grupo G y $A, B \subset G$ dos subconjuntos arbitrarios.

(a) AB es un subgrupo de G sii $AB = BA$.

(b) $G = AB$ sii $G = \langle A, B\rangle$ y $AB = BA$.

(c) Si $AB = BA$ y $C \subset G$ es un subgrupo tal que $A \subset C$, entonces $AB \cap C = A(B \cap C)$.

(d) Si $G = AB$ y $C \subset G$ es un subgrupo tal que $A \subset C$, entonces $C = A(B \cap C)$.

1.10.22. Sea G un grupo. Si $a, b \in G$, escribimos $[a, b] = aba^{-1}b^{-1}$; $[a, b]$ es el *conmutador de a y b*. Claramente $[a, b] = 1$ sii a y b conmutan, así que en cierta forma $[a, b]$ mide la no-conmutatividad de a y b.

(a) Sea $X = \{[a, b] : a, b \in G\}$ y sea $G' = \langle X\rangle$ el subgrupo generado por X en G. Mostrar que G' es normal en G. Llamamos a G' el *subgrupo derivado de G* y lo escribimos $[G, G]$.

(b) G es abeliano sii $[G, G] = 1$.

(c) Determinar $[G, G]$ cuando G es $\mathbb{H}$ o un grupo diedral D_n.

Definición. Un grupo es *perfecto* si coincide con su subgrupo derivado.

†*(d)* Sea k un cuerpo finito. Mostrar que $[\mathrm{GL}_n(k), \mathrm{GL}_n(k)] = \mathrm{SL}_n(k)$ con la excepción de $\mathrm{GL}_2(\mathbb{F}_2)$. Mostrar que $\mathrm{SL}_n(k)$ es perfecto con la excepción de $\mathrm{SL}_2(\mathbb{F}_2)$ y $\mathrm{SL}_2(\mathbb{F}_3)$. ¿Qué sucede en los casos excepcionales?

1.10.23. *(a)* Sea G un grupo y sea

$$\mathcal{Z}(G) = \{g \in G : gh = hg \text{ para todo } h \in G\}.$$

Mostrar que $\mathcal{Z}(G)$ es un subgrupo normal de G. Llamamos a $\mathcal{Z}(G)$ el *centro de* G y decimos que los elementos de $\mathcal{Z}(G)$ son *centrales* en G.

(b) Sea G un grupo y $X \subset G$ un subconjunto tal que $G = \langle X \rangle$. Mostrar que es

$$\mathcal{Z}(G) = \{g \in G : gx = gx \text{ para todo } x \in X\}.$$

(c) Encontrar el centro de un grupo abeliano, de D_n para cada $n \geq 1$, de $\mathbb{H}$, de S_n para cada $n \geq 1$, de $\mathrm{GL}_n(R)$ para cada $n \geq 1$ y $R \in \{\mathbb{R}, \mathbb{Z}, \mathbb{C}, \mathbb{F}_p\}$.

(d) Sea G un grupo y X un conjunto. Determinar el centro de G^X.

1.10.24. Calcular el centro del grupo de Hamilton.

1.10.25. Sea G un grupo y H un subgrupo abeliano de G. Mostrar que $H\mathcal{Z}(G)$ es un subgrupo abeliano de G.

1.10.26. Sea G un grupo.

(a) Sea $g \in G$. El *centralizador de g en G* es el subconjunto

$$\mathcal{C}(g) = \{h \in G : gh = hg\}.$$

Mostrar que se trata de un subgrupo de G y que es, en efecto, el subgrupo más grande de G que contiene a g y en el que g es central.

(b) Sea $N \subset G$ un subconjunto. El *centralizador de N en G* es el subconjunto $\mathcal{C}(N) = \{h \in G : nh = hn \text{ para cada } n \in N\}$. Mostrar que se trata de un subgrupo de G.

(c) Mueste que si $N \subset G$ es un subconjunto, $\mathcal{C}(\langle N \rangle) = \mathcal{C}(N)$.

(d) Sea $H \subset G$ un subgrupo de G. El *normalizador de H en G* es el subconjunto $\mathcal{N}(H) = \{g \in G : gH = Hg\}$. Mostrar que se trata de un subgrupo de G. Mostrar, más aún, que H es un subgrupo normal de $\mathcal{N}(H)$.

(e) Si $N \subset G$ es un subconjunto normal (es decir, si para cada $g \in G$, gNg^{-1}), entonces $\mathcal{Z}(N)$ es un subgrupo normal de G.

1.10.27. Si $g = (i_1\, i_2 \cdots i_{k-1}\, i_k) \in S_n$ es un ciclo de orden k, determinar $\mathcal{C}(g)$.

1.10.28. Calcular el centralizador de $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}_3)$ en $\mathrm{SL}_2(\mathbb{Z}_3)$ y en $\mathrm{GL}_2(\mathbb{Z}_3)$.

1.10.29. Calcular el orden de $\mathrm{SL}_2(\mathbb{Z}_3)$. Sugerencia: para hacer cuentas, escribir a $\mathbb{Z}_3$ como $\{\overline{0}, \overline{1}, \overline{-1}\}$). Describir el centro y encontrar las clases de conjugación.

1.10.30. Sea G un grupo y S y T subconjuntos de G tales que $S \subset T$. Entonces:

(a) $\mathcal{C}(S) \supset \mathcal{C}(T)$;

(b) $\mathcal{C}(\mathcal{C}(S)) \supset S$; y

(c) $\mathcal{C}(\mathcal{C}(\mathcal{C}(S))) = \mathcal{C}(s)$.

1.10.31. Sea G un grupo y $g \in G$. Entonces:

(a) $g \in \mathcal{C}(g)$;

(b) $\mathcal{C}(\mathcal{C}(g)) = \mathcal{Z}(\mathcal{C}(g))$;

(c) $\mathcal{C}(g) \subset \mathcal{C}(h)$ sii $h \in \mathcal{Z}(\mathcal{C}(g))$; y

(d) $\mathcal{C}(g) \subset \mathcal{C}(h)$ sii $\mathcal{Z}(\mathcal{C}(g)) \supset \mathcal{Z}(\mathcal{C}(h))$.

1.10.32. Sean G un grupo y H y K subgrupos de G.

(a) Si alguno de H o K es normal en G entonces HK es un subgrupo.

(b) Si los dos son normales, entonces $HK = KH$ y se trata de un subgrupo normal de G.

1.10.33. Sea G un grupo y N un subgrupo normal de G. Mostrar que $[N, G] \subset N$.

†**1.10.34.** El objetivo de este ejercicio es dar un ejemplo de que la normalidad de subgrupos no es transitiva.

(a) Sea G el conjunto de todas las funciones $f : \mathbb{R}^2 \to \mathbb{R}^2$ que pueden escribirse en la forma

$$f\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by + e \\ cx + dy + f \end{pmatrix}$$

para ciertos $a, b, c, d, e, f \in \mathbb{R}$ con $ad - bc \neq 0$. Mostrar que G, con respecto a la composición de funciones, es un grupo.

(b) Sea T el subconjunto de G formado por todas las funciones $f : \mathbb{R}^2 \to \mathbb{R}^2$ que pueden escribirse en la forma

$$f\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + e \\ y + f \end{pmatrix}$$

para ciertos $e, f \in \mathbb{R}$. Mostrar que T es un subgrupo *normal* en G.

(c) Sea L el subconjunto de T de las funciones $f : \mathbb{R}^2 \to \mathbb{R}^2$ que pueden escribirse en la forma

$$f\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + e \\ y + f \end{pmatrix}$$

para ciertos $e, f \in \mathbb{Z}$. Mostrar que se trata de un subgrupo de T; como T es abeliano, L es normal en T.

(d) Mostrar que L no es normal en G.

1.10.35. Encontrar todos los subgrupos de D_4. Clasifíquelos bajo isomorfismo y determinar cuáles son normales.

1.10.36. Sea $\mathbb{H}$ el grupo de los cuaterniones. Mostrar que posee un único elemento de orden 2 y que éste es central. Deducir de esto que $H \ncong D_4$ y que todo subgrupo de H es normal.

Un grupo no abeliano con esta propiedad se dice *Hamiltoniano*. El siguente teorema de Reinhold Baer (1902–1979) describe completamente esta clase de grupos:

Teorema. (R. Baer, Situation der Untergruppen und Struktur der Gruppe, S. B. Heidelberg. Akad. Wiss. 2 (1933), 12-17) *Un grupo finito es hamiltoniano sii es isomorfo a* $\mathbb{H} \times A$ *para algún grupo abeliano que no tiene elementos de orden* 4.

1.10.37. Sea G un grupo y N un subgrupo normal de G de índice finito n. Mostrar que si $g \in G$, entonces $g^n \in N$. Dar un ejemplo para mostrar que esto puede ser falso si N no es normal.

1.10.38. *(a)* Mostrar que un grupo no trivial sin subgrupos propios es cíclico de orden primo.

(b) Sea G un grupo cíclico y $g \in G$ un generador. Sea $n = |G|$ y sea p un número primo tal que $p \mid n$. Entonces $\langle g^p \rangle$ es un subgrupo maximal de G.

(c) Mostrar que un grupo finito que posee un solo subgrupo maximal es cíclico que tiene como orden una potencia de un número primo.

†**1.10.39.** Sea G un grupo finito y H el subgrupo de G generado por los elementos de orden impar. Entonces H es normal y tiene índice una potencia de 2.

†**1.10.40.** *Subgrupo de Frattini.* Sea G un grupo. Sea $\mathcal{M}$ el conjunto de subgrupos propios maximales de G. Si $\mathcal{M} \neq \varnothing$, ponemos

$$\Phi(G) = \bigcap_{M \in \mathcal{M}} M;$$

si, en cambio, $\mathcal{M} = \varnothing$, ponemos $\Phi(G) = G$. $\Phi(G)$ es el *subgrupo de Frattini*, en honor de Giovanni Frattini (1852–1925, Italia).

(a) Determinar el subgrupo de Frattini de $\mathbb{Z}_{p^2}$ si p es primo.

Un elemento $g \in G$ es un *no-generador* si siempre que $X \subset G$ es un conjunto generador de G y $g \in X$, entonces $X \setminus \{g\}$ también genera a G.

(d) Mostrar que $\Phi(G)$ es el conjunto de elementos no-generadores de G.

(e) Mostrar que $\Phi(G)$ es normal.

1.10.41. Sea G un grupo y H un subgrupo propio de G. Entonces $\langle G \setminus H \rangle = G$.

1.10.42. Sea $G \subset \mathbb{C}^\times$ un subgrupo finito del grupo multiplicativo $\mathbb{C}^\times$. Entonces existe $n \in \mathbb{N}$ tal que $G = \mathbb{G}_n$ es el grupo de las raíces n-ésimas de la unidad.

Homomorfismos

1.10.43. Sea G un grupo y X un conjunto. Sea $x_0 \in X$ y sea

$$\mathrm{ev}_{x_0} : f \in G^X \mapsto f(x_0) \in G.$$

Mostrar que se trata de un homomorfismo de grupos. Determinar su núcleo e imagen.

1.10.44. Mostrar que cualquiera sea el grupo G, existe un isomorfismo $G \cong G^{\mathrm{op}}$ entre G y su grupo opuesto.

1.10.45. Sean G y H grupos, y sea $\hom_{\mathrm{Gr}}(G, H)$ el conjunto de todos los homomorfismos $f : G \to H$. ¿Se trata en general de un subgrupo de H^G? Encuentre condiciones sobre H que garanticen que lo sea.

1.10.46. Muestre que el grupo $\mathbb{H}$ del ejercicio **1.10.5** y el grupo $\mathbb{H}_1$ del ejercicio **1.10.16** son isomorfos.

1.10.47. Mostrar que no hay morfismos no nulos de $\mathbb{Q}$ en $\mathbb{Z}$.

1.10.48. ¿Es la función $f : \mathbb{H} \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$ definida por

$$\begin{aligned} f(\pm 1) &= (0,0), & f(\pm i) &= (1,0), \\ f(\pm j) &= (0,1), & f(\pm k) &= (1,1), \end{aligned}$$

un morfismo de grupos? Si lo es, calcule núcleo e imagen.

1.10.49. ¿Existe un isomorfismo de grupos entre:

1. $\mathbb{Z}_4 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$?
2. $\mathbb{Z}_{2n} \cong D_n$?
3. $\mathbb{Z}_8 \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong \mathbb{H} \cong D_4$?
4. $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$?
5. $(\mathbb{R}, +) \cong (\mathbb{R} - \{0\}, \cdot)$?

1.10.50. Sea G un grupo.

(a) Sea $g \in G$ e $\mathrm{inn}_g : h \in G \mapsto ghg^{-1} \in G$. Mostrar que es $\mathrm{inn}_g \in \mathrm{Aut}(G)$.

(b) Mostrar que la aplicación $\mathrm{inn} : g \in G \mapsto \mathrm{inn}_g \in \mathrm{Aut}(G)$ es un homomorfismo de grupos.

(c) Describir el núcleo de inn. Los automorfismos que están en la imagen de G se llaman *automorfismos interiores* y la imagen misma se denota $\mathrm{Inn}(G)$.

(d) Mostrar que $\mathrm{Inn}(G)$ es un subgrupo normal de $\mathrm{Aut}(G)$.

1.10.51. Sea G un grupo finito. Supongamos que existe $f \in \mathrm{Aut}(G)$ tal que $f^2 = 1$ y f no deja fijo ningún elemento de G aparte de 1.

Entonces cada cada $g \in G$ es $f(g) = g^{-1}$ y G es abeliano de orden impar.

Sugerencia. Muestre la aplicación $\phi : g \in G \mapsto g^{-1}f(g) \in G$ es biyectiva y muestre que $f(g) = g^{-1}$ escribiendo a g en la forma $h^{-1}f(h)$ para algún elemento h de G.

1.10.52. Sea G un grupo. Un subgrupo H de G se dice *característico* si cualquiera sea $f \in \mathrm{Aut}(G)$, $f(H) \subset H$.

(a) Muestre que si $H \subset G$ es un subgrupo característico, entonces para cada $f \in \mathrm{Aut}(G)$ es $f(H) = H$.

(b) Muestre que $\mathcal{Z}(G)$ y $[G, G]$ son característicos.

(c) $\Phi(G)$ es un subgrupo característico de G.

(d) Si H es un subgrupo característico de G, entonces H es normal en G.

(e) Si un grupo G posee un único subgrupo H de un orden dado, éste es característico.

(f) Si H es un subgrupo característico en G y K es un subgrupo característico en H, entonces H es un subgrupo característico de G. Comparar con **1.10.34**.

(g) Si $N \subset G$ es un subconjunto característico (es decir, si para cada $f \in \mathrm{Aut}(G)$, $f(N) \subset N$), entonces $\langle N \rangle$ y $\mathcal{C}(N)$ son subgrupos característicos de G.

Un subgrupo H de G se dice *totalmente característico* si $f(H) \subset H$ siempre que $f \in \mathrm{End}(G)$.

(f) Un subgrupo totalmente característico es característico.

(g) Dar ejemplos de un subgrupo totalmente característico y de un subgrupo característico pero no totalmente característico.

(h) Todos los subgrupos de un grupo cíclico son totalmente invariantes. ¿Vale la recíproca?

†**1.10.53.** *(a)* Sea G un grupo y sean H y K subgrupos de G de índice finito. Entonces $L = H \cap K$ también tiene índice finito.

Sugerencia. Para verlo, defina una aplicación $\phi : G/L \to G/H \times G/K$ de manera que $\phi(xL) = (xH, xK)$ y muestre que ésta es inyectiva.

(b) El conjunto de elementos de un grupo que poseen un número finito de conjugados es un subgrupo característico.

1.10.54. Sea $f : G \to H$ un homomorfismo de grupos.

(a) Si H es abeliano, entonces $[G, G] \subset \ker f$.

(b) Mostrar que $f([G,G]) \subset [H,H]$. En particular, concluya que $[G,G]$ es un subgrupo característico de G.

1.10.55. Sea $f : G \to H$ un homomorfismo de grupos. ¿Es cierto en general que $f(\mathcal{Z}(G)) \subset \mathcal{Z}(H)$? En caso negativo, de condiciones suficientes que garanticen esta inclusión. Bajo esas condiciones, ¿es $f(\mathcal{Z}(G)) = \mathcal{Z}(H)$?

1.10.56. Sea G un grupo.

(a) Mostrar que la función $\mathrm{ev}_1 : f \in \hom_{\mathrm{Gr}}(\mathbb{Z}, G) \mapsto f(1) \in G$ es una biyección.

(b) Describir $\hom_{\mathrm{Gr}}(\mathbb{Z}^2, G)$ y, para cada $n \in \mathbb{N}$, $\hom_{\mathrm{Gr}}(\mathbb{Z}_n, G)$.

1.10.57. *(a)* Determinar $\hom_{\mathrm{Gr}}(\mathbb{Q}, \mathbb{Z})$ y $\hom_{\mathrm{Gr}}(\mathbb{Q}, G)$ cuando G es un un grupo finito.

(b) Describir la imagen $D(G)$ de la aplicación

$$\mathrm{ev}_1 : f \in \hom_{\mathrm{Gr}}(\mathbb{Q}, G) \mapsto f(1) \in G.$$

(c) Mostrar que cuando G es abeliano, $D(G)$ es un subgrupo característico de G

1.10.58. Sea G un grupo.

(a) Encontrar una condición necesaria y suficiente sobre G para que la aplicación $(g,h) \in G \times G \mapsto gh \in G$ resulte un homomorfismo de grupos.

(b) Encontrar una condición necesaria y suficiente sobre G para que la aplicación $g \in G \mapsto g^{-1} \in G$ resulte un homomorfismo de grupos.

(c) Encontrar una condición necesaria y suficiente sobre G para que la aplicación $g \in G \mapsto g^2 \in G$ resulte un homomorfismo de grupos.

1.10.59. Sean $m, n \in \mathbb{N}$. Si $(m,n) = 1$, entonces $\hom_{\mathrm{Gr}}(\mathbb{Z}_m, \mathbb{Z}_n)$ es trivial. ¿Qué sucede en general?

1.10.60. Sea G un grupo finito y $\phi : G \to G$ un endomorfismo de G.

(a) Existe $n \in \mathbb{N}$ tal que si $m \geq n$, entonces $\phi^m(G) = \phi^n(G)$. Sea $\alpha = \phi^n$.

(b) Mostrar que $\operatorname{Im} \alpha$ es normal o dar un contraejemplo.

1.10.61. Usando el hecho que $\mathrm{GL}_2(\mathbb{F}_2)$ permuta los elementos no nulos de $\mathbb{F}_2^2$, encuentre un isomorfismo $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$.

1.10.62. *(a)* Sea G un grupo y sea $X \subset G$ un subconjunto tal que $\langle X \rangle = G$. Sea $f \in \mathrm{End}(G)$ tal que $f(x) = x$ para todo elemento $x \in X$. Entonces $f = \mathsf{Id}_G$.

(b) Sea X el conjunto de los elementos de orden 2 de S_3. Muestre que cada automorfismo de S_3 induce una permutación de X y deduzca que $\mathrm{Aut}(S_3) \cong S_3$.

1.10.63. Sea $n \geq 2$. Consideramos el polinomio *discriminante*

$$\Delta(x_1, \ldots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j) \in \mathbb{Z}[x_1, \ldots, x_n]$$

Si $\pi \in S_n$ es una permutación de $\{1, \ldots, n\}$, definimos

$$\varepsilon(\pi) = \frac{\Delta(x_{\pi(1)}, \ldots, x_{\pi(n)})}{\Delta(x_1, \ldots, x_n)}.$$

(a) Mostrar que cualquiera sea $\pi \in S_n$, es $\varepsilon(\pi) \in \{\pm 1\}$.

(b) Mostrar que $\varepsilon : S_n \to \{\pm 1\}$ es un homomorfismo de grupo si dotamos a $\{\pm 1\}$ del producto usual.

El subgrupo $A_n = \ker \varepsilon$ es el *n-ésimo grupo alternante*.

(f) Describir A_2 y A_3.

(g) Sea $\tau = (i\,j) \in S_n$ una transposición. Determinar el valor de $\varepsilon(\tau)$.

(h) Recordemos que todo elemento $\pi \in S_n$ puede ser escrito—de muchas maneras—como producto de transposiciones. Muestre que la paridad del número de transposiciones empleadas depende solamente de π.

Una permutación que puede escribirse de alguna forma como un producto de un número par de transposiciones se dice *par*.

1.10.64. *Automorfismos de $\mathbb{H}$.*

(a) Determine todos los automorfismos interiores de $\mathbb{H}$.

(b) De ejemplos de automorfismos de $\mathbb{H}$ no interiores.

(c) Muestre que $\mathrm{Aut}(\mathbb{H}) \cong S_4$.

†**1.10.65.** *Automorfismos de S_n.*

(a) Sea $\phi \in \mathrm{Aut}(S_n)$ y sea $g = (1\,2\,3)$. Mostrar que $\phi(g)$ es un producto de 3-ciclos disjuntos, que $\phi(\mathrm{cl}(g)) \subset \mathrm{cl}(\phi(g))$ y que, de hecho, la restricción $\phi : \mathrm{cl}(g) \to \mathrm{cl}(\phi(g))$ es una biyección.

(b) Mostrar que

$$|\mathrm{cl}(g)| = \frac{n!}{3(n-3)!}$$

y que si $\phi(g)$ es producto de r 3-ciclos disjuntos,

$$|\mathrm{cl}(\phi(g))| = \frac{n!}{3^r r!(n-3r)!}.$$

(c) Mostrar que o bien $r = 1$ o bien $r = 2$ y $n = 6$.

Supongamos desde ahora que $n \neq 6$.

(f) La imágen de todo 3-ciclo por ϕ es un 3-ciclo.

(g) Sea $3 \leq i \leq n$ y supongamos que es $\phi((1\,2\,3)) = (\alpha\,\beta\,\gamma)$ y $\phi((1\,2\,i)) = (\alpha'\,\beta'\,\gamma')$. Muestre que $(\alpha\,\beta\,\gamma)(\alpha'\,\beta'\,\gamma')$ tiene orden dos y use esto para concluir que $|\{\alpha, \beta, \gamma, \alpha', \beta', \gamma'\}| = 4$.

(h) Muestre que existen $\alpha, \beta, \gamma_3, \ldots, \gamma_n$ distintos de manera que para cada $3 \leq i \leq n$ es $\phi((1\,2\,i)) = (\alpha\,\beta\,\gamma_i))$.

(i) Sea $\pi \in S_n$ tal que $\pi(1) = \alpha$, $\pi(2) = \beta$ y $\pi(i) = \gamma_i$ para cada $3 \leq i \leq n$. Muestre que $\phi(x) = \pi x \pi^{-1}$.

(j) Muestre que $\mathrm{inn} : S_n \to \mathrm{Aut}(S_n)$ es un isomorfismo.

(k) Determine $\mathrm{Aut}(S_6)$.

Cocientes

1.10.66. Mostrar que

(a) $\mathbb{C}^\times/\mathbb{R}^+ \cong S^1$;

(b) $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$ cualquiera sea $m \in \mathbb{N}$;

(c) $\mathrm{GL}_n(k)/\mathrm{SL}_n(k) \cong k^\times$ si k es un cuerpo y $n \in \mathbb{N}$;

(d) $S^1/\mathbb{G}_n \cong S^1$ si $n \in \mathbb{N}$;

(e) si $m|n$, $\mathbb{G}_n/\mathbb{G}_m \cong \mathbb{G}_{n/m}$.

1.10.67. Si G es un grupo no abeliano, entonces $G/\mathcal{Z}(G)$ no es cíclico.

Sugerencia. Use **1.10.25**.

1.10.68. Muestre que $G/\mathcal{Z}(G) \cong \mathrm{Inn}(G)$.

1.10.69. Si G es un grupo y H y K son subgrupos normales de G, muestre que $G/(H \cap K)$ es isomorfo a un subgrupo de $G/H \times G/L$.

1.10.70. Dado un grupo G, el *grupo* $\mathrm{Out}(G)$ *de automorfismos exteriores de* G es el cociente $\mathrm{Aut}(G)/\mathrm{Inn}(G)$; recordemos que en el ejercicio 4*(d)* vimos que $\mathrm{Inn}(G)$ es normal en $\mathrm{Aut}(G)$. Es importante observar que los elementos de $\mathrm{Out}(G)$ *no* son automorfismos de G.

Determinar $\mathrm{Out}(G)$ cuando $G \in \{S_3, S_4, \mathbb{H}\}$.

1.10.71. Sea G un grupo y sea H un subgrupo no normal. Mostrar que el conjunto de coclases izquierdas de H en G no forma un grupo bajo la multiplicación usual.

Productos

1.10.72. Sean U y V dos grupos y $f : U \to W$ y $g : V \to W$ homomorfismos de grupos. Entonces la aplicación

$$h : (u, v) \in U \times V \mapsto f(u)g(v) \in K$$

es un homomorfismo de grupos sii todo elemento de $f(U)$ conmuta con todo elemento de $h(V)$.

1.10.73. Si G y H son grupos, determine $\mathcal{Z}(G \times H)$.

1.10.74. *Producto directo interno.* Sea G un grupo.

(a) Sean N y M dos subgrupos normales de G y supongamos que $N \cap M = 1$ y $G = NM$. Mostrar que entonces es $G \cong N \times M$.

(b) Supongamos que G es grupo finito de orden mn con $(m, n) = 1$. Si G posee exactamente un subgrupo N de orden n y exactamente un subgrupo M de orden m, entonces G es isomorfo al producto directo de N y M.

†*(c)* Sean $k \in \mathbb{N}$ y $(N_i)_{i=1}^k$ una familia de subgrupos normales de G tales que $G = \langle \bigcup_{i=1}^k N_i \rangle$ y para cada $j \in \{1, \ldots, k\}$ se tiene que

$$N_j \cap \langle \bigcup_{\substack{1 \le i \le k \\ i \neq j}} N_i \rangle = 1.$$

Mostrar que entonces $G \cong N_1 \times \cdots \times N_k$.

†*(d)* Otra vez, supongamos que G es finito y sean $N_1, \dots, N_k$ subgrupos normales de G de órdenes $r_1, \dots, r_k$ tales que $(r_i, r_j) = 1$ si $1 \leq i, j \leq k$ y $|G| = r_1 \cdots r_k$. Entonces $G \cong N_1 \times \cdots \times N_k$.

1.10.75. *Producto semi-directo.*

(a) Sean G y N grupos y sea $\theta : G \to \mathrm{Aut}(N)$ un homomorfismo de grupos. Sea $K = N \times G$ y consideremos el producto en K dado por

$$(n, g) \cdot (n', g') = (n\theta(g)(n'), gg'), \qquad \forall (n, g), (n', g') \in K.$$

Mostrar que, con respecto a este producto, K es un grupo.

Llamamos al grupo K construido el *producto semi-directo (o cruzado) de N por G con respecto a θ* y lo notamos $N \rtimes_\theta G$.

(d) Encontrar morfismos de grupo 'naturales' $\iota : N \to N \rtimes_\theta G$ y $\pi : N \rtimes_\theta G \to N$ tales que ι sea inyectivo, π sea sobreyectivo e $\mathrm{Im}\, \iota = \ker \pi$.

(e) Mostrar que si $\theta = 1$ es el homomorfismo trivial, $N \rtimes_\theta G \cong N \times G$ es simplemente el producto directo.

1.10.76. *Producto semi-directo interno.* Sea K un grupo y sean G y N subgrupos de K con N normal en K. Las siguientes afirmaciones son equivalentes:

(a) $K = NG$ y $N \cap G = \{1\}$;

(b) $K = GN$ y $N \cap G = \{1\}$;

(c) Todo elemento de K puede escribirse de forma única como un producto de un elemento de N por uno de G.

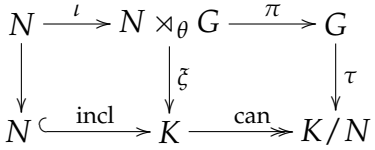
(d) Todo elemento de K puede escribirse de forma única como un producto de un elemento de G por uno de N.

(e) La composición de la inclusión $\mathrm{incl} : : G \hookrightarrow K$ con la proyección canónica $\mathrm{can} : K \twoheadrightarrow K/N$ es un isomorfismo $\tau : G \cong K/N$.

(f) Existe un homomorfismo $\sigma : K \to N$ que se restringe a la identidad de N y cuyo núcleo es N.

Además, cuando estas afirmaciones valen, existen un morfismo de grupos $\theta : G \to \mathrm{Aut}(N)$ y un isomorfismo $\xi : N \rtimes_\theta G \to K$ tales que

el siguiente diagrama conmuta:



Los homomorfismos ι y π del diagrama fueron construidos en el ejercicio **1.10.75**.

1.10.77. Mostrar que existe un morfismo $\theta : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$ tal que $S_3 \cong \mathbb{Z}_3 \rtimes_\theta \mathbb{Z}_2$.

1.10.78. Mostrar que S_n es el producto semi-directo de A_n y $\langle (1\,2) \rangle$.

†**1.10.79.** Mostrar que $\mathbb{H}$ no es un producto semi-directo de forma no trivial.

†**1.10.80.** Sea G un grupo finito y $\phi : G \to G$ un endomorfismo de G y α el endomorfismo de G construido en el ejercicio **1.10.60**. Mostrar que G es el producto semi-directo de $\ker \alpha$ e $\mathrm{Im}\, \alpha$.

Acciones

1.10.81. Si un grupo G actúa sobre un conjunto finito X, el *carácter* de X es la aplicación $\chi_X : G \to \mathbb{N}_0$ dada por

$$\chi_X(g) = |\{x \in X : gx = x\}|, \qquad \forall g \in G.$$

Si no hay ambigüedad sobre X, escribimos simplemente χ.

(a) Si G actúa transitivamente sobre X, es muestre que

$$\frac{1}{|G|} \sum_{g \in G} \chi(g) = 1.$$

Sugerencia. Considere el conjunto $S = \{(g, x) \in G \times X : gx = x\}$ y cuente sus elementos de dos formas distintas.

(b) En general, si la acción no es necesariamente transitiva, es

$$\frac{1}{|G|} \sum_{g \in G} \chi(g) = |X/G|.$$

Aquí, X/G es el conjunto de órbitas de G en X.

†*(c)* Si G actúa transitivamente sobre X y $x_0 \in X$, entonces, si G_{x_0} es el estabilizador de x_0 en G, es

$$\frac{1}{|G|}\sum_{g\in G}\chi(g)^2 = |X/G_{x_0}|.$$

Sugerencia. Una forma de hacer esto consiste en contar los elementos del conjunto $S = \{(g,x,y) \in G\times X\times X : gx = x,\, gy = y\}$ de dos formas distintas.

1.10.82. *Grupos lineales finitos.* Sea k un cuerpo finito de q elementos.

(a) Sea $V = k^2$ el k-espacio vectorial de vectores columna y sea X el conjunto de vectores no nulos de V. Mostrar que la acción de $\mathrm{GL}_2(k)$ sobre V por multiplicación a izquierda preserva a X y que la acción de $\mathrm{GL}_2(k)$ sobre X es transitiva.

(b) Sea $v_0 = (1,0)^t \in X$. Determinar el estabilizador $\mathrm{GL}_2(k)_{v_0}$ de v_0 en $\mathrm{GL}_2(k)$.

(c) Mostrar que $|\mathrm{GL}_2(k)| = (q^2-1)(q^2-q)$.

†*(d)* Más generalmente, mostrar que si $n \in \mathbb{N}$, es

$$|\mathrm{GL}_n(k)| = \prod_{i=0}^{n-1}(q^n - q^i).$$

†*(e)* Sea $n \in \mathbb{N}$. Muestre que el morfismo $\det : \mathrm{GL}_n(k) \to k^\times$ es sobreyectivo y concluya que

$$|\mathrm{SL}_n(k)| = \frac{1}{q-1}\prod_{i=0}^{n-1}(q^n - q^i).$$

1.10.83. *Subgrupos grandes.*

(a) Sea G un grupo finito y H un subgrupo de índice 2. Construya explícitamente un homomorfismo de grupos $f : G \to \mathbb{Z}_2$ tal que $\ker f = H$, mostrando en particular que H es normal.

El objetivo de lo que sigue es obtener una prueba de la siguiente proposición que generaliza a este resultado:

Proposición. *Sea G un grupo finito, sea p el menor número primo que divide a $|G|$ y sea H un subgrupo de G de índice p. Entonces H es normal.*

Notemos que, en las condiciones de este enunciado G no puede poseer subgrupos de índice menor que p.

(d) Sea $X = G/H = \{gH : g \in G\}$ el conjunto de coclases a izquierda de H en G; así, $|X| = p$. Consideramos sobre X la acción usual de G por multiplicación, dada por

$$(g, hH) \in G \times X \mapsto ghH \in X.$$

y sea $\theta : G \to S(X)$ el homomorfismo de grupos correspondiente. Mostrar que si $K = \ker\theta$, se tiene que $H \supset K$ y, como $\operatorname{Im}\theta$ es un subgrupo de $S(X)$, que $|G : K|$ divide a $p!$.

(e) Muestre que $|G : K| = |G : H|$, para concluir que $H = K$ y, así, que H es normal.

Sugerencia. Para hacerlo, observe primero que $p = |G : H| \leq |G : K|$, de manera que $|G : K| \neq 1$. Si q es un primo que divide a $|G : K|$, lo hecho en la parte anterior implica que $q \leq p$; esto junto con la elección de p implica que $|G : K| = p^r$ para algún $r \geq 1$. Muestre para terminar que debe ser $r = 1$.

1.10.84. Si $G = \mathbb{Z}_3$ y $X = \mathbb{R}^3$, ver que poniendo

$$\begin{aligned}
\overline{0} \cdot (x, y, z) &= (x, y, z),\\
\overline{1} \cdot (x, y, z) &= (y, z, x),\\
\overline{2} \cdot (x, y, z) &= (z, x, y)
\end{aligned}$$

obtenemos una acción lineal de G sobre X.

Mostrar que el subespacio V generado por el vector $(1, 1, 1)$ es un subespacio estable por la acción de $\mathbb{Z}_3$ y que la accióon restringida a V es trivial. Mostrar además que el complemento ortogonal de V (con respecto al producto interno canónico de $\mathbb{R}^3$) es estable por la acción de $\mathbb{Z}_3$, donde la acción no es trivial. Ver que $V^\perp$ no contiene subespacios propios $\mathbb{Z}_3$-estables.

Teoremas de Sylow

1.10.85. Sea p un número primo. Un grupo abeliano finito de exponente p^r con $r > 0$ posee elementos de orden p.

1.10.86. Sea p un número primo y G un grupo de orden $p^r > 1$. Entonces $\mathcal{Z}(G)$ no es trivial.

1.10.87. Sea G un grupo finito de orden $|G| = p^r m$ con p primo y $(p, m) = 1$. Entonces G posee subgrupos de orden p^r.

Definición. Sea p un número primo. Decimos que un elemento g de G es *p-primario* si su orden es una potencia de p. Un grupo G es un *p-grupo* si el orden de todo elemento de G es una potencia de p.

1.10.88. Sea p un número primo.

(a) Si G es un p-grupo y H es un subgrupo de G, entonces H es un p-grupo.

(b) Si G es un p-grupo y $f : G \to H$ es un homomorfismo sobreyectivo, H es un p-grupo.

(c) Si G es un grupo, H un subgrupo normal de G y tanto H como G/H son p-grupos, entonces G es un p-grupo.

1.10.89. Un grupo finito G es un p-grupo sii $|G| = p^r$ para algún $r \geq 1$.

Definición. Sea p un número primo y G un grupo. Un *p-subgrupo de Sylow* de G es un p-subgrupo maximal de G. Escribimos $\mathrm{Syl}_p(G)$ al conjunto de los p-subgrupos de Sylow de G.

1.10.90. Sea G un grupo finito y p un número primo.

(a) Si $|G| = p^r m$ con $(p, m) = 1$ y $H \subset G$ es un subgrupo tal que $|H| = p^r$, entonces $H \in \mathrm{Syl}_p(G)$.

(b) Si $p \mid |G|$, entonces $\mathrm{Syl}_p(G) \neq \varnothing$.

1.10.91. Si G es un grupo y $H \in \mathrm{Syl}_p(G)$ y $x \in G \setminus H$ tiene orden $|x| = p^n$, entonces $x \notin \mathcal{N}(H)$.

Sugerencia. Suponga lo contrario y considere el orden del elemento xH en el grupo $\langle H \cup \{x\}\rangle / H$.

1.10.92. Sea G un grupo finito y $K \in \mathrm{Syl}_p(G)$. Sea $\mathcal{C}$ el conjunto de subgrupos de G conjugados de K.

(a) Sea $H \in \mathrm{Syl}_p(G)$ y sea $\sim$ la relación en $\mathcal{C}$ tal que

$$L \sim L' \text{ sii existe } h \in H \text{ tal que } hLh^{-1} = L.$$

Muestre que se trata de una relación de equivalencia.

(b) Sea $L \in \mathcal{C}$ y notemos $[L]$ a la clase de equivalencia de L. Entonces $|[L]| = [H : H \cap \mathcal{N}(L)]$. Además, si $L \neq H$ es $|[L]| > 1$ y es divisible por p. Si, por el contrario, $L = H$, entonces $|[H]| = 1$.

(c) Muestre que

$$|\mathcal{C}| \equiv \begin{cases} 0 \pmod{p}, & \text{si } H \notin \mathcal{C}; \\ 1 \pmod{p}, & \text{si } H \in \mathcal{C}. \end{cases}$$

(d) Concluya que H es conjugado de K y que $|\mathcal{C}| \cong 1 \pmod{p}$.

1.10.93. Pruebe el siguiente teorema debido a Peter Ludwig Mejdell Sylow (1832–1918, Noruega) que es, probablemente, el teorema más importante de la teoría de grupos finitos.

Teorema. (M. L. Sylow, Théorèmes sur les groupes de substitutions, Math. Ann. **5** (1872), no. 4, 584–594.) *Sea p un número primo. Sea G un grupo finito de orden $p^r m$ con $(p, m) = 1$. Entonces*

(a) *Un subgrupo H de G es un p-subgrupo de Sylow sii $|H| = p^r$.*

(b) *Todos los p-subgrupos de Sylow de G son conjugados.*

(c) *Sea n_p el número de p-subgrupos de Sylow de G. Entonces $n_p \equiv 1 \pmod{p}$.*

(d) $n_p \mid m$.

1.10.94. Muestre que no hay grupos simples de orden 28 ó 312.

1.10.95. Muestre que un grupo de orden 12 ó 56 no es simple.

1.10.96. Si p y q son primos distintos, un grupo de orden pq no es simple.

1.10.97. Sea G un grupo de orden $p^r m$ con p primo, $r \geq 1$ y $p > m$. Entonces G no es simple.

1.10.98. Sea G un grupo de orden $p^2 q$ con p y q primos distintos. Entonces G no es simple.

1.10.99. Muestre que un grupo de orden menor que 60 no es simple.

1.10.100. Mostrar que si G es un grupo y P es un subgrupo de Sylow de G, entonces P es un subgrupo característico de $\mathcal{N}(P)$.

1.10.101. Si todos los subgrupos de Sylow de un grupo finito G son normales, entonces $G \cong \prod_{p \text{ primo}} P_p$. En particular, un grupo abeliano finito es producto de sus subgrupos de Sylow.

Grupos múltiplemente transitivos

Sea G un grupo y supongamos que G actúa fielmente sobre un conjunto X. Sea $k \geq 1$.

1.10.102. Mostrar que obtenemos una acción de G sobre X^k si definimos

$$g \cdot (x_1, \ldots, x_k) = (gx_1, \ldots, gx_k), \qquad \text{si } g \in g \text{ y } (x_1, \ldots, x_k) \in X^k.$$

Mostrar que si $|X| > 1$, la acción de G sobre X^k no es transitiva.

Definición. Pongamos

$$X^{(k)} = \{(x_1, \ldots, x_n) \in X^k : x_i \neq x_j \text{ si } 1 \leq i < i \leq k\}.$$

Diremos que la acción de G sobre X es *k-transitiva* si G actúa transitivamente sobre $X^{(k)}$.

1.10.103. Mostrar que la acción canónica de S_n sobre $\{1, \ldots, n\}$ es n-transitiva.

1.10.104. Mostrar que la acción canónica de A_n sobre $\{1, \ldots, n\}$ es $(n-2)$-transitiva pero no $(n-1)$-transitiva.

1.10.105. Sea K un cuerpo, V un K-espacio vectorial. Mostrar que $\mathrm{Aut}_k(V)$ actúa 1-transitivamente sobre $V \setminus \{0\}$ pero no 2-transitivamente.

1.10.106. Sea otra vez K un cuerpo, V un K-espacio vectorial con $\dim_K \geq 2$, y sea X el conjunto de todos los subespacios de V de dimensión 1. Mostrar que la acción de $\mathrm{Aut}_K(V)$ sobre V induce una acción natural sobre X, que es 2-transitiva pero no 3-transitiva.

1.10.107. Mostrar que la acción sobre el conjunto de vértices de un tetraedro regular del grupo de rotaciones del sólido es 2- pero no 3-transitiva.

1.10.108. Sea A un grupo finito no trivial y $A' = A \setminus \{1\}$. Claramente $\mathrm{Aut}(A)$ actúa sobre A'.

(a) Si $\mathrm{Aut}(A)$ actúa 1-transitivamente en A', entonces existe un número primo p tal que todo elemento de A' es de orden p. Esto implica que A es un p-grupo, así que su centro no es trivial. Concluir que A es abeliano y entonces, usando el ejercicio **1.10.10**, que $G \cong \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$.

(b) Determinar todos los grupos A tales que $\mathrm{Aut}(A)$ actúa de manera 2-transitiva sobre A'.

Definición 1.10.1. Diremos que la acción de G sobre X es *finamente k-transitiva* si es k-transitiva y además, para cada $(x_1, \ldots, x_k) \in X^{(k)}$ y cada $g_1, g_2 \in G$, vale que

$$\forall i \in \{1, \ldots, k\},\ g_1(x_i) = g_2(x_i) \implies g_1 = g_2.$$

En otras palabras, esta condición dice que dos elementos de G que actúan de la misma forma sobre k elementos de k deben coincidir.

1.10.109. Si la acción de G es finamente k-transitiva sobre X y ponemos $n = |X|$, entonces

$$|G| = \frac{n!}{(n-k)!}.$$

1.10.110. La acción de S_n sobre $\{1, \ldots, n\}$ es finamente n-transitiva, finamente $(n-1)$-transitiva pero no finamente $(n-2)$-transitiva.

1.10.111. La acción de A_n sobre $\{1, \ldots, n\}$ es finamente $(n-2)$-transitiva.

1.10.112. *Acciones finamente 1-transitivas.* Este ejercicio describe todas las acciones finamente 1-transitivas.

(a) Sea G un grupo finito. Pongamos $R = G$ y consideremos la acción regular a izquierda $G \times R \to R$; recordemos que

$$g \cdot r = gr, \qquad \forall g \in G, r \in R.$$

Mostrar que la acción de G sobre R es finamente 1-transitiva.

(b) Sea G un grupo finito que actúa sobre un conjunto X no vacío de forma finamente 1-transitiva. Mostrar que existe una función biyectiva $\phi : R \to X$ tal que el diagrama

$$\begin{array}{ccc} G \times R & \longrightarrow & R \\ {\scriptstyle \mathrm{Id}_G \times \phi}\downarrow & & \downarrow{\scriptstyle \phi} \\ G \times X & \longrightarrow & X \end{array}$$

conmuta, si las flechas verticales están dadas por las acciones de G.

1.10.113. Sea K un cuerpo finito de q elementos.

(a) Consideremos el conjunto $\mathrm{AGL}(1,K) = K^\times \times K$ y dotémoslo de un producto dado por

$$(a,b)\cdot(a',b') = (aa', b+ab'),.$$

si $(a,b), (a',b') \in \mathrm{AGL}(1,K)$. Muestre que $(\mathrm{AGL}(1,K),\cdot)$ es un grupo.

(b) Consideremos ahora el conjunto $X = K$ y la aplicación

$$\mathrm{AGL}(1,K)\times K \to K$$

dada por

$$(a,b)\cdot x = ax + b$$

para cada $(a,b) \in \mathrm{AGL}(1,K)$ y cada $x \in X$. Muestre que esto da una acción de $\mathrm{AGL}(1,K)$ sobre X.

(c) Muestre que esta acción es finamente 2-transitiva.

1.10.114. Sea G un grupo finito y sea X un conjunto no vacío sobre el que G actúa de forma finamente 2-transitiva.

(a) Sea $x_0x \in X$ y $H = G_{x_0}$. Pongamos $X' = X \setminus \{x_0\}$. Entonces H actúa de forma finamente 1-transitiva sobre X' y es un subgrupo maximal de G.

(b) $H \cap gHg^{-1} \neq 1$ sii $g \in H$. En particular, es $\mathcal{N}(H) = H$ y $C(h) \subset H$ para cada $h \in H \setminus \{1\}$.

(c) G posee involuciones y son todas conjugadas. Notemos I al conjunto de las involuciones de G.

(d) Sea

$$N' = \{g \in G : \text{para cada } x \in X,\, gx \neq x\}$$

y $N = N' \cup \{1\}$. Entonces es $|N'| = n-1$. Además, N es un subconjunto normal de G.

(e) La acción de N sobre X es simplemente transitiva.

(f) H posee a lo sumo una involución. Si H posee una involución, $|I| = n$; en caso contrario, $|I| = n-1$.

(g) Si $s,t \in I$ y $s \neq t$, entonces st no tiene puntos fijos en X.

(h) Sea $j \in G \setminus H$ una involución. Si $H \cap I \neq \varnothing$, sea además i la única involución de H. Entonces

$$I = \begin{cases} j^H, & \text{si } H \cap I = \varnothing; \\ j^H \cup \{i\}, & \text{si } H \cap I \neq \varnothing. \end{cases}$$

Aquí $j^H = \{hjh^{-1} : h \in H\}$.

(i) Es $I^2 \setminus \{1\} = N'$ y N es un subgrupo normal abeliano de G. De hecho, si $H \cap I = \varnothing$, se tiene que $I = N'$. Más precisamente, existe un número primo p tal que $N \cong \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, y $p = 2$ sii $H \cap I = \varnothing$.

(j) Si T es un subgrupo normal de G con $\mathcal{Z}(T) \neq 1$, entonces es $G = \mathcal{Z}(T) \rtimes H$.

(k) $G \cong N \rtimes H$ con respecto a la acción por conjugación de H sobre N.

(l) Fijemos $x_1 \in X'$. Definimos una aplicación $\xi : N' \to H$ de la siguiente manera: si $n \in N'$, entonces $nx_0 \in X'$ porque n no deja fijo ningún elemento de X, así que como la acción de H sobre X' es simplemente transitiva, existe exactamente un elemento $\xi(n) \in H$ tal que $\xi(n)x_1 = nx_0$. Mostrar que ξ es una biyección.

(m) Fijemos $x_1 \in X'$. Definimos en X dos operaciones $\cdot$ y $+$ en X de la siguiente manera.

Sean $x, y \in X$. Si $x = x_0$, ponemos $x \cdot y = x_0$. Si $x \neq x_0$, existe exactamente un elemento $h \in H$ tal que $hx_1 = x$, y ponemos $x \cdot y = hy$. Por otro lado, sabemos que existe exactamente un elemento $n \in N$ tal que $nx_0 = x$; ponemos $x + y = ny$.

Mostrar que $(X, +)$ es un grupo abeliano isomorfo a N y que $(X', \cdot)$ es un grupo isomorfo a H.

(n) Mostrar que si H es abeliano, entonces $(X, +, \cdot)$ es un cuerpo K y que $G \cong \mathrm{AGL}(1, K)$.

Grupos nilpotentes

Sea G un grupo. Definimos una sucesión creciente

$$1 = Z_0 \subset Z_1 \subset \cdots \subset Z_n \subset Z_{n+1} \subset \cdots$$

de subgrupos normales de G inductvamente de la siguiente manera, empezando por $Z_0 = 1$: sea $i \in \mathbb{N}_0$ y supongamos que ha hemos

contruido Z_i. Como Z_i es normal, podemos considerar el homomorfismo canónico $\pi : G \to G/Z_i$. Ponemos entonces

$$Z_{i+1} = \pi^{-1}\big(\mathcal{Z}(G/Z_i)\big).$$

Se trata claramente de un subgrupo normal de G y es

$$Z_{i+1}/Z_i \cong \mathcal{Z}(G/Z_i).$$

La sucesión de subgrupos $(Z_i)_{i\geq 0}$ se llama la *cadena central superior* de G.

Definición. Si existe $n \in \mathbb{N}_0$ tal que $Z_n = G$, decimos que G es *nilpotente*. El menor tal n es la *longitud nilpotente* de G.

1.10.115. Un grupo abeliano es nilpotente. ¿Es nilpotente S_3? Dé un ejemplo de un grupo nilpotente y no abeliano.

Definición. Una sucesión creciente $(N_i)_{i\geq 0}$ de subgrupos normales de un grupo G tal que $N_0 = 1$ y $N_{i+1}/N_i \subset \mathcal{Z}(G/N_i)$ para cada $i \geq 0$ es una *cadena central ascendente*. Si existe $n \in \mathbb{N}_0$ tal que $N_i = G$ entonces decimos que la cadena *termina* o que *llega* a G.

1.10.116. Si G es un grupo y $(N_i)_{i\geq 0}$ es una cadena central ascendente en G, muestre que para cada $i \geq 0$ se tiene que $[N_{i+1}, G] \subset N_i$.

1.10.117. Si G es un grupo y $(Z_i)_{i\geq 0}$ es su cadena central superior, entonces para cada $i \geq 0$ se tiene que $Z_{i+1} = \{g \in G : [g, G] \subset Z_i\}$.

1.10.118. Mostrar que si un grupo G posee una cadena central ascendente $(N_i)_{i\geq 0}$ que llega a G, entonces es nilpotente. Una forma de hacer esto es ver que $N_i \subset Z_i$ para cada $i \geq 0$.

1.10.119. Sea G un grupo tal que $G/\mathcal{Z}(G)$ es nilpotente. Entonces G es nilpotente.

1.10.120. Un p-grupo finito es nilpotente.

1.10.121. Los subgrupos Z_i que aparecen en la serie central de G son subgrupos característicos en G.

Sugerencia. Esto puede verse por inducción en i, siendo inmediato para $i = 0$. Para ver que Z_{i+1} es característico en G si Z_i lo es, proceda de la siguiente manera:

muestre que todo $\alpha \in \mathrm{Aut}(G)$ induce un automorfismo $\bar{\alpha} \in \mathrm{Aut}(G/Z_i)$ tal que conmuta

$$\begin{array}{ccc} G & \twoheadrightarrow & G/Z_i \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\bar{\alpha}} \\ G & \twoheadrightarrow & G/Z_i \end{array}$$

Usando que el centro de un grupo es característico, concluir que Z_{i+1} es característico.

1.10.122. Un cociente de un grupo nilpotente es nilpotente. Para mostrarlo, considere un homomorfismo es $f : G \to G'$ con dominio G nilpotente y verifique que si $(Z_i)_{i\geq 0}$ es la cadena central superior de G, entonces $(f(Z_i))_{i\geq 0}$ es una cadena central ascendente de G' que termina en G'.

1.10.123. Todo subgrupo de un grupo nilpotente es nilpotente.

1.10.124. Todo producto de grupos nilpotentes es nilpotente.

1.10.125. Si G es un grupo nilpotente y $N \subset G$ es unsubgrupo normal, entonces $N \cap \mathcal{Z}(G) \neq 1$.

1.10.126. Todo subgrupo propio de un grupo nilpotente está estrictamente contenido en su normalizador. En particular, todo subgrupo maximal es normal.

1.10.127. Si G es nilpotente y $P \subset G$ es un subgrupo de Sylow de G, entonces P es normal y, en particular, único.

1.10.128. Si G es nilpotente y finito y para cada primo p, P_p es el p-subgrupo de Sylow, entonces $G \cong \prod_p P_p$.

Esta serie de ejercicios prueba el siguiente teorema:

Teorema. *Un grupo finito es nilpotente sii es isomorfo al producto de sus subgrupos de Sylow.*

Capítulo 2

Anillos

2.1 Definiciones y ejemplos

Dado un grupo finito G de n elementos, siempre puede identificarse a G con un subgrupo del grupo de permutaciones S_n de la siguiente forma. Sea $G = \{x_1, \ldots, x_n\}$ una enumeración de los elementos de G. Si $g \in G$, la multiplicación por g es una biyección de G en G (cuya inversa es la multiplicación por g^{-1}), así que existe una única permutación $\sigma_g \in S_n$ tal que $gx_i = x_{\sigma_g(i)}$ para todo $i = 1, \ldots, n$. La función $g \in G \mapsto \sigma_g \in S(G)$ es claramente un monomorfismo.

Por otro lado, S_n puede pensarse como un subgrupo del grupo $\mathrm{GL}(V)$ de las transformaciones lineales biyectivas de un espacio vectorial V de dimensión n, eligiendo una base $\{v_1, \ldots, v_n\}$ de V y permutando esos elementos. Más precisamente, a cada $\sigma \in S_n$ le asociamos la única transformación lineal t_σ tal que $t_\sigma(v_i) = v_{\sigma(i)}$. Decimos entonces que $(V, (\sigma \mapsto t_\sigma))$ es una *representación de* S_n sobre V, esto es, que los elementos de S_n se "representan" como transformaciones lineales del espacio vectorial V.

Los *anillos* son objetos que generalizan la noción de grupo (en el sentido de que a cada grupo se le puede asociar un anillo del grupo, y que tienen una teoría de "representaciones" natural, de manera análoga a lo que sucede con los grupos (o subgrupos) de permutaciones. Cada una de estas representaciones se llamará un *módulo*. Muchas de las propiedades de un anillo pueden describirse conociendo la clase de módulos que el mismo admite, es decir, sus

representaciones.

Definición 2.1.1. Una terna $(A, +, \cdot)$ en la que $(A, +)$ es un grupo abeliano y $\cdot : A \times A \to A$ es un *anillo con unidad* si se satisfacen las siguientes propiedades:

- *Asociatividad.* Si $a, b, c \in A$, es

  $$(ab)c = a(bc).$$

- *Unidad.* Existe un elemento en A distinto del cero de $(A, +)$, que escribiremos 1_A o simplemente 1, tal que

  $$1a = a1 = a$$

  para todo $a \in A$.
- *Distributividad.* Si $a, b, c \in A$, es

  $$a(b + c) = ab + ac$$

  y

  $$(a + b)c = ac + bc.$$

Si además se tiene que $ab = ba$ para todo par de elementos $a, b \in A$, diremos que el anillo A es *conmutativo*.

Observaciones.
1. En la definición se pide $1 \neq 0$, porque si fuera $1 = 0$ resultaría que $a = a1 = a0 = 0$ para cualquier elemento $a \in A$, con lo que tendríamos $A = \{0\}$.

2. Dado un anillo unitario $(A, +, \cdot)$, el elemento 1_A está unívocamente determinado por la segunda condición de la definición.

3. Si $(A, +, \cdot)$ es una terna que satisface todas las condiciones de la definición de anillo salvo la de existencia del elemento unidad 1_A, diremos que A es un anillo sin unidad. Sin embargo, todo anillo sin unidad puede incluirse en un anillo con unidad.

Ejemplos.
1. Son ejemplos de anillos: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ y $(\mathbb{Z}_n, +, \cdot)$. Si k es un anillo, $(k[x], +, \cdot)$ es también un anillo.

2. Si $(A, +, \cdot)$ es un anillo, entonces también lo es el conjunto $\mathsf{M}_n(A)$ de las matrices $n \times n$ con coeficientes en A, con respecto a las operaciones de suma coeficiente a coeficiente y el producto usual de matrices. Llamamos a este anillo el *anilo de matrices con coeficientes en A*.

3. Si X es un conjunto y A es un anillo, el conjunto de funciones $A^X = \{f : X \to A\}$ hereda de A una estructura de anillo, sumando y multiplicando punto a punto. Restringiendo las operaciones definidas en el ejemplo anterior, vemos que $C(\mathbb{R}^n)$ y $C^\infty(\mathbb{R}^n)$ también son anillos, así como sus respectivas variantes tomando subconjuntos adecuados de $\mathbb{R}^n$.

4. Considerando los ejemplos $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ con las operaciones habituales, vemos que en esos casos el producto satisface una propiedad adicional, ya que para todo elemento a no nulo existe otro elemento a' tal que $aa' = a'a = 1$.

Describimos esto diciendo que todo elemento no nulo de A tiene un *inverso a izquierda*, esto es, que para todo $a \in A$, existe $a' \in A$ tal que $a'a = 1$, y un *inverso a derecha*. En estos ejemplos ambos inversos coinciden (¿que sucede en general?).

Observación. Si a es inversible a izquierda y $x, y \in A$, son tales que $ax = ay$, entonces $x = y$.

Si A es un anillo tal que todo elemento de A es inversible a izquierda y a derecha, diremos que A es un *anillo de división*.

Observación. Existen anillos de división no conmutativos. El anillo de los cuaterniones es un ejemplo de esto.

Consideremos el anillo de matrices $\mathsf{M}_2(\mathbb{Q})$. Claramente, el elemento $x = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ es no nulo. Existen, sin embargo, matrices no nulas $z \in M_2(\mathbb{Q})$ tales que $xz = 0$. Decimos que x es un *divisor de cero a izquierda* y que un tal z es un *divisor de cero a derecha*. Se ve fácilmente que $x = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ no puede tener un inverso a izquierda.

Esto se generaliza a un anillo cualquiera A: es claro que si un elemento es inversible a izquierda, entonces no puede ser divisor de cero a izquierda (análogamente a derecha).

Definición 2.1.2. Un anillo A sin divisores de cero es un *anillo íntegro*. Si además el producto en A es conmutativo, decimos que A *dominio íntegro*.

Observación. Un dominio íntegro que es un anillo de división resulta un cuerpo.

Definición 2.1.3. Sea k un cuerpo. Una *k-álgebra* es un anillo $(A, +, \cdot)$ en el que $(A, +)$ es un k-espacio vectorial y la multiplicación es compatible con la acción de k, esto es, tal que

$$(ax + by)z = a(xz) + b(yz)$$

y

$$z(ax + by) = a(zx) + b(zy)$$

siempre que $a, b \in k$ y $x, y, z \in A$.

Ejemplos.
1. *Un anillo íntegro no conmutativo.* Sea k un cuerpo y consideremos el anillo $k\langle x, \delta_x\rangle$ de polinomios no conmutativos en x y δ_x, donde x y δ_x satisfacen la relación

$$\delta_x x - x\delta_x = 1.$$

Este anillo se denomina el álgebra de Weyl y se denota $A_1(k)$.

2. El anillo de polinomios usuales $k[x]$ con coeficientes en un cuerpo. es un dominio íntegro que no es un anillo de división.

3. El anillo de cuaterniones es un anillo de división que no es conmutativo.

Consideremos los anillos $(\mathbb{Z}, +, \cdot)$ y $(\mathbb{R}, +, \cdot)$. La suma y el producto en $\mathbb{Z}$ son la restricción de la suma y el producto en $\mathbb{R}$ al subconjunto $\mathbb{Z}$ y $1_{\mathbb{Z}} = 1_{\mathbb{R}}$. Podemos decir que $\mathbb{Z}$ adquiere su estructura de anillo por ser un subconjunto de $\mathbb{R}$ que cumple ciertas propiedades.

Definición 2.1.4. Dados un anillo $(A, +, \cdot)$ y un subconjunto B de A, decimos que B es un *subanillo* de A si y solo si:

- $(B, +)$ es un subgrupo de $(A, +)$.
- $1_A \in B$.
- B es cerrado para el producto, es decir, si $x, y \in B$, entonces $xy \in B$.

Ejemplos.
1. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ son subanillos de cada uno del siguiente.

2. Cualquiera sea k, k es subanillo de $k[x]$.

3. El conjunto de funciones constantes de $\mathbb{R}$ en $\mathbb{R}$ es un subanillo de $C(\mathbb{R})$.

Observaciones.
1. Todo subanillo de un anillo íntegro es íntegro. Sin embargo, si B es subanillo de A y B es íntegro, A puede no serlo.

2. Veremos más adelante que si A es un dominio íntegro, puede encontrarse un cuerpo K del cual A resulte un subanillo. Como ejemplo de esto, podemos tomar a $\mathbb{Z}$ como subanillo de $\mathbb{Q}$.

A continuación, se construirá un importante ejemplo de anillo. La importancia de este ejemplo reside en que tener un módulo sobre este anillo será equivalente a tener un k-espacio vectorial sobre el cual un grupo G actúe:

Ejemplo. Dado un grupo G y un anillo de base k, podemos construir un anillo llamado *anillo de grupo de* G, al que notaremos $k[G]$. Los elementos de $k[G]$ son combinaciones lineales finitas con coeficientes en k de elementos del grupo G. Así, como conjunto es

$$k[G] = \{\sum_{g\in G} \lambda_g g : \lambda_g \in k, \lambda_g = 0 \text{ para casi todo } g \in G\}.$$

Si $x = \sum_{g\in G} \lambda_g g \in k[G]$, el conjunto $\operatorname{sop}(x) = \{g \in G : \lambda_g \neq 0\}$ es el *soporte* de x.

La suma en $k[G]$ se define pensando que los elementos de G forman una base, es decir:

$$\Big(\sum_{g\in G} \lambda_g g\Big) + \Big(\sum_{g\in G} \mu_g g\Big) = \sum_{g\in G} (\lambda_g + \mu_g) g.$$

Notemos que si las dos primeras sumas son finitas, la tercera también lo es, así que esto define una operación en $k[G]$.

El producto se define a partir del producto de G, de la estructura de anillo de k y del hecho de que el producto tiene que ser distributivo con respecto a la suma:

$$\Big(\sum_{g\in G} \lambda_g g\Big) \cdot \Big(\sum_{g\in G} \mu_g g\Big) = \sum_{h,g\in G} (\lambda_g \mu_h) gh = \sum_{g\in G} \Big(\sum_{h\in G} \lambda_{gh^{-1}} \mu_h\Big) g.$$

Por ejemplo, si $x = \lambda g, y = \mu h \in k[G]$, el producto xy es simplemente $xy = (\lambda g) \cdot (\mu h) = (\lambda\mu)gh$. Si x e y son, más generalmente, sumas finitas de elementos de este tipo, el producto se calcula a partir de los productos de cada sumando imponiendo la ley distributiva.

Ejercicio. Verificar que con estas operaciones $(k[G], +, \cdot)$ resulta una k-álgebra con unidad. ¿Qué elementos son el neutro de la suma y el del producto? ¿Y el inverso aditivo de un elemento? ¿Hay elementos que tengan inverso multiplicativo? ¿Cuándo $k[G]$ es un anillo conmutativo?

Observación. En la construcción anterior no se utilizó el hecho de que G fuera un grupo, sino solamente que se trata un monoide con elemento neutro. La asociatividad de G implica la asociatividad del producto de $k[G]$ y el elemento neutro de G funciona como unidad del producto de $k[G]$.

Se puede definir entonces el anillo de un monoide M con elemento neutro, al que notamos también $k[M]$. Por ejemplo, cuando $M = \mathbb{N}_0$, el anillo $k[\mathbb{N}_0]$ puede identificarse con el anillo de polinomios en una variable con coeficientes en k.

2.2 Morfismos

En un anillo existen una estructura de grupo abeliano y una multiplicación. Del mismo modo en que en el caso de los grupos nos interesaban particularmente las funciones que respetaban la estructura de grupo, dentro de la clase de funciones entre anillos que sean morfismos de grupos abelianos, nos interesarán aquellas que también respeten la estructura multiplicativa.

Definición 2.2.1. Sean $(A, +_A, \cdot_A)$ y $(B, +_B, \cdot_B)$ dos anillos. Un *morfismo de anillos unitarios* entre A y B es una función $f : A \to B$ tal que

- $f : (A, +_A) \to (B, +_B)$ es un morfismo de grupos.
- $f(a \cdot_A a') = f(a) \cdot_B f(a')$ si $a, a' \in A$.
- $f(1_A) = 1_B$.

Diremos que f es un *isomorfismo* si es inversible. En ese caso, la función inversa resulta también morfismo de anillos.

Ejemplos.
1. Las inclusiones $\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C} \hookrightarrow \mathbb{H}$ son morfismos inyectivos de anillos.

2. Sea k un anillo con unidad y sean G y H grupos. Si $f : G \to H$ es un morfismo de grupos, definimos una función $k[f] : k[G] \to k[H]$ poniendo

$$k[f]\Big(\sum_{g\in G} \lambda_g g\Big) = \sum_{g\in G} \lambda_g f(g).$$

Entonces $k[f]$ es un morfismo de anillos unitarios. Es evidente que $k[\mathsf{Id}_G] = \mathsf{Id}_{k[G]}$. Además, si f y h son dos morfismos de grupos con dominios tales que tiene sentido calcular $f \circ h$, entonces

$$k[f \circ h] = k[f] \circ k[h].$$

Vemos de esta forma que la asignación $k[-] : \mathrm{Gr} \to \mathrm{An}_1$ dada por $G \mapsto k[G]$ es funtorial.

3. La función $\pi : r \in \mathbb{Z} \mapsto \overline{r}\mathbb{Z}_n$ es un morfismo suryectivo de anillos.

4. Si A es un anillo, existe un único morfismo de anillos $f : \mathbb{Z} \to A$.

5. Sea X un abierto de $\mathbb{R}^n$, $x_0 \in X$ y $A = C(X)$ ó $C^n(X)$ ó $C^\infty(X)$, entonces $\mathrm{ev}_{x_0} : f \in A \mapsto f(x_0) \in \mathbb{R}$ es un morfismo de anillos.

6. Sea A un anillo, $a \in A$ y $\mathrm{ev}_a : \mathbb{Z}[X] \to A$ la aplicación tal que si $P = \sum_{i=0}^n \lambda_i X^i \in \mathbb{Z}[X]$, entonces $\mathrm{ev}_a(P) = \sum_{i=0}^n \lambda_i a^i$. Entonces ev_a es un morfismo de anillos.

Observación. La composición de dos morfismos de anillos es también un morfismo de anillos y, dado un anillo A, la función identidad $\mathsf{Id}_A : A \to A$ es trivialmente un morfismo de anillos. Esto nos dice que la clase de objetos formada por los anillos y los morfismos de anillos forman una categoría (ver el apéndice). Las nociones de monomorfismo e isomorfismo categórico coinciden en este caso con las nociones de morfismo inyectivo y morfismo inversible respectivamente. Dejamos como ejercicio los monomorfismos, haremos la cuenta para isomorfismos.

Sea $f : A \to B$ un isomorfismo de anillos, es decir, un morfismo de anillos inversible. Sea $g : B \to A$ una función tal que $f \circ g = \mathsf{Id}_B$ y $g \circ f = \mathsf{Id}_A$. Sabemos que g es necesariamente un morfismo de

grupos abelianos. Para ver que se trata de hecho de un morfismo de anillos basta ver que g preserva la estructura multiplicativa. Si $b, b' \in B$, entonces

$$\begin{aligned} f(g(bb')) &= \mathsf{Id}_B(bb') = bb' = \mathsf{Id}_B(b)\mathsf{Id}_B(b') \\ &= f(g(b))f(g(b')) = f(g(b)g(b')). \end{aligned}$$

Como f es isomorfismo, en particular es inyectiva, y podemos concluir que $g(bb') = g(b)g(b')$. Como además $f(1_A) = 1_B$,

$$1_A = \mathsf{Id}_A(1_A) = g(f(1_A)) = g(1_B),$$

así que g preserva la unidad.

Sin embargo, veremos a continuación que en el caso de anillos las nociones de epimorfismo categórico y morfismo suryectivo no coinciden.

Ejemplo. ¿Hay algún morfismo de anillos de $\mathbb{Q}$ a $\mathbb{R}$ además de la inclusión $i : \mathbb{Q} \hookrightarrow \mathbb{R}$? La respuesta es no: si $f : \mathbb{Q} \to \mathbb{R}$ es un morfismo, es aditivo y se tiene que $f\left(\frac{m}{n}\right) = mf\left(\frac{1}{n}\right)$. Como además $f(1) = 1$ y $1 = n\frac{1}{n}$, vemos que $1 = nf\left(\frac{1}{n}\right)$. Como se puede dividir por n, concluimos que $f\left(\frac{1}{n}\right) = \frac{1}{n}$. Esto nos dice que f es la inclusión.

Si, por el contrario, buscamos morfismos $f : \mathbb{R} \to \mathbb{Q}$ en el otro sentido, la respuesta es diferente. En efecto, si $f : \mathbb{R} \to \mathbb{Q}$ es un morfismo de anillos y $x \in \mathbb{R}$ es no nulo, se tiene que

$$1 = f(1) = f(xx^{-1}) = f(x)f(x^{-1}).$$

En particular, $f(x) \neq 0$. Vemos así que todo morfismo de anillos que sale de $\mathbb{R}$ tiene núcleo cero y por lo tanto es inyectivo (esto sucede para todo morfismo de anillos unitarios que "sale" de un cuerpo), pero una razón puramente conjuntista nos recuerda que no puede haber ninguna función inyectiva de $\mathbb{R}$ en $\mathbb{Q}$, ya que $\mathbb{R}$ tiene cardinal estrictamente mayor que $\mathbb{Q}$.

Ejemplo. Los epimorfismos categóricos no tienen por qué ser necesariamente funciones suryectivas. A partir del ejemplo anterior con $\mathbb{Q}$, se puede ver fácilmente que todo morfismo de anillos que "salga" de $\mathbb{Q}$ queda univocamente determinado por la condición $f(1) = 1$. De este hecho se desprenden dos cosas:

- Dado un anillo B, o bien existe un único morfismo de anillos $f : \mathbb{Q} \to B$ o bien no existe ninguno. ¿Cuándo sí y cuándo no? (Sugerencia: ver primero que siempre existe un único morfismo de anillos $\mathbb{Z} \to B$.)
- La inclusión $i : \mathbb{Z} \hookrightarrow \mathbb{Q}$ es un epimorfismo categórico (en la categoría de anillos unitarios y morfismos de anillos unitarios).

A diferencia del caso de grupos, en el que entre dos grupos siempre había por lo menos un morfismo de grupos (el morfismo nulo), en el caso de los anillos la condición de que "f(1)=1" junto con la de multiplicatividad restringe muchísimo las posibilidades de morfismos entre anillos, hasta el punto en que dados dos anillos puede no haber morfismos de anillos entre ellos, o haber sólo uno.

2.3 Ideales biláteros

Dado un morfismo de anillos $f : A \to B$, es claro (¡verificarlo!) que $\mathrm{Im}(f) \subseteq B$, además de ser un subgrupo de B, es un subanillo. Sin embargo $\mathrm{Ker}(f)$ no es un subanillo, porque por ejemplo $1 \notin \mathrm{Ker}(f)$ (ya que $f(1) = 1 \neq 0$), aunque sigue siendo un subgrupo. En el caso de los grupos habíamos visto que no todo subgrupo es núcleo de un morfismo de grupos, sino que ésto sólo sucede para los subgrupos invariantes. En un anillo la estructura subyacente de grupo es conmutativa, por lo tanto todo subgrupo es invariante, pero no todo subgrupo es el núcleo de un morfismo de anillos.

Si A es un anillo e I es un subgrupo de $(A, +)$, A/I es un grupo abeliano. La definición que daremos ahora es la que clasifica exactamente a los subgrupos I de un anillo para los que A/I hereda de A una estructura de anillo tal que la proyección al cociente $A \to A/I$ sea un morfismo de anillos (al igual que en el caso de grupos, esa estructura está únívocamente determinada):

Definición 2.3.1. Sea A un anillo e I un subgrupo de $(A, +)$. Diremos que I es un *ideal bilátero* si siempre que $x \in I$ y $a \in A$ se tiene que tanto ax como xa pertenecen a I.

Si sólo pedimos que $ax \in I$ para todo $x \in I$ y $a \in A$, diremos que I es un *ideal a izquierda*. Si sólo pedimos la condición simétrica de que $xa \in I$ para todo $x \in I$ y $a \in A$, diremos que I es un *ideal*

a derecha. Por supuesto, estas distinciones se desvanecen si el anillo es conmutativo, pero en el caso general pueden no coincidir.

El ejemplo fundamental es el siguiente: si $f : A \to B$ es un morfismo de anillos, entonces $\mathrm{Ker}(f)$ es un ideal bilátero. En efecto, es claro que se trata de un subgrupo de A, y si $x \in I$ y $a \in A$ entonces

$$f(ax) = f(a)f(x) = f(a)0 = 0$$

y

$$f(xa) = f(x)f(a) = 0f(x) = 0,$$

así que ax y xa están también en el núcleo de f. Notemos que aunque el anillo A no sea conmutativo, $\mathrm{Ker}(f)$ es siempre un ideal bilátero.

Ejemplos.
1. Sea A un anillo conmutativo y $b \in A$, entonces el conjunto

$$\langle b \rangle = \{ba : a \in A\}$$

de los múltiplos de b es un ideal bilátero. Todo ideal de esta forma es un *ideal principal*.

Así, si $m \in \mathbb{Z}$, $\langle m \rangle = m\mathbb{Z}$ es un ideal de $\mathbb{Z}$; análogamente, en $k[X]$, el conjunto $\langle P \rangle$ de los múltiplos de un polinomio fijo P es un ideal bilátero.

2. Notar que todo subgrupo de $\mathbb{Z}$ es de la forma $m\mathbb{Z}$ para algún m. Más aún, todos ellos son ideales.

Si k es un cuerpo e I es un ideal de $k[X]$, entonces existe un polinomio $P \in k[X]$ tal que $I = \langle P \rangle$. (Demostrarlo: tomar la función "grado" e imitar la demostración de que en $\mathbb{Z}$ los únicos subgrupos son de la forma $m\mathbb{Z}$). Si en cambio consideramos el anillo $k[X, Y]$ o $\mathbb{Z}[X]$, existen ideales no principales (¡dar ejemplos de esto!)

3. Si I es un ideal bilátero de A y $\mathsf{M}_n(I)$ es el conjunto de las matrices de $\mathsf{M}_n(A)$ que en cada lugar tiene elementos de I, entonces $\mathsf{M}_n(I)$ es un ideal bilátero de $\mathsf{M}_n(A)$.

4. Sea X un abierto de $\mathbb{R}^n$, $x_0 \in X$ y $A = C^\infty(X)$. Entonces el conjunto $I_{x_0} = \{f \in A : f(x_0) = 0\}$ es un ideal de A. De hecho, si $\mathrm{ev}_{x_0} : A \to \mathbb{R}$ es el morfismo de evaluación en x_0, esto es, si $\mathrm{ev}_{x_0}(f) = f(x_0)$, entonces $I = \mathrm{Ker}(\mathrm{ev}_{x_0})$.

5. Si $A = C(\mathbb{R})$, entonces $I = \{f \in A : \text{sop}(f) \text{ es acotado}\}$ es un ideal de A.

Observaciones.
1. Si I es un ideal de A y $1_A \in I$ entonces $I = A$. La misma conclusión se obtiene si suponemos sólamente que existe un elemento $a \in I$ que es una unidad.

Un anillo A siempre tiene al menos dos ideales biláteros: *(i)* $\{0\}$, que corresponde a $\text{Ker}(\text{Id}_A : A \to A)$ y *(ii)* A, que no es un núcleo a menos que incluyamos anillos con $1 = 0$. Sin embargo, puede suceder que éstos sean los únicos: por ejemplo, si A es un cuerpo o un anillo de división. Diremos en ese caso que A es un anillo *simple*.

Es fácil ver que un anillo conmutativo simple es un cuerpo, pero en el caso no conmutativo hay anillos simples que no son de división. Por ejemplo, si k es un cuerpo, en anillo de matrices $\mathsf{M}_n(k)$ es un anillo simple.

2. Si $f : A \to B$ es un isomorfismo de anillos, entonces los ideales biláteros de A están en correspondencia 1-1 con los ideales biláteros de B.

