Anillos y sus categorías de representaciones

M.A. Farinati A.L. Solotar

11 de julio de 2003

Indice

> Messieurs,
> Le hasard veut que je supplée votre honorable professeur M. Jacquau . Mais je me permets de ne point partager son opinion sur le système d'enseignement à suivre .
> Mon avis , à moi , est qu'il ne faut *rien apprendre , rien* , de ce que l'Université vous recommende . *(Rumeurs au centre .)* Je pense être plus utile à votre avenir en vous conseillant de jouer aux dominos , aux dames , à l'écarté –les plus jeunes seront autorisés à planter du papier dans le derrière des mouches . *(Mouvements en sens divers .)*
> Par exemple , messieurs , du silence ! Il n'est pas nécessaire de réfléchir pour apprendre du Démosthène et du Virgile , mais quand il faut faire le quatre-vingt-dix ou le cinq cents , ou échec au roi , ou empaler des mouches sans les faire souffrir , le calme est indispensable à la pensée , et le recueillement est bien dû à l'insecte innocent que va , messieurs , sonder votre curiosité , si j'ose m'exprimer ainsi . *(Sensation prolongée .)*
> Je voudrais enfin que le temps que nous allons passer ensemble ne fût pas du temps perdu .
>
> Jules Vallès, *L'insurgé*. 1885.

Introducción

Este libro surgió luego del dictado, en diversas oportunidades, del curso para la licenciatura en Cs. Matemáticas de la FCEyN-UBA "Algebra II", que es la tercer materia de álgebra que cursan los alumnos. La escasez de bibliografía en castellano sobre los temas abarcados por esta materia fue uno de las principales motivaciones para escribir este libro.

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 directamente literatura especializada.

Un curso semestral de estructuras algebraicas debería contar con los contenidos completos de los capítulos 1,2,3 y 4 como esqueleto sobre el cual desarrollar con mayor o menor profundidad los contenidos de los otros capítulos.

El capítulo sobre grupos (capítulo 1) 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 en vez de la categoría de grupos. 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 (capítulo 6) está formado por dos partes a la vez muy diferentes y análogas. Se trata de los teoremas de estruc-

tura de módulos sobre un anillo semisimple, y sobre un dominio principal. Si bien las categorías semisimples tienen un comportamiento muy diferente al 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 se tuvo en mente fue el de un álgebra de grupo, los ejemplos modelo que tomamos de dominios principales son $\mathbb{Z}$ (obteniendo así 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, en el caso que k sea algebraicamente cerrado, la descomposición en formas de Jordan. Dada la importancia de esta aplicación, la hemos descripto separadamente como última sección de este capítulo.

El capítulo sobre categorías (capítulo 9) 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 así lo indicaban. Generalmente este tema resulta muy difícil de asimilar si no se cuenta con ejemplos concretos de categorías sobre las que 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 (capítulo 8) 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.

Este libro está principalmente destinado a alumnos de un curso de teoría de módulos. Como tales, asumimos que tienen un profesor, y por lo tanto hemos evitado todo lo que molesta a la comprensión de un texto matemático como largas explicaciones técnicas (que los alumnos difícilmente compren-

den y que los profesores no necesitan leer) o una presentacion estrictamente secuencial.

Finalmente, queremos agradecer los comentarios, sugerencias y correcciones de los alumnos que cursaron Algebra II en los últimos cuatrimestres que contaron con versiones previas de este manuscrito. Queremos agradecer tambien a Mariano Suárez Álvarez por su ayuda con el LaTeX.

Marco A. Farinati - Andrea L. Solotar
Buenos Aires, 23 de agosto de 2001.

1

Grupos

1.1. Grupo: definición y ejemplos

El concepto de grupo apareció inicialmente como grupo 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** $(G, *)$ *es un conjunto* G *provisto de una operación* $* : G \times G \to G$ *que verifica:*

1. Asociatividad*: para todo* $g_1,\ g_2,\ g_3 \in G,\ (g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$.
2. Elemento neutro*: existe* $e \in G$ *tal que* $e * g = g * e = g\ \forall g \in G$.
3. Inverso*:* $\forall\ g \in G,\ \exists\ g' \in G$ *tal que* $g * g' = g' * g = e$.

Si además para todo par $g,\ h \in G$ se verifica $g * h = h * g$ entonces el grupo se llama **abeliano** o **conmutativo**. Al cardinal del conjunto G se lo llamará **orden** de G y se lo notará $|G|$. Un grupo G se dirá **finito** si $|G| < \infty$, se dirá **infinito** en otro caso.

Observaciones: 1) El elemento neutro de un grupo es único, porque si e y e' son dos neutros, entonces $e = e * e' = e'$ (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 inverso g' de un elemento g es único, ya que si g' y g'' son dos inversos para un mismo g entonces

$$g' = g' * e = g' * (g * g'') = (g' * g) * g'' = e * g'' = g''$$

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

Ejemplos:

1. Sea X un conjunto, $G = \{\text{funciones biyectivas de } X\}$, $*$ =composición. En este caso e = función identidad y dado g, g^{-1} es la función inversa. Si el conjunto X es finito, $X = \{1, 2, 3, ..., n\}$, entonces G se denota $\mathcal{S}_n$ y se llama el **n-ésimo grupo simétrico**.

2. Sea V un k espacio vectorial. $G = GL(V) = \{\text{endomorfismos lineales inversibles de } V\}$ es un grupo con la composición de transformaciones como producto y la identidad como neutro. Si $V = k^n$, $GL(V)$ se nota $GL_n(k)$ y se identifica (luego de fijar una base del espacio vectorial) 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 (conmutativos).

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

5. Si $m \in \mathbb{N}$, $G_m = \{$ raíces m-ésimas de la unidad $\}$ con la operación producto (como números complejos) es también un grupo abeliano con m elementos, el neutro es el 1.

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

$$(f *_\Gamma g)(x) := f(x) *_G g(x) \quad (\forall f, g \in \Gamma,\ \forall x \in X)$$

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

7. 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

$$(g_1, g_2) * (g_1', g_2') := (g_1 * g_1', g_2 * g_2')$$

Nota: Para un grupo arbitrario $(G, *)$, denotaremos indistintamente el producto de dos elementos g_1, g_2 por $g_1 * g_2 = g_1.g_2 = g_1 g_2$. Los símbolos $*$ y . se utilizarán para cualquier tipo de grupo (abeliano o no), el símbolo $+$ se utilizará *solamente* para grupos abelianos. Cuando se desprenda del contexto no explicitaremos la operación y hablaremos simplemente del 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 asume la existencia de elemento neutro, y a veces no. Damos pues la definición de monoide:

Definición 1.2.1. *Un* **monoide** $(M, *)$ *es un conjunto M provisto de una operación $* : M \times M \to M$ que es asociativa, es decir, que verifica $m*(n*l) = (m*n)*l$, para toda terna de elementos $m,\ n,\ l \in M$. Si además existe $e \in M$ tal que $e*m = m*e\ \forall m \in M$, 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 $\mathcal{U}(M)$ definido por $\mathcal{U}(M) := \{m \in M \text{ tal que existe } m' \in M \text{ con } m' * m = e = m * m'\}$ se denomina las **unidades** M. Tautológicamente $\mathcal{U}(M)$ es un grupo.

Ejemplos:

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

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

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

4. Existen monoides con elemento neutro que admiten elementos inversibles a izquierda pero no a derecha. Consideremos

$$M = CFM_{\mathbb{N}}(\mathbb{R}) = \{(a_{ij})_{i,j\in\mathbb{N}} /\ a_{ij} \in \mathbb{R},\ \text{y } \forall j,\ a_{ij} = 0 \text{ salvo para finitos valores de } i\}$$

   con el producto usual de matrices. 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 $n \in \mathbb{N}$ consideremos $X^n := X \times \cdots \times X$ el producto cartesiano de X consigo mismo n-veces. Se define

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

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

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

   Esta operación da una estructura de monoide (sin elemento neutro) en $L(X)$.

   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 $(G, *)$, un* **subgrupo** *de G es un subconjunto $H \subseteq G$ tal que $(H, *|_{H\times H})$ es un grupo, o en forma equivalente:*

1. *$*$ es cerrado en H, i.e. $\forall h_1, h_2 \in H$, $h_1 * h_2 \in H$.*
2. *$e \in H$.*
3. *$\forall h \in H,\ h^{-1} \in H$.*

Observación: La condición 2 implica que $H \neq \emptyset$, a su vez las condiciones 1 y 3 junto con $H \neq \emptyset$ implican la condición 2, por lo tanto en la definición de subgrupo se puede cambiar 2 por $H \neq \emptyset$.

Ejemplos:

1. Dado $n \in \mathbb{N}$, sea $G_n = \{w \in \mathbb{C} \ / \ w^n = 1\}$, entonces $(G_n, .)$ es un subgrupo de $(\mathbb{C} - \{0\}, .)$.
2. Si $n \in \mathbb{N}$, los múltiplos de n: $n.\mathbb{Z} = \{nk \ / \ k \in \mathbb{Z}\}$ es un subgrupo de los enteros $(\mathbb{Z}, +)$.
3. $G = \mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$, $H_1 = \{\overline{0}, \overline{2}, \overline{4}\}$ y $H_2 = \{\overline{0}, \overline{3}\}$ son subgrupos de G.
4. Si $(G, *)$ es un grupo, G y $\{e\}$ son siempre subgrupos. Por ejemplo 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 $X = \{1, 2, 3, ..., n\}$, $G = \mathcal{S}_n = \{$ permutaciones de $X\}$. Si $1 \leq i \leq n$, el conjunto de permutaciones que fijan el elemento i de X: $H_i = \{g \in G \ / \ g(i) = i\}$ es un subgrupo de G. ¿Cuántos elementos tiene G? ¿Cuántos elementos tiene H_i?
6. Sea $G = GL_n(k)$. Sea $H = \{A \in G \ / \ det(A) = 1\}$, entonces H es un subgrupo de G.

Observemos que si H es un subgrupo de un grupo G, entonces para cada $x \in G$, el conjunto $x.H.x^{-1} = \{xhx^{-1} : h \in H\}$ es también un subgrupo de G (verificar: $(xhx^{-1})(xh'x^{-1}) = x(hh')x^{-1} \in x.H.x^{-1}$ 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, 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. De los ejemplos anteriores, si tomamos $G = S_n$ y $\sigma \in G$ la permutación cíclica definida por

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

podemos considerar $H = \{id, \sigma, \sigma^2, \sigma^3, ..., \sigma^{n-1}\}$, H resulta un subgrupo, pero (ejercicio) es falso en general que si $x \in G$ entonces $x.H.x^{-1} = H$.

Definición 1.3.2. *Un subgrupo H de un grupo G se dirá* **invariante** *(o normal, o distinguido) si verifica que $x.H.x^{-1} = H \ \forall x \in G$. Se notará $H \triangleleft G$*

Pregunta: Cómo pueden descubrirse todos los subgrupos normales de un grupo dado?

Observaciones / ejercicios:

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

2. Si H es un subgrupo de un grupo G, demostrar que $\bigcap\limits_{x \in G} x.H.x^{-1}$ es un subgrupo invariante.

3. Si S es un subconjunto de G, sea $N_S = \{x \in G \ / \ x.S.x^{-1} = S\}$ entonces N_S es un subgrupo de G llamado el **normalizador** de S en G. En particular, si $S = \{a\}$, $N_S = \{x \in G \ / \ xa = ax\}$.
   Si S es un subgrupo de G, S es también un subgrupo de N_S y $S \triangleleft N_S$.
   Además N_S es el subgrupo de G mas grande con esa propiedad.

4. Sea $Z_G = \{x \in G \ / \ xg = gx \ \forall g \in G\}$. Z_G es un subgrupo de G, se llama el **centro** de G. Se tiene $Z_G \triangleleft G$, y además $\forall S \subseteq G$, $Z_G \subseteq N_S$.

5. Sea G un grupo cualquiera, $x, y \in G$, definimos el **conmutador** de x e y como $[x, y] := xyx^{-1}y^{-1}$. Dejamos como ejercicio verificar que si $z \in G$, entonces $z[x, y]z^{-1} = [zxz^{-1}, zyz^{-1}]$. Llamamos **subgrupo conmutador** y denotamos $[G, G]$ al subgrupo de G generado por los conmutadores. Tenemos entonces que $[G, G] \triangleleft G$.

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 $(G, *_G)$, $(G', *_{G'})$ dos grupos. Una función $f : G \to G'$ se dice un* **morfismo** *(u homomorfismo) de grupos si y solamente si para todo $g_1, g_2 \in G$ es válida la igualdad:*

$$f(g_1 *_G g_2) = f(g_1) *_{G'} f(g_2)$$

Ahora se puede dar la definición de subgrupo de manera mas compacta (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 $i : H \to G$ $(h \mapsto h)$ sea un morfismo de grupos.

Nombres:

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

Notar que si designamos por $\mathrm{Hom}_G(G, G')$ al conjunto de morfismos de grupos $f : G \to G'$, este conjunto es siempre no vacío porque la función que a todo elemento de G le asigna el neutro de G' (el "morfismo nulo") es trivialmente un morfismo de grupos.

Propiedades:

1. Un morfismo $f : G \to G'$ es isomorfismo $\Leftrightarrow$ es monomorfismo y epimorfismo, además en tal caso la función inversa $f^{-1} : G' \to G$ también es un morfismo de grupos (verificar!).

2. Si f es un morfismo, entonces $f(e_G) = e_{G'}$ pues como $e_G = e_G * e_G$, entonces $f(e_G) = f(e_G) * f(e_G)$ por lo tanto $e_{G'} = f(e_G) * (f(e_G))^{-1} = f(e_G) * f(e_G) * (f(e_G))^{-1} = f(e_G)$.

3. $\forall g \in G$, $f(g^{-1}) = f(g)^{-1}$.

4. f monomorfismo $\Leftrightarrow (f(g) = e_{G'} \Rightarrow g = e_G)$.

Si $f : G \to G'$ es un morfismo de grupos, se tienen automáticamente dos subgrupos (uno de G y otro de G') asociados a dicho morfismo, que llamaremos el núcleo (en inglés o alemán: kernel) y la imagen de f:

- **Núcleo**: $\mathrm{Ker}(f) := \{g \in G \ / \ f(g) = e_{G'}\}$
- **Imagen:** $\mathrm{Im}(f) := \{g' \in G' \ / \ \exists g \in G \text{ tal que } f(g) = g'\}$.

Ejercicio 1: verificar que efectivamente son subgrupos. Verificar que $\mathrm{Ker}(f) \triangleleft G$, sin embargo, $\mathrm{Im}(f)$ no tiene porque ser invariante, mostrar un contraejemplo.

Ejercicio 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 $H' \triangleleft G'$ entonces $f^{-1}(H') \triangleleft G$. En particular como $\{e\} \triangleleft G'$ resulta $\mathrm{Ker}(f) \triangleleft G$.

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

Ejemplos:

1. La función exponencial $exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, .)$ $(x \mapsto e^x)$ es un isomorfismo de grupos, cuyo inverso es la función logaritmo.

2. Morfismos entre $\mathbb{Z}_2$ y $\mathbb{Z}_4$:
   Sea $f : \mathbb{Z}_2 \to \mathbb{Z}_4$ morfismo de grupos. Luego sabemos que $f(\overline{0}) = \overline{0}$. ¿Cuánto vale $f(\overline{1})$? Como $\overline{0} = \overline{1} + \overline{1}$ entonces $f(\overline{1}) + f(\overline{1}) = \overline{0}$ por lo tanto $f(\overline{1})$ 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. (ejercicio) Sea $f : \mathbb{Z}_2 \to \mathbb{Z}_3$ un morfismo de grupos, entonces f es el morfismo nulo.

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

5. (ejercicio) Definir un morfismo de grupos $f : \mathcal{S}_3 \to \mathcal{S}_3$ tal que $\mathrm{Im}(f) \not\lhd \mathcal{S}_3$.

Vimos que si $f : G \to G'$ es un morfismo de grupos, entonces $\mathrm{Ker}(f) \lhd G$. El siguiente lema muestra que todo subgrupo normal de G es el núcleo de algún morfismo de G en algún grupo G'.

Lema 1.4.2. *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: Se quiere definir un f y un G' de modo tal que $\mathrm{Ker}(f) = H$. Definimos para eso una relación de equivalencia $\sim_H$.

Si $x, y \in G$, diremos que $x \sim_H y \Leftrightarrow y^{-1}x \in H$ (verificar que al ser H un subgrupo, esa relación es de equivalencia). Notar que en el caso $H = \{e\}$ esta relación es simplemente la igualdad.

Dada una relación de equivalencia en un conjunto, se tiene automáticamente otro conjunto (el conjunto cociente) y una aplicación natural:

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

donde $\overline{x} = \{y \in G \ / \ x \sim_H y\}$

Se toma $f = \pi$ y $G' = G/\sim_H$, en G' se define la siguiente estructura de grupo:

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

Notar que es la única estructura de grupo posible que hace de π un morfismo de grupos.

Hay que verificar lo siguiente:

1. La operación en el conjunto cociente está bien definida.

2. La operación definida en G' da una estructura de grupo, es decir es asociativa, hay un elemento neutro y todo elemento tiene inverso.

3. f es un morfismo de grupos y $\mathrm{Ker}(f) = H$.

Veamos 1.: Sean x, x', y, y' tales que $\overline{y} = \overline{y'}$ y $\overline{x} = \overline{x'}$. Es decir, x está relacionado con x' y lo mismo para y e y', esto equivale a que existan $h_1, h_2 \in H$ tales que

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

o equivalentemente

$$x = x'h_1 \ ; \ y = y'h_2$$

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

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

donde $h_3 = y'^{-1}h_1y'$ que es un conjugado de h_1, como H es un subgrupo *invariante* entonces $h_3 \in H$, también pertenece a H el producto h_3h_2, por lo tanto xy está relacionado con $x'y'$ y por lo tanto $\overline{xy} = \overline{x'y'}$.

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

Una vez que se sabe que la operación en G' está bien definida, es fácil (ejercicio) ver que es asociativa y que $e_{G'} = \overline{e}$, $(\overline{x})^{-1} = \overline{x^{-1}}$.

El hecho de que f sea 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 $\mathrm{Ker}(f)$:

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

Notación: $G' := G/H$

Definición 1.4.3. *Dado un grupo G y un subgrupo invariante H, a la construcción precedente G/H se le llama el grupo* **cociente** *de G por H (o G módulo H).*

Notar que la estructura de grupo de G/H se debe a que $H \triangleleft G$, si no, el conjunto cociente G/H es tan sólo un conjunto.

Ejemplos:

1. Sea $m.\mathbb{Z}$ considerado como subgrupo de $(\mathbb{Z}, +)$, entonces $\mathbb{Z}/m.\mathbb{Z} = \mathbb{Z}_m$

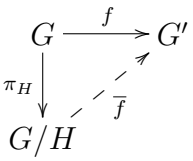
2. Sea $(\mathbb{R}, +)$ y consideremos el subgrupo (normal porque $(\mathbb{R}, +)$ es conmutativo) $\mathbb{Z} \subset \mathbb{R}$, se obtiene entonces que $\mathbb{R}/\mathbb{Z}$ es un grupo isomorfo a $(S^1, .) = \{z \in \mathbb{C} \ / \ |z| = 1\} \subset (\mathbb{C} - \{0\}, .)$ bajo la aplicación

$$\begin{aligned} \mathbb{R}/\mathbb{Z} &\to S^1 \\ \overline{x} &\mapsto e^{2i\pi x} \end{aligned}$$

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

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

Proposición 1.4.4. *Sea G un grupo, $H \triangleleft G$ y la aplicación al cociente $\pi_H : G \to G/H$. Entonces para todo morfismo de grupos $f : G \to G'$ (donde G' es arbitrario) 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:

Existencia de $\overline{f}$: Si $\overline{x} \in G/H$, se define $\overline{f}(\overline{x}) := f(x)$. Esta aplicación resulta bien definida pues si $\overline{x} = \overline{x'}$ entonces ${x'}^{-1}x \in H \subseteq \mathrm{Ker}(f)$, luego $f({x'}^{-1}x) = e'_G$ con lo cual $f(x) = f(x')$.

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

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

y que (por la definición de $\overline{f}$) $f = \overline{f} \circ \pi_H$.

Unicidad de $\overline{f}$: Es una consecuencia de la sobreyectividad de π_H. Sean $\overline{f}_1$ y $\overline{f}_2$ tales que $\overline{f}_i \circ \pi = f$ $(i = 1, 2)$, entonces

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

luego $\overline{f}_1 = \overline{f}_2$.

Observación: Con las notaciones como en la proposición anterior, $\mathrm{Im}(\overline{f}) = \mathrm{Im}(f)$ y $\mathrm{Ker}(\overline{f}) = \pi_H(\mathrm{Ker}(f))$. En particular f epimorfismo implica $\overline{f}$ epimorfismo, y si $H = \mathrm{Ker}(f)$ entonces $\overline{f}$ es monomorfismo.

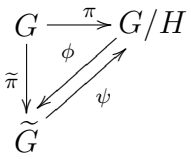
1.5. Teoremas de isomorfismo

1.5.1. Definición por propiedad universal

El grupo G/H queda determinado de manera única por las siguientes propiedades:

- Existe un morfismo de grupos $\pi : G \to G/H$ tal que $\mathrm{Ker}(\pi) = H$.
- Todo morfismo de grupos $f : G \to G'$ tal que $H \subseteq \mathrm{Ker}(f)$ se factoriza de manera única por G/H, o sea, si $f : G \to G'$ es un morfismo de grupos y $f(H) = \{e\}$ entonces $\exists! \overline{f} : G/H \to G'$ (morfismo de grupos) tal que $\overline{f} \circ \pi = f$.

Si $(\widetilde{G}, \widetilde{\pi} : G \to \widetilde{G})$ es un par con las mismas dos propiedades anteriores de $(G/H, \pi)$ entonces $\widetilde{G} \cong G/H$ porque: aplicando la segunda propiedad a G/H y $\widetilde{G}$ sucesivamente se tienen únicos morfismos ϕ y ψ como en el diagrama



tales que $\phi \circ \pi = \widetilde{\pi}$ y $\psi \circ \widetilde{\pi} = \pi$. Luego, por ejemplo $\widetilde{\pi} = \phi \circ \pi = (\phi \circ \psi) \circ \widetilde{\pi}$. Si aplicamos la segunda propiedad al diagrama

$$\begin{array}{ccc} G & \xrightarrow{\widetilde{\pi}} & \widetilde{G} \\ {\scriptstyle \widetilde{\pi}}\downarrow & & \\ \widetilde{G} & & \end{array}$$

a partir de la cuenta anterior vemos que $id_{\widetilde{G}} \circ \widetilde{\pi} = \widetilde{\pi} = (\phi \circ \psi) \circ \widetilde{\pi}$, por unicidad se sigue entonces que $\phi \circ \psi = id_{\widetilde{G}}$. La otra composición es completamente análoga, y queda demostrado así que ϕ y ψ son isomorfismos, uno inverso del otro.

1.5.2. Primer teorema de isomorfismo

Si $f : G \to G'$ es un morfismo de grupos, consideramos $f : G \to \mathrm{Im}(f)$ y $H = \mathrm{Ker}(f)$, entonces $\overline{f} : G/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ es un isomorfismo de grupos. Para esto, basta observar que $\overline{f}$ es mono y epi.

1.5.3. Segundo teorema de isomorfismo

Sean H y K dos subgrupos normales de G tales que $K \subseteq H$ ($\Rightarrow K \triangleleft H$). Se tiene entonces el diagrama conmutativo:

$$\begin{array}{ccc} G & \xrightarrow{\pi_H} & G/H \\ {\scriptstyle \pi_K}\downarrow & \nearrow_{\overline{\pi_H}} & \\ G/K & & \end{array}$$

$\overline{\pi_H}$ es claramente sobreyectiva pues π_H lo es, el núcleo de $\overline{\pi_H}$ es la imagen de H por π_K en G/K o sea H/K, aplicando ahora el primer teorema de isomorfismo a π_H se tiene $\frac{G/K}{H/K} \cong G/H$.

Ejemplo: Si consideramos $\mathbb{Z} \subset \mathbb{R} \subset \mathbb{C}$ (todos grupos con la suma), entonces $\frac{\mathbb{C}/\mathbb{Z}}{\mathbb{R}/\mathbb{Z}} \cong \mathbb{C}/\mathbb{R} \cong \mathbb{R}$.

1.5.4. Tercer teorema de isomorfismo

Sean H y K subgrupos de un grupo G tal que $K \subseteq N_H$ (es decir, $k.H.k^{-1} = H \ \forall k \in K$), si $HK = \{h.k \ / \ h \in H, \ k \in K\}$, entonces HK es un subgrupo de G porque

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

pues $kh'k^{-1} \in H$. Además $(hk)^{-1} = k^{-1}h^{-1} = (k^{-1}h^{-1}k).k^{-1}$.

Notar que $H \triangleleft HK$, por lo tanto tiene sentido calcular HK/H.

Si consideramos la aplicación $K \to HK/H$ dada por $k \mapsto \overline{1.k}$, es sobreyectiva (verificar!), y el núcleo son los elementos de K que también están en H, esto da el isomorfismo:

$$K/(H \cap K) \cong HK/H.$$

1.6. Teorema de Lagrange

Si H es un subgrupo (no necesariamente invariante) de un grupo G, se sigue llamando G/H al conjunto cociente por la relación de equivalencia $\sim_H$ del lema 1.4.2. Si $H \triangleleft G$ entonces G/H es un grupo, si no, es solamente un conjunto.

Definición 1.6.1. *Si G es un grupo y H un subgrupo (normal o no) de G, se llama* **índice de H en G** *al cardinal del conjunto G/H. Se lo nota $(G : H) := \#(G/H)$*

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

El siguiente resultado, si bien se puede generalizar a cardinales arbitrarios, es de principal utilidad cuando $|G| < \infty$. Supongamos ahora entonces que se tiene un grupo finito G y $H \subseteq G$ un subgrupo. Recordando la relación de equivalencia $\sim_H$, para un $x \in G$ 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, $\overline{x} \cap \overline{y} = \emptyset$ o $\overline{x} = \overline{y}$.
2. Para todo $x \in G$: $\#(\overline{x}) = \#(x.H) = |H|$ (verificar!).
3. $\#(G/H) = \#\{\overline{x} : \ x \in G\}$.

En las condiciones anteriores se tiene el siguiente teorema:

Teorema 1.6.2. *(Lagrange) Sea G un grupo, 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 (observación 1. anterior) de sus clases de equivalencia, por lo tanto

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

de la observación 2. anterior se sigue que todos los números que se suman son iguales a $|H|$, por lo tanto $|G| = \sum_{\overline{x} \in G/H} |H| = \#(G/H).|H| = (G : H).|H|$.

Este simple teorema tiene consecuencias inmediatas importantes:

Corolario 1.6.3. *Sea G un grupo finito:*

1. *El orden de cualquier subgrupo de G divide al orden de G.*
2. *Sea $H \triangleleft G$, entonces $|G/H| = \frac{|G|}{|H|}$.*
3. *Sea $a \in G$, se denotará por $\langle a \rangle$ al subgrupo de G dado por el conjunto $\{a^n\}_{n \in \mathbb{Z}}$ (verificar que es un subgrupo, para la definición formal de a^n con $n \in \mathbb{Z}$ ver al principio de la siguiente sección) y se denotará $|a| := |\langle a \rangle|$. Entonces para un grupo finito, $|a|$ es un número que divide a $|G|$. Notar que (ejercicio) $|a| = min\{n \in \mathbb{N} \ / \ a^n = e_G\}$.*
4. *Sea G finito, para todo $x \in G$, $x^{|G|} = e_G$.*
5. *(Fermat) Si $a \in \mathbb{Z}$ y p es un número primo entonces $a^p \equiv a(p)$.*
6. *Si $f : G \to G'$ es un morfismo de grupos y $a \in G$, entonces $|f(a)|$ divide a $|a|$.*
7. *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 todo G.*

Los puntos 1, 2 y 3 son evidentes, demostremos ahora 4:

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

el resultado se sigue ahora de que $x^{|x|} = e_G$.

5.: Si $a \equiv 0(p)$ el resultado es obvio, así que basta probarlo para $\overline{a} \in (\mathbb{Z}_p - \{0\})$.

Consideramos $G = (\mathbb{Z}_p - \{0\}, .)$, que es un grupo porque p es un número primo (por qué?). Por el punto 3., $|raa|$ divide a $|G| = p - 1$, por lo tanto $a^{p-1} \equiv 1(p)$.

6.: Considerar $f|_{\langle a\rangle} : \langle a\rangle \to G'$, $\mathrm{Im}(f|_{\langle a\rangle}) = \langle f(a)\rangle$. Por el teorema de isomorfismo $\langle f(a)\rangle \cong \langle a\rangle / \mathrm{Ker}(f|_{\langle a\rangle})$, entonces $|f(a)| = \frac{|a|}{|\mathrm{Ker}(f|_{\langle a\rangle})|}$.

1.7. Grupos cíclicos

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

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

Claramente, $a^r.a^s = a^s.a^r = a^{r+s}$, es decir, la función $f_a : \mathbb{Z} \to G$ definida por $n \mapsto a^n$ es un morfismo de grupos. De hecho, también vale que si $a, b \in G$ son tales que $ab = ba$ entonces $(ab)^m = a^m b^m$.

Definición 1.7.1. *Un grupo $(G, .)$ se dice* **cíclico** *si existe un elemento $a \in G$ tal que $\forall b \in G,\ \exists m \in \mathbb{Z}$ con $a^m = b$. En otras palabras, G es cíclico si existe un $a \in G$ con $\langle a\rangle = G$. Un tal elemento se dirá un* **generador** *de G.*

Observaciones:

1. Un generador de un grupo cíclico no tiene por qué ser único, por ejemplo $G = (\mathbb{Z}_5, +)$ es un grupo cíclico pues $\mathbb{Z}_5 = \langle\overline{1}\rangle = \langle\overline{2}\rangle = \langle\overline{3}\rangle = \langle\overline{4}\rangle$.

2. Sea G un grupo. Entonces $\forall a \in G$, $|\langle a\rangle| = |a|$.

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

Vimos antes que G_n y $\mathbb{Z}_n$ son grupos isomorfos, pero si $n \neq m$, $\mathbb{Z}_n \ncong \mathbb{Z}_m$ (por qué?); además ningún $\mathbb{Z}_n$ es isomorfo a $\mathbb{Z}$ (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 la da el siguiente teorema que caracteriza a todos los grupos cíclicos.

Teorema 1.7.2. *Sea G un grupo cíclico, ($G = \langle a \rangle$ para algún $a \in G$). Entonces:*

$$\text{si } |a| = n \Rightarrow G \cong (\mathbb{Z}_n, +)$$
$$\text{si } |a| = \infty \Rightarrow G \cong (\mathbb{Z}, +)$$

Demostración: Por hipótesis, para algún $a \in G$ vale $\langle a \rangle = G$. Consideramos la función $f : \mathbb{Z} \to G$ definida por $m \mapsto a^m$. Como $a^{r+s} = a^r a^s$, f es un morfismo de grupos, y la imagen de f coincide con $\langle a \rangle = G$, entonces por el primer teorema de isomorfismo $G \cong \mathbb{Z}/\operatorname{Ker}(f)$. Si $|a| = \infty$ entonces la única posibilidad de que $f(m) = a^m = e_G$ es $m = 0$, por lo tanto $\operatorname{Ker}(f) = \{0\}$ y $G \cong \mathbb{Z}$.

Por otro lado, definimos antes $|a| := |\langle a \rangle|$, . Entonces a partir la definición misma de orden de un elemento, si $|a| = n$ resulta $n.\mathbb{Z} = \operatorname{Ker}(f)$ (¿por qué es exactamente $n.\mathbb{Z}$?), luego $G \cong \mathbb{Z}/n.\mathbb{Z} \cong \mathbb{Z}_n$.

Corolario 1.7.3. *1. Si G y G' son dos grupos cíclicos y $|G| = |G'|$ entonces $G \cong G'$.*

2. Si $|G| = p$ con $p \in \mathbb{N}$ un número primo, entonces $G \cong \mathbb{Z}_p$.

Para demostrar 2., basta ver que G es cíclico. Tomemos $a \in G$ un elemento cualquiera que no sea e_G y consideremos el subgrupo $\langle a \rangle$. Por Lagrange, el orden de este subgrupo divide al orden de G que es p, por lo tanto es 1 ó p, pero $|\langle a \rangle| \neq 1$ ya que contiene por lo menos a los elementos a y e_G, luego $\langle a \rangle = G$.

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 actúa a izquierda) sobre X si y sólo si se tiene dada una función, llamada acción:*

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

que denotamos $g.x$, y que verifica:

- Asociatividad*: $(g.g').x = g(g'.x)$ para todo $x \in X$, $g, g' \in G$. (Atención que 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*: $e_G.x = x \ \forall \ x \in X$.*

Si A, B, C son tres conjuntos, es válida la siguiente igualdad:

$$C^{A \times B} = (C^B)^A$$

es decir, si una función tiene dos variables, fijando una se obtiene una función de la otra:

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

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

$$\begin{aligned} \phi_g := \phi(g, -) = g.- : X &\to X \\ x &\mapsto g.x \end{aligned}$$

Las propiedades de la acción aseguran que $\phi_g \circ \phi_h = \phi_{gh}$ (verificar!), en particular $\phi_{g^{-1}} \circ \phi_g = \phi_g \circ \phi_{g^{-1}} = \phi_{e_G} = id_X$. Esto dice que ϕ_g es una función biyectiva, con inversa $\phi_{g^{-1}}$. Por lo tanto, dar una acción de G en X es dar una función que sale del grupo G y llega al grupo de funciones biyectivas del conjunto X (que denotamos $\mathcal{S}(X)$). La propiedad de asociatividad de la acción no dice otra cosa que el hecho de que esta función es un morfismo de grupos, i.e. la aplicación

$$\begin{aligned} G &\to \mathcal{S}(X) \\ g &\mapsto \phi_g \end{aligned}$$

verifica $\phi_g \circ \phi'_g = \phi_{g.g'}$.

Esta aplicación junto al conjunto X 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. $G = G_n$ ($n \in \mathbb{N}$), $X = \mathbb{R}^2$ identificado con $\mathbb{C}$).

$$\begin{aligned} &G_n \times \mathbb{C} \to \mathbb{C} \\ &(\omega_n, z) \mapsto (\omega_n.z) \text{ rotación en ángulo } = arg(\omega_n) \end{aligned}$$

Es decir, G_n se representa como rotaciones del plano.

2. $G = \mathcal{S}_n$ (grupo simétrico de $n!$ elementos). $X = \mathbb{R}^n$,

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

Notar que en realidad σ actúa como una transformación lineal, aquí la acción es un morfismo $\mathcal{S}_n \to GL_n(\mathbb{R}) \subset \mathcal{S}(\mathbb{R}^n)$.

3. *Conjugación* o acción por automorfismos interiores. En este caso, G opera sobre sí mismo:

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

Verificar que tiene las propiedades para ser una acción. Análogamente al caso anterior, la acción respeta la estructura adicional que existe sobre el conjunto $X = G$, pues la acción tiene por imagen a los automorfismos de grupo de G ($\subset \mathcal{S}(G)$):

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

La imagen de la acción es un subgrupo de los automorfismos de grupo de G ($\mathrm{Aut}(G)$) que se llama es subgrupo de automorfismos interiores, y se denota $\mathrm{Aut}_{int}(G)$. Si el grupo 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

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

El núcleo de la acción son los elementos de g tales que $g.-.g^{-1}$ define el automorfismo identidad de G, que es el neutro de $\mathrm{Aut}(G)$. Pero

$$g.-.g^{-1} = id_G \Leftrightarrow gxg^{-1} = x \ \forall x \in G \Leftrightarrow gx = xg \forall x \in G$$

es decir, $g \in \mathcal{Z}(G)$, por lo tanto

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

4. G actúa por conjugación en el conjunto de partes de G: $\mathcal{P}(G) = \{X : X \subseteq G\}$. Si $A \in \mathcal{P}(G)$, $g \in G$, sea $\phi_g(A) = g.A.g^{-1} = \{g.a.g^{-1} : \ a \in A\} \in \mathcal{P}(A)$. Notar que esta acción se restringe bien al subconjunto de $\mathcal{P}(G)$ formado por los subconjuntos de G que además son subgrupos de G. ¿Quiénes son los "puntos fijos" por la acción de G?

5. Traslaciones: Si $X = G$, dado $g \in G$ se define $T_g : G \to G$ por $T_g(h) = gh$. Observar que T_g **no** es un morfismo de grupos (¿por qué?). También G actúa por traslaciones sobre $\mathcal{P}(G)$.

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

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

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

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

$$\begin{aligned} G &\to \mathcal{S}(X) \\ g &\to id_X \ \forall g \in G \end{aligned}$$

Cuando X sea un conjunto sobre el que G actúa de esta manera, se dirá 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:

Dado $g \in G$, se puede considerar el subconjunto más grande de X sobre el que el elemento g actúa trivialmente: $\{x \in X \ / \ g.x = x\}$. Si por ejemplo G actúa sobre sí mismo por conjugación, este subconjunto es el centralizador de g en G, si G actúa por traslaciones este conjunto es vacío.

Inversamente, si $x \in X$, se puede considerar el subgrupo de G formado por los elementos que fijan x: $\{g \in G \ / \ g.x = x\}$, que llamamos **estabilizador** de x y denotamos $\mathcal{E}_x$. También dado un $x \in X$ se puede buscar a todos los elementos de X que son "accesibles" a través de G, 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 $x \in X$. Se define la* **órbita** *de x, y se nota $\mathcal{O}_x$ al siguiente subconjunto de X:*

$$\{g.x : \ g \in G\} = \{y \in X \ / \ \exists g \in G \text{ tal que } y = g.x\}$$

Ejemplos:

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

2. Consideremos $\mathbb{Z}_2$ actuando en S^1 por

$$\begin{cases} \overline{0}(x) = x \\ \overline{1}(x) = -x \end{cases}$$

   Entonces $\mathcal{O}_x = \{x, -x\}$.

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

4. Sea $G = G_4$, X el conjunto de vértices de un cuadrado en el plano en donde G actúa por rotaciones (i rota en 90 grados en el sentido contrario al movimiento de las agujas de -casi todos- los relojes). Entonces la órbita de cualquier punto coincide con todos los elementos de X. 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 $\mathcal{O}_y = X$, $\forall y \in X$.

Observación: Las órbitas de una acción de G dan una partición de X, pues la noción de que dos elementos x, y sean tales que exista un elemento $g \in G$ con $x = g.y$ es una relación de equivalencia. Más precisamente:

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

Recordamos que si G opera en X y $x \in X$ es un elemento dado, se llama subgrupo **estabilizador** o **grupo de isotropía** de x al siguiente subgrupo de G, $\mathcal{E}_x := \{g \in G \ / \ g.x = x\}$ (verificar que es un subgrupo). Notar que el "tamaño" de este subgrupo $\mathcal{E}_x$ de alguna manera se contrapone al "tamaño" de la órbita del elemento x, pues 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 $x \in X$. Entonces $\#\mathcal{O}_x = \#G/\mathcal{E}_x$.*

Demostración: Si $g\mathcal{E}_x = g'\mathcal{E}_x$ entonces $g = g'h$ para algún $h \in \mathcal{E}_x$, con lo cual $g.x = g'.h.x = g'.x$. Esto dice que la funcion $G/\mathcal{E}_x \to \mathcal{O}_x$ dada por $g\mathcal{E}_x \mapsto g.x$ esta bien definida, y claramente es suryectiva. Por otro lado, si $g.x = g'.x$ entonces $(g')^{-1}.g.x = x$, luego $(g')^{-1}.g \in \mathcal{E}_x$, por lo tanto $g\mathcal{E}_x = g'\mathcal{E}_x$ y hemos demostrado la inyectividad. Como encontramos una biyeccion de conjuntos, sus cardinales son iguales.

Corolario 1.9.3. *Sea G un grupo finito que actúa en 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. Si G actúa por conjugación sobre el conjunto de subgrupos de G, y $H \subset G$ es un subgrupo, entonces la órbita de H son todos los subgrupos conjugados a H y el estabilizador de H es N_H (el mayor subgrupo de G tal que $H \lhd N_H$).

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

3. Sea V un k-espacio vectorial, $G = (k - \{0\}, .)$, $X = V - \{0\}$, G actúa en X vía

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

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

4. Sea X un conjunto y $G = \mathcal{S}(X) =$\{funciones biyectivas de 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 (ejercicio) G opera transitivamente sobre X. Si $x \in X$, $\mathcal{E}_x = \{f : X \to X \text{ tal que } f(x) = x\}$ se identifica con $\mathcal{S}(X - \{x\})$.

5. Si G actúa sobre G por conjugación, dados $s, t \in G$, $\mathcal{O}_s = \mathcal{O}_t$ si y sólo si s y t son conjugados, en ese caso, $\mathcal{E}_s$ es un subgrupo conjugado a $\mathcal{E}_t$ (verificar!) y por lo tanto isomorfo, en particular $|\mathcal{E}_s| = |\mathcal{E}_t|$

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

Proposición 1.9.4. *Consideramos a un grupo G actuando sobre sí mismo por conjugación y $s \in G$. Existe una biyección*

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

luego $\#(\mathcal{O}_s) = (G : \mathcal{E}_s)$

y su respectivo corolario:

Corolario 1.9.5. *El cardinal de toda órbita de G actuando sobre sí mismo por 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 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 $\exists\{a_1, ..., a_k\} \subset G$ que no están en el centro tales que*

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

($\coprod$ significa unión disjunta) luego

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

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

Demostración: Como la acción define una relación de equivalencia sobre el grupo G, se lo puede escribir como unión disjunta de dichas clases, que en este caso son las órbitas. Las órbitas que son puntuales (las que tienen un único elemento) corresponden a los elementos del centro de G, juntando por separado a estos elementos y eligiendo un a_i por cada órbita no puntual se tiene demostrado el teorema (al menos la primera ecuación). Tomando cardinales, como la unión es disjunta se obtienen sumas, y los ordenes de las órbitas coinciden con los índices de los estabilizadores de los a_i gracias a la proposición anterior.

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

Demostración: La demostración se obtiene considerando primero el caso conmutativo y después el caso no conmutativo. El caso conmutativo no usa la

ecuación de clases, y el caso no conmutativo es una consecuencia del anterior más la ecuación de clases.

1er. caso: G conmutativo.

Se procede por inducción en el orden de G. Sea $a \in G$ un elemento cualquiera salvo el neutro. Si $|a|$ es un múltiplo de p, por ejemplo $|a| = k.p$, entonces el elemento a^k tiene orden p. Si $|a|$ no es múltiplo de p, entonces se considera el grupo $G/\langle a\rangle$ (G conmutativo entonces todos sus subgrupos son invariantes), como $|a|$ no es un múltiplo de p, se sigue que p divide a $|G/\langle a\rangle|$, que es un grupo de orden estrictamente menor que $|G|$ porque $a \neq e_G$ y se aplica hipótesis inductiva al grupo cociente. Sea entonces $\overline{z} \in G/\langle a\rangle$ tal que $|\overline{z}| = p$, entonces $|z|$ es un múltiplo de p y se procede como al principio.

2do. caso: G no conmutativo.

Si p divide al orden del centro de G se considera $\mathcal{Z}(G)$, que es conmutativo, y se está en el caso anterior. Supondremos entonces que p no divide al orden de $\mathcal{Z}(G)$.

Utilizando la ecuación de clases, existen $\{a_1, \ldots, a_k\} \subset G$ 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 $(G : \mathcal{Z}(a_i)) = |G|/|\mathcal{Z}(a_i)|$, entonces $|\mathcal{Z}(a_i)|$ es un múltiplo de p. Considerando ahora el grupo $\mathcal{Z}(a_i)$, como es un subgrupo propio tiene orden estrictamente menor, usando un argumento inductivo se tiene que existe un elemento en ese grupo de orden p y listo.

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 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

1. Calcular el centro de los siguientes grupos:

   a) El grupo cuaterniónico o de Hamilton: $\mathcal{H} = \{\pm 1, \pm i, \pm j, \pm k\}$ donde la "tabla de multiplicación" de $\mathcal{H}$ está dada por

   $$i.j = -j.i = k \ ; \ jk = -kj = i \ ; \ ki = -ik = j \ ; \ i.i = j.j = k.k = -1$$

   (verificar primero que $\mathcal{H}$ es un grupo!)

   b) El grupo dihedral: D_n con $n > 2$ (sug. considere por separado n par o impar). Recordamos que $D_n = \langle r, s \ / \ r^n = 1, \ s^2 = 1, \ rs = sr^{-1} \rangle$.

   c) Calcular *todos* los subgrupos de $\mathcal{H}$. Ver que a pesar de que $\mathcal{H}$ no es conmutativo, todos sus subgrupos son invariantes. (nombre: un grupo con esa propiedad se llama Hamiltoniano).

2. Sean X un conjunto y G un grupo. Entonces $G^X = Func(X, G) = \{f : X \to G\}$ es un grupo con la multiplicación punto a punto inducida por la multiplicación de G, i.e. el producto de dos funciones se calcula como $(f.g)(x) := f(x).g(x)$. Si X y G son finitos, cuál es el orden de G^X en términos del orden de G y el cardinal de X? Sea $H_{x_0} \subset Func(X, G)$ el subconjunto formado por las funciones $f : X \to G$ tales $f(x_0) = e_G$, es H_{x_0} un subgrupo? Es normal? Sea $g \neq e_G$ y $H_{x_0,g} \subset Func(X, G)$ el subconjunto de funciones f que verifican $f(x_0) = g$, es $H_{x_0,g}$ un subgrupo?

3. Sean X y G como antes, $x_0 \in X$ y $ev_{x_0} : Func(X, G) \to G$ dado por

   $$ev_{x_0}(f) := f(x_0)$$

   donde $f : X \to G$. Verificar que ev_{x_0} es un morfismo de grupos. Calcular núcleo e imagen.

4. Sean K y G dos grupos, y $\mathrm{Hom}_{Gr}(K, G)$ el subconjunto de $Func(K, G)$ formado por las funciones que son morfismos. ¿Es un subgrupo? Responder la pregunta para el caso G conmutativo y para el caso G no conmutativo.

5. Sean G y G' grupos, G' abeliano y $f : G \to G'$ un morfismo de grupos. Ver que necesariamente $[G, G] \subseteq \mathrm{Ker}(f)$.

6. Si G es un grupo cualquiera, ver que la función

   $$\begin{aligned} ev_1 : \mathrm{Hom}_{Gr}(\mathbb{Z}, G) &\to G \\ f &\mapsto f(1) \end{aligned}$$

   es biyectiva.

7. Sea G un grupo **abeliano**. Considerar el grupo $(\mathbb{Z} \oplus \mathbb{Z})$ que consiste en $\mathbb{Z} \times \mathbb{Z}$ como conjunto y donde la suma está definida coordenada a coordenada. Ver que la función

   $$\begin{aligned} \mathrm{Hom}_{Gr}(\mathbb{Z} \oplus \mathbb{Z}, G) &\to G \times G \\ f &\mapsto (f(1,0), f(0,1)) \end{aligned}$$

es una biyección. ¿es cierto el enunciado anterior si se cambia G abeliano por G no abeliano? Dar una demostración o un contraejemplo según el caso.

8. Ver que $\mathrm{Hom}_{Gr}(\mathbb{Q},\mathbb{Z})$ sólo contiene el morfismo nulo.

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

$$f(\pm 1)=(0,0)\ ;f(\pm i)=(1,0)\ ;f(\pm j)=(0,1)\ ;f(\pm k)=(1,1)$$

un morfismo de grupos? En tal caso calcule núcleo e imagen.

10. ¿Existe un isomorfismo de grupos entre:

   a) $\mathbb{Z}_4\cong\mathbb{Z}_2\oplus\mathbb{Z}_2$?

   b) $\mathbb{Z}_{2n}\cong D_n$?

   c) $\mathbb{Z}_8\cong\mathbb{Z}_4\oplus\mathbb{Z}_2\cong\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2\cong\mathcal{H}\cong D_4$?

   d) $(\mathbb{R},+)\cong(\mathbb{R}_{>0},.)$?

   e) $(\mathbb{R},+)\cong(\mathbb{R}-\{0\},.)$?

11. Sean $m,n\in\mathbb{N}$ coprimos, ver que $\mathrm{Hom}_{Gr}(\mathbb{Z}_m,\mathbb{Z}_n)$ contiene sólo al morfismo nulo.

12. Sea k un cuerpo, ver que $det: GL_n(k)\to(k^*,.)$ es un morfismo de grupos, por lo tanto $Sl_n(k):=\{A\in k^{n\times n}\ /\ det(A)=1\}$ es un subgrupo (invariante) de $GL_n(k)$. ¿Cuánto vale $GL_n(k)/Sl_n(k)$?

13. Calcular el orden de $Sl_2(\mathbb{Z}_3)$. 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.

14. Sea H un subgrupo discreto de $(\mathbb{Q},+)$. Ver que es cíclico, por lo tanto $H=\frac{m}{n}.\mathbb{Z}$ para un (único a menos de signo) racional $\frac{m}{n}$.

15. Sea H un subgrupo de $\mathbb{Q}$ finitamente generado. Demostrar que H es cíclico. Concluir que $\mathbb{Q}$ no es finitamente generado.

16. Ver que $\mathcal{S}_3\cong D_3$.

17. Ver que el grupo de isometrías del tetraedro es isomorfo a S_4.

18. Calcular el centralizador de $\begin{pmatrix}0&1\\-1&0\end{pmatrix}$ en $Sl_2(\mathbb{Z}_3)$ y en $GL_2(\mathbb{Z}_3)$.

19. Sea G un grupo, ver que la aplicación $G\to\mathrm{Aut}_{Gr}(G)$, $g\mapsto g.-.g^{-1}$ $(x\mapsto g.x.g^{-1})$ es un morfismo de grupos. Si además H es un subgrupo de G, ver que el morfismo de grupos $G\to\mathrm{Aut}_{Gr}(H)$ con la misma fórmula que el anterior queda bien definido $\Leftrightarrow$ H es un subgrupo invariante.

20. *Producto semidirecto.* Sean H y K dos grupos y $\phi:K\to\mathrm{Aut}_{Gr}(H)$ un morfismo de grupos, es decir, K actúa (multiplicativamente) sobre H (por ejemplo si H y K son dos subgrupos de un grupo G, $H\lhd G$ y $K\to\mathrm{Aut}_{Gr}(H)$, $k\mapsto k.-.k^{-1}$). Se define sobre el conjunto $H\times K$ la operación:

$$(h,k).(h'.k'):=(h.(\phi(k))(h'),k.k')$$

(en el ejemplo entre paréntesis sería $(h,k).(h'.k')=(h.(k.(h').k^{-1}),k.k')$).

a) Probar que con esa operación, $H \times K$ tiene una estructura de grupo, que llamaremos **producto semidirecto** de H y K y notaremos $H \rtimes K$ (o $H \rtimes_\phi K$).

b) Encontrar el inverso de (h, e_K), el inverso de $(1_H, k)$, y el inverso de un (h, k) cualquiera.

c) Probar que el conjunto $H \times \{1_K\}$ es un subgrupo (isomorfo a H) invariante en $H \rtimes K$, más aún $(1_H, k)(h, 1_K)(1_H, k)^{-1} = ((\phi(k))(h), 1_K)$ (notar que esta igualdad es obvia para el ejemplo entre paréntesis).

d) Ver que la función $\pi : H \rtimes K \to K$ definida por $\pi(h, k) = k$ es un morfismo de grupos. Verificar que $\mathrm{Ker}(\pi) = H \times \{1_K\}$ (otra manera de ver que es invariante).

e) ¿Es siempre $\{1_H\} \times K$ invariante en $H \rtimes K$?

f) Sea G grupo y $\pi : G \to K$ un morfismo sobreyectivo (por lo tanto $K \cong G/\mathrm{Ker}(\pi)$) y sea $H = \mathrm{Ker}(\pi)$. Demostrar que *si existe* un morfismo de grupos $j : K \to G$ tal que $\pi(j(k)) = k \ \forall k \in K$ entonces $G \cong H \rtimes K$.

g) $\{1_H\} \times K$ es invariante en $H \rtimes K \Leftrightarrow$ los elementos de $H \times \{1_K\}$ conmutan con los elementos de $\{1_H\} \times K$.

h) Ver que $(-)^n : S^1 \to S^1$ $(z \to z^n)$ es un epimorfismo con núcleo G_n, pero S^1 *no* es isomorfo ni a $G_n \rtimes S^1$ ni a $S^1 \rtimes G_n$ para ninguna acción de S^1 sobre G_n ni de G_n sobre S^1.

21. Caracterizar $\mathrm{Hom}_{Gr}((\mathbb{Z}_n, +), (\mathbb{Z}_n, +))$, ¿cuáles de esos morfismos son isomorfismos? Caracterizar $\mathrm{Aut}_{Gr}((\mathbb{Z}_n, +))$.

22. Ver que $\mathcal{S}_3 \cong D_3 \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_2$ para una acción adecuada de $\mathbb{Z}_2$ sobre $\mathbb{Z}_3$.

23. Demostrar que $\mathcal{S}_n/A_n \cong \mathbb{Z}_2$, más aún, $\mathcal{S}_n \cong A_n \rtimes \mathbb{Z}_2$.

24. Ver que $\mathrm{Aut}_{Gr}((\mathbb{Z}_n, +)) \cong (\mathcal{U}(\mathbb{Z}_n), .)$ (las unidades de $\mathbb{Z}_n$). Verificar que $|\mathcal{U}(\mathbb{Z}_n)| = \phi(n)$ donde $\phi : \mathbb{N} \to \mathbb{N}$ es la función de Euler, $\phi(n) = \#\{m \in \mathbb{N} \text{ con } m < n \text{ y } (m, n) = 1\}$.