Si A es un anillo e $I \subseteq A$ es un idealbilátero, entonces $\mathsf{M}_n(I)$ es un ideal bilátero de $\mathsf{M}_n(A)$ y, de hecho, todos los ideales biláteros de $\mathsf{M}_n(A)$ se obtienen de esta forma.

Sin embargo, A y $\mathsf{M}_n(A)$, si $n > 1$, raramente son isomorfos como anillos (¡dé un ejemplo en el que sí resulten isomorfos!). De cualquier manera, los anillos A y $\mathsf{M}_n(A)$ comparten muchas otras propiedades: este hecho será tratado en el Capítulo de Teoremas de Morita.

3. Si I y J son ideales de A, el conjunto

$$IJ = \{\sum_{i=1}^{n} x_i y_i : x_i \in I,\, y_i \in J\}$$

es un ideal bilátero. Claramente IJ está contenido en I y en J.

4. De manera similar, si I y J son ideales de A, el conjunto

$$I + J = \{x + y : x \in I,\, y \in J\}$$

es un ideal de A.

5. Si I, J_1, y J_2 son ideales de A, entonces $I(J_1 + J_2) = IJ_1 + IJ_2$.

6. La intersección de ideales es un ideal.

7. Sea $a \in A$. El conjunto $\langle a \rangle = \{xa : x \in A\}$ es un ideal a izquierda de A, al que llamamos *ideal principal* (izquierdo) generado por A. Tambien escribimos Aa en vez de $\langle a \rangle$.

8. Si A es un anillo íntegro y $a, b \in A - \{0\}$, entonces entonces $\langle a \rangle = \langle b \rangle$ sii existe $u \in \mathcal{U}(A)$ tal que $a = ub$.

9. Si $X \subset A$, el *ideal generado* por X en A es la intersección $\langle X \rangle$ de todos los ideales de A que contienen a X. Si $X = \{a_1, \ldots, a_n\}$ es un conjunto finito, entonces escribimos $\langle a_1, \ldots, a_n \rangle$ en vez de $\langle X \rangle$. Por ejemplo, en $\mathbb{Z}$ tenemos que $(2, 3) = \mathbb{Z}$ y $(2, 4) = 2\mathbb{Z}$, y en $\mathbb{Q}[x]$, $(x - 2, x - 3) = \mathbb{Q}[x]$.

Definición 2.3.2. Sea I un ideal bilátero de un anilo A., Decimos que I es un ideal bilátero *maximal* si $I \neq A$ y, si J ideal es un bilátero de A tal que $I \subseteq J$, entonces o $J = I$ o $J = A$.

2.4 Cocientes

Vimos que todo núcleo de un morfismo de anillos es un ideal bilátero. En esta sección veremos que, como en el caso de grupos, dado un ideal bilátero I de un anillo A, siempre existe un anillo B y un morfismo $f : A \to B$ tal que $I = \text{Ker}(f)$. La construcción es similar al caso de grupos: se trata de definir una relación de equivalencia entre los elementos de A de manera tal que el conjunto cociente admita una estructura de anillo.

Fijemos entonces un anillo A y un ideal bilátero I de A.

Decimos entonces que dos elementos a y a' de A están relacionados si $a - a' \in I$. Es fácil ver que esto es una relación de equivalencia. Sea A/I el conjunto de clases de equivalencia. Si $a \in A$, escribimos $\overline{a}$ a la clase de a en A/I.

Como I es un subgrupo (normal) del grupo aditivo $(A, +)$, el cociente A/I es un grupo abeliano y $\pi : A \to A/I$ es un morfismo de grupos. La estructura de grupo sobre A/I está definida de manera que

$$\overline{a} + \overline{a'} = \overline{a + a'}.$$

Introducimos un producto en A/I mediante la fórmula:

$$\overline{a} \cdot \overline{a'} := \overline{aa'}$$

Para ver que así obtenemos una estructura de anillo sobre A/I, hay que ver que:

- la multiplicación está bien definida en el cociente, esto es, que si $\overline{a} = \overline{b}$ y $\overline{a'} = \overline{b'}$, entonces $\overline{aa'} = \overline{bb'}$;
- $(A/I, +, \cdot)$ es un anillo con unidad y $1 \neq 0$ si $I \neq A$;
- $\pi : A \to A/I$ es un morfismo de anillos con $\mathrm{Ker}(\pi) = I$.

Una vez vista la buena definición, el hecho de que $(A/I, +, \cdot)$ es un anillo con unidad es obvio. También es obvio que π es un morfismo de anillos, ya que la multiplicación en A/I está definida de la única posible para la cual π es multiplicativa. Finalmente, vemos que $\mathrm{Ker}(\pi) = I$, viendo sólo las estructuras de grupos. Veamos entonces la buena definición:

Sean $a, a', b, b' \in A$ tales que $\overline{a} = \overline{b}$ y $\overline{a'} = \overline{b'}$. Llamando $x = a - b$ e $y = a' - b'$, tenemos que la condición $\overline{a} = \overline{b}$ es equivalente a la condición $x \in I$, y lo mismo vale para y. Cuando calculamos el producto aa' a partir de b y b' tenemos:

$$aa' = (b + x)(b' + y) = bb' + (by + xb' + xy).$$

Como I es un ideal bilátero, tanto by como xb' y xy pertenecen a I, y por lo tanto $\overline{aa'} = \overline{bb'} + \overline{by + xb' + xy} = \overline{bb'} + \overline{0} = \overline{bb'}$. Notemos que, para hacer eso, es fundamental el hecho de que I sea un ideal bilátero, y no sólo a izquierda o a derecha. Si I es un ideal a izquierda pero no bilátero, entonces A/I no admite ninguna estructura de anillo tal que la proyección al cociente sea un morfismo de anillos.

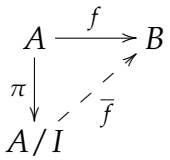
Observación. Como en el caso de grupos, el anillo cociente es una construcción que resuelve un problema de tipo universal con respecto ahora a los morfismos de anillos.

Proposición 2.4.1. *Sea A un anillo e $I \subset A$ un ideal bilátero. El par $(A, \pi : A \to A/I)$ tiene las siguientes dos propiedades:*

(a) $\pi : A \to A/I$ es un morfismo de anillos y $I \subseteq \mathrm{Ker}(\pi)$.

(b) Si B es un anillo y $f : A \to B$ un morfismo tal que $I \subseteq \mathrm{Ker}(f)$, entonces existe un único morfismo de anillos $\overline{f} : A/I \to B$ tal que

$f = \overline{f} \circ \pi$. *El diagrama correspondiente es:*



Demostración. El primer punto de la proposición es claro. Supongamos que se tiene un morfismo de anillos $f : A \to B$ tal que $I \subseteq \operatorname{Ker}(f)$. Como $\pi : A \to A/I$ es un morfismo de grupos con su propiedad universal y f es en particular un morfismo de grupos, se tiene asegurada la existencia y unicidad del morfismo de grupos $\overline{f}$. Luego sólo falta ver que $\overline{f}$ es multiplicativo. Recordemos que $\overline{f}$ está definida por $\overline{f}(\overline{a}) = f(a)$ para todo $a \in A$. A partir de esa fórmula y de la definición de producto en el cociente es claro que $\overline{f}$ es multiplicativa cuando f lo es pues

$$\overline{f}(\overline{a}\overline{a'}) = \overline{f}(\overline{aa'}) = f(aa') = f(a)f(a') = \overline{f}(\overline{a})\overline{f}(\overline{a'}).$$

Esto termina la prueba. □

Como siempre, dos objetos que verifican una misma propiedad universal resultarán isomorfos (verificarlo, calcando la demostración hecha para grupos).

Corolario 2.4.2. *Si $f : A \to B$ un morfismo de anillos, entonces hay un isomorfismo de anillos*

$$A/\operatorname{Ker}(f) \cong \operatorname{Im}(f).$$

Demostración. Basta observar que $\operatorname{Im}(f)$ es un subanillo de B y que $f : A \to \operatorname{Im}(f)$ es un morfismo de anillos. Sabemos que la aplicación $\overline{f} : A/\operatorname{Ker}(f) \to \operatorname{Im}(f)$ es un isomorfismo de grupos abelianos, pero como $\operatorname{Ker}(f)$ es un ideal bilátero, la propiedad del cociente asegura que $\overline{f}$ también respeta el 1 y la estructura multiplicativa. □

Ejemplos.
1. Si $n \in \mathbb{N}$, hay un isomorfismo de anillos $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$.

2. Si k es un anillo y $a \in k$, $\mathrm{ev}_a : k[X] \to k$ es un epimorfismo de anillos con núcleo $\langle X - a \rangle$ (¡verificarlo!), luego $k[X]/\langle X - a \rangle \cong k$.

3. Consideremos el anillo $\mathbb{R}[X]$, el elemento $i \in \mathbb{C}$ y el morfismo de evaluación $\mathrm{ev}_i : \mathbb{R}[X] \to \mathbb{C}$ definido por

$$\sum_{k=0}^{n} a_k X^k \mapsto \sum_{k=0}^{n} a_k i^k.$$

El polinomio $X^2 + 1$ está en el núcleo de ev_i. Se puede ver que, de hecho, $\mathrm{Ker}(\mathrm{ev}_i) = \langle X^2 + 1 \rangle$, y por lo tanto, que $\mathbb{R}[X]/\langle X^2 + 1 \rangle \cong \mathbb{C}$.

4. Si X es un abierto de $\mathbb{R}^n$ y $x_0 \in X$ entonces

$$C(X)/\{f \in C(X) : f(x_0) = 0\} \cong \mathbb{R}.$$

5. Si $I \subseteq A$ es un ideal bilátero entonces

$$\mathsf{M}_n(A)/\mathsf{M}_n(I) \cong \mathsf{M}_n(A/I).$$

6. Sea A un anillo y $e \in A$ un elemento tal que $e^2 = e$. Notemos que entonces $(1 - e)^2 = (1 - e)$. Consideremos el subconjunto

$$eAe = \{exe : x \in A\}.$$

La estructura de anillo está dada por la multiplicación de A restringida a eAe, con unidad $1_{eAe} = e$. Es importante notar que eAe no es subanillo a menos que $e = 1$; en ese caso, por supuesto, $eAe = A$. Por otro lado, $1_{eAe} \neq 0$ siempre que $e \neq 0$.

Dejamos como ejercicio mostrar que si e conmuta con todos los elementos de A, entonces la aplicación

$$\tau_e : x \in A \to exe \in eAe = eA$$

es un morfismo de anillos suryectivo y $\mathrm{Ker}(\tau_e) = (1 - e)A$. De esto deducimos que es $eA \cong A/(1 - e)A$.

Por otro lado, consideremos el anillo $A = \mathsf{M}_n(k)$ y la matriz $e \in A$ con coeficientes

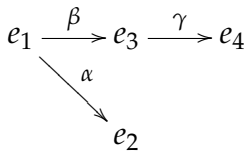
$$e_{ij} = \begin{cases} 1, & \text{si } i = j = 1; \\ 0, & \text{otro caso.} \end{cases}$$

En este caso es claro que $e^2 = e$ y $eAe \cong k$ pero el morfismo de grupos $\tau_e : \mathsf{M}_n(k) \to e\mathsf{M}_n(k)e \cong k$ no es multiplicativo. ¿Por qué?

7. Si $H \lhd G$, k es un anillo y $\pi : G \to G/H$ es la proyección canónica, entonces $k[\pi] : k[G] \to k[G/H]$ induce un isomorfismo

$$k[G]/\langle (1-h) : h \in H \rangle \cong k[G/H].$$

8. Sea k un cuerpo y Q un grafo orientado, es decir, un par (Q_0, Q_1) formado por un conjunto Q_0, cuyos elementos se llaman *vértices*, y un conjunto Q_1, cuyos elementos se llaman *flechas*, y dos funciones s, $t : Q_1 \to Q_0$, que son las que determinan origen y fin de una flecha ("source" y "target"). Por ejemplo, en el grafo



los conjuntos son $Q_0 = \{e_1, e_2, e_3\}$, $Q_1 = \{\alpha, \beta, \gamma\}$, las funciones s y t están definidas por $s(\alpha) = e_1$, $t(\alpha) = e_2$, $s(\beta) = e_1$, $t(\beta) = e_3$, $s(\gamma) = e_3$, $t(\gamma) = e_4$.

Asociado a Q hay un anillo kQ que como k-espacio vectorial tiene base el conjunto de los caminos del grafo (los vértices se consideran como caminos de largo cero); un camino es, por definición, una composición de flechas consecutivas. El producto se define en esa base de caminos, y está dado por la yuxtaposición en el caso del producto de dos caminos consecutivos y cero en otro caso. En el ejemplo del grafo anterior, es

$$kQ = k.e_1 \oplus k\,e_2 \oplus k\,e_3 \oplus k\,e_4 \oplus k\,\alpha \oplus k\,\beta \oplus k\,\gamma \oplus k\,\beta\alpha.$$

Los productos en kQ están determinados por

$$\begin{aligned}
&e_i^2 = e_i, && \text{si } i = 1, \ldots, 4;\\
&e_i e_j = 0, && \text{si } i \neq j;\\
&e_2\alpha = \alpha e_1 = \alpha,\\
&e_3\beta = \beta e_1 = \beta,\\
&e_4\gamma = \gamma e_3 = \gamma,\\
&\beta \cdot \alpha = \beta\alpha,
\end{aligned}$$

y todos los otros productos entre paes de elementos de la base de caminos de Q se anulan.

9. Sea Q el grafo

$$e_1 \xrightarrow{\alpha} e_2$$

Entonces $kQ = ke_1 \oplus ke_2 \oplus k\alpha$ y es fácil ver que kQ resulta isomorfo al subanillo de matrices triangulares de dos por dos vía el morfismo tal que

$$e_1 \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right), \qquad e_2 \mapsto \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right), \qquad \alpha \mapsto \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right).$$

2.5 Producto de anillos

Sea I un conjunto no vacío y, para cada $\alpha \in I$, sea $(A_\alpha, +_\alpha, \cdot_\alpha)$ un anillo. Sea $A = \prod_{\alpha\in I} A_\alpha$ el producto cartesiano. Damos a A una estructura de anillo considerando la suma y el producto definidos coordenada a coordenada. Es fácil ver que con estas operaciones obtenemos en efecto un anillo, al que escribimos $(\prod_{\alpha\in I} A_\alpha, +, \cdot)$. Este anillo tiene las siguientes propiedades:

- Para todo $\beta \in I$ existe un epimorfismo $\pi_\beta : \prod_{\alpha\in I} A_\alpha \to A_\beta$, la proyección en la coordenada β.
- Si A' es un anillo y tenemos una familia de morfismos de anillos $(f_\beta : A' \to A_\beta)_{\beta\in I}$, entonces existe un único morfismo $f : A' \to A$ tal que $\pi_\beta \circ f = f_\beta$. Esto es, el siguiente diagrama conmutativo se completa de manera única con la flecha punteada:

$$\begin{array}{ccc} A' & \xrightarrow{f_\beta} & A_\beta \\ {\scriptstyle f}\downarrow & \nearrow_{f} & \\ \prod_{\alpha\in I} A_\alpha & & \end{array}$$

  Esto nos dice que para definir un morfismo de un anillo A' en $\prod_{\alpha\in I} A_\alpha$ basta definir morfismos de A' en cada uno de los A_β, $\beta \in I$.

Se observa que ésta es otra construcción de tipo "universal" (como por ejemplo el cociente) y que cualquier otro anillo que satisfaga estas dos condiciones será necesariamente isomorfo al producto cartesiano $\prod_{\alpha\in I} A_\alpha$.

Un caso particular de esta construcción resulta cuando $A_\alpha = A$ para todo $\alpha \in I$. En esta situación, $\prod_{\alpha \in I} A_\alpha$ es el anillo de funciones A^I. Recordemos que en este anillo el producto y la suma se definen a partir de las operaciones de A.

Ejemplo. Si G es un grupo y k un anillo, considerar k^G.

2.6 Localización

En esta sección analizaremos la construcción de $\mathbb{Q}$ a partir de $\mathbb{Z}$ "agregando" los inversos multiplicativos de los enteros no nulos. Veremos generalizaciones de esta construcción y la interpretación geométrica que se le puede dar en ciertos ejemplos, que motiva el nombre de localización.

Cuando se trabaja con números enteros, hay operaciones que no se pueden realizar, como invertir elementos que no sean ni 1 ni -1. Por ejemplo, una ecuación de la forma $ax = b$, con $a \neq 0$, no siempre se puede resolver, porque no podemos "pasar a dividiendo". Si uno mira esa ecuación en $\mathbb{Q}$ no tiene ningún problema, la resuelve, y la solución es un número racional. Lo que se realizó al pasar de $\mathbb{Z}$ a $\mathbb{Q}$ es invertir todos los elementos no nulos de $\mathbb{Z}$. Además, $\mathbb{Q}$ es de alguna manera un anillo minimal con la propiedad de contener a $\mathbb{Z}$ y a los inversos de los números no nulos. Más precisamente (o más categóricamente):

Proposición 2.6.1. *El par $(\mathbb{Z}, i : \mathbb{Z} \to \mathbb{Q})$ tiene las siguientes dos propiedades:*

(a) Si $n \in \mathbb{Z}$ es un elemento no nulo, entonces $i(n) = \frac{n}{1}$ es una unidad de $\mathbb{Q}$.

(b) Si $f : \mathbb{Z} \to B$ es un morfismo de anillos tal que para todo entero $n \neq 0$, $f(n)$ es una unidad de B, entonces existe un único morfismo de anillos $\overline{f} : \mathbb{Q} \to B$ tal que $\overline{f} \circ i = f$.

Demostración. Es claro que si existe un morfismo de anillos de $\mathbb{Q}$ en otro anillo B, éste debe ser único, ya que $f\left(\frac{1}{1}\right) = 1_B$. Para ver la existencia, definamos

$$\overline{f}\left(\tfrac{m}{n}\right) = f(m)f(n)^{-1}.$$

Esto tiene sentido porque la hipótesis es que $f(n)$ es inversible en B para todo $n \neq 0$. Dejamos como ejercicio verificar que este morfismo $\overline{f}$ cumple las condiciones del enunciado. □

La construcción en general se hará según las siguientes líneas: dado un subconjunto S (con ciertas propiedades) de un anillo conmutativo A se buscará otro anillo y una aplicación de A en éste de manera tal que la imagen de S esté incluida en las unidades. La construcción seguirá la intuición de escribir fracciones $\frac{a}{s}$ con elementos $a \in A$ y $s \in S$, sumando y multiplicando como fracciones.

Definición 2.6.2. Sea $S \subset A$ un subconjunto de un anillo A. S es *multiplicativamente cerrado* si:

(a) para cada par de elementos $s, t \in S$ se tiene que $st \in S$; y
(b) $1 \in S$.

La primera propiedad es la que motiva el nombre de multiplicativamente cerrado, si S la satisface pero $1 \notin S$, entonces $S' = S \cup \{1\}$ verifica ambas.

Fijemos un anillo A conmutativo y un subconjunto $S \subset A$ multiplicativamente cerrado. Tratamos de construir a partir de A y S un anillo A_S en el que todo elemento de S sea inversible (en el caso anterior, es $A = \mathbb{Z}$, $S = \mathbb{Z} - \{0\}$ y resulta $A_S = \mathbb{Q}$) y tal que exista un morfismo de anillos $A \to A_S$ que factorice todo morfismo de anillos con dominio A tal que las imágenes de los $s \in S$ sean inversibles.

Consideremos el conjunto cociente

$$A_S = \{(a, s) \in A \times A : a \in A,\, s \in S\}/\sim,$$

de $A \times A$ bajo la relación de equivalencia $\sim$ tal que un par (a, s) es equivalente a otro (a', s') sii existe $t \in S$ tal que $(as' - a's)t = 0$. (Verificar que es una relación de equivalencia; ¿qué propiedades de S se usan para eso?) Escribiremos a/s a la clase de equivalencia $\overline{(a, s)}$.

Definimos ahora sobre A_S operaciones suma y producto de manera que

$$a/s + a'/s' = (as' + a's)/ss'$$

y

$$(a/s) \cdot (a'/s') = (aa')/(ss')$$

Ejercicio. Verificar que las operaciones están bien definidas y que hacen de A_S un anillo.

Hay un morfismo de anillos $i : A \to A_S$ tal que $i(a) = a/1$. Es fácil ver que la imagen por i de todo $s \in S$ es inversible en A_S, con inverso $1/s$. Además, si B es otro anillo y $f : A \to B$ es un morfismo anillos tal que $f(s) \in \mathcal{U}(B)$ para todo $s \in S$, entonces existe un único morfismo $\overline{f} : A_S \to B$ tal que $\overline{f} \circ i = f$: $\overline{f}$ puede ser definido por $\overline{f}(a/s) = f(a)(f(s))^{-1}$.

Ejemplos.

1. Si A es un anillo conmutativo y $S \subseteq \mathcal{U}(A)$, entonces $A_S \cong A$.

2. Si $0 \in S$, entonces $A_S = \{0\}$ porque $a/s = 0/1$ si y sólo si existe $t \in S$ tal que $t(a - s) = 0$, lo cual siempre es cierto si $0 \in S$.

3. Sea $A = \mathbb{Z}$, $S = \{1, 2, 2^2, \dots\} = \{2^i : i \in \mathbb{N}_0\}$. Entonces

$$A_S = \{m/2^i : m \in \mathbb{Z},\, i \in \mathbb{Z}\} = \mathbb{Z}[\frac{1}{2}].$$

4. Sean A un anillo conmutativo y $\mathfrak{p}$ un ideal primo de A. El conjunto $S = A - \mathfrak{p}$ es un subconjunto multiplicativamente cerrado, precisamente porque $\mathfrak{p}$ es primo. En este caso denotamos $A_{\mathfrak{p}}$ a la localización A_S. El subconjunto $\{a/s \in A_S : a \in \mathfrak{p}\}$ es un ideal maximal de $A_{\mathfrak{p}}$ y es además el único ideal maximal de este anillo, que por lo tanto es un anillo local. Puede verse que los ideales primos de $A_{\mathfrak{p}}$ están en correspondencia biunívoca con los ideales primos de A contenidos en $\mathfrak{p}$.

5. Sea X un espacio topológico (por ejemplo, $\mathbb{R}$ con la topología usual), $A = C(X)$ el anillo de funciones reales continuas sobre X y sean $x_0 \in X$ y $S = \{f \in A : f(x_0) \neq 0\}$. Entonces

$$A_S = \{f/g : f, g \in A,\, g(x_0) \neq 0\}/\sim .$$

Observemos que estamos usando la notación f/g en este caso de forma coherente con la notación dada para localizaciones y no para indicar cociente de funciones definidas sobre X.

Supongamos que $f_1, f_2 \in A$ son tales que $f_1/1 \sim f_2/1$ en A_S. Existe entonces $h \in S$ tal que $h(f_1 - f_2) = 0$. Como $h \in S$, $h(x_0) \neq 0$. Como además h es continua, existe un entorno U de x_0 en X tal que $h|_U \neq 0$. Esto nos dice que si $x \in U$, $h(x)$ es inversible en $\mathbb{R}$ y como $h(x)(f_1(x) - f_2(x)) = 0$, concluimos que $f_1(x) = f_2(x)$.

Esto nos dice que dos funciones $f_1, f_2 \in A$ tienen la misma imagen en A_S sii existe un entorno U' de x_0 sobre el cual coinciden.

Este último ejemplo, además de motivar el nombre de *localización*, muestra que la aplicación $i : A \to A_S$ no siempre es inyectiva.

2.7 Ejercicios

Definiciones

2.7.1. Sea A un conjunto y $+, \cdot : A \times A \to A$ dos operaciones en A que satisfacen todos los axiomas de la definicion de anillos salvo posiblemente aquel que dice que el grupo $(A, +)$ es abeliano. Muestre que $(A, +, \cdot)$ es un anillo.

2.7.2. *(a)* Si A es un anillo en el que cada elemento tiene un inverso a izquierda, entonces A es un anillo de división.

(b) Sea A un anillo y $a \in A$ un elemento que es inversible a izquierda y que no divide a 0 por la derecha. Entonces a es inversible.

(c) Sea $a \in A$. Si existe $n \in \mathbb{N}$ tal que a^n es inversible, entonces a es inversible.

2.7.3. Sea A un anillo posiblemente sin unidad. Muestre que si A posee una única unidad a izquierda e, entonces A posee una unidad.

Sugerencia. Sea $a \in A$ y considere para cada $c \in A$ el elemento $(e - ae - a)c$.

2.7.4. Describa, a menos de isomorfismo, todos los anillos con a lo sumo 10 elementos.

2.7.5. Sea k un cuerpo algebraicamente cerrado. Entonces no existen k-álgebras de dimensión finita que no tengan divisores de cero.

2.7.6. Sea k un cuerpo algebraicamente cerrado. Describa, a menos de isomorfismo, todas las k-álgebras de dimensión a lo sumo 3.

Ejemplos

2.7.7. *Anillo opuesto.*

(a) Sea A un anillo. Sea $* : A \times A \to A$ la operación definida por

$$a * b = ba, \qquad \forall a, b \in A.$$

Mostrar que $(A, +, *)$ es un anillo. Se trata del *anillo opuesto de* A, que escribimos habitualmente A^{op}.

(b) Muestre con un ejemplo que en general $A \ncong A^{\mathrm{op}}$.

2.7.8. *Anillos de matrices.*

(a) Sea A un anillo y sea $n \in \mathbb{N}$. El conjunto de matrices $M_n(A)$ con coeficientes en A es un anillo con respecto a las operaciones usuales de suma y producto de matrices. Si $n > 1$, entonces $M_n(A)$ no es conmutativo.

(b) Sea otra vez A un anillo y sea $M_\infty(A) = \{f : \mathbb{N} \times \mathbb{N} \to A\}$. Decimos que un elemento $f \in M_\infty(A)$ tiene *filas finitas* si para cada $n \in \mathbb{N}$, existe $k \in \mathbb{N}$ tal que $f(n, m) = 0$ si $m > k$; de manera similar, decimos que $f \in M_\infty(A)$ tiene *columnas finitas* si para cada $m \in \mathbb{N}$, existe $k \in \mathbb{N}$ tal que $f(n, m) = 0$ si $n > k$.

Sean $M_\infty^f(A)$ y $M_\infty^c(A)$ los subconjuntos de $M_\infty(A)$ de las matrices con filas finitas y con columnas finitas, respectivamente, y sea $M_\infty^{fc}(A) = M_\infty^f(A) \cap M_\infty^c(A)$. Mostrar que con el producto "usual" de matrices, $M_\infty^f(A)$, $M_\infty^c(A)$ y $M_\infty^{fc}(A)$ son anillos.

2.7.9. *Anillos de funciones.*

(a) Sea A un anillo y X un conjunto no vacío. Sea X^A el conjunto de todas las funciones $X \to A$. Definimos dos operaciones $+, \cdot : A \times A \to A$ poniendo

$$(f + g)(x) = f(x) + g(x), \qquad \forall x \in X$$

y

$$(f \cdot g)(x) = f(x)g(x), \qquad \forall x \in X$$

para cada $f, g \in A^X$. Mostrar que $(A, +, \cdot)$ es un anillo. ¿Cuándo es conmutativo?

(b) Sea $n \in \mathbb{N}$, $k \in \mathbb{N}_0$ y sea $C^k(\mathbb{R}^n) \subset (\mathbb{R}^n)^{\mathbb{R}}$ el conjunto de todas las funciones $f : \mathbb{R}^n \to \mathbb{R}$ continuas y derivables k veces. Muestre que se trata de un subanillo.

2.7.10. *Anillos de polinomios.* Sea A un anillo y sea

$$S = \{f : \mathbb{N}_0 \to A : \text{existe } X \subset \mathbb{N}_0 \text{ finito tal que } f|_{\mathbb{N}_0 \setminus X} \equiv 0\}.$$

Definimos $+, \cdot : S \times S \to S$ poniendo, para cada $f, g \in S$ y cada $n \in \mathbb{N}_0$,

$$(f+g)(n) = f(n) + g(n)$$

y

$$(f \cdot g)(n) = \sum_{\substack{k,l \geq 0 \\ k+l=n}} f(k)g(l).$$

Muestre que estas operaciones están bien definidas y que $(S, +, \cdot)$ es un anillo.

Sea X es una variable. Si $f \in S$ y $X \subset \mathbb{N}_0$ es finito y tal que $f|_{\mathbb{N}_0 \setminus X} \equiv 0$, podemos representar a f por la suma finita formal

$$f = \sum_{n \in X} f(n) X^n.$$

Es fácil ver que usando esta notación las operaciones de S se corresponden con las operaciones usuales de polinomios. Por eso, llamamos a S el *anillo de polinomios con coeficientes en* A y lo notamos $A[X]$.

2.7.11. *Anillos de series formales.*

(a) Sea A un anillo y sea $S = \{f : \mathbb{N}_0 \to A\}$ el conjunto de todas las funciones de $\mathbb{N}_0$ a A. Definimos operaciones $+, \cdot : S \times S \to S$ poniendo, para cada $f, g \in S$ y cada $n \in \mathbb{N}_0$,

$$(f+g)(n) = f(n) + g(n)$$

y

$$(f \cdot g)(n) = \sum_{\substack{k,l \geq 0 \\ k+l=n}} f(k)g(l).$$

Muestre que $(S, +, \cdot)$ es un anillo.

Sea X una variable. Podemos representar escribimos a una función $f \in S$ por una serie formal

$$f = \sum_{n \in \mathbb{N}0} f(n) X^n.$$

Usando esta notación, las definiciones de la suma y el producto de S imitan formalmente a las correspondientes operaciones con las series. Esto hace que llamemos a S el *anillo de series formales de potencias con coeficientes en* A. La notación usual para este anillo es $A[\![X]\!]$.

(b) Tomamos ahora $A = \mathbb{R}$ y sea $\mathbb{R}\{\{X\}\} \subset \mathbb{R}[\![X]\!]$ el subconjunto de las series formales que tienen radio de convergencia positivo. Mostrar que se trata de un subanillo.

2.7.12. *Series de Dirichlet.* Sea A un anillo y sea $S = \{f : \mathbb{N} \to A\}$ el conjunto de todas las funciones de $\mathbb{N}$ a A. Definimos operaciones $+, \cdot : S \times S \to S$ poniendo, para cada $f, g \in S$ y cada $n \in \mathbb{N}$,

$$(f + g)(n) = f(n) + g(n)$$

y

$$(f \cdot g)(n) = \sum_{\substack{d \in \mathbb{N} \\ d|n}} f(d)g(n/d).$$

Muestre que $(S, +, \cdot)$ es un anillo.

Si s es una variable, a un elemento $f \in S$ podemos asignarle la expresion formal

$$f = \sum_{n \in \mathbb{N}} \frac{f(n)}{n^s}.$$

Las operaciones de S se corresponden entonces con las operaciones evidentes de estas series.

2.7.13. *Anillo de grupo.*

(a) Sea G un grupo, sea A un anillo y sea $A[G]$ el conjunto de todas las funciones de $f : G \to A$ tales que

$$|\{g \in G : f(g) \neq 0\}| < \infty.$$

Definimos operaciones $+, \cdot : A[G] \times A[G] \to A[G]$ poniendo, para cada $s, t \in A[G]$ y cada $g \in G$,

$$(s + t)(g) = s(g) + t(g)$$

y

$$(s \cdot t)(g) = \sum_{h \in G} s(gh^{-1})t(h).$$

Muestre que $(A[G], +, \cdot)$ es un anillo.

(b) Supongamos desde ahora que $A = k$ es un cuerpo. Mostrar que $k[G]$ es un subespacio vectorial del espacio vectorial k^G de todas las funciones $G \to k$.

(c) Si $g \in G$, sea $\hat{g} : G \to k$ la función tal que

$$\hat{g}(h) = \begin{cases} 1, & \text{si } g = h; \\ 0, & \text{en caso contrario.} \end{cases}$$

Mostrar que $\{\hat{g} : g \in G\}$ es una base de $k[G]$. En particular, mostrar que todo elemento $f \in k[G]$ puede escribirse en la forma

$$f = \sum_{g \in G} \alpha_g \, \hat{g}$$

con coeficientes $\alpha_g \in k$ casi todos nulos.

(d) Mostrar que si $g, h \in G$, entonces $\hat{g} \cdot \hat{h} = \widehat{gh}$.

(e) Describa el centro de $k[G]$ cuando G es finito. ¿Qué pasa cuando G es infinito?

2.7.14. *Álgebra de cuaterniones.* Sea k un cuerpo y sea $\mathbb{H} = k^4$. Sean 1, i, j y k los vectores de la base canónica de $\mathbb{H}$. Mostrar que existe exactamente un producto asociativo k-bilineal $\cdot : \mathbb{H} \times \mathbb{H} \to \mathbb{H}$ tal que 1 es el elemento unidad y

$$\begin{aligned} &i^2 = j^2 = k^2 = 1, \\ &ij = -ji = k, \qquad jk = -kj = i, \qquad ki = -ik = j. \end{aligned}$$

Si queremos poner en evidencia el cuerpo k, escribimos $\mathbb{H}(k)$.

(a) Muestre que con este producto $\mathbb{H}$ es una k-álgebra.

(b) Muestre que $\mathbb{H}(k)$ es conmutativa sii k tiene característica 2.

(c) Determine el centro de $\mathbb{H}$.

(d) Si $u = \alpha 1 + \beta i + \gamma j + \delta k$, sea $\bar{u} = \alpha 1 - \beta i - \gamma j - \delta k$. Muestre que de esta manera obtenemos un anti-automorfismo de k-álgebras $\iota : u \in \mathbb{H} \mapsto \bar{u} \in \mathbb{H}$; esto es, muestre que ι es un isomorfismo de k-espacios vectoriales tal que

$$\overline{uv} = \overline{v}\,\overline{u}.$$

(e) Muestre que existe una función $N : \mathbb{H} \to k$ tal que

$$u\,\bar{u} = N(u)1, \qquad \forall u \in \mathbb{H}.$$

Además, si $u, v \in \mathbb{H}$, entonces $N(uv) = N(u)N(v)$.

(f) Muestre que si $u \in \mathbb{H}$ es tal que $N(u) \neq 0$, entonces u es inversible en $\mathbb{H}$.

(g) Muestre que $\mathbb{H}(\mathbb{R})$ es un álgebra de división pero que $\mathbb{H}(\mathbb{C})$ no lo es.

2.7.15. *Algebras de caminos.*

(a) Un *carcaj* Q es una 4-upla (Q_0, Q_1, s, t) en la que:

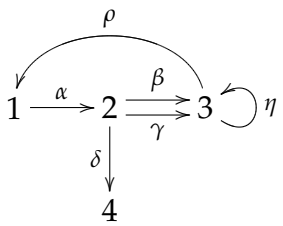
— Q_0 y Q_1 son conjuntos. Los elementos de Q_0 son los *vértices* de Q y los de Q_1 las *flechas*.

— s y t son funciones $Q_1 \to Q_0$. Si $\alpha \in Q_1$ es una flecha, decimos que $s(\alpha)$ es el *origen* de α y que $t(\alpha)$ es su final.

Por ejemplo, obtenemos un carcaj si ponemos $Q = (Q_0, Q_1, s, t)$ con $Q_0 = \{1, 2, 3, 4\}$, $Q_1 = \{\alpha, \beta, \gamma, \delta, \eta, \rho\}$ y s y t están dados por la tabla siguiente:

	α	β	γ	δ	η	ρ
s	1	2	2	2	3	3
t	2	3	3	4	3	1

Podemos describir este carcaj más eficientemente dando el siguiente dibujo:



Fijemos un carcaj Q. Si $x, y \in Q_0$, un *camino de x a y en Q* es una secuencia finita $\gamma = (x; \alpha_1, \dots, \alpha_n; y)$ de flechas de Q tal que $s(\alpha_1) = x$, $t(\alpha_n) = y$ y para cada $i \in \{1, \dots, n-1\}$ se tiene que $t(\alpha_i) = s(\alpha_{i+1})$. El número n es la *longitud* de γ. En particular, si $x \in Q_0$, hay un camino $(x; ; x)$ de x a x de longitud 0.

Sea $P(Q)$ el conjunto de todos los caminos de Q, sea k un cuerpo y sea kQ el espacio vectorial que tiene a $P(Q)$ como base. Un elemento $u \in kQ$ es una combinación lineal finita de caminos de Q con coeficientes en k:

$$u = \sum_{\gamma \in P(Q)} a_\gamma \gamma.$$

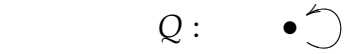
Muestre que hay exactamente una forma de definir un producto asociativo $\cdot : kQ \times kQ \to kQ$ de manera que para cada par de caminos $\gamma = (x; \alpha_1, \ldots, \alpha_n; y)$ y $\eta = (z; \beta_1, \ldots, \beta_m; w)$ en Q, es

$$\gamma \cdot \eta = \begin{cases} (x; \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m; w), & \text{si } y = z; \\ 0, & \text{en caso contrario.} \end{cases}$$

Mostrar que, con este producto, kQ es una k-álgebra. ¿Cuál es la unidad de esta álgebra? Llamamos a kQ la *k-álgebra de caminos de Q*.

(b) Si Q tiene un solo vértice y ninguna flecha, entonces $kQ = k$

(c) Si Q tiene un solo vertice y una única flecha, entonces kQ es isomorfo a $k[X]$, el anillo de polinomios en una variable con coeficientes en k.

Q : 

(d) *k-álgebras libres.* Sea X un conjunto y sea Q el carcaj (Q_0, Q_1, s, t) en el que Q_0 tiene un único elemento p, $Q_1 = X$ y las aplicaciones s, $t : Q_1 \to Q_0$ son las evidentes. Escribimos $L(X)$ en vez de kQ. Describa una base de $L(X)$ y su multiplicación

(e) ¿Cuándo es kQ un dominio de integridad? ¿Cuándo tiene dimensión finita? ¿Cuándo es conmutativa?

(f) Describa el centro de kQ.

2.7.16. *(a)* Sea A un anillo y $\mathcal{C}$ una familia de subanillos de A. Muestre que $B = \bigcap_{C \in \mathcal{C}} C$ es un subanillo de A.

(b) Sea A un anillo, $B \subset A$ un subanillo y $X \subset A$. Mostrar que existe un subanillo $B[X]$ de A que contiene a X y a B y tal que todo otro subanillo de A con esta propiedad contiene a $B[X]$.

(c) Tomemos $A = \mathbb{C}$, $B = \mathbb{Z}$. Describa explícitamente los anillos $B[\sqrt{2}]$, $B[\sqrt[3]{5}]$ y $B[\omega]$ si ω es una raíz primitiva p-ésima de la unidad y p un número primo. Describa $B[i]$ y $B[\eta]$ si η es una raíz primitiva sexta de la unidad.

2.7.17. *El álgebra de Weyl.* Sea $\mathrm{End}_{\mathbb{C}}(\mathbb{C}[X])$ el anillo de endomorfismos de $\mathbb{C}[X]$ considerado como $\mathbb{C}$-espacio vectorial y consideremos los elementos $p, q \in \mathrm{End}_{\mathbb{C}}(\mathbb{C}[X])$ definidos de la siguiente manera: si $f \in \mathbb{C}[X]$, entonces

$$p(f) = \frac{\mathrm{d}f}{\mathrm{d}X}, \qquad \text{y} \qquad q(f) = Xf$$

y sea $A = \mathbb{C}[p, q]$ el menor subanillo de $\mathrm{End}_{\mathbb{C}}(\mathbb{C}[X])$ que contiene a $\mathbb{C}$, a p y a q. Llamamos a A el *álgebra de Weyl*.

(a) A es una $\mathbb{C}$-álgebra de dimensión infinita.

(b) En A es $pq - qp = 1$.

(c) El conjunto $\{p^i q^j : i, j \in \mathbb{N}_0\}$ es una base de A como $\mathbb{C}$-espacio vectorial.

(d) Describa el centro de A.

(e) Muestre que A no posee divisores de cero.

(f) Describa el conjunto de unidades de A.

2.7.18. *El álgebra de funciones en el plano cuántico.* Sea $q \in \mathbb{C} \setminus 0$ y supongamos que q no es una raíz de la unidad. Sea $V = \{f : \mathbb{N}_0 \to \mathbb{C}\}$ el $\mathbb{C}$-espacio vectorial de todas las funciones de $\mathbb{N}_0$ en $\mathbb{C}$. Consideramos dos elementos $x, y \in \mathrm{End}_{\mathbb{C}}(V)$ definidos de la siguiente manera: si $f \in V$ y $n \in \mathbb{N}_0$, entonces $x(f), y(f) : \mathbb{N}_0 \to \mathbb{C}$ son tales que

$$\big(x(f)\big)(n) = q^n f(n)$$

y

$$\big(y(f)\big)(n) = f(n+1).$$

Sea $A_q = \mathbb{C}[x, y]$ la menor subálgebra de $\mathrm{End}_C\, C(V)$ que contiene a $\mathbb{C}$, a x y a y. Llamamos a A_q el *álgebra de funciones en el plano cuántico*.

(a) En A_q vale que $yx = qxy$.

(b) El conjunto $\{x^i y^j : i, j \in \mathbb{N}_0\}$ es una base de A_q.

(c) Se tiene que $\mathcal{Z}(A_q) = \mathbb{C}$.

(d) Muestre que no hay en A_q divisores de cero.

(e) Describa el conjunto de unidades de A_q.

†*(f)* Para cada $n \in \mathbb{N}$ definimos

$$(n)_q = \frac{q^n - 1}{q - 1}.$$

Ponemos, además, $(0)_q! = 1$ y si $n \in \mathbb{N}$,

$$(n)_q! = (1)_q (2)_q \cdots (n)_q.$$

Finalmente, si $n \in \mathbb{N}_0$ y $0 \leq k \leq n$, ponemos

$$\binom{n}{k}_q = \frac{(n)_q!}{(k)_q!(n-k)_q!}.$$

Muestre que:

(i) Si $0 \leq k \leq n$, es

$$\binom{n}{k}_q = \binom{n}{n-k}_q.$$

(ii) Si $0 \leq k \leq n$, entonces

$$\binom{n}{k}_q = \binom{n-1}{k-1}_q + q^k \binom{n-1}{k}_q = \binom{n-1}{k}_q + q^{n-k} \binom{n-1}{k-1}_q.$$

(iii) Si $0 \leq k \leq n$, $\binom{n}{k}_q$ es un polinomio en q con coeficientes enteros.

(iv) Sean $x, y \in A_q$ los generadores del álgebra de funciones del plano cuántico. Si $n > 0$, entonces

$$(x + y)^n = \sum_{0 \leq k \leq n} \binom{n}{k}_q x^k y^{n-k}.$$

†*(g)* ¿Qué pasa si q es una raíz primitiva de la unidad de orden e?

2.7.19. Sea X un conjunto. Mostrar que $(\mathcal{P}(X), \triangle, \cap)$ es un anillo. Aquí $\triangle$ es la operación de diferencia simétrica.

2.7.20. *Idempotentes.* Sea A un anillo. Un elemento $e \in A$ es *idempotente* si $e^2 = e$.

(a) Si $e \in A$ es idempotente, el subconjunto eAe, con las operaciones de A restringidas, es un anillo. Se trata de un subanillo exactamente cuando $e = 1$.

(b) Si $e \in A$ es idempotente, entonces $1 - e$ también lo es.

2.7.21. *Anillos booleanos.* Un anillo A es *booleano* si todos sus elementos son idempotentes.

(a) Si X es un conjunto, entonces el anillo $(\mathcal{P}(X), \triangle, \cap)$ es booleano.

(b) Un anillo booleano es conmutativo.

†**2.7.22.** *Álgebras de division reales.* El objetivo de este ejercicio es probar el siguiente teorema de Ferdinand Georg Frobenius (1849–1917, Prusia):

Teorema 2.7.1. *Sea D una $\mathbb{R}$-álgebra de división tal que $\dim_{\mathbb{R}} D < \infty$. Entonces D es isomorfa a $\mathbb{R}$, a $\mathbb{C}$ o a $\mathbb{H}$.*

La conclusión del teorema vale más generalmente (y con exactamente la misma demostración) para una $\mathbb{R}$-álgebra de división arbitraria si suponemos que es *algebraica* sobre $\mathbb{R}$: esto es, si para todo elemento $d \in D$ existe $p \in \mathbb{R}[X]$ tal que $p(d) = 0$.

(a) Si $\dim_{\mathbb{R}} D = 1$ no hay nada que hacer, así que suponga que $\dim_{\mathbb{R}} D > 1$. Sea $a \in D \setminus \mathbb{R}$. Muestre que $\mathbb{R}[a] \subset D$ es un cuerpo y que debe ser isomorfo a $\mathbb{C}$. En particular, concluya que existe $i \in D \setminus \mathbb{R}$ tal que $i^2 = -1$. Identifiquemos a $\mathbb{C}$ con $\mathbb{R}[i]$.

(b) Definamos subespacios

$$D^+ = \{d \in D : di = id\}$$

y

$$D^- = \{d \in D : di = -id\}$$

de D. Muestre que $D = D^+ \oplus D^-$.

(c) Claramente $\mathbb{C} \subset D^+$. Si $d \in D^+ \setminus \mathbb{C}$, muestre que $\mathbb{C}[d]$ es un cuerpo que contiene a $\mathbb{C}$. Concluya que $D^+ = \mathbb{C}$.

(d) Si $D^- = 0$, entonces $D = \mathbb{C}$. Supongamos desde ahora que $D^- \neq 0$. Sea $z \in D^-$ y consideremos la aplicación

$$s : d \in D^- \mapsto dx \in D^+.$$

Muestre que es $\mathbb{C}$-lineal e inyectiva, de manera que debe ser $\dim_{\mathbb{C}} D^- = 1$. Concluya que $\dim_{\mathbb{R}} D = 4$.

(e) Muestre que existe $j \in D^-$ tal que $j^2 = -1$. Concluya que $D \cong \mathbb{H}$.

†**2.7.23.** *Álgebras de division finitas.* El objetivo de este ejercicio es mostrar el siguiente teorema de Joseph Henry Maclagen Wedderburn (1882–1948, Escocia):

Teorema 2.7.2. *Un anillo de división finito es un cuerpo.*

(a) Sea $\mu : \mathbb{N} \to \mathbb{Z}$ la función de Möbius, de manera que si $n \in \mathbb{N}$ y $n = p_1^{r_1} \cdots p_k^{r_k}$ es la descomposición de n como producto de potencias de primos distintos,

$$\mu(n) = \begin{cases} 1, & \text{si } n = 1; \\ (-1)^k, & \text{si } p_1 = \cdots = p_k = 1; \\ 0, & \text{si } r_i > 1 \text{ para algún } i. \end{cases}$$

Muestre que si $n, m \in \mathbb{N}$ son coprimos, entonces se tiene que $\mu(nm) = \mu(n)\mu(m)$. Decimos por esto que μ es una función *multiplicativa*.

(b) Sea $M : n \in \mathbb{N} \mapsto \sum_{d|n} \mu(d) \in \mathbb{Z}$. Muestre que si $n, m \in \mathbb{N}$ son coprimos, entonces $M(nm) = M(n)M(m)$, de manera que M tambñien es multiplicativa. Muestre además que $M(1) = 1$ y que si p es primo y $r \in \mathbb{N}$, entonces $M(p^r) = 0$.

Concluya que vale la siguiente *identidad de Möbius*:

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{si } n = 1; \\ 0, & \text{en caso contrario.} \end{cases}$$

(c) Sea $n \in \mathbb{N}$. Sea $\Omega_n = \{w \in \mathbb{C} : w^n = 1\}$ el conjunto de las raíces n-ésimas de la unidad y sea $\Omega_n^* \subset \Omega_n$ el subconjunto

de Ω_n formado por aquellas que son primitivas. Recordemos que $X^n - 1 = \prod_{\omega \in \Omega_n}(X - \omega)$. Sea $\Phi_n \in \mathbb{C}[X]$ dado por

$$\Phi_n = \prod_{\omega \in \Omega_n^*} (X - \omega).$$

Muestre que $X^n - 1 = \prod_{d|n} \Phi_d(X)$ y, usando eso, que

$$\Phi_n = \prod_{d|n} (X^d - 1)^{\mu(d)}.$$

Concluya que $\Phi_n \in \mathbb{Z}[X]$.

(d) Muestre que si $q \in \mathbb{Z} \setminus \{1\}$ y $n, r \in \mathbb{N}$ son tales que $r \mid n$, entonces

$$\Phi_n(q) \;\Big|\; \frac{q^n - 1}{q^r - 1}.$$

(e) Sea D un anillo de división finito y sea F su centro. Muestre que F es un cuerpo y que D es un F-espacio vectorial de dimensión finita. Sean $q = |F|$ y $n = \dim_F D$, de manera que $|D| = q^n$ y $|D^\times| = q^n - 1$.

Supongamos que D no es conmutativo. Debe ser entonces $n > 1$.

(f) Sea $a \in D$ y sea

$$\mathcal{C}(a) = \{d \in D : da = ad\}.$$

Muestre que $\mathcal{C}(a)$ es un subanillo de D que es de división y que contiene a F. Otra vez, se trata de un F-espacio vectorial. Sea $r(a) = \dim_F \mathcal{C}(A)$. Entonces es $|\mathcal{C}(a)| = q^{r(a)}$ y, como $\mathcal{C}(a)$ es de división, $|\mathcal{C}(a)^\times| = q^{r(a)} - 1$. Como $\mathcal{C}(a)^\times$ es un subgrupo de $D^\times$, debe ser $q^{r(a)} - 1 \mid q^n - 1$. Concluya que $r(a) \mid n$.

(g) Si $a \in D^\times$, entonces la clase $\mathrm{cl}(a)$ de conjugación de a en el grupo $D^\times$ tiene cardinal

$$|\mathrm{cl}(a)| = \frac{q^n - 1}{q^{r(a)} - 1}.$$

(h) Sean $a_1, \ldots, a_l$ representantes de las clases de conjugación no triviales de $D^\times$. Entonces la ecuación de clases para $D^\times$ es:

$$q^n - 1 = q - 1 + \sum_{i=1}^{l} \frac{q^n - 1}{q^{r(a)} - 1}.$$

y vemos que $\Phi_n(q) \mid (q - 1)$.

(i) En particular,

$$q - 1 \geq |\Phi_n(q)| = \prod_{\omega \in \Omega_n^*} |q - \omega|.$$

Muestre que esto es imposible.

Morfismos, ideales y cocientes

2.7.24. Sea A un anillo.

(a) Muestre que hay exactamente un morfismo de anillos $\mathbb{Z} \to A$.

(b) Muestre que hay a lo sumo un morfismo de anillos $\mathbb{Q} \to A$ y que puede no haber ninguno. Describa cuándo se da cada uno de estos dos casos.

2.7.25. Sea A un anillo.

(a) Si $\mathcal{I}$ es una familia de ideales a izquierda (a derecha, biláteros) de A, muestre que $\bigcap_{I \in \mathcal{I}} I$ es un ideal a izquierda (a derecha, bilatéro) de A. Se trata del ideal más grande contenido en cada elemento de $\mathcal{I}$.

(b) Si $\mathcal{I}$ es una familia de ideales a izquierda (a derecha, biláteros) de A, entonces $\sum_{I \in \mathcal{I}} I$ es un ideal a izquierda (a derecha, bilátero) de A. Se trata del ideal más chico que contiene a todos los elementos de $\mathcal{I}$.

2.7.26. Sea A un anillo e $I \subset A$ un ideal a izquierda. Muestre que existe un subanillo $\mathbb{I}(I) \subset A$ tal que

- $I \subset \mathbb{I}(I)$ e I es un ideal bilátero de $\mathbb{I}(I)$;
- $\mathbb{I}(I)$ es el menor subanillo de A con esa propiedad.

Llamamos a $\mathbb{I}(I)$ el *idealizador de I en A*.

2.7.27. *(a)* Sea A un anillo conmutativo e $I \subset A$ un ideal. Sea

$$\sqrt{I} = \{a \in A : \text{existe } r \in \mathbb{N} \text{ tal que } a^r \in I\}.$$

Muestre que $\sqrt{I}$ es un ideal de A.

(b) Sea A un anillo conmutativo e I, $J \subset A$ ideales. Sea

$$(I : J) = \{a \in A : aJ \subset I\}$$

Muestre que $(I : J)$ es un ideal de A.

2.7.28. Sea A un anillo conmutativo

(a) Sea $a \in A$ un elemento que no es inversible. Mostrar que existe un ideal maximal $\mathfrak{m} \subset A$ tal que $a \in \mathfrak{m}$.

(b) Sea $I \subset A$ un ideal propio. Mostrar que existe un ideal maximal $\mathfrak{m} \subset A$ tal que $I \subset \mathfrak{m}$.

2.7.29. Muestre que un anillo conmutativo simple es un cuerpo.

2.7.30. Sea A un anillo y $I \subset A$ un ideal bilátero. Sea $J = (I)$ el ideal generado por I en $A[X]$. Muestre que $A[X]/J \cong (A/I)[X]$.

2.7.31. Sea A un anillo y $I \subset A$ un ideal bilátero. Sea $n \in \mathbb{N}$ y sea $M_n(I) \subset M_n(A)$ el subconjunto de las matrices de $M_n(A)$ que tienen todos sus coeficientes en I. Mostrar que $M_n(I)$ es un ideal bilátero de $M_n(A)$ y que $M_n(A)/M_n(I) \cong M_n(A/I)$.

2.7.32. Sea k un cuerpo.

(a) Encuentre todos los ideales a izquierda de $M_n(k)$.

(b) Muestre que $M_n(k)$ es simple.

(c) Sea ahora A un anillo y $n \in \mathbb{N}$. Si $J \subset M_n(A)$ es un ideal bilátero, entonces existe un ideal bilátero $I \subset A$ tal que $J = M_n(I)$.

Sugerencia. Sea $\mathbf{n} = \{1, \dots, n\}$. Sea $J \subset M_n(A)$ un ideal bilátero y, para cada $(i, j) \in \mathbf{n} \times \mathbf{n}$, sea $I_{i,j} \subset A$ el conjunto de todos los elementos de A que aparecen en la coordenada (i, j)-ésima de algún elemento de J. Muestre que $I_{i,j}$ es un ideal bilátero en A y que de hecho $I_{i,j} = I_{1,1}$ para todo $(i, j) \in \mathbf{n} \times \mathbf{n}$. Llamemos $I = I_{1,1}$. Muestre que $J = M_n(I)$.

2.7.33. Sea G un grupo y sea $H \subset G$ un subgrupo normal y sea k un cuerpo. Consideremos la proyección canónica $\pi : G \to G/H$.

Muestre que π determina un morfismo sobreyectivo de anillos $k[\pi] : k[G] \to k[G/H]$. Describa el núcleo de $k[\pi]$.

2.7.34. Sea k un cuerpo y considere el carcaj Q de n vértices de la figura:

$$1 \longrightarrow 2 \longrightarrow \quad \cdots \quad \longrightarrow n-1 \longrightarrow n$$

Sea $T_n \subset M_n(k)$ el subanillo de las matrices triangulares superiores. Muestre que $kQ \cong T_n$.

2.7.35. Sea $f : \mathbb{R} \to \mathbb{R}$ un homomorfismo de anillos.

(a) Muestre que $f(\mathbb{Q}) \subset \mathbb{Q}$ y que, de hecho, $f|_{\mathbb{Q}} = \mathsf{Id}_{\mathbb{Q}}$.

(b) La aplicación f es estrictamente creciente.

(c) Más aún, f es continua. Concluya que $f = \mathrm{Id}_{\mathbb{R}}$.

2.7.36. En cada uno de los siguientes casos, decidir si existe un homomorfismo de anillos $f : A \to B$:

(a) $A = \mathbb{Z}[i]$ y $B = \mathbb{R}$;

(b) $A = \mathbb{Z}[\sqrt{-5}]$ y $B = \mathbb{Z}[\sqrt{3}]$;

(c) $A = k$, un cuerpo, y $B = M_n(k)$;

(d) $A = M_n(k)$ con k un cuerpo y $B = k$.

2.7.37. Sea $G_3 = \{1, t, t^2, \text{con } t^3 = 1\}$, $A = \mathbb{R}[G_3]$.

(a) Sea $e = \frac{1}{3}(1 + t + t^2)$ y $e' = (1 - e)$. Ver que $e^2 = e$, $e'^2 = e'$ y $ee' = 0 = e'e$.

(b) Sea B el anillo eA y C el anillo $e'A$ con la multiplicación inducida por la de A. ¿Por qué no son subanillos de A? Probar que la aplicación

$$\begin{aligned} A &\to B \times C \\ a &\mapsto (ea, e'a) \end{aligned}$$

define un isomorfismo de anillos, si $B \times C$ tiene la suma y producto coordenada a coordenada.

(c) Ver que B tiene dimensión 1 sobre $\mathbb{R}$ y que C tiene dimensión 2. Una base de B es por ejemplo $\{e\}$ y una base de C es $\{e', f\}$, donde $f = t - t^2 = e'(t - t^2)$. Mostrar además que las siguientes aplicaciones son isomorfismos de anillos:

(a) $(e(x1 + yt + zt^2) \in B \mapsto x + y + z\mathbb{R}$;

(b) $(ae' + bj) \in C \mapsto a + bi \in \mathbb{C}$, donde $j = \frac{f}{\sqrt{3}}$.

2.7.38. Sea $A = \mathbb{C}[G_3]$, sea $\omega \in \mathbb{C}$ una raíz cúbica primitiva de la unidad y pongamos

$$\begin{aligned} e_1 &= \frac{1}{3}(1 + t + t^2), \\ e_2 &= \frac{1}{3}(1 + \omega t + \omega^2 t^2), \\ e_3 &= \frac{1}{3}(1 + \omega^2 t + \omega t^2). \end{aligned}$$

Probar que:

(a) $e_i e_j = 0$ si $i \neq j$ y $e_i^2 = e_i$ si $i, j \in \{1, 2, 3\}$;

(b) $e_1 + e_2 + e_3 = 1$;

(c) los anillos $e_i A$ tienen dimensión compleja igual a uno y son isomorfos a $\mathbb{C}$ como anillos;

(d) la aplicación

$$\begin{aligned} A &\to e_1\mathbb{C} \times e_2\mathbb{C} \times e_3\mathbb{C} \\ a &\mapsto (e_1 a, e_2 a, e_3 a) \end{aligned}$$

es un isomorfismo de anillos, dotando a $e_1\mathbb{C} \times e_2\mathbb{C} \times e_3\mathbb{C}$ de las operaciones coordenada a coordenada.

2.7.39. Sea $n \in \mathbb{N}$ compuesto. ¿Existe un producto $\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ que haga del grupo abeliano $\mathbb{Z}_n$ un cuerpo?

Definición. Sea A un anillo conmutativo. Decimos que un ideal $\mathfrak{p} \subset A$ es primo si

$$ab \in \mathfrak{p} \implies a \in p \vee b \in p.$$

Escribimos Spec A al conjunto de todos los ideales primos de A.

2.7.40. *(a)* Un ideal $\mathfrak{p} \subset A$ es primo sii $A/\mathfrak{p}$ es un dominio de integridad.

(b) Un ideal maximal de A es primo.

2.7.41. Determine Spec $\mathbb{Z}$. ¿Cuáles ideales primos de $\mathbb{Z}$ son maximales?

2.7.42. Sea k un cuerpo. Muestre que si $\mathfrak{p} \in$ Spec $k[X]$, entonces existe $f \in \mathfrak{p}$ mónico e irreducible tal que $\mathfrak{p} = (f)$. Recíprocamente, todo ideal principal generado por un polinómio mónico e irreducible es primo en $k[X]$.

2.7.43. Sea A un anillo conmutativo.

(a) Si $\mathfrak{p} \in$ Spec A y $B \subset A$ es un subanillo, $B \cap \mathfrak{p} \in$ Spec B.

(b) Si $I \subset A$ es un ideal, $f : A \to A/I$ es la proyección canónica y $\mathfrak{p} \in$ Spec A/I, entonces $f^{-1}(\mathfrak{p}) \in$ Spec A.

(c) Sea $I \subset A$ un ideal y $\mathfrak{p} \in$ Spec A es tal que $\mathfrak{p} \supset I$. Entonces $\mathfrak{p}/I \in$ Spec A/I.

2.7.44. Muestre que si $\mathfrak{p} \in \operatorname{Spec} \mathbb{Z}[X]$ entonces existe un número primo $p \in \mathbb{N}$ tal que o bien $\mathfrak{p} = (p)$ o bien existe un polinomio $f \in \mathbb{Z}[X]$ mónico e irreducible sobre $\mathbb{Z}$ tal que $\mathfrak{p} = (p, f)$.

Sugerencia. Sea $\mathfrak{p} \in \operatorname{Spec} \mathbb{Z}[X]$. Muestre que $\mathfrak{p} \cap \mathbb{Z}$ es un ideal principal de $\mathbb{Z}$ generado por un número primo p, así que en particular $(p) \subset \mathfrak{p}$. Considere ahora el ideal $\mathfrak{p}/(p)$ de $\mathbb{Z}[X]/(p) \cong \mathbb{Z}_p[X]$ y use un ejercicio anterior que describe los ideales primos de este anillo.

2.7.45. *Nilradical.* Sea A un anillo conmutativo. Un elemento $a \in A$ es *nilpotente* si existe $n \in \mathbb{N}$ tal que $a^n = 0$. El *nilradical de* A es el conjunto $\operatorname{nil}(A) = \{a \in A : a \text{ es nilpotente}\}$.

(a) $\operatorname{nil}(A)$ es un ideal de A.

(b) $\operatorname{nil}(A/\operatorname{nil}(A)) = 0$.

(c) $\operatorname{nil}(A) = \bigcap_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}$.

(d) Muestre que si $x \in \operatorname{nil}(A)$, entonces $1 + x$ es inversible.

2.7.46. *Radical de Jacobson.* Sea A un anillo conmutativo. El *radical de Jacobson de* A es la intersección $J(A)$ de todos los ideales maximales de A. Muestre que $x \in J(A)$ sii para cada $y \in A$ es $1 - xy \in A^\times$.

Localización

En estos ejercicios los anillos son conmutativos.

2.7.47. Sea A un anillo y sea $S \subset A^\times$ un subconjunto multiplicativamente cerrado de unidades de A. Entonces $A_S \cong A$.

2.7.48. Sea A un anillo y sea $S \subset A$ un subconjunto multiplicativamente cerrado. Si $0 \in S$, entonces $A_S \cong 0$.

2.7.49. Sea A un anillo, $S \subset A$ un subconjunto multiplicativamente cerrado e $I \subset A$ un ideal. Sea $\bar{S}$ la imagen de S por la aplicación canónica $A \to A/I$. Entonces $(A/I)_{\bar{S}} \cong A_S/IA_S$.

2.7.50. Sea A un anillo, $S, T \subset A$ subconjuntos multiplicativamente cerrados de A y sea T' la imagen de T por la aplicación canónica $A \to A_S$. Sea $U = ST = \{st : s \in S,\, t \in T\}$.

Muestre que U es un conjunto multiplicativamente cerrado en A y que $(A_S)_T \cong A_U$.

2.7.51. *(a)* Sea X un espacio topológico y sea $A = C_{\mathbb{R}}(X)$ el anillo de las funciones reales continuas sobre X. Sea $x_0 \in X$ y ponga-

mos $S = \{f \in A : f(x_0) \neq 0\}$. Muestre que S es multiplicativamente cerrado. ¿Es inyectiva la aplicación canónica $A \to A_S$? De no serlo, describa su núcleo.

(b) Supongamos que A es un dominio de interidad y $S \subset A$ es multiplicativamente cerrado. Muestre que la aplicación canónica $A \to A_S$ es inyectiva.

(c) Sea A un anillo y $S \subset A$ un subconjunto multiplicativamente cerado. Dé condiciones necesarias y suficientes para que la aplicación canónica $A \to A_S$ sea inyectiva.

2.7.52. Sea A un anillo y $\mathfrak{p} \in \operatorname{Spec} A$. Muestre que $S = A \setminus \mathfrak{p}$ es un conjunto multiplicativamente cerrado. En geeral, escribimos $A_\mathfrak{p}$ en lugar de $A_{A\setminus\mathfrak{p}}$.

2.7.53. Sea $A = \mathcal{C}(\mathbb{R})$, $U = (0,1)$ y $S = \{f \in A : \forall t \in U,\ f(t) \neq 0\}$.

(a) S es multiplicativamente cerrado en A.

(b) Sea $r : \mathcal{C}(\mathbb{R}) \to \mathcal{C}(U)$ la restricción de funciones. Muestre que existe $\bar{r} : \mathcal{C}(\mathbb{R})_S \to \mathcal{C}(U)$ tal que conmuta el diagrama:

$$\begin{array}{ccc} \mathcal{C}(\mathbb{R}) & \xrightarrow{r} & \mathcal{C}(U) \\ {\scriptstyle \text{can}}\downarrow & \nearrow_{\bar{r}} & \\ \mathcal{C}(\mathbb{R})_S & & \end{array}$$

Además, verifique que $\bar{r}$ es inyectiva.

(c) Muestre que $\bar{r}$ es sobreyectiva.

2.7.54. Sea A un anillo, $S \subset A$ un subconjunto multiplicativamente cerrado y sea $f : A \to A_S$ la aplicación canónica.

(a) Muestre que si $I \subset A_S$ es un ideal, entonces $f^{-1}(I)$ es un ideal de A.

(b) De esta forma, se obtiene una aplicación $f^* : \mathsf{Id}(A_S) \to \mathsf{Id}(A)$ del conjunto de ideales de A_S al conjunto de ideales de A. Muestre que f^* preserva inclusiones e intersecciones y que es inyectiva.

(c) Si $J \subset A$ es un ideal, entonces J está en la imagen de f^* sii $J = f^{-1}(JA_S)$ sii ningún elemento de S es un divisor de cero en A/J.

(d) Muestre que $f^*(\text{Spec } A_S) \subset \text{Spec } A$ de manera que, por restricción, obtenemos una inyección $f^* : \text{Spec } A_S \to \text{Spec } A$. La imagen de esta aplicación es exactamente el conjunto

$$\{\mathfrak{p} \in \text{Spec } A : \mathfrak{p} \cap S = \varnothing\}.$$

2.7.55. Sea A un anillo y $S \subset A$ un subconjunto multiplicativamente cerrado.

(a) Si $I \subset A$ es un ideal maximal entre los que no intersecan a S, entonces I es primo.

(b) Describa el niradical de A_S.

2.7.56. Sea $p \in \mathbb{N}$ un número primo y $\mathfrak{p} = (p)$ el ideal primo de $\mathbb{Z}$ correspondiente. Muestre que si $I \subset \mathbb{Z}_{\mathfrak{p}}$ es un ideal no nulo, entonces existe $r \in \mathbb{N}_0$ tal que $I = p^r\mathbb{Z}_p$.

2.7.57. Sea A un anillo y $T \subset A$ un subconjunto. Sea $X = \{x_t\}_{t\in T}$ un conjunto de variables indexadas por T y sea $A[X]$ en anillo de polinomios con variables en X. Sea $S \subset A$ el menor subconjunto multiplicativamente cerrado de A que contiene a T. Muestre que hay un isomorfismo

$$A_S \cong A[X]/\left\langle tx_t - 1 : t \in T\right\rangle.$$

†**2.7.58.** Sea A un anillo. Muestre que $S \subset A$ es un subconjunto multiplicativamente cerrado maximal sii $A \setminus S$ es un ideal primo minimal.

†**2.7.59.** Sea A un anillo y $S \subset A$ un subconjunto multiplicativamente cerrado. Decimo que S es *saturado* si

$$ab \in S \iff a \in S \quad \text{y} \quad b \in S.$$

Muestre que S es saturado sii $A \setminus S$ es unión de ideales primos.

2.7.60. Sea A un anillo. Describa el subconjunto $S \subset A$ multiplicativamente cerrado maximal tal que $A \to A_S$ es inyectivo.

2.7.61. Sea la aplicación $A \to \prod_{\mathfrak{m}} A_{\mathfrak{m}}$ dada por $a \mapsto \{\frac{a}{1}\}_{\mathfrak{m}}$, donde $\mathfrak{m}$ recorre el conjunto de ideales maximales de A y cada $\frac{a}{1}$ pertenece al $A_{\mathfrak{m}}$ correspondiente. Ver que esa aplicación es inyectiva.

Sugerencia. Si a es inversible en A, ver que $\frac{a}{1}$ es distinto de cero en cualquier localización; si no, entonces existe un maximal M que contiene a a, ver que $\frac{a}{1} \neq 0$ en el localizado por ese maximal.

Capítulo 3

Módulos

3.1 Primeras definiciones y ejemplos

Dado un anillo A, nos interesa estudiar su categoría de representaciones, que está formada por objetos llamados módulos en los cuales A actúa, y por funciones entre tales objetos que respetan la acción de A.

Sabemos que si $(M, +)$ es un grupo abeliano, entonces

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

con el producto dado por composición de funciones, es un anillo.

Definición 3.1.1. Un *A-módulo* a izquierda es un grupo abeliano $(M, +)$ provisto de un morfismo de anillos

$$\begin{aligned} \rho : A &\to \mathrm{End}_{\mathbb{Z}}(M) \\ a &\mapsto \rho_a \end{aligned}$$

En otras palabras, dar una estructura de A-módulo a un grupo abeliano M es asignar a cada elemento $a \in A$ una endomorfismo del grupo M. La condición de que esta asignación sea un morfismo de anillos dice que:

- $\rho_1 = \mathsf{Id}_M$.
- $\rho_{ab} = \rho_a \circ \rho_b$.
- $\rho_{a+b} = \rho_a + \rho_b$.

Ejemplos.
1. Cualquiera sea A, podemos tomar $M = A$ y $\rho_a(b) = ab$.

2. Si $A = k$ es un cuerpo y V un k-espacio vectorial, V resulta un A-módulo si definimos $\rho_\lambda(v) = \lambda v$.

3. Si M es un grupo abeliano, entonces $\mathrm{End}_{\mathbb{Z}}(M)$ es un anillo y por lo tanto existe un único morfismo de anillos $\mathbb{Z} \to \mathrm{End}_{\mathbb{Z}}(M)$. Luego todo grupo abeliano es, de manera única, un $\mathbb{Z}$-módulo.

Explícitamente, el morfismo $\rho : \mathbb{Z} \to \mathrm{End}_{\mathbb{Z}}(M)$ que da esta estructura es tal que, si $n > 0$, $\rho_n(m) = m + m + \cdots + m$, con n sumandos.

4. Si G es un grupo que actúa por morfismos de grupos en un grupo abeliano M, entonces M es un $\mathbb{Z}[G]$-módulo tomando $\rho_g(m) = gm$ si $g \in G$ y $m \in M$, y extendiendo ρ linealmente a todo $\mathbb{Z}[G]$. Habitualmente, llamamos a los $\mathbb{Z}[G]$-módulos *representaciones lineales* de G.

5. Si V es un k-espacio vectorial y G es un subgrupo de $\mathrm{GL}(V)$, entonces V es un $k[G]$-módulo.

Otra manera de mirar la estructura de A-módulo a izquierda de un grupo abeliano $(M, +)$ es pensar que se tiene una función $A \times M \to M$ que asigna a cada par (a, m) un elemento am, donde am es una notación para designar a $\rho_a(m)$. El hecho de que ρ sea un morfismo de anillos $A \to \mathrm{End}_{\mathbb{Z}}(M)$ es equivalente a que, para cada $a, b \in A$, y $x, y \in M$, se tenga

- $1x = x$,
- $(ab)m = a(bm)$,
- $(a + b)m = am + bm$, y
- $a(x + y) = ax + ay$.

Se puede tomar estas últimas cuatro propiedades de una función $A \times M \to M$ como definición de la estructura de A-módulo a izquierda. La equivalencia entre las dos definiciones es inmediata.

Ejemplos.
1. Para cualquier anillo A, el grupo abeliano $\{0\}$ es un A-módulo.

2. Si M es un grupo abeliano y $A = \mathrm{End}_{\mathbb{Z}}(M)$ entonces M es un A-módulo con acción $(f, m) \in \mathrm{End}_{\mathbb{Z}}(M) \times M \mapsto f(m) \in M$. Dejamos como ejercicio verificar que esta acción corresponde al morfismo de anillos $\mathsf{Id} : A \to \mathrm{End}_{\mathbb{Z}}(M)$.

3. Si I es un conjunto y M un A-módulo, el grupo abeliano M^I de todas las funciones $f : I \to M$ posee una estructura de A-módulo tal que si $a \in A$ y $f \in M^I$, entonces $af : I \to M$ la función tal que $(af)(i) = af(i)$ para cada $i \in I$.

4. $\mathsf{M}_n(A)$ es un A-módulo con $(am)_{ij} = am_{ij}$.

5. Si V es un k-espacio vectorial de dimensión n, entonces es un $\mathsf{M}_n(k)$-módulo (¿por qué?).

6. Si A es un anillo y $n \in \mathbb{N}$, $M = A^n$ es un A-módulo y también un $\mathsf{M}_n(A)$-módulo. En ambos casos, la multiplicación por escalares del anillo está dada por la multiplicación matricial.

Observación. En un A-módulo M se tiene que

- $a0 = 0$ para todo $a \in A$;
- $0m = 0$ para todo $m \in M$; y
- $(-a)m = -(am)$ para todo $a \in A$ y $m \in M$.

Dejamos la verificación como un ejercicio para el lector.

De manera similar a lo hecho arriba, se puede definir sobre un grupo abeliano una estructura de *A-módulo a derecha*, a partir de una función $M \times A \to M$ que verifique propiedades simétricas a las que cumple una acción a izquierda.

Ejercicio. Escribir explícitamente la definición de A-módulo a derecha, ver que equivale a tener una función $A \to \mathrm{End}_{\mathbb{Z}}(M)$ con ciertas propiedades y escribir esas propiedades.

Sean A un anillo conmutativo y sea M un A-módulo a izquierda. En este caso, podemos definir sobre M una estructura de A-módulo a derecha poniendo $ma = am$. Es fácil erificar que esto define en efecto una estructura de A-módulo a derecha. ¿Qué sucede cuando A no es conmutativo?

Ejemplo. Sea $A = \mathsf{M}_n(\mathbb{C})$ y consideremos la aplicación

$$(-)^* : (a_{ij}) \in \mathsf{M}_n(\mathbb{C}) \mapsto (\overline{a}_{ij})^t \in \mathsf{M}_n(\mathbb{C}).$$

Esto es, sea, para cada $a \in \mathsf{M}_n(\mathbb{C})$, a^* la matriz transpuesta conjugada de a.

Sea ahora M un A-módulo. Se puede dotar a M de una estructura de A-módulo a derecha con acción dada por

$$(m, a) \in M \times \mathsf{M}_n(\mathbb{C}) \mapsto a^* m \in M.$$

Dejamos al lector verificar que ésto efectivamente da una estructura de A-módulo a derecha. ¿Qué propiedades de la función $(-)^*$ se usaron?

Observación. M es un A-módulo a izquierda si y solo si M es un A^{op}-módulo a derecha.

Definición 3.1.2. Sean A y B dos anillos. Un *A-B-bimódulo* M es un grupo abeliano M que es a la vez un A-módulo a izquierda y un B-módulo a derecha y cuyas dos estructuras son tales que

$$(am)b = a(mb)$$

siempre que $a \in A$, $b \in B$ y $m \in M$.

Ejemplos.
1. Si A es conmutativo, todo A-módulo M es un A-A-bimódulo.
2. Todo A-módulo (por ejemplo a izquierda) es un A-$\mathbb{Z}$-bimódulo.
3. A es un A-A-bimódulo.
4. Sea $M = \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Se trata de un $\mathsf{M}_2(\mathbb{Z}_2)$-módulo a derecha con la acción dada por la multiplicación de matrices.