25. Este ejercicio, entre otras cosas, muestra que la función de Euler es multiplicativa con respecto a los pares de números coprimos. Sean n y m dos números naturales coprimos, entonces

a) $\mathbb{Z}_{n.m} \cong \mathbb{Z}_n \oplus \mathbb{Z}_m$

b) $\mathrm{Hom}_{Gr}(\mathbb{Z}_n, \mathbb{Z}_m) = \mathrm{Hom}_{Gr}(\mathbb{Z}_m, \mathbb{Z}_n) = 0$

c) $\mathrm{Hom}_{Gr}(\mathbb{Z}_n \oplus \mathbb{Z}_m, \mathbb{Z}_n \oplus \mathbb{Z}_m) \cong \mathrm{Hom}_{Gr}(\mathbb{Z}_n, \mathbb{Z}_n) \oplus \mathrm{Hom}_{Gr}(\mathbb{Z}_m, \mathbb{Z}_m)$

d) $\mathrm{Aut}_{Gr}(\mathbb{Z}_{n.m}) \cong \mathrm{Aut}_{Gr}(\mathbb{Z}_n) \times \mathrm{Aut}_{Gr}(\mathbb{Z}_m)$

e) Concluir que $\phi(mn) = \phi(m)\phi(n)$ para todo par de números m, n con $(m, n) = 1$.

26. Sea G el grupo de transformaciones afines de $\mathbb{R}$, es decir, el grupo de funciones de la forma $x \mapsto a.x + b$ con $a \neq 0$. Ver que es efectivamente un grupo (encontrar inversos), y que es isomorfo al subgrupo de matrices inversibles formado por las matrices de la forma

$$G \cong \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \text{ con } a, b \in \mathbb{R},\ a \neq 0 \right\}$$

Ver que $G \cong (\mathbb{R}, +) \rtimes (\mathbb{R} - \{0\}, .)$.
Si se considera el grupo de transformaciones afines en $\mathbb{R}^n$, es decir, las transformaciones del tipo $x \mapsto A.x^t + v$ con $A \in GL_n(\mathbb{R})$ y $v \in \mathbb{R}^n$, ver que este grupo es isomorfo a $(\mathbb{R}^n, +) \rtimes GL_n(\mathbb{R})$.

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

$$\begin{array}{rcl} \overline{0}.(x, y, z) & = & (x, y, z) \\ \overline{1}.(x, y, z) & = & (y, z, x) \\ \overline{2}.(x, y, z) & = & (z, x, y) \end{array}$$

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

28. Sea $G = \mathbb{Z}_4$ actuando en $\mathbb{R}^4$ por la fórmula

$$\overline{1}.(x, y, z, t) = (t, x, y, z)$$

descomponer a $\mathbb{R}^4$ en suma directa de subespacios $\mathbb{Z}_4$-estables lo "más chicos posible". (sugerencia: dado un subespacio estable buscar complementos con los ortogonales).

29. Sea $\mathcal{H}$ el grupo de Hamilton actuando sobre sí mismo por conjugación. Para cada elemento de $\mathcal{H}$ describir las órbitas. Separar las órbitas puntuales para así encontrar de nuevo el centro. Encontrar los "a_i" del teorema de la ecuación de clases y los respectivos subgrupos $\mathcal{Z}(a_i)$.

30. Sea G un grupo finito, $|G| = p^n$ para algún número primo p, entonces el centro de G es no trivial, i.e. $|Z(G)| > 1$.

31. Sea G un grupo de orden p^2, entonces G es abeliano. Ver que si $|G| = p^2$ entonces $G \cong \mathbb{Z}_{p^2}$ o bien $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$. (por qué $\mathbb{Z}_{p^2} \ncong \mathbb{Z}_p \oplus \mathbb{Z}_p$?).

32. Sea G un grupo no abeliano de orden p^3, entonces $Z(G) = [G, G]$ y $|Z(G)| = p$ (en particular $Z(G)$ es cíclico, y está generado por cualquiera de sus elementos salvo la identidad). Ver que el grupo de matrices de la forma $\left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \text{ con } a, b, c \in \mathbb{Z}_p \right\}$ es un ejemplo de grupo no abeliano de orden p^3. Describir en este caso $[G, G]$.

33. **Teoremas de Sylow**: Este ejercicio es una guía o esquema de demostración de los teoremas de Sylow, que son los siguientes:

    Sea G un grupo finito, p un número primo, supongamos que $|G| = p^r.m$ donde $(p, m) = 1$.

    - (1er teorema de Sylow) Existe por lo menos un subgrupo S de G tal que $|S| = p^r$. Un tal subgrupo se llamara un p-subgrupo de Sylow.
    - (2do teorema de Sylow) Si S y S' son dos p-subgrupos de Sylow de G, entonces son conjugados.
    - (3er teorema de Sylow) La cantidad de p-subgrupos de Sylow de G es un número congruente a 1 modulo p.

    Se propone el siguiente esquema:

    1 Hacer inducción en el orden de G. Resolver primero el caso G conmutativo. Despues para el caso no conmutativo, separar a su vez el caso $|\mathcal{Z}(G)| = 1$ y $|\mathcal{Z}(G)| > 1$. Para el caso $|\mathcal{Z}(G)| > 1$ considerar el grupo (de orden estrictamente menor!) $G/\mathcal{Z}(G)$. Para el caso $|\mathcal{Z}(G)| = 1$, a partir de la ecuación de clases, deducir que existe un subgrupo $\mathcal{E}_i$ tal que $|\mathcal{E}_i| = p^r.m'$ con $m' < m$, y usar la hipótesis inductiva en $\mathcal{E}_i$.

    2 Para el segundo teorema, también por inducción en G, seguir la misma estructura que en el 1er teorema, es decir, resolver primero el caso conmutativo, después suponer G no conmutativo y $|\mathcal{Z}(G)| > 1$ y considerar $G/\mathcal{Z}(G)$. Si p^r divide a $|\mathcal{Z}(G)|$ mostrar que todos los subgrupos de Sylow están incluidos en el centro. Si no, dados S y S' dos subgrupos de Sylow, considerar $\langle S, \mathcal{Z}(G)\rangle$ y demostar que tiene orden menor que G, y que S' está contenido en $\langle S, \mathcal{Z}(G)\rangle$. Finalmente si $|\mathcal{Z}(G)| = 1$ considerar el subgrupo $\mathcal{E}_i$ que provee la ecuación de clases.

    3 Para el tercer teorema, considerar el conjunto $X = \{S/\ S$ es p-subgrupo de Sylow de $G\}$. Como dos grupos conjugados son isomorfos, por lo tanto tienen el mismo orden, G actúa por conjugación en X, y a partir del teorema anterior la acción es transitiva. ...

2

Anillos

2.1. Anillos: definiciones básicas y ejemplos

Si G es un grupo finito de n elementos, siempre puede identificarse a G con un subgrupo del grupo de permutaciones $\mathcal{S}_n$ de la siguiente forma:
Si $G = \{x_1, ..., x_n\}$, dado un $g \in G$, la multiplicación por g es una biyección de G en G (con inversa multiplicar por g^{-1}), luego existe una única permutación $\sigma_g \in \mathcal{S}_n$ tal que $g.x_i = x_{\sigma_g(i)}$ $\forall i = 1, ..., n$. La función $g \mapsto \sigma_g$ es claramente un monomorfismo.

A su vez, $\mathcal{S}_n$ puede pensarse como un subgrupo de las transformaciones lineales biyectivas de un espacio vectorial V de dimensión n, simplemente eligiendo una base $\{v_1, ..., v_n\}$ y permutando esos elementos. Es decir: a cada $\sigma \in \mathcal{S}_n$ se le asocia la única transformación lineal t_σ tal que $t_\sigma(v_i) = v_{\sigma(i)}$. Se dice entonces que $(V, (\sigma \mapsto t_\sigma))$ es una **representación** de $\mathcal{S}_n$, es decir, los elementos de $\mathcal{S}_n$ se "representan" como transformaciones lineales de algún espacio vectorial.

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 $(A, +, .)$ donde $(A, +)$ es un grupo abeliano y*

$. : A \times A \to A$ *se dirá un* **anillo con unidad** *si se verifican las siguientes propiedades:*

1. (Asociatividad del producto) $\forall a, b, c \in A$, $(a.b).c = a(b.c)$
2. (Unidad) *Existe un elemento en* A *distinto del cero de* $(A, +)$ *que llamaremos* 1_A *(o simplemente* 1*) tal que* $1.a = a$,$1 = a$ $\forall a \in A$.
3. (Distributividad) $\forall a, b, c \in A$, $a.(b+c) = a.b+a.c$ *y* $(a+b).c = a.c+b.c$.

Si además se satisface $a.b = b.a$ *para todo par* $a, b \in A$*, el anillo se dirá* **conmutativo**.

Observaciones:

1) En la definición, se pide $1 \neq 0$, porque si fuera $1 = 0$ resultaría que $a = a$,$1 = a$,$0 = 0$ para cualquier elemento $a \in A$, luego $A = \{0\}$.

2) Dado $(A, +, .)$ un anillo unitario, el elemento 1_A es único.

3) Si $(A, +, .)$ es una terna que satisface todos los puntos de la definición de anillo salvo la de existencia del 1_A, A se llamará un anillo sin unidad. Sin embargo, todo anillo sin unidad puede incluirse en un anillo con unidad, esta afirmación se precisará en los ejercicios.

Son ejemplos de anillos $(\mathbb{Z}, +, .)$, $(\mathbb{Q}, +, .)$, $(\mathbb{R}, +, .)$, $(\mathbb{C}, +, .)$, $(\mathbb{Z}_n, +, .)$, $(k[x], +, .)$(con k un anillo).

Si $(A, +, .)$ es un anillo, entonces también lo es $M_n(A) = \{$ matrices de $n \times n$ con coeficientes en $A\}$ con suma coeficiente a coeficiente y el producto usual de matrices.

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

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 $a.a' = a'.a = 1$.

Es decir que todo elemento no nulo de A tiene un **inverso a izquierda** (o sea, dado $a \in A$, existe $a' \in A$ tal que $a'.a = 1$) y un **inverso a derecha**, que en estos ejemplos coinciden (y en general, coinciden?).

Observación: Si a es inversible a izquierda, dados $x, y \in A$, $ax = ay$ implica $x = y$.

Si todo elemento de A es inversible a izquierda y a derecha, A se dirá un **anillo de división**.

Observación: Existen anillos de división no conmutativos, por ejemplo, los cuaterniones.

Consideremos ahora el anillo de matrices $M_2(\mathbb{Q})$. El elemento $x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ es claramente no nulo, sin embargo existen matrices no nulas $z \in M_2(\mathbb{Q})$ tales que $x.z = 0$ (en este caso x se llamará un **divisor de cero a izquierda** y z se llamará un **divisor de cero a derecha**. Se ve facilmente que $x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ no puede tener un inverso a izquierda.

Generalizando este razonamiento 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 se dice un* **anillo íntegro**. *Si además el producto en A es conmutativo, A se dirá un* **dominio íntegro**.

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

Ejemplos:

1. (de anillo íntegro no conmutativo) Sea k un cuerpo, consideremos $k\{x, \delta_x\}$, el anillo de polinomios (no conmutativos) en x y δ_x, donde x y δ_x verifican la relación $\delta_x.x - x.\delta_x = 1$.

2. (de dominio íntegro que no es anillo de división) $k[x]$ con k cuerpo.

3. (de anillo de división que no es conmutativo) El anillo de cuaterniones.

Consideremos ahora los anillos $(\mathbb{Z}, +, .)$ y $(\mathbb{R}, +, .)$. Se observa que la suma y el producto de enteros es en realidad la restricción de la suma y el producto en $\mathbb{R}$ al subconjunto $\mathbb{Z}$, y que $1_{\mathbb{Z}} = 1_{\mathbb{R}}$. Es decir que $\mathbb{Z}$ hereda su estructura de anillo por ser un subconjunto de $\mathbb{R}$ que cumple ciertas propiedades.

Definición 2.1.3. *Dados un anillo $(A, +, .)$ y un subconjunto B de A, se dice que B es un* **subanillo** *de A si y solo si:*

1. *$(B,+)$ es un subgrupo de $(A,+)$.*
2. *$1_A \in B$.*
3. *B es cerrado para el producto, es decir, dados $x, y \in B$, entonces $x._A y \in B$.*

Ejemplos:

1. $(\mathbb{Z},+,.)$, $(\mathbb{Q},+,.)$, $(\mathbb{R},+,.)$, $(\mathbb{C},+,.)$ son subanillos de cada uno de los siguientes.
2. 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 (por ejemplo, los enteros como subanillo de los racionales).

A continuación, se construirá un importante ejemplo de anillo (ya 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, se le puede asociar de manera natural un anillo llamado **anillo del grupo** G y notado $k[G]$. Los elementos de $k[G]$ son combinaciones lineales finitas con coeficientes en k de elementos del grupo G, es decir que como conjunto:

$$k[G] = \{\sum_{g\in G} \lambda_g.g, \text{ tal que } \lambda_g \in k \text{ y } \lambda_g = 0 \text{ salvo para finitos elementos de } G\}$$

Notación: $\{g \in G \ / \ \lambda_g \neq 0\}$ se llama **soporte** de $\sum_{g\in G} \lambda_g.g$.

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

$$\sum_{g\in G} \lambda_g.g + \sum_{h\in G} \mu_h.h := \sum_{g\in G} (\lambda_g + \mu_g).g$$

Observación: si las dos primeras sumas son finitas, la tercera también lo es. 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, es decir:

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

Por ejemplo, si se tienen dos elementos $\lambda.g,\ \mu.h\ \in k[G]$, el producto de estos dos es simplemente $(\lambda.g).(\mu.h) = (\lambda\mu).(g.h)$, y si se tienen 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 esas operaciones $(k[G], +, .)$ resulta un anillo con unidad. ¿Cuál es 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 sólamente un monoide con elemento neutro. La asociatividad de G implica la asociatividad del producto de $k[G]$, el elemento neutro de G funciona como unidad del producto de $k[G]$. Se puede definir entonces el anillo de un monoide (con elemento neutro) M, notado también $k[M]$. Por ejemplo $k[\mathbb{N}_0]$; este anillo se llama **anillo de polinomios** en una variable a coeficientes en k.

2.2. Morfismos

En un anillo existen una estructura de grupo abeliano y una multiplicación, luego, así como en el caso de grupos 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. *Dados dos anillos unitarios $(A, +_A, .A)$ y $(B, +_B, .B)$, un* **morfismo de anillos unitarios** *entre A y B es una función $f : A \to B$ que verifica:*

1. *$f : (A, +_A) \to (B, +_B)$ es un morfismo de grupos.*

2. $f(a._A a') = f(a)._B f(a')$ *para todo* $a, a' \in A$.

3. $f(1_A) = 1_B$

Un morfismo se dirá **monomorfismo**, **epimorfismo** o **isomorfismo** si lo es como morfismo de la estructura de grupo abeliano subyacente.

Ejemplos:

1. Las inclusiones $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$ son todas morfismos de anillos.

2. Sea k un anillo con 1, G y H grupos y $f : G \to H$ un morfismo de grupos. Si se define el morfismo "$k[f]$", $k[f] : k[G] \to k[H]$ a partir de la fórmula:

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

   entonces $k[f]$ es un morfismo de anillos unitarios. Además vale que $k[id_G] = id_{k[G]}$ y si f y h son dos morfismos de grupos con dominios tales que se puede componer, entonces $k[f \circ h] = k[f] \circ k[h]$, es decir, la asignación $k[-] : Gr \to An_1$, $G \mapsto k[G]$ es funtorial.

3. La función $\pi : \mathbb{Z} \to \mathbb{Z}_n$ $(r \mapsto \overline{r})$ es un morfismo 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 $ev_{x_0} : A \to \mathbb{R}$ $(f \mapsto f(x_0))$ es un morfismo de anillos.

6. Sea A un anillo, $a \in A$, $ev_a : \mathbb{Z}[X] \to A$, $P = \sum_{i=0}^n \lambda_i.x^i \mapsto \sum_{i=0}^n \lambda_i.a^i$ es un morfismo de anillos.

Observaciones: La composición de dos morfismos de anillos es también un morfismo de anillos, y dado un anillo A, id_A es trivialmente un morfismo de anillos, luego la clase de objetos formada por los anillos junto con los morfismos de anillos forman una categoría (ver apéndice de categorías). Remarcamos entonces que una categoría conlleva sus propias definiciones de epimorfismo, monomorfismo e isomorfismo, que no tienen necesariamente que coincidir con las definiciones que dimos anteriormente, ya que para hacer esas definiciones sólo se tuvo en cuenta la estructura de grupo abeliano subyacente

y se "olvidó" la multiplicación. Sin embargo, las nociones de monomorfismo e isomorfismo definidas antes y las nociones categóricas coinciden en este caso. 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, que como morfismo de grupos abelianos es un isomorfismo. Luego existe $g : B \to A$ morfismo de grupos abelianos tal que $f \circ g = id_B$ y $g \circ f = id_A$, basta ver que g es morfismo de anillos. Sean $b, b' \in B$, entonces

$$f(g(b.b')) = id_B(b.b') = b.b' = id_B(b).id_B(b') = f(g(b)).f(g(b')) = f(g(b).g(b'))$$

como f es isomorfismo, en particular inyectiva, resulta $g(b.b') = g(b).g(b')$. Además como $f(1_A) = 1_B$, $1_A = id_A(1_A) = g(f(1_A)) = g(1_B)$.

Ejemplo: Sea la inclusión $i : \mathbb{Q} \to \mathbb{R}$, que es un morfismo de anillos. ¿Hay otros morfismos de anillos además de ese? La respuesta es no, porque si $f : \mathbb{Q} \to \mathbb{R}$ es un morfismo, al ser aditivo resulta $f\left(\frac{m}{n}\right) = m.f\left(\frac{1}{n}\right)$, como además $f(1) = 1$ y $1 = n.\frac{1}{n} \Rightarrow 1 = n.f\left(\frac{1}{n}\right)$, al estar en un cuerpo se puede dividir por n y se obtiene $f\left(\frac{1}{n}\right) = \frac{1}{n}$, es decir, f es la inclusión. Si en cambio buscamos morfismos en el otro sentido, $f : \mathbb{R} \to \mathbb{Q}$, para un $x \in \mathbb{R}$ no nulo se tiene $1 = f(1) = f(x.x^{-1}) = f(x).f(x^{-1})$, es decir, $f(x)$ no puede ser cero si x no lo era, por lo tanto 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 $\mathbb{Q}$.

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. ¿Cuando si y cuándo no? (Sugerencia: ver primero que dado cualquier anillo B, siempre existe un único morfismo de anillos $\mathbb{Z} \to B$.)

- La inclusión $i : \mathbb{Z} \to \mathbb{Q}$ es un epimorfismo categórico (en la categoría de anillos unitarios y morfismos de anillos unitarios).

A diferencia del caso de grupos, en el que dados dos grupos siempre había por lo menos un morfismo de grupos entre ellos (el morfismo nulo), en este caso la condición de "f(1)=1" (más la de multiplicatividad) restringe muchísimo las posibilidades de morfismos entre anillos, hasta tal 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 (verificar) que $\mathrm{Im}(f) \subseteq B$ además de ser un subgrupo de B, también es un subanillo, sin embargo, $\mathrm{Ker}(f)$ no es un subanillo, porque por ejemplo $1 \notin \mathrm{Ker}(f)$ ($f(1) = 1 \neq 0$), aunque sí sigue siendo un subgrupo. Para el caso de grupos, habíamos visto que no todo subgrupo es núcleo de un morfismo de grupos, sino que esto sólo sucede para los subgrupos invariantes. En un anillo, la estructura subyacente de grupo es conmutativa, por lo tanto todo subgrupo es invariante, sin embargo 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 tales que A/I hereda de A una estructura de anillo (de hecho al igual que en el caso de grupos, tal estructura es única) tal que la proyección al cociente $A \to A/I$ sea un morfismo de anillos:

Definición 2.3.1. *Sea A un anillo e I un subgrupo de $(A, +)$. I se llamará* **ideal bilátero** *si y sólo si para todo $x \in I$, $a \in A$ tanto $a.x$ como $x.a$ pertenecen a I.*

Nota: Si sólo se pide la condición "$a.x \in I \ \forall x \in I,\ a \in A$" el ideal se llamará **ideal a izquierda**, y si se pide sólo la condición "$x.a \in I \ \forall x \in I,\ a \in A$" el ideal se llamará **ideal a derecha**, estas distinciones se desvanecen si el anillo es conmutativo, pero en el caso general pueden no coincidir.

El ejemplo fundamental es el siguiente: sea $f : A \to B$ morfismo de anillos, entonces $\mathrm{Ker}(f)$ es un ideal bilátero. Es claro que es un subgrupo de A, y si $x \in I$ y $a \in A$ entonces

$$f(a.x) = f(a).f(x) = f(a),0 = 0 = 0.f(a) = f(x).f(a) = f(x.a)$$

es decir, $a.x$ y $x.a$ están también en el núcleo de f. Notar que aunque el anillo A no sea conmutativo, si $f : A \to B$, $\mathrm{Ker}(f)$ es siempre un ideal bilátero,

porque cero multiplicado por cualquier cosa da cero, sin importar que se lo multiplique a derecha o a izquierda.

Ejemplos:

1. Sea A un anillo conmutativo y $b \in A$, entonces el conjunto de los múltiplos de b, notado $\langle b \rangle = \{b.a \ / a \in A\}$ es un ideal bilátero. Subejemplos de éste son $m.\mathbb{Z}$, o en $k[X]$ los múltiplos de un polinomio fijo P.

2. Notar que todo subgrupo de $\mathbb{Z}$ es $m.\mathbb{Z}$ para algún m, y todos ellos son ideales. Si k es un cuerpo, entonces todos los ideales de $k[X]$ son como en el ejemplo anterior, es decir, los múltiplos de un polinomio fijo (ejercicio: demostrarlo, sugerencia: tomar la función "grado" e imitar la demostración de que en $\mathbb{Z}$ los únicos subgrupos son $m.\mathbb{Z}$). Si tomamos en cambio $k[X, Y]$ eso ya no es más cierto, tampoco es cierto para $\mathbb{Z}[X]$.

3. Si I es un ideal bilátero de A, $M_n(I) :=$ { matrices de $n \times n$ que en cada lugar tiene elementos de I}, es un ideal bilátero del anillo $M_n(A)$.

4. Sea X un abierto de $\mathbb{R}^n$ y $x_0 \in X$ y $A = C^\infty(X)$, entonces $I_{x_0} = \{f \in A$ tal que $f(x_0) = 0\}$ es un ideal de A (de hecho, es el núcleo de la evaluación en x_0).

5. Sea $A = C(\mathbb{R})$, entonces $I = \{f \in A \ / \ sop(f)$ es acotado $\}$ es un ideal de A ($sop(f) = \overline{\{x \ / \ f(x) \neq 0\}}$).

Observaciones: 1) Si I es un ideal y $1 \in I$ entonces $I = A$, lo mismo si $a \in I$ y a es una unidad. Un anillo A siempre tiene por lo menos dos ideales biláteros, $\{0\}$ (corresponde a $\mathrm{Ker}(id_A : A \to A)$) y todo 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), en ese caso A se dirá un anillo **simple**. Todo anillo conmutativo simple es un cuerpo (ejercicio), pero en el caso no conmutativo hay anillos simples que no son de división, por ejemplo $M_n(k)$ con k cuerpo o anillo de división.

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. Un hecho notable con las matrices es que si $I \subset A$ es un ideal bilátero de A entonces $M_n(I)$ es un ideal bilátero de $M_n(A)$, y además esos son todos los ideales

biláteros de $M_n(A)$, sin embargo A y $M_n(A)$ $(n > 1)$ nunca son isomorfos como anillos. De cualquier manera, los anillos A y $M_n(A)$ comparten muchas otras propiedades; este hecho será tratado en el Capítulo de Teoremas de Morita.

3) Si I y J son ideales de A, sea $I.J = \{\sum_{i=1}^{n} x_i.y_i / x_i \in I, y_i \in J\}$. Entonces $I.J$ es un ideal (bilátero?) e $I.J$ está contenido en I y en J.

4) Si I y J son ideales de A, sea $I + J = \{x + y / x \in I, y \in J\}$. Entonces $I + J$ es un ideal.

5) La intersección de ideales es un ideal.

6) Si I, J_1,...,J_n son ideales de A, entonces $I.(J_1+...+J_n) = I.J_1+...+I.J_n$.

7) Dado un elemento $a \in A$, se obtiene un ideal (por ejemplo a izquierda) de A de la siguiente forma:

Sea $(a) = \{x.a / x \in A\}$. Este es el menor ideal a izquierda de A que contiene a a, se llama el **ideal principal** generado por a.

8) Sea A un anillo íntegro. Dados $a, b \in A$ (ambos no nulos), entonces $(a) = (b) \Leftrightarrow \exists u \in \mathcal{U}(A)$ tal que $a = ub$.

9) Si $a_1, ..., a_n \in A$, el **ideal generado por** $a_1, ..., a_n$ (denotado $(a_1, ..., a_n)$) es la intersección de los ideales de A que contienen a todos los a_i. Por ejemplo, en $\mathbb{Z}$, $(2, 3) = \mathbb{Z}$, $(2, 4) = 2.\mathbb{Z}$, en $\mathbb{Q}[x]$, $(x - 2, x - 3) = \mathbb{Q}[x]$.

Definición 2.3.2. *Sea I un ideal bilátero, diremos que I es un ideal* **bilátero maximal** *si $I \neq A$ y, dado J ideal bilátero de A, entonces $I \subseteq J$ implica $J = I$ o $J = A$.*

2.4. Cocientes

Vimos que todo núcleo de un morfismo de anillos es un ideal bilátero. Como en el caso de grupos, veremos que dado un ideal bilátero cualquiera I de un anillo A, siempre existe un anillo B y un morfismo $f : A \to B$ tal que $I = \mathrm{Ker}(f)$. La construcción es similar al caso de grupos, se trata de definir una relación de equivalencia entre los elementos de A de manera de que el conjunto cociente admita una estructura de anillo.

Dado I, decimos entonces que dos elementos a y a' de A están relacionados $\Leftrightarrow a - a' \in I$. Sea A/I el conjunto de clases de equivalencia, $A/I = \{\overline{a} \ / \ a \in A\}$.

Sabemos que, como I es un subgrupo (normal) de $(A,+)$, A/I es un grupo abeliano y que $\pi : A \to A/I$ es un morfismo de grupos. La estructura de grupo sobre A/I está definida por $\overline{a}+\overline{a'} = \overline{a+a'}$. Definimos un producto en A/I por la fórmula:

$$\overline{a}.\overline{a'} := \overline{a.a'}$$

Hay que ver que:

- La multiplicación está bien definida en el cociente, i.e. si $\overline{a} = \overline{b}$ y $\overline{a'} = \overline{b'}$ hay que verificar que $\overline{a.a'} = \overline{b.b'}$.
- $(A/I,+,.)$ es un anillo (con 1, 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 $(A/I,+,.)$ 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 como la única posible para la cual π es multiplicativa, y 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 para y. Cuando hacemos la cuenta $a.a'$ y calculamos a partir de b y b' tenemos:

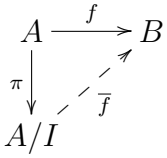
$$a.a' = (b+x).(b'+y) = b.b' + (b.y + x.b' + x.y)$$

Al ser I un ideal bilátero tanto $b.y$ como $x.b'$ y $x.y$ pertenecen a I, por lo tanto $\overline{a.a'} = \overline{b.b'} + \overline{b.y + x.b' + x.y} = \overline{b.b'} + \overline{0} = \overline{b.b'}$. Aquí fue 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. *(Propiedad universal) Dado un anillo A y un ideal bilátero I, el par $(A, \pi : A \to A/I)$ tiene las siguientes dos propiedades:*

- $\pi : A \to A/I$ *es un morfismo de anillos con* $I \subseteq \mathrm{Ker}(\pi)$.
- *Si* B *es un anillo cualquiera 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 $f : A \to B$ un morfismo de anillos con la propiedad $I \subseteq \mathrm{Ker}(f)$. Como $\pi : A \to A/I$ sigue siendo un morfismo de grupos con su propiedad universal, y f es en particular un morfismo de grupos, se tiene asegurada la existencia y unicidad de la función $\overline{f}$, y además también sabemos que es un morfismo de grupos, asi que sólo falta ver que es multiplicativa. Recordamos que $\overline{f}$ está definida por

$$\overline{f}(\overline{a}) = f(a) \ \forall a \in A$$

A partir de esa fórmula y de la multiplicación en el cociente es claro que $\overline{f}$ es multiplicativa cuando f lo es pues

$$\begin{aligned} \overline{f}(\overline{a}.\overline{a'}) &= \overline{f}(\overline{a.a'}) \\ &= f(a.a') = f(a).f(a') \\ &= \overline{f}(\overline{a}).\overline{f}(\overline{a'}) \end{aligned}$$

Como siempre dos objetos que verifican una misma propiedad universal resultarán isomorfos (verificar! sugerencia: calcar la demostración de grupos).

Corolario 2.4.2. *Sea* $f : A \to B$ *un morfismo de anillos, entonces se tiene el isomorfismo de anillos*

$$A/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$$

Demostración: basta notar que $\mathrm{Im}(f)$ es un subanillo de B y que $f : A \to \mathrm{Im}(f)$ también es un morfismo de anillos. Ya sabemos que $\overline{f} : A/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ da un isomorfismo de grupos abelianos, pero como $\mathrm{Ker}(f)$ es un ideal bilátero, la propiedad del cociente asegura que $\overline{f}$ también respeta el 1 y la estructura multiplicativa.

Ejemplos:

1. Si $n \in \mathbb{N}$, $\mathbb{Z}_n \cong \mathbb{Z}/n.\mathbb{Z}$ (isomorfismo de anillos).

2. Si k es un anillo y $a \in k$, $ev_a : k[X] \to k$ es un epimorfismo de anillos con núcleo $\langle X - a\rangle$ (verificar!), luego $k[X]/\langle X - a\rangle \cong k$.

3. Consideremos $\mathbb{R}[X]$, $i \in \mathbb{C}$, y la evaluación $ev_i : \mathbb{R}[X] \to \mathbb{C}$ definida 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, verificar que en realidad $\mathrm{Ker}(ev_i) = \langle X^2 + 1\rangle$, y por lo tanto $\mathbb{R}[X]/\langle X^2 + 1\rangle \cong \mathbb{C}$.

4. Si X es un abierto de $\mathbb{R}^n$ y $x_0 \in X$ entonces $C(X)/\{f \in C(X) \,/\, f(x_0) = 0\} \cong \mathbb{R}$.

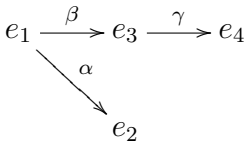
5. Si $I \subseteq A$ es un ideal bilátero entonces $M_n(A)/M_n(I) \cong M_n(A/I)$.

6. Sea A un anillo y $e \in A$ un elemento tal que $e^2 = e$ (notar que si $e^2 = e$ entonces $(1-e)^2 = (1-e)$). Este elemento permite construir otro anillo asociado a A que es el conjunto $e.A.e = \{e.x.e \,/\, x \in A\}$. Este es un anillo con $1_{e.A.e} = e$ utilizando la multiplicación de A restringida a $e.A.e$. Notar que nunca es subanillo a menos que $e = 1$ y por lo tanto $e.A.e = A$, y que el uno no es cero en $e.A.e$ siempre que $e \neq 0$. Ver que si e conmuta con los elementos de A entonces $\tau_e : A \to e.A.e = e.A$ definida por $\tau_e(x) = e.x.e = e.x$ es un morfismo de anillos suryectivo con núcleo $\mathrm{Ker}(\tau_e) = (1 - e).A$, es decir $e.A \cong A/(1 - e).A$.

   - Sea $A = M_n(k)$ y $e = (e_{ij})_{ij}$ definido por $e_{ij} = \begin{cases} 1 & \text{si } i = j = 1 \\ 0 & \text{otro caso} \end{cases}$
     Verificar que $e^2 = e$ y que $e.A.e \cong k$ Sin embargo $\tau_e : M_n(k) \to e.M_n(k).e \cong k$ no es multiplicativo, ¿por qué?

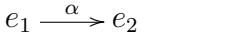
7. Si $H \triangleleft G$ y k es un anillo, entonces $k[\pi] : k[G] \to k[G/H]$ induce un isomorfismo $k[G]/\langle (1-h) \ : \ h \in H\rangle \cong k[G/H]$.

8. Sea k un cuerpo y Q un grafo orientado, es decir, se tienen dados dos conjuntos Q_0 y Q_1, los elementos de Q_0 se llaman vértices, los elementos de Q_1 se llaman flechas, y el dato que determina el grafo orientado (o Quiver, o Carcaj) son 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 siguiente:



   Los conjuntos son $Q_0 = \{e_1, e_2, e_3\}$, $Q_1 = \{\alpha, \beta, \gamma\}$, las funciones s y t están definidas por $s(\alpha) = e_1$, $t(\alpha) = e_3$, $s(\beta) = e_1$, $t(\beta) = e_2$, $s(\gamma) = e_3$, $t(\gamma) = e_4$. Se define el anillo kQ como el k-espacio vectorial con base los caminos del grafo (los vértices se consideran como caminos de largo cero), donde 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 se tiene $kQ = k.e_1 \oplus k.e_2 \oplus k.e_3 \oplus k.e_4 \oplus k.\alpha \oplus k.\beta \oplus k.\gamma \oplus k.\beta\alpha$. Los productos están determinados por $e_i^2 = e_i$ $(i = 1, \ldots, 4)$, $\beta.\alpha = \beta\alpha$, el producto $e_i\alpha$ de un vértice e_i con la flecha α coincide con α en caso de que e_i sea igual a $t(\alpha)$, idem multiplicando a derecha por el vértice en donde empiece α, los otros dan cero, de manera similar las otras flechas con los otros vértices. Y los productos de dos flechas dan cero salvo $\beta.\alpha$.

9. Sea el grafo Q el grafo



   entonces $kQ = ke_1 \oplus ke_2 \oplus k\alpha$, resulta un anillo isomorfo al subanillo de matrices triangulares de dos por dos via el morfismo $e_1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $e_2 \mapsto \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, $\alpha \mapsto \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

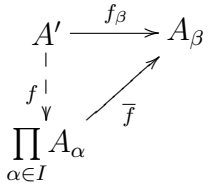
2.5. Producto de anillos

Sean $(A_\alpha, +_\alpha, \cdot_\alpha)$ $(\alpha \in I)$ una colección de anillos indexados por los elementos de un conjunto no vacío I. Para dar una estructura de anillo al producto cartesiano de los A_α, consideramos la suma y el producto definidos coordenada a coordenada. Es fácil ver que con estas operaciones obtenemos un anillo denotado $(\prod_{\alpha\in I} A_\alpha, +, .)$.

Este anillo tiene las siguientes propiedades:

1. 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).

2. Si A' es un anillo provisto de morfismos de anillos $f_\beta : A' \to A_\beta (\forall \beta \in I)$, entonces existe un único morfismo $f : A' \to A$ tal que $\Pi_\beta \circ f = f_\beta$. O sea, el siguiente diagrama conmutativo se completa de manera única por la flecha punteada:



   Es decir 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 esta es otra construcción de tipo "universal" (como por ejemplo el cociente), y que cualquier otro anillo que verificara (1) y (2) sería necesariamente isomorfo al producto $\prod_{\alpha\in I} A_\alpha$.

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 (recordar 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, tomar k^G.

2.6. Localización

En esta sección analizaremos la construcción de $\mathbb{Q}$ a partir de $\mathbb{Z}$ "agregando" inversos multiplicativos a $\mathbb{Z}$, veremos generalizaciones de esta construcción y la interpretación geométrica que se le puede dar en ciertos ejemplos, lo que motiva el nombre de dicha construcción.

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 que se escribe

$$a.x = b$$

no siempre se puede resolver, porque no es válido "pasar a dividiendo". Si uno mira esa ecuación en $\mathbb{Q}$ no tiene ningún problema, la resuelve, y el resultado da en $\mathbb{Q}$. Lo que se realizó al pasar de $\mathbb{Z}$ a $\mathbb{Q}$ es invertir todos los elementos de $\mathbb{Z}$ (salvo el 0). 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:*

- *Si $n \in \mathbb{Z}$ es un elemento no nulo, entonces $i(n) = \frac{n}{1}$ es una unidad de $\mathbb{Q}$.*
- *Si $f : \mathbb{Z} \to B$ es un morfismo de anillos tal que $f(n)$ es una unidad de B $\forall n \neq 0$, 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 a partir de la condición $f\left(\frac{1}{1}\right) = 1_B$. Para ver la existencia, basta definir

$$\overline{f}\left(\frac{m}{n}\right) := f(m).f(n)^{-1}$$

que tiene sentido porque la hipótesis es que $f(n)$ es inversible para todo $n \neq 0$. Queda como ejercicio verificar que este morfismo $\overline{f}$ cumple las condiciones pedidas (por ejemplo $\overline{f}\left(\frac{m}{1}\right) = f(m).f(1)^{-1} = f(m)$,$1 = f(m)$).

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 se dirá un subconjunto* **multiplicativamente cerrado** *si:*

- *Para todo par $s, t \in S$, $s.t \in S$.*
- $1 \in S$.

La primera propiedad es la que le da el nombre de multiplicativamente cerrado, si S verifica la primer propiedad pero $1 \notin S$, entonces $S' = S \cup \{1\}$ verifica las dos.

Se trata 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, $A = \mathbb{Z}$, $S = \mathbb{Z} - \{0\}$, $A_S = \mathbb{Q}$) y tal que exista un morfismo de anillos $A \to A_S$ que factorice todo morfismo de anillos que salga de A en el que las imágenes de los $s \in S$ sean inversibles.

Definimos entonces A_S:

Como conjunto, $A_S = \{(a, s) \in A \times A / a \in A, s \in S\}/\sim$, donde (a, s) es equivalente a $(a', s') \Leftrightarrow \exists t \in S$ tal que $(as' - a's)t = 0$ (verificar que es una relación de equivalencia, ¿Qué propiedades de S se usan para eso?).

Usaremos la siguiente notación $(a, s) = a/s$.

Definiendo en A_S las siguientes suma y producto, se tendrá una estructura de anillo:

- $a/s + a'/s' = (as' + a's)/ss'$
- $(a/s).(a'/s') = (aa'/ss')$

Ejercicio: verificar que las operaciones están bien definidas y que $(A_S, +, .)$ resulta un anillo con elemento neutro $1/1$.

Se tiene entonces un morfismo de anillos $i : A \to A_S$ $(a \mapsto a/1)$ tal que la imagen por i de un elemento $s \in S$ es inversible, de inverso $1/s$. Además, si B es otro anillo y $f : A \to B$ un morfismo tal que $f(s) \in \mathcal{U}(B), \forall s \in S$,

entonces existe una única $\overline{f} : A_S \to B$ tal que $\overline{f} \circ i = f$ ($\overline{f}$ está definida 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 se verifica si se permite $t = 0$.

3. Sea $A = \mathbb{Z}$, $S = \{1, 2, 2^2, ...\} = \{2^i \ / \ i \in \mathbb{N}_0\}$. Entonces $A_S = \{m/2^i \ : \ m \in \mathbb{Z}, \ i \in \mathbb{Z}\} = \mathbb{Z}[\frac{1}{2}]$.

4. Sea X un espacio topológico (por ejemplo $\mathbb{R}$ con la topología usual), $A = C(X)$ y sean $x_0 \in X$, $S = \{f \in A : \ f(x_0) \neq 0\}$. Entonces $A_S = \{f/g : f, g : X \to \mathbb{R}, g(x_0) \neq 0\}/\sim$. (la notación f/g se usa en este caso de forma coherente con la notación dada para localizaciones y no para indicar cociente de funciones definidas sobre X). En A_S, $f_1/g_1 \sim f_2/g_2 \Leftrightarrow \exists h \in S$ tal que $h(f_1g_2 - f_2g_1) = 0$.

   Pero $h \in S$ quiere decir que $h(x_0) \neq 0$. Como h es continua, debe existir un entorno U de x_0 en X tal que $h|U \neq 0$. Entonces, si $x \in U$, $h(x)$ es inversible en $\mathbb{R}$, pero:

   $$h(x)(f_1(x)g_2(x) - f_2(x)g_1(x)) = 0 \text{ entonces } (f_1(x)/g_1(x) = f_2(x)/g_2(x))$$

   (Observar que existen entornos U_1 y U_2 de x_0 tales que si $x \in U_1 \cap U_2$ entonces $g_1(x) \neq 0 \neq g_2(x)$, luego se toma $U' = U_1 \cap U_2 \cap U$ entorno de x_0).

   Por lo tanto, dos funciones coinciden como elementos de A_S si y solo si 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

1. Sea $(A, +, .)$ un anillo. Ver que el producto en $M_n(A)$ dado por

$$(m.n)_{ij} = \sum_{k=1}^{n} m_{ik} n_{kj}$$

(m y n son dos matrices con coeficientes en A, $(m)_{ij} = m_{ij}$, idem n) es un producto asociativo, poniendo además la suma coordenada a coordenada, $M_n(A)$ es un anillo. Ver que si $n > 1$, $M_n(A)$ nunca es conmutativo, sin importar si A lo es o no.

2. Sea A un anillo conmutativo. Convencerse de que $\det : M_n(A) \to A$ es una función multiplicativa, es decir, que la misma demostración que se usó en algebra lineal para ver que $\det(M.N) = \det(M).\det(N)$ vale. Ver que $M \in M_n(A)$ es inversible si y sólo si $\det(M)$ es una unidad. Encuentre todos los elementos de $\mathcal{U}(M_2(\mathbb{Z}_4))$.

3. 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 $e.e' = 0 = e'.e$.

   b) Sea B el anillo $e.A$ 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

$$\begin{aligned} A &\to B \times C \\ a &\mapsto (e.a, e'.a) \end{aligned}$$

   define un isomorfismo de anillos, en donde $B \times C$ tiene la suma y producto coordenada a coordenada $(b, c)(b', c') = (bb', cc')$.

   c) Ver que B tiene dimensión (sobre $\mathbb{R}$) 1 y C tiene dimensión 2, una base de B es por ejemplo $\{e\}$, y una base de C es $\{e', f\}$ donde $f = t - t^2 = e'.(t - t^2)$. Ver que valen los siguientes isomorfismos de anillos:

   1) $B \cong \mathbb{R}$ $(e.(x, 1 + y.t + z.t^2) \mapsto x + y + z)$
   2) $f^2 = -3.e'$, luego $C \cong \mathbb{C}$ vía $(a.e' + b.j) \mapsto a + b.i$, donde $j = \frac{f}{\sqrt{3}}$.

4. Sea $A = \mathbb{C}[G_3]$, $\omega \in \mathbb{C}$ una raíz cúbica primitiva de la unidad, $e_1 = \frac{1}{3}(1 + t + t^2)$, $e_2 = \frac{1}{3}(1 + \omega.t + \omega^2.t^2)$, $e_3 = \frac{1}{3}(1 + \omega^2.t + \omega.t^2)$. Probar que:

   a) $e_i.e_j = 0$ si $i \neq j$, $e_i^2 = e_i$ $(i, j = 1, 2, 3)$ y $e_1 + e_2 + e_3 = 1$.

   b) Los anillos $e_i.A$ tienen dimensión (sobre $\mathbb{C}$) igual a uno y son isomorfos a $\mathbb{C}$ (isomorfismo de anillos).

   c) 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 tomando en $e_1\mathbb{C} \times e_2\mathbb{C} \times e_3\mathbb{C}$ la suma y el producto coordenada a coordenada (es decir, con la estructura producto).

5. Sea A un anillo y $A[[x]]$ (llamado series formales con coeficientes en A e indeterminada x) el siguiente conjunto:

   $$A[[x]] = A^{\mathbb{N}_0} = \{ \text{ funciones de } \mathbb{N}_0 \text{ en } A\}$$

   donde se adopta por notación $\sum a_n x^n$ = la función que a cada $n \in \mathbb{N}_0$ le asigna $a_n \in A$. Se define en $A[[x]]$ la operación:

   $$(\sum a_n x^n).(\sum b_n x^n) := \sum (\sum_{k=0}^{n} a_k.b_{n-k})x^n$$

   Ver que está bien definida y si definimos la suma como

   $$(\sum a_n x^n) + (\sum b_n x^n) := \sum (a_n + b_n)x^n$$

   entonces $A[[x]]$ resulta un anillo. ¿Quién es $1_{A[[x]]}$? Sea $s \in A[[x]]$, entonces $1 + x.s$ es inversible en $A[[x]]$.

6. Sea A un anillo, probar:

   a) Si $a \in A - \mathcal{U}(A)$ entonces existe un ideal a izquierda maximal que contiene a a.

   b) Si $a \in A$ es un elemento nilpotente, es decir, existe $n \in \mathbb{N}$ tal que $a^n = 0$, entonces $1 - a$ es una unidad.

   c) $1 - a.b$ es unidad si y sólo si $1 - b.a$ es unidad. (sug.: demuéstrelo primero suponiendo que $a.b$ es nilpotente para así hallar una relación entre $(1-a.b)^{-1}$ y $(1 - b.a)^{-1}$, ver despues que esa relación vale en general).

7. Hallar todas las unidades de $\mathbb{Z}[x]/\langle x^3 \rangle$.

8. Sea $P \subset A$ un ideal bilátero de un anillo A. Diremos que P es un ideal **primo** si cada vez que $a.b \in P$ entonces $a \in P$ o $b \in P$. Demuestre:

   - Si $A = \mathbb{Z}$ e $I = n.\mathbb{Z}$ entonces I es un ideal primo si y sólo si n es un número primo.
   - Todo ideal maximal es primo.
   - I es un ideal primo si y sólo si A/I es íntegro.
   - I es un ideal maximal si y sólo si A/I es simple.

9. Si I es un ideal bilátero de A entonces $M_n(I)$ es ideal bilátero de $M_n(A)$ y $M_n(A)/M_n(I) \cong M_n(A/I)$.

10. Sea $A = k[x]$, $f \in A$ e $I = \langle f \rangle$. Ver que $A/\langle f \rangle$ es un cuerpo si y sólo si f es irreducible.

11. Sea k un cuerpo y sea $k[i]$ un k-espacio vectorial de dimensión 2, con base $\{1, i\}$, o sea, todo elemento de $k[i]$ es de la forma $a{,}1 + b.i$ con $a, b \in k$, que también notaremos $a + b.i$. Definimos el producto

$$(a + b.i).(c + d.i) := ac - bd + (ad + bc).i$$

Ver que $k[i]$ es un anillo. Si $k = \mathbb{Z}_2$ ó $\mathbb{Z}_5$, entonces $k[i]$ no es un cuerpo, si $k = \mathbb{Z}_3$ sí es un cuerpo, también si $k = \mathbb{Z}_7$.

12. Un anillo A se llama **anillo de Boole** si todos sus elementos son idempotentes (i.e. $x^2 = x$ para todo $x \in A$). Probar:

   a) Todo anillo de Boole es conmutativo y $\forall a \in A, a = -a$.

   b) Todo subanillo y todo cociente de un anillo de Boole es anillo de Boole.

   c) Si X es un conjunto, entonces $\mathcal{P}(X)$ (las partes de X con la operación $+ =$ diferencia simétrica, y producto $=$ intersección), es un anillo de Boole.

   d) Todo anillo de Boole es un $\mathbb{Z}_2$-espacio vectorial.

   e) Sea X un conjunto, entonces $\mathbb{Z}_2^X = Func(X, \mathbb{Z}_2)$ es un anillo de Boole.

13. Sea $f : \mathbb{R} \to \mathbb{R}$ un morfismo de anillos. Ver:

   a) $f(\mathbb{Q}) \subset \mathbb{Q}$ y $f|_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{Q}$ es la identidad.

   b) $f : \mathbb{R} \to \mathbb{R}$ es necesariamente creciente.

   c) $f = id_{\mathbb{R}}$.

14. Sea k un cuerpo. Basándose en la demostración de que $\mathbb{Z}$ es un dominio principal y usando la función grado $gr : (k[x] - \{0\}) \to \mathbb{N}_0$ ver que $k[x]$ es también un dominio principal.

15. *Enteros de Gauβ.* Sea $\mathbb{Z}[i]$ la subalgebra de $\mathbb{C}$ generada por i, es decir, los elementos de $\mathbb{C}$ de la forma $a + b.i$ con a y b en $\mathbb{Z}$. Sea $N : \mathbb{Z}[i] \to \mathbb{N}_0$ la función (llamada norma) definida por

$$N(a + b.i) = |a + b.i|^2 = a^2 + b^2$$

   a) Ver que $N(x.y) = N(x).N(y)$ $\forall x, y \in \mathbb{Z}[i]$.

   b) Ver que si $x, y \in \mathbb{Z}[i]$ entonces existen (no necesariamente únicos) $q, r \in \mathbb{Z}[i]$ tales que $x = q.y + r$ donde $N(r) < N(y)$. (sugerencia: hacer primero la cuenta en $\mathbb{Q}[i]$ y después volver (como pueda) a $\mathbb{Z}[i]$).

   c) Deducir que $\mathbb{Z}[i]$ es un dominio principal, por lo tanto de factorización única.

   d) Ver que $\mathbb{Z}[i]/\langle 5\rangle \cong \mathbb{Z}_5[i]$ que no es un cuerpo, por lo tanto $\langle 5\rangle$ no es un ideal maximal, luego 5 se puede factorizar, factorícelo.

16. Sea A íntegro, entonces $j : A \to A_S$ $(a \mapsto \frac{a}{1})$ es inyectiva para cualquier S subconjunto multiplicativamente cerrado (de aqui en adelante se entiende que $0 \notin S$). En general, $j : A \to A_S$ es inyectiva si y solo si S no tiene divisores de cero. Dar un ejemplo en que j no sea inyectiva.

17. Sea $\mathcal{P} \subset A$ un ideal primo, entonces $S_{\mathcal{P}} := A \setminus \mathcal{P}$ es un subconjunto multiplicativamente cerrado. Idem con $\mathcal{M} \subset A$ un ideal maximal y $S_{\mathcal{M}} = A \setminus \mathcal{M}$. NOTACION: para estos casos, se escribirá $A_{\mathcal{P}} := A_{A \setminus \mathcal{P}}$, idem $A_{\mathcal{M}}$.

18. Sea $A = C(\mathbb{R})$ el anillo de funciones continuas sobre $\mathbb{R}$ y $x_0 \in \mathbb{R}$. Sea $\mathcal{M} = \{f \in A \ / \ f(x_0) = 0\}$. Ver que es un ideal maximal, y que $\frac{f}{1} = \frac{g}{1}$ en $A_{\mathcal{M}}$ si y sólo si existe un entorno de x_0 en donde f y g coinciden.

19. Sea la aplicación $A \to \prod_{\mathcal{M} \text{ max.}} A_{\mathcal{M}}$ dada por $a \mapsto \{\frac{a}{1}\}_{\mathcal{M} \text{ max.}}$ en donde cada $\frac{a}{1}$ pertenece al $A_{\mathcal{M}}$ correspondiente. Ver que esa aplicación es inyectiva. (sugerencia: si a es una unidad, ver que $\frac{a}{1}$ es distinto de cero en cualquier localización; si a no es una unidad, entonces existe un maximal $\mathcal{M}$ que contiene a a, ver que $\frac{a}{1} \neq 0$ en el localizado por ese maximal).

20. Sea $A = C(\mathbb{R})$, $U = (0,1)$, $S_U = \{f \in A \ / \ f(t) \neq 0 \ \forall t \in (0,1)\}$. Probar

    a) S_U es un subconjunto multiplicativamente cerrado.

    b) Sea $res : C(\mathbb{R}) \to C(0,1)$ el morfismo $f \mapsto f|_{(0,1)}$. Ver que es un morfismo de anillos, y que S_U se mapea en unidades, luego ese morfismo se factoriza por A_{S_U}

    $$\begin{array}{ccc} C(\mathbb{R}) & \xrightarrow{res} & C(0,1) \\ \downarrow{\scriptstyle j} & \nearrow & \\ A_{S_U} & & \end{array}$$

    Ver que la flecha punteada es inyectiva.

    c) (opcional) Suryectividad de la flecha punteada: si $f \in A$, $f = f_+ - f_-$ con f_+ y f_- mayores o iguales que cero, asi que para ver que toda funcion continua sobre $(0,1)$ es el cociente de una continua sobre $\mathbb{R}$ dividida por otra continua que no se anula sobre $(0,1)$ basta demostrarlo para las funciones positivas. Ahora dada $f \in C(0,1)$, $f \geq 0$, se define $f_1(x) := max\{1, f(x)\}$ y $g := f - f_1$. Ver que tanto f_1 como g pertenecen a $C(0,1)$, además f_1 se puede extender a una función continua globalmente definida.
    Sea $s : \mathbb{R} \to \mathbb{R}$ definida por

    $$s(x) = \begin{cases} 0 & \text{si } x \notin (0,1) \\ x & \text{si } 0 \leq x \leq 1/2 \\ 1 - x & \text{si } 1/2 \leq x \leq 1 \end{cases}$$

    Ver que s es continua y que $s \in S_U$. Además $s.g$ es una función que puede ser definida de manera continua sobre todo $\mathbb{R}$, y la función f original en $C(0,1)$ proviene del elemento $\frac{f_1}{1} + \frac{(s.g)}{s}$.

3

Módulos

3.1. Módulos: 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 $\mathrm{End}(M) = \{f : M \to M \ / \ f(x+y) = f(x) + f(y) \ \forall \ x, y \in M\}$ es un anillo con el producto dado por composición de funciones.

Definición 3.1.1. *Un* A**-módulo** *a izquierda es un grupo abeliano* $(M,+)$ *provisto de un morfismo de anillos*

$$\begin{aligned} \rho : A &\to \mathrm{End}(M) \\ a &\mapsto \rho_a \end{aligned}$$

Es decir, dar una estructura de A-módulo a un grupo abeliano M es asignar a cada elemento $a \in A$ una transformación del grupo M. La condición de que esta asignación sea un morfismo de anillos dice que

1. $\rho_1 = Id_M$.
2. $\rho_{a.b} = \rho_a \circ \rho_b$.
3. $\rho_{a+b} = \rho_a + \rho_b$ (i.e. $\rho_{a+b}(m) = \rho_a(m) + \rho_b(m)$ para todo $m \in M$).