   Sea $(-)^t : \mathsf{M}_2(\mathbb{Z}_2) \to \mathsf{M}_2(\mathbb{Z}_2)$ la transposición de matrices. Sabemos que $(ab)^t = b^t a^t$ si $a, b \in \mathsf{M}_2(\mathbb{Z}_2)$. Usando esto, es fácil ver que podemos hacer de M un $\mathsf{M}_2(\mathbb{Z}_2)$-módulo a *derecha* definiendo

$$(m, a) \in M \times \mathsf{M}_2(\mathbb{Z}_2) \mapsto a^t m \in M.$$

Dejamos al lector verificar que, con estas dos acciones de $\mathsf{M}_2(\mathbb{Z}_2)$ sobre M, M *no* es un bimódulo.

Ejercicio. Sea M un A-módulo a derecha y sea $B = \mathrm{End}_A(M)$. Mostrar que la acción $(f, m) \in \mathrm{End}_A(M) \times M \mapsto f(m) \in M$ define sobre M una estructura de $\mathrm{End}_A(M)$-módulo a izquierda y que M resulta un $\mathrm{End}_A(M)$-A-bimódulo.

Supongamos ahora que $M = A^{n\times 1}$, esto es, A^n visto como conjunto de 'vectores columna'. Entonces M es un A-módulo a derecha y también un $\mathsf{M}_n(A)$-módulo a izquierda con la multiplicación usual de matrices. Mostrar que esta estructura coincide con la definida antes, vía la identificación $\mathrm{End}_A(A^n) \cong \mathsf{M}_n(A)$.

Observación. En adelante, A-módulo querrá decir A-módulo a izquierda.

Definición 3.1.3. Sea A un anillo y M un A-módulo. Un subconjunto $N \subset M$ es un *submódulo* si

- N es un subgrupo de $(M, +)$; y
- $an \in N$ siempre que $a \in A$ y $n \in N$.

Se sigue de esta definición que si N es un submódulo de un A-módulo M, entonces N es, en si mismo, un A-módulo.

Ejemplos.
1. $\{0\}$ y M son siempre submódulos de M. En caso de que un módulo M tenga solamente a $\{0\}$ y a M como submódulos, diremos que M es *simple*. Por ejemplo, un k-espacio vectorial de dimension 1 es un k-módulo simple.

2. Si G es un grupo y $H \subseteq G$ es un subgrupo, entonces $k[G]$ es un $k[H]$-módulo y $k[H]$ es un $k[H]$-submódulo de $k[G]$.

3. Consideremos el grupo de las raíces cúbicas de la unidad

$$G_3 = \{1, \omega, \omega^2\} \subset \mathbb{C}^\times$$

y dotemos a $\mathbb{R}^3$ de la única estructura de $\mathbb{R}[G_3]$-módulo tal que $\omega(x, y, z) = (y, z, x)$. Entonces

$$N = \{(x, y, z) \in \mathbb{R}^3 : x + y + z = 0\}$$

es un $\mathbb{R}[G_3]$-submódulo. Es fácil ver que, además, N es un módulo simple.

4. Si $N \subseteq M$ es un A-submódulo e I es un conjunto, entonces N^I es un A-submódulo de M^I.

5. Si M es un A-módulo e I es un conjunto, consideramos el subconjunto $M^{(I)}$ de M^I formado por los elementos $\{m_i\}_{i \in I}$ tales que $m_i = 0$ para todos los elementos i de I salvo eventualmente una cantidad finita de ellos. Dejamos como ejercicio mostrar que $M^{(I)}$ es un submódulo de M^I.

6. Si $M = \mathsf{M}_n(A)$ con la estructura de A-módulo coordenada a coordenada, entonces el subconjunto $\mathfrak{sl}(A) = \{A \in A : \operatorname{tr} A = 0\}$ es un A-submódulo.

Observación. Si N_1 y N_2 son dos submódulos de M, entonces

$$N_1 + N_2 = \{x + y : x \in N_1,\, y \in N_2\}$$

es un submódulo de M, así como también lo es $N_1 \cap N_2$.

Sea M un A-módulo y sea $X \subset M$ un sobconjunto arbitrario. Es claro que si $N \subset M$ es un submódulo tal que $X \subset N$, entonces N contiene todos los elementos de la forma

$$a_1x_1 + \cdots a_nx_n$$

con $a_1, \ldots, a_n \in A$ y $x_1, \ldots, x_n \in X$. Por otro lado, el conjunto

$$S = \{a_1x_1 + \cdots a_nx_n : a_1, \ldots, a_n \in A,\, x_1, \ldots, x_n \in X\}$$

es un submódulo de M (¡verificarlo!). Esto nos dice que S es el menor (en el sentido de la inclusión) submódulo de M que contiene a X. Lo notamos $\langle X \rangle$ y lo llamamos el *submódulo generado por* X. Si $X = \{x_1, \ldots, x_n\}$ es finito, escribimos $\langle x_1, \ldots, x_n \rangle$ en lugar de $\langle X \rangle$.

3.2 Submódulos maximales

Un A-módulo M es *finitamente generado* o de *tipo finito* cuando existen $x_1, \ldots, x_n \in M$ tales que $\langle x_1, \ldots, x_n \rangle = M$.

Ejemplo. Todo anillo A considerado como módulo sobre si mismo es trivialmente finitamente generado, con generador 1_A pero, por ejemplo, $k[X]$ no es finitamente generado sobre k.

Veremos a continuación, usando el lema de Zorn, que dado un submódulo propio de un A-módulo finitamente generado, siempre existe un submódulo maximal que lo contiene. Como caso particular de esta situación, dado un ideal propio a izquierda de un anillo, siempre existe un ideal maximal (a izquierda) que lo contiene, ya que los ideales a izquierda de A son exactamente los A-submódulos de A visto como módulo a izquierda.

Proposición 3.2.1. *Si M es un A-módulo finitamente generado y N es un submódulo propio de M, entonces N está contenido en un submódulo maximal.*

Demostración. Sea $P = \{S : S \text{ es submódulo propio de } M \text{ y } N \subseteq S\}$, parcialmente ordenado por inclusión. P es no vacío porque $N \in P$.

Queremos ver que P posee elementos maximales. Sea $\mathcal{C}$ una cadena creciente no vacía en P y sea $V = \bigcup_{S\in\mathcal{C}} S$. Como la cadena $\mathcal{C}$ es creciente, V es un submódulo de M. Es claro que V contiene a N y a todos los elementos de $\mathcal{C}$. Para ver que V es un elemento de P bastará entonces probar que es un submódulo propio.

Supongamos que $V = M$. Como M es finitamente generado, existen $n \in \mathbb{N}$ y $x_1, \ldots, x_n \in M$ tales que $M = \langle x_1, \ldots, x_n\rangle$. Como cada x_i pertenece a V, cada x_i pertenece a algún elemento de $\mathcal{C}$. Como la cadena $\mathcal{C}$ es creciente y n es finito, existe $S \in \mathcal{C}$ tal que $x_1, \ldots, x_n \in S$. Pero como los x_i generan a M, resulta $S = M$ y esto contradice que $S \in \mathcal{C} \subset P$. Concluimos que $V \subsetneq M$.

El lema de Zorn nos dice entonces que P posee un elemento maximal con respecto al orden dado por la inclusión. Este submódulo es un submódulo maximal como se buscaba. □

Ejemplo. Consideremos un conjunto X provisto con una acción de un grupo G. Sea k un anillo y

$$k^{(X)} = \{ \sum_{\lambda_x\in k} \lambda_x x : \lambda_x = 0 \text{ para casi todo } x \in X\}.$$

Se trata de un k-módulo, que además es un $k[G]$-módulo (¡verificarlo!) con respecto a la única acción $k[G] \times k^{(X)} \to k^{(X)}$ tal que

$$g \cdot \lambda x = \lambda g(x).$$

Por ejemplo, sea $G = \mathbb{Z}_n$ (escrito multiplicativamente) y $t \in G$ es un generador, de manera que $G = \{t^i : 0 \leq i < n\}$, y consideremos el conjunto $X = \{x_1, \ldots, x_n\}$ y la acción de G sobre X tal que

$$t \cdot x_i = \begin{cases} x_{i+1}, & \text{si } i < n; \\ x_1, & \text{si } i = n. \end{cases}$$

Entonces $k^{(X)} \cong k^n$ resulta un $k[\mathbb{Z}_n]$-módulo extendiendo linealmente esta acción.

¿Cuáles son los $k[G]$-submódulos de $k^{(X)}$? Por ejemplo, si S es un submódulo que contiene a x_{i_0}, entonces $tx_{i_0} = x_{i_0+1} \in S$, de

la misma forma, $x_i \in S$ cualquiera sea i. Vemos que en este caso $S = M$.

Esto nos dice que un submódulo propio de $k^{(X)}$ no puede contener a nunguno de los x_i. En cambio, si $\tau = x_1 + \cdots + x_n$, entonces $\langle \tau \rangle = \{\lambda\tau : \lambda \in k\}$ es un submódulo propio si $n > 1$.

Ejercicio. Si $\omega \in k$ es una raíz n-ésima de la unidad (por ejemplo $\omega = 1$, o $\omega = -1$ si n es par, o $\omega = e^{\frac{2k\pi i}{n}}$ si $k = \mathbb{C}$) entonces el k-submódulo generado por $\sum_{i=1}^{n} \omega^i x_i$ es también un $k[G]$-submódulo de $k^{(X)}$.

Observación. Existen módulos finitamente generados con submódulos que no son de tipo finito. Consideremos, por ejemplo, un cuerpo k, y el anillo $A = k[x_i]_{i\in\mathbb{N}}$. Como A-módulo, A es claramente finitamente generado pero el ideal $N \subset A$ generado por todos los x_i no es de tipo finito.

3.3 Morfismos

Dado un anillo A, podemos construir una categoría que tiene como objectos a los A-módulos y como morfismos a las funciones entre A-módulos que respetan la estructura de A-módulos. Más precisamente,

Definición 3.3.1. Sean A un anillo, M y N dos A-módulos y sea $f : M \to N$ una función. Diremos entonces que f es un *morfismo* de A-módulos si es un morfismo de grupos abelianos A-lineal, es decir, si:

- $f(x + y) = f(x) + f(y)$ para todo $x, y \in M$; y
- $f(ax) = af(x)$ para todo $a \in A$ y $x \in M$.

Observemos que en la igualdad de la segunda condición, la acción que aparece a la izquierda es la de A sobre M y la que aparece a la derecha es la de A sobre N.

Ejemplos.
1. Para todo A-módulo M, la aplicación identidad $\mathsf{Id}_M : M \to M$ es un morfismo de A-módulos. Por otro lado, si $f : M \to N$ y

$g : N \to T$ son dos morfismos de A-módulos, entonces (¡verificarlo!) $g \circ f : M \to T$ también lo es. Esto nos dice que los A-módulos con sus morfismos como flechas forman una categoría.

2. Si V es un k-espacio vectorial y $t : V \to V$ un endomorfismo, entonces podemos definir sobre V una estructura de $k[X]$-módulo poniendo

$$P \cdot v = P(t)(v), \qquad \forall P \in k[X],\, v \in V.$$

Si W otro espacio vectorial, $s : W \to W$ un endomorfismo de W, y consideramos a W como $k[X]$-módulo como arriba, entonces una transformación lineal $f : V \to W$ es un morfismo de $k[X]$-módulos si y sólo si $f \circ t = s \circ f$.

3. Si M y N son grupos abelianos considerados como $\mathbb{Z}$-módulos, entonces los morfismos de $\mathbb{Z}$-módulos entre M y N son exactamente los morfismos de grupos abelianos.

Observación. Si $f : M \to N$ es un morfismo de A-módulos, entonces $\mathrm{Ker}(f)$ e $\mathrm{Im}(f)$ son submódulos (de M y N, respectivamente). Más aún, para cada submódulo S de M, $f(S)$ es un submódulo de N, y para cada submódulo T de N, $f^{-1}(T)$ es un submódulo de M.

Definición 3.3.2. Un morfismo f de A-módulos es un *isomorfismo* si existe f^{-1}.

Observación. En ese caso es fácil ver que f^{-1} resulta también un morfismo de A-módulos.

Proposición 3.3.3. *Sean M y N dos A-módulos y sea $f : M \to N$ un morfismo de A-módulos. Las siguientes afirmaciones son equivalentes:*

(a) *f es inyectiva.*
(b) $\mathrm{Ker}(f) = \{0\}$.
(c) *Para todo A-módulo T y todo par de morfismos $g, h : T \to M$, la igualdad $f \circ g = f \circ h$ implica que $g = h$.*
(d) *Para todo A-módulo T y para todo morfismo $g : T \to M$, la igualdad $f \circ g = 0$ implica que $g = 0$.*

Demostración. (a) ⇒ (b) Supongamos f es inyectiva y sea $x \in M$ tal que $f(x) = 0 = f(0)$. Entonces, como f es inyectiva, resulta que $x = 0$. Vemos así que $\mathrm{Ker}(f) = 0$.

(b) ⇒ (a) Supongamos ahora que $\mathrm{Ker}(f) = 0$. Sean $x, y \in M$ tales que $x \neq y$, de manera que $x - y \neq 0$. Como el único elemento del núcleo de f es el cero, $f(x) - f(y) = f(x - y) \neq 0$ y, por lo tanto, $f(x) \neq f(y)$.

(b) ⇒ (c) Supongamos que $\mathrm{Ker}(f) = 0$ y consideremos morfismos $g, h : T \to M$ tales que $f \circ g = f \circ h$. Sea $x \in T$ un elemento cualquiera. La hipótesis dice que $f(g(x)) = f(h(x))$ o, equivalentemente, que $f(g(x) - h(x)) = 0$. Luego $g(x) - h(x) \in \mathrm{Ker}(f) = 0$, así que $g(x) - h(x) = 0$. La arbitrariedad de x implica entonces que $g = h$.

(c) ⇒ (d) Esto es claro, tomando $h = 0$.

(d) ⇒ (b) Sea $T = \mathrm{Ker}(f)$ y sea g la inclusión $i_K : \mathrm{Ker}(f) \to M$. Es claro que $f \circ i_K = 0$, así que la hipótesis nos dice que $i_K = 0$. Como i_K es inyectiva y tiene imagen $\{0\}$, resulta $\mathrm{Ker}(f) = \{0\}$, como queríamos. □

Observación. La afirmación *(c)* de la proposición dice que la noción de inyectividad para morfismos de A-módulos coincide con la de monomorfismo categórico en la categoría de A-módulos (ver apéndice). En la categoría de A-módulos la noción de morfismo suryectivo coincide también con la de epimorfismo categórico. Esto lo veremos más adelante, una vez que hayamos caracterizado los objetos cociente.

Definición 3.3.4. Consideremos una sucesión $(M_n, f_n)_{n\in\mathbb{Z}}$ de A-módulos y morfismos $f_n : M_n \to M_{n-1}$. Diremos que la sucesión

$$\cdots \xrightarrow{f_{n+2}} M_{n+1} \xrightarrow{f_{n+1}} M_n \xrightarrow{f_n} M_{n-1} \xrightarrow{f_{n-1}} \cdots$$

es *exacta* en el lugar n si $\mathrm{Ker}(f_n) = \mathrm{Im}(f_{n+1})$. Si la sucesión es exacta en todo lugar diremos simplemente que la sucesión es exacta.

Observaciones.
1. La sucesión

$$0 \longrightarrow M \xrightarrow{f} N$$

es exacta en M si y sólo si f es un monomorfismo.

2. Dualmente, la sucesión

$$M \xrightarrow{f} N \longrightarrow 0$$

es exacta en N si y sólo si f es un epimorfismo.

3. Una clase particular de sucesiones exactas que aparecerá a menudo son las llamadas sucesiones exactas cortas, que son las del tipo

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$$

Decir que esta sucesión es exacta equivale a decir que f es monomorfismo, que g es un epimorfismo y que $\mathrm{Im}(f) = \mathrm{Ker}(g)$.

3.4 Cocientes

Si k es un cuerpo, V un espacio vectorial V y S es un subespacio de V, siempre existe otro subespacio $T \subset V$ tal que $V = S \oplus T$. Por otro lado, si A es un anillo arbitrario y M es un A-módulo, no es cierto que todo submódulo $S \subset M$ siempre posea un complemento: por ejemplo, podemos tomar $A = M = \mathbb{Z}$ y $S = 2\mathbb{Z}$.

En el caso de espacios vectoriales, como $V = S \oplus T$, podemos construir un proyector $p : V \to V$ tal que $\mathrm{Im}(p) = T$, $\mathrm{Ker}(p) = S$ y $p|_T = \mathrm{Id}_T$. Así, aplicando p uno "olvida" a los elementos de S, identificando dos elementos de V que difieran entre si por un elemento de S.

En el caso de módulos, este último punto de vista de identificar elementos que difieran en "un resto" de un submódulo S puede ser llevado a cabo: uno encontrará una aplicación sobreyectiva $\pi : M \to T$ cuyo núcleo sea exactamente S. El módulo T se llamará el cociente de M por S, y en general no habrá una manera de identificarlo con un submódulo de M.

Consideremos un anillo A, un A-módulo M y un submódulo $S \subset M$. Es claro que S es un subgrupo de M (normal porque M es abeliano), así que M/S es un grupo abeliano y tenemos un morfismo sobreyectivo de grupos abelianos $\pi : M \to M/S$. Queremos dar a M/S una estructura de A-módulo de manera que π resulte un morfismo de A-módulos. Notemos que, como π es suryectiva, esta estructura, de existir, es única. Definimos pues la acción de manera que si $a \in A$ y $m \in M$,

$$a \cdot \overline{m} = \overline{am}.$$

Lema 3.4.1. *Con las notaciones anteriores, la acción de A sobre M/S está bien definida.*

Demostración. Supongamos $\overline{m} = \overline{n}$, de manera que $m - n = s \in S$. Entonces $am - an = as \in S$, y $\overline{am} - \overline{an} = \overline{am - an} = \overline{as} = 0$ en M/S, esto es, $\overline{am} = \overline{an}$. □

Ejercicio. Verificar que, con esa acción, M/S es un A-módulo y que π es A-lineal. Observar que en la demostración del lema se utilizó el hecho de que el subgrupo por el que se cocienta es un submódulo. Si M es un A-módulo y S un subgrupo que no es submódulo, no es cierto que M/S admita una estructura de A-módulo que haga de π un morfismo de módulos.

Ejemplos.
1. Si tomamos $A = \mathbb{Z}$, la noción de cociente de $\mathbb{Z}$-módulos coincide con la noción de cociente de grupos abelianos.

2. Sea $A = \mathbb{Z} = M$ y $S = 2\mathbb{Z}$. Entonces $M/S \cong \mathbb{Z}_2$, que no es isomorfo a ningún submódulo de M.

3. Si V es un espacio vectorial y $V = S \oplus T$, entonces $V/S \cong T$.

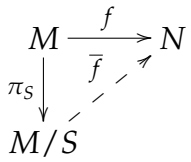
4. Si $M = A = k[X]$ y $S = \langle X - a \rangle = \{(X - a)p : p \in k[X]\}$, entonces $\mathrm{ev}_a : P \in k[X] \mapsto P(a) \in k$ es un morfismo sobreyectivo, de manera que $k[X]/\langle x - a \rangle \cong k$. La acción de $k[X]$ sobre k en este caso está dada por $P \cdot \lambda = P(a)\lambda$ para cada $P \in k[X]$ y cada $\lambda \in k$.

Como todo objeto cociente, M/S queda caracterizado por una propiedad universal:

Proposición 3.4.2. *Dados un A-módulo M y un submódulo S, el par $(M/S, \pi_S : M \to M/S)$ tiene las siguientes dos propiedades:*

(a) $S \subseteq \mathrm{Ker}(\pi_S)$.

(b) *Si* $f : M \to N$ *es un morfismo de* A*-módulos tal que* $S \subseteq \mathrm{Ker}(f)$*, entonces el siguiente diagrama de flechas llenas se completa de manera única con la flecha punteada:*



esto es, existe un único morfismo $\overline{f} : M/S \to N$ *tal que* $f = \overline{f} \circ \pi_S$.

Observación. Es claro que $\mathrm{Im}(\overline{f}) = \mathrm{Im}(f)$ y $\mathrm{Ker}(\overline{f}) = \pi_S(\mathrm{Ker}(f))$. Luego f es suryectiva si y sólo si $\overline{f}$ es suryectiva y $\overline{f}$ es inyectiva si y sólo si $\mathrm{Ker}(f) = S$.

De manera completamente análoga al caso de grupos se tiene el siguiente corolario:

Corolario 3.4.3. (Teoremas de isomorfismo) *Sea* A *un anillo.*

(a) *Si* M *y* N *son* A*-módulos y* $f : M \to N$ *es un morfismo de* A*-módulos, hay un isomorfismo*

$$\frac{M}{\mathrm{Ker}(f)} \cong \mathrm{Im}(f).$$

(b) *Si* $T \subseteq S \subseteq M$ *son submódulos de* M*, entonces*

$$\frac{M/T}{S/T} \cong M/S.$$

(c) *Si* S *y* T *son dos submódulos de* M*, entonces*

$$\frac{S+T}{S} \cong \frac{T}{S \cap T}.$$

Demostración. La cuenta es idéntica al caso de grupos. Dejamos al lector la verificación de que todos los morfismos que aparecen son A-lineales. □

Ejemplos.
1. Sea V un espacio vectorial de dimensión finita sobre un cuerpo k, $t : V \to V$ un endomorfismo. Supongamos que además existe en V un vector t-cíclico, es decir, un vector $v_0 \in V$ con

$$\langle v_0, t(v_0), t^2(v_0), \dots \rangle = V.$$

Por ejemplo, podemos tomar $k = \mathbb{R}$, $V = \mathbb{R}^3$, $t(x, y, z) = (y, z, x)$ y $v_0 = (1, 0, 0)$.

Consideremos la aplicación

$$\phi : P \in k[X] \mapsto P(t)v_0 \in V.$$

Como v_0 es un vector cíclico, ϕ es sobreyectiva. Por otro lado, si $m_{v_0} \in k[X]$ es el polinomio mónico de grado mínimo tal que es $m_{v_0}(t)(v_0) = 0$, entonces $\mathrm{Ker}(\phi) = \langle m_{v_0} \rangle$. Notemos que como v_0 es un vector t-cíclico, m_{v_0} coincide con el polinomio minimal y con el polinomio característico de t.

Ahora bien, (V, t) es un $k[X]$-módulo a través de t. Es fácil verificar que $(V, t) \cong k[X]/\langle m_{v_0} \rangle$ como $k[X]$-módulos.

2. Sea $I \subset \mathbb{R}$ un subconjunto cerrado y $X \subset \mathbb{R}$ un abierto que contiene a I. Se sabe que toda función continua definida sobre I se puede extender a todo $\mathbb{R}$, así que, en particular, puede extenderse a X. Esto nos dice que el morfismo de restricción $C(X) \to C(I)$ es sobreyectivo. Si

$$I^0 = \{f : X \to \mathbb{R} : f(y) = 0 \text{ para todo } y \in I\}$$

es el núcleo de esta aplicación, resulta que $C(X)/I^0 \cong C(I)$ como $C(X)$-módulos.

Ejercicio. Caracterizar el cociente de $\mathbb{Z}^2$ por el $\mathbb{Z}$-submódulo generado por $(2, 4)$ y $(0, 3)$. Sugerencia: trate de encontrar un morfismo cuyo dominio sea $\mathbb{Z} \oplus \mathbb{Z}$ y que tenga por núcleo el submódulo generado por $(2, 4)$ y $(0, 3)$, y después considere la imagen.

Observación. (Submódulos del cociente) Sea M un A-módulo, S un A-submódulo de M y $\pi : M \to M/S$ la proyección, que es un morfismo de A-módulos. Si T es un submódulo de M, la imagen $\pi(T)$ es un submódulo de M/S. Esta correspondencia no es, en general, uno-a-uno: si $T \subseteq S$, claramente es $\pi(T) = \{0\}$. Recíprocamente,

si T' es un submódulo de M/S, $\pi^{-1}(T')$ es un submódulo de M tal que $S \subseteq \pi^{-1}(T')$.

Dejamos como ejercicio verificar que para si T es un submódulo de M, vale la igualdad:

$$\pi^{-1}(\pi(T)) = \langle T, S \rangle = T + S$$

Demostrar también que, vía π y π^{-1}, los submódulos de M/S están en correspondencia 1-1 con los submódulos de M que contienen a S.

Veremos ahora una caracterización de los epimorfismos:

Proposición 3.4.4. *Sean M y N A-módulos, $f : M \to N$ un morfismo de A-módulos. Las siguientes afirmaciones son equivalentes:*

(a) *f es suryectiva.*
(b) $\operatorname{Coker}(f) = N/\operatorname{Im}(f) = \{0\}$.
(c) *Para todo A-módulo T y para todo par de morfismos $g, h : N \to T$, la igualdad $g \circ f = h \circ f$ implica que $g = h$.*
(d) *Para todo A-módulo T y para todo morfismo $g : N \to T$, la igualdad $g \circ f = 0$ implica que $g = 0$.*

Demostración. *(a) $\Leftrightarrow$ (b)* Esto es claro, porque

$$N/\operatorname{Im}(f) = \{0\} \iff N = \operatorname{Im}(f).$$

(b) $\Rightarrow$ (c) Sean $n \in N$ y g, h como en *(c)*. Como $\operatorname{Im}(f) = N$, existe $m \in M$ tal que $n = f(m)$. La hipótesis hecha sobre g y h dice que $g(f(m)) = h(f(m))$, así que $g(n) = h(n)$ para cualquier $n \in N$, esto es, $g = h$.

(c) $\Rightarrow$ (d) Es claro tomando $h = 0$.

(d) $\Rightarrow$ (b) Supongamos que vale *(d)* y tomemos $T = N/\operatorname{Im}(f)$ y $g = \pi : N \to N/\operatorname{Im}(f)$. Claramente $\pi \circ f = 0$, así que $\pi = 0$, pero como π es suryectiva, $N/\operatorname{Im}(f) = \{0\}$. □

Observación. La parte *(c)* de esta proposición demuestra, como fue anticipado, que la noción de morfismo suryectivo coincide con la noción de epimorfismo categórico. Esto no sucede en otras categorías: por ejemplo, en la categoría de espacios métricos y funciones continuas como morfismos, una función con imagen densa es un epimorfismo categórico. Un ejemplo más algebraico es el de la categoría de anillos y morfismos de anillos. En esta categoría, dado un

anillo B y un morfismo $\mathbb{Q} \to B$, la imagen del 1 tiene que ser necesariamente 1_B. Usando la linealidad, vemos inmediatamente que el morfismo queda unívocamente determinado en $\mathbb{Z}$, y la multiplicatividad implica que queda determinado sobre todo $\mathbb{Q}$. En particular todo morfismo queda determinado por su restricción a $\mathbb{Z}$, por lo tanto la inclusión $\mathbb{Z} \to \mathbb{Q}$ es un epimorfismo categórico.

Ejercicio. Si

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$$

es una sucesión exacta corta, entonces $M \cong \mathrm{Ker}(g)$ y $T \cong \mathrm{Coker}(f)$. Además, si N es finitamente generado, T también lo es.

Definición 3.4.5. Si A un anillo conmutativo y M es un A-módulo, la *torsión* de M es el conjunto

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

Observación. Si A es íntegro, $t(M)$ es un A-submódulo de M.

Definición 3.4.6. Un A-módulo M se dice *de torsión* si $t(M) = M$ y *sin torsión* si $t(M) = 0$.

Ejemplos.
1. Si $n \in \mathbb{N}$, $\mathbb{Z}_n$ es de torsión como $\mathbb{Z}$-módulo pero sin torsión como $\mathbb{Z}_n$-módulo.

2. Todo k-espacio vectorial es sin torsión sobre k.

3. Si A es un dominio íntegro y M es un A-módulo, $M/t(M)$ es sin torsión.

Si A es un dominio íntegro y M es un A-módulo, hay una sucesión exacta de A-módulos:

$$0 \longrightarrow t(M) \xrightarrow{i} M \xrightarrow{\pi} M/t(M) \longrightarrow 0$$

Terminamos esta sección mencionando otra dirección en la que se pueden generalizar las nociones de monomorfismo y epimorfismo en el contexto de espacios vectoriales.

Si $f : V \to W$ es una transformación lineal entre dos espacios vectoriales que es un monomorfismo, entonces f induce un isomorfismo entre V e $\mathrm{Im}(f)$, que es un subespacio de W. Como para cualquier subespacio de un espacio vectorial se puede encontrar un complemento, si escribimos $W = \mathrm{Im}(f) \oplus T$ podemos definir una transformación lineal $r : W \to V$ como $r(w) = f^{-1}(w)$ si $w \in \mathrm{Im}(f)$ y $r(w) = 0$ si $w \in T$. Para un w cualquiera escribimos (de manera única) $w = w_f + w_T$ con $w_f \in \mathrm{Im}(f)$ y $w_T \in T$ y definimos $r(w) := r(w_f)$. Esta transformación lineal verifica $r \circ f = \mathsf{Id}_V$.

Dualmente, si $f : V \to W$ es un epimorfismo, $\mathrm{Ker}(f) \subseteq V$ es un subespacio y uno puede encontrar un complemento S y escribir $V = \mathrm{Ker}(f) \oplus S$. Es un ejercicio sencillo verificar que $f|_S$ es un monomorfismo y que $f(S) = f(V) = W$, de manera que $f|_S : S \to W$ es un isomorfismo. Podemos definir entonces una transformación lineal $s : W \to V$ como la composición

$$W \xrightarrow{(f|_S)^{-1}} S \hookrightarrow V$$

Se puede ver sin dificultad que $f \circ s = \mathsf{Id}_W$.

Definición 3.4.7. Sea $f : M \to N$ un morfismo de A-módulos.

- f es una *sección* si existe un morfismo $g : N \to M$ tal que $g \circ f = \mathsf{Id}_M$.
- f es una *retracción* si existe un morfismo $g : N \to M$ tal que $f \circ g = \mathsf{Id}_N$.

Observación. Si f es una sección entonces es inyectiva porque

$$f(m) = 0 \implies x = g(f(m)) = g(0) = 0 \implies \mathrm{Ker}(f) = 0.$$

Si f es una retracción entonces es sobreyectiva porque si $n \in N$, $n = f(g(n))$, así que $n \in \mathrm{Im}(f)$.

Como corolario de los comentarios de los dos párrafos anteriores, vems que las nociones de epimorfismo y de retracción, por un lado, y de monomorfismo y de sección, por otro, coinciden en la categoría de espacios vectoriales. En la categoría de A-módulos con A un anillo cualquiera no sucede lo mismo. Dejamos como ejercicio verificar que la proyección al cociente $\mathbb{Z} \to \mathbb{Z}_2$ es un epimorfismo que no es una retracción, y que la inclusión $2\mathbb{Z} \to \mathbb{Z}$ es un monomorfismo que no es una sección. Otro ejemplo puede ser fabricado

tomando los grupos abelianos $\mathbb{Z}_2$ y $\mathbb{Z}_4$: el lector podrá encontrar morfismos entre estos grupos que sean monomorfismos o epimorfismos pero que no sean ni secciones ni retracciones.

3.5 Módulos cíclicos

En el caso de grupos se tiene a una descripción muy concisa de los grupos cíclicos: todos son cocientes de $\mathbb{Z}$. Como los subgrupos de $\mathbb{Z}$ son conocidos, entonces son conocidos todos los grupos cíclicos.

Si se tiene ahora un A-módulo cíclico M, es decir, un A-módulo en el que existe un elemento $x \in M$ con $Ax = \langle x \rangle = M$, podemos definir un morfismo sobreyectivo de A en M de manera que $a \mapsto ax$. El núcleo de esta aplicación es un submódulo (a izquierda) del A-módulo A, es decir, un ideal a izquierda de A. Si $I = \mathrm{Ker}(A \to M)$, entonces $M \cong A/I$ como A-módulo.

Recíprocamente, si I es un ideal a izquierda de A, entonces I es un A-submódulo de A y A/I es un A-módulo, que además es cíclico porque $A/I = \langle \overline{1} \rangle$. Vemos así que todo módulo cíclico es isomorfo a un cociente de A por un ideal a izquierda.

Esto nos dice que conocemos todos los A-módulos cíclicos en cuanto tenemos una caracterización de los ideales a izquierda de A.

3.6 Suma y producto

Sean I un conjunto de índices, A un anillo, y $(M_i)_{i \in I}$ una familia de A-módulos. El producto cartesiano $\prod_{i \in I} M_i$ es un A-módulo si definimos

$$a(m_i)_{i \in I} = (am_i)_{i \in I}$$

Recordamos que el producto cartesiano es

$$\prod_{i \in I} M_i = \{f : I \to \cup_{i \in I} M_i : f(i) \in M_i \text{ tal que } i \in I\}.$$

Este módulo producto viene provisto de proyecciones a cada factor, que son morfismos A-lineales, y tiene la propiedad de que para definir un morfismo $\phi : N \to \prod_{i \in I} M_i$ (donde N es un A-módulo cualquiera) basta definir "sus coordenadas", es decir, para cada $i \in I$, hay que dar un morfismo $\phi_i : N \to M_i$.

Observación. La estructura de A-módulo del producto cartesiano es la única estructura posible que hace de las proyecciones a las coordenadas morfismos de A-módulos. Además, la propiedad mencionada en el párrafo anterior es una propiedad universal que caracteriza completamente al producto (ver definición 9.2.1 del capítulo de categorías).

Notemos ademas que si $i_0 \in I$, el subconjunto de $\prod_{i\in I} M_i$ de los elementos $(m_i)_{i\in I}$ con $m_i = 0$ si $i \neq i_0$ es un submódulo y puede identificarse con M_{i_0}.

De esta manera, tiene sentido considerar el A-submódulo de $\prod_{i\in I} M_i$ "generado por los M_i", que es, de alguna manera, el módulo más chico que contiene a los M_i sin relaciones extra. Más precisamente, definimos la *suma directa* de los M_i como:

$$\bigoplus_{i\in I} M_i = \{(m_i)_{i\in I} : m_i = 0 \text{ para casi todo } i \in I\}.$$

Se trata de un submódulo del producto y para cada $i_0 \in I$ se tienen inyecciones $j_{i_0} : M_{i_0} \to \bigoplus_{i\in I} M_i$. Si el conjunto de índices es finito, la suma directa obviamente coincide con el producto directo.

Si N es un A-módulo y se tienen morfismos $\phi_i : M_i \to N$, usando el hecho de que $\oplus_{i\in I} M_i$ está generado por los M_i, se obtiene un único morfismo $\phi : \oplus_{i\in I} M_i \to N$ tal que restringido a cada M_{i_0} coincide con ϕ_{i_0}. Esta propiedad, de hecho, es una propiedad universal que caracteriza en términos categóricos a la suma directa (ver definición la definición 9.2.3 y sus propiedades fundamentales en el capítulo de categorías).

Una proposición que da una idea de cómo la noción de sección y retracción se distingue de la de monomorfismo y epimorfismo es la siguiente:

Proposición 3.6.1. *Supongamos que*

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$$

es una sucesión exacta corta de A-módulos. Entonces las siguiente afirmaciones son exactas:

(a) f es una sección.
(b) g es una retracción.

(c) La sucesión exacta es trivial. Más precisamente, se tiene el siguiente diagrama conmutativo:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{f} & N & \xrightarrow{g} & T & \longrightarrow & 0 \\ & & \| & & \| \sim & & \| & & \\ 0 & \longrightarrow & M & \xrightarrow{j} & M \oplus T & \xrightarrow{\pi} & T & \longrightarrow & 0 \end{array}$$

En esa situación, diremos que la sucesión exacta es *escindida*, que la sucesión *se parte* o que es *"split"*.

Demostración. Si vale la condición *(c)*, es claro que π es una retracción y que j es una sección. Usando el isomorfismo $N \cong M \oplus T$ del diagrama vemos inmediatamente, entonces que *(c)* implica *(a)* y *(b)*. Veamos ahora que *(a)* implica *(c)*, dejando como ejercicio ver que por ejemplo *(b)* implica *(c)*.

Sea $h : N \to M$ una retracción de f, de manera que $h \circ f = \mathsf{Id}_M$. Definimos $\phi : N \to M \oplus T$ poniendo $\phi(n) = (h(n), g(n))$. Afirmamos que ϕ es un isomorfismo y que hace del diagrama en *(c)* un diagrama conmutativo.

Es claro que $\pi \circ \phi = g$. La propiedad de que h sea retracción de f es la conmutatividad del cuadrado de la izquierda.

Veamos que ϕ es un monomorfismo. Si $n \in \mathrm{Ker}(\phi)$, entonces, en particular, $n \in \mathrm{Ker}(g) = \mathrm{Im}(f)$. Si $m \in M$ es tal que $n = f(m)$, se tiene que $0 = h(n) = h(f(m)) = m$, por lo tanto $n = 0$.

Veamos que ϕ es un epimorfismos. Sea $m \in M$ y $t \in T$. Como g es un epimorfismo, existe $n \in N$ tal que $g(n) = t$. Pongamos $x = f(m) - f(h(n)) + n \in N$. Entonces

$$\phi(x) = \phi(f(m) - f(h(n)) + n) = (m, t).$$

Esto termina la prueba. □

3.7 Ejercicios

Módulos y morfismos

3.7.1. Sea A un anillo, $n \geq 1$ y $M \in M_{m,n}(A)$. Muestre que la multiplicación matricial da un morfismo de A-módulos

$$f : x \in A^n \mapsto Mx \in A^m.$$

3.7.2. Sea A un anillo.

(a) Sea M un A-módulo a izquierda. Si definimos un producto $M \times A^{\mathrm{op}} \to M$ poniendo $m \cdot a = am$, podemos dotar a M de una estructura de A^{op}-módulo a derecha. Lo notamos M^{op}.

(b) Si $f : M \to N$ es un morfismo de A-módulos a izquierda, entonces $f : M^{\mathrm{op}} \to N^{\mathrm{op}}$ es un morfismo de A^{op}-módulos a derecha.

(c) Recíprocamente, todo A^{op}-módulo a derecha es de la forma M^{op} para algún A-módulo a izquierda M y todo morfismo de A^{op}-módulos está inducido como en la parte anterior.

3.7.3. Sean N y M dos $\mathbb{Q}$-módulos. Muestre que $f : N \to M$ es un morfismo de $\mathbb{Q}$-módulos sii es un morfismo de grupos abelianos.

3.7.4. Sea A un anillo y N, M dos A-módulos.

(a) Muestre que $\hom_A(M, N)$ es un grupo abeliano, con

$$(f+g)(m) = f(m) + g(m), \qquad \forall f,\, g \in \hom_A(M,N),\ \forall m \in M.$$

(b) Sea $\mathcal{Z}(A)$ el centro de A. Definimos una operación

$$\mathcal{Z}(A) \times \hom_A(M,N) \to \hom_A(M,N)$$

poniendo

$$(a \cdot f)(m) = f(am), \qquad \forall f \in \hom_A(M,N),\ \forall a \in \mathcal{Z}(A),\ \forall m \in M.$$

Muestre que esto hace de $\hom_A(M, N)$ un $\mathcal{Z}(A)$-módulo.

(c) Muestre que para todo A-módulo M existe un isomorfismo de $\mathcal{Z}(A)$-módulos $\hom_A(A, M) \to M$.

3.7.5. Sean A, B y C anillos.

(a) Sean M un (A, B)-bimódulo y N un (A, C)-bimódulo. Muestre que el grupo abeliano $\hom_A(M, N)$ posee una única estructura de (B, C)-bimódulo tal que

$$(b \cdot f \cdot c)(m) = f(mb)c, \qquad \forall b \in B,\ \forall c \in C,\ \forall m \in M.$$

(b) Sea M un A-módulo a izquierda. Viendo a A como (A, A)-bimódulo, muestre que hay un isomorfismo de A-módulos a izquierda $\hom_A(A, M) \cong M$.

3.7.6. *Cambios de anillo.* Sea $\phi : A \to B$ un morfismo de anillos.

(a) Muestre que si definimos un producto $A \times B \to B$ poniendo

$$a \cdot b = \phi(a)b$$

dotamos a B de una estructura de A-módulo a izquierda sobre B. De la misma forma, podemos obtener una estructura de A-módulo a derecha y de A-bimódulo sobre B.

(b) Sea M un B-módulo a izquierda. Muestre que el producto

$$(a, m) \in A \times M \to \phi(a)m \in M$$

hace de M un A-módulo a izquierda. Lo notamos $\phi^*(M)$.

(c) Si $f : M \to N$ es un morfismo de B-módulos a izquierda, entonces $f : \phi^*(M) \to \phi^*(N)$ es un morfismo de A-módulos a izquieda. Lo notamos $\phi^*(f)$.

(d) Si M y N son B-módulos a izquierda, la aplicación

$$\phi^* : f \in \hom_B(M, N) \mapsto \phi^*(f) \in \hom_A(\phi^*(M), \phi^*(N))$$

es un morfismo de grupos abelianos.

(e) Sean M, N y P B-módulos a izquierda y sean $f : M \to N$ y $g : N \to P$ son morfismos de B-módulos. Entonces

$$\phi^*(g \circ f) = \phi^*(g) \circ \phi^*(f).$$

En particular, la aplicación $\phi^* : \mathrm{End}_B(M) \to \mathrm{End}_A(\phi^*(M))$ es un morfismo de anillos.

(f) De condiciones sobre ϕ que impliquen que la aplicación

$$\phi^* : \hom_B(M, N) \to \hom_A(\phi^*(M), \phi^*(N))$$

sea inyectiva (sobreyectiva) cualesquiera sean los B-módulos M y N.

3.7.7. Sea A un anillo, sea M un A-módulo a izquierda. Sea además $B = \mathrm{End}_A(M)$ el anillo de endomorfismos de M.

(a) Muestre que M es un B-módulo a derecha de manera natural y que con esa estructura resulta de hecho un (A, B)-bimódulo.

(b) ¿Qué relación hay entre A y $\mathrm{End}_B(M)$?

3.7.8. Sea A un anillo.

(a) Sea $f : M \to M'$ un morfismo de A-módulos a izquierda. Para cada A-módulo a izquierda definimos un aplicaciones

$$f_P^* : h \in \hom_A(M', P) \mapsto h \circ f \in \hom_A(M, P)$$

y

$$f_*^P : h \in \hom_A(P, M) \mapsto f \circ h \in \hom_A(P, M').$$

Se trata de morfismos de grupos abelianos.

(b) Sean $f : M \to M'$ y $g : M' \to M''$ morfismos de A-módulos. Entonces para cada A-módulo a izquierda P vale que

$$f_P^* \circ g_P^* = (g \circ f)_P^*$$

y

$$g_*^P \circ f_*^P = (g \circ f)_*^P.$$

(c) Una sucesión de A-módulos a izquierda

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M''$$

es exacta sii la sucesión de grupos abelianos

$$0 \longrightarrow \hom_A(N, M') \xrightarrow{f_*^N} \hom_A(N, M) \xrightarrow{g_*^N} \hom_A(N, M'')$$

es exacta para todo A-módulo a izquierda N. ¿Hay un enunciado similar que involcre a los morfismos f_N^* y g_N^*?

(d) ¿Es cierto que si

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

es una sucesión exacta de A-módulos a izquierda entonces

$$0 \longrightarrow \hom_A(N, M') \xrightarrow{f_*^N} \hom_A(N, M) \xrightarrow{g_*^N} \hom_A(N, M'') \longrightarrow 0$$

es una sucesión exacta de grupos abelianos?

3.7.9. Un A-módulo M es simple sii para todo $m \in M \setminus 0$, $Am = M$.

3.7.10. *(a) Lema de Schur.* Sea $f : M \to N$ un morfismo de A-módulos.

(a) Si M es simple, entonces f es o bien nula o bien inyectva.

(b) Si N es simple, entonces f es o bien nula o bien sobreyectiva.

(c) Si M y M son simples, entonces f es o bien nula o bien un isomorfismo.

(b) Si M es un A-módulo simple, $\mathrm{End}_A(M)$ es un anillo de división.

3.7.11. Sea A un dominio íntegro y sean $v_1, \ldots, v_n \in A^n$. Sea $M \in M_n(A)$ la matriz cuyas columnas son los vectores $v_1, \ldots, v_n$.

(a) Si $\det M \neq 0$, el conjunto $\{v_1, \ldots, v_n\}$ es linealmente independiente.

(b) Si $\det M \in A^\times$, el conjunto $\{v_1, \ldots, v_n\}$ es un sistema de generadores.

3.7.12. *(a)* Todo módulo de tipo finito posee un conjunto generador minimal.

(b) Para todo $n \in \mathbb{N}$ existe un conjunto generador minimal de $\mathbb{Z}$ de cardinal n.

3.7.13. Sea k un cuerpo y V un k-espacio vectorial. Sea $f \in \mathrm{End}_k(V)$. Muestre que existe exactamente una estructura de $k[X]$-módulo a izquierda sobre V para la cual $k \subset k[X]$ actúa por multiplicación escalar y

$$X \cdot v = f(v), \qquad \forall v \in V.$$

3.7.14. Sea A un anillo y M un A-módulo a izquierda.

(a) El conjunto $\mathrm{ann}\, M = \{a \in A : am = 0,\ \forall m \in M\}$ es un ideal a izquierda de A. Si $\mathrm{ann}\, M = 0$, decimos que M es un A-módulo *fiel*.

(b) De ejemplos de módulos fieles.

3.7.15. Sea k un cuerpo. Sea V un k-espacio vectorial y sean ϕ y ψ transformaciones lineales de V en V.

(a) Probar que $(V, \phi) \cong (V, \psi)$ como $k[X]$-módulos si y sólo si ϕ es un endomorfismo conjugado a ϕ, es decir, si existe $\alpha \in \mathrm{Aut}_k(V)$ tal que $\phi = \alpha \circ \psi \circ \alpha^{-1}$.

(b) Sea (V, ϕ) como antes. Mostrar que los subespacios ϕ-estables se corresponden unívocamente con los $k[X]$-submódulos de V y que hallar una base en la que la matriz de ϕ se escriba en bloques equivale a hallar una descomposición de V como suma directa de $k[X]$-submódulos.

(c) Encontrar un $k[X]$-módulo de dimensión 2 sobre k que no admita sumandos directos no triviales.

(d) Si $\lambda \in k$, $\mathrm{ev}_\lambda : P \in k[X] \mapsto P(\lambda) \in k$ es un morfismo de anillos. Induce, por lo tanto, una estructura de $k[X]$-módulo sobre k. Sea k_λ el $k[X]$-módulo definido de esa manera, ¿es $k_\lambda \cong k_{\lambda'}$ como $k[X]$-módulo si $\lambda \neq \lambda'$?

(e) Si V es un espacio vectorial de dimensión finita, entonces ϕ es diagonalizable si y sólo si V se descompone como $k[X]$-módulo en suma directa de submódulos isomorfos a los k_λ ($\lambda \in k$).

(f) Si M es un $k[X]$-módulo cíclico, entonces o bien es de dimensión finita, o bien es isomorfo a $k[X]$.

Sugerencia. Ver el teorema de 'clasificación' de grupos cíclicos y copiar la idea.

3.7.16. Sea (V, ϕ) un $k[X]$-módulo con ϕ nilpotente. ¿Es (V, ϕ) un $k[\![X]\!]$-módulo?

3.7.17. Sabiendo que en $k[\![X]\!]$ los elementos de la forma $\lambda + xp$ con $p \in k[\![X]\!]$ y $0 \neq \lambda \in k$ son inversibles (si no lo sabe, ¡demuéstrelo!), probar que los ideales de $k[\![X]\!]$ son 0 y $\langle x^n \rangle$ con $n \in \mathbb{N}_0$.

3.7.18. Sea M un $k[\![X]\!]$-módulo (y por lo tanto un $k[X]$-módulo).

(a) Si M es cíclico entonces $M = (M, \phi)$ con M de dimensión finita y ϕ nilpotente, o bien $M \cong k[\![X]\!]$.

(b) Si M es de dimensión finita entonces el endomorfismo 'multiplicar por x' es nilpotente en M.

Localización de módulos

3.7.19. *Localización de módulos.* Sea A un anillo, $S \subset A$ un subconjunto central multiplicativamente cerrado y sea M un A-módulo a izquierda.

(a) Muestre que existe un A-módulo M_S y un homomorfismo de A-módulos $j_M : M \to M_S$ que satisfacen la siguiente propiedad:

> Para cada homomorfismo $f : M \to N$ con codominio en un A-módulo N para el cual todas las aplicaciones $n \in N \mapsto sn \in N$ con $s \in S$ son isomorfismos, existe un único homomorfismo $\bar{f} : M_S \to N$ tal que $f = \bar{f} \circ j_M$.

(b) El par (M_S, j_M) está determinados a menos de un isomorfismo canónico.

(c) El A-módulo M_S es de forma natural un A_S-módulo.

(d) Si M es un A-módulo tal que para todo $s \in S$ la aplicación $m \in M \mapsto sm \in M$ es biyectiva, entonces $j_M : M \to M_S$ es un isomorfismo.

(e) Si $f : M \to N$ es un morfismo de A-modulos, entonces existe un único morfismo $f_S : M_S \to N_S$ tal que conmuta el siguiente diagrama:

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle j_M}\downarrow & & \downarrow{\scriptstyle j_N} \\ M_S & \xrightarrow{f_S} & N_S \end{array}$$

Si $S = A \setminus \mathfrak{p}$ para un ideal primo $\mathfrak{p} \in \operatorname{Spec} A$, entonces escribimos $M_\mathfrak{p}$ en vez de M_S.

3.7.20. Sea A un anillo, $S \subset A$ un subconjunto central multiplicativamente cerrado y sea M un A-módulo a izquierda finitamente generado. Entonces $M_S = 0$ sii existe $s \in S$ tal que $sM = 0$.

De un contraejemplo para esta equivalencia cuando M no es finitamente generado.

3.7.21. *Exactitud de la localización.*

(a) Sea A un anillo y $S \subset A$ un subconjunto central multiplicativamente cerrado. Si

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

es una sucesión exacta corta de A-módulos, entonces

$$0 \longrightarrow M'_S \xrightarrow{f_S} M_S \xrightarrow{g_S} M''_S \longrightarrow 0$$

es una sucesión exacta corta.

(b) En particular, si $M' \subset M$ es un submódulo de un A-módulo M, entonces M'_S puede ser considerado un submódulo de M_S.

3.7.22. Sea A un anillo, $S \subset A$ un subconjunto central multiplicativamente cerrado y M un A-módulo.

(a) Si P y Q son submódulos de M, entonces $(P+Q)_S = P_S + Q_S$.

(b) Si P y Q son submódulos de M, entonces $(P \cap Q)_S = P_S \cap Q_S$.

(c) Si $P \subset M$ es un submódulos, entonces hay un isomorfismo canónico $(M/P)_S \cong M_S/P_S$.

3.7.23. *Propiedades locales.* Sea A un anillo conmutativo.

(a) Sea M un A-módulo. Las siguientes afirmaciones son equivalentes:
  (i) $M = 0$;
  (ii) $M_\mathfrak{p} = 0$ para todo $\mathfrak{p} \in \operatorname{Spec} A$; y
  (iii) $M_\mathfrak{m} = 0$ para todo ideal maximal $\mathfrak{m} \subset A$.

(b) Sea $f : M \to N$ un morfismo de A-módulos. Las siguientes afirmaciones son equivalentes:
  (i) f es inyectivo;
  (ii) $f_\mathfrak{p}$ es inyectivo para todo $\mathfrak{p} \in \operatorname{Spec} A$; y
  (iii) $f_\mathfrak{m}$ es inyectivo para todo ideal maximal $\mathfrak{m} \subset A$.

(c) Sea $f : M \to N$ un morfismo de A-módulos. Las siguientes afirmaciones son equivalentes:
  (i) f es sobreyectivo;
  (ii) $f_\mathfrak{p}$ es sobreyectivo para todo $\mathfrak{p} \in \operatorname{Spec} A$; y
  (iii) $f_\mathfrak{m}$ es sobreyectivo para todo ideal maximal $\mathfrak{m} \subset A$.

3.7.24. *Soporte de un módulo.* Sea A un anillo conmutativo. Si M es un A-módulo, el *soporte de* M es el conjunto

$$\operatorname{sop} M = \{\mathfrak{p} \in \operatorname{Spec} A : M_\mathfrak{p} \neq 0\}.$$

Muestre que si M es finitamente generado, es

$$\operatorname{sop} M = \{\mathfrak{p} \in \operatorname{Spec} A : \mathfrak{p} \subset \operatorname{ann} M\}.$$

3.7.25. Sea $S \subset k[X]$, $S = \{X^i : i \in \mathbb{N}_0\}$. Entonces:

(a) $k[X]_S \cong k[X, X^{-1}] \cong k[X, Y]/\langle X.Y - 1\rangle$.

(b) Si (V, ϕ) es un $k[X]$-módulo, entonces $V_S \cong V$ sii ϕ es un isomorfismo.

(c) Sea (V, ϕ) un $k[X]$-módulo de dimensión finita. Mostrar que $\mathrm{Ker}(\phi^n)$ es un $k[X]$-submódulo de V para todo $n \in \mathbb{N}$.

Sea $t(V) = \bigcup_{n\in\mathbb{N}} \mathrm{Ker}(\phi^n)$. Entonces $t(V)$ es el núcleo de la aplicación canónica $V \to V_S$ y que $V_S \cong V/t(V)$.

Sugerencia. Ver que $\phi : V \to V$ induce un isomorfismo $V/t(V) \to V/t(V)$ para asi obtener un morfismo natural $V_S \to V/t(V)$, para el morfismo en el otro sentido usar que $t(V) = \mathrm{Ker}(V \to V_S)$.

3.7.26. Sea k un cuerpo. Sea $l : k[X, X^{-1}] - \{0\} \to \mathbb{N}_0$ la función tal que, si $P = \sum_{k=n}^{m} a_k X^k \in k[X, X^{-1}]$, con $n \leq m$ y $a_n a_m \neq 0$, entonces $l(P) = m - n$

(a) Mostrar que l hace de $k[X, X^{-1}]$ un dominio euclideano.

Sugerencia. Para obtener un algoritmo de división, primero multiplicar por una potencia conveniente de X, hacer la cuenta en $k[X]$ y después volver.

(b) Todo $k[X, X^{-1}]$-módulo cíclico o bien es de dimensión finita o bien es isomorfo a $k[X, X^{-1}]$.

Capítulo 4

Condiciones de cadena sobre módulos y anillos

4.1 Módulos noetherianos

En el contexto de espacios vectoriales sobre un cuerpo k, puede considerarse la dimensión como función de los espacios en los números naturales. Esta función es monótona con respecto a la inclusión: si S es un subespacio de V entonces $\dim_k(S) \leq \dim_k(V)$. En particular, si V es finitamente generado, entonces todos sus subespacios también lo son. En el caso de módulos sobre un anillo arbitrario no existe una noción análoga a la de dimensión y la propiedad de ser finitamente generado no tiene por qué ser hereditaria, es decir, submódulos de un módulo finitamente generado no tienen por qué ser finitamente generados.

El ejemplo clásico es el siguiente. Sea

$$A = \mathbb{R}^{[0,1]} = \{f : [0,1] \to \mathbb{R}\},$$

con la estructura usual de un anillo de funciones y sean $M = A$ y

$$S = \{f \in A : f(x) \neq 0 \text{ sólo para finitos valores de } x\}.$$

El conjunto S es un ideal de A y, por lo tanto, un A-submódulo de M. M está generado por la función constante 1 y, sin embargo, S no es un A-módulo finitamente generado. Para ver esto, supongamos que existen $f_1, \ldots, f_n \in S$ tales que $\langle f_1, \ldots, f_n \rangle = S$. Sea

$\{x_1, \dots x_s\} \subset [0,1]$ el conjunto de todos los puntos $x \in [0,1]$ tales que existe $i \in \{1, \dots, n\}$ con $f_i(x) \neq 0$ (claramente se trata de un conjunto finito) y sea $x_0 \in [0,1] - \{x_1, \dots, x_s\}$. Si definimos $\phi : [0,1] \to \mathbb{R}$ de manera que $\phi(x_0) = 1$ y $\phi(x) = 0$ si $x \neq x_0$, entonces $\phi \in S$ pero ϕ no puede pertenecer a $\langle f_1, \dots, f_n \rangle$.

Tampoco puede asegurarse, para un anillo A arbitrario, que dados un A-módulo M y un par M_1 y M_2 de A-submódulos de tipo finito, esto es, finitamente generados, entonces $M_1 \cap M_2$ sea de tipo finito. Sin embargo, para algunos anillos A (además de los cuerpos) y ciertos A-módulos M puede afirmarse que la propiedad de ser de tipo finito es hereditaria. Por ejemplo, los anillos principales como $\mathbb{Z}$ o $k[X]$ (si k es un cuerpo) tienen la propiedad siguiente: todo ideal puede ser generado por un único elemento. De esta manera todo $\mathbb{Z}$-submódulo de $\mathbb{Z}$ es finitamente generado y lo mismo con los $k[X]$-submódulos de $k[X]$.

La situación para cocientes es más sencilla, porque todo cociente de un módulo finitamente generado es finitamente generado. Más generalmente:

Proposición 4.1.1. *Sea A un anillo cualquiera y sea*

$$0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$$

una sucesión exacta corta de A-módulos. Entonces:

(a) Si M_2 de tipo finito, entonces M_3 es de tipo finito.
(b) Si M_1 y M_3 son de tipo finito, entonces M_2 es de tipo finito.

Demostración. (a) Sea $\{y_1, \dots, y_n\}$ un conjunto finito de generadores para M_2 y sea $z \in M_3$. Como g es un epimorfismo, existe $y \in M_2$ con $g(y) = z$. Ahora, $y = \sum_{i=1}^{n} a_i y_i$ para ciertos $a_i \in A$, así que $z = \sum_{i=1}^{n} a_i g(y_i)$. Por lo tanto $\{g(y_1), \dots, g(y_n)\}$ genera a M_3.

(b) Supongamos que $M_1 = \langle x_1, \dots, x_r \rangle$ y que $M_3 = \langle z_1, \dots, z_s \rangle$ y sean $y_1, \dots, y_s \in M_2$ tales que $g(y_i) = z_i$ si $1 \leq i \leq s$. Afirmamos que $M_2 = \langle f(x_1), \dots, f(x_r), y_1, \dots, y_s \rangle$.

En efecto, sea $y \in M_2$. Como $g(y) \in M_3$, existen $a_1, \dots, a_s \in A$ tales que $g(y) = \sum_{i=1}^{s} a_i z_i = g(\sum_{i=1}^{s} a_i y_i)$. Luego $g(y - \sum_{i=1}^{s} a_i y_i) = 0$ y la exactitud implica que el elemento $y' = y - \sum_{i=1}^{s} a_i y_i$ está en la imagen de f. En consecuencia, existe $x \in M_1$ tal que $f(x) = y'$. Por

hipótesis, entonces, existen $b_1, \ldots, b_r \in A$ tales que $x = \sum_{i=1}^{r} b_i x_i$. En particular, $y' = f(x) = \sum_{i=1}^{r} b_i f(x_i)$. Pero entonces

$$y = y' + \sum_{i=1}^{s} a_i y_i = \sum_{i=1}^{r} b_i f(x_i) + \sum_{i=1}^{s} a_i y_i \in \langle f(x_1), \ldots, f(x_r), y_1, \ldots, y_s \rangle.$$

Esto prueba nuestra afirmación. □

Corolario 4.1.2. *Si $\phi : M \to N$ es un morfismo de A-módulos tal que* $\mathrm{Ker}(\phi)$ *e* $\mathrm{Im}(\phi)$ *son de tipo finito, entonces M es de tipo finito.*

Definición 4.1.3. Sea A un anillo. En A-módulo M es *noetheriano* si todo submódulo de M es finitamente generado

Notemos que, en particular, para que un módulo M sea noetheriano debe ser él mismo de tipo finito.

Ejemplos.
1. Los A-módulos nulos, simples, finitos (en tanto conjuntos, como $\mathbb{Z}_n$ como $\mathbb{Z}$-módulo) y los A-módulos con un número finito de submódulos son noetherianos.

2. Si A es principal, entonces A es un A-módulo noetheriano.

3. Si k es un cuerpo, un k-espacio vectorial V es noetheriano si y sólo si $\dim_k V < \infty$.

Proposición 4.1.4. *Sea A un anillo y M un A-módulo. Las siguientes afirmaciones son equivalentes:*

(a) M es noetheriano.
(b) Todo conjunto no vacío de submódulos de M tiene un elemento maximal respecto a la inclusión.
(c) Toda sucesión no vacía y creciente de submódulos se estaciona.

Demostración. (b) $\Rightarrow$ (c) Sea $(M_i)_{i \in \mathbb{N}_0}$ una sucesión creciente de submódulos de M y consideremos el conjunto $\{M_i : i \in \mathbb{N}_0\}$ de submódulos de M. Por hipótesis, este conjunto posee un elemento maximal. Como este pertenece a la sucesión de partida, que es creciente, esta debe estacionarse en el conjunto de submódulos que aparecen en la sucesión.

(c) ⇒ (b) Sea $\mathcal{C} \neq \varnothing$ un conjunto de submódulos de M que no posee un elemento maximal. Como $\mathcal{C} \neq \varnothing$, existe $S_1 \in \mathcal{C}$. Como S_1 no es maximal en $\mathcal{C}$, existe $S_2 \in \mathcal{C}$ tal que $S_1 \subsetneq S_2$. Siguiendo así inductivamente, encontramos una sucesión $(S_i)_{i\in\mathbb{N}_0}$ de elementos de $\mathcal{C}$ tales que $S_i \subsetneq S_{i+1}$ para cada $i \in \mathbb{N}_0$. Esto es absurdo, porque contradice la hipotesis.

(b) ⇒ (a) Supongamos que M satisface la condición de *(b)* y sea N un submódulo de M. Queremos ver que N es finitamente generado.

Consideremos la familia $\mathcal{C}$ de los submódulos de M que son de tipo finito y que están contenidos en N. Como $\{0\} \in \mathcal{C}$, entonces $\mathcal{C}$ no es vacío.

Nuestra hipótesis nos dice que $\mathcal{C}$ tiene un elemento maximal N_0. Veamos que $N_0 = N$. Supogamos que no es este el caso y consideremos un elemento $x \in N - N_0$. Sea $N_0' = N_0 + \langle x \rangle$. Entonces N_0' es de tipo finito y está contenido en N. Pero N_0 está contenido estrictamente en N_0', lo que contradice la elección de N_0. Luego debe ser $N_0 = N$.

(a) ⇒ (c) Supongamos ahora M noetheriano y consideremos una cadena creciente

$$N_1 \subseteq N_2 \subseteq \cdots \subseteq N_k \subseteq N_{k+1} \subseteq \ldots$$

de submódulos de M. Como la cadena es creciente, $N = \bigcup_{k\in\mathbb{N}} N_k$ es un submódulo de M, que es finitamente generado, porque M es noetheriano. Sean $x_1, \ldots, x_n \in N$ tales que

$$\langle x_1, \ldots, x_n \rangle = N = \bigcup_{k\in\mathbb{N}} N_k.$$

Si $i \in \{1, \ldots, n\}$, existe $k_i \in \mathbb{N}$ tal que $x_i \in N_{k_i}$. Si n_0 es el máximo de los k_i, entonces, como la sucesión es creciente, todos los x_i pertenecen a N_k cada vez que $k \geq n_0$. Luego $N_k = N$ para todo $k \geq n_0$. □

Como la propiedad de noetherianidad de un A-módulo M se enuncia en términos de todos sus submódulos, resulta que todo submódulo S de un A-módulo noetheriano es noetheriano. Por otro lado, si S es un submódulo de M, los submódulos del cociente M/S están en correspondencia con los submódulos de M que contienen a S. Luego un cociente de un módulo noetheriano es también noetheriano. Más generalmente:

Proposición 4.1.5. *Sea*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

una sucesión exacta de A-módulos. Entonces

(a) Si M noetheriano, M' y M'' son noetherianos.
(b) Si M' y M'' son noetherianos, entonces M es noetheriano.

Demostración. Como f es un monomorfismo, $M' \cong \mathrm{Im}(f)$ de M y, como g es un epimorfismo, $M'' \cong M/\operatorname{Ker}(g)$. Luego la primera afirmación ya ha sido probada.

Supongamos ahora M'' y M' son noetherianos. Sea N un submódulo de M. Queremos ver que N es finitamente generado. Para eso, consideremos la siguiente sucesión exacta corta:

$$0 \longrightarrow f^{-1}(N) \xrightarrow{f} N \xrightarrow{g} \mathrm{Im}(g|_N) \longrightarrow 0$$

Como M'' y M' son noetherianos, tanto $\mathrm{Im}(g)$ como $f^{-1}(N)$ son finitamente generados. La proposición 4.1.1 nos dice entonces que N es finitamente generado. □

Observación. Ser noetheriano es una propiedad que se preserva por sumas directas finitas, ya que si $M_1, \ldots, M_n$ son módulos noetherianos, tenemos una sucesión exacta corta

$$0 \longrightarrow M_1 \longrightarrow \bigoplus_{i=1}^{n} M_i \longrightarrow \bigoplus_{i=2}^{n} M_i \longrightarrow 0$$

así que nuestra afirmación sigue de la proposición por inducción.

Por el contrario, ser noetheriano es una propiedad que no se preserva por sumas directas infinitas ni por productos infinitos. Por ejemplo $\mathbb{Z}$ es un $\mathbb{Z}$-módulo noetheriano (ya que es $\mathbb{Z}$ es un dominio de ideales principales), pero $\mathbb{Z}^{(\mathbb{N})}$ no es noetheriano porque no es finitamente generado: basta considerar considerar la cadena creciente

$$\langle e_1 \rangle \subset \langle e_1, e_2 \rangle \subset \langle e_1, e_2, e_3 \rangle \subset \cdots$$

Como $\mathbb{Z}^{(\mathbb{N})}$ es un submódulo de $\mathbb{Z}^{\mathbb{N}}$, entonces $\mathbb{Z}^{\mathbb{N}}$ tampoco es noetheriano.

Definición 4.1.6. Un anillo A es *noetheriano a izquierda* si A es un A-módulo noetheriano.

La noción de anillo noetheriano a derecha se define, por supuesto, de manera análoga.

Observación. Si un anillo A es conmutativo, entonces A es anillo noetheriano a izquierda si y sólo si es anillo noetheriano a derecha.

Ejemplos.
1. $\mathbb{Z}$ y, si k es un cuerpo, $k[X]$ son anillos noetherianos porque son dominios de ideales principales.

2. El anillo con numerables indeterminadas $k[X_1, \dots, X_n, \dots]$ es un anillo que no es noetheriano. Como es íntegro, se lo puede considerar como subanillo de su cuerpo de fracciones, que es trivialmente noetheriano. Vemos así que un subanillos de un anillo noetheriano no tiene por qué ser noetheriano.

3. El anillo $A \subset M_2(\mathbb{R})$ formado por las matrices triangulares superiores tales que $a_{12} \in \mathbb{Q}$ es anillo noetheriano a izquierda pero no a derecha.

Si A es un anillo noetheriano a izquierda y M un A-módulo, ¿podemos afirmar que M es noetheriano? Como mínimo, M debería ser finitamente generado, así que no todo A-módulo será noetheriano. Pero como demostraremos ahora, esa es la única obstrucción:

Proposición 4.1.7. *Sea A un anillo noetheriano a izquierda. Si M es un A-módulo de tipo finito, entonces M es noetheriano.*

Demostración. Como M es de tipo finito, existe $n \in \mathbb{N}$ y un epimorfismo $A^n \to M$. Luego basta mostrar que A^n es un A-módulo noetheriano. Esto sigue inmediatamente de la observación hecha arriba de que una suma de módulos noetherianos es noetheriana. □

Proposición 4.1.8. *Sea $\phi : A \to B$ un morfismo sobreyectivo de anillos. Si A es noetheriano, entonces B es noetheriano.*

Demostración. Consideremos a B como A-módulo vía ϕ. Como A es noetheriano y ϕ es un morfismo sobreyectivo de A-módulos, vemos que B es un A-módulo noetheriano.

Ahora bien, un B-submódulo de-B es, en este caso, lo mismo que un A-submódulo de B, así que como toda cadena creciente de

A-submódulos de B se estaciona, lo mismo ocurre con las cadenas crecientes de B-submódulos. Así, B es noetheriano. □

Observaciones.
1. Si A es un anillo noetheriano a izquierda y $S \subset Z(A)$ es un subconjunto multiplicativamente cerrado, entonces A_S es un anillo noetheriano a izquierda: en efecto, los ideales de A_S están en correspondencia con los ideales de A que no contienen a ningún elemento de S y esa correspondencia preserva la inclusión.

Si M es un A-módulo noetheriano, ¿es M_S un A_S-módulo noetheriano?

2. Sea A un anillo y $J \subset A$ un ideal bilátero. Si A es un anillo noetheriano a izquierda, entonces A/J es un anillo noetheriano a izquierda.

4.2 El teorema de Hilbert

EL siguiente teorema es una herramienta poderosa y no trivial para probar, en casos específicos, la noetherianidad de un anillo:

Teorema 4.2.1. (Hilbert) *Si A un anillo noetheriano a izquierda, entonces $A[X]$ es un anillo noetheriano a izquierda.*

Demostración. Sea J un ideal de $A[X]$. Tenemos que mostrar que J es finitamente generado sobre $A[X]$. Consideramos para eso el conjunto de los coeficientes principales de los elementos de J,

$$I = \{a \in A : \text{existe } p \in J \text{ con } p = aX^m + \sum_{i=0}^{m-1} a_i X^i\} \cup \{0\}.$$

Se trata de un ideal a izquierda de A:

- Es evidente que $0 \in I$.
- Sean a, $a' \in I$, de manera que existen p, $p' \in J$ tales que $p = aX^m + \sum_{i=0}^{m-1} a_i X^i$ y $p' = a'X^{m'} + \sum_{i=0}^{m'-1} a'_i X^i$. Sin pérdida de generalidad, podemos suponer que $m \geq m'$ (si no fuese ese el caso, podemos multiplicar a p por una potencia de X suficientemente grande). Entonces $a + a'$ es el coeficiente principal del polinomio $p + X^{m-m'}p' \in J$, así que $a + a' \in I$.

- Sean $a \in I$ y $b \in A$. Si $ba = 0$, entonces por supuesto $ba \in I$. Si no, consideremos un polinomio $p = aX^m + \sum_{i=1}^{m-1} a_i X^i \in J$. Entonces ba es el coeficiente principal de bp, así que $ba \in I$.

Como I es un ideal a izquierda en A, que es noetheriano, es finitamente generado. Sea $\{a_1, \ldots, a_r\}$ un sistema de generadores de I sobre A y sean $p_1, \ldots, p_r \in J$ tales que el coeficiente principal de p_i es a_i. Multiplicando cada p_i por una potencia adecuada de X, podemos suponer que todos los polinomios p_i son del mismo grado m. Mostremos que estos polinomios "casi generan" a J en el siguiente sentido:

> Sea N el A-módulo formado por los elementos de J de grado menor que m, es decir, $N = J \cap A_{<m}[X]$. Entonces J está generado por los p_i "a menos de N", esto es, se tiene que $J = \langle p_1, \ldots, p_r \rangle_{A[X]} + M$. (4.1)

Esto es suficiente para ver que J es finitamente generado sobre $A[X]$. En efecto, como $A_{<m}[X]$ es un A-módulo de tipo finito, como A es noetheriano y como $N \subseteq A_{<m}[X]$ es un A-submódulo, entonces N es finitamente generado como A-módulo. Si $\{q_1, \ldots, q_s\} \subset N$ un subconjunto finito que genera a N sobre N, entonces J está generado como $A[X]$-módulo por $\{p_1, \ldots, p_r, q_1, \ldots, q_s\}$.

Nos queda, entonces, probar la afirmación (4.1). Si ponemos

$$J' = \langle p_1, \ldots, p_r \rangle_{A[X]} + M,$$

tenemos que mostrar que $J \subset J'$. Ahora bien, los a_i son los coeficientes principales de los polinomios p_i, cuyos grados son todos menores o iguales que g, así que el polinomio $\widetilde{p} = X^{g-m} \sum_{i=1}^{r} \lambda_i p_i$ es un elemento de J que tiene tiene a a como coeficiente principal. Claramente, $\widetilde{p} \in \langle p_1, \ldots, p_r \rangle_{A[X]}$. Sea $p' = p - \widetilde{p}$. Es $p' \in J$ y $\deg(p') < g$, de manera que la hipótesis inductiva nos dice este $p' \in J'$. Entonces

$$p = \widetilde{p} + p' \in \langle p_1, \ldots, p_r \rangle_{A[X]} + J' = J'.$$

Vemos que $p \in J'$. Esto termina la prueba. □

Corolario 4.2.2. *Si A es un anillo noetheriano y $n \in \mathbb{N}$, entonces el anillo de polinomios $A[X_1, \ldots, X_n]$ es anillo. En particular, si k es un cuerpo, $k[X_1, \ldots, X_n]$ es noetheriano.*

Demostración. Esto es claro si observamos que es

$$A[X_1, \ldots, X_n] = (A[X_1, \ldots, X_{n-1}])[X_n],$$

y hacemos inducción en base al teorema de Hilbert. □

Corolario 4.2.3. *Sean B un anillo y A un subanillo de B. Supongamos que A es noetheriano. Supongamos además que existe un elemento $b \in B$ que conmuta con los elementos de A y tal que b genera a B como A-álgebra, es decir, que todo elemento de B se escribe como combinación lineal de potencias de b (incluido $1 = b^0$) con coeficientes en A. Entonces B es noetheriano.*

La misma conclusión vale si B si está generado como A-álgebra por finitos elementos que conmuten entre si.

Demostración. Sea $b \in B$ un elemento como en el enunciado. La aplicación $\mathrm{ev}_b : p \in A[X] \mapsto p(b)B$ es un morfismo de anillos, porque b conmuta con los elementos de A, y es sobreyectivo, porque b genera a B como A-álgebra. Como A es noetheriano, $A[X]$ es noetheriano. Esto implica que B es noetheriano. La aserción final, con varios generadores, se demuestra de la misma forma, sustituyendo $A[X]$ por $A[X_1, \ldots, X_n]$. □

Ejemplo. Sean $d \in \mathbb{Z}$ un número que no es un cuadrado, sea $\sqrt{d} \in \mathbb{C}$ una raíz cuadrada de d y sea

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}.$$

Este subconjunto de $\mathbb{C}$ es un subanillo de $\mathbb{C}$ (¡verifíquelo!). Existe un epimorfismo de anillos $\phi : \mathbb{Z}[X] \to \mathbb{Z}[\sqrt{d}]$ tal que $\phi(X) = \sqrt{d}$. Entonces, como $\mathbb{Z}$ es noetheriano, $\mathbb{Z}[\sqrt{d}]$ resulta también un anillo noetheriano.

4.3 Módulos artinianos

Los módulos artinianos se suelen presentar dentro del marco de una teoría dual a la teoría de módulos noetherianos. Si M es un A-módulo, ¿cuál es la afirmación "dual" a "M es finitamente generado"?

Observemos que decir que M es finitamente generado es equivalente a decir que existen $n \in \mathbb{N}$ y un epimorfismo $\pi : A^n \to M$. Dado un A-módulo arbitrario M, siempre existe un conjunto I y un epimorfismo $A^{(I)} \to M$, pues siempre existe un sistema de generadores (por ejemplo $I = M$). Lo que dice el hecho de que M sea finitamente generado es que se puede extraer un subconjunto finito de I, de digamos n elementos, de manera tal que la proyección $A^n \to M$ siga siendo un epimorfismo. Más aún, en esta afirmación se puede cambiar el módulo que aparece sumado con el índice I (es decir A) para pasar a un enunciado más genérico:

Proposición 4.3.1. *Sea A un anillo y M un A-módulo. Las siguientes afirmaciones son equivalentes:*

(a) M es finitamente generado.

(b) Si $\{N_i\}_{i\in I}$ es una familia arbitraria de A-módulos y

$$f : \bigoplus_{i\in I} N_i \to M$$

es un epimorfismo, entonces existe un subconjunto finito $F \subseteq I$ tal que la restricción

$$f|_{\bigoplus_{i\in F} N_i} : \bigoplus_{i\in F} N_i \to M$$

es un epimorfismo.

Demostración. (b) $\Rightarrow$ (a) Esta implicación es evidente si aplicamos la hipótesis al epimorfismo $A^{(M)} \to M$ tal que $e_m \mapsto m$ para todo $m \in M$. Extrayendo un subconjunto finito de índices se obtiene precisamente un subconjunto finito de generadores.

(b) $\Rightarrow$ (a) Sea $\{m_1, \ldots, m_r\} \subset M$ un subconjunto finito que genera a M y sea $f : \bigoplus_{i\in I} N_i \to M$ un epimorfismo. Entonces, para cada $k \in \{1, \ldots, r\}$, existe $z^k = (z_i^k)_{i\in I} \in \bigoplus_{i\in I} N_i$ tal que

$$f(z^k) = \sum_{i\in I} f(z_i^k) = m_k.$$

Ahora bien, como $z^k = (z_i^k)_{i\in I} \in \bigoplus_{i\in I} N_i$, $z_i^k = 0$ salvo a lo sumo para un número finito de índices $i \in I$. Existe entonces un conjunto finito $F \subset I$ tal que si $i \notin F$, es $z_i^k = 0$ para todo $k \in \{1, \ldots, r\}$.

Consideremos la restricción $f|_{\bigoplus_{i\in F} N_i} : \bigoplus_{i\in F} N_i \to M$. Dado que $z^k \in \bigoplus_{i\in F} N_i$, es $m_k \in \mathrm{Im}(f|_{\bigoplus_{i\in F} N_i})$, y entonces $f|_{\bigoplus_{i\in F} N_i}$ es un epimorfismo porque los m_k generan M. □

Esta condición equivalente a ser finitamente generado puede ser dualizada (en el sentido categórico) sin problemas.

Definición 4.3.2. Diremos que un A-módulo M es *finitamente cogenerado* si para cada familia de A-módulos $\{N_i\}_{i\in I}$ y cada monomorfismo $f = \prod_{i\in I} f_i : M \to \prod_{i\in I} N_i$, existe un subconjunto finito $F \subseteq I$ tal que $\prod_{i\in F} f_i : M \to \prod_{i\in F} N_i$ es un monomorfismo.

Observación. La condición de la definición es equivalente a decir que la condición $\bigcap_{i\in I} \mathrm{Ker}(f_i) = \{0\}$ implica que existe un subconjunto finito $F \subseteq I$ tal que $\bigcap_{i\in F} \mathrm{Ker}(f_i) = \{0\}$.

Observamos que si M es un A-módulo finitamente cogenerado y $N \subseteq M$ es un submódulo, entonces N también es finitamente cogenerado. Por otro lado, un cociente de un módulo finitamente cogenerados no tiene por qué ser finitamente cogenerados.

Definición 4.3.3. Decimos que un A-módulo M es *artiniano* si todo cociente de M es finitamente cogenerado. Decimos que el anillo A es *artiniano a izquierda* si A es artiniano como A-módulo a izquierda.

Ejemplo. $\mathbb{Z}$ no es un $\mathbb{Z}$-módulo artiniano, porque si $a \in \mathbb{Z} - \{0, \pm 1\}$, la aplicación $\mathbb{Z} \to \prod_{n\in\mathbb{N}} \mathbb{Z}/\langle a^n\rangle$ definida por $x \mapsto \{\overline{x}\}_{n\in\mathbb{N}}$ es un monomorfismo (porque para cada $m \in \mathbb{Z}$ basta tomar $n \in \mathbb{N}$ tal que $|m| < |a|^n$ para que su clase módulo $a^n\mathbb{Z}$ sea distinta de cero) y, sin embargo, para cualquier subconjunto finito $F \subset \mathbb{N}$, la corestricción $\mathbb{Z} \to \prod_{n\in F} \mathbb{Z}/\langle a^n\rangle$ no es un monomorfismo.

A continuación daremos propiedades equivalentes a la definición de módulo artiniano, que permitirán encontar más fácilmente ejemplos de tales módulos.

Observación. Si M es finitamente cogenerado, entonces M tiene la siguiente propiedad:

> Para toda familia $\{M_i\}_{i\in I}$ de A-submódulos de M, $\bigcap_{i\in I} M_i = 0$ implica que existe un subconjunto finito $F \subseteq I$ con $\bigcap_{i\in F} M_i = 0$. (†)

Para verlo, basta tomar $\prod \pi_i : M \to \prod_{i \in I} M/M_i$ y mirar los núcleos.

Recíprocamente, si M satisface la propiedad (†), entonces M es finitamente cogenerado.

Al igual que en el contexto de módulos noetherianos, la condición de ser artiniano puede expresarse en términos del reticulado de submódulos :

Proposición 4.3.4. *Sea M un A-módulo. Las siguientes afirmaciones son equivalentes:*

(a) M es artiniano.
(b) Toda cadena decreciente de submódulos de M se estaciona.
(c) Todo conjunto no vacío de submódulos de M tiene un elemento minimal.

Nos referimos a la segunda condición del enunciado como la *condición de cadena descendente*.

Demostración. (a) $\Rightarrow$ (b) Supongamos M es artiniano y sea $\mathcal{C}$ una cadena decreciente

$$L_1 \supseteq L_2 \supseteq \cdots L_n \supseteq L_{n+1} \supseteq \cdots$$

de submódulos de M. Sea $K = \bigcap_{n \in \mathbb{N}} L_n$, que es justamente el núcleo de la aplicación $\prod_{n \in \mathbb{N}} \pi_n : M \to \prod_{n \in N} M/L_n$. Consideremos la aplicación inducida $M/K \to \prod_{n \in N} M/L_n$ que es un monomorfismo. Como M/K es finitamente cogenerado, existe $m \in \mathbb{N}$ tal que tal que la restricción $M/K \to \prod_{n<m} M/L_n$ es un monomorfismo, así que $K = \bigcap_{n \in \mathbb{N}} L_n = \bigcap_{n<m} L_n = L_{m-1}$. Esto nos dice que $\mathcal{C}$ se estaciona a partir de L_{m-1}.

(b) $\Rightarrow$ (c) . Supongamos que M satisface la condición de cadena descendente y sea S un subconjunto no vacío de submódulos de M. Supongamos que S no tiene elemento minimal. Entonces para todo $L \in S$ el conjunto $\{L' \in S : L' \subsetneq L\}$ es no vacío.

Sea $L_1 \in S$ unelemento arbitrario. Como L_1 no es minimal, existe $L_2 \in S$ tal que $L_2 \subsetneq L_1$. De la misma forma, como L_2 no es minimal, existe $L_3 \in S$ tal que $L_3 \subsetneq L_2$. Procediendo de esta manera, obtenemos una cadena

$$L_1 \supsetneq L_2 \supsetneq \cdots L_n \supsetneq L_{n+1} \supsetneq \cdots$$

que no se estaciona, lo cual es absurdo. Vemos que S debe contener un elemento minimal.

(c) ⇒ (a) Supongamos que todo conjunto no vacío de submódulos de M tiene un submódulo minimal. Sea $K \subseteq M$ un submódulo, $\{N_i\}_{i\in I}$ una familia de A-módulos y $f : M/K \to \prod_{i\in I} N_i$ un monomorfismo. Sea $i_0 \in I$ y M_{i_0} el núcleo de la composición $M \to M/K \to \prod_{i\in I} N_i \to N_{i_0}$. Es fácil ver que $K = \bigcap_{i\in I} M_i$. Para ver que M es artiniano, bastará probar entonces que si $K \subseteq M$ es un submódulo y S es una colección de submódulos de M con $K = \bigcap_{M'\in S} M'$, entonces existe $S' \subset S$ finito tal que $K = \bigcap_{M'\in S'} M'$.

Consideremos la familia de submódulos de M

$$\mathscr{P} = \Big\{ \bigcap_{M'\in F} M' : F \subset S \text{ es finito} \Big\}.$$

Usando *(c)*, concluimos que $\mathscr{P}$ tiene un elemento minimal, esto es, que existe $F_0 \subset S$ finito tal que $K' = \bigcap_{M'\in F_0} M'$ es un elemento minimal de $\mathscr{P}$. La construcción hecha permite mostrar fácilmente que $K' = K$. □

Ejemplos.
1. $\mathbb{Z}_{p^\infty} \cong G_{p^\infty}$ es un $\mathbb{Z}$-módulo artiniano. Para verlo, observamos que sus únicos submódulos son $\{1\}$, G_{p^∞} y los $(G_{p^n})_{n\in\mathbb{N}}$ y que estos forman una cadena. Como todos salvo G_{p^∞} son finitos, toda cadena descendente de submódulos se estaciona.

2. Si k es un cuerpo y V un k-espacio vectorial, entonces V es artiniano si y sólo si es de dimensión finita.

3. Sea A un anillo que contiene un cuerpo k y M un A-módulo. Claramente podemos ver a M como un k-espacio vectorial. Si M es de dimensión finita sobre k, entonces M es artiniano como A-módulo.

A continuación enunciamos algunas propiedades de los módulos artinianos cuyas demostraciones omitimos ya que son análogas al caso noetheriano.

Proposición 4.3.5. *Si A es un anillo artiniano a iquierda y M es un A-módulo finitamente generado, entonces M es un A-módulo artiniano.* □

Proposición 4.3.6. *Sea*

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$$

una sucesión exacta corta de A-módulos. Entonces M es artiniano si y sólo si L y N lo son. □

Proposición 4.3.7. *Sea $(M_i)_{1\leq i\leq n}$ una familia finita de A-módulos. Entonces $\bigoplus_{i=1}^n M_i$ es artiniano si y sólo si el sumando M_i es artiniano para todo $i \in \{1,\dots,n\}$.* □

Definición 4.3.8. Un módulo se dice *indescomponible* si no admite sumandos directos propios.

Una de las propiedades más importantes de los módulos noetherianos o artinianos es que admiten una descomposición en suma directa finita de submódulos indescomponibles. Notemos que esto no es cierto si se pide que el módulo sea finitamente generado.

Proposición 4.3.9. *Sea M un A-módulo noetheriano o artiniano no nulo. Entonces existen submódulos indescomponibles $M_1, \dots, M_n$ tales que $M \cong \bigoplus_{i=1}^n M_i$.*

Demostración. Digamos que un submódulo X de M es malo si no es suma directa de submódulos indescomponibles. Queremos mostrar que si M es artiniano o noetheriano, entonces M no es malo.

Observemos primero que

$$\text{Si } X \subset M \text{ es un submódulo malo, entonces } X \text{ posee un sumando directo propio } Y \subset X \text{ que es malo.} \tag{4.2}$$

En efecto, si X es malo, no puede ser indescomponible, así que existen submódulos Y, $Y' \subset X$ tales que $X = Y \oplus Y'$. Pero entonces alguno de Y o Y' debe ser malo.

Supongamos que M es malo. Escribamos $Y_{-1} = M$. Por (4.2), existen submódulos propios Y_0, $Z_0 \subset M$ tales que $M = Y_0 \oplus Z_0$ y Z_0 es malo. Supongamos ahora, inductivamente, que $n \geq 0$ y que hemos construido submódulos $Y_0, \dots, Y_n$, $Z_0, \dots Z_n$ de M tales que

- $Y_i = Y_{i+1} \oplus Z_{i+1}$ si $-1 \leq i < n$;
- Z_i es malo si $0 \leq i \leq n$

Aplicando (4.2) a Z_n, vemos que existen submódulos no nulos Y_{n+1} y Z_{n+1}, no nulos y estrictamente contenidos en Z_n, tales que Z_{n+1} es malo y $Z_n = Y_{n+1} \oplus Z_{n+1}$. Esto completa la inducción.

De esta forma, obtenemos una cadena estrictamente decreciente

$$Z_0 \supsetneq Z_1 \supsetneq \cdots Z_n \supsetneq Z_{n+1} \supsetneq \cdots$$

y una cadena estrictamente creciente

$$Y_0 \subsetneq Y_0 \oplus Y_1 \subsetneq \cdots \subsetneq \bigoplus_{i=1}^{n} Y_i \subsetneq \bigoplus_{i=0}^{n+1} Y_i \subsetneq \cdots$$

de sumbódulos de M. Luego M no puede ser ni artiniano ni noetheriano. □

4.4 Ejercicios

4.4.1. Un A-módulo es finitamente generado si es isomorfo a un cociente de A^n para algún $n \in \mathbb{N}$-

4.4.2. Si

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

es una sucesión exacta corta de A-módulos a izquierda y M' y M'' son finitamente generados, entonces M es finitamente generados.

4.4.3. Sea A un anillo, M un A-módulo a izquierda finitamente generado y sea $f : M \to A^n$ un morfismo sobreyectivo de A-módulos. Muestre que $\ker f$ es finitamente generado.

4.4.4. Muestre que existen módulos finitamente generados que no son noetherianos y módulos tales que todos sus submódulos propios son finitamente generados pero que no son noetherianos.

4.4.5. Un k-espacio vectorial V es noetheriano sii $\dim_k V < \infty$.

4.4.6. Un anillo principal a izquierda es noetheriano a izquierda.

4.4.7. Sea A un anillo. Sea M un A-módulo a izquierda y consideremos un endomorfismo $f \in \mathrm{End}_A(M)$. Si $n \in \mathbb{N}_0$, pongamos $K_n = \ker f^n$ y $I_n = \mathrm{Im}\, f^n$. Entonces:

(a) $K_1 = K_2 \implies K_1 \cap I_1 = 0$;
(b) $I_1 = I_2 \implies K_1 + I_1 = M$;
(c) si M es noetheriano, existe $n \in \mathbb{N}_0$ tal que $K_n \cap I_n = 0$;
(d) si M es noetheriano y f es sobreyectivo, entonces f es un automorfismo.

4.4.8. Sea $d \in \mathbb{Z}$ y sea $\sqrt{d} \in \mathbb{C}$ una raíz cuadrada de d. Muestre que el anillo $\mathbb{Z}[\sqrt{d}]$ es noetheriano.

4.4.9. Sea k un cuerpo, V un k-espacio vectorial de dimensión infinita y $A = \mathrm{End}_k(V)$ el anillo de endomorfisos de V. Muestre que existe un A-módulo M no nulo tal que $M \cong M \oplus M$.

4.4.10. *Anillos de matrices.* Sea $n \in \mathbb{N}$.

(a) Un anillo A es noetheriano a izquierda sii $M_n(A)$ es noetheriano a izquierda.

(b) Un anillo A es noetheriano a izquierda sii $M_n(A)$ es noetheriano a izquierda.

4.4.11. Un dominio integro artiniano es un cuerpo.

4.4.12. *Extensiones finitas de anillos.* Sea B un subanillo de un anillo A tal que A es finitamente generado como B-módulo a izquierda. Si B es noetheriano a izquierda, entonces A es noetheriano a izquierda.

4.4.13. *Algebras de matrices.* Sean A y B anillos y M y N un A-B-bimódulo y un B-A-bimódulo, respectivamente. Sea

$$T = \begin{pmatrix} A & M \\ N & B \end{pmatrix}$$

el álgebra de matrices. Entonces T es noetheriana a derecha sii A y B son anillos noetherianos a derecha y M es un B-módulo noetheriano y N es un A-módulo noetheriano.

4.4.14. *Polinomios de Laurent.* Sea k un cuerpo y sea $A = k[X, X^{-1}]$ el anillo de polinomios de Laurent con coeficientes en k. Muestre que A es noetheriano.

Sugerencia. Imite la demostración del teorema de Hilbert para $k[X]$.

4.4.15. *Extensiones de Ore.* Sea A un anillo y sea $\sigma : A \to A$ un homomorfismo de anillos.

(a) Muestre que existe exactamente una estructura de anillo sobre el grupo abeliano $B = A[X]$ de polinomios con coeficientes a izquierda en A en una variable X tal que

$$Xa = \sigma(a)X, \qquad \forall a \in A.$$

Escribimos $A[X;\sigma]$ al anillo correspondiente.

(b) Si σ es inyectivo y A es un dominio, entonces $A[X;\sigma]$ es un dominio.

(c) Si σ es inyectivo y A es un anillo de división, entonces $A[X;\sigma]$ es un dominio de ideales principales.

(d) Si σ es automorfismo y A es noetheriano a izquierda (derecha), entonces $A[X;\sigma]$ es noetheriano a izquierda (derecha).

4.4.16. *Extensiones de Ore, II.* Sea A un anillo y sea $\sigma : A \to A$ un homomorfismo de anillos. Una *σ-derivación* de A es un homomorfismo de grupos $\delta : A \to A$ que satisface

$$\delta(ab) = \delta(a)\sigma(b) + a\delta(b), \qquad \forall a, b \in A.$$

Si $\sigma = \mathsf{Id}_A$, decimos simplemente que δ es una *derivación* de A.

(a) Muestre que existe exactamente una estructura de anillo sobre el grupo abeliano $B = A[X]$ de polinomios con coeficientes a izquierda en A en una variable X tal que

$$Xa = \sigma(a)X + \delta(a), \qquad \forall a \in A.$$

Escribimos $A[X; \sigma, \delta]$ al anillo correspondiente.

(b) Si σ es inyectivo y A es un dominio, entonces la extensión $A[X; \sigma, \delta]$ es un dominio.

(c) Si σ es inyectivo y A es un anillo de división, entonces la extensión $A[X; \sigma, \delta]$ es un dominio de ideales principales.

(d) Si σ es automorfismo y A es noetheriano a izquierda (derecha), entonces $A[X; \sigma, \delta]$ es noetheriano a izquierda (derecha).

4.4.17. Sea $A = k[X]$, $\sigma = \mathsf{Id}_A : A \to A$ y $\delta = \frac{\partial}{\partial X} : A \to A$.

(a) Muestre que δ es una derivación de A.

(b) Muestre que el álgebra de Weyl A_1 es isomorfa a $A[X; \sigma, \delta]$. En particular, concluya que A_1 es noetheriana.

Capítulo 5

Módulos libres, proyectivos e inyectivos

5.1 Módulos libres

En el caso de espacios vectoriales, la existencia de bases es una herramienta que permite, por ejemplo, definir transformaciones lineales indicando su valor en los elementos de una base, y luego extendiendo por linealidad. A su vez ésto asegura, entre otras cosas, que si V y W son k-espacios vectoriales y $t : V \to W$ es una transformación lineal suryectiva, existe entonces una transformación lineal $f : W \to V$ tal que $t \circ f = \mathrm{Id}_W$. En otras palabras, las nociones de epimorfismo y retracción coinciden en la categoría de espacios vectoriales.

Sabemos que existen anillos A tales que ésto no sucede en la categoría de A-módulos. Habrá, por lo tanto, módulos en los que no se pueda encontrar subconjuntos privilegiados que jueguen el rol de las bases en los espacios vectoriales sobre los cuales por ejemplo uno pueda definir una inversa a derecha de un epimorfismo. Aún conociendo un sistema de generadores, las posibles relaciones que pudiera haber entre ellos hacen que uno no pueda extender por linealidad funciones definidas sobre este subconjunto. Esto mismo sucedía con los sistemas de generadores de un espacio vectorial, pero el problema desaparecía eligiendo un subconjunto de generadores que fuera linealmente independiente. Este proceso no puede copiarse al caso general, el siguiente ejemplo muestra que la noción

de base en un A-módulo es más sutil que en espacios vectoriales:

Ejemplo. Consideremos a $\mathbb{Z}$ como $\mathbb{Z}$-módulo. El conjunto $\{2,3\}$ es un sistema de generadores de $\mathbb{Z}$ que no es "linealmente independiente" sobre $\mathbb{Z}$ (es claro que por ejemplo $3 \cdot 2 + (-2) \cdot 3 = 0$) y sin embargo es minimal en el sentido de que si se extrae un subconjunto propio, deja de ser un sistema de generadores. Por otro lado, $\{1\}$ (o también $\{-1\}$) es un sistema de generadores minimal que merece ser llamado base.

Definición 5.1.1. Dado un anillo A, un A-módulo M y un subconjunto $S \subset M$ diremos que S es un *conjunto linealmente independiente* de A si toda combinación lineal finita de elementos de S con coeficientes en A no todos nulos es no nula.

Ejemplos.
1. Si $M = A$, el conjunto $\{1\}$ es linealmente independiente. Si $a \in A$ es un divisor de cero, entonces $\{a\}$ no es linealmente independiente.

2. Sea $A = M_2(k)$ y $M = \{\left(\begin{smallmatrix} 0 & x \\ 0 & y \end{smallmatrix}\right) \in M_2(k)\}$. M es un A-módulo a izquierda y el conjunto $\{\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)\}$ es un sistema de generadores minimal, que no es linealmente independiente. Probar que no existen conjuntos de generadores que sean linealmente independientes.

3. Si $A = \mathbb{Z}$ y $M = \mathbb{Z}_n$ entonces ningún subconjunto de M es linealmente independiente.

4. Si $r, s \in \mathbb{Z}$, entonces $\{r, s\}$ es siempre un conjunto linealmente dependiente.

5. Sean $A = \mathbb{Z}$ y $M = \mathbb{Q}$. Si $0 \neq r \in \mathbb{Q}$, entonces $\{r\}$ es un conjunto linealmente independiente. Si $r, s \in \mathbb{Q}$, entonces $\{r, s\}$ es siempre linealmente dependiente.

Observación. A partir del ejemplo 3. se observa que un subconjunto linealmente independiente no puede tener elementos de torsión. En el ejemplo 1, $\{1\}$ no sólo es linealmente independiente sino que además genera.

Algunas de las propiedades que tienen los subconjuntos linealmente independientes y los conjuntos de generadores de un espacio vectorial pueden generalizarse al caso de módulos sobre un anillo A con demostraciones análogas, por ejemplo:

Proposición 5.1.2. *Sea $f : M \to N$ un morfismo de A módulos y $S \subset M$ un subconjunto.*

(a) Si S es un conjunto linealmente dependiente entonces $f(S)$ es un conjunto linealmente dependiente.
(b) Si S es un conjunto linealmente independiente y f es un monomorfismo, entonces $f(S)$ es un conjunto linealmente independiente.
(c) Si S es un conjunto de generadores y f es un epimorfismo entonces $f(S)$ es un conjunto de generadores de N.

Diremos que un subconjunto $S \subset M$ es una *base* de M si y sólo si S es linealmente independiente y S genera M.

Observación. No todo A-módulo M tiene una base. Por ejemplo, el $\mathbb{Z}$-módulo $\mathbb{Z}_n$.

Definición 5.1.3. Un A-módulo M se dice *libre* si M admite una base

Ejemplos.
1. Si k es un cuerpo, todo k-espacio vectorial es libre.

2. Si A es un anillo, entonces A es un A-módulo libre. Una base, es por ejemplo, el conjunto $\{1\}$.

3. $\mathbb{Q}$ no es un $\mathbb{Z}$-módulo libre, ya que todo par de elementos es linealmente dependiente: si $\mathbb{Q}$ fuera un $\mathbb{Z}$-módulo libre, la base tendría a lo sumo un elemento y $\mathbb{Q}$ sería un $\mathbb{Z}$-módulo cíclico. Pero entonces sería isomorfo a $\mathbb{Z}$ o a $\mathbb{Z}_n$ como $\mathbb{Z}$-módulo.

4. Sea V un k-espacio vectorial de dimensión finita y $t : V \to V$ una transformación lineal. El par (V, t) es un $k[x]$-módulo que no es libre, ya que todo elemento es de torsión: si $p = m_t$, entonces $pv = 0$ para todo $v \in V$.

Observaciones.
1. Un cociente de un A-módulo libre M no tiene por qué ser libre: por ejemplo el grupo abeliano $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ no es $\mathbb{Z}$-libre.

2. Un submódulo de un A-módulo libre no es necesariamente libre. Por ejemplo, si un A-módulo libre contiene un elemento de torsión, entonces el submódulo generado por ese elemento no es libre.

Como ejemplo concreto, podemos tomar $M = A = \mathsf{M}_2(\mathbb{Z})$, que es A-libre con base $\{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\}$ y, sin embargo, $N = \{\left(\begin{smallmatrix} a & 0 \\ b & 0 \end{smallmatrix}\right) : a, b \in \mathbb{Z}\}$ es un submódulo de torsión de M, que por lo tanto no puede tener una base como A-módulo.

3. Sean M y N dos A-módulos. Si M es libre y $f : M \to N$ es un isomorfismo, entonces N es libre.

4. Sea $A^{(I)} = \{f : I \to A : \text{sop}(f) < \infty\}$. $A^{(I)}$ es un A-módulo libre con base $\{e_i\}_{i\in I}$, donde, para todo $i \in I$, e_i es la función definida por $e_i(j) = \delta_{ij}$.

5.2 El A-módulo libre generado por un conjunto X

Sea X un conjunto.

Definición 5.2.1. Un *A-módulo libre sobre X* es un A-módulo $L_A(X)$ con una función $j_X : X \to L_A(X)$ tal que si M es un A-módulo arbitrario y $f : X \to M$ es una función, entonces existe un único morfismo de A-módulos $\overline{f} : L_A(X) \to M$ tal que $\overline{f} \circ j_X = f$.

Notemos que la unicidad dice que si ϕ, $\psi : L_A(X) \to M$ son morfismos de A-módulos tales que $\phi \circ j_X = \psi \circ j_X$, entonces $\phi = \psi$. En el caso de los espacios vectoriales, esto dice precisamente que basta definir los morfismos sobre una base.

Lema 5.2.2. *Si existe un A-módulo libre sobre X entonces, éste es único salvo isomorfismos.* □

Teorema 5.2.3. *Para todo conjunto X existe un A-módulo libre sobre X.*

Demostración. Sea $L_A(X) = A^X = \bigoplus_{x\in X} A$ y sea $j_X : X \to L_A(X)$ definida por $j_X(\lambda) = e^\lambda = (e^\lambda_\mu)_{\mu\in X}$ tal que $e^\lambda_\mu = \delta_{\lambda\mu}$. Todo elemento de $L_A(X)$ se escribe como $\sum_{\lambda\in X} a_\lambda e^\lambda$ con soporte $\text{sop}(a_\lambda)$ finito.

Si M es un A-módulo y $f : X \to M$ es una función, hay una única aplicación tal que

$$\overline{f}(\sum_{\lambda\in X} a_\lambda e^\lambda) = \sum_{\lambda\in X} a_\lambda \overline{f}(e^\lambda) = \sum_{\lambda\in X} a_\lambda \overline{f}(j_X(\lambda)) = \sum_{\lambda\in X} a_\lambda f(\lambda).$$

Es claro que $\overline{f}$ es A-lineal y que $\overline{f} \circ j_X = f$ □

Ejemplos.
1. Si $X = \{*\}$ es un conjunto con un único elemento, entonces $L_A(X) \cong A$.

2. Si $X = \mathbb{N}$, entonces $L_A(X) \cong A^{\mathbb{N}}$.

A continuación caracterizaremos los A-módulos libres, mostrando que todo A-módulo libre es isomorfo a un módulo del tipo $A^{(I)}$, para algún conjunto I.

Proposición 5.2.4. *Si M es un A-módulo, las siguientes afirmaciones son equivalentes:*

(a) M es un A-módulo libre con base $\{x_i\}_{i\in I}$.
(b) Sea $\rho_i : a \in A \mapsto ax_i \in M$. Entonces $\rho = \oplus_{i\in I}\rho_i : A^{(I)} \to M$ es un isomorfismo, o sea que M es un A-módulo libre sobre I.
(c) Para todo A-módulo N y para todo subconjunto $\{y_i\}_{i\in I} \subset N$, existe un único morfismo de A-módulos $f : M \to N$ tal que $f(x_i) = y_i$.

Demostración. (a) $\Rightarrow$ (b) Sea $z \in A^{(I)}$ tal que $\rho(z) = 0$. Escribamos $z = \sum_{i\in I} a_i e_i$, con la familia $(a_i)_{i\in I} \subset A$ de soporte finito. Entonces $0 = \rho(z) = \sum_{i\in I} a_i x_i$. Como el conjunto $\{x_i : i \in I\}$ es linealmente independiente, los a_i deben ser todos cero. Luego $z = 0$ y consecuentemente ρ es un monomorfismo. Por otro lado $\rho(e_i) = x_i$, así que la imagen de ρ contiene a un conjunto de generadores. Esto nos dice que ρ también es un epimorfismo, así que es un isomorfismo.

(b) $\Rightarrow$ (c) La demostración es igual que para el caso de espacios vectoriales. En primer lugar, está claro que de existir un tal morfismo, es único, pues está determinado su valor en los x_i y éstos generan a M. Para demostrar la existencia se extiende linealmente el valor de f en la base. Si $x \in M$, por ser $\{x_i\}_{i\in I}$ un sistema de generadores, $x = \sum_{i\in I} a_i x_i$ (suma con soporte finito) y esa escritura es única debido a la independencia lineal (en efecto, si $\sum_{i\in I} a_i x_i = \sum_{i\in I} a'_i x_i$, entonces $\sum_{i\in I}(a_i - a'_i)x_i = 0$ y vemos que $a_i - a'_i = 0$ para todo $i \in I$). Luego está bien definida la función $f(x) = \sum_{i\in I} a_i y_i$. La verificación de que f es un morfismo de A-módulos es inmediata.

(c) $\Rightarrow$ (a) Veremos que si M satisface *(c)*, entonces $M \cong A^{(I)}$. Sean $N = A^{(I)}$ e $y_i = e_i$ para todo $i \in I$. Entonces existe un único morfismo $f : M \to A^{(I)}$ tal que $f(x_i) = e_i$. Consideremos la composición $\rho \circ f : M \to M$. Como $\rho \circ f(x_i) = x_i$, es claro que $\rho \circ f$ coincide con Id_M en los x_i. Luego, (eligiendo $N = M$ e $y'_i = x_i$) por

la unicidad, $\rho \circ f = \mathsf{Id}_M$. Por otro lado, se tiene

$$f \circ \rho\big(\sum_{i\in I} a_i e_i\big) = f\big(\sum_{i\in I} a_i x_i\big) = \sum_{i\in I} a_i f(x_i) = \sum_{i\in I} a_i e_i,$$

así que $f \circ \rho = \mathsf{Id}_{A^{(I)}}$. Vemos así que M es isomorfo a $A^{(I)}$, que es libre de base $\{e_i\}_{i\in I}$. Además, resulta que ρ es también un isomorfismo: esto dice que $\{f(e_i)\}_{i\in I} = \{x_i\}_{i\in I}$ es una base de M. □

Corolario 5.2.5. *Con las notaciones de la proposición anterior, se tiene que:*

(a) Si $\{y_i\}_{i\in I}$ es una base de N, entonces f es un isomorfismo.
(b) Dos A-módulos con bases de igual cardinal son isomorfos.

Demostración. Dejamos la demostración como ejercicio. □

Observación. Si $(M_j)_{j\in J}$ es una familia de A-módulos libres, entonces el A-módulo $\bigoplus_{j\in J} M_j$ es libre. Más aún, si $\{x_i^j : i \in I_j\}$ es una base de M_j para cada $j \in J$, entonces $\{x_i^j : j \in J, i \in I_j\}$ es una base de $\bigoplus_{j\in J} M_j$.

Vimos que la propiedad de "ser libre" no es estable en general ni por cocientes ni por submódulos. Veremos ahora sin embargo que todo módulo es cociente de un libre:

Proposición 5.2.6. *Sea M un A-módulo. Entonces existe un A-módulo libre L y un epimorfismo $f : L \to M$.*

Demostración. Sea $\{x_i\}_{i\in I}$ un sistema de generadores para M. Por ejemplo, podemos tomar $\{m\}_{m\in M}$. Sea $L = A^{(I)}$; se trata de un A-módulo libre. El morfismo $h : A^{(I)} \to M$ que sobre los elementos de la base canónica de $A^{(I)}$ vale $h(e_i) = x_i$, es un epimorfismo, porque la imagen contiene a un sistema de generadores. Se tiene, además, que $M \cong L/\operatorname{Ker} h$. □

El submódulo $\operatorname{Ker} h$ de L construido en esta demostración suele llamarse el núcleo de relaciones de M.

Teorema 5.2.7. *Sea A es un anillo de división, M un A-módulo y X un sistema de generadores de M. Si $E \subseteq X$ es un subconjunto linealmente independiente, entonces existe un conjunto B tal que $E \subseteq B \subseteq M$ y B es base de M.*

Demostración. Sea

$$\mathcal{E} = \{\mathcal{E}' : E' \subseteq M, E \subseteq E' \subseteq X \text{ y } E' \text{ es linealmente independiente}\},$$

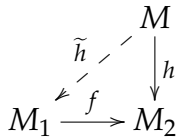
ordenado por inclusión. Observemos que este conjunto no es vacío, ya que $E \in \mathcal{E}$. Si $\mathcal{F}$ es una cadena creciente contenida en $\mathcal{E}$, pongamos $E'' = \bigcup_{Y \in \mathcal{F}} Y$. Entonces E'' es un conjunto linealmente independiente. y $E \subseteq E'' \subseteq X$. Luego E'' es una cota superior de $\mathcal{F}$ en $\mathcal{E}$. Por el Lema de Zorn, entonces, $\mathcal{E}$ tiene algún elemento maximal B.

El conjunto B es linealmente independiente y $E \subseteq B \subseteq X$. Falta ver que B genera a M. Para eso es suficiente mostrar que B genera a X. Sea $x \in X$. Si $x \in B$, no hay nada que hacer. Si no, como B es maximal en $\mathcal{E}$, $B \cup \{x\}$ no es linealmente independiente, así que existe una combinación lineal $ax + \sum_\lambda a_\lambda x_\lambda = 0$ con $a \in A$ no nulo y $a_\lambda \in A, x_\lambda \in B$. Como A es un anillo de división podemos despejar $x = -\sum_\lambda a^{-1} a_\lambda x_\lambda$. □

Corolario 5.2.8. *Si A es un anillo de división, entonces todo A-módulo no nulo es libre.* □

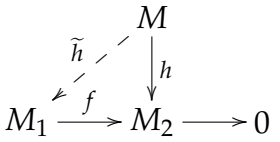
Observemos que si M es un A-módulo libre y $f : N \to M$ es un epimorfismo, entonces existe una sección $g : M \to N$ tal que $f \circ g = \mathsf{Id}_M$. En efecto, si $\{x_i\}_{i \in I}$ es una base de M, existen $n_i \in N$ tales que $f(n_i) = x_i$ porque f es un epimorfismo y podemos definir entonces $g(x_i) = n_i$ y extender por linealidad. Vemos así que todo epimorfismo con imagen en un módulo libre M es una retracción.

De manera análoga, puede probarse que los módulos libres tienen una propiedad de "levantamiento" de morfismos. Consideremos el siguiente diagrama de flechas llenas:



Nos preguntamos si existe un morfismo $\widetilde{h}$ en la dirección de la flecha punteada que haga el diagrama conmutativo, esto es, para el cual se tenga que $f \circ \widetilde{h} = h$. En principio, de levantarse h a un morfismo $\widetilde{h}$, debería valer que $\mathrm{Im}(h) = \mathrm{Im}(f \circ \widetilde{h}) \subseteq \mathrm{Im}(f)$ así que, restringiéndonos entonces al submódulo $\mathrm{Im}(f)$, supondremos que f es un epimorfismo.

Proposición 5.2.9. *Sea M un A-módulo libre. Entonces M resuelve el siguiente problema de tipo universal, esquematizado mediante el diagrama:*



Para cualquier epimorfismo $f : M_1 \to M_2$ entre dos A-módulos arbitrarios y para cualquier morfismo $h : M \to M_2$, existe un morfismo $\widetilde{h} : M \to M_1$ (no necesariamente único) tal que $f \circ \widetilde{h} = h$.

Demostración. Sea $\{x_i\}_{i\in I}$ una base de M. Como f es un epimorfismo, para cada x_i existe un $m_i \in M_1$ tal que $h(x_i) = f(m_i)$. Definimos $f : M \to M_1$ poniendo $\widetilde{h}(x_i) = m_i$ para cada $i \in I$ y extendiendo por linealidad. Como $f(\widetilde{h}(x_i)) = f(m_i) = h(x_i)$, entonces $f \circ \widetilde{h} = h$, ya que ambos morfismos coinciden en una base. □

Observamos que la propiedad de que todo epimorfismo que tiene como codominio a un libre es una retracción puede obtenerse como consecuencia de la proposición anterior, tomando $M_2 = M$ y $h = \mathsf{Id}_M$.

Corolario 5.2.10. *Sea M un A-módulo y $S \subseteq M$ un submódulo. Si M/S es libre, entonces S es un sumando directo de M.*

Demostración. Basta ver que la sucesión exacta corta

$$0 \longrightarrow S \xrightarrow{i} M \xrightarrow{\pi} M/S \longrightarrow 0$$

se parte. Pero como M/S es libre, $\pi : M \to M/S$ es una retracción, es decir, hay un morfismo $s : M/S \to M$ tal que $\pi \circ s = \mathsf{Id}_M/S$. Por lo tanto i es una sección y S es un sumando directo de M con proyector asociado $p = \mathsf{Id}_M - s \circ \pi$. □

Supongamos que A es un anillo tal que todo submódulo de un A-módulo libre es libre. En particular, todo ideal de A es libre. A continuación probaremos que esta afirmación sobre los ideales de A, que en principio parece más débil, resulta sin embargo equivalente a la primera:

Teorema 5.2.11. *Sea A un anillo. Las siguientes afirmaciones son equivalentes:*

(a) Todo submódulo de un A-módulo libre es libre.
(b) Todo ideal de A es A-libre.

Un anillo tal que todo submódulo de un libre es libre se denomina *hiperhereditario*.

Demostración. Una de las implicaciones es obvia. Veamos la otra. Supongamos que todo ideal de A es libre. Consideremos un A-módulo libre $M \neq 0$ con base $\{x_i : i \in I\}$ y sea S un submódulo de M. Notemos que, como M no es nulo, $I \neq \varnothing$. Por el Lema de Zorn, podemos suponer que I es un conjunto bien ordenado, es decir, que I tiene un orden tal que todo par de elementos es comparable y todo subconjunto no vacío de I tiene primer elemento.

Sean

$$F_i := \{x \in M : x \text{ es combinación lineal de los } x_j \text{ con } j < i\}$$

y

$$\overline{F}_i := \{x \in M : x \text{ es combinación lineal de los } x_j \text{ con } j \leq i\}.$$

Si $i < k$, resulta que $\overline{F}_i \subset \overline{F}_k$. Además, $M = \bigcup_{i \in I} \overline{F}_i$.

Sea $x \in S$. Existe i tal que $x \in S \cap \overline{F}_i$, así que existen únicos $a_x \in A$ y $x' \in S \cap F_i$ tal que $x = x' + a_x x_i$. Notemos que la unicidad se sigue de que $\{x_i : i \in I\}$ es base de M y $S \subseteq M$.

Consideremos ahora el morfismo $\phi : S \cap \overline{F}_i \to A$ definido por $\phi(x) = a_x$. (Ejercicio: verificar que es una función bien definida y que es un morfismo de A-módulos).

$\mathrm{Im}(\phi)$ resulta entonces un ideal de A, así que, en particular, es un A-módulo libre. Además $\mathrm{Ker}(\phi) = S \cap F_i$. Como

$$\mathrm{Im}(\phi) \cong \frac{S \cap \overline{F}_i}{S \cap F_i}$$

es libre, $S \cap F_i$ es un sumando directo de $S \cap \overline{F}_i$, esto es, existe un submódulo $C_i \subset M$ tal que $S \cap \overline{F}_i = (S \cap F_i) \oplus C_i$.

Queremos ver que $S = \bigoplus_{i \in I} C_i$. Esto implicará que S es libre, porque cada C_i lo es (notar que $C_i \cong \mathrm{Im}(\phi)$, que es libre). Es claro que cada C_i es un sumando directo de S. Queremos ver que $\bigoplus_{i \in I} C_i = S$.

Supongamos que no, y sea

$$H = \{j \in I : \text{existe } x \in S \cap \overline{F}_j \text{ con } x \notin \bigoplus_{i\in I} C_i\}.$$

Sea j_0 el primer elemento de J, que existe por el buen orden y porque $H \neq \varnothing$. Sea $z \in S \cap \overline{F}_{j_0}$ tal que $z \notin \bigoplus_{i\in I} C_i$. Entonces existe un único $z' \in S \cap F_{j_0}$ y un único $a \in A$ tal que $z = z' + ax_{j_0}$. Como j_0 es el primer elemento de H, z' es necesariamente una combinación lineal de x_k con $k < j_0$, así que $z' \in \oplus_{i\in I} C_i$ y por lo tanto $z \in \bigoplus_{i\in I} C_i$, lo que es absurdo. En consecuencia $S = \bigoplus_{i\in I} C_i$. □

Corolario 5.2.12. *Sea A un dip, es decir, un dominio íntegro tal que todo ideal es principal. Entonces todo submódulo de un módulo libre es libre. En particular, esto dirá que todo módulo proyectivo es libre.*

Demostración. Sea $0 \neq I \subset A$ un ideal. Como A es principal, existe $a \in A$ tal que $I = \langle a \rangle$. Como A es íntegro, $\{a\}$ es linealmente independiente (como $a \neq 0$, $ba = 0$ implica $b = 0$), así que $\{a\}$ es una base. Vemos que I es libre.

Como todo ideal de A es libre, la primera aserción se debe ahora al teorema anterior. Como todo módulo proyectivo es isomorfo a un sumando directo de un libre (en particular a un submódulo), resulta que todo módulo proyectivo es libre. □

Ejemplo. Como ejemplos en donde se aplica el corolario anterior, tenemos que todo subgrupo de un grupo abeliano libre es libre, en particular todo grupo abeliano proyectivo es libre. Análogamente, si k es un cuerpo, todo $k[x]$-submódulo de un $k[x]$-módulo libre es $k[x]$-libre. Lo mismo sucede con los anillos $k[x, x^{-1}]$ y $k[\![x]\!]$.

5.3 Noción de rango

Definición 5.3.1. Sea A un anillo. Diremos que A tiene *noción de rango* si $A^{(I)} \cong A^{(J)}$ implica $\#I = \#J$.

Veamos que si A es un cuerpo, o más generalmente si A es un anillo de división, entonces A tiene noción de rango. Si I y J son finitos, el resultado se obtiene fácilmente usando por ejemplo matrices. Si I o J es infinito, el resultado se sigue del siguiente lema:

Lema 5.3.2. *Sean k un cuerpo y V un k-espacio vectorial. Sea $\{v_i\}_{i\in I}$ una base de V y S un sistema de generadores de V. Supongamos que I es infinito. Entonces $\#S \geq \#I$.*

Demostración. Dado $x \in X$, sea

$$C_x = \{i \in I : \text{el coeficiente } i\text{-ésimo de } x \text{ es no nulo }\}.$$

Sea $C = \bigcup_{x\in S} C_x$. Como S genera V, entonces $C = I$: supongamos que C está incluido estrictamente en I y sea $i_0 \in I - C$. Como $v_{i_0} = \sum a_s s$ (con soporte finito) resulta combinación lineal de los otros elementos de la base. Luego S también es infinito y $\#I = \#C$. Como cada C_x es finito y los conjuntos C_x pueden intersecarse, se tiene que $\#C \leq \#S$. □

La siguiente proposición da otros ejemplos de anillos con noción de rango.

Proposición 5.3.3. *Sea A un anillo tal que existe un anillo de división D y un morfismo de anillos $f : A \to D$, entonces A tiene noción de rango.*

Demostración. D admite una estructura de A-módulo a partir de f. Sea L un A-módulo libre y $\{x_i\}_{i\in I}$, $\{y_j\}_{j\in J}$ dos bases de L. Sea finalmente $g : L \to A^{(J)}$ un isomorfismo.

El conjunto $\{g(x_i)\}_{i\in I}$ es una base de $A^{(J)}$. Si $\{e_j\}_{j\in J}$ es la base canónica de $A^{(J)}$, entonces existen elementos $a_{ij} \in A$ tales que, para todo $j \in J$, $e_j = \sum_{i\in I} a_{ij} g(x_i)$. El morfismo de A-módulos $f : A \to D$ induce un morfismo $h = f^{(J)} : A^{(J)} \to D^{(J)}$, que sobre los elementos de la base canónica vale $h(e_k) = \{f(\delta_{jk})\}_{j\in J} = \{\delta_{jk}\}_{j\in J}$, es decir, que da la base canónica de $D^{(J)}$. Como

$$h(e_k) = h\Big(\sum_{i\in I} a_{ik} g(x_i)\Big) = \sum_{i\in I} a_{ik} hg(x_i),$$

vemos que $\{hg(x_i)\}_{i\in I}$ genera a $D^{(J)}$ sobre D, de manera que es $\#I \geq \#J$. La desigualdad recíproca es se obtiene de manera análoga, así que $\#I = \#J$. □

Corolario 5.3.4. *Si A es un anillo conmutativo, entonces A tiene noción de rango.*

Demostración. A posee un ideal maximal $\mathfrak{m}$. Podemos considerar entonces la proyección canónica $A \to A/\mathfrak{m}$. □

Proposición 5.3.5. *Sea A un anillo con noción de rango y $M = \bigoplus_{i\in I} M_i$ un A-módulo tal que todos los A-módulos M_i son libres. Entonces M es libre y* $\operatorname{rg}(M) = \sum_{i\in I} \operatorname{rg}(M_i)$.

Demostración. Si para cada $i \in I$, $\{x_j\}_{j\in J_i}$ es una base de M_i, entonces es claro que $\{x_j : i \in I,\ j \in J_i\}$ es una base de M. □

Proposición 5.3.6. *Sea A un dominio principal, L un A-módulo libre de rango finito N y M un submódulo de L. Entonces M es libre y* $\operatorname{rg}(M) \leq n$.

Demostración. Sea $\{x_1, \ldots, x_n\}$ una base de L y, si $i \in \{1, \ldots, n\}$, $M_i = M \cap \langle x_1, \ldots, x_i\rangle$. En particular $M_1 = M \cap \langle x_1\rangle$ es un submódulo de $\langle x_1\rangle$ y, por lo tanto, existe $a \in A$ tal que $M_1 = \langle ax_1\rangle$. Si $a = 0$ entonces $M_1 = 0$ y si no $\operatorname{rg}(M_1) = 1$; en todo caso, $\operatorname{rg}(M_1) \leq 1$. Veamos inductivamente que para todo r, $\operatorname{rg}(M_r) \leq r$.

Supongamos que M_r es libre de rango menor o igual que r y sea

$$\mathcal{A} = \{a \in A : \exists b_1, \ldots, b_r \in A \text{ con } \sum_{i=1}^{r} b_i x_i + a x_{r+1} \in M_{r+1}\}.$$

Se puede ver fácilmente que $\mathcal{A}$ es un ideal de A y, como A es principal, existe $a_{r+1} \in A$ tal que $\mathcal{A} = \langle a_{r+1}\rangle$. Si es $a_{r+1} = 0$, entonces $M_{r+1} = M_r$ y por lo tanto $\operatorname{rg}(M_{r+1}) \leq r < r+1$. Si no, sea $x \in M_{r+1}$ y escribamos $x = \sum_{i=1}^{r+1} c_i x_i$. El coeficiente c_{r+1} resulta entonces divisible por a_{r+1}, así que existe $a \in A$ tal que $x - a a_{r+1} x_{r+1} \in M_r$. Esto dice que $M_{r+1} = M_r + \langle a_{r+1} x_{r+1}\rangle$, pero además esta suma es directa porque porque los x_i son linealmente independientes. Concluimos que $\operatorname{rg}(M_{r+1}) = \operatorname{rg}(M_r) + 1 \leq r + 1$. □

5.4 El funtor Hom

Si M y N son dos A-módulos a izquierda, consideremos el conjunto $\operatorname{Hom}_A(M, N)$ de los morfismos de A-módulos. Recordemos que es un grupo abeliano con respecto a la suma punto a punto, esto es, es un subgrupo de M^N.

Si k es un cuerpo, V un k-espacio vectorial de dimensión n y W un k-espacio vectorial de dimensión m, entonces sabemos que

$\mathrm{Hom}_k(V,W)$, además de ser un grupo abeliano, es un espacio vectorial de dimensión nm.

En el caso general de módulos sobre un anillo A, uno se pregunta sobre la estructura de $\mathrm{Hom}_A(M,N)$. En general, no es posible darle siempre una estructura de A-módulo: consideraremos a continuación las posibles estructuras de módulo sobre algún anillo que puede admitir $\mathrm{Hom}_A(M,N)$.

Sea B el anillo $\mathrm{End}_A(M)^{\mathrm{op}}$ y $C = \mathrm{End}_A(N)^{\mathrm{op}}$. M no sólo es un A-módulo a izquierda sino también un B-módulo a derecha y las acciones conmutan, es decir, M es un A-B-bimódulo. De manera similar, N es un A-C-bimódulo.

Como la composición de morfismos A-lineales es un morfismo A-lineal, la aplicación

$$\begin{aligned}(f,g,h) \in \mathrm{End}_A(M) \times \mathrm{Hom}_A(M,N) \times \mathrm{End}_A(N)& \\ \mapsto f \circ g \circ h \in \mathrm{Hom}_A(M,N)&\end{aligned}$$

provee a $\mathrm{Hom}_A(M,N)$ de una estructura de $\mathrm{End}_A(M)$-$\mathrm{End}_A(N)$-bimódulo.

Supongamos, más generalmente, que M no sólo es un A-módulo sino que existe un anillo B tal que M es un A-B-bimódulo y, similarmente, supongamos también que N es un A-C-bimódulo para algún anillo C. Para indicar este hecho, usaremos a veces la notación ${}_AM_B$ y ${}_AN_C$.

Afirmamos entonces que en estas condiciones $\mathrm{Hom}_A(M,N)$ admite una estructura de B-C-bimódulo, definiendo, para $b \in B$, $c \in C$ y $f \in \mathrm{Hom}_A(M,N)$,

$$(bf) : m \in M \mapsto f(mb) \in N$$

y

$$(fc) : m \in M \mapsto f(m)c \in N$$

Ejercicio. Verificar la asociatividad de las acciones y la compatibilidad de ambas.

Observaciones.
1. Si M y N son A-módulos, siempre puede tomarse $B = C = \mathbb{Z}$. Entonces M y N son A-$\mathbb{Z}$-bimódulos, de manera que $\mathrm{Hom}_A(M,N)$ tiene una estructura de $\mathbb{Z}$-$\mathbb{Z}$-bimódulo, es decir, de grupo abeliano. Esta estructura concida con la usual.

2. Si A es conmutativo, sabemos que a todo A-módulo M puede considerarse como un A-A-bimódulo "simétrico", definiendo

$$m \cdot a = am$$

si $m \in M$ y $a \in A$. Entonces $\mathrm{Hom}_A({}_AM_A, {}_AN_A)$ tiene una estructura de A-A-bimódulo.

Notemos que la acción de A sobre $\mathrm{Hom}_A(M, N)$ puede calcularse de cualquiera de las siguientes maneras:

$$(af)(m) = f(ma) = f(am) = af(m) = f(m)a = (fa)(m).$$

Vemos así que $\mathrm{Hom}_A(M, N)$ resulta un A-A-bimódulo simétrico.

3. Si $N = A$, que es un A-A-bimódulo, y M es un A-módulo a derecha, entonces $M^* = \mathrm{Hom}_A({}_AM_{\mathbb{Z}}, {}_AA_A)$ es un $\mathbb{Z}$-A-bimódulo, es decir, un A-módulo a derecha. La estructura es tal que

$$(f \cdot a)(m) = f(m)a$$

para cada $f \in M^*$, $a \in A$ y $m \in M$.

Ejemplo. Sea k un anillo conmutativo, G un grupo (o un semigrupo) y $k[G]$ el anillo del grupo. $\mathrm{Hom}_k(k[G], k)$ es un $k[G]$-bimódulo isomorfo a k^G. El isomorfismo está dado por:

$$\begin{aligned} k^G &\longrightarrow \mathrm{Hom}_k(k[G], k) \\ f &\longmapsto \left(\sum_{g \in G} \lambda_g g \mapsto \sum_{g \in G} \lambda_g f(g) \right) \end{aligned}$$

En particular, $k[x]^* \cong k[\![x]\!]$.

Sea ahora ${}_AM_B$ un A-B-bimódulo fijo y consideremos el funtor tal que

$$\begin{aligned} \mathrm{Hom}_A({}_AM_B, -) : {}_A\mathrm{Mod}_C &\longrightarrow {}_B\mathrm{Mod}_C \\ {}_AN_C &\longmapsto \mathrm{Hom}_A(M, N) \end{aligned}$$

y si $f : {}_AN_C \to {}_AN'_C$ es un morfismo de A-C-bimódulos, definimos

$$\begin{aligned} \mathrm{Hom}_A(M, f) = f_* : \mathrm{Hom}_A(M, N) &\longrightarrow \mathrm{Hom}_A(M, N') \\ g &\longmapsto f \circ g \end{aligned}$$

Dejamos como ejercicio la verificación de las siguientes propiedades:

(i) $(f \circ f')_* = f_* \circ f'_*$.
(ii) $(\mathsf{Id}_N)_* = \mathsf{Id}_{\mathrm{Hom}_A(M,N)}$.
(iii) $(f + f')_* = f_* + f'_*$.
(iv) $f_*(b.g) = b.f_*(g)$ $(b \in B)$.
(v) $f_*(g.c) = f_*(g).c$ $(c \in C)$.

Notemos que $0_* = 0$. Esto se sigue, por ejemplo, de la buena relación del funtor $(-)_*$ con la suma: como $0_* = (0+0)_* = 0_* + 0_*$, resulta que 0_* debe ser el elemento neutro en el Hom.

Ejemplos.
1. Si $M = A$, $\mathrm{Hom}_A(A, -)$ es naturalmente isomorfo al funtor identidad, vía el isomorfismo

$$\phi \in \mathrm{Hom}_A(M, N) \mapsto \phi(1) \in N.$$

2. Si $M = A^{(I)}$, es

$$\mathrm{Hom}_A(M, N) = \mathrm{Hom}_A(A^{(I)}, N) \cong \mathrm{Hom}_A(A, N)^I \cong N^I.$$

3. Si $A = B = C = \mathbb{Z}$ y $M = \mathbb{Z}_n$, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, N) \cong \{x \in N : nx = 0\}$ es el subgrupo de N formado por los elementos de n-torsión.

4. Si $A = B = C = k$, k un cuerpo, y V y W dos k-espacios vectoriales, $M = V \otimes_k W$, entonces $\mathrm{Hom}_k(V \otimes_k W, -)$ es naturalmente isomorfo al funtor $\mathrm{Hom}_k(V, \mathrm{Hom}_k(W, -))$.

5. Como caso particular del anterior, sean $V = k[G]$ y $W = k[H]$ donde G y H son dos grupos. Entonces

$$\mathrm{Hom}_k(k[G \times H], -) \cong \mathrm{Hom}_k(k[G], \mathrm{Hom}_k(k[H], -)).$$

Proposición 5.4.1. *El funtor* $\mathrm{Hom}_A({}_AM_B, -)$ *es exacto a izquierda, es decir, si*

$$0 \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z$$

es una sucesión exacta de B-C-bimódulos, entonces

$$0 \longrightarrow \mathrm{Hom}_A(M, X) \xrightarrow{f_*} \mathrm{Hom}_A(M, Y) \xrightarrow{g_*} \mathrm{Hom}_A(M, Z)$$

es una sucesión exacta de B-C-bimódulos.

Demostración. Por el ejercicio anterior, ya sabemos que f_* y g_* son morfismos de B-C-bimódulos. Sabemos que

$$g_* \circ f_* = (g \circ f)_* = 0_* = 0,$$

asi que sólo falta ver que f_* es un inyectivo y que $\mathrm{Ker}(g_*) \subseteq \mathrm{Im}(f_*)$. Dejamos esto al lector. □

Este resultado admite la siguiente recíproca:

Lema 5.4.2. *Sea A un anillo cualquiera, M, N, T tres A-módulos. Entonces*

(a) La sucesión $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T$ *es exacta si y sólo si*

$$0 \longrightarrow \mathrm{Hom}_A(R, M) \xrightarrow{f_*} \mathrm{Hom}_A(R, N) \xrightarrow{g_*} \mathrm{Hom}_A(R, T)$$

es una sucesión exacta de grupos abelianos para todo A-módulo R.

(b) La sucesión $M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$ *es exacta si y sólo si*

$$0 \longrightarrow \mathrm{Hom}_A(T, R) \xrightarrow{g^*} \mathrm{Hom}_A(N, R) \xrightarrow{f^*} \mathrm{Hom}_A(M, R)$$

es una sucesión exacta de grupos abelianos para todo A-módulo R.

Demostración. Sólo hace falta demostrar la "vuelta", ya que la "ida" ha sido demostrada en la proposición anterior.

Para la primera afirmación. tomamos $R = A$, entonces tenemos el siguiente diagrama conmutativo (¡verificar que es conmutativo!):

$$\begin{array}{ccccccc}
0 & \longrightarrow & M & \xrightarrow{f} & N & \xrightarrow{g} & T \\
 & & \| & & \| & & \| \\
0 & \longrightarrow & \mathrm{Hom}_A(A, M) & \xrightarrow{f_*} & \mathrm{Hom}_A(A, N) & \xrightarrow{g_*} & \mathrm{Hom}_A(A, T)
\end{array}$$

en donde las flechas dobles verticales indican los isomorfismos naturales — notemos que la definición de naturalidad de estos isomorfismos es justamente la conmutatividad de estos cuadrados. Luego, al ser exacta la sucesión de abajo, también lo es la de arriba.

La segunda afirmación es un poco más sutil, pero igualmente es fácil eligiendo en cada caso un R conveniente. Vemos por ejemplo

que la frase "$g^* : \mathrm{Hom}_A(T, R) \to \mathrm{Hom}_A(N, R)$ es un monomorfismo para todo A-módulo R" es justamente la definición categórica de epimorfismo, por lo tanto ya sabemos que g es epimorfismo.

Sabemos $f^* \circ g^* = 0$, de manera que $(g \circ f)^* = f^* \circ g^* = 0$ para todo A-módulo R. Luego si $h : R \to T$ es un morfismo cualquiera, resulta que $h \circ g \circ f : M \to T$ es el morfismo nulo. En particular, si tomamos $R = T$ y $h = \mathrm{Id}_T$ obtenemos que $g \circ f$ es cero y por lo tanto $\mathrm{Im}(f) \subset \mathrm{Ker}(g)$. Veamos por último la inclusión inversa.

Tomando $R = N/\mathrm{Im}(f)$, tenemos la sucesión exacta

$$0 \longrightarrow \mathrm{Hom}_A(T, N/\mathrm{Im}(f)) \longrightarrow$$
$$\longrightarrow \mathrm{Hom}_A(N, N/\mathrm{Im}(f)) \longrightarrow \mathrm{Hom}_A(M, N/\mathrm{Im}(f))$$

y consideremos la proyección al cociente $\pi : N \to N/\mathrm{Im}(f)$. Claramente $f^*(\pi) = \pi \circ f = 0$, así que $\pi \in \mathrm{Ker}(f^*) = \mathrm{Im}(g^*)$. Esto significa que existe $h : T \to N/\mathrm{Im}(f)$ tal que $\pi = h \circ g$. Ahora resulta claro que $\mathrm{Ker}(g) \subset \mathrm{Im}(f)$ porque si $n \in N$, $n \in \mathrm{Im}(f)$ si y sólo si $\pi(n) = 0$ y, usando la igualdad $\pi = h \circ g$, se tiene que si $n \in \mathrm{Ker}(g)$ entonces $n \in \mathrm{Ker}(\pi) = \mathrm{Im}(f)$. □

Ejemplo. Dado un epimorfismo de A-módulos $f : Y \to Z$ y un módulo cualquiera M, uno puede preguntarse si el morfismo inducido $f_* : \mathrm{Hom}_A(M, Y) \to \mathrm{Hom}_A(M, Z)$ es también un epimorfismo. Esto no tiene por qué suceder en general. Consideremos el siguiente ejemplo: sean $A = Y = \mathbb{Z}$, $M = Z = \mathbb{Z}_n$ y sea $f = \pi : \mathbb{Z} \to \mathbb{Z}_n$ la proyección canónica. Entonces $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}) = 0$ y, por lo tanto, nunca puede haber un epimorfismo en $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_n)$, ya que este último es no nulo — por ejemplo, está la identidad de $\mathbb{Z}_n$.

A pesar del ejemplo anterior, hay muchos casos en que, para un M en particular, el funtor $\mathrm{Hom}_A(M, -)$ preserva epimorfismos. Por ejemplo si $M = A$, el funtor $\mathrm{Hom}_A(A, -)$ se identifica con la identidad, así que, trivialmente, preserva epimorfismos. Otro ejemplo es cuando M es libre.

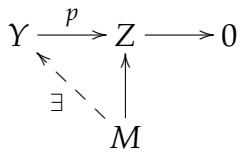
Ejercicio. Si $M \cong A^{(I)}$ para algún conjunto I, y si $f : X \to Y$ es un epimorfismo de A-módulos, entonces el morfismo inducido $f_* : \mathrm{Hom}_A(M, Y) \to \mathrm{Hom}_A(M, Z)$ es también un epimorfismo.

5.5 Módulos proyectivos

El objetivo de esta sección es estudiar los módulos M tales que el funtor $\mathrm{Hom}_A(M, -)$ es exacto. Comenzamos con una definición:

Definición 5.5.1. Diremos que un A-módulo M es *A-proyectivo* si el funtor $\mathrm{Hom}_A(M, -)$ es exacto.

Es decir, M es proyectivo si y sólo si $\mathrm{Hom}_A(M, -)$ preserva epimorfismos, y esto sucede si y sólo si, dado el siguiente diagrama de flechas llenas de A-módulos, se lo puede completar (de manera no necesariamente única) con la flecha punteada, de modo tal que el diagrama completo siga siendo conmutativo:



Observaciones.
1. Vimos en la sección anterior que todo A-módulo libre es proyectivo.

2. Un cociente de un módulos proyectivos no es necesariamente proyectivo. Por ejemplo, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

3. Los submódulos de proyectivos no son necesariamente proyectivos. Por ejemplo, considerar $A = M = \mathbb{Z}_4$ y el submódulo $2\mathbb{Z}_4$. Se deja como ejercicio verificar que $2\mathbb{Z}_4$ no es proyectivo.

4. Las localizaciones de proyectivos no son necesariamente proyectivas: sean $A = M = \mathbb{Z}$ y $S = \{2^n : n \in \mathbb{N}_0\}$ consideremos la proyección canónica $\pi : \mathbb{Z} \to \mathbb{Z}_3$. Es $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_S, \mathbb{Z}) = 0$ pero el morfismo

$$\frac{n}{2^n} \in \mathbb{Z}_S \mapsto \pi(n2^n) \in \mathbb{Z}_3$$

está bien definido (porque 2 es el inverso de 2 en $\mathbb{Z}_3$) y no es cero. Luego no puede haber un epimorfismo de $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_S, \mathbb{Z}) = 0$ en $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_S, \mathbb{Z}_3) \neq 0$.

5. Veremos como corolario de la siguiente proposición que un sumando directo de un proyectivo es proyectivo.

Proposición 5.5.2. *Sea M un A-módulo. Las siguientes afirmaciones son equivalentes:*

(a) M es un A-módulo proyectivo.
(b) Toda sucesión exacta corta de A módulos del tipo

$$0 \longrightarrow X \longrightarrow Y \longrightarrow M \longrightarrow 0$$

se parte.
(c) M es sumando directo de un A-módulo libre.

Demostración. (a) $\Rightarrow$ (b) . Sea M un A-módulo proyectivo y consideremos una sucesión exacta

$$0 \longrightarrow X \longrightarrow Y \longrightarrow M \longrightarrow 0$$

Tenemos un diagrama

$$\begin{array}{ccccc} Y & \xrightarrow{p} & M & \longrightarrow & 0 \\ & \nwarrow^{\overline{id}} & \| id & & \\ & & M & & \end{array}$$

La existencia de $\overline{id} : M \to Y$ tal que $p \circ \overline{id} = \mathsf{Id}_M$ se debe a la proyectividad de M. Luego la sucesión se parte.

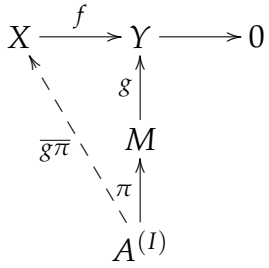
(b) $\Rightarrow$ (c) Dado M, sabemos que existe un conjunto I y un epimorfismo $\pi : A^{(I)} \to M$. Consideremos la sucesión exacta corta

$$0 \longrightarrow \mathrm{Ker}(\pi) \longrightarrow A^{(I)} \longrightarrow M \longrightarrow 0$$

Por hipótesis esta sucesión exacta se parte, de manera que existe $i : M \to A^{(I)}$ tal que $\pi \circ i = \mathsf{Id}_M$. Por lo tanto M es un sumando directo de $A^{(I)}$.

(c) $\Rightarrow$ (a) Sea M un sumando directo de $A^{(I)}$. Queremos ver que M es proyectivo. Consideramos un epimorfismo $f : X \to Y$ y un morfismo cualquiera $g : M \to Y$ y llamamos $i : M \to A^{(I)}$ a la inclusión y $\pi : A^{(I)} \to M$ a la proyección. Tenemos que ver que existe algún $\overline{g} : M \to X$ tal que $f\overline{g} = g$.

El diagrama de rigor es el siguiente:



Definimos $\overline{g} = \overline{g\pi}i : M \to X$. Es claro que se trata de un morfismo de A-módulos y además

$$f\overline{g} = f(\overline{g\pi}i) = (f\overline{g\pi})i = (g\pi)i = g(\pi i) = g\mathsf{Id}_M = g.$$

Por lo tanto M es proyectivo. □

Observación. Si M es es un A-módulo finitamente generado, existe siempre un epimorfismo $A^{(I)} \to M$ con I finito. Si además M es proyectivo, existe $n \in \mathbb{N}$ tal que M es sumando directo de A^n.

Corolario 5.5.3. *Dada una familia de A-módulos $(M_i)_{i\in I}$, se tiene que:*

(a) $\bigoplus_{i\in I} M_i$ es proyectivo si y sólo si cada M_i es proyectivo.
(b) Si $\prod_{i\in I} M_i$ es proyectivo entonces cada M_i es proyectivo. La recíproca no es necesariamente cierta.

Demostración. Sea $f : X \to Y$ un epimorfismo y consideremos el cuadrado conmutativo:

$$\begin{array}{ccc} \mathrm{Hom}_A(\bigoplus_{i\in I} M_i, X) & \xrightarrow{f_*} & \mathrm{Hom}_A(\bigoplus_{i\in I} M_i, Y) \\ \| & & \| \\ \prod_{i\in I} \mathrm{Hom}_A(M_i, X) & \xrightarrow{\prod f_*^i} & \prod_{i\in I} \mathrm{Hom}_A(M_i, Y) \end{array}$$

Luego la flecha f_* de arriba es un epimorfismo si y sólo si la flecha $\prod f_*^i$ de abajo lo es y $\prod f_*^i$ es un epimorfismo si y sólo si todas las f_*^i lo son. Esto prueba la primera parte.

Para ver la segunda, sea $P = \prod_{i\in I} M_i$, $i_0 \in U$ y consideremos

$$Q = \{(m_i)_{i\in I} \in \prod_{i\in I} M_i : m_{i0} = 0\}.$$

Entonces $P = Q \oplus M_{i_0}$ y la primera parte, como P es proyectivo, implica que M_{i_0} es proyectivo. □

Ejemplo. Sea $A = T_2(k)$ el anillo de matrices triangulares inferiores sobre un cuerpo k. Sabemos que $A = Ae_{11} \oplus Ae_{22}$ como A-módulo a izquierda. Luego Ae_{11} y Ae_{22} son A-módulos proyectivos que no son libres: la dimensión como k-espacio vectorial de todo A-módulo libre finitamente generado es múltiplo de 3, pero $\dim_k(Ae_{11}) = 2$ y $\dim_k(Ae_{22}) = 1$.

Observación. Si $A = \mathbb{Z}$, todo A-módulo proyectivo es libre porque todo submódulo de un A-módulo libre es libre, ya que $\mathbb{Z}$ es un dominio principal.

5.6 Anillos hereditarios

Vimos ejemplos de módulos proyectivos con submódulos que no son proyectivos. Por ejemplo $2\mathbb{Z}_4 \subset \mathbb{Z}_4$ no es un $\mathbb{Z}_4$-módulo proyectivo.

Definición 5.6.1. Una anillo A se dice *hereditario a izquierda* si y sólo si todo submódulo de un A-módulo a izquierda proyectivo es proyectivo.

El siguiente teorema describe los submódulos de módulos libres en anillos hereditarios.

Teorema 5.6.2. *(Kaplansky) Sea A un anillo hereditario, L un A-módulo libre y $S \subseteq L$ un submódulo. Entonces si $L = \bigoplus_{i\in I} Ax_i$, existe una familia $\{\mathcal{A}_i\}_{i\in I}$ de ideales de A tales que $S \cong \bigoplus_{i\in I} \mathcal{A}_i$.*

Demostración. Sea $\{x_i\}_{i\in I}$ una base de L. Podemos suponer que I es bien ordenado y no vacío, con orden $\leq$. Para cada $i \in I$, sean $L_i' = \langle x_j : j \leq i\rangle$ y $L_i = \langle x_j : j < i\rangle$. Entonces $L_i' = L_i \oplus \langle x_i\rangle$.

Para cada $i \in I$, definimos un morfismo $f_i : L_i' \to A$ de manera que sea $f_i(y + ax_i) = a$ si $y \in L_i'$ y $a \in A$. Los f_i resultan retracciones de las inclusiones $A \cong \langle x_i\rangle \hookrightarrow L_i'$ y $\mathrm{Ker}(f_i) = L_i$.

Si $\mathcal{A}_i = f_i(S \cap L_i')$, resulta $g_i = f_i|_{S\cap L_i'} : S \cap L_i' \to \mathcal{A}_i$ sobreyectivo. Como $\mathcal{A}_i$ es proyectivo (pues A es hereditario), g_i es una retracción y, por lo tanto, $\mathrm{Ker}(g_i) = \mathrm{Ker}(f_i) \cap S = S \cap L_i$ es un sumando directo de $S \cap L_i'$. Sea T_i un complemento de $S \cap L_i$ en $S \cap L_i'$. Entonces $T_i \cong \mathcal{A}_i$. Basta ver que $S \cong \oplus_{i\in I} T_i$.

- Veamos primero que $S = \sum_{i\in I} \mathcal{T}_i$. Es $L = \bigcup_{i\in I} L'_i$, así que para todo $x \in L$ existe $\{a_i\}_{i\in I} \subset A$ tal que $x = \sum_{i\in I} a_i x_i$. Supongamos que $x \neq 0$ y sea $j = \max(\text{sop}\{a_i\})$ (que existe porque $sop(\{a_i\})$ es un conjunto finito). Es $x \in L'_j$. Si $S \neq \sum_{i\in I} T_i$, sea

$$\mathcal{C} = \{i \in I : S \cap L'_i - \sum_{j\in I} T_j \neq \varnothing\};$$

esto no es vacío. Sean finalmente $j_0 = \min(\mathcal{C})$ (que existe por la buena ordenación) y $x \in S \cap L'_{j_0} - \sum_{j\in I} T_j$.

Se puede escribir $x = y + z$ con $y \in S \cap L_{j_0}$ y $z \in T_{j_0}$, así que $y \notin \sum_{i\in I} T_i$ e $y \in L'_k$ para algún $k < j_0$. Entonces es $y \in S \cap L'_k - \sum_{i\in I} T_i$. Esto contradice la minimalidad de j_0.
- Veamos ahora que la suma es directa. Supongamos que es $\sum_{i\in I} t_i = 0$, con $t_i \in T_i$ para cada $i \in I$. Queremos ver que todos los t_i son nulos.

Sea $j = \max\{i : t_i \neq 0\}$. Entonces $0 = t_j + \sum_{i<j} t_i$. Tenemos que $t_j \in T_j$ y $\sum_{i<j} t_i \in S \cap L_j$, pero sabíamos que $\langle x_j \rangle$ está en suma directa con L_j, de manera que como $t_j = -\sum_{i<j} t_i$, es $t_j = 0$. □

Corolario 5.6.3. *Un anillo A es hereditario si y sólo si todo ideal de A es un A-módulo proyectivo.*

Demostración. La condición es obviamente necesaria pues A es libre como A-módulo. La suficiencia puede verse de la siguiente manera: en primer lugar notemos que el Teorema de Kaplansky es válido para todo anillo A tal que sus ideales son A-módulos proyectivos. Ahora, si P es un A-módulo proyectivo y $P' \subseteq P$ es un submódulo, sea L libre tal que P es sumando directo de L. Claramente P' es isomorfo a un submódulo de L y, por el Teorema de Kaplansky, $P' \cong \oplus_{i\in I} \mathcal{A}_i$ con $\mathcal{A}_i$ ideales de A. Por hipótesis los ideales $\mathcal{A}_i$ son proyectivos, así que P' es proyectivo. □

Recordando la noción de hiperhereditario y el Teorema 5.2.11, tenemos el siguiente corolario:

Corolario 5.6.4. *Sea A un anillo. Las siguiente afirmaciones son equivalentes:*

(a) A es hiperhereditario, esto es, todo submódulo de un libre es libre.
(b) A es hereditario y todo A-módulo proyectivo es libre.
(c) Todo ideal de A es un A-módulo libre.

Observaciones.
1. Si A es un dominio íntegro y principal, entonces A es hiperhereditario.

2. Si A es un anillo conmutativo e hiperhereditario, entonces A es un dominio principal. En efecto, sea I un ideal de A. Dos elementos $a, b \in I$ no pueden ser linealmente independientes, ya que es $ab + (-b)a = 0$. Así, la cantidad máxima de elementos de una base de I es uno, esto es, I es un ideal principal.

3. Si A es un dominio íntegro, A es principal si y sólo si es hiperhereditario.

4. En el caso particular en que $A = \mathbb{Z}$, vemos que todo subgrupo de un grupo abeliano libre es libre.

5.7 Módulos proyectivos en dominios principales

Durante esta sección A denotará un dominio íntegro de ideales principales.

Recordamos que si M es un A-módulo, entonces la *torsión* de M es el A-submódulo

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

Proposición 5.7.1. *Sea M un A-módulo finitamente generado. Las siguientes afirmaciones son equivalentes:*

(a) M es libre.
(b) M es proyectivo.
(c) $t(M) = 0$.

Demostración. Es claro que *(a)* $\Rightarrow$ *(b)* . Más aún, al ser A un dominio de ideales principales, A es hiperhereditario y las afirmaciones *(a)* y *(b)* son equivalentes. Veamos que *(a)* y *(c)* son equivalentes.

(a) $\Rightarrow$ *(c)* Como M es libre y finitamente generado, hay un isomorfismo $\phi : M \to A^n$ para algún número natural n. Supongamos que $m \in t(M)$, de manera que existe $a \neq 0$ en A tal que $am = 0$.

Sea $\phi(m) = (a_1, \ldots, a_n)$. Entonces $0 = \phi(am) = (aa_1, \ldots, aa_n)$, es decir, $aa_i = 0$ si $1 \leq i \leq n$. Como A es íntegro y $a \neq 0$, concluimos

que $a_i = 0$ para todo i. Usando ahora que ϕ es un isomorfismo, vemos que $m = 0$.

(c) $\Rightarrow$ (a) Sea M un A-módulo sin torsión y consideremos el cuerpo K de fracciones de A. Necesitaremos el siguiente Lema, cuya prueba dejamos para el final:

Lema 5.7.2. *Sea K el cuerpo de fracciones de A y $M \subseteq K$ un A-submódulo de tipo finito. Entonces existe $x \in K$ tal que $M = A.x$.*

Sea M_K la localización de M en $A - \{0\}$ y sea $j_M : M \to M_K$ el morfismo canónico de localización,

$$j_M : m \in M \mapsto \frac{m}{1} \in M_K.$$

Sabemos que $\mathrm{Ker}(j_M) = t(M) = 0$, así que j_M es inyectiva; por otro lado, la imagen de M en M_K no es cero. Por lo tanto existe una transformación lineal $M_K \to K$ tal que la composición

$$M \longrightarrow M_K \longrightarrow K$$

es no nula. Llamemos p a esta composición y consideremos la sucesión exacta corta de A-módulos

$$0 \longrightarrow \mathrm{Ker}(p) \longrightarrow M \longrightarrow p(M) \longrightarrow 0$$

Como M es finitamente generado como A-módulo y todos los morfismos son A-lineales, la imagen de p es finitamente generada como A-módulo. Esto implica (por el Lema anterior) que $p(M) \cong A$ y entonces la sucesión se parte. Vemos así que $M \cong \mathrm{Ker}(p) \oplus A$.