Ejemplos:

1. $M = A$ y $\rho_a(b) = ab$.
2. Si $A = k$ es un cuerpo y V un k-espacio vectorial, $\rho_\lambda(v) = \lambda.v$.
3. Dado M un grupo abeliano, $\mathrm{End}(M)$ es un anillo y por lo tanto existe un único morfismo de anillos $\mathbb{Z} \to \mathrm{End}(M)$. Luego todo grupo abeliano es, de manera única, un $\mathbb{Z}$-módulo. Explícitamente, el morfismo de estructura esta dado, por ejemplo para los $n > 0$, por $\rho_n(m) = m + m + ... + m$ n-veces.
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 $\rho_g(m) = g.m$ ($g \in G$ y $m \in M$) y extendiendo ρ linealmente. El módulo M también se denomina una representación de G.
5. Si V es un k-espacio vectorial y G es un subgrupo de $GL(V)$, 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 un par (a, m) a un elemento "$a.m$", donde $a.m$ es una notación para designar a $\rho_a(m)$. El hecho de que ρ sea un morfismo de anillos entre A y $\mathrm{End}(M)$ se escribe en esta notación como: ($a, b \in A$, $x, y \in M$)

1. $1.x = x$.
2. $(ab).m = a.(b.m)$.
3. $(a + b).m = a.m + b.m$.
4. y teniendo en cuenta que $\rho_a \in \mathrm{End}(M)$, $a.(x + y) = a.x + a.y$.

Se puede a tomar estas últimas 4 propiedades de una función $A \times M \to M$ como definición estructura de A-módulo a izquierda, la equivalencia entre las dos definiciones es inmediata.

Ejemplos:

1. El grupo abeliano $\{0\}$ es un A-módulo para cualquier anillo A.

2. Si M es un grupo abeliano y $A = \mathrm{End}(M)$ entonces M es un A-módulo con la acción $\mathrm{End}(M) \times M \to M$ dada por $(f, m) \mapsto f(m)$. Verificar que esta acción corresponde al morfismo de anillos $id : A \to \mathrm{End}(M)$.

3. Si I es un conjunto y M un A-módulo, se define, en el grupo abeliano $M^I = \{$ funciones $f : I \to M\}$, una estructura de A-módulo por $a.\{m_i\}_{i\in I} := \{a.m_i\}_{i\in I}$ (donde como siempre $\{m_i\}_{i\in I}$ es la notación para la función $i \mapsto m_i$).

4. $M_n(A)$ es un A-módulo con $(a.m)_{ij} = a.m_{ij}$.

5. Si V es un k-espacio vectorial de dimensión n, entonces es un $M_n(k)$-módulo (¿por qué?).

Observaciones: En un A-módulo M (ejercicio) se verifican:

1. $a,0 = 0 \ \forall\ a \in A$.

2. $0.m = 0 \ \forall\ m \in M$.

3. $(-a).m = -(a.m)$.

De manera similar se puede definir un A-módulo a derecha a partir de una función $M \times A \to M$ que verifique propiedades análogas a 1.- 4.
Ejercicio: escribir la definición de A-módulo a derecha, ver que equivale a tener una función $A \to \mathrm{End}(M)$ con ciertas propiedades, escriba esas propiedades.

Si A es un anillo conmutativo y M es un A-módulo a izquierda, entonces se puede definir sobre M una estructura de A-módulo a derecha mediante $m.a := a.m$. Las propiedades 1.- 4. se verifican porque A es conmutativo. ¿qué propiedades dejan de valer cuando A no es conmutativo?

Ejemplo: Sea $A = M_n(\mathbb{C})$ y M un $M_n(\mathbb{C})$-módulo a izquierda (por ejemplo un $\mathbb{C}$-espacio vectorial de dimensión n). Se puede dotar a M de una estructura de A-módulo a derecha definiendo $M \times M_n(\mathbb{C}) \to M$ a través de $(m, (a_{ij})) \mapsto (\overline{a}_{ij})^t.m$. Verificar que esto efectivamente da una estructura de A-módulo a derecha. ¿Qué propiedades de la función $(\_)^t$ se usaron?

Definición 3.1.2. *Sean A y B dos anillos, M un A-módulo a izquierda y B-módulo a derecha. Diremos que M es un A-B-bimódulo si para todo $a \in A,\ b \in B$ y $m \in M$ se verifica*

$$(a.m).b = a.(m.b)$$

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 $M = \mathbb{Z}_2 \oplus \mathbb{Z}_2$, que es naturalmente un $M_2(\mathbb{Z}_2)$-módulo a derecha con la acción dada por la multiplicación de matrices. Sea $(-)^t : M_2(\mathbb{Z}_2) \to M_2(\mathbb{Z}_2)$ la aplicación tomar traspuesta, verificar que como $(-)^t$ 'da vuelta' los productos, entonces $(a_{ij}).x := x.(a_{ij})^t$ ($x \in \mathbb{Z}_2 \oplus \mathbb{Z}_2$ y $(a_{ij}) \in M_2(\mathbb{Z}_2)$) define una estructura de $M_2(\mathbb{Z}_2)$-módulo a izquierda. Ejercicio con estas dos acciones a derecha y a izquierda verificar que $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ *no* es un bimódulo.

Ejercicio: Sea M un A-módulo a derecha y $B = \mathrm{End}_A(M)$. Ver que la acción $\mathrm{End}_A(M) \times M \to M$, $(f, m) \mapsto f(m)$ define sobre M estructura de $\mathrm{End}_A(M)$-módulo a izquierda, además M resulta un $\mathrm{End}_A(M) - A$-bimódulo (i.e. las dos estructuras son compatibles. Si $M = A^{n\times 1}$ (o sea A^n visto como 'vector columna') es un A-módulo a derecha, ver que M además es un $M_n(A)$-módulo a izquierda con la multiplicación usual de matrices. Ver que esta estructura coincide con la definida antes, identificando $\mathrm{End}_A(A^n) \cong M_n(A)$.

Nota: En adelante, A-módulo querrá decir A-módulo a izquierda.

Definición 3.1.3. *Dado un anillo A, un subconjunto N de un A-módulo M se dirá un* **submódulo** *si*

- *N es un subgrupo de $(M, +)$.*
- *$a.n \in N \ \forall\ a \in A,\ n \in N$.*

En particular, si N es un submódulo, entonces es en sí mismo A-módulo.

Ejemplos:

1. $\{0\}$ y M son siempre submódulos de M. En caso de que un módulo M tenga solamente a $\{0\}$ y M como submódulos se llamará **simple** (por ejemplo un k-espacio vectorial de dimension 1 es un k-módulo simple).

2. Si G es un grupo y $H \subset G$ es un subgrupo, entonces $k[G]$ es un $k[H]$-módulo y $k[H]$ es un $k[H]$-submódulo de $k[G]$.

3. Sea $G = G_3 = \{1, \omega, \omega^2\}$ y $\mathbb{R}^3$ con la estructura de $\mathbb{R}[G_3]$-módulo dada por $\omega.(x, y, z) = (y, z, x)$. Entonces $N = \{(x, y, z) \in \mathbb{R}^3 \ / x + y + z = 0\}$ es un $\mathbb{R}[G_3]$-submódulo, además N es un módulo simple.

4. Si $N \subseteq M$ es un A-submódulo e I un conjunto, entonces $N^I \subset M^I$ es un A-submódulo.

5. Si M es un A-módulo e I un conjunto se define $M^{(I)}$ como el subconjunto 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. (Verificar) $M^{(I)}$ es un submódulo de M^I.

6. Si $M = M_n(A)$ con la estructura de A-módulo coordenada a coordenada, entonces $sl(A) := \{A \in A \ / tr(A) = 0\}$ es un A-submódulo.

Observación: Si N_1 y N_2 son dos submódulos de M, entonces $N_1 + N_2 := \{x+y \ / x \in N_1 \text{ e } y \in N_2\}$ es un submódulo. También $N_1 \cap N_2$ es un submódulo.

Dados $\{x_1, ..., x_n\}$ elementos de un A-módulo M, siempre se puede hallar el menor submódulo de M (menor en el sentido de la inclusión) que contenga a $\{x_1, ..., x_n\}$. Es claro que si N es un submódulo que contiene a esos elementos y $a_1, ..., a_n$ son elementos cualesquiera de A entonces $a_1x_1 + ... + a_n.x_n \in N$, por lo tanto el conjunto $S = \{a_1x_1 + ... + a_n.x_n \ / a_i \in A\} \subset N$ y S (verificar) es un submódulo, luego S es el submódulo buscado. Notación: $S := \langle x_1, ..., x_n \rangle$ y se llamará el **submódulo generado** por $\{x_1, ..., x_n\}$.

Ejercicios:

1. $$\langle x_1, ..., x_n \rangle = \bigcap_{\substack{\{x_1,...,x_n\} \subset N \\ N \text{submódulo de } M}} N$$

2. Sean B y C dos anillos y $A = B \times C$ con la suma y el producto coordenada a coordenada. Ver que $e_1 = (1, 0)$ y $e_2 = (0, 1)$ son dos idempotentes que conmutan entre si. Si M es un A-módulo, a partir de esos dos idempotentes ver que $M \cong M_1 \times M_2$ donde M_1 es un B-módulo y M_2 es un C-módulo. Si $\{x_1, \ldots, x_n\}$ es un sistema de generadores de M_1 como B-módulo, e $\{y_1, \ldots, y_m\}$ es un sistemq de generqdores de M_2 como C-módulo, ver que

$(x_i, y_j)_{1\leq i\leq n; 1\leq j\leq m}$ es un sistema de generadores de $M_1 \times M_2$ como $B \times C$-módulo. De hecho, el conjunto $\{(x_1, 0), \ldots, (x_n, 0)\} \cup \{(0, y_1), \ldots, (0, y_m)\}$ también es un sistema de generadores de $M_1 \times M_2$ como $B \times C$-módulo.

3. Sea el anillo $A = k \times k$ con la suma y el producto coordenada a coordenada (donde k es otro anillo cualquiera). Ver que el morfismo diagonal $k \to k \times k$ $(\lambda \mapsto (\lambda, \lambda))$ es un morfismo de anillos por lo tanto todo A-módulo es un k-módulo. Ver que $k \times \{0\}$ y $\{0\} \times k$ son dos A-submódulos de A, que son isomorfos como k-módulos pero no como A-módulos.

3.2. Submódulos maximales

Dado un A-módulo M, cuando existan $x_1, ..., x_n \in M$ tales que $\langle x_1, ..., x_n\rangle = M$, M se dirá **finitamente generado** (f.g.) o de **tipo finito** sobre A. Todo anillo A considerado como módulo sobre si mismo es trivialmente finitamente generado, con generador $\{1\}$, pero por ejemplo $k[X]$ no es finitamente generado sobre k.

Vimos usando el lema de Zorn que dado un ideal propio a izquierda de un anillo, siempre existe un ideal maximal (a izquierda) que lo contiene. Los ideales a izquierda de A son exactamente los A-submódulos de A visto como módulo a izquierda, este resultado sobre ideales se generaliza a módulos finitamente generados:

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.*

La demostración es análoga al caso de ideales. La idea es construir un conjunto P parcialmente ordenado, probar que es inductivo superiormente para así tener un elemento maximal en el orden de P, y después ver que ese elemento maximal respecto al orden de P sirve como submódulo maximal.

Demostración: Sea $P = \{S \ / \ S$ es submódulo propio de M y $N \subset S\}$, parcialmente ordenado por inclusión. P es no vacío porque $N \in P$. Sea ahora $\mathcal{C}$ una cadena no vacía en P y sea $V = \cup\, \mathcal{C}$. Del hecho de que la cadena es creciente se tiene que V es un submódulo, también es claro que contiene a S y que contiene también a todos los elementos de la cadena, para ver que es un elemento de P basta ver que es un submódulo propio. Como $M = \langle x_1, ..., x_n\rangle$, si $V = M$ todos los $x_i \in V = \cup\, \mathcal{C}$, entonces cada x_i

pertenece a algún elemento de la cadena, como la cadena es creciente cada vez que un x_i está en un elemento de la cadena, digamos un $\mathcal{C}_\alpha$, entonces está en los $\mathcal{C}_\beta$ con $\beta \geq \alpha$. Como son una cantidad finita, podemos tomar un C_β que contenga a todos los x_1, pero entonces como los x_i generan, ese $\mathcal{C}_\beta = M$ lo que contradice que la cadena esté formada por elementos de P. Luego P tiene un elemento maximal con respecto al orden que es la inclusión, por lo tanto ese elemento 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 $k^{(X)} = \{\sum_{\lambda_x \in k} \lambda_x.x$ de soporte finito $\}$ es un k-módulo, que además es un $k[G]$-módulo (verificar!) con la acción

$$g.(\lambda.x) = \lambda.(g(x))$$

que se extiende linealmente. Por ejemplo $X = \{x_1, ..., x_n\}$ y $G = \mathbb{Z}_n = \langle t \rangle$ (escrito multiplicativamente, $G = \{1, t, t^2, ..., t^{n-1}\}$) que actúa sobre X mediante

$$t.x_i = \begin{cases} x_{i+1} & \text{si } i < n \\ x_1 & \text{si } i = n \end{cases}$$

Luego $k^{(X)} \cong k^n$ es 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 un x_{i_0}, entonces $t.x_{i_0} = x_{i_0+1} \in S$ y análogamente todos los $x_i \in S$, luego $S = M$. De esta manera vemos que ningún submódulo propio puede contener a alguno de los x_i. En cambio $\langle x_1 + x_2 + ... + x_n \rangle = \{\lambda.(x_1 + ... + x_n) \ / \ \lambda \in k\}$ sí es un submódulo propio ($n > 1$).

Ejercicio: si k tiene una raíz n-ésima de la unidad ω (por ejemplo $\omega = 1$, ó $\omega = -1$ si n es par y $2 \neq 0$ en k, ó $\omega = e^{\frac{2k\pi i}{n}}$ 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 $k^{(X)}$.

3.3. Morfismos

Dado un anillo A, tomando como objetos los A-módulos se puede formar una categoría obvia definiendo los morfismos como las funciones entre los A-módulos que respeten la estructura de A-módulos, más precisamente:

Definición 3.3.1. *Sean A un anillo, M y N dos A-módulos y $f : M \to N$ una función. Diremos que f es un* **morfismo** *de A-módulos si es morfismo de grupos abelianos y A lineal, es decir:*

- $f(x+y) = f(x) + f(y)\ \forall\ x, y \in M$.
- $f(a.x) = a.f(x)\ \forall\ a \in A,\ x \in M$ *(notar que en esta igualdad, la acción en la izquierda es la de* M *y en la derecha es la de* N*).*

Ejemplos:

1. Para todo A-módulo M, $Id : M \to M$ es un morfismo de A-módulos, y si $f : M \to N$ y $g : N \to T$ son dos morfismos de A-módulos entonces (verificar) $g \circ f : M \to T$ también es morfismo de A-módulos, por lo tanto 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 V (a través de t) es un $k[X]$-módulo definiendo $P(x).v := P(t)(v)$. Sea W otro espacio vectorial y $s : W \to W$ un endomorfismo de W, si se considera a W como $k[X]$-módulo a través de s, 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 dos grupos abelianos considerados como $\mathbb{Z}$-módulos (dado que ambas categorías son equivalentes), 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 dos submódulos (de M y N resp.). Más aún, por cada submódulo S de M, $f(S)$ es un submódulo de N, y por cada submódulo T de N, $f^{-1}(T)$ es un submódulo de M.

Definición 3.3.2. *Un morfismo de* A*-módulos se dirá* **monomorfismo** *si es inyectivo,* **epimorfismo** *si es sobreyectivo e* **isomorfismo** *si es una biyección.*

En la siguiente proposición se darán varias caracterizaciones de monomorfismo:

Proposición 3.3.3. *Sean* M *y* N *dos* A*-módulos y* $f : M \to N$ *un morfismo de* A*-módulos. Las siguientes afirmaciones son equivalentes:*

1. f *es monomorfismo.*
2. $\mathrm{Ker}(f) = 0$.
3. *Para todo* A*-módulo* T *y todo par de morfismos* $g, h : T \to M$*, la igualdad* $f \circ g = f \circ h$ *implica* $g = h$.

4. *Para todo A-módulo T y para todo morfismo $g : T \to M$, la igualdad $f \circ g = 0$ implica $g = 0$.*

Demostración: 1. $\Leftrightarrow$ 2. supongamos f un monomorfismo, es decir inyectivo. Sea $x \in M$ tal que $f(x) = 0 = f(0)$, como f es inyectivo resulta $x = 0$, es decir $\mathrm{Ker}(f) = 0$.

Suponiendo ahora $\mathrm{Ker}(f) = 0$, sea $x \neq y$, por lo tanto $x - y \neq 0$. Como el único elemento del núcleo de f es el cero, $f(x) - f(y) = f(x - y) \neq 0$ por lo tanto $f(x) \neq f(y)$.

2. $\Rightarrow$ 3. Supongamos $\mathrm{Ker}(f) = 0$ y $g, h : T \to M$ tal que $f \circ g = f \circ h$ y sea $x \in T$ un elemento cualquiera. Por la igualdad anterior, $f(g(x)) = f(h(x))$ o equivalentemente $f(g(x) - h(x)) = 0$, por lo tanto $g(x) - h(x) \in \mathrm{Ker}(f) = 0$ entonces $g(x) - h(x) = 0$ y el x era cualquier elemento de T, entonces $g = h$.

3. $\Rightarrow$ 4. Es claro tomando $h = 0$.

4. $\Rightarrow$ 2. Supongamos 4. y consideremos el caso particular $T = \mathrm{Ker}(f)$ y g la inclusión $i_K : \mathrm{Ker}(f) \to M$. Es claro que $f \circ i_K = 0$, por lo tanto $i_K = 0$, como i_K es inyectiva y tiene imagen 0 resulta $\mathrm{Ker}(f) = 0$.

Observación: La afirmación 3. de la proposición dice que la noción de monomorfismo dada aquí coincide con la noción de monomorfismo categórico (ver apéndice) en la categoría de A-módulos. En la categoría de A-módulos las nociones de epimorfismo e isomorfismo dadas son las mismas que las nociones categóricas. Para los isomorfismos basta notar (verificarlo) que si un morfismo de A-módulos es biyectivo, entonces la función inversa tambíen es un morfismo de A-módulos. Para los epimorfismos veremos más adelante, una vez que hayamos caracterizado los objetos cociente.

Definición 3.3.4. *Sean $(M_n)_{n\in\mathbb{Z}}$ una sucesión de A-módulos junto con 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. Un tipo 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

Consideramos un espacio vectorial V sobre un cuerpo k, dado un subespacio S de V, siempre existe T subespacio tal que $V = S \oplus T$. Si M es un A-módulo, dado un submódulo S no es cierto que siempre exista un complemento (observar el ejemplo $A = M = \mathbb{Z}$ y $S = 2.\mathbb{Z}$). En el caso de espacios vectoriales, al tener $V = S \oplus T$ uno se puede contruir un proyector $p : V \to V$ tal que $\mathrm{Im}(p) = T$, $\mathrm{Ker}(p) = S$ y $p|_T = Id_T$. De esta manera, aplicando p uno "olvida" a los elementos de S, identificando dos elementos de V que difieran entre sí 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 ningún submódulo de M.

Construcción del cociente: Dado un A-módulo M y un submódulo S, es claro que S es un subgrupo de M (normal porque M es abeliano) luego M/S es un grupo abeliano y se tiene un morfismo sobreyectivo de grupos abelianos $\pi : M \to M/S$. Para competar la construcción sólo hay que ver que es posible dar a M/S una estructura de A-módulo tal que la proyección sea un morfismo de A-módulos. Como π es suryectiva, esta estructura, de existir, es única. Definimos pues la acción $a.\overline{m} := \overline{a.m}$ donde $a \in A$ y $\overline{m} \in M/S$ $(\overline{m} = \pi(m))$.

Lema 3.4.1. *Con las notaciones anteriores, la acción de A sobre M/S está bien definida.*

Demostración: Supongamos $\overline{m} = \overline{n}$ o sea $m - n = s \in S$. Por lo tanto $a.m - a.n = a.s \in S$, luego $\overline{a.m} - \overline{a.n} = \overline{a.m - a.n} = \overline{a.s} = 0$, es decir, $\overline{a.m} = \overline{a.n}$.

Ejercicio: Ver 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.

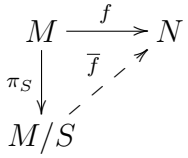
Ejemplos:

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 $A = \mathbb{Z} = M$, $S = 2\mathbb{Z}$, 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 $S = \langle x - a \rangle = \{$ múltiplos de $x - a\}$, entonces $ev_a : k[X] \to k$ $(P \mapsto P(a))$ es un morfismo sobreyectivo por lo tanto $k[X]/\langle x - a \rangle \cong k$. La acción de $k[X]$ sobre k en este caso está dada por $P.\lambda := P(a)\lambda$.

Como toda noción de 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:*

- $S \subseteq \mathrm{Ker}(\pi_S : M \to M/S)$.
- *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 por la flecha punteada:*



o sea, si $f(S) = 0$, existe un único morfismo $\overline{f} : M/S \to N$ tal que $f = \overline{f} \circ \pi_S$.

De manera completamente análoga al caso de grupos se tiene el siguiente

Corolario 3.4.3. *(Teoremas de isomorfismo)*

1. *Sean M y N dos A-módulos y $f : M \to N$ un morfismo de A-módulos. Entonces $M/\operatorname{Ker}(f) \cong \operatorname{Im}(f)$.*

2. *Si $T \subseteq S \subseteq M$ son submódulos de M, entonces $\frac{M/T}{S/T} \cong M/S$.*

3. *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, queda como ejercicio verificar que todos los morfismos que aparecen son A-lineales.

Ejemplos:

1. Sea V un espacio vectorial de dimensión finita y $t : V \to V$ un endomorfismo.
   Supongamos que además existe en V un vector cíclico, es decir un $v_0 \in V$ con $\langle \{v_0, t(v_0), t^2(v_0), \dots\} \rangle = V$ (por ejemplo $V = \mathbb{R}^3$, $t(x, y, z) = (y, z, x)$ y $v_0 = (1, 0, 0)$). Consideremos la aplicación $k[X] \to V$ dada por $P(x) \mapsto P(t)(v_0)$. Como v_0 es un vector cíclico la aplicación es sobreyectiva. $\operatorname{Ker}(k[X] \to V) = \langle m_{v_0}(t) \rangle$ donde $m_{v_0}(t)$ es el polinomio mónico de grado mínimo que anula a t evaluado en v_0. Notar que en este caso, por ser v_0 un vector cíclico, m_{v_0} coincide con el polinomio minimal y con el característico Por otro lado, (V, t) es un $k[X]$-módulo a través de t. Verificar que la acción en el cociente está dada justamente por t, es decir $(V, t) \cong k[X]/\langle m_{v_0}(t) \rangle$ como $k[X]$-módulos.

2. Sea $I \subset \mathbb{R}$ un cerrado y $X \subset \mathbb{R}$ un abierto que contiene al cerrado I. Se sabe que toda función continua definida sobre I se puede extender a todo $\mathbb{R}$, en particlar a X, esto dice que el morfismo restricción $C(X) \to C(I)$ es sobreyectivo, el núcleo de esta aplicación se lo nota $I^0 = \{f : X \to \mathbb{R} \ / \ f(y) = 0 \ \forall \ y \in I\}$. Se tiene entonces $C(X)/I^0 \cong C(I)$; el isomorfismo es de $C(X)$-módulos.

Ejercicio: Caracterizar el cociente $\mathbb{Z} \oplus \mathbb{Z}$ 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 $(0,3)$, después mire la imagen).

Observación: (Submódulos del cociente) Si $S \subseteq M$ es un A-submódulo, uno tiene el morfismo $\pi : M \to M/S$, luego por cada submódulo T de M, $\pi(T)$ es un submódulo de M/S. Esta correspondencia no es en general 1-1 pues si $T \subset S$, claramente $\pi(T) = \{0\}$, si tomamos T' un submódulo de M/S, $\pi^{-1}(T')$ es un submódulo de M, pero además $S \subseteq \pi^{-1}(T')$. Queda como ejercicio verificar que para los submódulos T de M vale la igualdad:

$$\pi^{-1}(\pi(T)) = \langle T, S \rangle = T + S$$

Demostrar también que a través de 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, N dos A-módulos, $f : M \to N$ un morfismo de A-módulos. Las siguientes afirmaciones son equivalentes:*

1. *f es un epimorfismo.*
2. $\mathrm{Coker}(f) := N/\mathrm{Im}(f) = 0$.
3. *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 $g = h$.*
4. *Para todo A-módulo T y para todo morfismo $g : N \to T$, la igualdad $g \circ f = 0$ implica $g = 0$.*

Demostración: 1. $\Leftrightarrow$ 2. es claro, pues $N/\mathrm{Im}(f) = 0 \Leftrightarrow N = \mathrm{Im}(f)$.

2. $\Rightarrow$ 3. Sea $n \in N$ y g, h como en 3., al ser $\mathrm{Im}(f) = N$, existe un $m \in M$ tal que $n = f(m)$, ahora la identidad que verifican g y h dice que $g(f(m)) = h(f(m))$ es decir $g(n) = h(n)$ para cualquier $n \in N$, luego $g = h$.

3. $\Rightarrow$ 4. Es claro tomando $h = 0$.

4. $\Rightarrow$ 2. Suponemos que vale 4., tomamos en particular $T = N/\mathrm{Im}(f)$ y $g = \pi : N \to N/\mathrm{Im}(f)$. Claramente $\pi \circ f = 0$, luego $\pi = 0$, pero π es suryectiva, entonces $N/\mathrm{Im}(f) = 0$.

Observación: La parte 3. de esta proposición demuestra, como fue anticipado, que la noción de epimorfismo definida anteriormente 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, categoría, una función con imagen densa es un epimorfismo categórico. Un ejemplo mas algebraico el 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 1_B. Por linealidad, queda univocamente determinado en $\mathbb{Z}$, y por multiplicatividad queda determinado en $\mathbb{Q}$. En particular, queda determinado por su restriccion a $\mathbb{Z}$, por lo tanto la inclusion $\mathbb{Z} \to \mathbb{Q}$ 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 $T \cong \mathrm{Coker}(f)$.

Terminamos esta sección mencionando otra dirección hacia 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 uno le 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 $r \circ f = Id_V$.

Dualmente, si $f : V \to W$ es un epimorfismo, $\mathrm{Ker}(f) \subset V$ es un subespacio, uno puede encontrar un complemento y escribir $V = \mathrm{Ker}(f) \oplus S$. Es un ejercicio sencillo verificar que $f|_S$ es un monomorfismo y que $f(S) = f(V) = W$, por lo tanto $f|_S : S \to W$ es un isomorfismo. Podemos definir entonces una transformación lineal $s : W \to V$ a partir de la composición $W \xrightarrow{(f|_S)^{-1}} S \xrightarrow{inc} V$. Aquí verificamos sin dificultad $f \circ s = Id_W$.

Definición 3.4.5. *Sea $f : M \to N$ un morfismo entre dos A-módulos. El morfismo f se dirá*

- *una* **sección** *si existe un morfismo $g : N \to M$ tal que $g \circ f = Id_M$.*
- *una* **retracción** *si existe un morfismo $g : N \to M$ tal que $f \circ g = Id_N$.*

Observación: Si f es una sección entonces es inyectiva porque si $f(m) = 0 \Rightarrow x = g(f(m)) = g(0) = 0 \Rightarrow \mathrm{Ker}(f) = 0$. Si f es una retracción entonces es sobreyectiva porque dado un $n \in N$, $n = f(g(n))$, luego $n \in \mathrm{Im}(f)$.

Como corolario de los comentarios de los dos párrafos anteriores, las nociones de epimorfismo / retracción y monomorfismo / sección coinciden en la categoría de espacios vectoriales. En la categoría de A-módulos con A un anillo cualquiera no sucede lo mismo, queda 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 $\mathbb{Z}_4$, se deja como ejercicio encontrar morfismos entre estos grupos que sean monomorfismos o epimorfismos pero que no sean ni secciones ni retracciones.

3.5. Suma y producto

Sea I un conjunto de índices, A un anillo, y $(M_i)_{i\in I}$ una familia de A-módulos. Entonces el producto cartesiano $\prod_{i\in I} M_i$ es un A-módulo definiendo

$$a.\{m_i\}_{i\in I} := \{a.m_i\}_{i\in I}$$

Recordamos que el producto cartesiano está definido como

$$\prod_{i\in I} M_i := \{f : I \to \cup_{i\in I} M_i \text{ tales que } f(i) \in M_i \ \forall i \in I\}$$

Este módulo producto viene provisto de morfismos A-lineales que son las proyecciones a cada coordenada, 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 $i \in I$ 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).

Notamos que considerando en $\prod_{i\in I} M_i$ los elementos de la forma $(m_i)_{i\in I}$ donde $m_i = 0$ para todo i salvo eventualmente un i_0, el módulo M_{i_0} puede identificarse con un submódulo del producto.

De esta manera podemos definir el 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:

$$\bigoplus_{i\in I} M_i := \{(m_i)_{i\in I} \text{ tales que } m_i = 0 \text{ salvo eventualmente un número finito de índices}\}$$

Es un submódulo del producto (por lo tanto un A-módulo), y para cada $i_0 \in I$ se tienen inyecciones $j_{i_0} : M_{i_0} \to \oplus_{i\in I} M_i$. Si el conjunto de índices es finito, la suma directa obviamente coincide con el producto directo.

Si se tienen definidos morfismos $\phi_i : M_i \to N$ donde N es un A-módulo cualquiera, como $\oplus_{i\in I} M_i$ esta generado por los M_i, extendiendo por linealidad se tiene 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 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 3.5.1. *Sea* $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$ *una sucesión exacta corta de A-módulos. Son equivalentes:*

1. *f es una sección.*
2. *g es una retracción.*
3. *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, la sucesión exacta se dirá **escindida**, también diremos que la sucesión se parte, o que es "split", la sección de g o la retracción de f se denominan "splittings".

Demostración: Mirando la condición 3., es claro que π es una retracción, tanto como que j es una sección, usando el isomorfismo $N \cong M \oplus T$ del diagrama se tiene que 3. implica 1. y 2.

Veremos que 1. implica 3. y dejaremos como ejercicio ver que por ejemplo 2. implica 3. Sea $h : N \to M$ una retracción de f (o sea $h \circ f = Id_M$). Definimos $\phi : N \to M \oplus T$ por $\phi(n) := (h(n), g(n))$. Afirmamos que ϕ es un isomorfismo y que hace del diagrama en 3. un diagrama conmutativo.

Es claro que $\pi \circ \phi = g$ (conmutatividad del cuadrado de la derecha), y la propiedad de que h sea retracción de f es la conmutatividad del cuadrado de la izquierda.

Para ver que ϕ es un monomorfismo, si $n \in \mathrm{Ker}(\phi)$ entonces en particular $n \in \mathrm{Ker}(g) = \mathrm{Im}(f)$, escribiendo $n = f(m)$ se tiene que $0 = h(n) = h(f(m)) = m$, por lo tanto $n = 0$.

Para ver que ϕ es un epimorfismo, sea $m \in M$ y $t \in T$. Como g es epimorfismo, existe $n \in N$ tal que $g(n) = t$. Consideramos $f(m) - f(h(n)) + n \in N$, este elemento verifica $\phi(f(m) - f(h(n)) + n) = (m, t)$.

Concluimos el capítulo de generalidades de módulos con la caracterización de módulos generados por un único elemento:

3.6. Módulos cíclicos

En el caso de grupos abelianos se tenía una descripción muy concisa de los grupos cíclicos, todos son un cociente de $\mathbb{Z}$. Como los subgrupos de $\mathbb{Z}$ son conocidos, entonces son conocidos todos los grupos abelianos cíclicos.

Si se tiene ahora un A-módulo cíclico M, es decir, un A-módulo en el que exista un elemento $x \in M$ con $A.x = \langle x \rangle = M$, podemos definir un morfismo sobreyectivo de A en M a través de $a \mapsto a.x$. El núcleo de esta aplicación es un submódulo (a izquierda) del A-módulo A, es decir, un ideal a izquierda de A, llamando $I = \mathrm{Ker}(A \to M)$, se tiene $M \cong A/I$.

Recíprocamente, si I es un ideal a izquierda de A entonces es un A-submódulo de A, y A/I es un A-módulo (a izquierda), que además es cíclico, pues $A/I = \langle \overline{1} \rangle$. Luego todo módulo cíclico es isomorfo a un cociente de A por un ideal a izquierda. Se conocen así todos los A-módulos cíclicos siempre que se tenga una caracterización de los ideales a izquierda de A.

3.7. Ejercicios

1. Definición: dado un anillo A y un A-módulo M, M se dice **divisible** si para cualquier $0 \neq a \in A$ y $m \in M$ existe un $m' \in M$ tal que $a.m' = m$. Sea $G_\infty = \underset{n\in\mathbb{N}}{\cup} G_n \subset S^1$.

   a) Probar que es un subgrupo (abeliano) de S^1 por lo tanto un $\mathbb{Z}$-módulo. Ver que es divisible.

   b) Ver que $G_{p^\infty} := \underset{n\in\mathbb{N}}{\cup} G_{p^n}$ es un submódulo de G_∞ y que también es divisible.

2. Sea A un anillo conmutativo y M un A-módulo. Se define la **torsión** de M como $t(M) := \{m \in M \text{ tal que } \exists\ a \in A \text{ con } a \neq 0 \text{ y } a.m = 0\}$. Si A es íntegro ver que $t(M)$ es un submódulo. ¿dónde se usa que A sea íntegro?

3. Sea A íntegro, M y N dos submódulos y $f : M \to N$ un morfismo A-lineal. Ver que $f(t(M)) \subset t(N)$ y por lo tanto la asignación $M \mapsto t(M)$ es funtorial. Ver que $t(t(M)) = t(M)$ y $t(M/t(M)) = 0$.

4. Viendo al grupo abeliano $M = (\mathbb{C} - \{0\}, .)$ como $\mathbb{Z}$-módulo, encontrar los elementos de torsión.

5. Caracterizar $M = \mathbb{Z} \oplus \mathbb{Z}/\langle(4, 6)\rangle$ calcular $t(M)$ y $M/t(M)$.

6. 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.

7. Sea k un cuerpo, y C la categoría formada por:

   - $Obj(C)$ = pares (V, ϕ) donde V es un k-espacio vectorial y $\phi : V \to V$ es un endomorfismo.
   - Para cada par de objetos (V, ϕ) y (W, ψ), $\mathrm{Hom}_C((V, \phi), (W, \psi)) = \{f : V \to W \text{ transformación lineal tal que } f(\phi(v)) = \psi(f(v))\ \forall\ v \in V\}$.

   a) Ver que esta categoría se identifica con la categoría de $k[X]$-módulos. Probar que $(V, \phi) \cong (V, \psi)$ como $k[X]$-módulos si y sólo si ϕ es un endomorfismo conjugado a ϕ, es decir, que existe un $\alpha \in Aut_k(V)$ tal que $\phi = \alpha \circ \psi \circ \alpha^{-1}$.

b) Sea (V, ϕ) como antes. Ver 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 en $k[X]$-sumandos directos.

c) Encontrar un $k[X]$-módulo de dimensión 2 (sobre k) que no admita sumandos directos no triviales.

d) Si $\lambda \in k$, $ev_\lambda : k[X] \to k$ $(P \mapsto P(\lambda))$ es un morfismo de anillos, por lo tanto induce 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 $\lambda \neq \lambda'$?

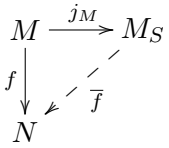
e) Sea V un espacio vectorial de dimensión finita, ϕ un endomorfismo de V. Entonces ϕ es diagonalizable si y sólo si V se descompone como $k[X]$-módulo en suma directa de submódulos isomorfos a los k_λ $(\lambda \in k)$.

f) Si M es un $k[X]$-módulo cíclico, entonces o bien es de dimensión finita, o bien es isomorfo a $k[X]$ (sug. ver el teorema de 'clasificación' de grupos cíclicos y copiar la idea).

8. (Localización de módulos) Sea A un anillo, $S \subset Z(A)$ un subconjunto multiplicativamente cerrado y M un A-módulo a izquierda. Se define M_S como el cociente de los pares (m, s) con $m \in M$ y $s \in S$ bajo la relación de equivalencia $(m, s) \equiv (m', s') \Leftrightarrow \exists\ t \in S$ tal que $t(s'.m - s.m') = 0$. La clase del elemento (m, s) bajo esta relación se lo denotará (como era de esperar) $\frac{m}{s}$, y $M_S := \{(m, s)\ : m \in M,\ s \in S\}/\sim = \{\frac{m}{s}\ :\ m \in M,\ s \in S\}$.

a) Ver que M_S es naturalmente un A-módulo a izquierda y que la función $j_M : M \to M_S$ $m \mapsto \frac{m}{1}$ es A-lineal.

b) Ver que además M_S es un A_S-módulo bajo la acción obvia $\frac{a}{s}.\frac{m}{t} = \frac{a.m}{st}$, y que además $j_M : M \to M_S$ tiene la siguiente propiedad: Si N es un A_S-módulo (y por lo tanto tambien un A-módulo (¿porqué?)) y $f : M \to N$ es una morfismo A-lineal entonces existe una única $\overline{f} : M_S \to N$ que factoriza a f a través de j_M, es decir, que $f = \overline{f} \circ j_M$. (diagrama de rigor:)



c) Por cada $s \in S$ sea $M.\frac{1}{s} := M$. Ver que $M_S \cong \underset{s\in S}{\oplus} M.\frac{1}{s}/\langle t.m.\frac{1}{st} - m.\frac{1}{s}\rangle$. La función j_M bajo este isomorfismo es la composición $M = M\frac{1}{1} \to \oplus_{s\in S} M.\frac{1}{s} \to^{\pi} \oplus_{s\in S} M.\frac{1}{s}/\langle t.m.\frac{1}{st} - m.\frac{1}{s}\rangle$.

d) Interpretar y demostrar la frase 'la asignación $M \mapsto M_S$ es funtorial'.

9. (Polinomios de Laurent) Sea $S \subset k[X]$, $S = \{1, X, X^2, X^3, ..., X^n, ...\}$. 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, $V_S \cong V \Leftrightarrow \phi$ es un isomorfismo.

   c) Sea V es de dimensión finita, $\mathrm{Ker}(\phi^n) \subset V$ es un $k[X]$-submódulo de V para todo n, sea $t(V) := \cup_{n\in\mathbb{N}} \mathrm{Ker}(\phi^n)$. Entonces $t(V)$ coincide con $\mathrm{Ker}(V \to V_S)$ y además $V_S \cong V/t(V)$. (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 $t(V) = \mathrm{Ker}(V \to V_S)$.)

10. Sea k un cuerpo, probar que para $P \in k[X, X^{-1}]$, la función l (l de 'largo') tal que $P = \sum_{k=n} ma_k x^k \mapsto m - n =: l(P)$ donde $P = \sum_{k=n}^{m} a_k x^k$ es una escritura tal que a_n y a_m son ambos distintos de cero 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). Ver que todo $k[X, X^{-1}]$-módulo cíclico o bien es de dimensión finita o bien es isomorfo a $k[X, X^{-1}]$.

11. Sea (V, ϕ) un $k[X]$-módulo con ϕ nilpotente. ¿Es (V, ϕ) un $k[[X]]$-módulo?

12. Sabiendo que en $k[[X]]$ los elementos de la forma $\lambda + x.p$ con $p \in k[[X]]$ y $0 \neq \lambda \in k$ son unidades (si no lo sabe, demuéstrelo), probar que los todos los ideales de $k[[X]]$ son 0, y $\langle x^n\rangle$ con $n \in \mathbb{N}_0$.

13. Sea M un $k[[X]]$-módulo (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.

14. (Ideales a izq. de matrices) Sea k un cuerpo, consideremos el anillo $M_3(k)$ y $e \in M_3(k)$ la matriz $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. Ver lo siguiente:

a) $e^2 = e$, el ideal a derecha $e.M_3(k)$ consiste de las matrices de la forma $\begin{pmatrix} * & * & * \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, el ideal a izquierda $M_3(k).e$ consiste de las matrices de la forma $\begin{pmatrix} * & 0 & 0 \\ * & 0 & 0 \\ * & 0 & 0 \end{pmatrix}$, y el ideal bilátero generado por e es $M_3(k)$.

b) Sea $I \subseteq A$ un ideal a izquierda, y sea S_I el subespacio $e.I \subseteq \begin{pmatrix} * & * & * \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, entonces el ideal generado por S_I (i.e. $M_3(k).S_I$) coincide exactamente con I.

c) Los ideales a izquierda de $M_3(k)$ están en correspondencia 1-1 con los subespacios de k^3. Encuentre los ideales asociados a los subespacios generados respectivamente por $(0,0,1)$, $(0,1,0)$ y $(1,0,0)$.

d) Generalización 1: demuestre que los ideales a izquierda de $M_n(k)$ están en correspondencia biyectiva con los subespacios de k^n (con $n \in \mathbb{N}$). Generalización 2: si A es un anillo cualquiera demuestre que los ideales a izquierda de $M_n(A)$ están en correspondencia biyectiva con los submódulos a izquierda de A^n.

15. Sea k un cuerpo y $n \in \mathbb{N}$, los únicos ideales biláteros de $M_n(k)$ son 0 y $M_n(k)$. Si A es un anillo, los únicos ideales biláteros de $M_n(A)$ son de la forma $M_n(I)$ con $I \subseteq A$ un ideal bilátero (sug. si e es una matriz tipo la del ejercicio anterior, entonces para $J \subseteq M_n(A)$, la asignación $J \mapsto e.J.e$ da una matriz 'concentrada' en el lugar 11 y establece una biyección entre ideales bilateros de A y de $M_n(A)$). ¿puede haber un morfismo de anillos $M_n(k) \to k$?

16. Sea M un A-módulo a derecha y $B = \mathrm{End}_A(M)$. Ver que la acción $\mathrm{End}_A(M) \times M \to M$, $(f, m) \mapsto f(m)$ define sobre M estructura de $\mathrm{End}_A(M)$-módulo a izquierda, además M resulta un $\mathrm{End}_A(M) - A$-bimódulo (i.e. las dos estructuras son compatibles. Si $M = A^{n\times 1}$ (o sea A^n visto como 'vector columna') es un A-módulo a derecha, ver que M además es un $M_n(A)$-módulo a izquierda con la multiplicación usual de matrices. Ver que esta estructura coincide con la definida antes, identificando $\mathrm{End}_A(A^n) \cong M_n(A)$.

4

Módulos noetherianos y artinianos

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, es decir, 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 dimensión, y la propiedad de ser finitamente generado no tiene por que 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 anillo de funciones, $M = A$ y $S = \{f \in A/\ f(x) \neq 0$ sólo para finitos valores de $x\}$. El conjunto S es un ideal de A, por lo tanto un A-submódulo de M. M está generado por la función constante 1, sin embargo S no es un A-módulo finitamente generado. Para ver esto, supongamos que existieran $f_1, \ldots, f_n \in S$ tales que $\langle f_1, \ldots, f_n \rangle = S$. Sea $\{x_1, \ldots x_s\} \subset [0,1]$ la unión de todos los puntos x tales que existe alguna f_i con $f_i(x) \neq 0$ (que claramente es un conjunto finito) y sea $x_0 \in [0,1] - \{x_1, \ldots, x_s\}$. Si definimos $\phi : [0,1] \to \mathbb{R}$ por $\phi(x_0) = 1$ y $\phi(x) = 0$ si $x \neq x_0$ entonces $\phi \in S$ pero ϕ nunca puede pertenecer a $\langle f_1, \ldots, f_n \rangle$.

Tampoco puede asegurarse, dado un anillo A arbitrario, que si dos A-

módulos M_1 y M_2 son de tipo finito (i.e. 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 $k[X]$ (k cuerpo) tienen la propiedad siguiente: todo ideal está generado por un 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. Mas generalmente:

Proposición 4.1.1. *Sea A un anillo cualquiera y*

$$0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$$

una sucesión exacta corta de A-módulos. Entonces:

1. *M_2 de tipo finito $\Rightarrow$ M_3 es de tipo finito.*
2. *M_1 y M_3 de tipo finito $\Rightarrow$ M_2 es de tipo finito.*

Demostración: 1. Sea $\{y_1, \ldots, y_n\}$ un conjunto de generadores de M_2 y $z \in M_3$. 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 $a_i \in A$, entonces $z = \sum_{i=1}^{n} a_i g(y_i)$, por lo tanto $\{g(y_1), \ldots, g(y_n)\}$ genera M_3.

2. Sean $M_1 = \langle x_1, \ldots, x_r \rangle$, $M_3 = \langle z_1, \ldots, z_s \rangle$ y sean $y_1, \ldots, y_s$ elementos de M_2 tales que $g(y_i) = z_i$ $(i = 1, \ldots, s)$. Afirmamos que $M_2 = \langle f(x_1), \ldots, f(x_r), y_1, \ldots, y_s \rangle$.

En efecto, sea $y \in M_2$, $g(y) \in M_3$ entonces existen $a_1, \ldots, a_s \in A$ con $g(y) = \sum_{i=1}^{s} a_i z_i$. Como $g(y) = g(\sum_{i=1}^{s} a_i y_i)$ entonces $g(y - \sum_{i=1}^{s} a_i y_i) = 0$. El elemento $y' = y - \sum_{i=1}^{s} a_i y_i$ está en la imagen de f, que es un módulo isomorfo a M_1 vía f, en consecuencia $\mathrm{Im}(f) = \langle f(x_1), \ldots, f(x_r) \rangle$ y existen $b_1, \ldots, b_r$ con $y' = \sum_{i=1}^{r} b_i f(x_i)$. Despejando y se tiene $y = \sum_{i=1}^{r} b_i f(x_i) + \sum_{i=1}^{s} a_i y_i$.

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. *Dado un anillo A, un A-módulo M se dirá* **noetheriano** *si y sólo si todo submódulo de M es finitamente generado (en particular M mismo es de tipo finito).*

Ejemplos:

1. Los A-módulos nulos, simples, finitos (como conjuntos, por ejemplo los $\mathbb{Z}_n$ como $\mathbb{Z}$-módulos) y A-módulos con un número finito de submódulos son noetherianos.

2. Si A es principal, entonces A es un A-módulo noetheriano.

3. Dado un cuerpo k, un espacio vectorial V es noetheriano si y sólo si $dim_k(V) < \infty$.

La propiedad "ser noetheriano" puede expresarse de manera equivalente mediante cualquiera de las siguientes afirmaciones:

1. Todo conjunto no vacío de submódulos de M tiene un elemento maximal (respecto a la inclusión).

2. Toda sucesión (no vacía) creciente de submódulos se estaciona.

Veamos que 1. y 2. son equivalentes:

$1 \Rightarrow 2$: Se toma como conjunto no vacío de submódulos de M al conjunto de submódulos que aparece en la sucesión. Este conjunto tiene un elemento maximal, que es un elemento de la sucesión, luego la sucesión se estaciona en ese elemento.

$2 \Rightarrow 1$: Sea $\mathcal{C} \neq \emptyset$ un conjunto de submódulos de M sin elemento maximal. Como $\mathcal{C} \neq \emptyset$, $\exists S_1 \in \mathcal{C}$, y como S_1 no es maximal $\Rightarrow \exists S_2 \in \mathcal{C}$ tal que $S_1 \subset S_2$ y la inclusión es estricta. Siguiendo inductivamente se puede encontrar una sucesión de elementos S_i de $\mathcal{C}$ tales que $S_i \subset S_{i+1}$ (inclusiones estrictas), lo que es un absurdo, porque sería una sucesión que no se estaciona.

Veamos ahora que 1. y 2. equivalen a la definición de noetheriano:

Sea M que verifica 1 y N un submódulo de M, queremos ver que N es finitamente generado. Definimos para ésto $\mathcal{C} = \{$ submódulos de M de tipo finito contenidos en $N\}$. Como $\{0\} \in \mathcal{C}$, entonces $\mathcal{C}$ no es vacío. Por 1, $\mathcal{C}$ tiene un elemeno maximal que llamaremos N_0. Veamos que $N_0 = N$. Si no, sea $x \in N - N_0$, y sea $N_0' = N_0 + \langle x \rangle$. Entonces N_0' es de tipo finito y N_0 está contenido estrictamente en N_0', absurdo. Luego $N_0 = N$.

Supongamos ahora M noetheriano y $N_1 \subset N_2 \subset \cdots \subset N_k \subset \ldots$ una cadena creciente de submódulos. Como es creciente, $N := \cup_{k \in \mathbb{N}} N_k$ es un submódulo, que es finitamente generado porque M es noetheriano. Sean $x_1, \ldots, x_n \in N$ tales que $\langle x_1, \ldots, x_n \rangle = N = \cup_{k \in \mathbb{N}} N_k$, luego, para cada $i = 1, \ldots, n$ $\exists k_i$ / $x_i \in N_{k_i}$. Si n_0 es el maximo de los k_i entonces por

ser la sucesión creciente, todos los $x_i \in N_k$ cada vez que $k \geq n_0$, luego $N_k = N \ \forall k \geq n_0$.

Observación: Como la propiedad de un A-módulo de ser noetheriano se enuncia en términos de todos los los submódulos de M, resulta que un submódulo S de un A-módulo noetheriano es noetheriano. Por otro lado, los submódulos del cociente M/S de M están en correspondencia con los submódulos de M que contienen a S. Luego, un cociente de un noetheriano es también noetheriano. Más generalmente:

Proposición 4.1.4. *Sea* $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ *una sucesión exacta de A-módulos. Entonces*

- M *noetheriano* $\Rightarrow$ M' *y* M'' *son noetherianos.*
- M' *y* M'' *son noetherianos* $\Rightarrow$ M *noetheriano.*

Demostración: Dado que (al ser f un monomorfismo) $M' \cong \mathrm{Im}(f)$ que es un submódulo de M y que (al ser g epimorfismo) $M'' \cong M/\operatorname{Ker}(g)$, el primer ítem ya se ha demostrado.

Supongamos ahora M'' y M' noetherianos. Sea N un submódulo de M, queremos ver que es finitamente generado. Consideramos 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, por lo tanto N es finitamente generado (Proposición 4.1.1).

Observación: Ser noetheriano es una propiedad que se preserva por sumas directas finitas, ya que si $M_1, \ldots, M_n$ son módulos noetherianos, se tiene la sucesión exacta corta

$$0 \to M_1 \to \oplus_{i=1}^{n} M_i \to \oplus_{i=2}^{n} M_i \to 0$$

y lo enunciado se sigue inductivamente. Sin embargo, ser noetheriano no se preserva por sumas directas infinitas ni por productos infinitos, por ejemplo $\mathbb{Z}$ es un $\mathbb{Z}$-módulo noetheriano (ya que es principal), pero $\mathbb{Z}^{(\mathbb{N})}$ no es noetheriano porque no es finitamente generado (considerar la cadena creciente $\langle e_1 \rangle \subset \langle e_1, e_2 \rangle \subset \langle e_1, e_2, e_3 \rangle \subset \ldots$). Como $\mathbb{Z}^{(\mathbb{N})}$ es un submódulo de $\mathbb{Z}^{\mathbb{N}}$, entonces $\mathbb{Z}^{\mathbb{N}}$ tampoco es noetheriano.

Definición 4.1.5. *Un anillo A se dirá un* **anillo noetheriano** *si y sólo si A es un A-módulo noetheriano.*

Ejemplos:

1. $\mathbb{Z}$ y $k[x]$ (k cuerpo) son anillos noetherianos porque son principales.
2. $k[x_1, \dots, x_n, \dots]$ es un anillo que no es noetheriano, sin embargo es íntegro, por lo que se lo puede considerar como un subanillo de su cuerpo de fracciones, que es trivialmente noetheriano. Esto muestra que subanillos de anillos noetherianos no tienen por que ser anillos noetherianos.

Sea A un anillo noetheriano y M un A-módulo. ¿Podemos afirmar que M es noetheriano? En principio M debería ser finitamente generado, por lo tanto no todo A-módulo será noetheriano. Pero como demostraremos ahora, esa es la única obstrucción para serlo:

Proposición 4.1.6. *Sea A un anillo noetheriano, M un A-módulo de tipo finito, entonces M es noetheriano.*

Demostración: Como M es de tipo finito, existe un epimorfismo $A^n \to M$ para algún $n \in \mathbb{N}$. Si A^n fuera noetheriano entonces la demostración estaría completa. Pero es consecuencia de que $A^n = \oplus_{i=1}^n A$, A es un A-módulo noetheriano, y "ser noetheriano" se preserva por sumas directas finitas.

Ejercicios:

1. Si A es un anillo noetheriano y $S \subset Z(A)$ es un subconjunto multiplicativamente cerrado, entonces A_S es un anillo noetheriano porque los ideales de A_S están en correspondencia con los ideales de A que no contienen a S (y esa correspondencia preserva la inclusión). Sea M un A-módulo noetheriano, ¿es cierto que M_S es un A_S-módulo noetheriano?
2. Sea A un anillo y J un ideal bilátero. Caracterizar los ideales (a izquierda) de A/J en términos de los ideales (a izquierda) de A. Concluir que si A es un anillo noetheriano, entonces A/J es un anillo noetheriano.

4.2. 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) Sea A un anillo noetheriano, entonces $A[x]$ es un anillo noetheriano.*

Demostración: Sea J un ideal de $A[x]$, queremos ver que J es finitamente generado sobre $A[x]$. Consideramos para eso el siguiente ideal de A:

Sea $I = \{a \in A/\ \exists p \in J \subset A[x] \text{ con } p = a.x^m + \sum_{i=0}^{m-1} a_i x^i\}$, es decir, I es el "ideal de coeficientes principales de los polinomios de J".

Ante todo veamos que I es un ideal (a izquierda) de A:

Sean $a, a' \in I$, luego existen $p, p' \in J$ con $p = a.x^m + \sum_{i=0}^{m-1} a_i x^i$ y $p' = a'.x^{m'} + \sum_{i=0}^{m'-1} a'_i x^i$. Podemos suponer sin pérdida de generalidad que $m \geq m'$ (sino se multiplica a p por alguna potencia de x suficientemente grande) y resulta entonces que $a + a'$ es el coeficiente principal del polinomio $p + x^{m-m'}.p'$ que pertenece a J y por lo tanto $a + a' \in I$.

Si $b \in I$ y $a \in A$, sea p un polinomio en J con coeficiente principal b, entonces $a.p \in J$ y consecuentemente $a.b \in I$.