Llamemos $M_1 := \mathrm{Ker}(p)$. Claramente, M_1 es un submódulo de M, así que $t(M_1) = 0$. Además A es noetheriano y M es finitamente generado, de manera que M es noetheriano y, en particular, M_1 es finitamente generado. Estamos de nuevo en las mismas hipótesis. Podemos entonces repetir la construcción para M_1 y descomponerlo como $M_1 \cong M_2 \oplus A$; en particular, $M \cong (M_2 \oplus A) \oplus A$. De esta manera obtenemos una cadena creciente de submódulos, cada uno isomorfo a A, $A \oplus A$, $A \oplus A \oplus A$, ..., y la noetherianidad de M implica que esta cadena se estaciona. Luego $M \cong A^n$ para algún $n \in \mathbb{N}$. □

Demostración del lema. Sea $M = \langle x_1, \ldots, x_n \rangle$. Como $M \subseteq K$, existen $p_1, \ldots, p_n, q_1, \ldots, q_n \in A$ con $q_i \neq 0$ y $x_i = \frac{p_i}{q_i}$ si $i = 1, \ldots, n$.

Sea $q = \prod_{i=1}^{n} q_i$. Como A es íntegro, $q \neq 0$. Por otro lado, como para todo $j = 1, \ldots, n$, $qx_j \in A$, qM es un submódulo de A, es decir, un ideal y, entonces, es principal. Luego existe $t \in A$ tal que $qM = tA$, es decir $M = \frac{t}{q}A$. □

Observación. De la demostración de la Proposición 5.7.1 se sigue que si M es finitamente generado, entonces

$$\begin{aligned} \mathrm{Hom}_A(M, K) \neq 0 &\iff M_K \neq 0 \\ &\iff M/t(M) \neq 0 \iff M \neq t(M). \end{aligned}$$

Corolario 5.7.3. *Sea M un A-módulo finitamente generado. Entonces $M \cong t(M) \oplus A^n$ para un único $n \in \mathbb{N}_0$.*

Demostración. Se considera la sucesión exacta corta

$$0 \longrightarrow t(M) \longrightarrow M \longrightarrow M/t(M) \longrightarrow 0$$

Como $t(M/t(M)) = 0$, $M/t(M)$ es libre y, en particular, proyectivo. Por lo tanto la sucesión exacta se parte y $M \cong t(M) \oplus M/t(M)$. Como $M/t(M)$ es libre y finitamente generado, es isomorfo a A^n para algún $n \in \mathbb{N}_0$. Pero $n = \dim_K((M/t(M))_K) = \dim_K(M_K)$, así que n está unívocamente determinado. □

5.8 Módulos inyectivos

Así como la noción de módulo proyectivo P está relacionada con las propiedades del funtor $\mathrm{Hom}_A(P, -)$, la de módulo inyectivo concierne al funtor $\mathrm{Hom}_A(-, I)$.

Si M es un A-módulo, $\mathrm{Hom}_A(-, M)$ es exacto a izquierda, es decir, para cualquier sucesión exacta

$$X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow 0$$

la sucesión

$$0 \longrightarrow \mathrm{Hom}_A(Z, M) \xrightarrow{g^*} \mathrm{Hom}_A(Y, M) \xrightarrow{f^*} \mathrm{Hom}_A(X, M)$$

es exacta. Resulta natural preguntarse, en caso de que f sea un monomorfismo, si f^* es epimorfismo o no. La respuesta es que en general ésto no es cierto, como se puede ver con el siguiente (contra)ejemplo:

Ejemplo. Tomemos $X = Y = \mathbb{Z}$ y sean $f : X \to Y$ el morfismo tal que $f(n) = 2n$ y $g : \mathbb{Z} \to \mathbb{Z}_2$ la proyección canónica a $Z = \mathbb{Z}_2$. Tenemos la siguiente sucesión exacta:

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}_2 \longrightarrow 0$$

Aplicando el funtor $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Z}_2)$, se obtiene la sucesión

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}_2) & \xrightarrow{\pi^*} & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}_2) & \xrightarrow{f^*} & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}_2) \\ & & \| & & \| & & \| \\ & & \mathbb{Z}_2 & & \mathbb{Z}_2 & & \mathbb{Z}_2 \end{array}$$

Esta sucesión no puede ser extendida por cero a la derecha manteniendo la exactitud porque, en caso contrario, la dimensión como $\mathbb{Z}_2$-espacio vectorial del objeto del medio sería la suma de las dimensiones de los objetos de las puntas. En efecto, podemos explicitar f^*: si $\phi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}_2)$,

$$f^*(\phi)(1) = \phi(f(1)) = \phi(2) = 2\phi(1) = 0,$$

así que $f^* = 0$. Evidentemente, entonces, f^* no es epimorfismo.

Notemos que el problema se debe a la 2-torsión de $\mathbb{Z}_2$: si hubieramos puesto un $\mathbb{Z}$-módulo divisible, el razonamiento para ver que $f^* = 0$ no habría funcionado. Veremos luego que si M es un $\mathbb{Z}$-módulo divisible entonces $\mathrm{Hom}_{\mathbb{Z}}(-, M)$ sí es exacto.

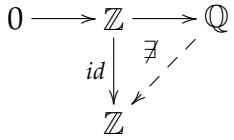
Definición 5.8.1. Un A-módulo M se llama *A-inyectivo* si el funtor $\mathrm{Hom}_A(-, M) : {}_A\mathrm{Mod} \to \mathrm{Ab}$ es exacto.

Así, un A-módulo M es inyectivo si y sólo si $\mathrm{Hom}_A(-, M)$ transforma monomorfismos en epimorfismos, si y sólo si dado el siguiente diagrama de flechas llenas de A-módulos se lo puede completar (de manera no necesariamente única) con la flecha punteada de manera tal que el diagrama completo sea conmutativo:

$$\begin{array}{ccccc} 0 & \longrightarrow & Y & \xrightarrow{i} & Z \\ & & \downarrow{\scriptstyle h} & \swarrow{\scriptstyle \widetilde{h}} & \\ & & M & & \end{array}$$

Observación. Si M es un A-B-bimódulo, el funtor $\mathrm{Hom}_A(-, M)$ toma valores en la categoría Mod_B. Como una sucesión de B-módulos es exacta si y sólo si es exacta vista como sucesión de grupos abelianos, un A-B-bimódulo ${}_AM_B$ es inyectivo como A-módulo si y sólo si el funtor $\mathrm{Hom}_A(-, M) : {}_A\mathrm{Mod} \to \mathrm{Mod}_B$ es exacto.

Ejemplos.
1. $\mathbb{Z}$ *no* es un $\mathbb{Z}$-módulo inyectivo. Consideramos, para ver ésto, el diagrama en el que las flechas son la inclusión $\mathbb{Z} \hookrightarrow \mathbb{Q}$ y la identidad de $\mathbb{Z}$ en $\mathbb{Z}$:

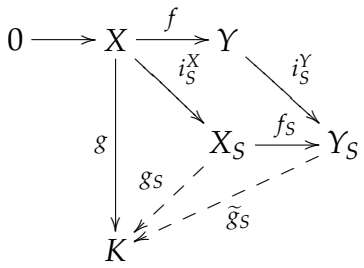


Es claro que no hay ningún morfismo $\mathbb{Q} \to \mathbb{Z}$ que restringido a $\mathbb{Z}$ sea la identidad, pues de hecho no hay ningún morfismo no nulo de $\mathbb{Q}$ en $\mathbb{Z}$.

2. Si k es un cuerpo, todo k-espacio vectorial es k-inyectivo.

3. Si A es un dominio íntegro y K es su cuerpo de fracciones, entonces K es un A-módulo inyectivo. Sea $S = A - \{0\}$; recordemos que si $f : X \to Y$ es un monomorfismo, entonces $f_S : X_S \to Y_S$ también lo es.

Si ahora $g : X \to K$ es un morfismo cualquiera de A-módulos, tenemos el siguiente diagrama:



Las flechas llenas f y g son los datos originales y, por otro lado, $i_S^X : x \in X \mapsto \frac{x}{1} \in X_S$ e i_S^Y son las flechas canónicas de localización. Como los elementos de S son inversibles en K, el morfismo $g : X \to K$ se factoriza a través de X_S mediante g_S. Si ahora sólo consideramos X_S, Y_S y K, el diagrama está en la categoría de K-espacios

vectoriales, en donde todos los objetos son inyectivos. Luego existe un morfismo $\widetilde{g}_S$ que preserva la conmutatividad.

Definimos entonces $\widetilde{g} : Y \to K$ poniendo $\widetilde{g} = \widetilde{g}_S \circ i_S^Y$. Como en el diagrama anterior todos los cuadrados y triángulos conmutan, se sigue que $g = \widetilde{g} \circ f$, es decir, que $\widetilde{g}$ extiende a g.

4. Como caso particular del ejemplo anterior, $\mathbb{Q}$ es un $\mathbb{Z}$-módulo inyectivo.

Observación. Si M es un submódulo de un módulo inyectivo, entonces M no tiene por qué ser inyectivo (considerar $\mathbb{Z} \subset \mathbb{Q}$), sin embargo veremos ahora que un sumando directo de un inyectivo es inyectivo.

Dado que la definición de inyectivo es dual a la definición de proyectivo, muchos de los resultados para proyectivos se dualizan y se obtienen enunciados sobre módulos inyectivos, que se demuestran muchas veces dualizando las demostraciones anteriores:

Proposición 5.8.2. *Sea A un anillo y $(M_i)_{i\in I}$ una familia de A-módulos. Entonces:*

(a) $\prod_{i\in I} M_i$ es inyectivo si y sólo si cada M_i es inyectivo.
(b) Si $\bigoplus_{i\in I} M_i$ es inyectivo entonces cada M_i es inyectivo. La recíproca no es necesariamente cierta.

Demostración. Sea $f : X \to Y$ un monomorfismo y consideremos el cuadrado conmutativo

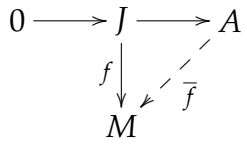
$$\begin{array}{ccc} \mathrm{Hom}_A(Y, \prod_{i\in I} M_i) & \xrightarrow{f^*} & \mathrm{Hom}_A(X, \prod_{i\in I} M_i) \\ \| & & \| \\ \prod_{i\in I} \mathrm{Hom}_A(Y, M_i) & \xrightarrow{\prod f_i^*} & \prod_{i\in I} \mathrm{Hom}_A(X, M_i) \end{array}$$

La flecha f^* es un epimorfismo si y sólo si la flecha $\prod f_i^*$ lo es. Y $\prod f_i^*$ es un epimorfismo si y sólo si todas las f_i^* lo son. Esto demuestra la primera afirmación.

Supongamos, por otro lado, que $M = \bigoplus_{i\in I} M_i$ es inyectivo y sea $i_0 \in I$. Entonces $M = \left(\bigoplus_{i\in I-\{i_0\}} M_i\right) \times M_{i_0}$. La primera parte implica entonces que también M_{i_0} inyectivo. □

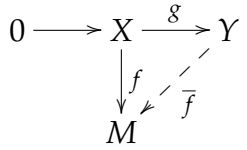
El siguiente resultado dice que para verificar la exactitud a derecha de $\mathrm{Hom}_A(-, M)$, basta aplicar el funtor a las inclusiones $J \hookrightarrow A$, donde J recorre el conjunto de ideales de A.

Teorema 5.8.3. *(Baer) Un A-módulo M es inyectivo si y sólo si tiene la siguiente propiedad: para todo J ideal de A y para todo $f : J \to M$ morfismo de A-módulos, existe $\overline{f} : A \to M$ tal que $\overline{f}|_J = f$.*



Demostración. Es claro que si M es inyectivo, entonces tiene la propiedad del enunciado. Veamos ahora que un módulo M con esa propiedad de extensión con respecto a ideales de A es en efecto un A-módulo inyectivo.

Dado un diagrama de líneas llenas



queremos ver que existe $\overline{f}$. Sin pérdida de generalidad, podemos suponer que X es un submódulo de Y y que g es la inclusión — si no, reemplazamos X por $g(X)$ y f por $f \circ g^{-1}$.

Sea $\mathfrak{Y}$ el conjunto de pares (Y', f') con $Y \subset Y$ un submódulo de Y tal que $Y' \supset X$ y $f' \in \hom_A(Y', M)$ tal que $f'|_X = f$. Ordenamos a $\mathfrak{Y}$ poniendo

$$(Y', f') \leq (Y'', f'') \iff Y' \subseteq Y'' \text{ y } f''|_{Y'} = f'.$$

Es fácil ver que $(\mathfrak{Y}, \leq)$ es un conjunto inductivo superiormente, así que tiene algún elemento maximal (Y_0, f_0).

Supongamos que $Y_0 \subsetneq Y$ y sea $y \in Y - Y_0$. Entonces $\langle y, Y_0 \rangle$ contiene estrictamente a Y_0. Sea $J = \{a \in A : ay \in Y_0\}$; como Y_0 es un submódulo de Y, J es un ideal de A (¡verificarlo!). Sea $\phi : J \to M$ tal que $\phi(a) = f_0(ay)$ para cada $a \in J$. Por hipótesis, ϕ se puede extender a $\overline{\phi} : A \to M$. Veamos que f_0 se puede extender a un morfismo $f_1 : \langle y, Y_0 \rangle \to M$.

Sea $x = ay + y_0$ donde $a \in A$ e $y_0 \in Y_0$. Ponemos

$$f_1(x) = \overline{\phi}(a) + f_0(y_0)$$

Esto está bien definido: si $ay + y_0 = a'y + y_0'$, entonces

$$(a - a')y = y_0' - y_0 \in Y_0,$$

es decir, $(a - a') \in J$, así que

$$\begin{aligned}\overline{\phi}(a) - \overline{\phi}(a') &= \overline{\phi}(a - a') = \phi(a - a') \\ &= f_0((a - a')y) = f_0(y_0' - y_0) \\ &= f_0(y_0') - f_0(y_0)\end{aligned}$$

Reordenando los términos de estas igualdades, vemos que

$$\overline{\phi(a)} + f_0(y_0) = \overline{\phi(a')} + f_0(y_0').$$

Esto nos dice que la función está bien definida. Es claro, además, que $(Y_0, f_0) < (\langle y, Y_0\rangle, f_1)$ en $\mathfrak{Y}$. Esto contradice la maximalidad de (Y_0, f_0), sí que debe ser $Y_0 = Y$. □

Ejercicio. Utilizando el teorema anterior, dar una nueva demostración de que $\mathbb{Q}$ es un $\mathbb{Z}$-módulo inyectivo.

Ejemplo. $\mathbb{Q}/\mathbb{Z}$ es un $\mathbb{Z}$-módulo inyectivo, así como también $\mathbb{Z}_{p^\infty}$ para cualquier primo p.

Definición 5.8.4. Un A-módulo M se dice *divisible* si para cualquier $a \in A$ no nulo y cada $m \in M$, existe $m' \in M$ tal que $am' = m$.

Ejemplo. $\mathbb{Q}$ es un $\mathbb{Z}$-módulo divisible.

Para obtener más ejemplos de módulos inyectivos, probaremos los siguientes dos lemas:

Lema 5.8.5. *Un grupo abeliano G es divisible si y sólo si es un $\mathbb{Z}$-módulo inyectivo.*

Demostración. Para ver la suficiencia de la condición, utilizaremos el Teorema de Baer, es decir, probaremos que todo diagrama de grupos abelianos

$$\begin{array}{ccccc} 0 & \longrightarrow & I & \longrightarrow & \mathbb{Z} \\ & & \downarrow{\scriptstyle h} & & \\ & & G & & \end{array}$$

en el que donde I es un ideal de $\mathbb{Z}$, se completa con un morfismo $\mathbb{Z} \to G$.

Como $\mathbb{Z}$ es un dominio de ideales principales, si $I \subseteq \mathbb{Z}$, existe $n \in \mathbb{N}_0$ tal que $I = n\mathbb{Z}$. Si $n = 0$ se puede extender el morfismo 0 por 0. Si $n \neq 0$, como G es un grupo abeliano divisible existe $v \in G$ tal que $h(n) = nv$. Por linealidad, esto implica que $h(jn) = jnv$ para todo $jn \in n\mathbb{Z}$, así que podemos definir $\overline{h} : \mathbb{Z} \to G$ de forma que $\overline{h}(m) := mv$.

Veamos ahora la necesidad. Supongamos que G es un $\mathbb{Z}$-módulo inyectivo. Si $g \in G$ y $n \in \mathbb{Z}$, $n \neq 0$, queremos ver que existe $g' \in G$ tal que $g = ng'$.

Definamos para eso un morfismo $h_g : \mathbb{Z} \to G$ poniendo, para cada $m \in \mathbb{Z}$, $h_g(m) = mg$ y consideremos el monomorfismo dado por la multiplicación por n, $\lambda_n : x \in \mathbb{Z} \to nx \in \mathbb{Z}$ y el diagrama

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\lambda_n} & \mathbb{Z} \\ & & \downarrow{\scriptstyle h_g} & \swarrow{\scriptstyle \overline{h_g}} & \\ & & G & & \end{array}$$

Como G es inyectivo, existe $\overline{h_g} : \mathbb{Z} \to G$ que hace del diagrama anterior un diagrama conmutativo, esto es, tal que

$$\overline{h_g}(nm) = h_g(m) = mg$$

para todo $m \in \mathbb{Z}$. Si tomamos $g' := \overline{h_g}(1)$, es

$$ng' = n\overline{h_g}(1) = \overline{h_g}(n) = h_g(1) = g.$$

Esto muestra que G es divisible. □

Proposición 5.8.6. *Si G es un grupo abeliano divisible, el A-módulo $\mathrm{Hom}_{\mathbb{Z}}(A, G)$ es inyectivo.*

Demostración. Sea N un submódulo de M y $h : N \to \mathrm{Hom}_{\mathbb{Z}}(A, G)$ un morfismo de A-módulos a izquierda. Recordemos que la estructura de A-módulo a izquierda en $\mathrm{Hom}_{\mathbb{Z}}(A, G)$ está dada por la estructura a derecha de A, es decir, si $\phi \in \mathrm{Hom}_{\mathbb{Z}}(A, G)$ y a, $a' \in A$, entonces $(a\phi)(a') = \phi(a'a)$.

Definamos $f : N \to G$ de manera que $f(n) = h(n)(1)$ para todo $n \in N$. Como G es $\mathbb{Z}$-inyectivo, existe un morfismo de grupos

abelianos $\overline{f} : M \to G$ que extiende a f. Obtenemos una extensión $\overline{h} : M \to \mathrm{Hom}_{\mathbb{Z}}(A, G)$ de h poniendo

$$\overline{h}(m)(a) = \overline{f}(am)$$

si $a \in A$ y $m \in M$. El morfismo $\overline{h}$ es A-lineal a izquierda (¡verificarlo!) y el diagrama conmuta porque, si $n \in N$, es

$$\overline{h}(n)(a) = \overline{f}(an) = f(an) = h(an)(1)$$

y, como h es A-lineal,

$$h(an)(1) = (ah(n))(1) = h(n)(a).$$

Esto termina la prueba. □

Ejercicio. Adaptar los resultados anteriores para demostrar que si A es un dominio de ideales principales y M es un A-módulo, entonces M es A-inyectivo si y sólo si es A-divisible.

Dado un A-módulo cualquiera M, siempre se puede encontrar un A-módulo proyectivo P y un epimorfismo $P \to M$. Podemos preguntarnos si el enunciado dual es cierto: dado un A-módulo cualquiera M, ¿existe siempre un A-módulo inyectivo I y un monomorfismo $M \to I$? La respuesta es sí y se da en dos etapas. Primero resolvamos el problema en la categoría de grupos abelianos:

Lema 5.8.7. *Sea M un grupo abeliano cualquiera. Entonces existe un grupo abeliano divisible D y un monomorfismo $M \to D$.*

Demostración. Supongamos primero que M es cíclico y no nulo. Entonces hay dos posibilidades: o bien $M \cong \mathbb{Z}$ o bien $M \cong \mathbb{Z}_n$ con $n \in \mathbb{N}$. En el primer caso, $M \cong \mathbb{Z} \hookrightarrow \mathbb{Q}$. En el segundo, se tiene que $M \cong \mathbb{Z}_n \hookrightarrow \mathbb{Q}/\mathbb{Z}$, con el monomorfismo de $\mathbb{Z}_n$ en $\mathbb{Q}/\mathbb{Z}$ definido por $\overline{1} \mapsto \overline{\frac{1}{n}}$.

Si ahora M es arbitrario y $m \in M$, $\langle m \rangle$ es cíclico y existe un monomorfismo $\langle m \rangle \hookrightarrow D_m$ con D_m un grupo abeliano divisible. Como los $\mathbb{Z}$-módulos divisibles son inyectivos, para cada $m \in M$, existe un morfismo $M \to D_m$ que extiende al monomorfismo anterior, de manera que conmuta

$$\begin{array}{ccccc} 0 & \longrightarrow & \langle m \rangle & \longrightarrow & M \\ & & \downarrow & \swarrow_{f_m} & \\ & & D_m & & \end{array}$$

El morfismo f_m no tiene por qué ser inyectivo, sin embargo es claro que $m \notin \operatorname{Ker}(f_m)$.

Consideremos ahora $D = \prod_{m \in M - \{0\}} D_m$ y el morfismo

$$f : x \in M \mapsto (f_m(x))_{m \in M - \{0\}} \in \prod_{m \in M - \{0\}} D_m$$

Como todos los D_m son $\mathbb{Z}$-módulos inyectivos, D es un $\mathbb{Z}$-módulo inyectivo. Además $\operatorname{Ker}(f) = \bigcap_{m \in M - \{0\}} \operatorname{Ker}(f_m)$. Pero si $m \in M$, $m \notin \operatorname{Ker}(f_m) \supseteq \ker(f)$. Esto nos dice que f es un monomorfismo. □

Proposición 5.8.8. *Sea M un A-módulo cualquiera. Existe un A-módulo inyectivo I y un monomorfismo $M \to I$.*

Demostración. Si consideramos a M como grupo abeliano, sabemos que existe un monomorfismo $M \to D$, con D un grupo abeliano divisible. Tenemos entonces una cadena de isomorfismos y monomorfismos:

$$M \cong \operatorname{Hom}_A(A, M) \hookrightarrow \operatorname{Hom}_{\mathbb{Z}}(A, M) \hookrightarrow \operatorname{Hom}_{\mathbb{Z}}(A, D).$$

Si llamamos $I = \operatorname{Hom}_{\mathbb{Z}}(A, D)$, resulta de la proposición 5.8.6 que I es A-inyectivo. □

Recordemos que los módulos proyectivos pueden ser caracterizados como los sumandos directos de un libre. Como tener epimorfismo de un objeto libre en un módulo cualquiera es equivalente a haber elegido un sistema de generadores, la manera de dualizar parcialmente esta caracterización es introduciendo la noción de cogenerador:

Definición 5.8.9. Un A-módulo M se dirá un *cogenerador* si para todo A-módulo X, existe un conjunto J y un monomorfismo $X \hookrightarrow M^J$.

El ejemplo típico es $\mathbb{Q}/\mathbb{Z}$. Si M es un $\mathbb{Z}$-módulo cíclico de torsión, digamos $\mathbb{Z}_n$, es claro que hay un monomorfismo $\mathbb{Z}_n \to \mathbb{Q}/\mathbb{Z}$. Si $M \cong \mathbb{Z}$, obtenemos un monomorfismo $\mathbb{Z} \to (\mathbb{Q}/\mathbb{Z})^{\mathbb{N}}$ definiendolo de manera que la imagen de $1 \in \mathbb{Z}$ sea $(\frac{1}{n})_{n \in \mathbb{N}}$.

Ahora un argumento similar al exhibido en la demostración del lema 5.8.7 (utilizando el hecho de que $\mathbb{Q}/\mathbb{Z}$ es inyectivo) muestra que siempre hay un monomorfismo de M en un producto de copias

de $\mathbb{Q}/\mathbb{Z}$. Considerando el A-módulo $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$ y recordando que $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z}^I) \cong (\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z}))^I$ se obtienen ejemplos de cogeneradores en categorías de A-módulos con A un anillo cualquiera.

Observación. El concepto dual al de cogenerador es el de generador: un A-módulo M es generador si, para todo A-módulo X existe un conjunto de índices J y un epimorfismo $M^{(J)} \to X$. Por ejemplo el A-módulo ${}_AA$ es generador, y cualquier módulo libre también lo es, aunque un generador no es necesariamente libre.

Proposición 5.8.10. *Sea M un A-módulo. Las siguientes afirmaciones son equivalentes:*

(a) M es inyectivo.

(b) Toda sucesión exacta corta

$$0 \longrightarrow M \longrightarrow X \longrightarrow Y \longrightarrow 0$$

se parte.

Además, cualquiera de las dos afirmaciones implica que M es un sumando directo de un cogenerador.

Demostración. (a) $\Rightarrow$ (b) Consideremos el diagrama

$$\begin{array}{ccccc} 0 & \longrightarrow & M & \longrightarrow & X \\ & & {\scriptstyle \mathrm{Id}_M}\downarrow & \swarrow & \\ & & M & & \end{array}$$

Sabemos que existe una flecha punteada que hace conmutar el diagrama, porque M es inyectivo. Esto nos dice que la sucesión

$$0 \longrightarrow M \longrightarrow X \longrightarrow Y \longrightarrow 0$$

se parte.

(b) $\Rightarrow$ (a) Supongamos que M es un A-módulo que satisface la condición *(b)*. Existe un monomorfismo $f : M \to I$ con I inyectivo. Consideremos la sucesión exacta corta

$$0 \longrightarrow M \longrightarrow I \longrightarrow \mathrm{Coker}(f) \longrightarrow 0$$

Sabemos que esta sucesión se parte, así que M es un sumando directo de un inyectivo. En particular, es un factor directo y vemos que M es inyectivo.

Veamos finalmente que si M satisface la condición *(b)*, entonces M es sumando directo de un cogenerador.

Sea M un tal módulo. Sabemos que $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$ es un cogenerador en la categoría de A-módulos. En particular, existe un conjunto I y un monomorfismo $f : M \to \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})^I$. La sucesión exacta

$$0 \longrightarrow M \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})^I \longrightarrow \mathrm{Coker}(f) \longrightarrow 0$$

se parte por hipótesis, de manera que M es un sumando directo de $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})^I$. Como es claro que si un A-módulo X es cogenerador, también lo es X^I para cualquier conjunto no vacío I, esto termina la prueba de la proposición. □

Observación. El A-módulo $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$ además de ser cogenerador, es inyectivo. Todo sumando directo de $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})^I$ será será entonces también inyectivo.

5.9 Ejercicios

Torsión y divisibilidad

Definición. Sea A un anillo y M un A-módulo. Decimos que M es *divisible* si para cualquier cualquier $a \in A$ y $m \in M$ tales que $a \neq 0$, existe $m' \in M$ tal que $am' = m$.

5.9.18. Sea $G_\infty = \bigcup_{n\in\mathbb{N}} G_n \subset S^1$ el conjunto de todas las raíces de la unidad.

(a) Probar que es un subgrupo abeliano de S^1 y, por lo tanto, que se trata de un $\mathbb{Z}$-módulo. Mostrar que es divisible.

(b) Mostrar que $G_{p^\infty} = \bigcup_{n\in\mathbb{N}} G_{p^n}$ es un submódulo de G_∞ y que también es divisible.

5.9.19. Sea A unanillo conmutativo y M un A-módulo. Mostrar que si A es íntegro, entonces el subconjunto $t(M)$ de los elementos de torsión de M es un A-submódulo. ¿Es necesario que A sea íntegro?

5.9.20. Sea A un anillo íntegro.

(a) Sean M y N dos A-módulos y $f : M \to N$ un morfismo lineal. Mostrar que $f(t(M)) \subset t(N)$ y que, por lo tanto, la asignación $M \mapsto t(M)$ es funtorial.

(b) Mostrar que $t(t(M)) = t(M)$ y $t(M/t(M)) = 0$ para todo A-módulo M.

5.9.21. Encontrar la torsión del grupo abeliano $(\mathbb{C} - \{0\}, \cdot)$.

5.9.22. Sea A íntegro y M un A-módulo divisible y sin torsión. Ver que entonces M admite una estructura de k-espacio vectorial donde k es el cuerpo de fracciones de A.

5.9.23. *(a)* Un grupo abeliano artiniano es de torsión.

(b) Un grupo abeliano es artiniano y noetheriano sii es finito.

5.9.24. Sea A un anillo conmutativo y M y N dos A-módulos a izquierda. Consideramos a M y N como A-bimódulos simétricos poniendo, por ejemplo, $ma = am$ si $a \in A$ y $m \in M$. Describir todas las formas en que se puede dar a $\mathrm{Hom}_A(M, N)$ una estructura de A-módulo a derecha o a izquierda. Mostrar que todas coinciden y por lo tanto $\mathrm{Hom}_A(M, N)$ es un A-módulo simétrico.

Probar además:

(a) Si M divisible, entonces $\mathrm{Hom}_A(M, N)$ no tiene torsión.

(b) Si N no tiene torsión, entonces $\mathrm{Hom}_A(M, N)$ no tiene torsión.

Módulos libres, proyectivos e inyectivos

5.9.25. $\mathbb{Q}$ no es un $\mathbb{Z}$-módulo libre.

5.9.26. Muestre que el grupo abeliano $\mathbb{Z}^{\mathbb{N}}$ no es proyectivo.

Sugerencia. Sea $M \subset \mathbb{Z}^{\mathbb{N}}$ el subgrupo de todos los elementos $x = (x_i)_{i\in\mathbb{N}} \in \mathbb{Z}^{\mathbb{N}}$ tales que para todo $n \in \mathbb{N}$, $|\{i \in \mathbb{N} : 2^n \nmid x_i\}| < \infty$. Entonces si $\mathbb{Z}^{\mathbb{N}}$ es libre, M es libre de rango no numerable. Analice ahora el grupo abeliano $M/2M$.

5.9.27. *Bases duales.* Sea A un anillo y P un A-módulo a izquierda. Una *base dual* para P es un par $((x_i)_{i\in I}, (f_i)_{i\in I})$ tal que $x_i \in P$ para todo $i \in I$, $f_i \in \hom_A(P, A)$ para todo $i \in I$ y se tiene que

(i) para todo $x \in P$, $|\{i \in I : f_i(x) \neq 0\}| < \infty$, y

(ii) para todo $x \in P$, es $x = \sum_{i\in I} f_i(x)x_i$.

Nótese que en la segunda condición la suma tiene sentido por la primera condición.

(a) Muestre que un A-módulo P es proyectivo sii posee una base dual.

(b) Muestre que un A módulo P es proyectivo y finitamente generado sii posee una base dual finita.

5.9.28. Probar que si M es un A-módulo a izquierda finitamente generado y proyectivo entonces $M^* = \mathrm{Hom}_A(M, A)$ es un A-módulo a derecha finitamente generado y proyectivo.

5.9.29. Sea A un anillo conmutativo, $S \subset A$ un subconjunto multiplicativo y M un A-módulo proyectivo de tipo finito. Demuestre que M_S es un A_S-módulo proyectivo de tipo finito.

5.9.30. Sea M un A-módulo proyectivo de tipo finito. Probar que M es isomorfo como A-módulo a $(M^*)^*$. Es cierto que M es isomorfo como A-módulo a M^*?

5.9.31. Sea A un anillo, $S \subset A$ un subconjunto multiplicativamente cerrado y sea M un A-módulo a izquierda.

(a) Si M es libre, entonces M_S es libre como A_S-módulo.

(b) Si M es proyectivo, entonces M_S es un A_S-módulo proyectivo.

(c) Si M es finitamente generado, entonces M_S es finitamente generado como A_S-módulo.

5.9.32. Sea A un anillo que contiene en su centro a un cuerpo k.

(a) Demuestre que $\mathrm{Hom}_k(A_A, k)$ es un A-módulo a izquierda inyectivo.

(b) Demuestre en general que si P_A es A-proyectivo, entonces el A-módulo $\mathrm{Hom}_k(P_A, k)$ es inyectivo.

(c) Supongamos que $\dim_k(A) < \infty$ y que P_A es finitamente generado, entonces P es proyectivo si y sólo si $\mathrm{Hom}_k(P_A, k)$ es inyectivo.

5.9.33. El objetivo de este ejercicio es proveer ejemplos de módulos inyectivos que tienen cocientes no inyectivos. Notar que en la categoría de $\mathbb{Z}$-módulos, un módulo es inyectivo si y sólo si es divisible, y cocientes de divisibles son divisibles, luego un (contra)ejemplo de este tipo no puede darse en la categoría de $\mathbb{Z}$-módulos.

Sea k un cuerpo y $A = k \oplus kx \oplus ky \oplus kxy$ el anillo con la multiplicación definida por

$$x \cdot x = 0, \qquad y \cdot y = 0, \qquad x \cdot y = xy, \qquad y \cdot x = -xy.$$

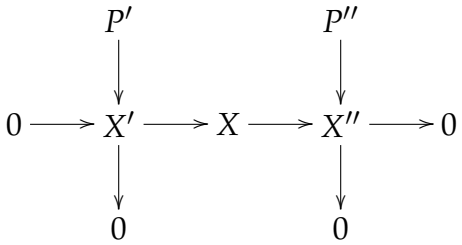
Sea $I = \langle x, y \rangle = kx \oplus ky \oplus kxy$. Verificar que es un ideal bilátero y demostrar que no es un sumando directo de A como A-módulo, en particular no es proyectivo.

Mostrar que hay isomorfismos de A-módulos

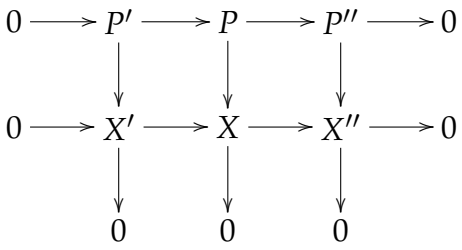
$$M = \operatorname{Hom}_k(I, k) \cong \operatorname{Hom}_k(A, k)/I^\perp,$$

donde $I^\perp = \{f \in \hom_k(A, k) : f|_I = 0\}$. Usar esto para ver que M no es inyectivo.

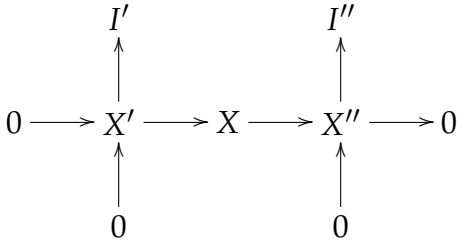
5.9.34. *(a)* Mostrar que si en el diagrama de A-módulos



P' y P'' son proyectivos y la fila es exacta, entonces puede completarse al siguiente diagrama de filas exactas, con P también proyectivo:



(b) Mostrar que si en el diagrama de A-módulos



I' e I'' son inyectivos y la fila es exacta, entonces puede completarse al siguiente diagrama de filas exactas, con I también inyectivo:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & I' & \longrightarrow & I & \longrightarrow & I'' & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & X' & \longrightarrow & X & \longrightarrow & X'' & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

5.9.35. *Resoluciones proyectivas.* Sea A un anillo.

(a) Para cada A-módulo M existe un diagrama

$$\cdots \longrightarrow P_p \longrightarrow P_{p-1} \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

de A-módulos y homomorfismos de A-módulos que es exacto y en el que cada P_p, $p \geq 0$, es proyectivo. Llamamos a este diagrama una *resolución proyectiva* de M.

(b) De hecho, los A-módulos P_p, $p \geq 0$, pueden elegirse libres.

(c) Si A es noetheriano a izquierda y M es finitamente generado, entonces los A-módulos P_p, $p \geq 0$, pueden elegirse finitamente generados.

(d) Si $f : M \to N$ es un morfismo de A-módulos y

$$\cdots \longrightarrow P_p \longrightarrow P_{p-1} \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

y

$$\cdots \longrightarrow Q_p \longrightarrow Q_{p-1} \longrightarrow \cdots \longrightarrow Q_1 \longrightarrow Q_0 \longrightarrow N \longrightarrow 0$$

son resoluciones proyectivas de M y N, respectivamente, entonces existen morfismos $f_p : P_p \to Q_p$ para cada $p \geq 0$ que hacen conmutar el siguiente diagrama:

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & P_p & \longrightarrow & P_{p-1} & \longrightarrow \cdots \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & M \longrightarrow 0 \\
 & & \downarrow{\scriptstyle f_p} & & \downarrow{\scriptstyle f_{p-1}} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle f} \\
\cdots & \longrightarrow & Q_p & \longrightarrow & Q_{p-1} & \longrightarrow \cdots \longrightarrow & Q_1 & \longrightarrow & Q_0 & \longrightarrow & N \longrightarrow 0
\end{array}$$

(e) Encuentre resoluciones proyectivas para

(i) un A-módulo proyectivo;

(ii) el $\mathbb{Z}$-módulo $\mathbb{Z}/n\mathbb{Z}$ para cada $n \in \mathbb{Z}$;

(iii) el $k[X]$-módulo $S = k[X]/(X)$.

5.9.36. Enuncie y pruebe resultados análogos a los del ejercicio anterior para resoluciones inyectivas.

5.9.37. Sea $\phi \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^n)$ y consideremos a $\mathbb{R}^n$ como un $\mathbb{R}[X]$-módulo en el que multiplicación por x está dada por la transformación lineal ϕ.

(a) Supongamos que la matriz de ϕ en la base canónica es o bien una matriz simétrica o bien es una matriz ortogonal. Mostrar que todo $\mathbb{R}[X]$-submódulo de $\mathbb{R}^n$ es un sumando directo.

(b) Dar ejemplos de endomorfismos $\phi \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^n)$ para los cuales el $\mathbb{R}[X]$-módulo $\mathbb{R}^n$ posea $\mathbb{R}[X]$-submódulos que no sean sumandos directos.

5.9.38. $\mathbb{Z}$ no es un $\mathbb{Z}$-módulo inyectivo.

5.9.39. Si A es un dominio de integridad y K es su cuerpo de fracciones, entonces K es un A-módulo inyectivo.

5.9.40. Sea G un grupo finito y k un cuerpo tal que $|G|$ es inversible en k. Mustrar que todo $k[Q]$-módulo es proyectivo e inyectivo. ¿Todo $k[G]$-módulo es necesariamente libre?

5.9.41. Si A un un anillo de división, todo A-modulo es inyectivo y proyectivo.

5.9.42. Sea A un anillo tal que existe un módulo que no es proyectivo. ¿Debe existir algún módulo cíclico no proyectivo? ¿Debe A tener algún ideal no proyectivo?

5.9.43. Describir todos los $\mathbb{Z}$-módulos proyectivos de tipo finito y, cuando k es un cuerpo, todos los $k[X]$-módulos proyectivos de tipo finito.

Algunos lemas usuales

5.9.44. *(a)* Sea

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \vdots{\scriptstyle f''} & & \\ 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0 \end{array}$$

un diagrama conmutativo de A-módulos izquierdos en el que las filas son exactas. Entonces existe exactamente un morfismo $f'' : M'' \to N''$ que completa el diagrama preservando la conmutatividad.

(b) Si f' y f son isomorfismos, entonces f'' es un isomorfismo.

5.9.45. *Lema de los cinco.* Consideremos un diagrama conmutativo de A-módulos izquierdos

$$\begin{array}{ccccccccc} M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 & \longrightarrow & M_5 \\ \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} & & \downarrow{\scriptstyle \alpha_4} & & \downarrow{\scriptstyle \alpha_5} \\ N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 & \longrightarrow & N_5 \end{array}$$

y supongamos que las dos filas son exactas.

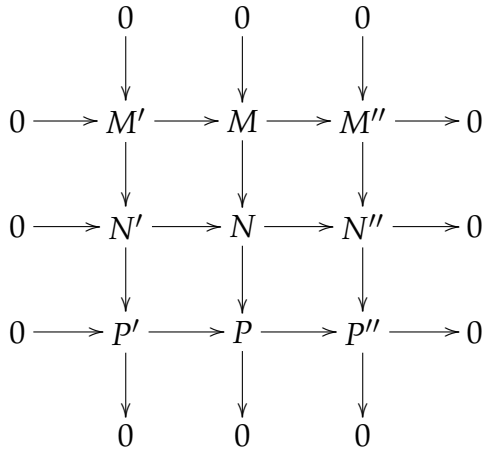
(a) Si α_1, α_2, α_4 y α_5 son isomorfismos, entonces α_3 es un isomorfismo.

(b) Si α_1 es sobreyectivo y α_2 y α_4 son inyectivos, entonces α_3 es inyectivo.

(c) Si α_5 es inyectivo y α_2 y α_4 son sobreyectivos, entonces α_3 es sobreyectivo.

5.9.46. *Lema de los nueve.* Consideremos un diagrama de A-módulos

izquierdos



en el que las tres columnas y las dos primeras (o las dos últimas) filas son exactas. Entonces la tercera fila también es exacta.

Capítulo 6

Teoremas de estructura

Este capítulo tratará dos situaciones diferentes en donde hay una descripción completa de la categoría de módulos o de la categoría de módulos finitamente generados. Comenzaremos con los anillos semisimples y luego veremos el teorema de estructura de módulos finitamente generados sobre anillos principales.

Estos teoremas de estructura tienen muchísimas aplicaciones. Particularmente, remarcamos el caso de representaciones de grupos finitos sobre k-espacios vectoriales, cuando la característica de k no divide al orden del grupo, como caso de categoría semisimple, e indicamos como obtener la forma normal de Jordan de un endomorfismo de un espacio vectorial como aplicación del teorema de estructura sobre un dominio principal.

6.1 Módulos y anillos semisimples

El punto de vista del capítulo anterior fue: dado un anillo A, ¿cuáles son los A-módulos inyectivos o proyectivos? El problema que planteamos ahora es, en cierto sentido, inverso: caracterizar los anillos A tales que todo A-módulo sea proyectivo, o inyectivo, o libre.

Por ejemplo, para que todo A-módulo sea proyectivo se necesita que todo A-módulo sea sumando directo de un libre. En particular, todo ideal de A debe ser un sumando directo de A.

Recordamos que un A-módulo M es *simple* si sus únicos submódulos son $\{0\}$ y M.

Sea A un anillo con la propiedad de que todo A-módulo a izquierda es proyectivo y sea B un subconjunto de A, maximal con respecto a las siguientes dos propiedades

- $b \in B$ sii $\langle b \rangle$ es simple; y
- si $b, b' \in B$ y $b \neq b'$, entonces $\langle b \rangle \bigcap \langle b' \rangle = \{0\}$.

Sea $M = \sum_{b \in B} \langle b \rangle$. Es fácil ver que la suma es necesariamente directa. Afirmamos que $M = A$.

Para llegar a un absurdo, supongamos que no es este el caso. Existe entonces un ideal a izquierda maximal I tal que $M \subseteq I$. Como A/I es un A-módulo simple y por lo tanto cíclico, existe $b \in A$ tal que $\langle r \rangle$ es simple y $\langle r \rangle \cong A/I$. Por hipótesis, A/I es un A-módulo proyectivo, así que consderando la sucesión exacta evidente

$$0 \longrightarrow I \longrightarrow A \longrightarrow A/I \longrightarrow 0$$

vemos que $A \cong I \oplus A/I$. Pero entonces $\langle r \rangle \subseteq M \subseteq I$, lo que es un absurdo. Concluimos que debe ser $M = A$, como afirmamos, y que el A-módulo ${}_AA$ es suma directa de submódulos simples.

Definición 6.1.1. Un A-módulo M es *semisimple* si M es suma directa de submódulos simples. El anillo A es *semisimple* si A, considerado como A-módulo a izquierda, es semisimple.

Ejemplos.
1. Todo módulo simple es semisimple. En particular, el módulo $\{0\}$ es semisimple.

2. Si k es un cuerpo, todo k-espacio vectorial es k-módulo semisimple.

3. Si k es un cuerpo y $A = k \times \cdots \times k$ (n-factores), entonces A es un anillo semisimple.

4. $\mathbb{Z}$ no es un $\mathbb{Z}$-módulo semisimple pues los ideales de $\mathbb{Z}$ no son sumandos directos de $\mathbb{Z}$.

5. Un grupo abeliano G es simple si y sólo si $G \cong \mathbb{Z}_p$ para algún número primo p. G es semisimple si y sólo si

$$G \cong \bigoplus_{p \text{ primo}} \mathbb{Z}_p^{(I_p)}$$

para ciertos conjuntos I_p.

6. Si $I \subset A$ un ideal a izquierda maximal, entonces A/I es un A-módulo simple.

7. Si k es un cuerpo, G es un grupo finito y la característica de k es $|G|$, entonces kG no es kG-módulo semisimple.

Observación. Si M es un A-módulo simple, entonces M es cíclico y está generado por cualquiera de sus elementos no nulos. En efecto, si $0 \neq m \in M$, $\langle m \rangle$ es un submódulo de M que no puede ser propio.

Ejercicio. Sea M un A-módulo. Entonces M es simple si y sólo si existe un ideal a izquierda maximal $I \subset A$ tal que $M \cong A/I$.

Proposición 6.1.2. *Sea M un A-módulo. Entonces M es semisimple si y sólo si todo submódulo de M es un sumando directo.*

Demostración. Supongamos que todo submódulo de M es un sumando directo. Mostremos primero que

> todo submódulo no nulo de M contiene un submódulo simple. (6.1)

Claramente, alcanza con mostrar que todo submodulo cíclico no nulo de M contiene un submódulo simple. Sea entonces $m \in M - \{0\}$ y consideremos el submódulo $\langle m \rangle \subset M$ y el ideal izquierdo

$$\operatorname{ann}(m) = \{a \in A : am = 0\}.$$

Como $\operatorname{ann}(m)$ es un ideal propio, existe un ideal izquierdo maximal $\mathfrak{m} \subset A$ tal que $\operatorname{ann}(m) \subset \mathfrak{m}$. Es fácil ver que $\mathfrak{m}m$ es un submódulo maximal de $\langle m \rangle$ y que, entonces, $\langle m \rangle / \mathfrak{m}m$ es un A-módulo simple. La hipótesis sobre M nos dice que $\mathfrak{m}m$ es un sumando directo de M, así que existe un submódulo $L \subset M$ tal que $M = L \oplus \mathfrak{m}m$. Pero entonces

$$\langle m \rangle = (L \oplus \mathfrak{m}m) \cap \langle m \rangle = (L \cap \langle m \rangle) \oplus \mathfrak{m}m,$$

así que $L \cap \langle m \rangle \cong \langle m \rangle / \mathfrak{m}m$ es un submódulo simple de $\langle m \rangle$.

Mostremos ahora que M es semisimple, como afirma la proposición. Sea $M' \subset M$ un submódulo de M maximal con respecto a la propiedad de ser suma directa de submódulos simples y supongamos, para llegar a un absurdo, que $M' \subsetneq M$. Por hipótesis, M'

es un sumando directo de M, así que existe un submódulo $N \subset M$ no nulo tal que $M = M' \oplus N$. Usando (6.1), vemos que existe un submódulo simple no nulo $S \subset N$. Pero entonces $M' \oplus S$ es un submódulo de M que es suma de simples y que contiene estrictamente a M'. Esto contradice la elección de M'.

Supongamos ahora que M es semisimple y sea T un submódulo propio de M. Por hipótesis, existe una familia $\{M_i\}_{i\in I}$ de submódulos simples de M tal que $M = \bigoplus_{i\in I} M_i$. Sea

$$\mathcal{F} = \{J \subseteq I : T \cap \bigoplus_{i\in J} M_i = \{0\}\}.$$

Como T es un submódulo propio, existe $i \in I$ tal que $M_i \not\subset T$ y entonces, como M_i es simple, $T \cap M_i = \{0\}$. Esto dice que $\{i\} \in \mathcal{F}$ y que $\mathcal{F} \neq \varnothing$. Es fácil ver que $\mathcal{F}$ es un conjunto inductivo, así que posee un elemento maximal J_0.

Sea $T' = \bigoplus_{i\in J_0} M_i$. La elección de J_0 implica que $T \cap T' = \{0\}$, así que $T \oplus T'$ es un submódulo de M. Veamos que, de hecho, es $M = T \oplus T'$, de manera que T es un sumando directo de M.

Para ver que $T \oplus T' = M$ basta mostrar que para todo $i \in I$, $M_i \subset T \oplus T'$. Sea entonces $k \in I$. La elección de J_0 nos dice que $M_k \cap (T \oplus T') \neq \{0\}$ así que $M_k = M_k \cap (T \oplus T')$ porque M_k es simple. Esto es, $M_k \subset T \oplus T'$, como queríamos. □

Corolario 6.1.3. *Sea M un A-módulo semisimple y N un submódulo. Entonces N y M/N también son semisimples.*

Demostración. Sea $P \subset N$ un submódulo. Como P es un submódulo de M, es un sumando directo y existe entonces un morfismo $p : M \to P$ tal que $p|_P = \mathsf{Id}_P$. Pero entonces el morfismo restringido $q = p|_N : N \to P$ es tal que $q|_P = \mathsf{Id}_P$, así que P es un sumando directo de N.

Esto nos dice que todo submódulo de N es un sumando directo. La proposición, entonces, nos permite asegurar que N es semisimple. Por otro lado, como N es un sumando directo de M, entonces M/N es isomorfo a un sumando directo de M, así que es semisimple. □

Ejercicio. Sean A y B dos anillos. Entonces $A \times B$ es un anillo semisimple si y sólo si A y B lo son.

Observación. Si M es un A-módulo tal que admite un submódulo semisimple N tal que además M/N es semisimple, no es cierto en general que M sea semisimple. Un (contra)ejemplo de esta situación es la extensión

$$0 \longrightarrow \mathbb{Z}_p \longrightarrow \mathbb{Z}_{p^2} \longrightarrow \mathbb{Z}_p \longrightarrow 0$$

Proposición 6.1.4. *Sea A un anillo, son equivalentes:*

(a) A es semisimple.
(b) Todo A-módulo es semisimple.
(c) Todo A-módulo libre es semisimple.
(d) Todo A-módulo es proyectivo.
(e) Toda extensión de A-módulos es trivial.
(f) Todo A-módulo es inyectivo.
(g) Todo ideal (a izquierda) de A es inyectivo.
(h) Todo cociente de A es proyectivo.

Demostración. (a) $\Rightarrow$ (b) Todo A-módulo es suma de submódulos cíclicos, así que basta ver que todo A-módulo cíclico es semisimple. Si M es cíclico, $M \cong A/I$ para algún ideal (a izquierda) I. Como A es semisimple, el corolario 6.1.3 nos dice que M es semisimple.

(b) $\Rightarrow$ (c) Esto es inmediato.

(c) $\Rightarrow$ (d) Sea M un A-módulo. Existe un módulo libre L y un epimorfismo $p : L \to M$. La proposición 6.1.2 nos dice que $\operatorname{Ker}(p)$ es un sumando directo de L, así que $L/\operatorname{Ker}(p) \cong M$ también es isomorfo a un sumando directo de L. Esto muesta que M es proyectivo.

(d) $\Rightarrow$ (e) Consideramos una extensión de A-módulos

$$0 \longrightarrow X \longrightarrow Y \longrightarrow Z \longrightarrow 0$$

Como Z es proyectivo, esta sucesión se parte.

(e) $\Rightarrow$ (f) Sea M un A-módulo. Como la hipótesis implica que toda sucesión exacta de la forma

$$0 \longrightarrow M \longrightarrow X \longrightarrow Y \longrightarrow 0$$

se parte, M es inyectivo.

(f) $\Rightarrow$ (g) Esto es inmediato.

(g) $\Rightarrow$ (h) Sea I un ideal. Por hipótesis, I es inyectivo, así que la sucesión exacta

$$0 \longrightarrow I \longrightarrow A \longrightarrow A/I \longrightarrow 0$$

se parte. Esto dice que A/I es isomorfo a un sumando directo de A. En particular, A/I es proyectivo.

(h) $\Rightarrow$ (a) Por la Proposición 6.1.2 basta ver que todo ideal I de A es un sumando directo. Consideremos de nuevo la sucesión

$$0 \longrightarrow I \longrightarrow A \longrightarrow A/I \longrightarrow 0$$

Como A/I es proyectivo, esta sucesión se parte. Luego I es un sumando directo. □

Proposición 6.1.5. *Si A es semisimple, entonces A es anillo artiniano y noetheriano a izquierda.*

Demostración. Para ver que es noetheriano, basta ver que todo ideal es finitamente generado. Pero como todo ideal es un sumando directo, todo ideal es isomorfo a un cociente de A, que es cíclico y entonces finitamente generado.

Para ver que A es artiniano consideremos una cadena descendente de ideales

$$I_1 \supset I_2 \supset I_3 \supset \cdots$$

Sea $i \in \mathbb{N}$. Como I_i es un submódulo de A, es semisimple, así que el submódulo $I_{i+1} \subset I_i$ es un sumando directo, esto es, existe un ideal $C_i \subset A$ tal que $I_i = C_i \oplus I_{i+1}$.

Consideremos ahora la cadena creciente de ideales

$$C_1 \subset (C_1 \oplus C_2) \subset (C_1 \oplus C_2 \oplus C_3) \subset \cdots$$

Como A es noetheriano, esta cadena se estaciona, así que existe $n_0 \in \mathbb{N}$ tal que $C_n = 0$ para todo $n \geq n_0$. Esto es, $I_n = I_{n+1}$ si $n \geq n_0$. Luego la cadena descendente original de ideales se estaciona. □

Ejemplo. Sea D un anillo de división y $A = \mathsf{M}_2(D)$. Llamemos $I_1 = \{\left(\begin{smallmatrix} a & 0 \\ b & 0 \end{smallmatrix}\right) : a, b \in D\}$ e $I_2 = \{\left(\begin{smallmatrix} 0 & a \\ 0 & b \end{smallmatrix}\right) : a, b \in D\}$.

Es claro que se trata de A-submódulos a izquierda y que $A \cong I_1 \oplus I_2$. Veamos que ambos son simples — consideramos solamente I_1, ya que I_2 puede manejarse de la misma forma.

Sea $m = \left(\begin{smallmatrix} a & 0 \\ b & 0 \end{smallmatrix}\right) \in I_1 - \{0\}$. Supongamos primero que $a \neq 0$. Entonces

$$\begin{pmatrix} a^{-1} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

y

$$\begin{pmatrix} 0 & 0 \\ a^{-1} & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Usando esto, es fácil ver que m genera a I_1.

Si, en cambio, es $a = 0$, debe ser necesariamente $b \neq 0$. Dejamos como ejercicio ver que en este caso m también genera a I_1.

Concluimos así que $\mathsf{M}_2(D)$ es semisimple. De la misma forma puede verse que $\mathsf{M}_n(D)$ es semisimple para cualquier $n \in \mathbb{N}$.

Teorema 6.1.6. (Teorema de Maschke) *Sea G un grupo finito y sea k un cuerpo en el que $|G|$ es inversible. Entonces $k[G]$ es un anillo semisimple.*

Demostración. Sea M un $k[G]$-módulo y $S \subseteq M$ un submódulo. Mostremos que S es un sumando directo. Para eso, alcanza con mostrar que existe un morfismo de $k[G]$-módulos $\phi : M \to S$ tal que $\phi|_S = \mathsf{Id}_S$.

Como k es un cuerpo, existe ciertamente una transformación k-lineal $\pi : M \to S$ tal que $\pi|_S = \mathsf{Id}_S$. Definamos $\phi : M \to S$ poniendo

$$\phi(m) = \tfrac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}m)$$

para todo $m \in M$. Afirmamos que ϕ es $k[G]$-lineal y que $\phi|_S = \mathsf{Id}_S$.

Si $s \in S$, entonces $g^{-1}s \in S$ y $\pi(g^{-1}s) = g^{-1}s$, así que

$$\begin{aligned} \phi(s) &= \tfrac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}s) = \tfrac{1}{|G|} \sum_{g \in G} gg^{-1}s \\ &= \tfrac{1}{|G|} \sum_{g \in G} s = \tfrac{|G|}{|G|}s = s. \end{aligned}$$

Esto dice que $\phi|_S = \mathsf{Id}_S$. Por otro lado, si $h \in G$ y $m \in M$, es

$$\phi(hm) = \tfrac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}hm);$$

Si ponemos $g' = hg$ en la suma, esto queda

$$\begin{aligned} &= \tfrac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}hm) = \tfrac{1}{|G|} \sum_{g' \in G} g'\pi((g')^{-1}hm) \\ &= \tfrac{1}{|G|} \sum_{g' \in G} hg\pi(g^{-1}h^{-1}hm) = \tfrac{1}{|G|} h\Big(\sum_{g' \in G} g\pi(g^{-1}m) \Big) \\ &= h\phi(m) \end{aligned}$$

Vemos así que ϕ es un morfismo de $k[G]$-módulos. □

Ejemplo. *(Lema de Schur)* Sea M un A-módulo simple. Entonces el anillo $\mathrm{End}_A(M)$ es un anillo de división, esto es, todo morfismo A-lineal $f : M \to M$ o bien es cero, o bien es un isomorfismo.

Teorema 6.1.7. (Wedderburn) *Sea A un anillo semisimple. Entonces existe $N \in \mathbb{N}$, anillos de división $D_1, \ldots, D_N$ y números $r_1, \ldots, r_N \geq 1$ tales que*

$$A^{\mathsf{op}} \cong \prod_{i=1}^{N} \mathsf{M}_{r_i}(D_i).$$

Demostración. Como A es semisimple, existen números N, r_1, …, $r_N \in \mathbb{N}$ y un conjunto finito de ideales simples

$$\{L_{i,j} : 1 \leq i \leq N, 1 \leq j \leq r_i\}$$

tales que

- $A \cong \bigoplus_{i=1}^{N} \bigoplus_{j=1}^{r_i} L_{i,j}$
- $L_{i,j} \cong L_{i'j'}$ sii $i = i'$.

Escribamos $A_i = \bigoplus_{j=1}^{r_j} L_{i,j}$. Hay una cadena de isomorfismos de anillos

$$\begin{aligned} A^{\mathsf{op}} &\cong \mathrm{Hom}_A(A, A) \cong \mathrm{Hom}_A(\bigoplus_{i=1}^{N} A_i, \bigoplus_{j=1}^{N} A_j) \\ &\cong \bigoplus_{i,j=1}^{N} \mathrm{Hom}_A(A_i, A_j). \end{aligned}$$

Si $i \neq j$, entonces $\mathrm{Hom}_A(A_i, A_j) = 0$ porque $L_{i,1} \ncong L_ij, 1$. Luego es

$$A \cong \bigoplus_{i=1}^{N} \mathrm{Hom}_A(A_i, A_i). \tag{6.2}$$

Sea $i \in \{1, \ldots, N\}$. Como $A_i = \bigoplus_{j=1}^{r_i} L_{i,j}$,

$$\mathrm{Hom}_A(A_i, A_i) \cong \bigoplus_{j,j'=1}^{r_i} \mathrm{Hom}_A(L_{i,j}, L_{i,j'}).$$

Si ponemos $D_i = \mathrm{End}_A(L_{i,1})$, entonces es fácil ver que

$$\mathrm{Hom}_A(A_i, A_i) \cong \mathsf{M}_{r_i}(D_i)$$

como anillo. Esto y (6.2) prueba el teorema. □

Corolario 6.1.8. *Sea A un anillo semisimple sin ideales biláteros propios. Entonces A es isomorfo a un anillo de matrices con coeficientes en un anillo de división.*

Corolario 6.1.9. *Sea A un anillo. Entonces A es semisimple a izquierda si y sólo si es semisimple a derecha.*

Demostración. Esto es claro en vista del Teorema de Wedderburn y notando que la trasposición de matrices da un isomorfismo de anillos $\mathsf{M}_n(D)^{\mathsf{op}} \cong \mathsf{M}_n(D^{\mathsf{op}})$ y que un anillo D es de division si y sólo si D^{op} es de división. □

Ejercicios.
1. Descomponer a $\mathbb{R}[\mathbb{Z}_2]$, $\mathbb{R}[\mathbb{Z}_3]$ y $\mathbb{C}[\mathbb{Z}_3]$ como producto de anillos de matrices sobre álgebras de división, como en el Teorema de Wedderburn. Sugerencia: encontrar módulos simples sobre los respectivos anillos. Antes de hacer cuentas, sabiendo que las únicas álgebras de dimensión finita sobre $\mathbb{R}$ son $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{H}$, ¿cuales son las posibilidades?

2. Si A es un anillo, $\mathrm{rad}(A)$ es la intersección de todos los ideales a izquierda maximales de A. Mostrar que si A es semisimple, $\mathrm{rad}(A) = 0$.

Proposición 6.1.10. *Sea A un anillo. Entonces A es semisimple si y sólo si es artiniano y* $\mathrm{rad}(A) = 0$.

Demostración. Ya vimos que si A es semisimple, entonces es artiniano y su radical es cero. Supongamos ahora que A es artiniano y que $\mathrm{rad}(A) = 0$ y veamos que todo ideal de A es un sumando directo.

Sea $I \subseteq A$ un ideal de A. Consideremos el conjunto

$$\mathcal{J} = \{J \subset A : J \text{ es un ideal a izquierda de } A \text{ tal que } I + J = A\}.$$

Como $A \in \mathcal{J}$, $\mathcal{J} \neq \varnothing$. Además $\mathcal{J}$ posee elementos minimales para la inclusión porque A es artiniano. Sea $J \in \mathcal{J}$ un elemento minimal. Por supuesto, $I + J = A$.

Supongamos que $I \cap J \neq \{0\}$. Elijamos un un ideal a izquierda B no nulo minimal entre aquellos que están contenidos en $I \cap J$; notemos que esto tiene sentido porque A es artiniano.

Como $\operatorname{rad}(A) = 0$, existe un ideal maximal $\mathfrak{m}$ tal que $B \not\subseteq \mathfrak{m}$ y, por lo tanto, $A = B + \mathfrak{m}$. Como $B \subseteq J$, resulta que $J \not\subseteq \mathfrak{m}$. Sea $J' = \mathfrak{m} \cap J \subseteq J$. Entonces

$$A = I + J = I + (B + \mathsf{M}) \cap J \subseteq I + B + J' = I + J',$$

ya que $B \subseteq I$. Pero esto nos dice que $J' \in \mathcal{J}$, lo que contradice la minimalidad de J.

Debe ser entonces $I \cap J = \{0\}$. En particular, $A = I \oplus J$. □

Ejercicio. Mostrar que si A es un anilo arbitrario, entonces $\operatorname{rad}(A)$ es un ideal bilátero.

Corolario 6.1.11. *Sea A un anillo artiniano sin ideales biláteros propios. Entonces A es isomorfo a un anillo de matrices con coeficientes en un anillo de división. En particular A es semisimple.*

Corolario 6.1.12. *Si A es artiniano, entonces el cociente $A/\operatorname{rad}(A)$ es semisimple.*

Demostración. Basta demostrar que $\operatorname{rad}(A/\operatorname{rad}(A)) = 0$, lo cual se deja como ejercicio. □

Ejercicio. Sea G un grupo finito no trivial y k un cuerpo. Mostrar que la función $\epsilon : k[G] \to k$ tal que $\epsilon(g) = 1$ para todo $g \in G$ es un morfismo de anillos. En particular, $k[G]$ siempre tiene por lo menos un ideal bilátero propio.

Observación. En algunos textos, aparece la siguiente definición de anillo simple: *un anillo A se dice simple si es artiniano y no tiene ideales biláteros propios*. Notamos que la condición de artiniano es esencial si se desea que la definición de simple implique semisimple, como lo muestra el siguiente ejemplo:

Sea k un cuerpo de característica cero. El *álgebra de Weyl* $A_1(k)$ es la subálgebra de $\operatorname{End}_k(k[X])$ generada por los endomorfismos p, $q \in \operatorname{End}_k(k[X])$ tales que

$$q(f) = Xf$$

y

$$p(f) = \frac{\mathrm{d}}{\mathrm{d}X} f$$

para todo $f \in k[X]$.

Es fácil ver que $[p, q] = 1$ (¡verificarlo!). Usando esto, se puede ver que $\{p^i q^j : i, j \in \mathbb{N}_0\}$ es una base de $A_1(k)$ como k-espacio vectorial. Si $P \in A_1(k)$ se escribe de la forma $P = \sum_{i=0}^{n} f_i(q) p^i$, en donde cada f_i es un polinomio en q y $f_n \neq 0$, diremos que el *grado* de P es n y que el polinomio $f_n \in k[q]$ es el coeficiente principal de P.

Dejamos como ejercicio verificar que:

- Si $P \in A_1(k)$ es un elemento de grado n con coeficiente principal f_n, entonces $[P, q]$ es un elemento de grado $n - 1$ y su coeficiente principal es nf_n.
- Si $f \in k[q]$, entonces $[p, f] = f'$.

Usando estas dos afirmaciones, es fácil ver que $A_1(k)$ no tiene ideales biláteros propios. En efecto, supongamos que I es un ideal bilátero no nulo de $A_1(k)$.

Sea $P_0 \in I$ un elemento no nulo arbitrario y sea g el grado de P_0. Definamos inductivamente $P_{i+1} = [P_i, q]$ para cada $i \in \mathbb{N}_0$. Entonces es fácil ver, usando la primera afirmación, que P_g es un elemento no nulo de $I \cap k[q]$. Escribamos $Q_0 = P_g$ y sea d el grado de Q_0 en $k[q]$. Definamos $Q_{i+1} = [p, Q_i]$ para cada $i \in \mathbb{N}_0$. Usando ahora la segunda afirmación, vemos que Q_d es un elemento no nulo de $I \cap k$. Como es inversible, vemos que $I = A_1(k)$.

6.2 Anillos euclídeos, principales y de factorización única

Comenzaremos recordando algunas definiciones generales y daremos algunas propiedades básicas de los dominios principales que se utilizarán luego.

Definición 6.2.1. Sea A un dominio íntegro. Diremos que A es *euclídeo* si existe una función $d : A - \{0\} \to \mathbb{N}_0$ tal que

- si $r, s \in A - \{0\}$, $d(r) \leq d(rs)$;
- si $a, b \in A$ y $b \neq 0$, existen $q, r \in A$ tales que $a = bq + r$ con $r = 0$ ó $d(r) < d(b)$.

Notemos que en la segunda condición no exigimos la unicidad de q o de r.

Ejemplos.
1. Un cuerpo k es euclídeo: podemos tomar $d \equiv 0$.
2. El anillo $\mathbb{Z}$ es euclídeo, con $d(m) = |m|$.
3. Si k es un cuerpo, $k[X]$ es euclídeo, con $d = \deg$.
4. Si p es un número primo, $\mathfrak{p} = p\mathbb{Z}$, el anillo $\mathbb{Z}_{\mathfrak{p}}$ es euclídeo, con $d : \mathbb{Z}_{\mathfrak{p}} - \{0\} \to \mathbb{N}_0$ dada por $d(\frac{m}{n}) = p^q$ si $m = p^q m'$ y $(m : m') = 1$.

Ejercicio. Mostrar que si k es un cuerpo, el anillo de polinomios de Laurent $k[X^{-1}, X]$ es un dominio euclídeo.

Proposición 6.2.2. *Si A es un dominio euclídeo, entonces es un dominio de ideales principales.*

Demostración. Sea $I \subseteq A$ un ideal no nulo y llamemos d a la función euclídea de A. Sea $n = min\{d(x) : x \in I - \{0\}\}$ y sea $y \in I$ tal que $d(y) = n$. Es claro que $\langle y \rangle \subseteq I$. Veamos que, de hecho, vale la igualdad.

Sea $x \in I - \{0\}$. Por hipótesis, existen $q, r \in A$ con $x = qy + r$, y o bien $r = 0$ o bien $d(r) < d(y)$. Como $r = x - qy \in I$, es $d(y) \leq d(r)$ por la elección de y. Necesariamente, entonces, $r = 0$, es decir, $x \in \langle y \rangle$. □

Recordamos que un elemento p en un anillo conmutativo A es *primo* si $p \notin \mathcal{U}(A)$ y

$$a, b \in A,\ ab \in \langle p \rangle \implies a \in \langle p \rangle \text{ ó } b \in \langle p \rangle.$$

Equivalentemente, p es primo si y sólo si $A/\langle p \rangle$ es un dominio íntegro.

Por otro lado, un elemento $q \in A$ es *irreducible* si $q \neq 0, q \notin \mathcal{U}(A)$ y si

$$b, c \in A,\ q = bc \implies b \in \mathcal{U}(A) \text{ ó } c \in \mathcal{U}(A).$$

Si q es irreducible y u es una unidad, claramente uq es también irreducible. Decimos que uq es un irreducible *asociado* a q.

Ejercicio. Si p es un primo en un anillo A, entonces p es irreducible.

Un anillo A es un *dominio de factorización única* (dfu) si es un dominio íntegro y satisface la siguiente condición:

> para todo $a \in A - \{0\}$, existen $q_1, \ldots, q_r \in A$ irreducibles y $u \in \mathcal{U}(A)$ tales que $a = u \prod_{i=1}^{r} q_i$ y esta escritura es única a menos de permutación y/o cambio de irreducibles por sus asociados.

Observación. Si A es un dominio de factorización única y $q \in A$ es irreducible, entonces q es primo.

Ejercicio. Mostrar que en un dominio de ideales principales todo elemento irreducible es primo.

Proposición 6.2.3. *Si A es un dominio principal, entonces A es un dominio de factorización única.*

Demostración. Sea $a \in A$ tal que $a \neq 0$ y $a \notin \mathcal{U}(A)$ y supongamos que a no puede escribirse como producto de irreducibles — en particular, a no es irreducible. Entonces existen elementos $a_1, b_1 \in A$ tales que ni a_1 ni b_1 es una unidad, $a = a_1 b_1$ y a_1, por ejemplo, no es producto de irreducibles.

Como $a_1 \mid a$ y $b_1 \notin \mathcal{U}(A)$, es $\langle a \rangle \subsetneq \langle a_1 \rangle$. Por otro lado, como a_1 no es producto de irreducibles, podemos repetir el razonamiento anterior. Obtenemos de esta forma una cadena de ideales estrictamente creciente, lo que es absurdo porque A es noetheriano ya que todos sus ideales son principales.

La unicidad se demuestra de la misma manera en que se prueba la unicidad de factorización en primos para los números enteros. □

Ejemplo. Todos los dominios euclídeos, como $\mathbb{Z}$ y, si k es un cuerpo, $k[X]$, son de factorización única. También lo es $k[X, X^{-1}]$. Más generalmente, toda localización de un dominio de factorización única es un dominio de factorización única.

Ejercicio. Si A es un anillo arbitrario y $a_1, \ldots, a_r \in A$, un *máximo común divisor para $a_1, \ldots, a_r$* es un elemento de A que divide todos los a_i y que es maximal, relativamente al orden de divisibilidad, con esta propiedad.

Muestre que si un conjunto de elementos de A posee un máximo común divisor, éste esta unívocamente determinado a menos de multiplicación por unidades de A. Además, muestre que todo conjuntofinito de elementos de un dominio de factorización única posee un máximo común divisor.

Si A es un dominio de factorización única y $f \in A[X]$, decimos que f es *primitivo* si el máximo comun divisor de los coeficientes de f es 1.

Lema 6.2.4. (Lema de Gauss) *Sea A un dominio de factorización única y $f, g \in A[X]$. Si f y g son primitivos, entonces fg es primitivo.*

Demostración. Por el absurdo, supongamos que fg no es primitivo y sea $p \in A$ un elemento primo de A que divide a todos los coeficientes de fg. Consideremos la proyección canónica $\pi : A \to A/\langle p\rangle$ sobre el cociente $A/\langle p\rangle$ y notemos también $\pi : A[X] \to (A/\langle p\rangle)[X]$ a la extesión de π a los anillos de polinomios.

Como p es primo, $A/\langle p\rangle$ es un dominio íntegro, así que en anillo $(A/\langle p\rangle)[X]$ también es un domínio íntegro. La elección de p implica que $\pi(f)\pi(g) = \pi(fg) = 0$, así que $\pi(f) = 0$ o $\pi(g) = 0$. Pero esto es imposible, porque ambas posibilidades contradicen la hipótesis hecha sobre f y g. □

Teorema 6.2.5. *Si A es un dominio de factorización única, entonces $A[X]$ también lo es.*

Demostración. Sea $f \in A[X] - \{0\}$. Sean $c \in A$ y $g \in A[X]$ tales que $f = cg$ y g es primitivo.

Sea F el cuerpo de fracciones de A. Como $F[X]$ es un dominio de factorización única y $g \in A[X] \subset F[X]$, existe una factorización

$$g = \tfrac{a}{b} h_1 \cdots h_k,$$

con $a, b \in A$, $b \neq 0$ y $h_1, \ldots, h_k \in F[X]$ polinomios irreducibles. Sin pérdida de generalidad, a menos de cambiar a y b, podemos suponer que para todo $i \in \{1, \ldots, k\}$, el polinomio h_i tiene sus coeficientes en A y es primitivo. En ese caso, cada h_i es un elemento irreducible de $A[X]$.

Como es $bg = ah_1 \cdots h_k$ y como el polinomio $h_1 \cdots h_k$ es primitivo por el lema de Gauss, vemos que existe $u \in \mathcal{U}(A)$ tal que $a = ub$.

Luego $g = uh_1 \cdots h_k$ y, en definitiva, $f = uch_1 \cdots h_k$. Factorizando ahora a c como producto de irreducibles de A, obtenemosuna factorización de f como producto de irreducibles de $A[X]$.

La unicidad de la factorización obtenida sigue de la unicidad de la factorización en $F[X]$ y de la unicidad de la factorización de c en A. □

Ejemplo. El anillo $\mathbb{Z}[x]$ es un dominio de factorización unica y no es un dominio de ideales principales: por ejemplo, el ideal $\langle 2, X\rangle$ no es principal. De la misma forma, si k es un cuerpo, $k[X_1, \ldots, X_n]$ es un dominio de factorización única que es de ideales principales sólo cuando $n = 1$.

6.3 Módulos finitamente generados sobre un dominio de ideales principales

Hemos visto en la sección de módulos libres que si M es un módulo finitamente generado sobre un dominio de ideales principales A, entonces $M \cong t(M) \oplus A^r$ para un $r \in \mathbb{N}_0$ unívocamente determinado. El objetivo de esta sección es describir completamente los módulos sobre un dominio principal que son finitamente generados y de torsión.

Lema 6.3.1. *Sea A un dominio de ideales principales. Sea L un A-módulo libre y sea $M \subseteq L$ un submódulo no nulo. Entonces existen $z \in L$ no nulo, un submódulo S de L y $c \in A$ tales que*

- $L = \langle z\rangle \oplus S$;
- $M = \langle cz\rangle \oplus (S \bigcap M)$; *y*
- *si $f : L \to A$ es un morfismo de A-módulos tal que $f(z) = 1$, entonces es $f(M) = \langle c\rangle$.*

Demostración. Sea $\{x_j : j \in J\}$ una base para L y sea $\{f_j : j \in J\}$ la base dual. Consideremos el conjunto

$$\mathcal{I} = \{f(M) : f \in \mathrm{Hom}_A(L, A),\ f(M) \neq 0\}.$$

Los elementos de $\mathcal{I}$ son ideales no nulos de A y es $\mathcal{I} \neq \varnothing$: si $m \in M - \{0\}$, existe $j \in J$ tal que $0 \neq f_j(m) \in f(M)$, así que $f(M) \in \mathcal{I}$.

Como A es noetheriano, $\mathcal{I}$ posee un elemento maximal, al que notamos I_0. Sea $h : L \to A$ un morfismo tal que $h(M) = I_0$. Como A es un dominio de ideales principales, existe $c \in A$ tal que $I_0 = \langle c \rangle$. Sea $u \in M$ un elemento tal que $h(u) = c$.

Afirmamos que u es divisible por c en L. Para verlo, claramente alcanza con mostrar que c divide a $f_j(u)$ para todo $j \in J$.

Sea $j \in J$. Sea $d \in A$ el máximo común divisor de c y $f_j(u)$ y sean $r, s \in A$ tales que $d = rc + sf_j(u)$. Entonces

$$d_i = rc + sf_j(u) = rh(u) + sf_j(u) = (rh + sf_j)(u).$$

Si ponemos $\phi = rh + sf_j : L \to A$, hemos mostrado que

$$\phi(M) \supset \langle d \rangle \supset \langle c \rangle.$$

Esto contradice la maximalidad de I_0, a menos que sea $d_i = c$, esto es, a menos que c divida a $f_j(u)$. Esto prueba nuestra afirmación.

Ahora, como c divide a u en L, existe $z \in L$ tal que $u = cz$. Recordando que A es íntegro, es claro que $h(z) = 1$. Sea $S = \mathrm{Ker}(h)$.

Verifiquemos con estas elecciones para z, S y c se satisfacen las condiciones del enunciado:

- Consideremos la sucesión exacta

  $$0 \longrightarrow \mathrm{Ker}(h) \longrightarrow L \longrightarrow \mathrm{Im}(h) \longrightarrow 0$$

  Como $\mathrm{Im}(h) = A$ es proyectivo, la sucesión se parte y S es un sumando directo de L. Un complemento para L puede obtenerse a partir de una sección de h como, por ejemplo, el morfismo $A \to L$ tal que $1 \mapsto z$. Luego $L = \langle z \rangle \oplus S$.
- La inclusión $\langle cz \rangle \oplus (S \bigcap M) \subseteq M$ es clara, pues $cz = u \in M$. En el otro sentido, si $x \in M$, entonces $h(x)z \in \langle cz \rangle \subset M$. Luego podemos escribir $x = h(x)z + (x - h(x)z)$. Como el elemento $h(x)z$ está en M, se sigue que $(x - h(x)z) \in M$ y, además, $h(x - h(x)z) = h(x) - h(x)h(z) = 0$. Esto nos dice que $(x - h(x)z) \in M \cap S$.
- Sea $f : L \to A$ un morfismo de A-módulos tal que $f(z) = 1$. Entonces $f(u) = f(cz) = cf(z) = c$, así que $\langle c \rangle \subseteq f(M)$. Pero como $\langle c \rangle = I_0$ es un ideal maximal con respecto a esa propiedad, entonces debe ser $\langle c \rangle = f(M)$.

Esto termina la prueba. □

Corolario 6.3.2. *Sea A un dominio de ideales principales y sean L un A-módulo libre y $M \subset L$ un submódulo de tipo finito. Entonces existe una base $\{e_i : i \in I\}$ de L, una subfamila finita $\{e_{i_j} : 1 \leq j \leq n\}$ de $\{e_i : i \in I\}$ y elementos $a_1, \ldots, a_n \in A$ tales es $a_j \mid a_{j+1}$ para $1 \leq j < n$ y $M = \bigoplus_{j=1}^{n} \langle a_j e_{i_j} \rangle$.*

Demostración. Hacemos inducción en el rango de M. Por la proposición anterior, si $M \neq \{0\}$, existe $z \in L$, $c \in A$ y un submódulo S de L tales que $L = \langle z \rangle \oplus S$ y $M = \langle cz \rangle \oplus (S \cap M)$. Por lo tanto el rango de $S \cap M$ es igual al rango de M menos uno. Aplicando la hipótesis inductiva a $M \cap S$ considerado como submódulo del módulo libre S, vemos que existe una base $\{x_k : k \in K\}$ de S, una subfamilia finita $\{x_{k_l} : 2 \leq l \leq n\}$ y elementos $a_2\ a_3, \ldots, a_n \in A$ tales que $S \cap M = \bigoplus_{j=2}^{n} \langle a_j x_{k_j} \rangle$ y $a_i \mid a_{i+1}$ si $2 \leq i < n$.

Escribamos $a_1 = c$ y $x_{k_1} = z$. Sabemos que $M = \bigoplus_{j=1}^{n} \langle a_j x_{k_j} \rangle$. Nos falta ver que $a_1 \mid a_2$.

Definamos $f : L \to A$ poniendo

$$f(x_i) = \begin{cases} 1, & \text{si existe } j \text{ tal que } i = i_j; \\ 0, & \text{en caso contrario.} \end{cases}$$

Para todo $j \in \{1, \ldots, n\}$, es $a_j = f(a_j x_{i_j}) \in f(M)$ por el último ítem de la proposición anterior. Como $f(z) = 1$, tenemos que $f(M) = \langle c \rangle = \langle a_1 \rangle$, así que, en particular, $a_j \in \langle a_1 \rangle$ para todo j. Esto nos dice que $a_1 \mid a_2$. □

Teorema 6.3.3. *Sea A un dominio de ideales principales y sea M un A-módulo de tipo finito. Entonces*

(a) Existe una sucesión $d_1 \mid d_2 \mid \cdots \mid d_n$ de elementos no inversibles de A tales que $M \cong \bigoplus_{i=1}^{n} A/\langle d_i \rangle$

(b) Si $\{d_i\}_{i=1}^{n}$ y $\{d'_i\}_{i=1}^{n'}$ son dos familias de elementos de A como en la primera parte, entonces $n = n'$ y existen $u_1, \ldots, u_n \in \mathcal{U}(A)$ tales que $d_i = u_i d'_i$ si $1 \leq i \leq n$.

Demostración. Veamos ahora la demostración de la primera parte. Probaremos la segunda luego de enunciar algunos corolarios.

Sabemos que existen A-módulo libre de tipo finito L y un epimorfismo $p : L \to M$. En particular, $M \cong L/\operatorname{Ker}(p)$.

Como A es noetheriano, $\operatorname{Ker}(p)$ es de tipo finito. El corolario anterior nos dice, entonces, que existe una base $\{e_i : 1 \leq i \leq r\}$ de L

y elementos $d_1, \ldots, d_s \in A$ con $d_j \mid d_{j+1}$ si $1 \leq j < s$ y tales que $\{d_i e_i : 1 \leq i \leq s\}$ es una base de $\mathrm{Ker}(p)$. Notemos que es $r = \mathrm{rg}(L)$ y $s = \mathrm{rg}(\mathrm{Ker}(p))$.

Si j es tal que $s+1 \leq j \leq r$, sea $d_j = 0$. Entonces

$$M \cong L/\operatorname{Ker}(p) \cong \frac{\bigoplus_{i=1}^{r} \langle e_i \rangle}{\bigoplus_{i=1}^{s} \langle d_i e_i \rangle} \cong \bigoplus_{i=1}^{r} A/\langle d_i \rangle.$$

Sea $m = \max\{i : d_i \in \mathcal{U}(A)\} \cup \{0\}$. Entonces

$$M \cong \bigoplus_{i=m+1}^{r} A/\langle d_i \rangle,$$

ya que cuando d es una unidad, es $A/\langle d \rangle = 0$.

Renumerando los d_i y tomando $n = r - m$, vemos que los d_i resultantes no son unidades, que se dividen consecutivamente y que $M \cong \bigoplus_{i=1}^{n} A/\langle d_i \rangle$, como queríamos □

Corolario 6.3.4. *Sea A un dominio de ideales principales. Un A-módulo M es de tipo finito si y sólo si existe una familia $\{C_i : 1 \leq i \leq n\}$ de A-módulos cíclicos tales que $M \cong \bigoplus_{i=1}^{n} C_i$.* □

Observaciones.

1. La recíproca de este corolarioes cierta para cualquier anillo.
2. Con las notaciones del teorema de estructura, se tiene que

$$t(M) = \bigoplus_{\substack{1 \leq i \leq n \\ d_i \neq 0}} A/\langle d_i \rangle.$$

Corolario 6.3.5. *Sea A un dominio de ideales principales y sea M un A-módulo finitamente generado. Entonces existe $n \in \mathbb{N}_0$, una familia $\{p_1, \ldots p_r\}$ de primos de A y números enteros $1 \leq n_i^1 \leq \cdots \leq n_i^r$ $(i = 1, \ldots, r)$ tales que*

$$M \cong A^n \oplus \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{r} A/\langle p_i^{n_i^j} \rangle.$$

Demostración. Elijamos n igual al rango de la parte libre de M. Encuanto a la parte de torsión, sabemos que $t(M) = \bigoplus_{i=1}^{m} A/\langle d_i \rangle$.

Lo que hacemos ahora es escribir a cada d_i como producto de primos. De hecho, como $d_1 \mid d_2 \mid \cdots \mid d_m$, basta encontrar una factorización $d_m = \prod_{i=1}^{r} p_i^{n_i^r}$, ya que los primos que aparecen en los otros d_i son los mismos, con eventualmente exponentes menores (que pueden ser cero). Por el teorema chino del resto,

$$A/\langle \prod_{i=1}^{r} p_i^{n_i^r} \rangle \cong \bigoplus_{i=1}^{r} A/\langle p_i^{n_i^r} \rangle.$$

Ahora el corolario se sigue de reordenar todos los sumandos. □

Corolario 6.3.6. *Sean A un dominio de ideales principales y M un A-módulo finitamente generado de torsión. Entonces existe una familia finita de A-módulos cíclicos $\{C_i : i \in I\}$ y elementos primos $p_i \in A$, $i \in I$, de manera que C_i es p_i-primario para todo $i \in I$ y $M \cong \bigoplus_{i \in I} C_i$.*

Observaciones.
1. La condición de ser "de tipo finito" es esencial en la demostración del teorema, como lo muestra el siguiente ejemplo:

Sean $A = \mathbb{Z}$ y $M = \mathbb{Q}$. Es claro que $\mathbb{Q}$ no tiene torsión. Si el teorema de estructura fuera cierto sin la hipótesis de finitud, $\mathbb{Q}$ sería libre. Pero $\mathbb{Q}$ no es libre, pues cualquier par de elementos es linealmente dependiente y $\mathbb{Q}$ no es isomorfo ni a $\mathbb{Z}$ ni a $\{0\}$.

2. La condición $d_i \mid d_{i+1}$ es necesaria para la unicidad. Por ejemplo $\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$, son dos descomposiciones, pero la segunda descomposición no es "del tipo" de la del teorema de estructura.

Demostración la unicidad en el Teorema 6.3.3. Consideremos dos sucesiones decrecientes de ideales propios de A, $\{I_i\}_{1 \le i \le n}$ y $\{J_j\}_{1 \le j \le m}$, tales que $\bigoplus_{i=1}^{n} A/I_i \cong \bigoplus_{j=1}^{m} A/J_j$. Sea $\mathfrak{m}$ un ideal maximal cualquiera de A. Es claro que

$$\mathrm{Hom}_A\Big(\bigoplus_{i=1}^{n} A/I_i, A/\mathfrak{m}\Big) \cong \mathrm{Hom}_A\Big(\bigoplus_{j=1}^{m} A/J_j, A/\mathfrak{m}\Big),$$

o, equivalentemente,

$$\bigoplus_{i=1}^{n} \mathrm{Hom}_A(A/I_i, A/\mathfrak{m}) \cong \bigoplus_{j=1}^{m} \mathrm{Hom}_A(A/J_j, A/\mathfrak{m}).$$

Consideremos los ideales transportadores

$$(\mathfrak{m} : I_i) = \{a \in A : aI_i \subseteq \mathfrak{m}\}$$

y sea

$$\begin{aligned} \phi_i : (\mathfrak{m} : I_i) &\to \mathrm{Hom}_A(A/I_i, A/\mathfrak{m}) \\ a &\mapsto (f_a : \overline{x} \mapsto \overline{ax}) \end{aligned}$$

Es un ejercicio sencillo ver que ϕ_i es un epimorfismo con núcleo $\mathfrak{m}$ y que por lo tanto hay un isomorfismo

$$\mathrm{Hom}_A(A/I_i, A/\mathfrak{m}) \cong (\mathfrak{m} : I_i)/\mathfrak{m}.$$

En definitiva, tenemos que

$$\bigoplus_{i=1}^{n} (\mathfrak{m} : I_i)/\mathfrak{m} \cong \bigoplus_{j=1}^{m} (\mathfrak{m} : J_j)/\mathfrak{m}.$$

Elijamos ahora a $\mathfrak{m}$ de manera que contenga a I_1; como los I_i están encajados, $\mathfrak{m}$ contiene, de hecho, a todos los I_i, y por lo tanto $(\mathfrak{m} : I_i) = A$ si $1 \leq i \leq n$. Luego es

$$(A/\mathfrak{m})^n \cong \bigoplus_{j=1}^{m} (\mathfrak{m} : J_j)/\mathfrak{m}.$$

Como $\mathfrak{m} \subseteq (\mathfrak{m} : J_j)$, o bien $(\mathfrak{m} : J_j) = A$ o bien $(\mathfrak{m} : J_j) = \mathfrak{m}$. Sea $q = \#\{j : (\mathfrak{m} : J_j) = A\}$. Entonces $(A/\mathfrak{m})^n \cong (A/\mathfrak{m})^q$ como A-módulo y, en particular, como $A/\mathfrak{m}$-espacios vectoriales. Comparando dimensiones, concluimos que $n = q \leq m$.

De la misma forma puede verse que $m \leq n$ y por lo tanto $m = n$. Tenemos entonces que $\bigoplus_{i=1}^{n} A/I_i \cong \bigoplus_{i=1}^{n} A/J_i$, con $I_i \supseteq I_{i+1}$ y $J_i \supseteq J_{i+1}$ para todo $i = 1, \ldots, n-1$.

Notemos que si $c \in A$, este isomorfismo implica que

$$\bigoplus_{i=1}^{n} c\,A/I_i \cong \bigoplus_{i=1}^{n} c\,A/J_i.$$

Utilizaremos el siguiente lema, cuya demostración dejamos como ejercicio.

Lema. *Sean A un anillo arbitrario, I un ideal de A y $c \in A$. Entonces $c(A/I) \cong A/(I : cA)$.*

Como los ideales I_i y los J_i forman sucesiones decrecientes, es $(I_i : cA) \supseteq (I_{i+1} : cA)$ y $(J_i : cA) \supseteq (J_{i+1} : cA)$. Sean $i_I = \max\{i : c \in I_i\}$ y sea $i_J = \max\{i : c \in J_i\}$. Entonces

$$\bigoplus_{i=i_I+1}^{n} A/(I_i : cA) \cong \bigoplus_{i=i_J+1}^{n} A/(J_i : cA).$$

Por la primera parte de la demostración, resulta que $i_I = i_J$ y, por lo tanto, $I_i = J_i$ para todo i. □

Ejemplo. *(Forma normal de Jordan)* Sea k un cuerpo algebraicamente cerrado y sea (V, ϕ) un $k[X]$-módulo. Sabiendo que los polinomios irreducibles de $k[X]$ son de la forma $(x - \lambda)$ con $\lambda \in k$ y uando el teorema chino del resto en el contexto de polinomios, se puede demostrar fácilmente que existe una base de V en la que ϕ se escribe en bloques de Jordan, es decir, en bloques de la forma

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

En efecto, esto se consigue calculando en $k[X]/\langle (X-\lambda)^n \rangle$ la matriz del endomorfismo "multiplicar por X" en la base

$$\{\bar{1}, \overline{(X-\lambda)}, \overline{(X-\lambda)^2}, \ldots, \overline{(X-\lambda)^{n-1}}\}.$$

6.4 Ejercicios

Anillos semisimples

6.4.1. Sea A un anillo.

(a) Demuestre que $\operatorname{rad}(A/\operatorname{rad}(A)) = 0$.

(b) Demuestre que

$$\operatorname{rad}(A) = \{a \in A : 1 - xa \text{ es inversible a izquierda para todo } x\}.$$

(c) Demuestre que si $r \in \operatorname{rad}(A)$ entonces $1 - r$ es una unidad de A.

6.4.2. Probar que si A es anillo semisimple y L es un ideal a izquierda de A entonces:

(a) existe $e \in A$ idempotente tal que $L = Ae$.

(b) A no tiene ideales a izquierda nilpotentes.

(c) Si L es simple entonces el idempotente es primitivo, esto es, si $e = e_1 + e_2$ con $e_i^2 = e_i$ y $e_1e_2 = 0 = e_2e_1$, entonces alguno de los e_i es cero.

6.4.3. Sea k un cuerpo y $T_2(k) = \{\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) : a, b, c \in k\}$, que no es un anillo semisimple. Calcular $\operatorname{rad}(T_2(k))$ y $T_2(k)/\operatorname{rad}(T_2(k))$.

6.4.4. Sea k un cuerpo y $A = k \times k$ con el producto coordenada a coordenada. Mostrar que A es semisimple pero no simple. ¿Quiénes son los idempotentes ortogonales que suman uno?

6.4.5. ¿Para que $n \in \mathbb{N}$ es $\mathbb{Z}_n$ un anillo semisimple? Para alguno que no sea semisimple, dar un ejemplo de módulo que no sea proyectivo.

6.4.6. Sea A un anillo semisimple y M un A-módulo. A partir del teorema de Wedderburn sabemos que $A \cong \prod_{i=1}^{n} M_{r_i}(D_i)$ donde cada $D_i = \operatorname{End}_A(L_i)^{\mathsf{op}}$ es el anillo de endomorfismos del ideal simple L_i, y r_i es la cantidad de veces que aparece L_i en A como sumando directo. A su vez, M se descompone en suma directa de submódulos simples, cada uno de ellos isomorfo a algún L_i (¿porqué?). Dar una condición necesaria y suficiente sobre la multiplicidad de cada L_i en M para decidir cuándo M es libre. Concluir que si A es semisimple, entonces A tiene noción de rango.

6.4.7. Sea $A = M_n(k)$ con k un cuerpo, ver que es un ejemplo de anillo con noción de rango pero que no existe ningún morfismo de anillos $A \to D$ con D un anillo de división.

6.4.8. Sea k un cuerpo y G un grupo finito tal que $|G|$ es inversible en k. A partir de la caracterización que da el Teorema de Wedderburn obtener una fórmula que relacione las dimensiones de las álgebras de división y el tamaño de las matrices que aparecen con el orden del grupo.

6.4.9. Sea A un anillo y sea M un A-módulo simple. Entonces o bien M, considerado como grupo abeliano, es isomorfo a una suma directa de copias de $\mathbb{Q}$, o bien existe $p \in \mathbb{N}$ primo tal que M es, considerado como grupo abeliano, isomorfo a una suma directa de copias de $\mathbb{Z}_p$.

6.4.10. Sea A un anillo conmutativo y M y N dos A-módulos. Si alguno de M o N es semisimple, $M \otimes_A N$ es semisimple.

6.4.11. *(a)* Si A es un anillo semisimple y $B \subset A$ es un subanillo, ¿es B necesariamente semisimple?

(b) Si A es un anillo semisimple e $I \lhd A$ es un ideal bilátero, entonces A/I es semisimple.

6.4.12. *Anillos de matrices.*

(a) Sean A y B anillos y $n, m \in \mathbb{N}$. Entonces $\mathsf{M}_m(\mathsf{M}_n(A)) \cong \mathsf{M}_{mn}(A)$ y $\mathsf{M}_n(A \times B) \cong \mathsf{M}_n(A) \times \mathsf{M}_n(B)$.

(b) Si A es un anillo semisimple y $n \in \mathbb{N}$, entonces $\mathsf{M}_n(A)$ es semisimple.

(c) Sea A un anillo y sea $n \in \mathbb{N}$. Sea P el conjunto de vectores *fila* de n componentes en A y sea Q el conjunto de vectores *columna* de n componentes en A. Entonces P es un A-$\mathsf{M}_n(A)$-bimódulo y Q es un $\mathsf{M}_n(A)$-A-bimódulo con acciones de $\mathsf{M}_n(A)$ inducidas por el producto matricial. Más aún, hay un isomorfismo $Q \otimes_A P \cong \mathsf{M}_n(A)$ de $\mathsf{M}_n(A)$-bimódulos y un isomorfismo $P \otimes_{\mathsf{M}_n(A)} Q \cong A$ de A-bimódulos.

Como consecuencia de esto, si M es un A-módulo izquierdo, entonces

$$P \otimes_{\mathsf{M}_n(A)} (Q \otimes_A M) \cong M.$$

(d) Si M es un A-B-bimódulo y N es un B-módulo izquierdo proyectivo, entonces $M \otimes_B N$ es un A-módulo proyectivo.

(e) Sea A un anillo. Si existe $n \in \mathbb{N}$ tal que $\mathsf{M}_n(A)$ es semisimple, entonces el anillo A mismo es semisimple.

6.4.13. Sea A un anillo, M un A-módulo finitamente generado. Si $B = \mathrm{End}_A(M)$ y A es semisimple, entonces B es semisimple. Notemos que esto tiene como caso particular a la segunda parte del ejercicio **6.4.12**, ya que si $M = A^n$, entonces $\mathrm{End}_n(M) \cong \mathsf{M}_n(A)$.

6.4.14. *(a)* Un anillo artiniano a izquierda sin divisores de cero es un anillo de división.

(b) Si A es un anillo sin divisores de cero tal que $\mathsf{M}_n(A)$ es semisimple para algún $n \in \mathbb{N}$, entonces A es un anillo de división.

Álgebras de grupos cíclicos

Si $n \in \mathbb{N}$, sea G_n un grupo cíclico de orden n y sea $g_n \in G_n$ un generador.

6.4.15. Sea k un cuerpo de característica cero. Si $kG_n \cong \mathsf{M}_{n_1}(D_1) \times \cdots \times \mathsf{M}_{n_r}(D_r)$ es la factorización de kG_n como k-álgebra dada por el teorema de Wedderburn, de manera que es $r \in \mathbb{N}$, $n_1, \ldots, n_r \in \mathbb{N}$ y $D_1, \ldots, D_r$ son k-álgebras de división, entonces $n_1 = n_2 = \cdots = n_r = 1$ y D_i es un cuerpo para cada $i \in \{1, \ldots, r\}$.

En particular, hay exactamente r isoclases de kG_n-módulos simples y si $S_1, \ldots, S_n$ son representantes de estas clases, hay un isomorfismo de kG_n-módulos $kG_n \cong \bigoplus_{i=1}^{r} S_i$.

6.4.16. Sea k un cuerpo de característica cero. Sea M un kG_n-módulo simple y sea $a : m \in M \mapsto g_n m \in M$ la multiplicación por g_n. Entonces $a \in \mathrm{End}_{kG_n}(M)$ porque kG_n es un anillo conmutativo. Sea $\mu \in k[X]$ el polinomio minimal de a sobre k. Muestre que μ es irreducible en $k[X]$. Además, si $k = \mathbb{Q}$, entonces μ tiene coeficientes enteros.

6.4.17. *Álgebras de grupos cíclicos sobre* $\mathbb{C}$. Sea $\Omega_n \subset \mathbb{C}^\times$ el subgrupo multiplicativo de $\mathbb{C}^\times$ de las raíces n-ésimas de la unidad.

(a) La aplicación $\phi : \chi \in \hom_{\mathrm{Gr}}(G_n, \Omega_n) \mapsto \chi(g_1) \in \Omega_n$ es un isomorfismo de grupos abelianos. Esto implica que el conjunto $\hat{G}_n = \hom_{\mathrm{Gr}}(G_n, \Omega_n)$ tiene exactamente n elementos; llamemoslos $\chi_1, \ldots, \chi_n$.

(b) Muestre que si $\chi, \rho \in \hat{G}_n$, entonces

$$\sum_{g \in G_n} \chi(g)\rho(g^{-1}) = \delta_{\chi,\rho}.$$

Sugerencia. Multiplique el miembro izquierdo de esta igualdad por $(1 - \chi(g_1)\rho(g_1^{-1}))$.

(c) Si $\chi \in \hat{G}_n$, sea $e_\chi = \frac{1}{n}\sum_{g\in G_n} \chi(g^{-1})g \in \mathbb{C}G_n$. Entonces si χ, $\rho \in \hat{G}_n$,

$$e_\chi^2 = e_\chi,$$
$$e_\chi e_\rho = 1, \qquad \text{cuando } \chi \neq \rho,$$

y

$$\sum_{\chi\in\hat{G}_n} e_\chi = 1.$$

(d) Consideremos el anillo $A = \mathbb{C} \times \cdots \times \mathbb{C}$ con n factores y sean $x_1, \ldots, x_n \in A$ los elementos de la base canónica. Hay un isomorfismo de anillos $\phi : \mathbb{C}G_n \to A$ tal que $\phi(e_{\chi_i}) = x_i$ si $1 \leq i \leq n$. Describa representantes para cada isoclase de $\mathbb{C}G_n$-módulos simples.

6.4.18. *Álgebras de grupos cíclicos sobre* $\mathbb{Q}$.

(a) Sea p un número primo. Si $0 \leq k < l$, sea $\phi_{k,l} : \mathbb{Q}G_{p^l} \to \mathbb{Q}G_{p^k}$ el único morfismo de anillos tal que $\phi_{k,l}(g_{p^l}) = g_{p^k}$. Entonces $\ker \phi_{k,l} = \langle g_{p^l}^{p^k} - 1\rangle$. Además, si $0 \leq r < k < l$, es $\phi_{r,l} = \phi_{r,k} \circ \phi_{k,l}$.

(b) Sea p un número primo y pongamos $\Phi_p = \sum_{i=0}^{p-1} X^i \in \mathbb{Z}[X]$. Entonces

$$X^{p^l} - 1 = (X-1)\prod_{i=0}^{l-1} \Phi_p(X^{p^i})$$

y cada uno de los factores $\Phi_p(X^{p^i})$ con $0 \leq i < l$ es irreducible en $\mathbb{Q}[X]$.

(c) Sea p un número primo impar. Sea $l \geq 1$ y sea M un $\mathbb{Q}G_{p^l}$-módulo simple. Si $\dim_{\mathbb{Q}} M < p^l - p^{l-1}$, entonces existe $k < l$ y un $\mathbb{Q}G_{p^k}$-módulo simple N tal que $M \cong \phi_{k,l}^*(N)$.

(d) Sea p un número primo impar. Notemos M_0 al único $\mathbb{Q}G_1$-módulo simple. Entonces, para todo $l \geq 1$ existe, a menos de isomorfismo, un único $\mathbb{Q}G_{p^l}$-módulo simple M_l tal que

$$\dim_{\mathbb{Q}} M_l \geq p^l - p^{l-1}.$$

Además, se tiene que

- $\dim_{\mathbb{Q}} M_l = p^l - p^{l-1}$; y
- $\mathbb{Q}G_{p^l} \cong \bigoplus_{l=0}^{l-1} \phi_{i,l}^*(M_i) \oplus M_l$.

Sugerencia. Haga inducción con respecto a l.

(e) Enuncie y pruebe enunciados análogos a los dos últimos para $p = 2$.

(f) Sea $p \in \mathbb{N}$ primo, $l \geq 1$ y sea M_l un $\mathbb{Q}G_{p^l}$-módulo simple de dimensión $p^l - p^{l-1}$. Entonces M_l posee una base con respecto a la cual la matriz de la aplicación $a : m \in M \mapsto g_{p^l} m \in M$ es la matriz compañera del polinomio $\Phi_p(X^{p^l})$.

(g) Sea $f \in \mathbb{Q}[X]$ un polinomio mónico irreducible. Sea $a \in \mathsf{M}_n(\mathbb{Q})$ la matriz compañera de f. Entonces, si $\mathcal{C}(a) \subset \mathsf{M}_n(\mathbb{Q})$ es el centralizador de a en $\mathsf{M}_n(\mathbb{Q})$, hay un isomorfismo de anillos $\mathcal{C}(a) \cong \mathbb{Q}[X]/(f)$.

(h) Sea $p \in \mathbb{N}$ primo. Para cada $l \in \mathbb{N}$, sea $\zeta_l \in \mathbb{C}$ una raíz primitiva p^l-ésima de la unidad y sea $\mathbb{Q}(\zeta_l)$ el menor subcuerpo de $\mathbb{C}$ que la contiene. Entonces hay un isomorfismo de álgebras

$$\mathbb{Q}G_{p^l} \cong \mathbb{Q} \times \mathbb{Q}(\zeta_1) \times \cdots \times \mathbb{Q}(\zeta_l).$$

(i) Supongamos que n es impar y que $n = p_1^{m_1} \cdots p_r^{m_r}$ es la factorización de n como producto de potencias de primos distintos. Entonces $G_n \cong G_{p_1^{m_1}} \times \cdots \times G_{p_r^{m_r}}$.

Si M es un $\mathbb{Q}G_n$-módulo simple, entonces existen $l_1, \ldots, l_r \in \mathbb{N}$ tales que $l_i \leq m_i$ si $i \in \{1, \ldots, r\}$ y

$$M \cong M_{p_1,m_1,l_1} \boxtimes \cdots \boxtimes M_{p_r,m_r,l_r}.$$

Aquí $M_{p,m,l}$ es el único $\mathbb{Q}G_{p^m}$-módulo simple de dimensión $p^l - p^{l-1}$.

Álgebras de grupo

6.4.19. Muestre que si $k \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, entonces $kS_3 \cong k \times k \times \mathsf{M}_2(k)$.

6.4.20. Encuentre la descomposición de Wedderburn para kD_4 con $k \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ si $D_4 = \langle s, t : s^2 = t^4 = 1, sts = t^{-1} \rangle$.

6.4.21. Sea $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ el grupo de los cuaterniones unitarios. Muestre que

$$\mathbb{Q}Q \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{H}_{\mathbb{Q}},$$
$$\mathbb{R}Q \cong \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{H}_{\mathbb{R}},$$

y

$$\mathbb{C}Q \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathsf{M}_2(\mathbb{C}).$$

Aquí $\mathbb{H}_{\mathbb{R}}$ es el anillo de los cuaterniones reales y $\mathbb{H}_{\mathbb{Q}}$ es el análogo definido sobre $\mathbb{Q}$.

Dominios principales

6.4.22. Mostrar que $\mathbb{Z}[\sqrt{10}]$ y $\mathbb{Z}[\sqrt{-10}]$ no son dominios de factorización única. Encontrar ideales no principales en estos anillos.

6.4.23. *(a)* Mostrar que $\mathbb{Z}[\sqrt{d}]$ es euclideano si $d \in \{-2, 2, 3\}$.

(b) Factorizar a $16 + 11\sqrt{2}$ como producto de elementos irreducibles del anillo $\mathbb{Z}[\sqrt{2}]$.

(c) Un número primo $p \in \mathbb{Z}$ es irreducible en $\mathbb{Z}[\sqrt{-2}]$ sii -2 es un cuadrado en $\mathbb{Z}_p$. Dé ejemplos de factorizaciones en $\mathbb{Z}[\sqrt{-2}]$ de números primos de $\mathbb{Z}$.

6.4.24. Sea $p \in \mathbb{N}$ un número primo, $\mathfrak{p} = (p)$ el ideal primo correspondiente y sea $\mathbb{Z}_{\mathfrak{p}}$ la localización de $\mathbb{Z}$ en $\mathfrak{p}$. Describir todos sus ideales. Mostrar que $\mathbb{Z}_{\mathfrak{p}}$ es un dominio de ideales principales con un único ideal maximal y encontrar un conjunto completo de elementos primos no asociados dos a dos.

6.4.25. Sea A un dominio de ideales principales y sea M un A-módulo finitamente generado. Mostrar que

(a) M es de torsión sii $\hom_A(M, A) = 0$; y

(b) M es indescomponible sii o bien $M \cong A$ o bien existe $p \in A$ irreducible y $n \in \mathbb{N}$ tal es que $M \cong A/(p^n)$.

¿Qué puede decir cuando M no es finitamente generado?

6.4.26. Sea $p \in \mathbb{N}$ un número primo. Encuentre todos los grupos abelianos de orden p^2, p^3, p^4 y p^5.

6.4.27. Sea G un grupo abeliano finito y sea $p \in \mathbb{N}$ un número primo tal que $p \mid |G|$. Entonces el número de elementos de orden p de G es coprimo con p.

6.4.28. *(a)* Para los siguientes grupos abelianos, dar la factorización del teorema de estructura:

(a) $\mathbb{Z}_4 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_9$;

(b) $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_{14}$;

(c) $\mathbb{Z}_2 \oplus \mathbb{Z} \oplus \mathbb{Z}_{49} \oplus \mathbb{Z}$;

(d) $\mathbb{Z}_{12} \oplus \mathbb{Z}_{21} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}_{20} \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_7$.

(b) Determinar la factorización canónica de un grupo abeliano G de orden 36 que tiene exactamente 2 elementos de orden 3 y que no tiene elementos de orden 4.

(c) Determinar la factorización canónica de un grupo abeliano G de orden 225 que tiene por lo menos 40 elementos de orden 15 y tal que todo subgrupo de orden 9 es isomorfo a $\mathbb{Z}_3 \oplus \mathbb{Z}_3$.

6.4.29. Sea $G \subset \mathbb{Z}^n$ un subgrupo.

(a) $[\mathbb{Z}^n : G]$ es finito sii G tiene rango n.

(b) Si G tiene rango n y $\{g_1, \ldots, d_n\}$ es una base de G, sea $M \in \mathsf{M}_n(\mathbb{Z})$ la matriz que tiene a los g_i como columnas. Mostrar que $[\mathbb{Z}^n : G] = |\det M|$.

6.4.30. Sea k un cuerpo y sea V un espacio vectorial sobre k tal que $\dim_k(V) < \infty$. Sea $\phi : V \to V$ una transformación lineal.

(a) Mostrar que las siguientes afirmaciones son equivalentes:

- Existe una base en la que la matriz de ϕ se parte en dos bloques .
- (V, ϕ) se descompone en suma directa de dos $k[x]$-submódulos.

(b) Mostrar que las siguientes afirmaciones son equivalentes:

- No existe ninguna base en la que ϕ se escriba en bloques.
- (V, ϕ) es un $k[x]$-módulo indescomponible, luego cíclico.

6.4.31. *Teorema chino del resto.*. Sea A un anillo conmutativo y sean $a_1, \ldots, a_n \in A$. Sea $b_i = a_1 a_2 \ldots \widehat{a_i} \ldots a_n$. Supongamos que $1 = \sum_{i=1}^n t_i b_i$ para ciertos elementos t_i. Sean $I = bA$ y $I_i = a_i A$. Entonces $I \subseteq I_i$, así que A/I_i es un A/I-módulo para todo $i = 1, \ldots, n$. Demuestre que $A/I \cong \oplus A/I_i$.

6.4.32. Sea (V, ϕ) un $k[x]$-módulo indescomponible, luego cíclico, $(V, \phi) \cong k[x]/\langle p \rangle$. Si escribimos a $p = q_1^{\alpha_1} \dots q_s^{\alpha_s}$ con los q_i irreducibles y sin repeticiones, considerar $a_i = q_i^{\alpha_i}$. Ver que se está en las condiciones del teorema chino del resto.(Sugerencia: usar argumentos de divisibilidad) Concluir a partir del teorema chino del resto que existe una base de V en la que ϕ se escribe en n bloques, cada uno de ellos correspondiene a un $k[x]$ submódulo isomorfo a $k[x]/\langle a_i \rangle$.

6.4.33. Sea $T : \mathbb{Q}^3 \to \mathbb{Q}^3$ la transformación lineal definida por la matriz $\begin{pmatrix} -1 & -2 & 6 \\ -1 & 0 & 3 \\ -1 & -1 & 4 \end{pmatrix}$ considerar a $\mathbb{Q}^3$ como $\mathbb{Q}[x]$-módulo a través de T, hallar su descomposición en sumandos directos indescomponibles.

6.4.34. Listar las clases de isomorfismo de los grupos abelianos de orden 16, 18, 20, 189.

6.4.35. Caracterizar a todos los grupos abelianos G en cada una de las siguientes situaciones:

- todo elemento no nulo tiene orden primo.
- todo subgrupo propio es de orden primo.
- $|G| = 36$, G no tiene elementos de orden 4 y G tiene dos elementos de orden 3.

6.4.36. Sea k un cuerpo finito, considerar el grupo abeliano $G = (k - 0, .)$, es decir, el grupo multiplicativo de los elementos no nulos de k. Demostrar que G es cíclico. Para ello se sugieren los siguientes pasos:

1. ver que el subgrupo aditivo generado por el 1 es un subcuerpo, necesariamente isomorfo a $\mathbb{Z}_p$ para algún número primo p y conlcuir que $|k| = p^n$ para algún n,
2. considerar el grupo abeliano $G = (k - \{0\}, .)$, usar el teorema de estructura y dar todas las posibilidades de G. A través de la traducción de la notación aditiva a la multiplicativa, relacionar la cantidad de ceros que pueden tener en k los polinomios, y los órdenes de los elementos de G.

Formas de Jordan

6.4.37. Hallar todos los $\mathbb{C}[x]$-módulos M tales que $\dim_{\mathbb{C}}(M) \leq 3$. Decir cuáles de ellos son cíclicos, indescomponibles, simples, suma

de simples o suma de indescomponibles.

6.4.38. Hallar todos los $\mathbb{R}[x]$-módulos M tales que $\dim_{\mathbb{R}}(M) \leq 3$. Decir cuáles de ellos son cíclicos, indescomponibles, simples, suma de simples o suma de indescomponibles.

6.4.39. Deducir de la forma normal de Jordan que si $A \in \mathbb{C}^{n\times n}$ entonces $A = D + N$ donde D es diagonalizable, N nilpotente, y $DN = ND$.

Capítulo 7

Producto tensorial

7.1 Existencia y unicidad del producto tensorial

Sea A un anillo y sean M y N un A-módulo a derecha y a isquierda, respectivamente. Si P es un grupo abeliano, diremos que una función $\phi : M \times N \to P$ es *bilineal A-balanceada* si

- ϕ es lineal en la primera variable: para todo $m, m' \in M$, $n \in N$

$$\phi(m + m', n) = \phi(m, n) + \phi(m', n).$$

- ϕ es lineal en la segunda variable: para todo $m \in M$, $n, n' \in N$,

$$\phi(m, n + n') = \phi(m, n) + \phi(m, n').$$

- ϕ es A-balanceada: para todo $a \in A$, $m \in M$ y $n \in N$,

$$\phi(ma, n) = \phi(m, an).$$

Escribimos $\mathrm{Bil}_A(M, N; P)$ al conjunto de todas las aplicaciones bilineales A-balanceadas $M \times N \to P$.

Ejemplos.
1. Si $M = N = P = A$, el producto $\phi : (a, b) \in A \times A \mapsto ab \in A$ es bilineal A-balanceado

2. Si $M = A^{1\times n}$ es el A-módulo de vectores fila y $N = A^{n\times 1}$ es el A-módulo de vectores columna, es bilineal A-balanceada la aplica-

ción $\phi : A^{1\times n} \times A^{n\times 1} \to A$ tal que

$$\phi((a_1, \ldots, a_n), (b_1, \ldots, b_n)) = \sum_{i=1}^{n} a_i b_i.$$

3. Si $X \subset \mathbb{R}^N$ es un subconjunto compacto y $C(X)$ es es anillo de funciones continuas sobre X, la aplicación $\phi : C(X) \times C(X) \to C(X)$ dada por

$$\phi(f, g) = \int_X fg$$

es bilineal y $C(X)$-balanceada.

4. Si N es un A-módulo a izquierda y $M = N^* = \hom_A(N, A)$, $\phi : (f, n) \in N^* \times N \mapsto f(m) \in A$.

5. Como subejemplo del anterior, sea k un anillo cualquiera y sean $N = k[X]$ y $M = k^{\mathbb{N}_0}$. Entonces la aplicación $\phi : M \times N \to k$, dada por $\phi((a_n)_{n\in\mathbb{N}_0}, p) = \sum_{i=1}^{gr(p)} a_i\lambda_i$ si $p = \sum_{i=0}^{\deg(p)} \lambda_i x^i$, es bilineal y A-balanceada.

El objetivo de construir el producto tensorial $M \otimes_A N$ es encontrar un objeto de tipo universal que sea equivalente tener una función $\phi : M \times N \to P$ bilineal A-balanceada que una función lineal $\widetilde{\phi} : M \otimes_A N \to P$, es decir, se busca un grupo abeliano $M \otimes_A N$ tal que

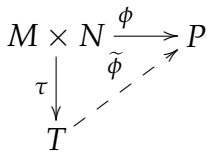
$$\mathrm{Bil}_A(M \times N, P) \cong \mathrm{Hom}_{\mathbb{Z}}(M \otimes_A N, P)$$

de manera natural. Nos proponemos entonces mostrar que tal objeto existe y que es único salvo isomorfismos de grupos abelianos.

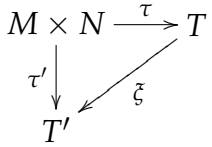
Proposición 7.1.1. *Sea A un anillo. Sea M un A-módulo a derecha y N un A-módulo a izquierda. Entonces existe un grupo abeliano T y una función $\tau : M \times N \to T$ con las siguientes propiedades:*

(a) τ es bilineal y A-balanceada.
(b) Si P es un grupo abeliano cualquiera y $\phi : M \times N \to P$ es una función bilineal A-balanceada, entonces existe un único morfismo de grupos $\widetilde{\phi} : T \to P$ tal que $\phi = \widetilde{\phi} \circ \tau$, es decir, se completa el

siguiente diagrama en forma conmutativa:



(c) *Si* (T', τ') *es un par con la misma propiedad, entonces existe un único isomorfismo* $\xi : T \to T'$ *de grupos abelianos tal que conmuta*



Demostración. Existencia. Construimos el par (T, τ) de la siguiente manera. Sea $F = \mathbb{Z}^{(M\times N)}$ el $\mathbb{Z}$-módulo libre con base el conjunto $M \times N$ y sea K el subgrupo generado por los elementos de la forma

$$(m + m', n) - (m, n) - (m', n),$$
$$(m, n + n') - (m, n) - (m, n')$$

y

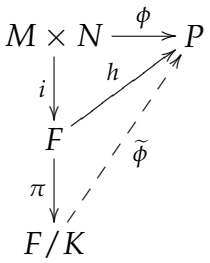
$$(ma, n) - (m, an)$$

con $m, m' \in M$, $n, n' \in N$ y $a \in A$. Notemos que estamos haciendo un abuso de notación, identificando a un par (m, n) con la función de $M \times N \to \mathbb{Z}$ que vale 1 en el par (m, n) y 0 en el resto del dominio.

Definimos ahora $T = F/K$ y denotamos $m \otimes n$ a la clase de (m, n) en T. Definimos además $\tau : M \times N \to T$ poniendo $\tau(m, n) = m \otimes n$ para cada $(m, n) \in M \times N$. Es inmediato, a partir de cómo se definió K, que τ es bilineal y A-balanceada. Veamos que τ satisface además las otras propiedades.

Sea P un grupo abeliano y sea $\phi : M \times N \to P$ una función bilineal A-balanceada. Como F es libre con base $M \times N$, existe un único morfismo de $\mathbb{Z}$-módulos $h : F \to P$ tal que el siguiente diagrama de

líneas llenas conmuta:

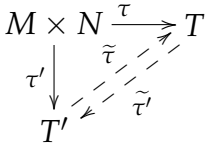


Como ϕ es bilineal y balanceada, ϕ se anula en K y por lo tanto induce una flecha $\widetilde{\phi}$ definida sobre el cociente, que es tal que

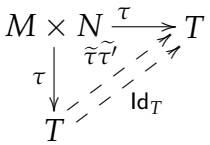
$$\phi = \widetilde{\phi} \circ \pi \circ i = \widetilde{\phi} \circ \tau.$$

Notemos que $\widetilde{\phi}$ queda unívocamente determinada.

Unicidad. Sea (T', τ') un objeto con las mismas propiedades de (T, τ) y consideremos el siguiente diagrama de flechas llenas:



Como (T, τ) tiene la propiedad demostrada anteriormente, existe un único morfismo de grupos $\widetilde{\tau'} : T \to T'$ tal que $\widetilde{\tau'}\tau = \tau'$. Análogamente, existe un único morfismo de grupos $\widetilde{\tau} : T' \to T$ tal que $\widetilde{\tau}\tau' = \tau$. Luego se tiene el siguiente diagrama conmutativo



Por unicidad, resulta entonces que $\widetilde{\tau}\widetilde{\tau'} = \mathsf{Id}_T$. De la misma forma se demuestra que $\widetilde{\tau'}\widetilde{\tau} = \mathsf{Id}_{T'}$. □

Definición 7.1.2. El grupo abeliano T construido en la prueba de esta proposición es el *producto tensorial* sobre A de M con N y se nota $M \otimes_A N$.

Observamos que $M \otimes_A N$ es un grupo abeliano y que $\{m \otimes n : (m,n) \in M \times N\}$ es un conjunto de generadores para $M \otimes_A N$ que satisfacen las siguientes relaciones:

$$(m+m') \otimes n = m \otimes n + m' \otimes n,$$
$$m \otimes (n+n') = m \otimes n + m \otimes n',$$
$$ma \otimes n = m \otimes an.$$

Notemos, además, que no todo elemento de $M \otimes_A N$ es necesariamente de la forma $m \otimes n$ para algún $m \in M$ y $n \in N$ sino que, en general, un una combinación lineal finita de ellos con coeficientes en $\mathbb{Z}$. Los elementos de $M \otimes_A N$ de la forma $m \otimes n$ son los *tensores elementales*.

Finalmente, es importante tener en cuenta que la escritura de un elemento de $M \otimes_A N$ en términos de tensores elementales no es necesariamente única; por ejemplo $x' \otimes y + x \otimes y = (x+x') \otimes y$.

Observación. Para todo $x \in M$, $x \otimes 0 = 0$. De la misma forma, $0 \otimes y = 0$ para todo $y \in N$. Veremos incluso que puede suceder que $x \otimes y = 0$ sin que ni x ni y sean cero. Así, puede ser que $M \otimes_A N$ sea el grupo trivial cero sin que M ni N lo sean: por ejemplo, si $M = \mathbb{Z}_n$ y $N = \mathbb{Q}/\mathbb{Z}$, entonces $M \otimes_{\mathbb{Z}} N = 0$, como veremos más adelante.

Otro ejemplo se obtiene tomando un anillo A en el que existe un elemento $x \in A$ con $x^2 = 0$ sin que x sea cero: en ese caso, si $M = N = A$, es claro que $x \otimes x = 1x \otimes x = 1 \otimes x^2 = 1 \otimes 0 = 0$ en $M \otimes_A N$.

Ejemplos.

1. Es $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}_n$, vía la aplicación $\overline{x} \otimes y \mapsto \overline{xy}$, que tiene inversa $\overline{x} \mapsto \overline{x} \otimes 1$. Notemos que la buena definición de esta aplicación se sigue de la propiedad universal del producto tensorial aplicada a la función bilineal $\mathbb{Z}$-balanceada $(\overline{x}, y) \in \mathbb{Z}_n \times \mathbb{Z} \to \overline{xy} \in \mathbb{Z}_n$.

2. $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Q} = 0$, porque $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Q}$ está generado por elementos de la forma $\overline{x} \otimes \frac{a}{b}$ con $x, a, b \in \mathbb{Z}$, $b \neq 0$, pero

$$\overline{x} \otimes \frac{a}{b} = \overline{x} \otimes n\frac{a}{nb} = \overline{x}\, n \otimes \frac{a}{nb} = 0 \otimes \frac{a}{nb} = 0.$$

3. Con esencialmente la misma demostración que el ejemplo 1, se puede ver que $M \otimes_A A \cong M$, como grupos abelianos, vía la aplicación que proviene de $(m,a) \in M \times A \mapsto ma \in M$. La aplicación

inversa es $m \in M \mapsto m \otimes 1 \in M \otimes_A A$. Observemos que se rata de un isomorfismo de A-módulos a derecha.

4. $k[X] \otimes_k k[Y] \cong k[X, Y]$, mediante la aplicación

$$p(x) \otimes q(y) \in k[X] \otimes_k k[Y] \mapsto p(x)q(y) \in k[X, Y].$$

Dejamos como ejercicio calcular la inversa de esta aplicación.

Notar que en este ejemplo se ve claramente que no todo elemento del producto tensorial es un tensor elemental: en caso contrario, todo polinomio en dos variables sería un producto de dos polinomios, uno que depende de X y otro que depende de y. Por otro lado, sí es cierto que todo polinomio es una suma de polinomios a "variables separadas".

5. El ejemplo 2 puede generalizarse de la siguiente manera: si M es un A-módulo de torsión y N es un A-módulo divisible, entonces $M \otimes_A N = 0$. Así, es $\mathbb{Z}_{p^\infty} \otimes_{\mathbb{Z}} \mathbb{Z}_{p^\infty} = 0$.

6. Si $m, n \in \mathbb{N}$, $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m = \mathbb{Z}_{(m,n)}$, si (m, n) denota el máximo común divisor. En particular, si $(m, n) = 1$, es $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m = 0$.

Observación. Dados dos A-módulos M_A y ${}_AN$ y A-submódulos $M' \subseteq M$ y $N' \subseteq N$, podemos considerar los grupos abelianos $M \otimes_A N$ y $M' \otimes_A N'$. Es fácil ver que hay un morfismo natural de grupos abelianos $M' \otimes_A N' \to M \otimes_A N$ inducido por las inclusiones $M' \hookrightarrow M$ y $N' \hookrightarrow N$, pero este morfismo no siempre es inyectivo.

Ejemplo. Sean $A = \mathbb{Z}$, $N' = M' = \mathbb{Z}_2$, $N = M = \mathbb{Q}/\mathbb{Z}$, viendo $\mathbb{Z}_2$ como subgrupo de $\mathbb{Q}/\mathbb{Z}$ consideramod la inyección $\overline{1} \mapsto \overline{\frac{1}{2}}$ como una inclusión. Sabemos que $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_2 \cong \mathbb{Z}_2$ y, por otro lado, el grupo $\mathbb{Q}/\mathbb{Z}$ es divisible y de torsión simultáneamente, de manera que $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$. Luego ninguna morfismo de grupos $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_2 \to \mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}$ puede ser inyectiva.

Si A es un anillo, consideremos el anillo A^{op} y notemos $*$ a su producto — recordemos que sus elementos son los mismos que los de A, con operación suma también igual a la de A pero con producto tal que por $a * b = ba$.

Se puede verificar sin dificultad (¡hacerlo!) que A^{op} es un anillo (con el mismo 1). Es claro, además, que si A es conmutativo, entonces $A = A^{\mathrm{op}}$. Si M es un A-módulo a derecha, entonces M puede

verse como un A^{op}-módulo a izquierda si definimos la acción mediante $a \cdot m = ma$.

Proposición 7.1.3. *Si M es un A-módulo a derecha y N es un A-módulo a izquierda, entonces, con respecto a las estructuras de A^{op}-módulos recién descritas, la aplicación*

$$\begin{aligned} M \otimes_A N &\cong N \otimes_{A^{\mathrm{op}}} M \\ m \otimes n &\mapsto n \otimes m \end{aligned}$$

es un isomorfismo de grupos abelianos.

Demostración. Es facil ver que la función $f : M \times N \to N \otimes_{A^{\mathrm{op}}} M$ tal que $f(m,n) = n \otimes m$ es bilineal y A-balanceada; de la misma forma, la función $g : N \times M \to M \otimes_A N$ tal que $g(n,m) = m \otimes n$ es bilineal y A^{op}-balanceada. Una vez hecha esta verificación, es claro que f y g inducen isomorfismos, uno el inverso del otro. □

Ejemplos.
1. Sea G un grupo y M un G-módulo a izquierda. Consideremos a $\mathbb{Z}$ como G-módulo a derecha trivial, de manera que $n \cdot g = n$ para todo $n \in \mathbb{Z}$ y $g \in G$. Entonces

$$\mathbb{Z} \otimes_{\mathbb{Z}[G]} M \cong \frac{M}{\langle m - g(m) : m \in M, g \in G \rangle}.$$

2. Sean V y W dos k-espacios vectoriales. La función

$$\begin{aligned} V^* \times W &\to \mathrm{Hom}_k(V,W) \\ (\phi, w) &\mapsto \phi(-)w, \end{aligned}$$

donde $\phi(-)w$ denota la aplicación $v \in V \mapsto \phi(v)w \in W$, es bilineal y k-balanceada y por lo tanto induce un morfismo de grupos abelianos $F : V^* \otimes_k W \to \mathrm{Hom}_k(V,W)$. La imagen de $\phi \otimes w$ es $\phi(-)w$, una transformación lineal cuya imagen tiene dimensión 1 ($\{w\}$ es una base de la imagen). Esto nos dice dos cosas: en primer lugar, que la imagen de F consiste en las transformaciones lineales cuya imagen es un subespacio de W de dimensión finita y, por lo tanto, si V y W tienen dimensión infinita entonces F no puede ser suryectiva. Por otro lado, vemos nuevamente que no todo elemento de $V^* \otimes_k W$ es un tensor elemental, pues es claro que no toda transformación lineal de V en W tiene imagen de dimensión 1.

En general, dados A-módulos M_A y ${}_AN$, el grupo abeliano $M \otimes_A N$ no tiene otra estructura que la de un grupo abeliano. En ciertos casos, sinembargo, este objeto posee más estructura.

En el ejemplo precedente, vimos que $V^* \otimes_k W$ es un k-espacio vectorial. Como segundo ejemplo, vimos que $M \otimes_A A \cong M$ y $A \otimes_A N \cong N$ como grupos abelianos y ambos miembros derechos en estos isomorfismos son A-módulos.

Proposición 7.1.4. *Sean A, B, C tres anillos y ${}_AM_B$ y ${}_BN_C$ dos bimódulos. Entonces $M \otimes_B N$ es naturalmente un A-C-bimódulo.*

Demostración. La estructura de A-C-bimódulo queda determinada por la fórmula

$$a \cdot (m \otimes n) \cdot c = (am) \otimes (nc),$$

extendiendo por $\mathbb{Z}$-linealidad a $M \otimes_B N$. Es claro que esto está bien definido porque, una vez fijados $a \in A$ y $c \in C$, la aplicación $(m, n) \in M \times N \to (am) \otimes (nc) \in M \otimes_B N$ es bilineal B-balanceada. Puede verse sin dificultad que la función

$$\begin{aligned} A \times M \otimes_B N \times C &\to M \otimes_B N \\ (a, m \otimes n, c) &\mapsto (am) \otimes (nc) \end{aligned}$$

da a $M \otimes_A N$ una estructura de A-C-bimódulo. □

Por otro lado, si $f : M \to M'$ es un morfismo de A-módulos derechos y $g : N \to N'$ un morfismo de A-módulos izquierdos, la aplicación

$$\begin{aligned} M \times N &\to M' \otimes_A N' \\ (m, n) &\mapsto f(m) \otimes g(n) \end{aligned}$$

es bilineal y A-balanceada, así que determina un único morfismo de grupos abelianos $M \otimes_A N \to M' \otimes_A N'$, que notamos $f \otimes g$, caracterizado por la identidad

$$(f \otimes g)(m \otimes n) = f(m) \otimes g(n).$$

Ejemplos.
1. Si M es un A-módulo a derecha, entonces $M \otimes_A A \cong M$ en tanto $\mathbb{Z}$-A-bimódulos. De la misma forma $A \otimes_A N \cong N$ como A-$\mathbb{Z}$-bimódulos cuando N es un A-módulo a izquierda.

2. Si M es un A-módulo a derecha y N un A módulo a izquierda y consideramos a M como un $\mathcal{Z}(A)$-A-bimódulo y a N como un A-$\mathcal{Z}(A)$-bimódulo, entonces $M \otimes_A N$ es un $\mathcal{Z}(A)$-bimódulo y el isomorfismo $M \otimes_A N \cong N \otimes_{A^{\mathrm{op}}} M$ es un isomorfismo de $\mathcal{Z}(A)$-bimódulos. De la misma forma, $M \otimes_{\mathcal{Z}(A)} N \cong N \otimes_{\mathcal{Z}(A)} M$ como $\mathcal{Z}(A)$-bimódulos.

3. El morfismo de grupos $F : V^* \otimes_k W \to \mathrm{Hom}_k(V, W)$ descripto en el ejemplo anterior a la proposición es una transformación k-lineal.

4. Dado un anillo A cualquiera y un par de números naturales r, s, consideremos el conjunto $\mathsf{M}_{r\times s}(A) = A^{r\times s}$ con la suma usual de matrices.

La multiplicación de matrices hace de este grupo abeliano un $\mathsf{M}_r(A)$-módulo a izquierda y un $\mathsf{M}_s(A)$-módulo a derecha. En particular, $A^{n\times 1}$ es un $\mathsf{M}_n(A)$-A-bimódulo y $A^{1\times n}$ es un A-$\mathsf{M}_n(A)$-bimódulo, y se tienen los siguientes isomorfismos:

- $A^{n\times 1} \otimes_A A^{1\times n} \cong A^{n\times n}$ como $\mathsf{M}_n(A)$-$\mathsf{M}_n(A)$-bimódulo.
- $A^{1\times n} \otimes_{\mathsf{M}_n(A)} A^{n\times 1} \cong A$ como A-A-bimódulo.
- En general, $A^{n\times r} \otimes_{\mathsf{M}_r(A)} A^{r\times s} \cong A^{n\times s}$ como $\mathsf{M}_n(A)$-$\mathsf{M}_s(A)$-bimódulo.

5. Si A es un anillo conmutativo, L un A-módulo libre finitamente generado y M es un A-módulo cualquiera, entonces hay un isomorfismo $L^* \otimes_A M \cong \mathrm{Hom}_A(L, M)$.

7.2 Funtorialidad de $\otimes$

Dados anillos A, B y C y un bimódulo ${}_AM_B$, se pueden definir dos funtores asociados a M:

$$\begin{aligned}(-) \otimes_A M : {}_C\mathrm{Mod}_A &\to {}_C\mathrm{Mod}_B\\ X &\mapsto X \otimes_A M\\ f &\mapsto f \otimes \mathsf{Id}_M\end{aligned}$$

y

$$\begin{aligned} M \otimes_B (-) : {}_B\mathrm{Mod}_C &\to {}_A\mathrm{Mod}_C \\ Z &\mapsto M \otimes_B Z \\ g &\mapsto \mathsf{Id}_M \otimes g \end{aligned}$$

Ejemplos.
1. Si $M = A$, el funtor $A \otimes_A (-)$ es isomorfo al funtor identidad, es decir, para todo A-módulo X, $A \otimes_A X \cong X$ como A-módulo a izquierda. Cuando X es un A-B-bimódulo, el isomorfismo precedente es también isomorfismo de A-B-bimódulos.

2. Si A es un anillo conmutativo y S es un subconjunto multiplicativo de A, entonces $A_S \otimes -$ es isomorfo al funtor localización, es decir, para todo A-módulo M, hay un isomorfismo de A_S-módulos

$$\begin{aligned} A_S \otimes_A M &\cong M_S \\ \frac{a}{s} \otimes m &\mapsto \frac{am}{s} \end{aligned}$$

con inverso $\frac{am}{s} \mapsto \frac{1}{s} \otimes am$.

3. Si V es un $\mathbb{R}$-espacio vectorial, podemos considerar su complexificación: $V \oplus i\,V$, que tiene una estructura de $\mathbb{C}$-espacio vectorial para la que si $a + bi \in \mathbb{C}$ y $v + iw \in V \oplus i\,V$,

$$(a + bi)(v + iw) = av - bw + i(bv + aw).$$

Por otro lado, $\mathbb{C}$ es un $\mathbb{C}$-$\mathbb{R}$-bimódulo y está entonces definido el funtor $\mathbb{C} \otimes_{\mathbb{R}} (-)$, que es isomorfo a la complexificación:

$$\begin{aligned} \mathbb{C} \otimes_{\mathbb{R}} V &\cong V \oplus i\,V \\ (a + bi) \otimes v &\mapsto av + ibv \end{aligned}$$

Más generalmente, todo morfismo de anillos $f : A \to B$ provee a B de una estructura de A-módulo, tanto a izquierda como a derecha, definiendo por ejemplo la acción a izquierda de manera que

$$a \cdot b = f(a)b.$$

Esto nos permite considerar los funtores $B \otimes_A (-) : {}_A\mathrm{Mod} \to {}_B\mathrm{Mod}$ y $(-) \otimes_A B : \mathrm{Mod}_A \to \mathrm{Mod}_B$. Estos funtores se denominan functores de *extensión de escalares*. Si M es un A-módulo, $B \otimes_A M$ se llama el *B-módulo extendido* o *inducido*.

Proposición 7.2.1. *Si M es un A-módulo a derecha, el funtor $M \otimes_A (-)$ preserva epimorfismos.*

Demostración. Sea $f : N \to N'$ un epimorfismo de A-módulos a izquierda. Entonces $\mathsf{Id} \otimes f : M \otimes_A N \to M \otimes_A N'$ es un epimorfismo, pues todos los tensores elementales de $M \otimes_A N'$ están en la imagen $\mathsf{Id} \otimes f$ y $M \otimes_A N'$ está generado por tensores elementales. □

Observación. El funtor $M \otimes_A (-)$ no siempre preserva monomorfismos. Para ver ésto exhibimos un contraejemplo: Sea $f : \mathbb{Z}_2 \to \mathbb{Z}_4$ definido por $f(\overline{1}) = \overline{2}$ y consideremos el funtor $\mathbb{Z}_2 \otimes_{\mathbb{Z}} (-)$. Tenemos las siguientes identificaciones:

$$\begin{array}{ccc} \mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_2 & \xrightarrow{\mathsf{Id}\otimes f} & \mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_4 \\ \| & & \| \\ \mathbb{Z}_2 & \xrightarrow{\quad g \quad} & \mathbb{Z}_2 \end{array}$$

Para calcular g, seguimos al elemento $\overline{1}$ bajo estas identificaciones. Llamemos $\mu : \mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_4 \to \mathbb{Z}_2$ al isomorfismo $\overline{a} \otimes \overline{b} \mapsto \overline{ab}$. Entonces

$$g(\overline{1}) = \mu((id \otimes f)(\overline{1} \otimes \overline{1})) = \mu(\overline{1} \otimes \overline{2}) = \overline{2} = 0.$$

Esto nos dice que $\mathsf{Id} \otimes f = 0$, que no es un monomorfismo.

Sin embargo, se tiene la siguiente propiedad de exactitud a derecha:

Proposición 7.2.2. *Sea*

$$N_1 \xrightarrow{f} N_2 \xrightarrow{g} N_3 \longrightarrow 0$$

una sucesión exacta de A-módulos a izquierda. Para cualquier A-módulo a derecha M, la sucesión de grupos abelianos

$$M \otimes_A N_1 \xrightarrow{\mathsf{Id}\otimes f} M \otimes_A N_2 \xrightarrow{\mathsf{Id}\otimes g} M \otimes_A N_3 \longrightarrow 0$$

es exacta.

Demostración. Ya vimos que $\mathsf{Id} \otimes g$ es un epimorfismo y es claro que $(\mathsf{Id} \otimes g) \circ (\mathsf{Id} \otimes f) = 0$, pues

$$(\mathsf{Id} \otimes g) \circ (\mathsf{Id} \otimes f)(m \otimes n) = m \otimes g(f(n)) = m \otimes 0 = 0.$$

Luego $\operatorname{Im}(\mathsf{Id} \otimes f) \subseteq \operatorname{Ker}(\mathsf{Id} \otimes g)$. Solo nos falta mostrar que

$$\operatorname{Ker}(\mathsf{Id} \otimes g) \subseteq \operatorname{Im}(\mathsf{Id} \otimes f).$$

Sea $\sum_i m_i \otimes n_i \in M \otimes_A N_2$ tal que $\sum_i m_i \otimes g(n_i) = 0$. Consideremos el grupo abeliano

$$M \otimes_A N_2 / \operatorname{Im}(\mathsf{Id} \otimes f) = M \otimes_A N_2 / \langle m \otimes f(n) : m \in M, n \in N \rangle$$

y definamos $\widetilde{\phi} : M \times N_3 \to M \otimes_A N_2 / \operatorname{Im}(\mathsf{Id} \otimes f)$ poniendo

$$\widetilde{\phi}(m, x) = \overline{m \otimes x'}$$

si $x' \in N_2$ es un elemento tal que $g(x') = x$ (recordar que g es epimorfismo). La aplicación $\widetilde{\phi}$ está bien definida: si x'' es otro elemento de N_2 tal que $g(x'') = x$, entonces $x' - x'' \in \operatorname{Ker}(g) = \operatorname{Im}(f)$, y esto nos dice que existe $y \in N_1$ tal que $x' - x'' = f(y)$. Luego

$$\overline{m \otimes x''} = \overline{m \otimes x'' + m \otimes f(y)} = \overline{m \otimes x'' + m \otimes (x' - x'')} = \overline{m \otimes x'}.$$

Ahora que sabemos que está bien definida, es claro que $\widetilde{\phi}$ es bilineal y A-balanceada, así que define un morfismo de grupos abelianos

$$\phi : M \otimes_A N_3 \to \frac{M \otimes_A N_2}{\operatorname{Im}(\mathsf{Id} \otimes f)}$$

que, por construcción, es tal que $\phi(m \otimes g(x')) = \overline{m \otimes x'}$, es decir, tal que $\phi \circ (\overline{\mathsf{Id} \otimes g})$ es la identidad de $M \otimes_A N_2 / \operatorname{Im}(\mathsf{Id} \otimes f)$.

Si ahora $w \in \operatorname{Ker}(\mathsf{Id} \otimes g)$, entonces $w \in \operatorname{Im}(\mathsf{Id} \otimes f)$ si y sólo si $\overline{w} = 0$ en $M \otimes_A N_2 / \operatorname{Im}(\mathsf{Id} \otimes f)$. Pero entonces tenemos que

$$\overline{w} = \phi(\overline{\mathsf{Id} \otimes g}(\overline{w})) = \phi(\overline{(\mathsf{Id} \otimes g)(w)}) = \phi(0) = 0,$$

como queríamos ver. □

La proposición anterior puede generalizarse de la siguiente manera:

Proposición 7.2.3. *Dadas una sucesión exacta de A-módulos a derecha*

$$N_1 \xrightarrow{f} N_2 \xrightarrow{g} N_3 \longrightarrow 0$$

y una sucesión exacta de A-módulos a izquierda

$$M_1 \xrightarrow{h} M_2 \xrightarrow{k} M_3 \longrightarrow 0$$

la sucesión de grupos abelianos

$$\mathrm{Im}(f) \otimes_A M_2 + N_2 \otimes_A \mathrm{Im}(h) \xrightarrow{\gamma} N_2 \otimes_A M_2 \xrightarrow{g\otimes k} N_3 \otimes_A M_3 \longrightarrow 0$$

es exacta.

Demostración. Esto puede probarse como la proposición anterior. Dejamos los detalles como ejercicio. En particular, queda como ejercicio ver la definición del morfismo γ del enunciado. □

Observación. Supongamos que la sucesión de A-módulos a izquierda

$$N_1 \xrightarrow{f} N_2 \xrightarrow{g} N_3 \longrightarrow 0$$

es tal que, para todo A-módulo a derecha M, la sucesión correspondiente

$$M \otimes_A N_1 \longrightarrow M \otimes_A N_2 \longrightarrow M \otimes_A N_3 \longrightarrow 0$$

es exacta. En particular, tomando $M = A$, la sucesión de grupos abelianos

$$A \otimes_A N_1 \longrightarrow A \otimes_A N_2 \longrightarrow A \otimes_A N_3 \longrightarrow 0$$

es exacta. Como sabemos que $A \otimes_A N_i \cong N_i$ como A-módulos a izquierda y que bajo esta identificación $\mathrm{Id} \otimes f$ se corresponde con f (y análogamente para g), vemos que la sucesión original es exacta.

Hay otra manera de demostrar estas propiedades de exactitud, aprovechando la relación de *adjunción* entre el funtor de producto tensorial y el Hom, de la que nos ocuparemos en la próxima sección. Esta propiedad tiene además la ventaja de que con ella podemos ver rápidamente la relación del funtor $\otimes$ con otras operaciones como la suma directa.

7.3 Adjunción entre $\otimes$ y *Hom*

Teorema 7.3.1. *Sean A, B y C tres anillos y ${}_AX_B$, ${}_BY_C$ y ${}_AZ_C$ tres bimódulos. Hay un isomorfismo de C-módulos a derecha*

$$\mathrm{Hom}_A(X \otimes_B Y, Z) \cong \mathrm{Hom}_B(Y, \mathrm{Hom}_A(X, Z))$$

y un isomorfismo de A-módulos a izquierda

$$\mathrm{Hom}_C(X \otimes_B Y, Z) \cong \mathrm{Hom}_B(X, \mathrm{Hom}_C(Y, Z))$$

Demostración. la demostración del teorema es sencilla, pero larga, con una cantidad considerable de verificaciones de carácter elemental. Daremos entonces las definiciones de los morfismos relevantes en el primer isomorfismo y dejaremos tanto las verificaciones como las definiciones del segundo isomorfismo como ejercicio.

Sea $g : X \otimes_B Y \to Z$ un morfismo de A-módulos. Para cada $y \in Y$, la aplicación $x \mapsto g(x \otimes y)$ es un morfismo de A-módulos de X en Z así que poemos definir una una aplicación

$$\begin{aligned} \phi : \mathrm{Hom}_A(X \otimes_B Y, Z) &\to \mathrm{Hom}_B(Y, \mathrm{Hom}_A(X, Z)) \\ g &\mapsto (x \mapsto g(x \otimes -)) \end{aligned}$$

donde, $g(x \otimes -))$ indica el morfismo $y \mapsto g(x \otimes y)$.

Recíprocamente, dado un morfismo $f : Y \to \mathrm{Hom}_A(X, Z)$ de B-módulos, es claro que el elemento $f(y)(x) \in Z$ depende linealmente tanto de y como de x, así que hay una función bilineal

$$f' : (x, y) \in X \times Y \mapsto f(y)(x) \in Z.$$

Como $f(by)(x) = f(y)(xb)$ si $x \in X$, $y \in Y$ y $b \in B$, la aplicación f' resulta B-balanceada y, por lo tanto, define un único morfismo de grupos $\phi(f) : X \otimes_B Y \to Z$. Dejamos al lector la verificación de que, de esta forma, obtenemos un morfismo de grupos abelianos

$$\begin{aligned} \psi : \mathrm{Hom}_B(Y, \mathrm{Hom}_A(X, Z)) &\to \mathrm{Hom}_A(X \otimes_B Y, Z) \\ f &\mapsto ((x \otimes y) \mapsto f(y)(x)) \end{aligned}$$

Finalmente, hay que mostrar que ϕ y ψ son uno el inverso del otro y que, además, son C-lineales a derecha. □

Ejemplo. Sea A un anillo conmutativo y sea L un A-módulo libre finitamente generado, entonces $L^* \otimes_A M^* \cong \mathrm{Hom}_A(L, M^*)$ y

$$\begin{aligned}\mathrm{Hom}_A(L, M^*) &= \mathrm{Hom}_A(L, \mathrm{Hom}_A(M, A)) \\ &\cong \mathrm{Hom}_A(M \otimes_A L, A) \\ &= (M \otimes_A L)^*.\end{aligned}$$

A partir del teorema de adjunción, es facil obtener una demostración de la asociatividad del producto tensorial:

Corolario 7.3.2. *Sean A, B, C, D cuatro anillos y ${}_AM_B$, ${}_BN_C$, ${}_CP_D$ tres bimódulos. Entonces hay un isomorfismo de A-D-bimódulos*

$$(M \otimes_B N) \otimes_C P \cong M \otimes_B (N \otimes_C P).$$

Demostración. Necesitaremos usar el siguiente hecho, cuya prueba dejamos al lector:

> si X e Y son A-D-bimódulos tales que para todo A-módulo Z, hay un isomorfismo natural
>
> $$\mathrm{Hom}_A(X, Z) \cong \mathrm{Hom}_A(Y, Z) \tag{7.1}$$
>
> de D-módulos a derecha, entonces $X \cong Y$.

Consideremos un A-módulo Z. El teorema de adjunción nos da isomorfismos naturales:

$$\begin{aligned}&\mathrm{Hom}_A((M \otimes_B N) \otimes_C P, Z) \\ &\qquad\cong \mathrm{Hom}_C(P, \mathrm{Hom}_A(M \otimes_B N, Z)) \\ &\qquad\cong \mathrm{Hom}_C(P, \mathrm{Hom}_B(N, \mathrm{Hom}_A(M, Z))) \\ &\qquad\cong \mathrm{Hom}_B(N \otimes_C P, \mathrm{Hom}_A(M, Z)) \\ &\qquad\cong \mathrm{Hom}_A(M \otimes_B (N \otimes_C P), Z)\end{aligned}$$

Esto junto con (7.1) prueba el corolario. □

A continuación, estudiaremos el comportamiento del producto tensorial con respecto a la suma directa.

Proposición 7.3.3. *Sea $\{M_i\}_{i \in I}$ una familia de A-módulos a izquierda y ${}_BX_A$ un B-A-bimódulo. Entonces existe un isomorfismo de B-módulos*

$$X \otimes_A \Big(\bigoplus_{i \in I} M_i \Big) \cong \bigoplus_{i \in I} (X \otimes_A M_i).$$

Demostración. Utilizamos la propiedad universal de la suma directa: $\bigoplus_{i\in I} M_i$ es una suma directa de la familia $\{M_i\}_{i\in I}$ si y sólo si para todo $i \in I$ existen morfismos $j_i : M_i \to \oplus_{r\in I} M_r$ tales que todo morfismo con dominio en $\bigoplus_{i\in I} M_i$ queda definido a partir de sus restricciones a cada M_i, esto es, si la flecha natural

$$\begin{aligned} \mathrm{Hom}_A(\bigoplus_{i\in I} M_i, X) &\cong \prod_{i\in I} \mathrm{Hom}_A(M_i, X) \\ f &\mapsto (f|_{M_i})_{i\in I} \end{aligned}$$

donde $f|_{M_i}$ denota $f \circ j_i : M_i \to X$, es una biyección.

Utilizando ahora la adjunción del producto tensorial, tenemos los siguientes isomorfismos:

$$\begin{aligned} &\mathrm{Hom}_B(X \otimes_A (\oplus_{i\in I} M_i), Z) \\ &\qquad \cong \mathrm{Hom}_A(\bigoplus_{i\in I} M_i, \mathrm{Hom}_B(X, Z)) \\ &\qquad \cong \prod_{i\in I} \mathrm{Hom}_A(M_i, \mathrm{Hom}_B(X, Z)) \\ &\qquad \cong \prod_{i\in I} \mathrm{Hom}_B(X \otimes_A M_i, Z) \end{aligned}$$

Esto dice que la aplicación

$$\mathrm{Hom}_B(X \otimes_A (\bigoplus_{i\in I} M_i), Z) \to \prod_{i\in I} \mathrm{Hom}_B(X \otimes_A M_i, Z)$$

es una biyección, de manera que $X \otimes_A (\oplus_{i\in I} M_i)$ satisface la propiedad universal de la suma directa. □

Un corolario de la relación del producto tensorial con la suma directa es su relación con los módulos libres:

Corolario 7.3.4. *Sean M un A-módulo e I un conjunto. Entonces hay un isomorfismo de A-módulos izquierdos $A^{(I)} \otimes_A M \cong M^{(I)}$. En particular, $A^{(I)} \otimes_A A^{(J)} \cong A^{(I\times J)}$.* □

Sin embargo, el producto tensorial no conmuta en general con productos arbitrarios, es decir, $(\prod_i M_i) \otimes_A N$ es en general distinto a $\prod_i (M_i \otimes_A N)$. Por supuesto, si el producto es finito, es cierto. Exhibimos un contraejemplo para el caso de un conjunto de índices infinito:

Ejemplo. Sea $A = k$ un cuerpo y consideremos los espacios vectoriales $N = k^{(\mathbb{N})}$ y $M = N^* \cong k^{\mathbb{N}}$. Hay un morfismo natural $\Xi : N^* \otimes_k N \to \mathrm{Hom}_k(k^{(\mathbb{N})}, k^{(\mathbb{N})})$ tal que por $\Xi(\phi \otimes v)(w) = \phi(w)v$ siempre que $v, w \in k^{(\mathbb{N})}$ y $\phi \in \left(k^{(\mathbb{N})}\right)^*$.