Ahora que sabemos que I es un ideal a izquierda de A, como A es noetheriano, I es finitamente generado sobre A. Sean $a_1, \ldots, a_r$ un sistema de generadores (sobre A) de I, y sean $p_1, \ldots, p_r$ polinomios en J tal que el coeficiente principal de cada p_i es a_i, los cuales supondremos todos del mismo grado m (sino, se multiplica a cada p_i por $x^{m-grad(p_i)}$ donde m es el máximo de los grados de los p_i). Veremos 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, $N = J \cap A_{<m}[x]$. J estará generado por los p_i "a menos de N". Como $A_{<m}[x]$ es un A-módulo finitamente generado, A es noetheriano y $N \subseteq A_{<m}[x]$ es un submódulo, entonces N es finitamente generado (como A-módulo). Sea entonces $\{q_1, \ldots, q_s\} \subset N$ un sistema de generadores (sobre A) de N; afirmamos que J está generado (como $A[x]$-módulo) por $\{p_1, \ldots, p_r, q_1, \ldots, q_s\}$.

Demostremos esta última afirmación. Sea p un polinomio de J, si $gra(p) < m$ entonces $p \in N = \langle q_1, \ldots, q_r \rangle_A \subset \langle q_1, \ldots, q_r \rangle_{A[x]}$. Si $gra(p) = g \geq m$ razonaremos inductivamente. Sea a el coeficiente principal de p, luego $a \in I$ y se lo puede escribir como $a = \sum_{i=1}^{r} \lambda_i a_i$ donde $\lambda_i \in A$ y los a_i son los generadores de I. Ahora bien, los a_i son los corficientes principales de los p_i que tienen todos grado $m \leq g$, luego el polinomio $\widetilde{p} = x^{g-m}.\sum_{i=1}^{r} \lambda_i p_i$ es un polinomio que pertenece a J y que tiene como coeficiente principal a a, de hecho, $\widetilde{p} \in \langle p_1, \ldots, p_r \rangle_{A[x]}$. Si consideramos el polinomio $p - \widetilde{p}$, es un polinomio en J con grado menor estricto que el grado de p, por hipótesis inductiva este

polinomio pertenece al ideal generado por $\{p_1, \ldots, p_r, q_1, \ldots, q_s\}$. Como $\widetilde{p} \in \langle p_1, \ldots, p_r \rangle_{A[x]} \subseteq \langle p_1, \ldots, p_r, q_1, \ldots, q_s \rangle$, despejando p resulta que también está en el generado por esos mismos polinomios.

Corolario 4.2.2. *1. Si A es un anillo noetheriano entonces $A[x_1, \ldots, x_n]$ es anillo noetheriano, en particular, para k un cuerpo, $k[x_1, \ldots, x_n]$ es noetheriano.*

2. Sea B un anillo y A un subanillo de B que es noetheriano como anillo. Supongamos que existe un $b \in B$ tal que b conmuta con los elementos de A y 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. Lo mismo se puede decir de B si estuviera generado como A-álgebra por finitos elementos que conmuten entre sí .

Demostración: 1. Es claro escribiendo $A[x_1, \ldots, x_n] = (A[x_1, \ldots, x_{n-1}])[x_n]$, y aplicando inducción más el teorema de Hilbert.

2. Sea $b \in B$ que genera a B como A-álgebra. La definición de "genera como A-álgebra" es equivalente a que el morfismo de anillos $ev_b : A[x] \to B$ $(p \mapsto p(b))$ sea sobreyectivo. Como A es noetheriano, por el teorema anterior $A[x]$ es noetheriano, luego B es un anillo noetheriano porque existe un epimorfismo de anillos de un noetheriano en B. La aserción con varios generadores es idéntica sustituyendo $A[x]$ por $A[x_1, \ldots, x_n]$.

Ejemplo: Sea $d \in \mathbb{Z}$ un número que no es un cuadrado, $\sqrt{d}$ una raíz compleja de d y sea $\mathbb{Z}[\sqrt{d}] = \{a + b.\sqrt{d} \ / \ a, b \in \mathbb{Z}\}$. Este subconjunto de $\mathbb{C}$ de hecho un subanillo de $\mathbb{C}$ (verificar que la multiplicacion de dos elementos de $\mathbb{Z}[\sqrt{d}]$ es de nuevo un elemento de $\mathbb{Z}[\sqrt{d}]$). Por otro lado, existe un epimorfismo de anillos $\mathbb{Z}[x] \to \mathbb{Z}[\sqrt{d}]$ determinado por $(x \mapsto \sqrt{d})$. 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. Dado un A-módulo M, cuál es la afirmación "dual" a "M es finitamente generado"? Observemos que decir que M sea finitamente generado es equivalente a decir que existe un $n \in \mathbb{N}$ y un

epimorfismo $\pi : A^n \to M$ (un sistema de generadores corresponde a tomar $\{\pi(e_1), \ldots, \pi(e_n)\}$). Si tomamos 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 M un A-módulo, son equivalentes:*

1. *M es finitamente generado.*
2. *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 $F \subset I$ un subconjunto finito tal que $f|_{\oplus_{i\in F} N_i} \bigoplus_{i\in F} N_i \to M$ es un epimorfismo.*

Demostración: 2.$\Rightarrow$ 1. es claro tomando el epimorfismo $A^{(M)} \to M$ ($e_m \mapsto m$). Extrayendo un subconjunto finito de índices se obtiene precisamente un subconjunto finito de generadores.

1.$\Rightarrow$ 2. Sea $f : \bigoplus_{i\in I} N_i \to M$ un epimorfismo, y sean $\{m_1, \ldots, m_r\}$ un sistema de generadores de M. Por cada m_k existe un $z^k = (z_i^k)_{i\in I} \in \bigoplus_{i\in I} N_i$ tal que $f((z_i^k)_{i\in I}) = \sum_{i\in I} f(z_i^k) = m_k$ ($k = 1, \ldots, r$). Ahora bien, como $z^k = (z_i^k)_{i\in I} \in \bigoplus_{i\in I} N_i \to M$, cada z^k es combinación lineal finita de elementos de N_i. Sea F la unión para $k = 1, \ldots, r$ de los índices $i \in I$ tales que los z_i^k son no nulos. Si tomamos ahora $f|_{\oplus_{i\in F} N_i} : \bigoplus_{i\in F} N_i \to M$, como los $z^k \in \oplus_{i\in F} N_i$ entonces los $m_k \in \mathrm{Im}(f|_{\oplus_{i\in F} N_i})$, y se tiene 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 dada una familia arbitraria de A-módulos $\{N_i\}_{i\in I}$ y un monomorfismo $f = \prod_{i\in I} f_i : M \to \prod_{i\in I} N_i$, entonces existe un subconjunto finito $F \subset I$ tal que $\prod_{i\in F} f_i : M \to \prod_{i\in F} N_i$ es un monomorfismo.*

Observamos que si M es un A-módulo finitamente cogenerado y $N \subset M$ es un submódulo, entonces N es finitamente cogenerado, pero cocientes de finitamente cogenerados no tienen por qué ser finitamente cogenerados.

Definición 4.3.3. *Se dice que un A-módulo M es* **artiniano** *si y sólo si todo cociente de M es finitamente cogenerado. El anillo A se dirá un anillo artiniano en caso de que A sea artiniano como A-módulo.*

Ejemplo: $\mathbb{Z}$ no es un $\mathbb{Z}$-módulo artiniano, porque dado $a \in \mathbb{Z}$, $a \neq 0, 1, -1$, 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, pues dado un $m \in \mathbb{Z}$ basta tomar un $n \in \mathbb{N}$ tal que $|m| < |a|^n$ para que su clase módulo $a^n.\mathbb{Z}$ sea distinta de cero. Sin embargo, para cualquier subconjunto finito $F \subset \mathbb{N}$, $\mathbb{Z} \to \prod_{n\in F} \mathbb{Z}/\langle a^n\rangle$ 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, $\cap_{i\in I} M_i = 0$ implica que existe un subconjunto finito $F \subset I$ con $\cap_{i\in F} M_i = 0$
(tomar $\prod \pi_i : M \to \prod_{i\in I} M/M_i$ y mirar los núcleos).

Recíprocamente, si M verifica 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:*

1. *M es artiniano.*
2. *(Condicion de cadena descendente.) Toda cadena decreciente de submódulos de M se estaciona.*
3. *Todo conjunto no vacío de submódulos de M tiene un elemento minimal.*

Demostración:

1.$\Rightarrow$ 2. Supongamos M artiniano y sea $\mathcal{C}$ una cadena decreciente $L_1 \supset L_2 \supset \dots$ de submódulos de M. Sea $K = \cap_{n\in\mathbb{N}} L_n$, 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 un $m \in \mathbb{N}$ tal que tal que $M/K \to \prod_{n<m} M/L_n$

es monomorfismo, por lo tanto $K = \cap_{n\in\mathbb{N}} L_n = \cap_{n<m} L_n = L_{m-1}$, es decir, a partir de L_{m-1} la cadena se estaciona.

2.$\Rightarrow$ 3. Supongamos que M verifica la condición de cadena descendente y sea $\mathcal{S}$ un subconjunto no vacío de submódulos de M. Supongamos que $\mathcal{S}$ no tiene elemento minimal, entonces $\forall L \in \mathcal{S}$ el conjunto $\{L' \in \mathcal{S} \ / \ L' \subset L$ (inclusión estricta)$\}$ es no vacío. Fijando L arbitrario, sea $L_0 = L$ y L_1 un elemento del conjunto anterior, como L_1 no es minimal, el conjunto $\{L'' \in \mathcal{S} \ / \ L'' \subset L_1$ (inclusión estricta)$\}$ es no vacío, sea L_2 un elemento de ese conjunto. Con este proceso se obtiene una cadena $L_0 \supset L_1 \supset L_2 \supset \dots$ que no se estaciona, lo cual es absurdo, luego $\mathcal{S}$ tiene algún elemento minimal.

3.$\Rightarrow$ 1. Supongamos que todo conjunto no vacío de submódulos de M tenga un submódulo minimal. Sea $K \subset M$ un submódulo y $f : M/K \to \prod_{i\in I} N_i$ un monomorfismo. Sea M_{i_0} el núcleo de la composición $M \to M/K \to \prod_{i\in I} N_i \to N_{i_0}$. Vale que $K = \cap_{i\in I} M_i$. Bastará probar entonces que si $K \subset M$ es un submódulo y $\mathcal{S}$ es una colección de submódulos de M con $K = \cap_{M'\in\mathcal{S}} M'$, entonces $K = \cap_{j=1}^{n} M'_j$ para algún número $n \in \mathbb{N}$ y elementos $M'_j \in \mathcal{S}$. Sea $\mathcal{P} = \{\cap_{M'\in F} M' : \ F \subset \mathcal{S}$ es un conjunto finito $\}$. Por la propiedad 3., $\mathcal{P}$ tiene un elemento minimal correspondiente a un F_0 y $K = \cap_{M'\in F_0} M'$.

Ejemplos:

1. $\mathbb{Z}_{p^\infty} \cong G_{p^\infty}$ es un $\mathbb{Z}$-módulo artiniano. Para ver esto, notamos que sus únicos submódulos son $\{1\}$, G_{p^∞} y los $(G_{p^n})_{n\in\mathbb{N}}$ que están todos "encajados", luego toda cadena descendente de submódulos se estaciona porque los G_{p^n} son finitos.

2. Si k es un cuerpo, V un k-espacio vectorial, 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 (por lo tanto un k-espacio vectorial). Si M es de dimensión finita sobre k entonces M es artiniano.

Una de las propiedades más importantes de los módulos noetherianos y/o artinianos es que admiten una descomposición en suma directa finita de submódulos indescomponibles, cosa que no es cierta si sólo se pide que el módulo sea finitamente generado. Un módulo se dice **indescomponible** si no admite sumandos directos propios.

Proposición 4.3.5. *Sea M un A-módulo noetheriano (o artiniano) no nulo. Entonces existen submódulos indescomponibles $M_1, \ldots, M_n$ tales que $M \cong \bigoplus_{i=1}^{n} M_i$.*

Demostración: Sea $M \neq 0$. Si M es indescomponible no hay nada que demostrar, si no, supongamos que M no verifica la propiedad del enunciado. Luego existe M' un sumando directo propio de M que no tiene una descomposición en suma directa finita de submódulos indescomponibles (un tal submódulo existe porque si no M la tendría). Como M' es un módulo no nulo noetheriano (es submódulo de un noetheriano) y no es suma directa finita de indescomponibles, entonces existe M'' un sumando directo propio de M' que no tiene una descomposición en suma directa finita de indescomponibles. Llamemos a N' al complemento de M'', i.e. $M = N' \bigoplus M'$, $M' = N'' \bigoplus M''$. Continuando con este proceso se consiguen cadenas de submódulos propios

$$M \supset M' \supset M'' \supset \ldots \qquad \text{y} \qquad N \subset N \oplus N' \subset N \oplus N' \oplus N'' \subset \ldots$$

que no se estacionan, con lo cual resulta que M no es noetheriano ni artiniano, lo que es absurdo.

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 esto 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 $t \circ f = Id_W$. 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, por lo tanto, habrá 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 "vuelta" 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 $\mathbb{Z}$ 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 $3{,}2 + (-2){,}3 = 0$) 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, $\{1\}$ (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. Si $A = M_2(k)$ y $M = \left\{ \begin{pmatrix} 0 & x \\ 0 & y \end{pmatrix} \in M_2(k) \right\}$. M es un A-módulo a izquierda, y el conjunto $\left\{ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right\}$ es un sistema de generadores minimal, que no es linealmente independiente. Probar que no existe ningun conjunto de generadores linealmente independiente.
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 $M = \mathbb{Q}$. Sea $0 \neq r \in \mathbb{Q}$, 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 (l.i.) no puede tener elementos de torsión. En el ejemplo 1., $\{1\}$ no sólo es l.i. sino que además genera.

Algunas de las propiedades que tienen los subconjuntos l.i. 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.*

1. *Si S es un conjunto l.d. entonces $f(S)$ es un conjunto l.d..*
2. *Si S es un conjunto l.i. y f es monomorfismo, entonces $f(S)$ es un conjunto l.i..*
3. *Si S es un conjunto de generadores y f es 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 l.i. y S genera M.

Definición 5.1.3. *Un A-módulo M se dice* **libre** *si y sólo 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 $\{1\}$.

3. $\mathbb{Q}$ no es un $\mathbb{Z}$-módulo libre ya que todo par de elementos es l.d. (y $\mathbb{Q}$ no es cíclico).

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 $p.v = 0 \ \forall \ v \in V$).

Observaciones:

1. Un cociente de un A-módulo libre M no tiene por qué ser libre, por ejemplo $\mathbb{Z}_n = \mathbb{Z}/n.\mathbb{Z}$ 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 tomemos $M = A = M_2(\mathbb{Z})$, que es A-libre con base $\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\}$. Sin embargo, $N = \left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}, a, b \in \mathbb{Z}\right\}$ es un submódulo de torsión de M, por lo tanto no puede tener una base como A-módulo.

3. Sean M y N A-módulos. Si M es un A-módulo libre y $f : M \to N$ es un isomorfismo entonces N es libre.

4. Sea $A^{(I)} = \{f : I \to A \ / \ sop(f) < \infty\}$. $A^{(I)}$ 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 $e_i(j) = \delta_{ij}$.

A continuación caracterizaremos los A-módulos libres, viendo que todo A-módulo libre es isomorfo a un módulo del tipo $A^{(I)}$, para algún conjunto I.

Proposición 5.1.4. *Dado un A-módulo M las siguientes afirmaciones son equivalentes:*

1. *M es un A-módulo libre con base $\{x_i\}_{i\in I}$.*
2. *Sea $\rho_i : A \to M$ $(a \mapsto a.x_i)$, entonces $\rho := \oplus_{i\in I}\rho_i : A^{(I)} \to M$ es un isomorfismo.*
3. *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: 1.⇒ 2. Sea $z \in A^{(I)}$ tal que $\rho(z) = 0$. Escribamos $z = \sum_{i\in I} a_i.e_i$ (donde la familia $(a_i)_{i\in I} \subset A$ es una familia con soporte finito). Entonces $0 = \rho(z) = \sum_{i\in I} a_i.x_i$. Como los x_i son independientes, los a_i deben ser todos cero, luego $z = 0$ y consecuentemente ρ es un monomorfismo. Por otro lado $\rho(e_i) = x_i$, por lo tanto la imagen de ρ contiene a un conjunto de generadores con lo que ρ resulta también un epimorfismo, luego un isomorfismo.

2.⇒ 3. 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 ya definido su valor en los x_i y éstos generan. 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 ($\sum_{i\in I} a_i.x_i = \sum_{i\in I} a'_i.x_i$ $\Rightarrow \sum_{i\in I}(a_i - a'_i).x_i = 0 \Rightarrow a_i - a'_i = 0 \forall\ i \in I$), 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.

3.⇒ 1. Veremos que si M verifica 3., entonces $M \cong A^{(I)}$. Sean $N = A^{(I)}$ e $y_i = e_i$ para todo $i \in I$. Entonces existe (un único) $f : M \to A^{(I)}$ tal que $f(x_i) = e_i$. Consideremos $\rho \circ f : M \to M$. Como $\rho \circ f(x_i) = x_i$, es claro que el morfismo $\rho \circ f$ coincide con Id_M en los x_i, luego, (eligiendo $N = M$ e $y'_i = x_i$) por unicidad, $\rho \circ f = Id_M$. Para la composición $f \circ \rho$ se tiene $f \circ \rho(\sum_{i\in I} a_i.e_i) = f(\sum_{i\in I} a_i.x_i) = \sum_{i\in I} a_i.f(x_i) = \sum_{i\in I} a_i.e_i$, por lo tanto $f \circ \rho = Id_{A^{(I)}}$ que es libre de base $\{e_i\}$, además resulta que ρ es también un isomorfismo, por lo tanto $\{f(e_i)\}_{i\in I} = \{x_i\}_{i\in I}$ es una base de M.

Corolario 5.1.5. *Con las notaciones de la proposición anterior, se verifica:*

1. *Si $\{y_i\}_{i\in I}$ es una base de N, entonces f es un isomorfismo.*

2. Dos A-módulos con bases de igual cardinal son isomorfos.

Las demostraciones son inmediatas, se dejan como ejercicio.

Observación: Si $(M_j)_{j\in J}$ es una familia de A-módulos libres, entonces $\oplus_{j\in J} M_j$ es un A-módulo libre. Mas aún, si $\{x_i^j\}_{i\in I_j}$ es una base de M_j $(j \in J)$, entonces $\cup_{j\in J}\{x_i^j\}_{i\in I_j}$ es una base de $\bigoplus_{j\in J} M_j$.

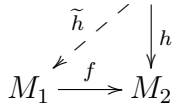
Vimos que la propiedad de "ser libre" no es estable en general ni por cocientes ni por subespacios. Veremos ahora sin embargo que todo módulo es cociente de un libre:

Proposición 5.1.6. *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 de M (por ejemplo $\{m\}_{m\in M}$) y sea $L := A^{(I)}$. L es un A-módulo libre, y $h : A^{(I)} \to M$, definido por $h(e_i) = x_i$ es un epimorfismo pues la imagen contiene a un sistema de generadores. Se tiene además $M \cong L/\operatorname{Ker}(h)$, $\operatorname{Ker}(h)$ suele llamarse el núcleo de relaciones de M.

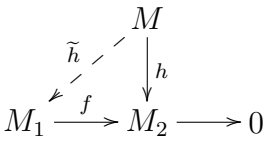
Observemos que si M es un A-módulo libre y $f : N \to M$ un epimorfismo, entonces existe una sección $g : M \to N$ tal que $f \circ g = Id_M$. En efecto, dada una base $\{x_i\}_{i\in I}$ de M, existen $n_i \in N$ tales que $f(n_i) = x_i$ ya que f es un epimorfismo. Se define entonces $g(x_i) = n_i$ y se extiende por linealidad. Es decir, todo epimorfismo con imagen en un módulo libre M es una retracción.

De manera análoga, puede probarse que los módulos libres verifican una propiedad de "levantamiento" de morfismos. Consideremos el siguiente diagrama de flechas llenas:



¿Existe entonces un $\widetilde{h}$ morfismo en la dirección de la flecha punteada que haga el diagrama conmutativo, i.e. que $f \circ \widetilde{h} = h$? En principio, de levantarse h a un morfismo $\widetilde{h}$ debería valer que $\operatorname{Im}(h) = \operatorname{Im}(f \circ \widetilde{h}) \subseteq \operatorname{Im}(f)$, restringiéndonos entonces al submódulo $\operatorname{Im}(f)$, para plantear correctamente el problema supondremos que f es un epimorfismo.

Proposición 5.1.7. *Sea M un A-módulo libre. Entonces M resuelve el siguiente problema de tipo universal, esquematizado a partir del 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 (no necesariamente único) $\widetilde{h} : M \to M_1$ 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 $h(x_i) = f(m_i)$. Se define pues $\widetilde{h}(x_i) := m_i$ y se extiende por linealidad. Como $f(\widetilde{h}(x_i)) = f(m_i) = h(x_i)$ entonces $f \circ \widetilde{h} = h$ (coinciden en una base).

Observamos que la propiedad de que todo epimorfismo con imagen en un libre es una retracción puede obtenerse como consecuencia de la proposición anterior poniendo $M_2 = M$ y $h = Id_M$.

Corolario 5.1.8. *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 $0 \to S \to^i M \to^\pi M/S \to 0$ se parte. Pero como M/S es libre, $\pi : M \to M/S$ es una retracción, es decir, admite una sección $s : M/S \to M$ tal que $\pi \circ s = Id_M/S$, por lo tanto i es una sección y S es un sumando directo cuyo proyector correspondiente es $p = Id_M - s \circ \pi$.

Supongamos que A es un anillo tal que todo submódulo de un A-módulo libre es libre, en particular todo ideal de A resultará libre. A conticuación probaremos que esta afirmación sobre los ideales de A, que en principio parece más débil, resulta sin embargo equivalente a la primera:

Teorema 5.1.9. *Sea A un anillo, son equivalentes:*

- *Todo submódulo de un A-módulo libre es libre.*
- *Todo ideal de A es A-libre.*

Nombre: Un anillo tal que todo submódulo de un libre es libre se denomina **hiperhereditario**.

Demostración: Una de las implicaciones es obvia, supongamos ahora que todo ideal de A es libre. Sea $M \neq 0$ un A-módulo libre con base $\{x_i\}_{i\in I}$ y S un submódulo. Por el lema de Zorn, podemos suponer que I ($I \neq \emptyset$) 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 $F_i := \{x \in M \ / x$ es combinación lineal de los x_j con $j < i\}$ y $\overline{F}_i := \{x \in M \ / x$ es combinación lineal de los x_j con $j \leq i\}$. Si $i < k$, resulta que $\overline{F}_i \subset \overline{F}_k$ y además $M = \cup_{i\in I}\overline{F}_i$. Dado $x \in S$, existe i tal que $x \in S \cap \overline{F}_i$, luego existen únicos $a_x \in A$ y $x' \in S \cap F_i$ tal que $x = x' + a_x.x_i$.

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 y por lo tanto 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, entonces $S \cap F_i$ es un sumando directo de $S \cap \overline{F}_i$. Esto es equivalente a que exista un submódulo $C_i \subset M$ tal que $S \cap \overline{F}_i = S \cap F_i \oplus C_i$; queremos ver que $S = \oplus_{i\in I} C_i$, luego S será 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 $\oplus_{i\in I} C_i = S$.

Supongamos que no, y sea $H = \{j \in I \ / \ \exists\ x \in S \cap \overline{F}_j$ con $x \notin \oplus_{i\in I} C_i\}$. Sea j_0 el primer elemento de J (existe por el buen orden y porque $H \neq \emptyset$). Sea $z \in S \cap \overline{F}_{j_0}$ tal que $z \notin \oplus_{i\in I} C_i$, entonces existe un único $z' \in S \cap F_{j_0}$ y un único $a \in A$ tal que $z = z' + a.x_{j_0}$. Como j_0 es el primer elemento de H, z' es necesariamente una combinación lineal de x_k con $k < j_0$, luego $z' \in \oplus_{i\in I} C_i$, y por lo tanto $z \in \oplus_{i\in I} C_i$, lo que es absurdo. En consecuencia $S = \oplus_{i\in I} C_i$.

Corolario 5.1.10. *Sea A un dip, es decir, un dominio íntegro tal que todo ideal es principal. Entonces todo submódulo de un 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, $\exists\ a \in A$ tal que $I = \langle a \rangle$. Como A es íntegro $\{a\}$ es linealmente independiente ($a \neq 0$, luego $b.a = 0 \Rightarrow b = 0$) por lo tanto $\{a\}$ es una base, es decir 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.

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 todo $k[x]$-submódulo de un $k[x]$-módulo libre (k cuerpo) es $k[x]$-libre. Lo mismo sucede con los anillos $k[x, x^{-}1]$ y $k[[x]]$.

5.1.1. Noción de rango

Definición 5.1.11. *Sea A un anillo, diremos que A tiene* **noción de rango** *si: $A^{(I)} \cong A^{(J)}$ implica $\#I = \#J$.*

Ejemplo: Si A es un cuerpo, o más generalmente si A es un anillo de división, entonces A tiene noción de rango.

La siguiente proposición da otros ejemplos de anillos con noción de rango.

Proposición 5.1.12. *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 $g : L \to A^{(J)}$ un isomorfismo, se tiene que $\{g(x_i)\}_{i\in I}$ es una base de $A^{(J)}$. Sea $\{e_j\}_{j\in J}$ 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 $h = f^{(J)} : A^{(J)} \to D^{(J)}$, que sobre la base canónica resulta $h(e_k) = \{f(\delta_{jk})\}_{j\in J} = \{\delta_{jk}\}_{j\in J}$, es decir que da la base canónica de $D^{(J)}$. Como

$$h(e_k) = h\left(\sum_{i\in I} a_{ik} g(x_i)\right) = \sum_{i\in I} a_{ik} hg(x_i)$$

obtenemos que $\{hg(x_i)\}_{i\in I}$ genera $D^{(J)}$ sobre D, por lo tanto $\#I \geq \#J$. La otra desigualdad es análoga, luego $\#I = \#J$.

Corolario 5.1.13. *Si A es un anillo conmutativo, entonces A tiene noción de rango.*

Demostración: A admite algun ideal maximal $\mathcal{M}$, consideramos entonces $A \to A/\mathcal{M}$.

Proposición 5.1.14. *Sea A un anillo con noción de rango, $M = \oplus_{i\in I} M_i$ un A-módulo tal que todos los A-módulos M_i son libres, entonces M es libre y $rg(M) = \sum_{i\in I} rg(M_i)$.*

Demostración: Si $\{x_{i_j}\}_{j\in J_i}$ es una base de M_i, entonces es claro que $\{x_{i_j} : i \in I,\ j \in J_i\}$ es una base de M.

Proposición 5.1.15. *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 $rg(M) \leq n$.*

Demostración: Sea $\{x_1, \ldots, x_n\}$ una base de L, sea $M_i = M \cap \langle x_1, \ldots, x_i\rangle$. 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 $rg(M_1) = 1$, en todo caso $rg(M_1) \leq 1$. Veamos inductivamente que para todo r, $rg(M_r) \leq r$.