Claramente Ξ no es un epimorfismo ya que la identidad no está en la imagen que, de hecho, sólo contiene transformaciones lineales con imagen de dimensión finita sobre k. Si el producto tensorial conmutara con productos arbitrarios, debería ser $k^{\mathbb{N}} \otimes k^{(\mathbb{N})} \cong \left(k^{(\mathbb{N})}\right)^{\mathbb{N}}$, es decir, el conjunto de de las funciones de $\mathbb{N}$ en $k^{(\mathbb{N})}$. Como $k^{(\mathbb{N})}$ es libre con base $\mathbb{N}$, tener una función de $\mathbb{N}$ en $k^{(\mathbb{N})}$ es lo mismo que tener un morfismo k-lineal de $k^{(\mathbb{N})}$ en $k^{(\mathbb{N})}$, es decir un endomorfismo. Pero sabemos que no todo endomorfismo de $k^{(\mathbb{N})}$ proviene de $\left(k^{(\mathbb{N})}\right)^* \otimes k^{(\mathbb{N})}$.

7.4 Módulos Playos

Vimos anteriormente que si

$$0 \longrightarrow X \longrightarrow Y \longrightarrow Z \longrightarrow 0$$

es una sucesión exacta de A-módulos a izquierda y M es un A-módulo a derecha, entonces la correspondiente sucesión

$$M \otimes_A X \longrightarrow M \otimes_A Y \longrightarrow M \otimes_A Z \longrightarrow 0$$

es exacta, pero no es posible afirmar en general que el morfismo $M \otimes_A X \to M \otimes_A Y$ sea un monomorfismo. Hay, sin embargo, casos particulares en que esto sucede:

Proposición 7.4.1. *Sea*

$$0 \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow 0$$

una sucesión exacta corta de A-módulos a izquierda.

(a) Si P es un A-módulo a derecha proyectivo, entonces

$$0 \longrightarrow P \otimes_A X \longrightarrow P \otimes_A Y \longrightarrow P \otimes_A Z \longrightarrow 0$$

es exacta.

(b) Si la sucesión exacta se parte y M es un A-módulo a derecha cualquiera, entonces la sucesión

$$0 \longrightarrow P \otimes_A X \longrightarrow P \otimes_A Y \longrightarrow P \otimes_A Z \longrightarrow 0$$

se parte, y en particular es exacta.

Demostración. (a) Si $P = A$, vimos antes que la sucesión quedaba exacta puesto que esencialmente la sucesión tensorizada es la misma.

Si $P = A^{(I)}$ utilizamos el hecho de que el producto tensorial conmuta con la suma directa, y que la suma directa de sucesiones exactas es exacta.

Si P es proyectivo, existe un A-módulo Q tal que $P \oplus Q = L$ con L libre y entonces tenemos un diagrama conmutativo

$$\begin{array}{ccccccccc}
0 & \longrightarrow & L \otimes_A X & \longrightarrow & L \otimes_A Y & \longrightarrow & L \otimes_A Z & \longrightarrow & 0 \\
 & & \| & & \| & & \| & & \\
0 & \rightarrowtail & (P \otimes_A X) \oplus (Q \otimes_A X) & \rightarrowtail & (P \otimes_A Y) \oplus (Q \otimes_A Y) & \rightarrowtail & (P \otimes_A Z) \oplus (Q \otimes_A Z) & \rightarrowtail & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & P \otimes_A X & \xrightarrow{\mathrm{Id}_P \otimes f} & P \otimes_A Y & \xrightarrow{\mathrm{Id}_P \otimes g} & P \otimes_A Z & \longrightarrow & 0
\end{array}$$

Falta sólo ver que $\mathrm{Id}_P \otimes f$ es un monomorfismo, pero $\mathrm{Id}_P \otimes f$ es la restricción a $(P \otimes_A X) \oplus (Q \otimes_A X)$ de $\mathrm{Id}_L \otimes f$, que sabemos que es inyectiva.

Dejamos la parte *(b)* como ejercicio para el lector. □

Ejemplo. Sea A un anillo y $S \subset \mathcal{Z}(A)$ un subconjunto multiplicativamente cerrado. Entonces el funtor $A_S \otimes_A (-)$ es exacto, es decir, preserva monomorfismos. Para demostrar ésto, identificamos el funtor $A_S \otimes_A (-)$ con el funtor de localización $(-)_S$. Consideremos entonces un monomorfismo de A-módulos $f : M \to N$ y queremos ver que $f_S : M_S \to N_S$ es un monomorfismo.

Sea $\frac{m}{s} \in \mathrm{Ker}(f_S)$, de manera que $\frac{f(m)}{s} = 0$ en N_S. Esto significa que existe $t \in S$ tal que $0s = 0 = tf(m)$ en N. Pero como f es lineal, esto nos dice que $f(tm) = 0$, y entonces $tm = 0$ en M ya que $f : M \to N$ es un monomorfismo. Ahora bien, si $tm = 0$ con $t \in S$, $\frac{m}{s} = \frac{tm}{ts} = 0$ en M_S. Vemos así que $\mathrm{Ker}(f_S) = 0$, como queríamos.

Definición 7.4.2. Un A-módulo a derecha M es *playo* si el funtor $M \otimes_A (-)$ es exacto.

La proposición anterior dice que los módulos proyectivos son playos. De la demostración de la proposición también se ve que sumas directas y sumandos directos de playos son playos. El ejemplo de la localización dice también que la clase de módulos de playos puede ser estrictamente más grande que la de los proyectivos. Por ejemplo, si $A = \mathbb{Z}$ y $S = \mathbb{Z} - \{0\}$, tenemos que $A_S = \mathbb{Q}$ es $\mathbb{Z}$-playo, pero no es $\mathbb{Z}$-proyectivo. En general, si A es un dominio íntegro y K es su cuerpo de fracciones, entonces K es A-playo.

Ejemplo. Sea $f : A \to B$ un morfismo de anillos y P un A-módulo a derecha. Si P es A-playo, entonces el módulo inducido $P \otimes_A B$ es B-playo. Esto es cierto pues el funtor $(P \otimes_A B) \otimes_B (-)$ aplicado a un B-módulo a izquierda M es $P \otimes_A B \otimes_B M \cong P \otimes_A M'$, donde M' es igual a M, pero con la estructura de A-módulo dada por el morfismo de anillos f. Luego $(P \otimes_A B) \otimes_B (-)$ es isomorfo a la composición de dos funtores, el primero es la restricción de escalares, que es obviamente exacto pues es la identidad en los morfismos, y el otro es tensorizar sobre A con P, que es exacto por hipótesis.

7.5 Ejercicios

Productos tensoriales

7.5.1. Muestre que $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$.

7.5.2. Sea A un anillo y M_A y ${}_AM$ A-módulos. Muestre que $M \otimes_A N$ es un $\mathrm{End}_A(M)$-$\mathrm{End}_A(N)$-bimódulo.

7.5.3. Sean A y B anillos y M_A, ${}_AN_B$ y ${}_BP$ módulos. Muestre que hay un isomorfismo natural

$$M \otimes_A (N \otimes_B P) \cong (M \otimes_A N) \otimes_B P.$$

7.5.4. Sea A un anillo conmutativo, $\mathfrak{a} \subset A$ un ideal y M un A-módulo. Muestre que hay un isomorfismo natural

$$A/\mathfrak{a} \otimes_A M \cong M/\mathfrak{a}M.$$

7.5.5. Sea A un anillo y sean M_A y ${}_AN$ módulos. Supongamos que $M = \sum_{i\in I} M_i$ es suma de una familia de submódulos $\{M_i\}_{i\in I}$. Si $M_i \otimes_A N = 0$ ara todo $i \in I$, entonces $M \otimes_A N = 0$.

7.5.6. Sea A un anillo y M un A-módulo playo. Si $N \subset M$ es un sumando directo, entonces N es playo.

7.5.7. Si A es un anillo conmutativo y M, N son A-módulos playos, entonces $M \otimes_A N$ es un A-módulo playo.

7.5.8. Sea A un anillo y $S \subset A$ un subconjunto multiplicativamente cerrado.

(a) Si M es un A-módulo izquierdo, entonces hay un isomorfismo $A_S \otimes_A M \cong M_S$.

(b) El A-módulo derecho A_S es playo.

†**7.5.9.** Sea A un anillo y M un A-módulo izquierdo. Entonces M es playo sii para todo ideal $\mathfrak{a} \subset A$ finitamente generado, la aplicación

$$a \otimes m \in \mathfrak{a} \otimes_A M \mapsto am \in \mathfrak{a}M$$

es un isomorfismo.

7.5.10. Sea A un anillo. Las siguientes afirmaciones son equivalentes:

(i) Todo A-módulo a izquierda es playo.

(ii) Todo A-módulo a derecha es playo.

(iii) Para todo $a \in A$, existe $x \in A$ tal que $a = axa$.

(iv) Todo ideal izquierdo principal está generado por un idempotente.

(v) Todo ideal derecho principal está generado por un idempotente.

7.5.11. *Criterio local de platitud.* Sea A un anillo conmutativo y M un A-modulo. Las siguientes afirmaciones son equivalentes:

(i) M es playo;

(ii) para cada $\mathfrak{p} \in \operatorname{Spec} A$, $M_\mathfrak{p}$ es un $A_\mathfrak{p}$-módulo playo;

(iii) para cada ideal maximal $\mathfrak{m} \subset A$, $M_\mathfrak{m}$ es un $A_\mathfrak{m}$-módulo playo.

7.5.12. Sea

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

una sucesión exacta de A-módulos.

(a) Si M y M'' playos entonces M' es playo.

Sugerencia. Este ejercicio no sale de manera obvia y directa. Se sugiere ir en etapas, pidiendo hipótesis adicionales para poder demostrar primero versiones más débiles de lo que se pide y después ver que con eso alcanza.

(b) Dar un ejemplo en el que M' y M sean playos, pero que M'' no lo sea.

Sugerencia. M' y M pueden incluso ser libres).

7.5.13. Sea A un dominio íntegro,

(a) Probar que si M es un A-módulo playo, entonces M es sin torsión.

(b) Encontrar un contraejemplo para la recíproca.

Sugerencia. Considerar $A = k[x, y]$ donde k es un cuerpo, M el ideal de A generado por x e y que es evidentemente sin torsión y ver que M no es playo.

(c) Sea K el cuerpo de fracciones de A, ver que si M es sin torsión y divisible, entonces admite una única estructura de K espacio vectorial compatible con la estructura de A-módulo original; concluir que M es A-playo.

7.5.14. Sean M y N dos A-módulos a izquierda. Ver que si M es A-proyectivo de tipo finito, entonces la aplicación natural $M^* \otimes_A N \to \mathrm{Hom}_A(M, N)$ es un isomorfismo.

Sugerencia. Demostrar que si para un M dado es un isomorfismo entonces es también un isomorfismo para los M' que sean sumandos directos de M y para los $M' = M^n$, finalmente demostrar que para $M = A$ es un isomorfismo.

7.5.15. Sea N un A-módulo tal que la aplicación del ejercicio anterior $N^* \otimes_A N \to End_A(N)$ es un isomorfismo, demostrar entonces que N es proyectivo de tipo finito.

Sugerencia. Explotar el hecho de que la identidad de N está en la imagen.

7.5.16. Sea ${}_AP$ un A-módulo a izquierda, ${}_AU_B$ un A-B-bimódulo y ${}_BN$ un B-módulo a izquierda. Se define el morfismo

$$\begin{aligned} \phi : \mathrm{Hom}_A(P, U) \otimes_B N &\to \mathrm{Hom}_A(P, U \otimes_B N) \\ \phi(f \otimes n)(p) &= f(p) \otimes n \end{aligned}$$

Verificar que está bien definido y que si P es proyectivo y finitamente generado entonces ϕ es un isomorfismo. Considerar el caso

particular de una k-álgebra A, $U = P = A^n$, $B = k$, C una k-álgebra cualquiera, y concluir que $M_n(A) \otimes_k C \cong M_n(A \otimes C)$.

7.5.17. Un anillo conmutativo A es *absolutamente playo* si todos sus módulos son playos.

(a) Muestre que las siguientes afirmaciones son equivalentes:
  (a) A es absolutamente playo.
  (b) Todo ideal principal de A es idempotente.
  (c) Todo ideal finitamente generado de A es un sumando directo de A.

(b) Muestre que un anillo booleano es absolutamente playo.

(c) Si A es un anillo conmutativo absolutamente playo y $S \subset A$ es un subconjunto multiplicativamente cerrado, entonces A_S es absolutamente playo.

7.5.18. *Producto tensorial de álgebras.* Sea k un cuerpo y sean A y B k-álgebras. Muestre que $A \otimes_k B$ es un álgebra de forma tal que el producto está dado por

$$a \otimes b \cdot a' \otimes b = (aa') \otimes (bb').$$

7.5.19. Sea k un cuerpo, A una k-álgebra y n, $m \in \mathbb{N}$. Muestre que hay isomorfismos naturales de álgebras

$$A[X] \cong k[X] \otimes_k A,$$
$$\mathsf{M}_n(A) \cong \mathsf{M}_n(k) \otimes_k A,$$

y

$$\mathsf{M}_{nm}(A) \cong \mathsf{M}_n(A) \otimes_k \mathsf{M}_m(A).$$

7.5.20. *Algebra tensorial, simétrica y exterior.* Sea k un anillo conmutativo y sea V un k-módulo simétrico. Sea $T(V) = \oplus_{n \geq 0} V^{\otimes n}$, conviniendo que $V^{\otimes 0} = k$ y $V^{\otimes (n+1)} = V^{\otimes n} \otimes V$. Se trata claramente de un k-módulo, que resulta una k-álgebra, llamada *k-álgebra tensorial de V*, con la multiplicación dada por la yuxtaposición.

Sea I_S el ideal bilátero generado por los elementos de la forma $v \otimes w - w \otimes v$, con v, $w \in V$, y sea I_Λ el ideal bilátero generado por los elementos de la forma $v \otimes w + w \otimes v$. Definimos $S(V) = T(V)/I_S$ y $\Lambda(V) = T(V)/I_\Lambda$. Llamamos a $S(V)$ el *álgebra simétrica* y a $\Lambda(V)$ el *álgebra exterior*. Denotaremos $v_1 \cdots v_k$ a la clase módulo I_S de $v_1 \otimes \cdots \otimes v_k$ y $v_1 \wedge \cdots \wedge v_k$ a su clase módulo I_Λ.

Mostrar que estas tres construcciones son funtoriales, que $S(V)$ es una k-álgebra conmutativa y que si V es un k-módulo finitamente generado, entonces $\Lambda(V)$ es también finitamente generado como k-módulo.

Probar además que si A es una k-álgebra cualquiera, entonces

$$\mathrm{Hom}_k(V, A) \cong \mathrm{Hom}_{k-\mathrm{alg}}(T(V), A).$$

Si además A es conmutativa, entonces

$$\mathrm{Hom}_k(V, A) \cong \mathrm{Hom}_{k-\mathrm{alg}}(S(V), A).$$

Si V es k-libre de base $\{x_1, \ldots, x_n\}$, muestre que hay un isomorfismos de k-álgebras $S(V) \cong k[x_1, \ldots, x_n]$.

7.5.21. Sea k un cuerpo, V un k-espacio vectorial de dimensión n y $f : V \to V$ un endomorfismo. Sea $\Lambda^i(V) = \mathrm{Im}(V^{\otimes i} \to \Lambda(V))$. Ver que $\Lambda(V) = \bigoplus_{i=0}^{n} \Lambda^i(V)$. Calcular la dimensión de $\Lambda^i(V)$ para cada i y ver, en particular, que $\dim_k(\Lambda^n(V)) = 1$.

Ver que $\Lambda(f) : \Lambda(V) \to \Lambda(V)$ (que fue definido en el ejercicio anterior) se restringe para dar varias transformaciones lineales $\Lambda^i(f) : \Lambda^i(V) \to \Lambda^i(V)$. Como $\Lambda^n(V)$ tiene dimensión 1, $\Lambda^n(f)$ debe ser un múltiplo de la identidad. Muestre que

$$\Lambda^n(f) = \det(f)\, \mathrm{Id}_{\Lambda^n(V)}.$$

Deducir de lo anterior y de la funtorialidad de Λ^n que $\det(g \circ f) = \det(g)\ \det(f)$.

7.5.22. Sea M un A-módulo a derecha de torsión y N un A-módulo a izquierda divisible, entonces $M \otimes_A N = 0$. Calcule $G_{p^\infty} \otimes_{\mathbb{Z}} G_{p^\infty}$. Demuestre que el único producto (distributivo con respecto a la suma) que se puede definir en G_{p^∞} es el idénticamente nulo.

7.5.23. Probar que si $n, m \in \mathbb{Z}$ son tales que $(n, m) = 1$ entonces $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m = 0$.

7.5.24. Calcular $\mathbb{Z}_{p^n} \otimes_{\mathbb{Z}} \mathbb{Z}_{p^m}$.

7.5.25. Sea G un grupo y M un $\mathbb{Z}[G]$-módulo, es decir, un grupo abeliano sobre el cual actúa G. Sea $\mathbb{Z}$ el $\mathbb{Z}[G]$-módulo definido por $g \cdot n = n$ para todo $n \in \mathbb{Z}$, $g \in G$. Entonces:

(a) $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M) \cong \{m \in M : g(m) = m,\ \forall g \in G\}$. Notamos al espacio de la derecha M^G y lo llamamos *espacio de invariantes* de M.

(b) $\mathbb{Z} \otimes_{\mathbb{Z}[G]} M \cong M/\langle m - g(m) : m \in M, g \in G\rangle$. Notamos al espacio de la derecha M_G y lo llamamos *espacio de coinvariantes* de M.

(c) Deducir que $(-)^G$ y $(-)_G$ son dos funtores de $\mathbb{Z}[G]$-módulos en la catetgoría de los grupos abelianos y que $(-)^G$ es exacto a izquierda y $(-)_G$ es exacto a derecha.

7.5.26. Sea A un anillo conmutativo. Mostrar que si $A^{(I)} \cong A^{(J)}$, entonces el cardinal de I es igual al cardinal de J.

Sugerencia. Usar $(-) \otimes_A A/\mathfrak{m}$, donde $\mathfrak{m}$ es algún ideal maximal de A.

7.5.27. Sea k un anillo conmutativo y sea $k-$ Algc la categoría de k-álgebras conmutativas, con morfismos los morfismos de anillos k-lineales. Mostrar que las aplicaciones $i_A : a \in A \to a \otimes 1 \in A \otimes_k B$ y $i_B : b \in B \to 1 \otimes b \in A \otimes_k B$ hacen de $A \otimes_k B$ el coproducto de A y B en la categoría $k-$ Algc.

7.5.28. Sean V y W dos k-módulos simétricos, demuestre que

$$S(V \oplus W) \cong S(V) \otimes_k S(W)$$

y que, en particular, $k[x] \otimes_k k[y] \cong k[x, y]$.

7.5.29. Sea A una k-álgebra conmutativa y sea V un l-módulo. Pongamos $M = A \otimes_k V$. Muestre que hay isomorfismos de k-álgebras

$$T_A(M) \cong A \otimes T_k(V),$$
$$S_A(M) \cong A \otimes S_k(V)$$

y

$$\Lambda_A(M) \cong A \otimes \Lambda_k(V).$$

Productos de torsión

7.5.30. Sean M y N grupos abelianos. Consideremos el conjunto

$$G(M, N) = \{(m, k, n) \in M \times \mathbb{Z} \times N : km = 0, kn = 0\}.$$

Sean $L(M,N)$ el $\mathbb{Z}$-módulo libre generado por $G(M,N)$ y $R(M,N)$ el subgrupo de $L(M,N)$ generado por los elementos

$$(m+m',k,n)-(m,k,n)-(m',k,n), \quad \text{si } km=km'=0 \text{ y } km=0;$$
$$(m,k,n+n')-(m,k,n)-(m,k,n'), \quad \text{si } km=0 \text{ y } kn=kn'=0;$$
$$(m,kk',n)-(mk,k',n), \quad \text{si } kk'm=0 \text{ y } k'n=0;$$
$$(m,kk',n)-(m,k,k'n), \quad \text{si } km=0 \text{ y } kk'n=0.$$

Definimos $M \odot N = L(M,N)/G(M,N)$.

(a) Si M ó N no posee elementos de orden finito, $M \odot N = 0$

(b) Hay un isomorfismo $M \odot N \cong N \odot M$.

(c) Dados $f : M \to M'$ y $g : N \to N'$ son morfismos de grupos abelianos, es posible construir un morfismo de grupos abelianos $f \odot g : M \odot N \to M' \odot N'$ de manera que se cumplan las siguientes condiciones:

(i) Si $f : M \to M'$, $f' : M' \to M''$, $g : N \to N'$ y $g : N' \to N''$ son morfismos de grupos abelianos, entonces

$$(f' \odot g') \circ (f \odot g) = (f' \circ f) \odot (g' \odot g).$$

(ii) Si $f, f' : M \to M'$ y $g, g' : N \to N'$ son morfismos de grupos abelianos, entonces

$$(f+f') \odot g = f \odot g + f' \odot g$$

y

$$f \odot (g+g') = f \odot g + f \odot g'.$$

(iii) Si M y N son grupos abelianos, es $\mathsf{Id}_M \odot \mathsf{Id}_N = \mathsf{Id}_{M \odot N}$.

(d) Si $f : M \to M'$ y $g : N \to N'$ son isomorfismos, entonces el morfismo $f \odot g : M \odot N \to M' \odot N'$ es un isomorfismo.

(e) Si M, M', N y N' son grupos abelianos, entonces hay isomorfismos naturales

$$(M \oplus M') \odot N \cong (M \odot N) \oplus (M' \odot N)$$

y

$$M \odot (N \oplus N') \cong (M \odot N) \oplus M \odot (M \odot N').$$

(f) Sea

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

una sucesión exacta de grupos abelianos y sea N un grupo abeliano. Entonces hay una sucesión exacta

$$\begin{aligned} 0 \longrightarrow M' \odot N \xrightarrow{f\odot \mathsf{Id}_N} M \odot N \xrightarrow{g\odot \mathsf{Id}_N} M'' \odot N \xrightarrow{\partial} \\ \longrightarrow M' \otimes N \xrightarrow{f\otimes \mathsf{Id}_N} M \otimes N \xrightarrow{g\otimes \mathsf{Id}_N} M'' \otimes N \longrightarrow 0 \end{aligned}$$

para un cierto morfismo $\partial : M'' \odot N \to M' \otimes N$.

(g) Si M es un grupo abeliano y $n \in \mathbb{N}$, calcule $M \odot \mathbb{Z}_n$.

(h) Si M es un grupo abeliano, sea $T(M) \subset M$ el subgrupo de los elementos de torsión. Muestre que hay un isomorfismo $M \odot \mathbb{Q}/ZZ \cong T(M)$.

(i) Sea p un número primo y $S = \{p^i : i \in \mathbb{N}_0\}$. Se trata de un conjunto multiplicativamente cerrado en $\mathbb{Z}$, así que podemos considerar la localización $\mathbb{Z}_S$. Si M es un grupo abeliano, describa el grupo $M \odot \mathbb{Z}_S$.

(j) Sean M y N grupos abelianos tales que si $m \in M$ tiene orden finito k y $n \in N$ tiene orden finito l, entonces $(k, l) = 1$. Muestre que $M \odot N = 0$.

(k) Muestre que si M y N son grupos abelianos finitos, entonces $M \otimes N \cong M \odot N$.

Capítulo 8

Teoremas de Morita

8.1 Equivalencias de categorías

En este capítulo estudiaremos las respuestas a la siguiente pregunta: *¿Cuándo dos anillos A y B son tales que las categorías de A-módulos y de B-módulos son equivalentes?*

Esta información resulta muy útil ya que muchas de las propiedades de un anillo no dependen de él sino de la categoría de módulos asociada. Por ejemplo dos anillos A y B cuyas categorías de módulos sean equivalentes verificarán $\mathcal{Z}(A) \cong \mathcal{Z}(B)$ y $A/[A,A] \cong B/[B,B]$.

Los teoremas 8.2.4 y 8.2.5 responden completamente a la pregunta. Ambos fueron demostrados por Morita en los años '60, es por esta razón que los teoremas similares demostrados posteriormente en otros contextos llevan el nombre de "teorema tipo Morita".

Comenzaremos discutiendo una situación genérica:

Sean A y B dos anillos, y supongamos que se tienen dos bimódulos ${}_AP_B$ y ${}_BQ_A$. Estos inducen dos funtores

$$(-) \otimes_A P : \mathrm{Mod}_A \to \mathrm{Mod}_B$$
$$(-) \otimes_B Q : \mathrm{Mod}_B \to \mathrm{Mod}_A$$

donde Mod_A (resp. Mod_B) denota la categoría de A-módulos (resp. B-módulos) a derecha. Estos dos funtores son siempre exactos a derecha y preservan sumas directas, pero en general no son equiva-

lencias. Componiéndolos, se obtienen funtores

$$\begin{array}{ll} \mathrm{Mod}_A \to \mathrm{Mod}_A & \mathrm{Mod}_B \to \mathrm{Mod}_B \\ M \mapsto M \otimes_A (P \otimes_B Q) & X \mapsto X \otimes_B (Q \otimes_A P) \end{array}$$

No hay razones *a priori* que permitan decir que $M \cong M \otimes_A (P \otimes_B Q)$ como A-módulos (y resp. con los B-módulos).

Hacemos entonces las siguientes suposiciones adicionales: $P \otimes_A Q \cong B$ (isomorfismo de B-bimódulos) y $Q \otimes_B P \cong A$ (isomorfismo de A-bimódulos), entonces $M \otimes_A (P \otimes_B Q) \cong M \otimes_A A \cong M$ para todo A-módulo M y $X \otimes_B Q \otimes_A P \cong X \otimes_B B \cong X$ para todo B-módulo X. Esto dice que uno puede "ir de una categoría a la otra" sin perder información. Notar de cualquier manera que la composición de $(-) \otimes_A P$ con $(-) \otimes_B Q$ no es el funtor identidad, sino naturalmente isomorfo a la identidad (ver definición 9.3.2).

Ejemplo. Sea A un anillo cualquiera, $n \in \mathbb{N}$ y $B = M_n(A)$. La multiplicación usual de matrices da una estructura de A-B-bimódulo a $P := A^{1\times n}$ y de B-A-bimódulo a $Q := A^{n\times 1}$. Llamamos $\{e_1, \ldots, e_n\}$ a la base canónica de P como A-módulo a izquierda y $\{f_1, \ldots, f_n\}$ a la base canónica de Q como A-módulo a derecha. Demuestre entonces que las aplicaciones determinadas por

$$\begin{array}{ll} P \otimes_{M_n(A)} Q \to A & Q \otimes_A P \to M_n(A) \\ e_i \otimes f_j \mapsto \delta_{ij} & f_i \otimes e_j \mapsto e_{ij} \end{array}$$

(en donde e_{ij} es la matriz con un uno en la fila i columna j y ceros en los demás lugares) están bien definidas y son isomorfismos de bimódulos.

La siguiente definición formaliza el concepto de categorías equivalentes:

Definición 8.1.1. Dos categorías $\mathfrak{C}$, $\mathfrak{D}$ se dirán *equivalentes* en caso de que existan funtores $F : \mathfrak{C} \to \mathfrak{D}$ y $G : \mathfrak{D} \to \mathfrak{C}$ tales que $G \circ F \cong \mathsf{Id}_{\mathfrak{C}}$ y $F \circ G \cong \mathsf{Id}_{\mathfrak{D}}$, donde "$\cong$" significa "isomorfismo natural". Los funtores F y G se llamarán equivalencias.

Las propiedades categóricas conservadas por equivalencias pueden ser entendidas (o mejor dicho deducidas) en términos de adjunciones, por lo que demostramos el siguiente Lema:

Lema 8.1.2. *Sea $F : {}_A\mathrm{Mod} \to {}_B\mathrm{Mod}$ una equivalencia, con cuasi-inverso G, entonces F es adjunto a derecha y a izquierda de G.*

Demostración. En primer lugar, notamos que si $M, N \in \mathrm{Obj}(\mathfrak{C})$, entonces F induce una biyección entre los espacios de morfismos $F : \mathrm{Hom}_{\mathfrak{C}}(M, N) \cong \mathrm{Hom}_{\mathfrak{D}}(F(M), F(N))$. Esto es una consecuencia de que $G \circ F \cong \mathrm{Id}_{\mathfrak{C}}$ y de que $F \circ G \cong \mathrm{Id}_{\mathfrak{D}}$, pues estas últimas dos igualdades dicen que $G \circ F : \mathrm{Hom}_{\mathfrak{C}}(M, N) \cong \mathrm{Hom}_{\mathfrak{C}}(GF(M), GF(N))$ para todo par de objetos de $\mathfrak{C}$, y su análogo para $F \circ G$ en $\mathfrak{D}$. □

Consideramos ahora un A-módulo M cualquiera y un B-módulo X cualquiera. Sean $F : {}_A\mathrm{Mod} \to {}_B\mathrm{Mod}$ y $G : {}_B\mathrm{Mod} \to {}_A\mathrm{Mod}$ dos funtores que dan una equivalencia. Se tienen entonces los siguientes isomorfismos naturales:

$$\mathrm{Hom}_A(M, G(X)) \cong \mathrm{Hom}_B(F(M), F(G(X)) \cong \mathrm{Hom}_B(F(M), X)$$

La naturalidad del último isomorfismo se debe a la naturalidad del isomorfismo $F(G(X)) \cong X$. Esto demuestra que F es adjunto a izquierda de G. Para ver que además es adjunto a derecha, utilizamos que G también es una equivalencia, por lo tanto se tienen isomorfismos naturales

$$\mathrm{Hom}_B(F(M), X) \cong \mathrm{Hom}_A(G(F(M)), G(X)) \cong \mathrm{Hom}_A(M, G(X))$$

donde el primer isomorfismo está dado por aplicar el funtor G y el segundo proviene del isomorfismo natural $G(F(M)) \cong M$.

Corolario 8.1.3. *Sea $F : {}_A\mathrm{Mod} \to {}_B\mathrm{Mod}$ una equivalencia. Entonces F preserva sumas directas, productos directos, núcleos, conúcleos, monomorfismos, epimorfismos, objetos inyectivos y objetos proyectivos.*

Demostración. Es consecuencia inmediata de los teoremas 9.3.4 y 9.3.5, válidos para adjunciones en categorías arbitrarias. □

Corolario 8.1.4. *Sea $F : {}_A\mathrm{Mod} \to {}_B\mathrm{Mod}$ una equivalencia, entonces F preserva generación finita y cogeneración finita.*

Demostración. Es consecuencia de la caracterización dada en la Proposición 4.3.1 de la propiedad de ser finitamente generado, y de la definición misma de finitamente cogenerado (definición 4.3.2). Veamos por ejemplo que F conserva objetos finitamente generados.

Sean M un A-módulo finitamente generado y $(X_i)_{i\in I}$ una familia de B-módulos. Sea $p : \oplus_{i\in I} X_i \to F(M)$ un epimorfismo arbitrario de B-módulos, y llamemos G al funtor cuasi-inverso de F. Como G es una equivalencia, G preserva sumas directas y epimorfismos, entonces $G(p) : \oplus_{i\in I} G(X_i) \to GF(M)$ es un epimorfismo. Como $GF(M) \cong M$ es finitamente generado, entonces existe un subconjunto finito $J \subseteq I$ tal que la restricción a $\oplus_{i\in J} G(X_i)$ de $G(p)$ sigue siendo suryectiva, aplicando ahora F obtenemos que la restricción de p a $\oplus_{i\in J} X_i$ es suryectiva, concluimos entonces que $F(M)$ cumple con la propiedad que caracteriza a los módulos finitamente generados. □

Dado que se trata de adjunciones entre categorías de módulos, en donde el Hom es un grupo abeliano, se puede obtener una versión más fuerte de los teoremas de adjunción mencionados anteriormente:

Teorema 8.1.5. *Sean A, B dos anillos y $F : {}_A\mathrm{Mod} \to {}_B\mathrm{Mod}$ un funtor que admite un adjunto a derecha $G : {}_B\mathrm{Mod} \to {}_A\mathrm{Mod}$. Entonces F es exacto a derecha y G es exacto a izquierda.*

Demostración. En particular, F preserva epimorfismos y G preserva monomorfismos, propiedad que ya conocíamos a partir del teorema anterior.

Para demostrar este teorema vamos usar del Lema 5.4.2, que es la traducción en términos del funtor Hom de la propiedad de exactitud.

Delineamos ahora la demostración del teorema de exactitud a derecha (resp. a izquierda) de funtores con adjunto a derecha (resp. a izquierda), dejamos los detalles como ejercicio.

Consideremos (con las notaciones del teorema 8.1.5) una sucesión exacta de A-módulos

$$M \to N \to T \to 0$$

Por el Lema 5.4.2,

$$0 \to \mathrm{Hom}_A(T, G(X)) \to \mathrm{Hom}_A(N, G(X)) \to \mathrm{Hom}_A(M, G(X))$$

es una sucesión exacta de grupos abelianos para cualquier B-módulo X. Utilizando ahora la naturalidad de la adjunción obtenemos

que

$$0 \to \mathrm{Hom}_B(F(T), X) \to \mathrm{Hom}_B(F(N), X) \to \mathrm{Hom}_B(F(M), X)$$

es una sucesión exacta de grupos abelianos para todo B-módulo X. Concluimos entonces a partir del lema anterior a 5.4.2 que

$$F(M) \to F(N) \to F(T) \to 0$$

es una sucesión exacta de B-módulos. La exactitud a izquierda de G es dual. □

Observación. El enunciado anterior sigue siendo válido para funtores adjuntos entre categorías aditivas.

Corolario 8.1.6. *Sea $F : {}_A\mathrm{Mod} \to {}_B\mathrm{Mod}$ una equivalencia, entonces F es un funtor exacto.*

Ejemplo. Sean ${}_AP_B$, ${}_BQ_A$ dos bimódulos tales que $P \otimes_B Q \cong A$ y $Q \otimes_B P \cong B$ como bimódulos. Consideremos las equivalencias $F = Q \otimes_A (-) : {}_A\mathrm{Mod} \to {}_B\mathrm{Mod}$ y $G = P \otimes_B (-) : {}_B\mathrm{Mod} \to {}_A\mathrm{Mod}$. Entonces $Q \cong F(A)$ como B-módulo a izquierda, luego Q es B-proyectivo, $P \cong G(B)$ como A-módulo a izquierda, luego P es A-proyectivo. Considerando las equivalencias entre categorías de módulos a derecha $(-) \otimes_A P$ y $(-) \otimes_B Q$ tenemos también que Q es A-proyectivo a derecha y P es B proyectivo a derecha. Concluimos así que la proyectividad de P y Q con respecto a sus dos estructuras es condición necesaria para que estos funtores induzcan una equivalencia.

Enumeramos a continuación algunas de las propiedades que son preservadas por equivalencias entre categorías de módulos.

Proposición 8.1.7. *Sea $F : {}_A\mathrm{Mod} \to {}_B\mathrm{Mod}$ una equivalencia, entonces para todo A-módulo M:*

1. *El conjunto de submódulos de M, ordenado por inclusión, está en correspondencia biunívoca con el conjunto de submódulos de $F(M)$. Esta correspondencia preserva el orden.*
2. *M es un A-módulo finitamente generado si y sólo si $F(M)$ es un B-módulo finitamente generado.*

3. *M es noetheriano (resp. artiniano) si y sólo si $F(M)$ es noetheriano (resp. artiniano).*
4. *M es indescomponible si y sólo si $F(M)$ es indescomponible.*
5. *M es simple si y sólo si $F(M)$ es simple.*

Demostración. 1. Dado un submódulo N de M y la inclusión $i_N : N \subseteq M$ le asignamos el submódulo de $F(M)$ obtenido mediante $\mathrm{Im}(F(i_N) : F(N) \to F(M)) \subseteq F(M)$. El hecho de que F preserve el orden es consecuencia de que preserva monomorfismos. Es claro que G induce (de manera análoga a F) una aplicación del conjunto de submódulos de $F(M)$ en el de $GF(M) \cong M$.
2. Si bien este resultado ya lo conocíamos, lo incluimos aquí porque puede ser considerado también como consecuencia de 1.
3. Es consecuencia directa de 1. utilizando la definición de cadena ascendente (resp. descendente).
4. Es claro que si M es descomponible entonces $F(M)$ es descomponible, luego $F(M)$ indescomponible implica M indescomponible. La otra implicación se demuestra de la misma forma utilizando G en vez de F.
5. M es simple si y sólo si el conjunto de sus submódulos está dado por $\{\{0\}, M\}$. En este caso el conjunto de submódulos de $F(M)$ (utilizando 1.) es $\{\{0\}, F(M)\}$, por lo tanto $F(M)$ es simple. Por simetría la recíproca también es cierta. □

Corolario 8.1.8. *Sea A un anillo cualquiera y $n \in \mathbb{N}$, entonces*

- *A es noetheriano a izquierda (resp. a derecha) si y sólo si el anillo de matrices $M_n(A)$ es noetheriano a izquierda (resp. a derecha).*
- *A es artiniano a izquierda (resp. a derecha) si y sólo si $M_n(A)$ es artiniano a izquierda (resp. a derecha).*
- *A es un anillo semisimple si y sólo si $M_n(A)$ es un anillo semisimple.*

Demostración. Sabemos a partir del primer ejemplo de este capítulo que $A^{n\times 1}$ y $A^{1\times n}$ son dos bimódulos que establecen una equivalencia entre las categorias de A-módulos y $M_n(A)$-módulos (versión a derecha y versión a izquierda), y entonces estamos en condiciones de utilizar la proposición anterior. □

Observación. La parte de semisimplicidad resulta un corolario de la última proposición pues hemos tomado la siguiente definición: A es semisimple (a izquierda) si y sólo si todo A-módulo (a izquierda) se descompone en suma directa de simples. Existe otra caracterización de los anillos semisimples: A es semisimple (a izq.) $\iff$ todo A-módulo (a izq.) es proyectivo $\iff$ todo A-módulo (a izq.) es inyectivo. Con esta caracterización, la invariancia por matrices de la semisimplicidad es corolario del hecho de que las equivalencias preservan proyectivos (e inyectivos).

8.2 Teoremas de Morita

Por razones de comodidad, durante esta sección consideraremos módulos a derecha en vez de módulos a izquierda. Veremos de cualquier manera que todos los teoremas de esta sección son simétricos en el sentido de que las afirmaciones que se demuestran para las categorías de módulos a derecha siguen siendo válidas si se cambia la palabra derecha por izquierda.

Definición 8.2.1. Sean A y B dos anillos. Diremos que A es *equivalente Morita* a B si las categorías Mod_A y Mod_B son equivalentes. Notaremos $A \sim_M B$.

Resulta claro que $\sim_M$ es una relación de equivalencia.

Ejemplos.
1. Sean A y B anillos tales que $B \sim_M A$. Sabemos entonces que se tienen los isomorfismos de anillos $B \cong \mathrm{End}_B(B) \cong \mathrm{End}_A(G(B))$ donde $G : \mathrm{Mod}_B \to \mathrm{Mod}_A$ es el funtor que da la equivalencia. Como B es B-proyectivo de tipo finito, entonces $G(B)$ es un A-módulo de tipo finito, luego B queda caracterizado como el anillo de endomorfismos de cierta clase de módulos proyectivos de tipo finito. Si A es tal que todo módulo proyectivo de tipo finito es libre (por ejemplo A un cuerpo, o un anillo de división, o un d.i.p., o un anillo local), entonces todo anillo equivalente Morita a A es isomorfo a un anillo de matrices con coeficientes en A.

2. Sean k un cuerpo, $A = k \times k$ y $B = k \times M_2(k)$. Es un ejercicio sencillo verificar que $A \sim_M B$, y uno puede preguntarse si existen $n, m \in \mathbb{N}$ tales que los anillos $M_n(A)$ y $M_m(B)$ sean isomorfos. La

respuesta es no, por un simple argumento de dimensión y divisibilidad: la dimensión sobre k de $M_n(A)$ es $2.n^2$ y la de $M_m(B)$ es $5.m^2$, y nunca puede ser cierta la igualdad $2.n^2 = 5.m^2$ ($n, m \in \mathbb{N}$) pues en la factorización de $2.n^2$, el primo 2 aparece una cantidad impar de veces, y en $5.m^2$ aparece una cantidad par. Observamos que $k \times k$ es un anillo tal que existen proyectivos de tipo finito que no son libres, un ejemplo es $k \times k^2$, cuyo anillo de endomorfismos es justamente

$$B = k \times M_2(k) \cong \mathrm{End}_k(k) \times \mathrm{End}_k(k^2) \cong \mathrm{End}_{k\times k}(k \times k^2)$$

Como ejemplo fundamental recordemos que si A y B son tales que existen bimódulos ${}_AP_B$ y ${}_BQ_A$ que verifican $P \otimes_B Q \cong A$ y $Q \otimes_A P \cong B$ (como bimódulos) entonces $A \sim_M B$. Veremos en esta sección que esta clase de ejemplos agota todas las posibilidades.

Supondremos que los funtores que dan la equivalencia son aditivos, es decir que vale $F(f+g) = F(f) + F(g)$ si f, g son morfismos y F es el funtor. De cualquier manera esta suposición es superflua pues se puede demostrar que todo funtor entre categorías de módulos que admite un adjunto es aditivo.

Para la demostración del primero de los teoremas principales de esta sección comenzaremos con dos lemas sencillos:

Lema 8.2.2. *Sea $F : \mathrm{Mod}_A \to \mathrm{Mod}_B$ un funtor que es una equivalencia, entonces:*

1. *Para cada par de A-módulos M y N, F induce un isomorfismo de grupos abelianos $\mathrm{Hom}_A(M,N) \to \mathrm{Hom}_B(F(M), F(N))$.*
2. *Para cada A-módulo M, el funtor F induce un isomorfismo de anillos $\mathrm{End}_A(M) \to \mathrm{End}_B(F(M))$.*

Demostración. En ambos casos, es claro que F induce biyecciones. Al ser F aditivo, dichas biyecciones son morfismos de grupos. Para el punto 2. notamos que el producto en End es la composición, luego que F preserve el producto y la unidad se debe sencillamente a la funtorialidad. □

Lema 8.2.3. *Sean M_A y N_A dos A-módulos a derecha y $F : \mathrm{Mod}_A \to \mathrm{Mod}_B$ una equivalencia. Entonces*

$$F : \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_B(F(M), F(N))$$

es un isomorfismo de $\mathrm{End}_A(M)$-$\mathrm{End}_A(N)$-bimódulos.

Demostración. Sabemos que es una biyección, basta ver que F es $\mathrm{End}_A(M)$-$\mathrm{End}_A(N)$-lineal.

Sean $f \in \mathrm{Hom}_A(M,N)$, $\phi \in \mathrm{End}_A(M)$ y $\psi \in \mathrm{End}_A(N)$. Es un ejercicio sencillo ver que en este caso la estructura de bimódulo de $\mathrm{Hom}_A(M,N)$ está dada por la composición, es decir $\phi.f.\psi = \phi \circ f \circ \psi$. Aplicando F y utilizando la funtorialidad tenemos

$$F(\phi.f.\psi) = F(\phi) \circ F(f) \circ F(\psi).$$

A su vez, como la estructura de $\mathrm{End}_A(M)$-$\mathrm{End}_A(N)$-bimódulo de $\mathrm{Hom}_B(F(M),F(N))$ está dada por la identificación de los anillos $\mathrm{End}_A(M) \cong \mathrm{End}_B(F(M))$ (resp. con N) vía F, luego

$$F(\phi) \circ F(f) \circ F(\psi) = \phi.F(f).\psi,$$

es decir que F es $\mathrm{End}_A(M)$-$\mathrm{End}_A(N)$-lineal. □

El siguiente teorema describe todas las equivalencias entre categorías de módulos.

Teorema 8.2.4. *(Morita) Sea $F : \mathrm{Mod}_A \to \mathrm{Mod}_B$ una equivalencia con inverso $G : \mathrm{Mod}_B \to \mathrm{Mod}_A$. Entonces existen bimódulos ${}_AP_B$ y ${}_BQ_A$ tales que $F \cong \mathrm{Hom}_A({}_BQ_A, -)$ y $G \cong \mathrm{Hom}_B({}_AP_B, -)$.*

Demostración. Sea M un A-módulo a derecha, consideremos la siguiente cadena de isomorfismos naturales:

$$F(M) \cong \mathrm{Hom}_B(B, F(M)) \cong \mathrm{Hom}_A(G(B), M)$$

Llamando Q a $G(B)$ queda casi demostrado el primer isomorfismo del teorema, pues sólo falta ver que Q es un B-A-bimódulo y que los isomorfismos anteriores son de B-A-bimódulos.

Considerando a B como B-módulo a derecha, tenemos el isomorfismo de anillos $B \cong \mathrm{End}_B(B_B, B_B)$ (notar que de haber considerado módulos a izquierda tendríamos $\mathrm{End}_B({}_BB, {}_BB) \cong B^{op}$). Además G induce un isomorfismo de anillos $\mathrm{End}_B(B) \cong \mathrm{End}_A(G(B))$. Como $G(B)$ es claramente un $\mathrm{End}_B(G(B))$-A-bimódulo, entonces es un B-A-bimódulo. La A-linealidad de los isomorfismos antes mencionados es consecuencia del Lema 8.2.3.

El otro isomorfismo de funtores es completamente análogo, si X es un B-módulo:

$$G(X) \cong \mathrm{Hom}_A(A, G(X)) \cong \mathrm{Hom}_B(F(A), X)$$

Llamamos $P := F(A)$ que es, de manera análoga a Q, un A-B-bimódulo. □

Observación. Una consecuencia del teorema anterior es que P y Q quedan simétricamente relacionados entre sí, pues si observamos las fórmulas del teorema para F y G y especializamos en A y en B obtenemos que

$$P = F(A) \cong \mathrm{Hom}_A({}_BQ_A, A) =: Q^{*A}$$
$$Q = G(B) \cong \mathrm{Hom}_B({}_AP_B, B) =: P^{*B}$$

Como corolario del teorema 8.2.4, se tiene una segunda caracterización de las equivalencias entre categorías de módulos que escribimos en forma de teorema:

Teorema 8.2.5. *(Morita) Con las mismas notaciones que el teorema anterior, se tienen isomorfismos de funtores:*

$$F \cong (-) \otimes_B P$$
$$G \cong (-) \otimes_A Q$$

Demostración. A partir del teorema 8.2.4 sabemos que

$$F \cong \mathrm{Hom}_A({}_BQ_A, -)$$
$$G \cong \mathrm{Hom}_B({}_AP_B, -)$$

Por otro lado, para cualquier bimódulo se tienen transformaciones naturales

$$(-) \otimes_A (Q)^{*A} \to \mathrm{Hom}_A({}_BQ_A, -)$$
$$(-) \otimes_B (P)^{*B} \to \mathrm{Hom}_B({}_AP_B, -)$$

Estas transformaciones naturales son isomorfismos naturales siempre que Q sea A-proyectivo de tipo finito y P sea B-proyectivo de tipo finito. Este es el caso que nos concierne pues las equivalencias preservan objetos proyectivos y finitamente generados y P y Q son imágenes por equivalencias de A y B que son trivialmente proyectivos finitamente generados.

Notar que por la observación anterior sabemos que $(Q)^{*A} \cong P$ y que $(P)^{*B} \cong Q$, por lo tanto podemos escribir $F \cong (-) \otimes_B P$ y $G \cong (-) \otimes_A Q$ como queríamos probar. □

Con este último teorema se demuestra un hecho notable, que es la simetría en la definición de equivalencia Morita. Resulta en principio un poco molesto que para definir una relación de equivalencia entre anillos, haya que elegir o bien los módulos a derecha, o bien lo módulos a izquierda, pero a partir de la caracterización del teorema anterior se tiene el siguiente corolario:

Corolario 8.2.6. *Sean A y B dos anillos. Las categorías ${}_A\mathrm{Mod}$ y ${}_B\mathrm{Mod}$ son equivalentes si y sólo si son equivalentes las categorías Mod_A y Mod_B. Además cualquiera de estas dos condiciones implica que las categorías ${}_A\mathrm{Mod}_A$ y ${}_B\mathrm{Mod}_B$ son equivalentes, donde ${}_A\mathrm{Mod}_A$ indica la categoría de A-A-bimódulos, analogamente para B.*

Demostración. A partir del teorema 8.2.5 sabemos que toda equivalencia entre módulos a derecha está dada por tensorizar con dos bimódulos ${}_AP_B$ y ${}_BQ_A$ tales que $P \otimes_B Q \cong A$ y $Q \otimes_A P \cong B$. Entonces, tomando los funtores $Q \otimes_A (-)$ y $P \otimes_B (-)$ obtenemos una equivalencia entre los módulos a izquierda. La recíproca es también cierta, para ésto hay que demostrar versiones análogas de los teoremas 8.2.4 y 8.2.5 para módulos a izquierda, las demostraciones son similares, cuidando algunos detalles como por ejemplo que el anillo $\mathrm{Hom}_A({}_AA, {}_AA)$ es isomorfo al anillo A^{op} en vez de a A.

Teniendo P y Q como antes, es claro que el funtor $Q \otimes_A (-) \otimes_A P : {}_A\mathrm{Mod}_A \to {}_B\mathrm{Mod}_B$ es una equivalencia, pues su inverso es $P \otimes_B (-) \otimes_B Q : {}_B\mathrm{Mod}_B \to {}_A\mathrm{Mod}_A$. □

Corolario 8.2.7. *Sean A y B dos anillos equivalentes Morita, entonces*

- $\mathcal{Z}(A) \cong \mathcal{Z}(B)$ *(isomorfismo de anillos).*
- $A/[A,A] \cong B/[B,B]$ *(isomorfismo de grupos abelianos).*

Demostración.

$$\begin{aligned}\mathcal{Z}(A) &\cong \mathrm{Hom}_{A-A}(A,A)\\ &\cong \mathrm{Hom}_{B-B}(Q \otimes_A A \otimes_A P, Q \otimes_A A \otimes_A P)\\ &\cong \mathrm{Hom}_{B-B}(Q \otimes_A P, Q \otimes_A P)\\ &\cong \mathrm{Hom}_{B-B}(B,B)\\ &\cong \mathcal{Z}(B)\end{aligned}$$

y todos estos isomorfismos son de anillos.

Para el segundo punto, observamos que la categoría ${}_A\mathrm{Mod}_A$ se identifica con las categorías ${}_{A^e}\mathrm{Mod}$ y Mod_{A^e}, donde $A^e = A \otimes_{\mathbb{Z}} A^{op}$ (analogamente para B). Utilizando el teorema 8.2.5, el funtor $Q \otimes_A (-) \otimes_A P$ debe ser necesariamente de la forma $\widetilde{P} \otimes_{A^e} (-)$ o bien $(-) \otimes_{A^e} \widetilde{Q}$, donde $\widetilde{Q}$ y $\widetilde{P}$ son dos bimódulos sobre A^e y B^e. El lector puede verificar que $\widetilde{P} = P \otimes_{\mathbb{Z}} Q$ y $\widetilde{Q} = Q \otimes_{\mathbb{Z}} P$ sirven. También es fácil verificar (de hecho ya lo hicimos en el punto anterior) que $\widetilde{P} \otimes_{A^e} A = A \otimes_{A^e} \widetilde{Q} \cong P \otimes_A A \otimes_A Q \cong B$, por lo tanto

$$\begin{aligned} A/[A,A] &\cong A \otimes_{A^e} A \\ &\cong (P \otimes_B Q) \otimes_{A^e} (P \otimes_B Q) \\ &\cong (Q \otimes_A P) \otimes_{B^e} (Q \otimes_A P) \\ &\cong B \otimes_{B^e} B \\ &\cong B/[B,B] \end{aligned}$$

□

Ejemplo. Sea k un cuerpo y $n \in \mathbb{N}$. Si se quiere calcular $\mathcal{Z}(M_n(k))$, una opción es demostrar "a mano" a partir de que una matriz que conmuta con cualquier otra en particular conmuta con las matrices elementales, obtener así condiciones sobre la matriz para llegar, luego de penosas y largas cuentas, a ver que las únicas matrices que conmutan con cualquier otra son múltiplos de la identidad. Otra manera es, a la luz de la equivalencia Morita entre k y $M_n(k)$, aplicar el corolario anterior y obtener $\mathcal{Z}(M_n(k)) \cong \mathcal{Z}(k) = k$. Otra aplicación elemental al álgebra lineal es por ejemplo responder a la pregunta ¿cuándo una matriz es combinación lineal de conmutadores? Para esto sabemos que $M_n(k)/[M_n(k), M_n(k)] \cong k/[k,k] = k$, por lo tanto $[M_n(k), M_n(k)]$ es un subespacio de codimensión uno, luego es el núcleo de algún elemento del dual. Es conocido que $\mathrm{tr}(M.N - N.M) = 0$, por lo tanto $[M_n(k), M_n(k)] \subseteq \mathrm{Ker}(\mathrm{tr})$, pero como tienen la misma dimensión resultan subespacios iguales.

8.3 Contextos

En esta sección veremos la noción de contexto de Morita, que junto al teorema 8.3.2 facilitan enormemente la tarea de verificación en casos concretos de que dos anillos sean equivalentes Morita.

Comenzamos comentando el caso en que $A \sim_M B$. Por el teorema 8.2.5 sabemos que existen bimódulos ${}_AP_B$ y ${}_BQ_A$ que inducen (a través del producto tensorial) la equivalencia entre las categorías de A-módulos y de B-módulos. Recordamos también que el anillo $A \cong \mathrm{End}_A(A)$ se identifica con $\mathrm{End}_B(F(A)) = \mathrm{End}_B(P)$ y que Q se puede tomar como P^{*B}. Tenemos entonces dos aplicaciones naturales:

- $v : P \otimes_B Q \to \mathrm{End}_B(P)$ definida por $p \otimes \phi \mapsto (x \mapsto p.\phi(x))$,
- la evaluación $u : Q \otimes_A P \to B$ definida por $\phi \otimes p \mapsto \phi(p)$.

Entre estos dos morfismos se verifican las siguientes propiedades de compatibilidad:

- Para todo ϕ, ψ en P^*, p en P, $\phi.v(p \otimes \psi) = u(\phi \otimes p).\psi$. En efecto:

$$(\phi.v(p \otimes \psi))(x) = (\phi.(p\psi(-))(x)) = \phi(p.\psi(-))(x)$$
$$= \phi(p.\psi(x)) = \phi(p)\psi(x) = (u(\phi \otimes p).\psi)(x)$$

- Para todo p, p' en P, ψ en P^*, $v(p \otimes \psi).p' = p.u(\psi \otimes p')$. En efecto:

$$v(p \otimes \psi)p' = p\psi(p') = p.u(\psi \otimes p')$$

Esto motiva la siguiente definición:

Definición 8.3.1. Dados dos bimódulos ${}_AP_B$ y ${}_BQ_A$ y dos morfismos de bimódulos $u : Q \otimes_A P \to B$ y $v : P \otimes_B Q \to A$ (no necesariamente isomorfismos), se dice que (A, B, P, Q, u, v) es un *contexto Morita* entre A y B en caso de que se verifiquen las siguientes condiciones de compatibilidad:

$$v(p \otimes q).p' = p.u(q \otimes p')$$
$$u(q \otimes p).q' = q.v(p \otimes q'),$$

para todo $p, p' \in P$, $q, q' \in Q$.

Cuando u y v son isomorfismos, P y Q inducen una equivalencia.

Teorema 8.3.2. *Sea (A, B, P, Q, u, v) un contexto Morita tal que u y v son epimorfismos, entonces u y v son isomorfismos. En particular A resulta equivalente Morita a B.*

Demostración. Consideremos $1_A \in \mathrm{Im}(v)$, luego existen $p_1, \ldots, p_r$ elementos de P y $q_1, \ldots, q_r$ elementos de Q tales que

$$1_A = \sum_{i=1}^{r} v(p_i \otimes q_i).$$

Definimos $s : A \to P \otimes_B Q$ a través de la fórmula

$$s(a) = \sum_{i=1}^{r} a.(p_i \otimes q_i).$$

Es claro que s es un morfismo de A-módulos a izquierda, veremos que es el inverso de v (en particular s será un morfismo de bimódulos). Calculamos para esto explícitamente las composiciones $s \circ v$ y $v \circ s$:

$$\begin{aligned} s(v(p \otimes q)) &= \sum_{i=1}^{r} v(p \otimes q)p_i \otimes q_i = \sum_{i=1}^{r} p.u(q \otimes p_i) \otimes q_i \\ &= \sum_{i=1}^{r} p \otimes u(q \otimes p_i)q_i = \sum_{i=1}^{r} p \otimes q.v(p_i \otimes q_i) \\ &= (p \otimes q) \sum_{i=1}^{r} v(p_i \otimes q_i) = p \otimes q \end{aligned}$$

$$v(s(a)) = \sum_{i=1}^{r} v(a.p_i \otimes q_i) = a. \sum_{i=1}^{r} v(p_i \otimes q_i) = a$$

La demostración para ver que u es también un isomorfismo es completamente análoga. □

Ejemplos.
1. Sea R un anillo cualquiera y $e \in R$ tal que $e = e^2$. Consideremos el anillo $e.R.e$. Es claro que $P = e.R$ es un $e.R.e$-R-bimódulo y que $Q = R.e$ es un R-$e.R.e$-bimódulo. La multiplicación de R induce morfismos de bimódulos

$$u : R.e \otimes_{e.R.e} e.R \to R$$
$$v : e.R \otimes_R R.e \to e.R.e$$

Es claro que v es siempre suryectiva. En cambio la imagen de u es $R.e.R$, o sea el ideal bilátero generado por e. Hay veces en que esto último es fácil de calcular, por ejemplo si R es un anillo simple. Como corolario del teorema 8.3.2 se tiene el siguiente resultado: si $e \in R$ es un idempotente tal que $R = R.e.R$, entonces $R \sim_M e.R.e$.

2. Como subejemplo del ejemplo anterior, considerar $R = M_n(A)$ donde A es un anillo cualquiera y e la matriz que tiene un uno en el lugar $(1,1)$ y cero en el resto. El anillo $e.M_n(A).e$ consiste de las matrices que tienen ceros en todas sus entradas salvo eventualmente en el lugar $(1,1)$. Este anillo claramente se identifica con el anillo A. Queda como ejercicio verificar que el ideal bilátero generado por e es $M_n(A)$. De esta manera hemos vuelto a demostrar que $M_n(A) \sim_M A$.

Ejercicio. Sean A y B dos anillos tales que $A \sim_M B$. Demuestre que existe un contexto Morita entre A y B que da la equivalencia.

8.3.1 Acciones de grupos sobre anillos y contextos Morita

Así como en la teoría de k-módulos, al considerar las acciones de grupos sobre los módulos nos interesaban las acciones k-lineales, al trabajar con anillos nos interesarán particularmente las acciones de grupos que respeten la estructura de anillo. Sean entonces A un anillo y G un grupo finito que actúa en A por automorfismos de anillos, es decir, se tiene una aplicación

$$\begin{aligned} G \times A &\to A \\ (g, a) &\mapsto g(a) \end{aligned}$$

que es una acción y que verifica además que para cada $g \in G$, $g(-)$ es un automorfismo de anillos (i.e. $g(a + a') = g(a) + g(a')$, $g(a.a') = g(a).g(a')$ $\forall a, a' \in A$ y $g(1_A) = 1_A$). En estas condiciones, siempre es posible construir dos anillos asociados a A y a G que están en contexto Morita, estos anillos son A^G (el subanillo de invariantes) y $A \rtimes G$ (el producto cruzado de A con G). Antes de ver la construcción, veamos dos ejemplos de acciones de grupos por automorfismos de anillos.

Ejemplos.
1. Sea A un anillo cualquiera y $G \subseteq \mathrm{Aut}_{anillos}(A)$, entonces claramente G actúa en A por automorfismos de anillos.

2. Si $A = \mathbb{C}$, $G = \mathbb{Z}_2$ actúa en $\mathbb{C}$ por conjugación.

3. Sea X un conjunto y $G \times X \to X$ una acción de G sobre X. Sea k un anillo conmutativo y consideramos $A = k^X = Func(X, k)$, el conjunto de funciones de X en k con la estructura de anillo heredada de k punto a punto. Entonces G actúa sobre A a través de la fórmula

$$\begin{aligned} &G \times A \to A \\ &(g, f) \mapsto \Big(x \mapsto f(g^{-1}(x))\Big) \end{aligned}$$

El lector podrá verificar sin dificultad que ésta es una acción por automorfismos de anillos.

Ejercicio. Sea G un grupo que actúa por automorfismos de anillos en un anillo A, entonces $A^G = \{a \in A \ / \ g(a) = a \ \forall g \in G\}$ es un subanillo de A.

Damos ahora la definición del producto cruzado:

Consideramos $A[G]$ con su estructura aditiva habitual pero con una estructura multiplicativa diferente. Si $a, a' \in A$, $g, g' \in G$ se define

$$(ag).(a'g') := (ag(a'))(gg')$$

y se extiende dicha definición bilinealmente a los demás elementos de $A[G]$.

Ejercicio. Con ese producto, el conjunto $A[G]$ es un anillo asociativo con 1 (¿cuál es el uno?), que se llama *producto cruzado* de A por G y se denota $A \rtimes G$

Observación. Aún teniendo $A \rtimes G$ un producto distinto en general al de $A[G]$, contiene de cualquier manera a A como subanillo, y tambien el morfismo evidente $\mathbb{Z}[G] \to A \rtimes G$ es un morfismo de anillos.

Los anillos A^G y $A \rtimes G$ son construcciones naturales a partir del anillo A y de una acción de G sobre A por automorfismos. Una relación importante entre ambos está dada por la siguiente proposición:

Proposición 8.3.3. *Sea A un anillo y G un grupo finito que actúa en A por automorfismos de anillos. Entonces A^G está en contexto Morita con $A \rtimes G$.*

Demostración. Debemos exhibir bimódulos P y Q que satisfagan la definición de contexto. Para esto tomamos, como grupos abelianos, $P = Q = A$, pero con diferentes acciones.

Es claro que $P = A$ es un A^G-módulo a derecha. Si $a.g \in A \rtimes G$ y $x \in A$ definimos

$$(ag).x = ag(x).$$

El lector podrá verificar que esta definición cumple con los axiomas de acción. Hacemos notar que si $b \in A^G$, entonces $ag(x).b = ag(xb)$. Esta última igualdad dice que las acciones de $A \rtimes G$ y A^G son compatibles, por lo tanto P es un $A \rtimes G$-A^G-bimódulo.

Consideramos a $Q = A$ de manera obvia como un A^G-módulo a izquierda, y definimos

$$x.(ag) = g^{-1}(xa),$$

donde $a, x \in A$ y $g \in G$. Definimos ahora dos morfismos:

$$\begin{aligned} \mu : P \otimes_{A^G} Q \to A \rtimes G \qquad & \tau : Q \otimes_{A \rtimes G} P \to A^G \\ \mu(a \otimes b) = \sum_{g \in G} ag(b)g \qquad & \tau(a \otimes b) = \sum_{g \in G} g(a.b) \end{aligned}$$

Veremos la buena definición, dejamos como ejercicio verificar que son morfismos de bimódulos.

Si $x, y \in A$, $a \in A^G$, entonces

$$\mu(xa \otimes y) = \sum_{g \in G} xag(y)g = \sum_{g \in G} xg(ay)g = \mu(x \otimes ay)$$

En el caso de τ, sean $x, y, a \in A$ y $h \in G$, entonces

$$\begin{aligned} \tau(x(ah) \otimes y) =& \tau(h^{-1}(xa) \otimes y) \\ =& \sum_{g \in G} g(h^{-1}(xa).y) \\ =& \sum_{g \in G} g.h^{-1}(xa.h(y)) \\ =& \sum_{g' \in G} g'(xah(y)) \\ =& \tau(x \otimes (ah).y) \end{aligned}$$

Veamos ahora la compatibilidad de μ y τ: sean $x, y, z \in A$ entonces

$$\begin{aligned} x\mu(y \otimes z) =& x\left(\sum_{g\in G} yg(z)g\right) \\ =& \sum_{g\in G} g^{-1}(xyg(z)) \\ =& \sum_{g\in G} g^{-1}(xy)z \\ =& \left(\sum_{g\in G} g^{-1}(xy)\right) z \\ =& \tau(x \otimes y)z \end{aligned}$$

Por otro lado

$$\begin{aligned} \mu(x \otimes y)z =& \left(\sum_{g\in G} xg(y)g\right) z \\ =& \sum_{g\in G} xg(y)g(z) \\ =& \sum_{g\in G} xg(yz) \\ =& x\left(\sum_{g\in G} g(yz)\right) \\ =& x\tau(y \otimes z) \end{aligned}$$

□

Observación. Una pregunta natural en este punto es: ¿cuándo el contexto entre A^G y $A \rtimes G$ es una equivalencia? En virtud del Teorema 8.3.2, basta ver cuándo μ y τ son morfismos sobreyectivos. El más sencillo es τ, pues es un promedio. Es claro que si $|G|$ es inversible en A y $a \in A^G$, entonces $a = \frac{1}{|G|}\sum_{g\in G} g(a) = \tau(a \otimes 1)$. Por otro lado, $\mathrm{Im}(\mu)$ es un subbimódulo de $A \rtimes G$, o sea, un ideal bilátero, luego $\mathrm{Im}(\mu) = A \rtimes G$ si y sólo si $1_{A\rtimes G} \in \mathrm{Im}(\mu)$. Esto significa que existen $a_1, \ldots, a_r, b_1, \ldots, b_r \in A$ tales que $1 = \mu\left(\sum_{i=1}^r a_i \otimes b_i\right) = \sum_{i=1}^r \sum_{g\in G} a_i g(b_i).g$.

Definición 8.3.4. Sean A un anillo y G un grupo que actúa por automorfismos de anillos en A. Diremos que la acción de G sobre A es **Galois** si existen elementos $a_1, \dots, a_s, b_1, \dots, b_s \in A$ tales que

$$\sum_{i=1}^{s} a_i.g(b_i) = \begin{cases} 1 & \text{si } g = 1_G, \\ 0 & \text{si } g \neq 1_G. \end{cases}$$

Si la acción de un grupo G sobre un anillo A es Galois y $a_1, \dots, a_s$, $b_1, \dots, b_s$ son los elementos de la definición de Galois, entonces

$$\mu(\sum_{i=1}^{s} a_i \otimes b_i) = \sum_{i=1}^{s} \sum_{g \in G} a_i g(b_i) g = \sum_{g \in G} \left(\sum_{i=1}^{r} a_i g(b_i) \right) g = 1$$

Luego, hemos demostrado el siguiente teorema:

Teorema 8.3.5. *Sea A un anillo y G un grupo que actúa por automorfismos de anillos tal que $|G|$ es inversible en A y la acción de G es Galois. Entonces la categoría de A^G-módulos es equivalente a la categoría de $A \rtimes G$-módulos.*

Ejemplos.
1. Sea k un anillo tal que $1/2 \in k$ y $A = k[x]$. Sea $G = \mathbb{Z}_2$ que actúa en A a través de $x \mapsto -x$. Ver que $A^G = k[x^2]$, pero la acción no es Galois. Demuestre que G actúa (con la misma fórmula) en $A' := k[x, x^{-1}]$, y en ese caso la acción es Galois.

2. Considerar $A = k[x, y]$ y $G = \mathbb{Z}_2$ actuando por permutación (i.e. $y \mapsto x$ y $x \mapsto y$). Probar que $A^G = k[s, t]$ donde $s = x + y$ y $t = x.y$ y que la acción no es Galois. Sea $\delta := x - y$, ver que G actúa en $A[\delta^{-1}]$ (el localizado de A en las potencias de δ) y que la acción de G es Galois en $A[\delta^{-1}]$.

8.4 Ejercicios

8.4.1. Sea $F : {}_A\text{Mod} \to {}_B\text{Mod}$ un funtor cualquiera. Ver que:

1. F preserva productos finitos si y sólo si F preserva sumas finitas.
2. Si F preserva sumas finitas (o productos finitos), entonces F es aditivo (i.e. si $F(f + g) = F(f) + F(g)$ para todo par de morfismos A-lineales f, g).

8.4.2. Sea $F : C \to D$ un funtor entre dos categorías C y D. Supongamos que F admite un funtor adjunto a derecha que llamaremos G. Demostrar que si G' es otro funtor adjunto a derecha de F entonces $G \cong G'$, es decir $G(X) \cong G'(X)$ para todo objeto X de la categoría D, y ese isomorfismo es natural (sugerencia: demostrar primero que el ejercicio es equivalente a probar que existe un isomorfismo natural $\mathrm{Hom}_C(M, G(X)) \cong \mathrm{Hom}_C(M, G'(X))$ para todo objeto X de D y M de C.

8.4.3. Sea $F : {}_A\mathrm{Mod} \to {}_B\mathrm{Mod}$ un funtor que admite un adjunto a derecha $G : {}_B\mathrm{Mod} \to {}_A\mathrm{Mod}$. Demostrar que existe un B-A-bimódulo X tal que $G \cong \mathrm{Hom}_B(X, -)$ y que $F \cong X \otimes_A -$, además la clase de isomorfismo (como bimódulo) de X queda unívocamente determinada.

8.4.4. Probar que si $A \sim_M B$ y $A' \sim_M B'$ entonces $A \times A' \sim_M B \times B'$ y que $A \otimes_{\mathbb{Z}} A' \sim_M B \otimes_{\mathbb{Z}} B'$.

8.4.5. Sean $(n_1, \ldots, n_r)$ y $(m_1, \ldots, m_r)$ dos r-uplas de números naturales y k un anillo cualquiera, ¿Es $M_{n_1}(k) \times M_{n_2}(k) \times \cdots \times M_{n_r}(k)$ equivalente Morita a $M_{m_1}(k) \times M_{m_2}(k) \times \cdots \times M_{m_r}(k)$? Supongamos que k es un cuerpo, ¿qué dimensión tiene el centro de estas dos álgebras?

8.4.6. Sea A el anillo de matrices triangulares superiores de 2×2, i.e. $A = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix},\ a, b, c \in k \right\}$ donde k es un cuerpo, ¿Es A equivalente Morita a k o a $k \times k$?

8.4.7. Sea G un grupo finito que actúa en un anillo A.

1. (Maschke) Probar que si $\frac{1}{|G|} \in A$ y $f : M \to N$ es un epimorfismo de $A \rtimes G$-módulos que se parte como morfismo de A-módulos, entonces f se parte como morfismo de $A \rtimes G$-módulos. En particular, si A es un anillo semisimple y $|G|$ inversible en A, entonces $A \rtimes G$ es semisimple.
2. Probar que si A es noetheriano entonces $A \rtimes G$ es noetheriano.
3. Concluir que si $|G| \in A$ y la acción es Galois, entonces A semisimple (resp. noetheriano) implica A^G semisimple (resp. noetheriano).

8.4.8. Consideremos a $\mathbb{Z}_2$ actuando en $\mathbb{C}$ por conjugación. Demostrar que $\mathbb{C}^G = \mathbb{R}$ y que $\mathbb{C} \rtimes \mathbb{Z}_2 \cong M_2(\mathbb{R})$. (Nota: sale de dos maneras diferentes). ¿Es Galois la acción de $\mathbb{Z}_2$ sobre $\mathbb{C}$?

8.4.9. Ver que la categoría de $A \rtimes G$-módulos consiste en la categoría cuyos objetos son A-módulos munidos de una acción del grupo G tal que vale la siguiente relación de compatibilidad:

$$g(a.m) = g(a).g(m)$$

y los morfismos son los morfismos A-lineales que conmutan con la acción de G.

1. Sea M un $A \rtimes G$-módulo, ver entonces que
$$M^G = \{m \in M \ / \ g(m) = m \ \forall m \in M\}$$
es un A^G-módulo.
2. Si consideramos a A como un objeto de ${}_{A^G}\mathrm{Mod}_{A\rtimes G}$, entonces ver que $A \otimes_{A\rtimes G} M \cong M^G$.
3. La acción de A en M induce un morfismo $A \otimes_{A^G} M^G \to M$ de tal manera que el siguiente diagrama (salvo eventualmente multiplicación por $|G|$) es conmutativo:
$$\begin{array}{ccc} A \otimes_{A^G} M^G & \longrightarrow & M \\ \| & & \| \\ A \otimes_{A^G} (A \otimes_{A\rtimes G} M) & \xrightarrow{\mu\otimes 1_M} & A \rtimes G \otimes_{A\rtimes G} M \end{array}$$
Concluir que si $|G|$ es inversible en A y la acción de G sobre A es Galois, entonces $A \otimes_{A^G} M^G \to M$ es un isomorfismo.

8.4.10. Sea A un anillo tal que todo módulo proyectivo de tipo finito es libre (por ejemplo un cuerpo, o un d.i.p. como $\mathbb{Z}$ ó $\mathbb{Z}[i]$, ó $k[x]$ ó $k[x, x^{-1}]$), entonces los únicos anillos equivalentes Morita a A son isomorfos a $M_n(A)$ para algún $n \in \mathbb{N}$.

8.4.11. Sea A un anillo y G un grupo que actúa en A por automorfismos de anillos tal que la acción es Galois y $1/|G| \in A$. Demuestre que si A^G es tal que todo A^G-módulo proyectivo de tipo finito es libre (por ejemplo A^G un cuerpo, o un d.i.p.) entonces $A \rtimes G \cong M_n(A^G)$ donde $n = |G|$ (notar que este es el caso del ejercicio **8.4.8**). Calcular $\mathcal{Z}(A \rtimes G)$.

Capítulo 9

Categorías: algunas definiciones y construcciones universales

9.1 Categorías

En este capítulo se tratarán nociones básicas de categorías que son necesarias a lo largo del curso, haciendo énfasis en los ejemplos más utilizados a tales fines.

9.1.1 Definición de Categoría y ejemplos básicos

Daremos, en esta sección, la definición de categoría, y presentaremos varios ejemplos ilustrando la definición.

Definición 9.1.1. Definir una *categoría* $\mathcal{C}$ es dar los siguientes datos:

- Una clase (no necesariamente un conjunto) de objetos, que se denotará $\mathrm{Obj}(\mathcal{C})$.
- Para cada par de objetos X e Y de $\mathcal{C}$, un conjunto de flechas de X en Y, que se denotará $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ (o a veces $[X, Y]$, o $[X, Y]_{\mathcal{C}}$, o $\mathcal{C}(X, Y)$, o $Mor_{\mathcal{C}}[X, Y]$).

Estos satisfacen los siguientes axiomas:

C1: Si X, X', Y, Y' son objetos de $\mathcal{C}$ y o bien $X \neq X'$ o bien $Y \neq Y'$, entonces $\mathrm{Hom}_{\mathcal{C}}(X, Y) \neq \mathrm{Hom}_{\mathcal{C}}(X', Y')$.

C2: Para cada terna de objetos X, Y, Z de $\mathcal{C}$ está definida una función que llamaremos composición

$$\begin{aligned} \mathrm{Hom}_{\mathcal{C}}(Y,Z) \times \mathrm{Hom}_{\mathcal{C}}(X,Y) &\to \mathrm{Hom}_{\mathcal{C}}(X,Z) \\ (f,g) &\longmapsto f \circ g \end{aligned}$$

que es asociativa (en el sentido obvio).

C3: Para cualquier objeto X, existe un elemento de $\mathrm{Hom}_{\mathcal{C}}(X,X)$ que es un elemento neutro (tanto a derecha como a izquierda) con respecto a la composición de morfismos que salen de, o que llegan a X. Tal morfismo (se puede ver que es único) se denota Id_X.

Damos a continuación la notación para categorías usuales, señalando primero los objetos, y luego las flechas:

Ejemplos.
$\mathfrak{Sets}$ Conjuntos y funciones.

${}_k\mathfrak{Vect}$ (k un cuerpo), los k-espacios vectoriales y las transformaciones k-lineales.

${}_A\mathrm{Mod}$ (A un anillo), los A-módulos (por ejemplo a izquierda) y los morfismos de A-módulos.

$\mathfrak{G}$ Grupos y homomorfismos de grupos.

$\mathfrak{Ab}$ Grupos abelianos y homomorfismos de grupos.

${}^{\mathbb{Z}}_{A}\mathrm{Mod}$ Los A-módulos $\mathbb{Z}$-graduados, y los morfismos de A-módulos graduados.

$\mathfrak{Sets}_0$ Los pares (X, x_0) donde X es un conjunto no vacío y $x_0 \in X$, un morfismo $f : (X, x_0) \to (Y, y_0)$ es una función $f : X \to Y$ tal que $f(x_0) = y_0$.

$\mathfrak{Top}_0$ Los pares (X, x_0) donde X es un espacio topológico no vacío y $x_0 \in X$, un morfismo $f : (X, x_0) \to (Y, y_0)$ es una función continua $f : X \to Y$ tal que $f(x_0) = y_0$.

$\mathfrak{An}_1$ Anillos con 1, morfismos de anillos que preservan la unidad.

$\mathfrak{An}$ Anillos (no necesariamente unitarios), morfismos de anillos (i.e. funciones a la vez aditivas y multiplicativas).

$k - \mathfrak{Alg}$ k-álgebras (k es un anillo conmutativo con uno) y morfismos de k-álgebras.

$k - \mathfrak{Alg}\mathfrak{C}$ k-álgebras conmutativas.

$\mathcal{C}^{op}$ Dada una categoría $\mathcal{C}$, se define $\mathrm{Obj}(\mathcal{C}^{op}) = \mathrm{Obj}(\mathcal{C})$ y para cada par de objetos X e Y: $\mathrm{Hom}_{\mathcal{C}^{op}}(X, Y) := \mathrm{Hom}_{\mathcal{C}}(Y, X)$, y la composición $f \circ_{op} g := g \circ f$. Entonces $\mathcal{C}^{op}$ resulta también una categoría, que se denomina la *categoría opuesta*.

Otro ejemplo de categoría es aquella formada por los conjuntos ordenados como objetos, y las funciones crecientes como morfismos.

Por otro lado, si I es un conjunto ordenado, podemos definir una categoría tomando como objetos a los elementos de I y como flechas

$$\mathrm{Hom}(i, j) = \begin{cases} \{*\} & \text{si } i \leq j, \\ \varnothing & \text{si } i \text{ y } j \text{ no están relacionados.} \end{cases}$$

donde $\{*\}$ denota a un conjunto con un único elemento. La transitividad de la relación $\leq$ hace que la composición esté bien definida, y el hecho de que siempre $i \leq i$ asegura la existencia del morfismo identidad.

Si M es un monoide con elemento neutro, entonces la categoría con un único objeto $\{*\}$ y cuyas flechas están definidas de la forma $\mathrm{Hom}(\{*\}, \{*\}) = M$ resulta efectivamente una categoría, definiendo la composición de funciones como el producto en el monoide.

9.1.2 Isomorfismos, monomorfismos y epimorfismos categóricos

La definición más sencilla que se puede hacer a partir de los axiomas de categorías es la de isomorfismo:

Definición 9.1.2. Sea $\mathcal{C}$ una categoría, dos objetos X e Y de $\mathcal{C}$ se dirán *isomorfos* si existen morfismos $f : X \to Y$ y $g : Y \to X$ tales que $f \circ g = \mathsf{Id}_Y$ y $g \circ f = \mathsf{Id}_X$, en tal caso denotaremos $X \cong Y$.

Un isomorfismo en la categoría de conjuntos es una biyección, los isomorfismos en las categorías de grupos, también son los morfismos que son biyectivos, pues si una función es un morfismo de grupos y además es biyectiva, entonces la función inversa también resulta un morfismo de grupos. En la categoría de módulos sobre

un anillo fijo sucede lo mismo. Llamamos la atención sin embargo a que aún cuando se tenga una categoría en donde los objetos sean conjuntos provistos de alguna otra estructura adicional, y las flechas sean un subconjunto del conjunto funciones entre los objetos, la noción de isomorfismo no tiene por qué coincidir con la de biyección. Presentamos los siguientes dos ejemplos.

En la categoría de espacios topológicos, un isomorfismo es un homoeomorfismo, es decir, una función continua $f : X \to Y$ biyectiva con inversa $f^{-1} : Y \to X$ también continua.

Un ejemplo de biyección que no es un homeomorfismo es considerar un mismo conjunto, pero definir dos topologías diferentes en él, una contenida en la otra, digamos (X, τ) y (X, τ') en donde todo abierto de τ' pertenece a τ, pero con τ estrictamente mayor que τ'. Entonces la función identidad $(X, \tau) \to (X, \tau')$ es continua, pero su inversa, que es de nuevo la función identidad, en este caso vista como función de (X, τ') en (X, τ) no es continua. Observamos que esta función "identidad", en realidad es la función identidad de X, pero no la identidad de (X, τ).

Otro ejemplo es el caso de la categoría cuyos objetos son los elementos de un conjunto ordenado y cuyos morfismos son las funciones crecientes. Esta categoría se llamará un *poset*. Si $(X, \leq)$ es un conjunto ordenado con una relación de orden no trivial (es decir, tal que existen por lo menos dos elementos distintos x e y tales que $x \leq y$), definimos sobre X otra relación de orden, que está dada por $x \leq x$, $\forall x \in X$, y si $x \neq y$, entonces x no está relacionado con y; llamemos $\leq'$ a esta nueva relación. Si consideramos la función identidad de X, como morfismo $(X, \leq') \to (X, \leq)$, es una función (notar que como la relación $\leq'$ es trivial, cualquier función con dominio en X es creciente) y biyectiva, pero $(X, \leq') \ncong (X, \leq)$.

Sea $\mathcal{C}_M$ la categoría con un único objeto $\{*\}$, y $\mathrm{Hom}(\{*\}, \{*\}) = M$ donde M es un monoide con elemento identidad, entonces M es un grupo si y sólo si todo morfismo es un isomorfismo.

Además de la noción de isomorfismo, hay muchas otras definiciones que se pueden hacer en el contexto genérico de una categoría. La clave de estas definiciones es encontar una caracterización, en términos de diagramas de flechas, de la propiedad que uno quiere generalizar, es decir, de una noción que uno conoce en una categoría y desea contar con esa construcción en alguna otra categoría. Cualquier definición hecha con diagramas con flechas puede ser enun-

ciada en una categoría arbitraria, uno de los ejemplos más sencillos es la noción de monomorfismo y epimorfismo, que damos a continuación en forma de proposición, en las categorías de conjuntos, y de módulos:

Proposición 9.1.3. *Sea $f : X \to Y$ un morfismo en la categoría $\mathfrak{Sets}$ o ${}_A\mathrm{Mod}$ (donde A es un anillo fijo). Entonces f es inyectiva si y sólo si cada vez que $g, h : Z \to X$ son dos morfismos (en las respectivas categorías) tales que $f \circ h = f \circ g$, entonces $g = h$.*

Demostración: En la categoría de conjuntos esta proposición es obvia, en la categoría de módulos es la proposición 3.3.3 del capítulo 3.

Definición 9.1.4. Dada una categoría $\mathcal{C}$, un morfismo $f : X \to Y$ se dirá un *monomorfismo* si y sólo si, para todo objeto Z y para todo par de morfismos $g, h : Z \to X$ tales que $f \circ g = f \circ h$, entonces $g = h$.

Reescribiendo esta definición, tenemos la siguiente proposición:

Proposición 9.1.5. *Sea $f : X \to Y$ un morfismo en una categoría $\mathcal{C}$, entonces f es un monomorfismo si y sólo si, para todo objeto Z la función de conjuntos*

$$\begin{aligned} f_* : \mathrm{Hom}_{\mathcal{C}}(Z, X) &\to \mathrm{Hom}_{\mathcal{C}}(Z, Y) \\ h &\mapsto f \circ h \end{aligned}$$

es inyectiva.

La noción de monomorfismo categórico en la categoría de módulos coincide con la noción de monomorfismo definida anteriormente. Como ejemplos extremos podemos comentar que todo isomorfismo es un monomorfismo (verificarlo!), y en categorías donde el Hom sea o bien vacío o bien un conjunto unitario, todo morfismo es un monomorfismo.

Dejamos como ejercicio verificar que en la categoría de espacios topológicos y funciones continuas, los monomorfismos son las funciones continuas inyectivas. Sin embargo, como lo muestra el siguiente ejemplo, la noción de monomorfismo categórico no tiene por qué coincidir con la de inyectividad.

Ejemplo. Consideremos la categoría formada por los grupos abelianos divisibles y los homomorfismos de grupos. La proyección al

cociente $p : \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ es un morfismo en esta categoría pues tanto $\mathbb{Q}$ como $\mathbb{Q}/\mathbb{Z}$ son divisibles. Claramente la proyección al cociente no es una función inyectiva, sin embargo afirmamos que es un monomorfismo en esta categoría. Para ello consideremos un grupo abeliano divisible G y dos morfismos de grupos $f, g : G \to \mathbb{Q}$, supongamos que $f \neq g$, veremos entonces que necesariamente $p \circ f \neq p \circ g$.

Como $f \neq g$, existe $x \in G$ tal que $f(x) - g(x) = \frac{r}{s}$ con r y s números enteros distintos de cero. Como G es divisible, existe $x' \in G$ tal que $rx' = x$, cambiando x por x' podemos suponer que $r = 1$. Con similar argumento, el elemento x puede siempre elegirse de manera tal que $s \neq \pm 1$, de esta manera, la clase de $\frac{1}{s}$ en $\mathbb{Q}/\mathbb{Z}$ es distinta de cero, es decir $(p \circ f)(x) \neq (p \circ g)(x)$.

La noción de epimorfismo es la noción "dual" de monomorfismo. Dado un enunciado a través de flechas, uno siempre puede dar vuelta el sentido de las flechas y así obtener un nuevo enunciado que se suele llamar enunciado dual. Más formalmente, una definición dual en una categoría $\mathcal{C}$ no es otra cosa que la misma definición pero enunciada en la categoría $\mathcal{C}^{op}$.

Definición 9.1.6. Sea $f : X \to Y$ un morfismo en una categoría $\mathcal{C}$, diremos que f es un *epimorfismo* en caso de que para todo objeto Z, dados dos morfismos $g, h : Y \to Z$ tales que $g \circ f = h \circ f$, entonces $g = h$.

La definición puede reformularse de la siguiente manera:

Proposición 9.1.7. *Sea $f : X \to Y$ un morfismo en una categoría $\mathcal{C}$. Son equivalentes:*

1. *f es un epimorfismo.*
2. *Para todo objeto Z, la función de conjuntos*

$$\begin{aligned} f^* : \mathrm{Hom}_{\mathcal{C}}(X, Z) &\to \mathrm{Hom}_{\mathcal{C}}(Y, Z) \\ h &\longmapsto h \circ f \end{aligned}$$

   es inyectiva.
3. *$f \in \mathrm{Hom}_{\mathcal{C}}(X, Y) = \mathrm{Hom}_{\mathcal{C}^{op}}(Y, X)$ es un monomorfismo en $\mathcal{C}^{op}$.*

Todo isomorfismo es un epimorfismo. En la categoría de conjuntos, un epimorfismo es una función suryectiva (verificarlo!), lo

mismo sucede en la categoría de módulos (ver Proposición 3.4.4 del capítulo 3).

Damos a continuación varios ejemplos cuya verificación quedará como ejercicio.

Ejemplos.

1. En la categoría cuyos objetos son los espacios métricos y cuyos morfismos son las funciones continuas, aquellas funciones continuas con imagen densa son epimorfismos categóricos. Este ejemplo muestra a su vez que la noción de isomorfismo no tiene por qué coincidir con la de un morfismo que sea simultáneamente mono y epi.

2. En la categoría de anillos unitarios, la incusión $\mathbb{Z} \to \mathbb{Q}$ es un epimorfismo categórico (otro ejemplo en donde "epi" no significa suryectividad).

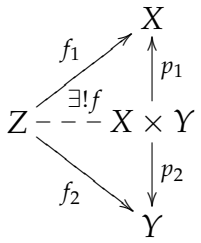
3. Si consideramos el ejemplo de categoría en donde la colección de sus objetos forma un conjunto ordenado, y entre un objeto i y otro j hay un (único) morfismo si y sólo si $i \leq j$, como los conjuntos $\mathrm{Hom}(\{i\}, \{j\})$ son o bien vacíos o bien unitarios, entonces todo morfismo es un epimorfismo. Notar que esta es una categoría en donde todo morfismo es a la vez monomorfismo y epimorfismo sin necesidad de que todo morfismo sea isomorfismo. ¿Para qué relaciones de orden todo morfismo es un isomorfismo?

9.2 Límites y Colímites

9.2.1 Productos

Si X e Y son dos conjuntos, el producto cartesiano $X \times Y$ es el conjunto de pares $\{(x, y) \ / \ x \in X, y \in Y\}$. Se observa que toda función de un conjunto Z en $X \times Y$ queda determinada de manera única por una función de Z en X y otra de Z en Y pues si $f : Z \to X \times Y$, dado $z \in Z$, $f(z) \in X \times Y$, luego es de la forma $f(z) = (f_1(z), f_2(z))$. La función f_1 se consigue componiendo f con la proyección $p_1 : X \times Y \to X$, $((x, y) \mapsto x)$, análogamente f_2 componiendo f con la proyección $p_2 : X \times Y \to Y$. Dicho en forma de

diagrama:



Es decir, dadas $f_1 : Z \to X$ y $f_2 : Z \to Y$, existe una única función $f : Z \to X \times Y$ tal que $f_i = p_i \circ f$, $i = 1, 2$.

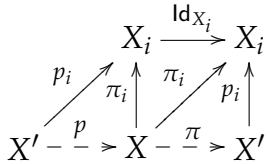
Esto último permite generalizar la noción de producto cartesiano a una categoría $\mathcal{C}$, obteniéndose:

Definición 9.2.1. Dada una familia $\{X_i\}_{i \in I}$ de objetos de una categoría $\mathcal{C}$, se define un *producto directo* $\prod_{i \in I} X_i$ como un objeto de $\mathcal{C}$ con las siguientes dos propiedades:

- $\forall j \in I$, existe un morfismo $p_j : \prod_{i \in I} X_i \to X_j$.
- (Propiedad universal) Si $Z \in \mathrm{Obj}(\mathcal{C})$ y para todo $j \in I$ se tiene dado un morfismo $f_j : Z \to X_j$, entonces existe un único morfismo $f : Z \to \prod_{i \in I} X_i$ tal que $f_i = p_i \circ f$ para todo $i \in I$.

Observación. Dados $\{X_i\}_{i \in I} \in \mathcal{C}$, si un objeto producto existe, entonces es único a menos de isomorfismos, por lo tanto puede hablarse (suponiendo que exista) de *el* objeto producto directo.

Demostración. Sean $(X, \{\pi_i : X \to X_i\})$, $(X', \{p_i : X \to X_i\})$ dos objetos producto. Por la propiedad universal del producto de X, al tener definidas flechas $p_i : X' \to X_i$ queda definida una única flecha $p : X' \to X$ tal que $\pi_i \circ p = p_i$. Simétricamente, como X' también es un producto, usando las flechas $\pi_i : X \to X_i$ queda definida una única flecha $\pi : X \to X'$ tal que $p_i \circ \pi = \pi_i$.

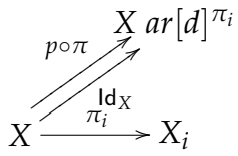


Afirmamos que estos morfismos son isomorfismos, uno el inverso del otro. Para ver ésto, consideramos la composición $p \circ \pi : X \to X$.

Al calcular la composición con las proyecciones tenemos las igualdades:

$$\pi_i \circ (p \circ \pi) = (\pi_i \circ p) \circ \pi = p_i \circ \pi = \pi_i = \pi_i \circ \mathsf{Id}_X.$$

Es decir, el diagrama siguiente conmuta usando cualquiera de las dos flechas.



Luego, por unicidad, tiene que ser $p \circ \pi = \mathsf{Id}_X$. La otra composición es análoga. □

Todo morfismo $f : X \to Y$ entre dos objetos de una categoría $\mathcal{C}$ induce, por composición, para cada objeto Z de $\mathcal{C}$, una función entre los conjuntos $f_* : \mathrm{Hom}_{\mathcal{C}}(Z, X) \to \mathrm{Hom}_{\mathcal{C}}(Z, Y)$. Si ahora uno tiene un objeto $\prod_{i\in I} X_i$ y para cada $j \in I$ morfismos $p_j : \prod_{i\in I} X_i \to X_j$, ésto induce para cada objeto Z funciones $(p_j)_* : \mathrm{Hom}_{\mathcal{C}}(Z, \prod_{i\in I} X_i) \to \mathrm{Hom}_{\mathcal{C}}(Z, X_j)$. Ahora bien, estas aplicaciones son funciones entre conjuntos, y en la categoría de conjuntos uno sabe qué es el producto cartesiano, luego tener una familia de funciones, una por cada coordenada, equivale a tener una función que llegue al producto cartesiano. Se puede comprobar sin dificultad que una definición equivalente de producto en una categoría $\mathcal{C}$ puede ser enunciada de la siguiente manera:

Proposición 9.2.2. *El par* $\left(\prod_{i\in I} X_i, \{p_j : \prod_{i\in I} X_i \to X_j\}_{j\in I}\right)$ *es un producto de la familia* $\{X_i\}_{i\in I}$ *en* $\mathcal{C}$ *si y sólo si la función natural*

$$\prod_{i\in I}(p_i)_* : \mathrm{Hom}_{\mathcal{C}}(Z, \prod_{i\in I} X_i) \to \prod_{i\in I} \mathrm{Hom}_{\mathcal{C}}(Z, X_i)$$
$$f \mapsto \{p_i \circ f\}_{i\in I}$$

es una biyección para todo $Z \in \mathrm{Obj}(\mathcal{C})$.

Demostración. que la función natural de la proposición sea suryectiva es precisamente la parte de "existencia" de la definición de producto, la parte de "unicidad" corresponde a que la función entre sea inyectiva. □

Ejemplos.

1. En la categorías de conjuntos, módulos sobre un anillo, anillos, grupos (conmutativos o no), el producto categórico es el producto cartesiano, pero ésto no tiene por qué ser siempre así. Consideremos, dado un cuerpo k, la categoría de k-espacios vectoriales $\mathbb{Z}$-graduados, donde los objetos son espacios vectoriales provistos de una descomposición $V = \oplus_{n\in\mathbb{Z}} V_n$, y los morfismos son transformaciones lineales que respetan la graduación, es decir, dados $V = \bigoplus_{n\in\mathbb{Z}} V_n$ y $W = \bigoplus_{n\in\mathbb{Z}} W_n$ dos espacios vectoriales graduados, $\mathrm{Hom}_{\mathcal{C}}(V, W) = \{f : V \to W \ k\text{-lineales tales que } f(V_n) \subseteq W_n \ \forall\ n \in \mathbb{Z}\}$. Respetar la graduación es estable por composición, y el morfismo identidad obviamente respeta la graduación, por lo tanto los espacios vectoriales graduados junto con los morfismos graduados forman una categoría. Se puede probar fácilmente (verificarlo!) que el producto en esta categoría existe, y se calcula coordenada a coordenada, es decir, si $\{V^i\}_{i\in I}$ es una familia de espacios vectoriales graduados, entonces el objeto $\oplus_{n\in\mathbb{Z}}(\prod_{i\in I} V_n^i)$ es el producto categórico.

Si definimos $k[n]$ como el espacio vectorial graduado que en grado n tiene a k y cero en los demás grados, entonces el producto categórico de $\{k[n]\}_{n\in\mathbb{Z}}$ es un espacio vectorial graduado con un espacio vectorial de dimensión uno en cada grado, es decir es que es isomorfo a $k^{(\mathbb{Z})}$. Si en cambio olvidamos la graduación, el producto en la categoría de espacios vectoriales (o en la categoría de conjuntos) de los $k[n]$ es $k^{\mathbb{Z}}$, que contiene estrictamente a $k^{(\mathbb{Z})}$.

2. Otro ejemplo en donde el producto no se calcula como el producto cartesiano es el de la categoría en donde los objetos forman un conjunto ordenado, y en donde existe una (única) flecha $i \to j$ si y sólo si $i \leq j$. Si $(k \to i, k \to j)$ es un producto, esto significa, por un lado que $k \leq i$ y que $k \leq j$, además la condición de la propiedad universal afirma que si existen flechas $k' \to i$ y $k' \to j$, entonces existe una única flecha $k' \to k$ haciendo conmutar el correspondiente diagrama. Traduciendo "existe una flecha" por "es menor o igual que", la propiedad universal se traduce en "dado un $k' \leq i$ y $k' \leq j$, entonces $k' \leq k$; en otras palabras, el producto de i y j no es otra cosa que el ínfimo entre i y j, que nada tiene que ver con productos cartesianos. Este ejemplo muestra además que los productos categóricos no necesariamente existen.

9.2.2 Coproductos

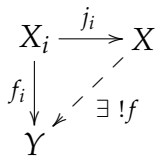
Definición 9.2.3. Sea $\{j_i : X_i \to X\}_{i\in I}$ una familia de morfismos en una categoría $\mathcal{C}$ indexada por un conjunto I. Diremos que X (junto con los morfismos j_i) es el *coproducto* de los X_i si y sólo si la familia $\{j_i : X \to X_i\}_{i\in I}$ es un producto en la categoría $\mathcal{C}^{op}$, se denotará $X := \coprod_{i\in I} X_i$.

Enunciamos la siguiente proposición, cuya demostración es obvia.

Proposición 9.2.4. *Dada una familia $\{X_i\}_{i\in I}$ de objetos de $\mathcal{C}$, si un coproducto existe, entonces es único a menos de isomorfismo.*

Proposición 9.2.5. *Sea $\{X_i\}_{i\in I}$ un conjunto de objetos de una categoría $\mathcal{C}$, X un objeto de $\mathcal{C}$ y $j_i : X_i \to X$ morfismos; son equivalentes:*

- *X es el coproducto de los X_i.*
- *Para cualquier objeto Y de $\mathcal{C}$ y cualquier familia de morfismos $f_i : X_i \to Y$, existe un único morfismo $f : X \to Y$ tal que $f \circ j_i = f_i$*



- *Dado cualquier objeto Y en $\mathcal{C}$, la función natural*

$$\prod_{i\in I} j_i^* : \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \prod_{i\in I} \mathrm{Hom}_{\mathcal{C}}(X_i, Y)$$

  es una biyección.

Demostración. Se deja como ejercicio. □

Ejemplos.
1. En la categoría de conjuntos, y en la categoría de espacios topológicos, el coproducto es la unión disjunta.

2. En la categoría de módulos sobre un anillo, el coproducto es la suma directa.

3. En la categoría de grupos (no necesariamente conmutativos), el coproducto de dos grupos G y H *no* es el producto cartesiano $G \times H$ (para demostrar esto, encuentre un contraejemplo, basándose en que los elementos de G conmutan con los de H en $G \times H$).

4. En la categoría de anillos conmutativos con uno, el coproducto es el producto tensorial sobre $\mathbb{Z}$.

5. En la categoría de anillos con uno (no necesariamente conmutativos) el producto tensorial sobre $\mathbb{Z}$ *no* es el coproducto (compare con la categoría de grupos).

6. En la categoría en donde los objetos forman un conjunto ordenado y existe una (única) flecha $i \to j$ si y sólo si $i \leq j$, el coproducto entre dos elementos i y j es el supremo y por lo tanto no siempre existe.

9.2.3 Objeto inicial, objeto final, Ker y Coker

En una categoría $\mathcal{C}$, un objeto I se denomina *inicial* en caso de que, dado cualquier otro objeto X de $\mathcal{C}$, exista un único morfismo $I \to X$. Como es de esperar, un objeto inicial, si existe, es único salvo isomorfismo. Para ver ésto, si J es otro objeto inicial, existe un único morfismo, llamémoslo $j : J \to I$. Por otro lado existe un único morfismo $i : I \to J$. Si componemos estos dos morfismos $j \circ i : I \to I$ obtenemos un morfismo de I en I, pero como I es un objeto inicial, el conjunto de morfismos de I en I contiene un único elemento, luego ese único elemento tiene que coincidir con $j \circ i$. A su vez, $\mathsf{Id}_I : I \to I$, luego por unicidad, $j \circ i = \mathsf{Id}_I$. La cuenta para ver que $i \circ j = \mathsf{Id}_J$ es similar.

Ejemplos.
1. En la categoría de conjuntos y en la categoría de espacios topológicos, el conjunto vacío es el objeto inicial.

2. En la categoría de espacios topológicos con punto de base, el par $(\{x_0\}, x_0)$ es un objeto inicial.

3. En la categoría de módulos sobre un anillo, el módulo $\{0\}$ es un objeto inicial. El grupo $\{e_G\}$ es el objeto inicial en la categoría de grupos.

4. En la categoría de anillos con uno (no necesariamente conmuta-

tivos), $\mathbb{Z}$ es un objeto inicial.

5. En la categoría en donde los objetos forman un conjunto ordenado y existe una única flecha $i \to j$ si y sólo si $i \leq j$, un objeto inicial es el mínimo. Este podría no existir.

Dualmente, un objeto F en $\mathrm{Obj}(\mathcal{C})$ se llama objeto *final* si, para cualquier otro objeto X de $\mathcal{C}$ existe un único morfismo $X \to F$.

Ejercicio. Dada una categoría $\mathcal{C}$, un objeto F es final si y sólo si F es un objeto inicial en $\mathcal{C}^{op}$. Si una categoría $\mathcal{C}$ tiene un objeto final, éste es único salvo isomorfismo.

Ejemplos.
1. En la categoría de conjuntos y de espacios topológicos un conjunto unitario es un objeto final.

2. En la categoría de espacios topológicos con punto de base, el par $(\{x_0\}, x_0)$ es un objeto final.

3. En la categoría de módulos sobre un anillo, el módulo $\{0\}$ es un objeto final. El grupo $\{e_G\}$ es un objeto final en la categoría de grupos.

4. En la categoría de anillos con uno el conjunto $\{0\}$ es un objeto final (en el anillo $\{0\}$, $1 = 0$).

5. En la categoría en donde los objetos forman un conjunto ordenado y existe una (única) flecha $i \to j$ si y sólo si $i \leq j$, la noción de objeto final coincide con la de máximo.

Notamos que a veces el objeto inicial coincide con el objeto final, y otras veces no. Una categoría se dice que tiene *objeto cero* en caso de que tenga objeto inicial, objeto final, y que éstos coincidan. Las categorías de módulos sobre algún anillo, así como la categoría de grupos y la categoría de conjuntos (o espacios topológicos) con punto de base tienen objeto 0, no así la de conjuntos o de espacios topológicos, ni la de anillos. En una categoría con objeto cero se puede definir la noción de núcleo y dualmente de conúcleo. Observar que la noción de objeto cero es autodual, es decir, $\mathcal{C}$ tiene objeto 0 si y sólo si $\mathcal{C}^{op}$ tiene objeto cero, y el cero de $\mathcal{C}$ sirve como cero de $\mathcal{C}^{op}$.

Observación. Sea $\mathcal{C}$ una categoría con objeto cero, entonces, dado un par de objetos X e Y, el conjunto $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ nunca es vacío

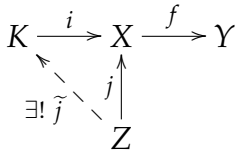
pues siempre existe el morfismo composición:

$$X \to 0 \to Y$$

La existencia de $X \to 0$ se debe a que 0 es objeto final, y la existencia del morfismo $0 \to Y$ se debe a que 0 es también un objeto inicial. El morfismo $X \to Y$ definido de esta manera se llama morfismo cero, y se lo denota también 0.

Definición 9.2.6. Sea $f : X \to Y$ un morfismo en una categoría $\mathcal{C}$ con objeto cero, un morfismo $i : K \to X$ se dice un *núcleo* de f en caso de que:

- $f \circ i = 0$.
- Si $j : Z \to X$ es un morfismo tal que $f \circ j = 0$, entonces existe un único morfismo $\widetilde{j} : Z \to K$ tal que $i \circ \widetilde{j} = j$. En forma de diagrama:



Se deja como ejercicio verificar que si un morfismo $f : X \to Y$ admite núcleo, éste es único salvo isomorfismo, este objeto se denomina $\mathrm{Ker}(f)$, y la flecha $\mathrm{Ker}(f) \to X$ se suele denominar $ker(f)$.

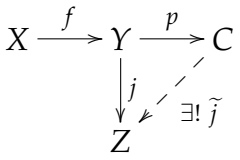
Comparando esta definición con la propiedad universal del núcleo en el contexto de grupos y de módulos, vemos que la noción de núcleo categórico dada aquí coincide, en estos casos, con la noción habitual de núcleo.

La noción de conúcleo es dual a la de núcleo:

Definición 9.2.7. Sea $f : X \to Y$ un morfismo en una categoría $\mathcal{C}$ con objeto cero, un morfismo $p : Y \to C$ se dice un *conúcleo* de f en caso de que:

- $p \circ f = 0$.
- Si $j : Y \to Z$ es un morfismo tal que $j \circ f = 0$, entonces existe un único morfismo $\widetilde{j} : C \to Z$ tal que $\widetilde{j} \circ p = j$. El diagrama

correspondiente es:



Ejercicio. Dada $f : X \to Y$, un morfismo $p : Y \to C$ es un conúcleo de f en $\mathcal{C}$ si y sólo si $p : C \to Y$ es un núcleo de $f : Y \to X$ en $\mathcal{C}^{op}$. Si una flecha f admite conúcleo, éste es único salvo isomorfismo.

Al igual que en caso de núcleo, el objeto conúcleo se suele denotar $\mathrm{Coker}(f)$, y el morfismo se denota en letras minúsculas.

En la categoría de módulos sobre un anillo, dado un morfismo $f : M \to N$, el conúcleo de f es la proyección $\pi : N \to N/\operatorname{Im}(f)$. En la categoría de grupos, si $f : G \to H$ es un morfismo de grupos, el conúcleo es la proyección al cociente $H \to H/N(\operatorname{Im}(f))$, donde $N(\operatorname{Im}(f))$ es el normalizador de $\operatorname{Im}(f)$ en H, es decir, el subgrupo normal más chico que contiene a $\operatorname{Im}(f)$ (que eventualmente puede contener estrictamente a $\operatorname{Im}(f)$).

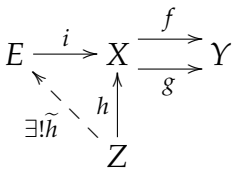
Si $f : (X, x_0) \to (Y, y_0)$ es un morfismo en la categoría $\mathfrak{Sets}_0$ (es decir, $f : X \to Y$ es una función tal que $f(x_0) = y_0$), se puede comprobar fácilmente que $\mathrm{Ker}(f) = (\{x \in X \,/\, f(x) = y_0\}, x_0)$, y $\mathrm{Coker}(f) = (Y/\sim, \overline{y_0})$ donde la relación de equivalencia $\sim$ está definida por $f(x) \sim y_0 \ \forall x \in X$.

9.2.4 Egalizadores y coegalizadores

Si consideramos intuitivamente los núcleos como los objetos formados por elementos que verifican una igualdad, y los conúcleos como cocientes, resulta natural generalizar estas construcciones a otras categorías en donde la noción de cero no exista pero si exista una noción de "ecuación" o igualdad, así como también a categorías en donde exista la noción de cociente por una relación de equivalencia.

Definición 9.2.8. Sean $f, g : X \to Y$ dos morfismos en una categoría cualquiera $\mathcal{C}$. Llamaremos un *egalizador* de f y g a un objeto E provisto de un morfismo $i : E \to X$ tal que $f \circ i = g \circ i$, que sea universal con respecto a esa propiedad. Más precisamente, si

$h : Z \to X$ es un morfismo tal que $f \circ h = g \circ h$, entonces existe un único morfismo $\widetilde{h} : Z \to E$ tal que $h = i \circ \widetilde{h}$

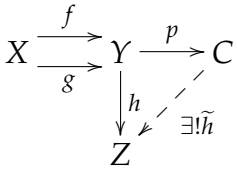


Ejercicios.
1. Si dos morfismos $f, g : X \to Y$ admiten egalizador, éste es único a menos de isomorfismo.

2. Si la categoría admite objeto cero y $f : X \to Y$, entonces $\mathrm{Ker}(f)$ coincide con el egalizador de los morfismos $f, 0 : X \to Y$.

La noción de coegalizador es la dual:

Definición 9.2.9. Sean $f, g : X \to Y$ dos morfismos en una categoría cualquiera $\mathcal{C}$. Llamaremos un *coegalizador* de f y g a un objeto C provisto de un morfismo $p : Y \to C$ tal que $p \circ f = p \circ g$ y que sea universal con respecto a esa propiedad. Más precisamente, si $h : Y \to Z$ es un morfismo tal que $p \circ f = p \circ g$, entonces existe un único morfismo $\widetilde{h} : C \to Z$ tal que $h = \widetilde{h} \circ p$



Ejercicios.
1. Si dos morfismos $f, g : X \to Y$ admiten coegalizador, éste es único a menos de isomorfismo.

2. Si la categoría admite objeto cero y $f : X \to Y$, entonces $\mathrm{Coker}(f)$ coincide con el coegalizador de los morfismos $f, 0 : X \to Y$.

3. Si $f, g : X \to Y$ son dos morfismos en la categoría de conjuntos, entonces el egalizador de f y g consiste en el cociente de Y por la relación de equivalencia $y \sim y' \iff \exists\, x \in X$ tal que o bien $y = f(x)$ e $y' = g(x)$, o bien $y = g(x)$ e $y' = f(x)$.

4. Si $f, g : M \to N$ son dos morfismos entre dos módulos sobre un anillo A, entonces el coegalizador de f y g es $N/\langle f(m) - g(m) \ : \ m \in M\rangle$.

9.2.5 Push-outs y pull-backs (productos fibrados y cuadrados cartesianos)

La noción de coproducto se utiliza frecuentemente para construir un objeto a partir de otros dos, pero puede ocurrir que un objeto quede determinado por un par de subobjetos sin ser necesariamente su coproducto. Ilustrando este hecho, podemos considerar un módulo M generado por dos submódulos M_1 y M_2, tales que $M_1 \cap M_2 \neq \{0\}$, y por lo tanto $M \neq M_1 \oplus M_2$, o bien un conjunto X que sea la unión de dos subconjuntos Y y Z, donde esta unión no sea necesariamente disjunta.

En el caso de los conjuntos, si se desea definir una función con dominio el conjunto $X = Y \cup Z$, es claro que basta definirla por un lado en Y y por otro lado en Z, pero como puede haber puntos en común, las funciones definidas por separado deben coincidir en $Z \cap Y$.

En el caso de módulos la situación es similar, si se tienen definidos morfismos $f_1 : M_1 \to N$ y $f_2 : M_2 \to N$, y $M = M_1 + M_2$, la condición para que f esté definida en M se puede deducir de la siguiente manera:

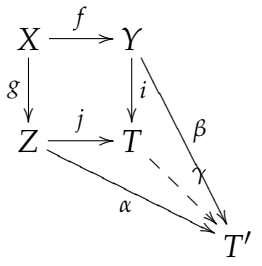
Como $M = M_1 + M_2$, las inclusiones $M_1 \hookrightarrow M$ y $M_2 \hookrightarrow M$ definen un único morfismo $M_1 \oplus M_2 \to M$ que es un epimorfismo. Por lo tanto M es un cociente de $M_1 \oplus M_2$. Si un par $(m_1, m_2) \in M_1 \oplus M_2$ es tal que $m_1 + m_2 = 0$ en M, o lo que es lo mismo $m_1 = -m_2$, como $m_1 \in M_1$ y $m_2 \in M_2$ se sigue que m_1 y m_2 son elementos de $M_1 \cap M_2$, luego $\mathrm{Ker}(M_1 \oplus M_2 \to M) = \{(m, -m) \ : \ m \in M_1 \cap M_2\}$. Si $f_1 \oplus f_2 : M_1 \oplus M_2 \to N$, la condición para que esta función pase al cociente es que se anule en el núcleo, es decir que $(f_1 \oplus f_2)(m, -m) = 0 \ \forall \ m \in M_1 \cap M_2 \iff f_1(m) + f_2(-m) = 0 \ \forall \ m \in M_1 \cap M_2$, o lo que es equivalente, si y sólo si f_1 y f_2 coinciden donde coinciden sus dominios.

Esta noción de construir un objeto a través de dos partes, que pueden tener relaciones entre ellas, es la que se formaliza categóricamente a través de la definición de push-out:

Definición 9.2.10. Sean $f : X \to Y$ y $g : X \to Z$ dos morfismos en una categoría $\mathcal{C}$ (ver diagrama).

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle g}\downarrow & & \\ Z & & \end{array}$$

Un objeto T, junto con dos morfismos $i : Y \to T$ y $j : Z \to T$ se llama un *push-out* de f y g en $\mathcal{C}$ si verifica las siguientes dos condiciones: 1) $i \circ f = j \circ g$, y 2) es universal con respecto a esa propiedad, es decir, dado un diagrama conmutativo de flechas llenas como el siguiente, siempre puede completarse de manera única y conmutativa con la flecha punteada:



El push-out de un diagrama $\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle g}\downarrow & & \\ Z & & \end{array}$ se denotará $Z \coprod_X Y$.

Ejercicios.

1. Sea X un conjunto, Y y Z dos subconjuntos de X. Demuestre que $\begin{array}{ccc} Y \cap Z & \rightarrowtail & Y \\ \downarrow & & \downarrow \\ Z & \rightarrowtail & Y \cup Z \end{array}$ es un cuadrado push-out.

2. Sea I un objeto inicial en una categoría $\mathcal{C}$ con coproductos, X e Y dos objetos de $\mathcal{C}$, entonces el pushout de $\begin{array}{ccc} I & \longrightarrow & X \\ \downarrow & & \\ Y & & \end{array}$ es $X \coprod Y$.

3. Sea $\mathcal{C}$ una categoría que admite coproductos y coegalizadores, entonces el push-out de dos morfismos $f : X \to Y$ y $g : X \to Z$ se calcula como el coegalizador de $i_Y \circ f : X \to Y \coprod Z$ y $i_Z \circ f : X \to Y \coprod Z$.

4. Calcule explícitamente el push-out en la categoría de módulos.

5. Ver que en la categoría de módulos, un diagrama $\begin{array}{ccc} M & \xrightarrow{f} & N \\ \downarrow & & \downarrow g \\ 0 & \longrightarrow & T \end{array}$ es un cuadrado push-out si y sólo si la siguiente sucesión es exacta

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$$

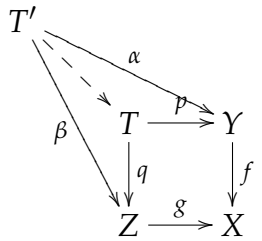
6. Describir al coegalizador como la "composición" de dos push-outs.

La noción de pull-back es el concepto dual:

Definición 9.2.11. Sean $f : Y \to X$ y $g : Z \to X$ dos morfismos en una categoría $\mathcal{C}$ (ver diagrama).

$$\begin{array}{ccc} & & Y \\ & & \downarrow f \\ Z & \xrightarrow{g} & X \end{array}$$

Un objeto T, junto con dos morfismos $p : T \to Y$ y $q : T \to Z$ se llama un *pull-back* de f y g en $\mathcal{C}$ si satisface las dos condiciones siguientes: 1) $f \circ p = g \circ q$, y 2) es universal con respecto a esa propiedad, es decir, dado un diagrama conmutativo de flechas llenas como el siguiente, siempre se pueda completar de manera única y conmutativa con la flecha punteada:



El pull-back de un diagrama $\begin{array}{ccc} & & Y \\ & & \downarrow f \\ Z & \xrightarrow{g} & X \end{array}$ se denotará $Z \prod_X Y$.

Ejercicios.

1. Sea $\mathcal{C}$ una categoría que admite productos y egalizadores, entonces el pull-back de dos morfismos $f : Y \to X$ y $g : Z \to X$ se calcula como el egalizador de $f \circ p_Y : Y \prod Z \to X$ y $f \circ p_Z : Y \prod Z \to X$.

2. Describir el pull-back en la categoría de conjuntos y en la de módulos.

3. Describa el pull-back en la categoría de espacios topológicos.

4. Sea $\begin{array}{ccc} T & \to & Y \\ \downarrow & & \downarrow \\ Z & \to & X \end{array}$ un cuadrado conmutativo en una categoría $\mathcal{C}$. Ver que es un cuadrado push-out (respectivamente pull-back) si y sólo si para todo objeto W en $\mathcal{C}$, aplicando $\mathrm{Hom}_{\mathcal{C}}(-, W)$ (respectivamente $\mathrm{Hom}_{\mathcal{C}}(W, -)$) queda un cuadrado pull-back en la categoría de conjuntos.

5. Sea $f : X \to Y$ un morfismo en una categoría cualquiera. Probar que f es un monomorfismo si y sólo si el diagrama $\begin{array}{ccc} X & \xrightarrow{\mathrm{Id}} & X \\ {\scriptstyle \mathrm{Id}}\downarrow & & \downarrow{\scriptstyle f} \\ X & \xrightarrow[f]{} & Y \end{array}$ es un pull-back.

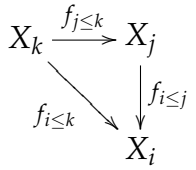
6. Enunciar y demostrar la versión dual del ejercicio anterior, con epimorfismos y push-outs.

9.2.6 Límites

Daremos en esta sección la definición de límite (o límite inverso, o límite proyectivo) y la de colímite (o límite directo, o límite inductivo). Estas son nociones categóricas. En categorías concretas, como la categoría de conjuntos o de módulos sobre un anillo, la parte de los datos que corresponde a los objetos puede interpretarse como las piezas con las que se construye el objeto límite, y las flechas como las relaciones que se le imponen. La noción de límite inverso generaliza la de producto, egalizador, y objeto final, la noción de colímite es la noción dual a la de límite, y como es de esperar generaliza la noción de coproducto, coegalizador y objeto inicial.

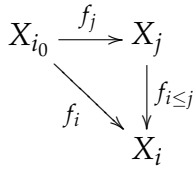
Para fijar ideas, comenzamos con la construcción del límite en la categoría de conjuntos.

Consideremos un conjunto parcialmente ordenado $(I, \leq)$ (que puede ser vacío), una familia de conjuntos $\{X_i\}_{i \in I}$ y por cada $i \leq j$ una función $f_{i \leq j} : X_j \to X_i$. A estos datos les pedimos la siguiente condición de compatibilidad: si $i \leq j \leq k$, entonces $f_{i \leq j} \circ f_{j \leq k} = f_{i \leq k}$ es decir, cada vez que hay tres elementos i, j, k de I tales que $i \leq j \leq k$, entonces el siguiente es un diagrama conmutativo:



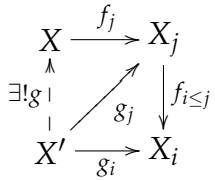
A un conjunto de datos con esas propiedades se lo llamará un *sistema proyectivo*. Notemos que si elegimos una familia de funciones entre varios conjuntos, esta familia siempre está parcialmente ordenada diciendo que una función f es menor o igual que otra función g si y sólo si son "componibles", es decir, si el codominio de f coincide con el dominio de g, luego, tratándose de datos que contienen una familia de funciones, resulta natural indexarlos por un conjunto parcialmente ordenado.

Lo que se busca es agregarle un supremo al conjunto parcialmente ordenado I, lo cual significaría agregar un conjunto X_{i_0} en donde, para todo $i \in I$ estén definidas funciones $f_i : X_{i_0} \to X_i$ (i.e. que $i_0 \geq i \; \forall \; i \in I$), y que el conjunto $I \cup \{i_0\}$ siga siendo un sistema compatible, es decir, que para cada $i \leq j$, los diagramas que se agregan



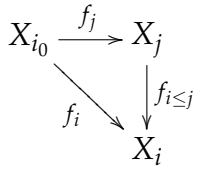
sean conmutativos. Queremos además que este conjunto X_{i_0} sea lo más grande posible, es decir, que si un conjunto X' tiene definidas funciones $g_i : X' \to X_i$ compatibles con la relación de orden de I,

entonces estas funciones se factoricen a través de X (ver diagrama).



La construcción de un conjunto X_{i_0} con tales propiedades puede ser dada como sigue.

Definir, para cada $i \in I$, una función de X en X_i es equivalente a definir una función $f : X \to \prod_{i\in I} X_i$. Si además, para cada $i \leq j$, el diagrama



es conmutativo, entonces la imagen de $f : X \to \prod_{i\in I} X_i$ está necesariamente contenida en el subconjunto $\{(x_i)_{i\in I} \ : \ f_{i\leq j}(x_j) = x_i \ \forall i \leq j\}$. Llamamos $\lim\limits_{\leftarrow I} X_i$ a este subconjunto del producto, y definimos $f_i : \lim\limits_{\leftarrow I} X_i \to X_i$ a la composición de la inclusión del límite en el producto con la proyección en la coordenada i-ésima:

$$\lim_{\leftarrow I} X_i \hookrightarrow \prod_{i\in I} X_i \longrightarrow X_i$$

Por construcción, queda demostrada la siguiente proposición:

Proposición 9.2.12. *(Propiedad universal del límite) Sean I un conjunto parcialmente ordenado y $\{f_{i\leq j} : X_j \to X_i\}_{i,j\in I,\ i\leq j}$ un sistema proyectivo, entonces:*

- *Las funciones $f_i : \lim\limits_{\leftarrow I} X_i \to X_i$ verifican que para todo $i \leq j$, $f_{i\leq j} \circ f_j = f_i$.*
- *Si $\{g_i : Y \to X_i\}$ es un conjunto de funciones que verifican que para todo $i \leq j$, $f_{i\leq j} \circ g_j = g_i$, entonces existe una única función $g : Y \to \lim\limits_{\leftarrow I} X_i$ tal que $g_i = f_i \circ g$*

La proposición anterior sirve como definición (en caso de que exista) del **límite** de un sistema proyectivo de morfismos en una categoría arbitraria.

Dejamos como ejercicio la demostración del siguiente resultado.

Proposición 9.2.13. *Dados un conjunto parcialmente ordenado I, y un sistema proyectivo $\{f_{i\leq j} : X_j \to X_i\}$, un objeto X es el límite de este sistema si y sólo si, para cada objeto Y, $\mathrm{Hom}_{\mathcal{C}}(Y, X)$ es el límite (en la categoría de conjuntos) del sistema proyectivo $\{(f_{i\leq j})_* : \mathrm{Hom}_{\mathcal{C}}(Y, X_j) \to \mathrm{Hom}_{\mathcal{C}}(Y, X_i)\}$.*

Ejemplos.

1. Consideremos un diagrama

$$\begin{array}{ccc} & & X_1 \\ & & \downarrow f \\ X_2 & \xrightarrow{g} & X_3 \end{array}$$

en una categoría cualquiera. Definamos sobre el conjunto $\{1, 2, 3\}$ el orden parcial en donde el 1 y el 2 no están relacionados, $3 \leq 1$ y $3 \leq 2$. Llamamos $f_{3\leq 1} := f$ y $f_{3\leq 2} := g$, entonces el límite del sistema proyectivo $\{f_{3\leq 1} : X_1 \to X_3, f_{3\leq 2} : X_2 \to X_3\}$ no es otra cosa que el pull-back del diagrama anterior.

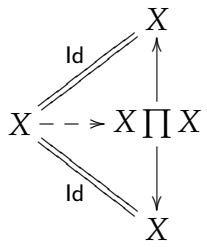
2. Sea $\{X_i\}_{i\in I}$ una familia de objetos de una categoría $\mathcal{C}$ indexados por un conjunto I, y consideremos el orden parcial en I en donde ningún elemento está relacionado con ningún otro (es decir, el conjunto de $\{f_{i\leq j} : i, j \in I,\ i \leq j\}$ sólo contiene las identidades $\mathrm{Id}_i = f_{i\leq i}$. Entonces el límite de este sistema proyectivo coincide con el producto de la familia $\{X_i\}_{i\in I}$.

3. Sea I el conjunto vacío, entonces $\varprojlim_{\leftarrow\varnothing}$ es un objeto final.

4. Los coegalizadores pueden calcularse a partir de dos límites consecutivos, de hecho, a partir de dos pull-backs consecutivos. En efecto, sean $f, g : X \to Y$ y consideremos el pull-back

$$\begin{array}{ccc} X \prod_Y X & \longrightarrow & X \\ \downarrow & & \downarrow g \\ X & \xrightarrow{f} & Y \end{array}$$

En la categoría de conjuntos $X \prod_Y X = \{(x, x') \in X \times X / \ f(x) = g(x')\}$, pero como queremos definir el subconjunto formado por $\{x \in X \ / \ f(x) = g(x)\}$, una manera es considerar la intersección de $X \prod_Y X$ con la diagonal $\{(x, x) \ / \ x \in X\}$, es decir, la imagen de X en $X \times X$ que se define a través del diagrama:



Llamemos $\Delta : X \to X \prod X$ al morfismo definido anteriormente (que tiene sentido en cualquier categoría). Demostrar entonces que el egalizador de f y g es el pull-back del diagrama

$$\begin{array}{ccc} & & X \prod_Y X \\ & & \downarrow \\ X & \xrightarrow{\Delta} & X \prod X \end{array}$$

Se deja como ejercicio descubrir cuál es la flecha natural

$$X \prod_Y X \to X \prod X$$

5. En la categoría de módulos sobre un anillo fijo, el límite de un sistema proyectivo coincide con el límite visto en la categoría de conjuntos.

6. Sea k un anillo cualquiera. Consideremos el conjunto $\mathbb{N}$ con el orden usual y $n \in \mathbb{N}$. En la categoría de anillos llamamos $k[x]_{\leq n} := k[x]/\langle x^{n+1} \rangle$ a los polinomios truncados en grado n. Dado $m \in \mathbb{N}$, si $n \leq m$, $f_{n \leq m} : k[x]_{\leq m} \to k[x]_{\leq n}$ denota la proyección canónica, probar que $\lim_{\leftarrow n} k[x]_{\leq n} = k[|x|]$, las series de potencias formales con coeficientes en k.

7. Sea I un conjunto parcialmente ordenado que tiene máximo, es decir tal que existe $i_0 \in I$ tal que i_0 es comparable con todo elemento de I y además $i_0 \geq i \, \forall \, i \in I$. Demostrar que si $\{f_{i \leq j} : X_j \to X_i\}$ es un sistema proyectivo cualquiera, entonces su límite existe y coincide con X_{i_0}.

8. En la categoría de conjuntos, si $\{X_i\}_{i\in I}$ es una familia de subconjuntos de X, ordenada por el orden inverso a la inclusión, y se consideran como morfismos también las inclusiones, entonces $\lim\limits_{\leftarrow I} X_i = \cap_{i\in I} X_i$.

9.2.7 Colímites

La noción dual a la de límite es la de colímite.

Definición 9.2.14. Sean I un conjunto parcialmente ordenado y sea $\{X_i\}_{i\in I}$ una familia de objetos de una categoría dada $\mathcal{C}$, y para cada i, j en I con $i \leq j$ un morfismo $f_{i\leq j} : X_i \to X_j$. La familia de objetos $\{X_i\}_{i\in I}$ junto con los morfismos $f_{i\leq j}$ se denominará un *sistema inductivo* en caso de que verifique la condición de compatibilidad $f_{j\leq k} \circ f_{i\leq j} = f_{i\leq k}$ para todo $i \leq j \leq k$.

Definición 9.2.15. Sea I un conjunto parcialmente ordenado, $\{f_{i\leq j} : X_i \to X_j\}$ un sistema inductivo. Llamaremos *límite directo* (o límite inductivo, o límite inyectivo, o colímite), en caso de que exista, a un par $(X, \{f_i : X_i \to X\})$ que verifique las siguientes propiedades:

- si $i \leq j$, $f_j \circ f_{i\leq j} = f_i$.
- Si Y es un objeto cualquiera, y $g_i : X_i \to Y$ es una familia de morfismos que satisface que $g_j \circ f_{i\leq j} = g_i$ para todo $i \leq j$, entonces existe un único morfismo $g : X \to Y$ tal que $g_i = g \circ f_i$.

A este objeto X lo denotaremos $\lim\limits_{\to I} X_i$.

La siguiente proposición tiene demostración obvia:

Proposición 9.2.16. *Sea I un conjunto parcialmente ordenado. Consideremos un sistema inductivo $\{f_{i\leq j} : X_i \to X_j\}$ en una categoría $\mathcal{C}$.*

1. *Si un límite directo existe, es único salvo isomorfismo.*
2. *Un límite directo en una categoría $\mathcal{C}$ es lo mismo que un límite inverso en la categoría opuesta.*
3. *Dado un objeto cualquiera Y, el sistema*

$$\{(f_{i\leq j})^* : \mathrm{Hom}_{\mathcal{C}}(X_j, Y) \to \mathrm{Hom}_{\mathcal{C}}(X_i, Y)\}$$

es un sistema proyectivo. Un objeto X es un límite directo de $\{X_i\}_{i\in I}$ si y sólo si $\mathrm{Hom}_{\mathcal{C}}(X,Y)$ es el límite inverso (en la categoría de conjuntos) de $\{\mathrm{Hom}_{\mathcal{C}}(X_i,Y)\}_{i\in I}$ para todo objeto Y.

Ejemplo. En la categoría de conjuntos, si $\{X_i\}_{i\in I}$ es una familia de subconjuntos de X, ordenada por inclusión, y se consideran como morfismos también las inclusiones, entonces $\varinjlim_{\to I} X_i = \cup_{i\in I} X_i$.

9.3 Funtores

9.3.1 Definición y ejemplos

Una vez definido el concepto de categoría, en donde se tienen en cuenta simultáneamente la noción de objeto y la de morfismo, el concepto de funtor resulta natural, pues es un "morfismo" de una categoría en otra:

Definición 9.3.1. Sean $\mathcal{C}$ y $\mathcal{D}$ dos categorías, un *funtor* F de $\mathcal{C}$ en $\mathcal{D}$, que denotaremos $F : \mathcal{C} \to \mathcal{D}$, es el siguiente par de datos:

- Una asignación, para cada objeto X de $\mathcal{C}$, de un objeto $F(X)$ de $\mathcal{D}$.
- Para cada par de objetos X e Y de $\mathcal{C}$, una función

$$F_{X,Y} : \mathrm{Hom}_{\mathcal{C}}(X,Y) \to \mathrm{Hom}_{\mathcal{D}}(F(X),F(Y)).$$

que verifiquen los siguientes dos axiomas:

F1: Si $g : X \to Y$ y $f : Y \to Z$ son dos morfismos en $\mathcal{C}$, entonces $F(f \circ g) = F(f) \circ F(g)$.

F2: Para todo objeto X de $\mathcal{C}$, $F(\mathsf{Id}_X) = \mathsf{Id}_{F(X)}$.

Muchas veces se denomina *funtor covariante* a un funtor según la definición anterior. Si en cambio se tiene una asignación de objetos $X \mapsto F(X)$ y de flechas $F_{X,Y} : \mathrm{Hom}_{\mathcal{C}}(X,Y) \to \mathrm{Hom}_{\mathcal{D}}(F(Y),F(X))$ que satisface el axioma F1 y el axioma F2': $F(f \circ g) = F(g) \circ F(f)$, entonces F se denomina *funtor contravariante*.

Ejemplos.
1. $\mathcal{O} : \mathfrak{G} \to \mathfrak{Sets}$, dado un grupo G, $\mathcal{O}(G)$ es el conjunto G, y si $f : G \to G'$ es un morfismo de grupos, $\mathcal{O}(f)$ es simplemente f, vista como función.

2. $\mathcal{O} : {}_A\mathrm{Mod} \to \mathfrak{Sets}$, dado un A-módulo M, $\mathcal{O}(M)$ es el conjunto subyacente M, si $f : M \to N$ es una aplicación A-lineal entre M y N, $\mathcal{O}(f) = f$.

3. Se pueden definir de la misma manera, funtores "olvido" de la categoría $\mathfrak{Top}$ en $\mathfrak{Sets}$, o de $\mathfrak{Top}_0$ en $\mathfrak{Top}$ (olvidando el punto de base), de la categoría ${}_A\mathrm{Mod}$ en $\mathfrak{Ab}$, tomando un A-módulo y considerando solamente la estructura subyacente de grupo abeliano.

4. Un ejemplo menos trivial es el funtor "abelianización" $Ab : \mathfrak{G} \to \mathfrak{Ab}$, definido por

$$G \mapsto G/[G,G]$$
$$f \mapsto \overline{f}$$

Notar que si $f : G \to G'$ es un morfismo de grupos, entonces $f([G,G]) \subseteq [f(G), f(G)]$. Es por eso que la aplicación de grupos abelianos $\overline{f} : G/[G,G] \to G'/[G',G']$ está bien definida. Queda como ejercicio demostrar la funtorialidad de Ab (es decir ver que $\overline{f \circ g} = \overline{f} \circ \overline{g}$ y que $\overline{\mathsf{Id}_G} = \mathsf{Id}_{G/[G,G]}$).

Un ejemplo de construcción que no es funtorial es la asignación, de $\mathfrak{G}$ en $\mathfrak{Ab}$ dada por $G \mapsto \mathcal{Z}(G)$ ($\mathcal{Z}(G) =$ el centro de G). ¿Por qué no es funtorial?

Ejemplos.
1. Si X es un objeto fijo en una categoría $\mathcal{C}$, entonces se tienen dos funtores en la categoría de conjuntos:

- $\mathrm{Hom}_{\mathcal{C}}(X, -) : \mathcal{C} \to \mathfrak{Sets}$ (covariante)

$$Y \mapsto \mathrm{Hom}_{\mathcal{C}}(X, Y)$$
$$(f : Y \to Z) \mapsto (f_* : \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{C}}(X, Z))$$

  donde, si $\phi : X \to Y$, $f_*(\phi) : X \to Z$ está definido por $f \circ \phi$.
- $\mathrm{Hom}_{\mathcal{C}}(-, X) : \mathcal{C} \to \mathfrak{Sets}$ (contravariante)

$$Y \mapsto \mathrm{Hom}_{\mathcal{C}}(Y, X)$$
$$(f : Y \to Z) \mapsto (f^* : \mathrm{Hom}_{\mathcal{C}}(Z, X) \to \mathrm{Hom}_{\mathcal{C}}(Y, X))$$

donde, si $\phi : Z \to X$, $f^*(\phi) : Y \to X$ está definido por $\phi \circ f$.

2. Si A es un dominio íntegro, entonces $t : {}_A\mathrm{Mod} \to {}_A\mathrm{Mod}$ dada por $M \mapsto t(M)$ (la A-torsión de M), es un funtor.

3. De $\mathfrak{Sets}$ en $\mathfrak{Top}$ pueden definirse dos funtores "extremos", usando la topología discreta: $X \mapsto (X, \mathcal{P}(X))$, o la indiscreta: $X \mapsto (X, \{\varnothing, X\})$.

4. De $\mathfrak{Sets}$ a $\mathfrak{G}$ o ${}_A\mathrm{Mod}$ se puede definir el funtor "libre", es decir $L(X) =$ el grupo libre generado por el conjunto X, o $A^{(X)}$, el A-módulo libre generado por X. Como definir un morfismo con dominio $L(X)$ (resp. $A^{(X)}$) equivale a definir una función de conjuntos sobre X con dominio en otro grupo (resp. en otro A-módulo), dada una función $X \to Y$ queda unívocamente determinada una flecha de grupos de $L(X) \to L(Y)$ (resp. flecha A-lineal de $A^{(X)} \to A^{(Y)}$).

9.3.2 Transformaciones naturales

Así como los funtores pueden considerarse como los morfismos entre las categorías, las transformaciones naturales pueden considerarse como los morfismos entre funtores.

Definición 9.3.2. Sean $F_1, F_2 : \mathcal{C} \to \mathcal{D}$ dos funtores (covariantes) entre dos categorías $\mathcal{C}$ y $\mathcal{D}$. Dar una *transformación natural* $\eta : F_1 \to F_2$ entre los funtores F_1 y F_2 es dar un morfismo $\eta_X : F_1(X) \to F_2(X)$ para cada objeto X de $\mathcal{C}$, con la propiedad siguiente: Si $f : X \to Y$ es un morfismo en $\mathcal{C}$ entonces el diagrama

$$\begin{array}{ccc} F_1(X) & \xrightarrow{F_1(f)} & F_1(Y) \\ {\scriptstyle \eta_X}\downarrow & & \downarrow{\scriptstyle \eta_Y} \\ F_2(X) & \xrightarrow{F_2(f)} & F_2(Y) \end{array}$$

es conmutativo en $\mathcal{D}$.

Si los funtores F_1, F_2 son contravariantes, se dirá que $\eta : F_1 \to F_2$ es una transformación natural si para todo morfismo $f : X \to Y$ el

diagrama siguiente es conmutativo.

$$\begin{array}{ccc} F_1(X) & \xleftarrow{F_1(f)} & F_1(Y) \\ {\scriptstyle \eta_X}\downarrow & & \downarrow{\scriptstyle \eta_Y} \\ F_2(X) & \xleftarrow{F_2(f)} & F_2(Y) \end{array}$$

Si η_X es un isomorfismo para todo objeto X de $\mathcal{C}$ (ya sea en el caso contravariante o en el covariante), diremos que F_1 y F_2 son naturalmente isomorfos y que η es un isomorfismo natural. Notar que en ese caso, el inverso de un isomorfismo natural también es una transformación natural.

Ejemplos.
1. Sean V, W dos k-espacios vectoriales y sea $f : V \to W$ una transformación lineal. Sabemos que las inclusiones en el doble dual son tales que el diagrama

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ {\scriptstyle i_V}\downarrow & & \downarrow{\scriptstyle i_W} \\ V^{**} & \xrightarrow{f^{**}} & W^{**} \end{array}$$

es conmutativo, esto dice que la inclusión en el doble dual es una transformación natural entre los funtores $F_1 = \mathsf{Id}$ y $F_2 = (-)^{**}$.

2. Sabemos que dados dos anillos A, B y bimódulos ${}_AX_B$, ${}_BY$, ${}_AZ$ se tiene un isomorfismo

$$\eta_{X,Y,Z} : \mathrm{Hom}_A(X \otimes_B Y, Z) \cong \mathrm{Hom}_B(Y, \mathrm{Hom}_A(X, Z))$$

(ver teorema 7.3.1). Fijados bimódulos X e Y consideremos los funtores $\mathrm{Hom}_A(X \otimes_B Y, -)$ y $\mathrm{Hom}_B(Y, \mathrm{Hom}_A(X, -))$. Dejamos como ejercicio verificar que este isomorfismo es una transformación natural.

De la misma manera fijando X y Z, los funtores contravariantes $\mathrm{Hom}_A(X \otimes_B (-), Z)$ y $\mathrm{Hom}_B(-, \mathrm{Hom}_A(X, Z))$ también son naturalmente isomorfos.

3. Dado un anillo A, los funtores Id, $\mathrm{Hom}_A(A, -)$ y $(-) \otimes_A A$ de Mod_A en Mod_A, son todos naturalmente isomorfos entre sí.

4. Sean A un anillo y ${}_AZ_A$ un A-bimódulo isomorfo a A como A-bimódulo, llamemos $u : Z \to A$ ese isomorfismo. Entonces

$$\begin{aligned} \eta_M : Z \otimes_A M &\to M \\ z \otimes m &\mapsto u(z).m \end{aligned}$$

define un isomorfismo natural entre el funtor $Z \otimes_A (-)$ y el funtor identidad.

5. Consideremos la categoría de anillos con unidad y la categoría de grupos. Está definido el funtor $\mathcal{U}(-)$ y para cada entero positivo n fijo el funtor $GL(n, -)$, que asocian respectivamente, dado un anillo A, el grupo de unidades de A, y las matrices inversibles de n por n con coeficientes en A. Demuestre la funtorialidad de estas construcciones, y muestre a su vez que la función determinante define una transformación natural entre $GL(n, -)$ y $\mathcal{U}(-)$.

6. Se consideran los funtores

$$\begin{aligned} sq : \mathfrak{Sets} &\to \mathfrak{Sets} \\ E &\mapsto E \times E \end{aligned}$$

y

$$\begin{aligned} \mathrm{Hom}_{\mathfrak{Sets}}(2, -) : \mathfrak{Sets} &\to \mathfrak{Sets} \\ E &\mapsto \mathrm{Hom}_{\mathfrak{Sets}}(2, E) \end{aligned}$$

donde 2 denota al conjunto de dos elementos $\{0, 1\}$. Probar que estos funtores son naturalmente isomorfos.

9.3.3 Funtores adjuntos, definición y propiedades

Podemos enunciar ahora la definición de adjunción de funtores, que será la noción central de esta sección:

Definición 9.3.3. Sean $\mathcal{C}$ y $\mathcal{D}$ dos categorías, $F : \mathcal{C} \to \mathcal{D}$ y $G : \mathcal{D} \to \mathcal{C}$ dos funtores tales que para todo par de objetos $M \in \mathrm{Obj}(\mathcal{C})$ y $X \in \mathrm{Obj}(\mathcal{D})$ existe un isomorfismo natural con respecto a las dos variables

$$\mathrm{Hom}_{\mathcal{D}}(F(M), X) \cong \mathrm{Hom}_{\mathcal{C}}(M, G(X))$$

En este caso diremos que F es *adjunto a izquierda* de G y que G es *adjunto a derecha* de F.

Ejemplos.
1. Sean ${}_AX_B$ un A-B-bimódulo, $F = X \otimes_B (-)$ y $G = \mathrm{Hom}_A(X, -)$. Entonces el isomorfismo

$$\mathrm{Hom}_A(X \otimes_B Y, Z) \cong \mathrm{Hom}_B(Y, \mathrm{Hom}_A(X, Z))$$

nos está diciendo que F es adjunto a izquierda de G.

2. Sean A un anillo e I un conjunto, Entonces el módulo $A^{(I)}$ es A-libre y tiene una base que está en biyección con I. La propiedad de la base nos dice que para definir un morfismo A-lineal con dominio en $A^{(I)}$ y codominio en otro A-módulo M, basta definir una función (de conjuntos) entre I y M. Llamemos $\mathcal{O} : A\text{-mod} \to \mathfrak{Sets}$ al funtor olvido, que a todo A-módulo M le asigna el conjunto subyacente M. Entonces se tiene que, identificando el conjunto I con la base canónica de $A^{(I)}$, la restricción de $A^{(I)}$ en I establece una biyección natural

$$\mathrm{Hom}_A(A^{(I)}, M) \cong \mathrm{Hom}_{\mathfrak{Sets}}(I, \mathcal{O}(M)).$$

3. Sea A un anillo conmutativo y $S \subseteq A$ un subconjunto multiplicativo de A. Sea $\mathcal{O} : A_S\text{-mod} \to A\text{-mod}$ el funtor que a todo A_S-módulo N le asigna el mismo N pero considerado como A-módulo, con la estructura definida a partir del morfismo canónico de anillos $A \to A_S$. Se puede verificar como ejercicio que la propiedad universal de la localización se traduce en la adjunción $\mathrm{Hom}_{A_S}(M_S, N) \cong \mathrm{Hom}_A(M, \mathcal{O}(N))$.

Ejercicios.
1. Dado un conjunto X, sea $\mathcal{P}(X)$ la categoría cuyos objetos son los subconjuntos de X, y las flechas son las inclusiones. Fijamos dos conjuntos A y B y $f : A \to B$ una función. Sea $f^{\to} : \mathcal{P}(A) \to \mathcal{P}(B)$ el funtor imagen y $f^{\leftarrow} : \mathcal{P}(B) \to \mathcal{P}(A)$ el funtor imagen inversa. Demuestre que $f^{\to}$ es adjunto a izquierda de $f^{\leftarrow}$.

2. Sean V un k-espacio vectorial, A una k-álgebra, $T(V)$ el álgebra tensorial, $\mathcal{O}$ el funtor olvido de k-álgebras en k-espacios vectoriales, entonces

$$\mathrm{Hom}_{k-\mathfrak{Alg}}(T(V), A) \cong \mathrm{Hom}_k(V, A)$$

3. Sean V un k-espacio vectorial, A una k-álgebra, $S(V)$ el álgebra simétrica, $\mathcal{O}$ el funtor olvido de k-álgebras conmutativas en k-espacios vectoriales, entonces

$$\mathrm{Hom}_{k-\mathfrak{Alg}_{\mathfrak{C}}}(S(V), A) \cong \mathrm{Hom}_k(V, A)$$

4. Sean G un grupo, A un anillo, $\mathcal{U}(A)$ el grupo de unidades de A, entonces

$$\mathrm{Hom}_{\mathfrak{G}}(G, \mathcal{U}(A)) \cong \mathrm{Hom}_{\mathfrak{An}}(\mathbb{Z}[G], A)$$

5. Sean G un grupo, A una k-álgebra, $\mathcal{U}(A)$ el grupo de unidades de A, entonces

$$\mathrm{Hom}_{\mathfrak{G}}(G, \mathcal{U}(A)) \cong \mathrm{Hom}_{k-\mathfrak{Alg}}(k[G], A)$$

6. Sea X un conjunto cualquiera, denotemos $F(X)$ al grupo libre generado por X, luego la propiedad universal del grupo libre se lee como:

$$\mathrm{Hom}_{\mathfrak{G}}(F(X), G) \cong \mathrm{Hom}_{\mathfrak{Sets}}(X, \mathcal{O}(G))$$

La propiedad fundamental de los funtores adjuntos está dada por el siguiente teorema:

Teorema 9.3.4. *Sea $G : \mathcal{C} \to \mathcal{D}$ un funtor que admite un adjunto a derecha $F : \mathcal{D} \to \mathcal{C}$, entonces F preserva límites. En particular preserva productos, push-outs, egalizadores, monomorfismos, objetos finales, y si existe objeto cero preserva cero y conúcleos. Dualmente G preserva colímites, en particular preserva coproductos, pull-backs, coegalizadores, epimorfismos, objetos iniciales, y si existe objeto cero preserva cero y núcleos.*

Demostración. Sea I un conjunto parcialmente ordenado y sea $\{f_{i\leq j} : X_j \to X_i\}$ un sistema proyectivo en $\mathcal{D}$ que admite límite $(X, p_i : X \to X_i)$, queremos ver entonces que también el sistema proyectivo $\{F(f_{i\leq j}) : F(X_j) \to F(X_i)\}$ admite límite, y que éste coincide con $(F(X), F(p_i) : F(X) \to F(X_i))$. Para ésto, recordemos que X es límite de los X_i si y sólo si la función natural

$$\mathrm{Hom}_{\mathcal{D}}(Y, X) \to \lim_{\leftarrow I} \mathrm{Hom}_{\mathcal{D}}(Y, X_i)$$

es una biyección para todo objeto Y. Si C es un objeto de $\mathcal{C}$, entonces se tienen las siguientes biyecciones naturales:

$$\begin{aligned}\mathrm{Hom}_{\mathcal{C}}(C, F(X)) &\cong \mathrm{Hom}_{\mathcal{D}}(G(C), X)\\ &\cong \lim_{\leftarrow I} \mathrm{Hom}_{\mathcal{D}}(G(Y), X_i)\\ &\cong \lim_{\leftarrow I} \mathrm{Hom}_{\mathcal{C}}(Y, F(X_i))\end{aligned}$$

La parte dual puede demostrarse de manera directa, o bien notando que $F : \mathcal{C} \to \mathcal{D}$ es adjunto a derecha de G si y sólo si $F : \mathcal{C}^{op} \to \mathcal{D}^{op}$ es adjunto a izquierda de $G : \mathcal{D}^{op} \to \mathcal{C}^{op}$, y los colímites en $\mathcal{D}$ coinciden con los límites en $\mathcal{D}^{op}$. □

Si $G : \mathcal{C} \to \mathcal{D}$ un funtor que admite un adjunto a derecha $F : \mathcal{D} \to \mathcal{C}$, no necesariamente G preserva epimorfismos, ni F monomorfismos. Sin embargo, en caso de que alguno de ellos tenga esa propiedad, tenemos el siguiente teorema:

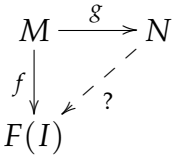
Teorema 9.3.5. *Sea $G : \mathcal{C} \to \mathcal{D}$ un funtor que admite un adjunto a derecha $F : \mathcal{D} \to \mathcal{C}$.*

- *Si G preserva monomorfismos entonces F preserva objetos inyectivos.*
- *Si F preserva epimorfismos entonces G preserva objetos proyectivos.*

Demostración. Veremos sólo el primer ítem, el segundo se demuestra o bien de manera análoga, o bien pasando a las categorías opuestas.

Supongamos ahora que G preserva monomorfismos, queremos demostrar que F preserva objetos inyectivos.

Dado un objeto inyectivo I en $\mathcal{D}$, consideremos $F(I)$ y un monomorfismo $g : M \to N$ en la categoría $\mathcal{C}$. La definición de objeto inyectivo se esquematiza mediante el diagrama



es decir, dada una $f \in \mathrm{Hom}_{\mathcal{C}}(M, F(I))$ se quiere saber si se "extiende" a N, o sea si existe $\widetilde{f} : N \to F(I)$ tal que $f = \widetilde{f} \circ g$. La manera

de reescribir este párrafo en términos del funtor $\mathrm{Hom}_{\mathcal{C}}(-, F(I))$ es decir si $g_* : \mathrm{Hom}_{\mathcal{C}}(N, F(I)) \to \mathrm{Hom}_{\mathcal{C}}(M, F(I))$ es o no una función sobreyectiva, cada vez que g es un monomorfismo. A partir de la naturalidad de la adjunción, tenemos el siguiente diagrama conmutativo:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(N, F(I)) & \xrightarrow{g_*} & \mathrm{Hom}_{\mathcal{C}}(M, F(I)) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathcal{D}}(G(N), I) & \xrightarrow{G(g)_*} & \mathrm{Hom}_{\mathcal{D}}(G(M), I) \end{array}$$

Por hipótesis, G preserva monomorfismos, luego $G(g) : G(M) \to G(N)$ es un monomorfismo, al ser I inyectivo en $\mathcal{C}$ se sigue que $G(g)_*$ es una función sobreyectiva, como las dos flechas verticales son biyecciones, se sigue que g_* es una función sobreyectiva, como se quería probar. □

Ejemplo. El funtor olvido $\mathcal{O} : {}_A\mathrm{Mod} \to \mathfrak{Sets}$ claramente conserva epimorfismos, usando el teorema reencontramos la propiedad bien conocida que dice que los A-módulos libres son proyectivos. El funtor olvido de k-algebras en k-espacios vectoriales tiene como adjunto al funtor álgebra tensorial, es claro que este funtor olvido preserva epimorfismos, luego las álgebras tensoriales son objetos proyectivos en la categoría de álgebras.

Capítulo 10

Bibliografía

[F. W. Anderson – K. R. Fuller] *Rings and categories of modules*, Springer - Verlag 1973.

[M. Auslander – I. Reiten – S. O. Smalø] *Representation theory of Artin algebras*. Cambridge University Press 1995.

[N. Bourbaki] *Éléments de mathématique. Algèbre*. Chap. II, III y VIII (Hermann 1970), Chap. X (Masson 1980).

[J. Dieudonné] *Sur les groupes classiques*. Troisième edition, Hermann, 1967.

[C. Faith] *Algebra II. Ring theory*. Springer 1976.

[S. Lang] *Algebra*. Second edition, Addison – Wesley 1984.

[S. Mac Lane] *Categories for the working mathematician*. Springer 1971.

[B. Mitchell] *Theory of categories*. Academic Press 1966.

[H. Weyl] *The classical groups*. Princeton University Press 1946.

Índice