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 verifica 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 $a_{r+1} = 0$ entonces $M_{r+1} = M_r$ y por lo tanto $rg(M_{r+1}) \leq r < r+1$. Si no, dado $x \in M_{r+1}$ escribimos $x = \sum_{i=1}^{r+1} c_i x_i$, el coeficiente c_{r+1} resulta entonces divisible por a_{r+1}, luego 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, por lo tanto $rg(M_{r+1}) = rg(M_r) + 1 \leq r + 1$.

Ejercicio: Sea G un grupo y consideremos el anillo de grupo $\mathbb{Z}[G]$. Se define el morfismo $\epsilon : \mathbb{Z}[G] \to \mathbb{Z}$ a través de $g \mapsto 1\ \forall\ g \in G$.

1. Probar que ϵ es un morfismo de anillos.
2. Probar que $\mathrm{Ker}(\epsilon)$ está generado por $\{(g-1)\}_{g\in G}$.
3. Probar que si $\{g_i\}_{i\in I}$ es un sistema de generadores de G (generadores como grupo), entonces $\{(g_i - 1)\}_{i\in I}$ es un sistema de generadores de $\mathrm{Ker}(\epsilon)$.
4. Sea G un grupo libre con generadores $\{g_i\}_{i\in I}$, probar entonces que el morfismo
$$\begin{aligned} \mathbb{Z}[G]^{(I)} &\to \mathrm{Ker}(\epsilon) \\ \sum_{i\in I} \lambda_i e_i &\mapsto \sum_{i\in I} \lambda_i (g_i - 1) \end{aligned}$$
es un isomorfismo.

Este ejercicio muestra que existen anillos en donde hay módulos libres de "rango" uno (e.g. $\mathbb{Z}[G]$ con G grupo libre) que tienen submódulos libres de rango mayor que uno.

5.2. El funtor Hom

Dados M y N dos A-módulos a izquierda, consideremos el conjunto $\mathrm{Hom}_A(M,N) = \{f : M \to N : f(m+m') = f(m) + f(m') \text{ y } f(a.m) = a.f(m) \ \forall\ m, m' \in M,\ a \in A\}$, que es un grupo abeliano, sumando punto a punto (i.e. es un subgrupo de M^N).

En el caso de espacios vectoriales, si k es un cuerpo, V un k-espacio vectorial de dimensión n y W un k-espacio vectorial de dimensión m, entonces uno sabe que $\mathrm{Hom}_k(V,W)$, además de ser un grupo abeliano, en realidad es un espacio vectorial de dimensión $n.m$. Volviendo al 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 $\mathrm{End}_A(M)^{op}$ y $C = \mathrm{End}_A(N)^{op}$. 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). Analogamente N es un A-C-bimódulo.

Como la composición de morfismos A-lineales es un morfismo A-lineal, tenemos que la aplicación

$$\begin{aligned}\mathrm{End}_A(M) \times \mathrm{Hom}_A(M,N) \times \mathrm{End}_A(N) &\to \mathrm{Hom}_A(M,N)\\ (f,g,h) &\mapsto f \circ g \circ h\end{aligned}$$

provee a $\mathrm{Hom}_A(M,N)$ de una estructura de $\mathrm{End}_A(M)$-$\mathrm{End}_A(N)$-bimódulo.

Supongamos en general que M no sólo es un A-módulo sino que existe un anillo B tal que M es un A-B-bimódulo. Y 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 ${}_AN_C$.

Se afirma entonces que $\mathrm{Hom}_A(M,N)$ admite una estructura de B-C-bimódulo, definiendo, para $b \in B$, $c \in C$ y $f \in \mathrm{Hom}_A(M,N)$:

$(b.f) : M \to N$ por: $(b.f)(m) = f(m.b)$

$(f.c) : M \to N$ por: $(f.c)(m) = f(m).c$

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, como se sabía de antes, $\mathrm{Hom}_A({}_AM_{\mathbb{Z}},{}_A N_{\mathbb{Z}})$ tiene una estructura de $(\mathbb{Z}-\mathbb{Z})$-bimódulo, es decir, de grupo abeliano (la misma de antes).

2. Si A es conmutativo, sabemos que a todo A-módulo M puede considerárselo como un A-A-bimódulo "simétrico", definiendo $m.a := a.m$. Entonces $\mathrm{Hom}_A({}_AM_A,{}_A N_A)$ tiene una estructura de A-A-bimódulo. Notar que la acción de A sobre el $\mathrm{Hom}_A(M,N)$ puede calcularse de cualquiera de las siguientes maneras:

$$(a.f)(m) = f(m.a) = f(a.m) = a.(f(m)) = f(m).a = (f.a)(m)$$

   es decir, $\mathrm{Hom}_A(M,N)$ 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 $M^* := \mathrm{Hom}_A({}_AM_{\mathbb{Z}},{}_A A_A)$ es un $\mathbb{Z}-A$-bimódulo, es decir, un A-módulo a derecha. La estructura está dada por $(f.a)(m) = f(m).a$ (donde $f \in M^*,\ a \in A,\ m \in M$).

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:

$$\begin{aligned} k^G &\to \mathrm{Hom}_k(k[G],k) \\ f &\mapsto \left(\sum_{g\in G} \lambda_g.g \mapsto \sum_{g\in G} \lambda_g f(g)\right) \end{aligned}$$

En particular, $k[x]^* \cong k[|x|]$.

Sea ahora ${}_AM_B$ un A-B-bimódulo fijo y consideremos el funtor:

$$\begin{aligned} \mathrm{Hom}_A({}_AM_B,-) : {}_A\mathrm{Mod}_C &\to {}_B\mathrm{Mod}_C \\ {}_AN_C &\mapsto \mathrm{Hom}_A(M,N) \end{aligned}$$

y si $f :_A N_C \to_A N'_C$ es un morfismo de A-C-bimódulos, definimos

$$\begin{aligned}\mathrm{Hom}_A(M,f) := f_* : \mathrm{Hom}_A(M,N) &\to \mathrm{Hom}_A(M,N')\\ g &\mapsto f\circ g\end{aligned}$$

Dejamos como ejercicio la verificación de las siguientes propiedades:

1. $(f\circ f')_* = f_*\circ f'_*$.
2. $(Id_N)_* = Id_{\mathrm{Hom}_A(M,N)}$.
3. $(f+f')_* = f_* + f'_*$.
4. $f_*(b.g) = b.f_*(g)$ $(b\in B)$.
5. $f_*(g.c) = f_*(g).c$ $(c\in C)$.

Ejemplos:

1. Si $M = A$, $\mathrm{Hom}_A(A,-)$ es naturalmente isomorfo al funtor identidad, a través de
$$\begin{aligned}\mathrm{Hom}_A(M,N) &\cong N\\ \phi &\mapsto \phi(1)\end{aligned}$$
2. Si $M = A^{(I)}$, $\mathrm{Hom}_A(M,N) = \mathrm{Hom}_A(A^{(I)},N) \cong \mathrm{Hom}_A(A,N)^I \cong N^I$.
3. Si $A = B = C = \mathbb{Z}$, $M = \mathbb{Z}_n$, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n,N) \cong \{x\in N \ / n.x = 0\}$ 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 paricular 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 5.2.1. *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. También sabemos que $g_* \circ f_* = (g \circ f)_* = 0_* = 0$, por lo tanto sólo falta ver que f_* es monomorfismo y que $\mathrm{Ker}(g_*) \subseteq \mathrm{Im}(f_*)$.

Nota: ¿Por qué 0_* es el morfismo nulo? 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.

Este resultado, admite la siguiente recíproca:

Lema 5.2.2. *Sea A un anillo cualquiera, M, N, T tres A-módulos. Entonces*

1. *La sucesión $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T$ es una sucesión 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.

2. *La sucesión $M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$ es una sucesión 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 el punto 1. 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 (notar 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.

El punto 2. 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 también que $f^* \circ g^* = 0$, pero entonces $(g \circ f)^* = f^* \circ g^* = 0$ para todo A-módulo R, o sea que si $h : R \to T$ es un morfismo cualquiera, resulta que $h \circ g \circ f : M \to T$ es el morfismo cero. Si tomamos $R = T$ y $h = Id_T$ obtenemos que $g \circ f$ es cero y por lo tanto $\mathrm{Im}(f) \subset \mathrm{Ker}(g)$. Veamos por último la inclusión al inversa.

Tomando $R = N/\mathrm{Im}(f)$, tenemos la sucesión exacta

$$0 \to \mathrm{Hom}_A(T, N/\mathrm{Im}(f)) \to \mathrm{Hom}_A(N, N/\mathrm{Im}(f)) \to \mathrm{Hom}_A(M, N/\mathrm{Im}(f))$$

y consideremos el morfismo $\pi : N \to N/\mathrm{Im}(f)$ (la proyección canónica al cociente). Claramente $f^*(\pi) = \pi \circ f = 0$, o sea 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 $\mathrm{Ker}(g) \subset \mathrm{Im}(f)$ pues si $n \in N$, $n \in \mathrm{Im}(f)$ si y sólo si $\pi(n) = 0$, y a partir de la fórmula $\pi = h \circ g$ se tiene que si $n \in \mathrm{Ker}(g)$ entonces $n \in \mathrm{Ker}(\pi) = \mathrm{Im}(f)$.

Ejemplo: Uno se podría preguntar, dado un epimorfismo de A-módulos $f : Y \to Z$, un módulo cualquiera M, si el morfismo $f_* : \mathrm{Hom}_A(M, Y) \to \mathrm{Hom}_A(M, Z)$ es también un epimorfismo. Esto no tiene por qué suceder en general, consideremos el siguiente ejemplo: $A = Y = \mathbb{Z}$, $M = Z = \mathbb{Z}_n$, $f = \pi : \mathbb{Z} \to \mathbb{Z}_n$ 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, asi que trivialmente preserva epimorfismos. Otro ejemplo es cuando M es libre.

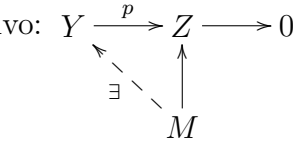
Ejercicio: Si $M \cong A^{(I)}$ para algún conjunto I, y si $f : X \to Y$ es un epimorfismo de A-módulos, entonces $f_* : \mathrm{Hom}_A(M, Y) \to \mathrm{Hom}_A(M, Z)$ es también un epimorfismo.

5.3. Módulos proyectivos

El objetivo de esta sección es estudiar los módulos M que son tales que el funtor $\mathrm{Hom}_A(M, -)$ es exacto. Comenzamos con una definición:

Definición 5.3.1. *Un A-módulo M se llama 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, si y sólo si, dado el siguiente diagrama de flechas llenas de A-módulos se puede completar, (de manera no necesariamente única) con la flecha punteada, de modo tal que el diagrama completo sea conmutativo:



Observaciones:

1. Vimos en la sección anterior que todo A-módulo libre es proyectivo.

2. Los cocientes de módulos proyectivos no son necesariamente proyectivos (considerar como 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: tomar $A = M = \mathbb{Z}$, $S = \{1, 2, 4, 8, \ldots, 2^n, \ldots\}$ considerar la proyección canónica $\mathbb{Z} \to \mathbb{Z}_3$. Se tiene que $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_S, \mathbb{Z}) = 0$ pero el morfismo

   $$\begin{aligned} \mathbb{Z}_S &\to \mathbb{Z}_3 \\ \frac{n}{2^n} &\mapsto \overline{n,2^n} \end{aligned}$$

   está bien definido (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 5.3.2. *Dado un A-módulo M, las siguientes afirmaciones son equivalentes:*

1. *M es un A-módulo proyectivo.*
2. *Toda sucesión exacta corta de A módulos del tipo $0 \to X \to Y \to M \to 0$ se parte.*
3. *M es sumando directo de un A-módulo libre.*

Demostración: $1 \Rightarrow 2$. Si M es A-proyectivo, dada una sucesión exacta

$$0 \to X \to Y \to M \to 0$$

se considera el 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 $p \circ \overline{id} = Id_M$ se debe a la proyectividad de M, luego la sucesión se parte.

$2 \Rightarrow 3$. Dado M, sabemos que existe un conjunto I y un epimorfismo $\pi : A^{(I)} \to M$. Consideremos la sucesión exacta corta

$$0 \to \mathrm{Ker}(\pi) \to A^{(I)} \to M \to 0$$

Por hipótesis esta sucesión exacta se parte, es decir existe $i : M \to A^{(I)}$ tal que $\pi \circ i = Id_M$, por lo tanto M es un sumando directo de $A^{(I)}$.

$3 \Rightarrow 1$. 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 $g : M \to Y$, llamamos $i : M \to A^{(I)}$ la inclusión y $\pi : A^{(I)} \to M$ la proyección. Se quiere ver que existe algún $\overline{g} : M \to X$ tal que $f\overline{g} = g$. El diagrama de rigor es el siguiente:

$$\begin{array}{ccccc} X & \xrightarrow{f} & Y & \longrightarrow & 0 \\ & \nwarrow^{\overline{g\pi}} & \uparrow g & & \\ & & M & & \\ & & \uparrow \pi & & \\ & & A^{(I)} & & \end{array}$$

Definimos $\overline{g} : M \to X$ por $\overline{g} = \overline{g\pi}i$. Es claro que es morfismo de A-módulos, además

$$f\overline{g} = f(\overline{g\pi}i) = (f\overline{g\pi})i = (g\pi)i = g(\pi i) = gId_M = g$$

Por lo tanto M es proyectivo.

Observación: Si M es finitamente generado, puede elegirse siempre un epimorfismo $A^{(I)} \to M$ con I finito, digamos $\#I = n$, y si además M es proyectivo, existe $n \in \mathbb{N}$ tal que M es sumando directo de A^n.

Corolario 5.3.3. *Dada una familia de A-módulos $(M_i)_{i\in I}$ se verifica:*

1. *$\oplus_{i\in I} M_i$ es proyectivo si y sólo si cada M_i es proyectivo.*
2. *Si $\prod_{i\in I} M_i$ es proyectivo entonces cada M_i es proyectivo. La recíproca no es necesariamente cierta.*

Demostración: 1. Sea $f : X \to Y$ un epimorfismo y consideremos el cuadrado conmutativo:

$$\begin{array}{ccc} \mathrm{Hom}_A(\oplus_{i\in I} M_i, X) & \xrightarrow{f_*} & \mathrm{Hom}_A(\oplus_{i\in I} M_i, Y) \\ \| & & \| \\ \prod_{i\in I} \mathrm{Hom}_A(M_i, X) & \xrightarrow{\prod f_*^i} & \prod_{i\in I} \mathrm{Hom}_A(M_i, Y) \end{array}$$

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, lo que demuestra 1.

2. Dado $P = \prod_{i\in I} M_i$ y M_{i_0} se considera $Q = \{(m_i)_{i\in I} \in \prod_{i\in I} M_i \,/\, m_{i0} = 0\}$. Tenemos entonces que $P = Q \oplus M_{i_0}$, y por el punto 1., dado que P es proyectivo resulta que M_{i_0} es proyectivo.

5.3.1. Anillos hereditarios

Vimos ejemplos de módulos proyectivos con submódulos no proyectivos (por ejemplo $2\mathbb{Z}_4 \subset \mathbb{Z}_4$ no es un $\mathbb{Z}_4$-módulo proyectivo).

Definición 5.3.4. *Una anillo A se dice* **hereditario** *si y sólo si todo submódulo de un A-módulo proyectivo es proyectivo.*

El siguiente teorema describe los submódulos de módulos libres en anillos hereditarios.

Teorema 5.3.5. *(Kaplansky) Sea A un anillo hereditario, L un A-módulo libre y $S \subseteq L$ un submódulo. Entonces si $L = \oplus_{i\in I} A.x_i$, existe una familia $\{\mathcal{A}_i\}_{i\in I}$ de ideales de A tales que $S \cong \oplus_{i\in I}\mathcal{A}_i$.*

Demostración: sea $\{x_i\}_{i\in I}$ una base de L, podemos suponer que I es bien ordenado y no vacío, con orden $\leq$. Dado $i \in I$, sean $L'_i = \langle x_j \ : \ j \leq i\rangle$ y $L_i = \langle x_j \ : \ j < i\rangle$, entonces $L'_i = L_i \oplus \langle x_i\rangle$. Se definen morfismos $f_i : L'_i \to A$ por $f_i(y + ax_i) = a$ donde $y \in L'_i$, $a \in A$. Los f_i resultan retracciones de las inclusiones $A \cong \langle x_i\rangle \hookrightarrow L'_i$, y $\mathrm{Ker}(f_i) = L_i$. Sea $\mathcal{A}_i = f_i(S\cap L'_i)$, entonces $g_i := f_i|_{S\cap L'_i} : S \cap L'_i \to \mathcal{A}_i$ es epi. Como $\mathcal{A}_i$ es proyectivo (pues A es hereditario), entonces 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 $S \cong \oplus_{i\in I} A_i$, lo que se realizará en dos partes:

- $S = \sum_{i\in I}\mathcal{A}_i$:

  $L = \cup_{i\in I} L'_i$, por lo tanto, para todo $x \in L$, existen $\{a_i\}_{i\in I} \subset A$ tal que $x = \sum_{i\in I} a_i x_i$. Si $x \neq 0$, sea $j = max(sop\{a_i\})$ (que existe porque $sop(\{a_i\})$ es un conjunto finito), luego $x \in L'_j$. Si $S \neq \sum_{i\in I} T_i$, sea $\mathcal{C} = \{i \in I \ / \ S \cap L'_i - \sum_{j\in I} T_j \neq \emptyset\}$, que resulta no vacío. Sea $j_0 = min(\mathcal{C})$ (que existe por buena ordenación) y sea $x \in S\cap L'_{j_0} - \sum_{j\in I} T_j$. Se puede escribir $x = y + z$ con $y \in S \cap L_{j_0}$ y $z \in T_{j_0}$, entonces $y \notin \sum_{i\in I} T_i$ e $y \in L'_k$ para algún $k < j_0$, es decir $y \in S \cap L'_k - \sum_{i\in I} T_i$, lo que contradice la minimalidad de j_0.

- La suma es directa:

  Sea $\sum_{i\in I} t_i = 0$, con $t_i \in T_i$, 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 $\langle x_j\rangle$ esta en suma directa con L_j, luego $t_j = -\sum_{i<j} t_i$ implica $t_j = 0$.

Corolario 5.3.6. *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 A-libre. La suficiencia se ve 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 $P' \subset P$ es un submódulo, sea L libre tal que P es sumando directo de L. Luego

P' resulta 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 $\mathcal{A}_i$ son proyectivos, luego P' es proyectivo.

Recordando la noción de hiperhereditario y el Teorema 5.1.9, tenemos el siguiente corolario:

Corolario 5.3.7. *Dado un anillo A, son equivalentes:*

1. *A es hiperhereditario (i.e. todo submódulo de un libre es libre).*
2. *A es hereditario y todo A-módulo proyectivo es libre.*
3. *Todo ideal de A es un A-módulo libre.*

Observaciones:

1. Si A es un dominio íntegro y principal, entonces A es hiperhereditario.
2. Conmutativo + hiperhereditario $\Rightarrow$ principal. En efecto, si A es conmutativo e hiperhereditario, sea I un ideal de A. Dados dos elementos a, b en I, nunca pueden ser linealmente independientes pues $a.b + (-b).a = 0$, luego la cantidad máxima de elementos de una base de I es uno, es decir, I es principal.
3. Si A es un dominio íntegro, A es principal si y sólo si es hiperhereditario.

5.3.2. Módulos proyectivos en dominios principales

Durante esta subsección A denotará un dominio íntegro de ideales principales (dip).

Recordamos que si M es un A-módulo, entonces la torsión de M es un A-submódulo, donde la torsión estaba definida por $t(M) = \{m \in M \ / \ \exists \ a \in A, \ a \neq 0 \text{ con } a.m = 0\}$.

Proposición 5.3.8. *Sea M un A-módulo finitamente generado, son equivalentes:*

1. *M es libre.*
2. *M es proyectivo.*

3. $t(M) = 0$.

Demostración: es claro que $1 \Rightarrow 2$. Más aún, al ser A un dip es hiperhereditario, luego 1. y 2. son equivalentes. Veremos $1 \Leftrightarrow 3$.

$1 \Rightarrow 3$. Como M es libre finitamente generado, entonces $M \cong A^n$ para algún numero natural n. Si $m = (a_1, \ldots, a_n)$ y $a \neq 0$ es tal que $a.m = 0$, entonces $0 = (a.a_1, \ldots, a.a_n)$, es decir que $a.a_i = 0$ para todo $i = 1, \ldots, n$. Por ser A íntegro y $a \neq 0$ se concluye que $a_i = 0 \ \forall \ i = 1, \ldots, n$.

$3 \Rightarrow 1$. Sea M sin torsión y consideremos K al cuerpo de fracciones de A. Necesitaremos el siguiente Lema:

Lema 5.3.9. *Sea K el cuerpo de fracciones de A y $M \subset K$ un A-submódulo de tipo finito. Entonces existe $x \in K$ tal que $M = A.x$.*

Demostración: Sea $M = \langle x_1, \ldots, x_n \rangle$, como $M \subset K$ existen $p_1, \ldots, p_n, q_1, \ldots, q_n \in A$ con los $q_i \neq 0$ tales que $x_i = \frac{p_i}{q_i}$, $i = 1, \ldots, n$.

Sea $q = \prod_{i=1}^{n} q_i$, que por integridad es distinto de cero. Como para todo $j = 1, \ldots, n$, $q.x_j \in A$, se sigue que $q.M$ es un submódulo de A, es decir un ideal, y entonces es principal. Luego existe $t \in A$ tal que $q.M = t.A$, es decir $M = \frac{t}{q}A$.

Volviendo a la demostración de $3 \Rightarrow 1$., sea $j_M : M \to M_K$ el morfismo canónico de localización:

$$\begin{aligned} j_M : M &\to M_K \\ m &\mapsto \frac{m}{1} \end{aligned}$$

Sabemos que $\mathrm{Ker}(j_M) = t(M) = 0$, luego j_M es inyectiva y 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 $M \to M_K \to K$ es distinta de cero; llamemos p a esta composición, y consideremos la sucesión exacta corta

$$0 \to \mathrm{Ker}(p) \to M \to p(M) \to 0$$

Ahora bien, 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 $p(M) \cong A$, luego tenemos que la sucesión anterior se parte, dando $M \cong \mathrm{Ker}(p) \oplus A$. Llamando $M_1 :=$

$\mathrm{Ker}(p)$, tenemos que M_1 es un submódulo de M, por lo tanto es sin torsión, además es isomorfo a un cociente de M, por lo tanto es finitamente generado, y se está de nuevo en las mismas hipótesis. Podemos entonces repetir la construcción para M_1 y descomponerlo como $M_1 \cong M_2 \oplus A$ (luego $M \cong (M_2 \oplus A) \oplus A$). De esta manera obtenemos una cadena creciente de submódulos, cada uno isomorfo a A, $A \oplus A$, $A \oplus A \oplus A, \ldots$, y por noetherianidad de M esta cadena se estaciona, luego $M \cong A^n$ para algún $n \in \mathbb{N}$.

Observación: De la demostración de la Proposición 5.3.8 se sigue que si M es finitamente generado, entonces

$$\mathrm{Hom}_A(M, K) \neq 0 \Leftrightarrow M_K \neq 0 \Leftrightarrow M/t(M) \neq 0 \Leftrightarrow M \neq t(M)$$

Corolario 5.3.10. *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

$$0 \to t(M) \to M \to M/t(M) \to 0$$

Como $t(M/t(M)) = 0$ se sigue que $M/t(M)$ es libre, 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, entonces es isomorfo a A^n para algún $n \in \mathbb{N}_0$, pero $n = dim_K((M/t(M))_K) = dim_K(M_K)$, luego está unívocamente determinado.

Ejercicios:

1. Sea A un dip, y M un A-módulo de tipo finito, se define $rg(M) := rg(M/t(M))$.
   - *a)* M, N de tipo finito, entonces $rg(M \oplus N) = rg(M) + rg(N)$.
   - *b)* Más en general, si $0 \to M \to N \to T \to 0$ es una sucesión exacta de módulos de tipo finito, entonces $rg(N) = rg(M) + rg(T)$.
   - *c)* Sea k el cuerpo de fracciones de A y M un A-módulo de tipo finito, entonces $rg(M) = dim_k(\mathrm{Hom}_A(M, k))$.
   - *d)* Ver que $rg(M) = rg(M^{*_A})$ (M es como siempre un A-módulo de tipo finito).
2. Sea A un dip, M un módulo de tipo finito y T un submódulo tal que M/T es sin torsión. Entonces M es libre si y sólo si T es libre.

5.4. Módulos inyectivos

Así como la noción de módulo proyectivo está relacionada con las propiedades del funtor $\mathrm{Hom}_A(P, -)$, la de módulo inyectivo concierne al funtor $\mathrm{Hom}_A(-, I)$.

Dado M un A-módulo, recordemos que $\mathrm{Hom}_A(-, M)$ 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 monomorfismo, si f^* es epimorfismo o no. La respuesta es que en general no es cierto, como se puede ver con el siguiente (contra)ejemplo:

Ejemplo: Tomamos $X = Y = \mathbb{Z}$, $f : X \to Y$ dada por $f(n) = 2n$, g la proyección canónica a $Z = \mathbb{Z}_2$. Tenemos la siguiente sucesión exacta:

$$0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}_2 \to 0$$

Aplicando el funtor $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Z}_2)$, se obtiene la sucesión

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}_2) & \xrightarrow{\pi^*} & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}_2) & \xrightarrow{f^*} & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}_2) \\ & & \| & & \| & & \| \\ & & \mathbb{Z}_2 & & \mathbb{Z}_2 & & \mathbb{Z}_2 \end{array}$$

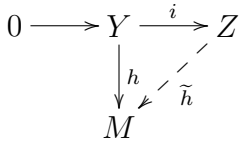
Esta sucesión nunca puede ser exacta porque en ese caso la dimensión, como $\mathbb{Z}_2$-espacio vectorial del objeto del medio sería la suma de las dimensiones de los objetos de las puntas. Igualmente en este caso se puede explicitar f^*. Tenemos que, si $\phi : \mathbb{Z} \to \mathbb{Z}_2$,

$$f^*(\phi)(1) = \phi(f(1)) = \phi(2) = 2\phi(1) = 0$$

luego $f^* = 0$, y por lo tanto f^* no es epimorfismo. Notar 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 $\mathrm{Hom}_{\mathbb{Z}}(-, M)$ es exacto.

Definición 5.4.1. *Un A-módulo M se llama A-***inyectivo** *si el funtor $\mathrm{Hom}_A(-, M) : {}_A\mathrm{Mod} \to Ab$ es exacto.*

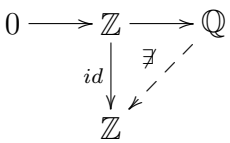
Es decir, M es inyectivo si y sólo si $\mathrm{Hom}_A(-, M)$ transforma monomorfismos en epimorfismos, si y sólo si, dado el siguiente diagrama de flechas llenas de A-módulos se puede completar, (de manera no necesariamente única) con la flecha punteada, de manera tal que el diagrama completo sea conmutativo:



Observación: Si además se tiene un A-B-bimódulo ${}_AM_B$, el funtor 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, ${}_AM_B$ 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, la inclusión $\mathbb{Z} \hookrightarrow \mathbb{Q}$ y la identidad de $\mathbb{Z}$ en $\mathbb{Z}$

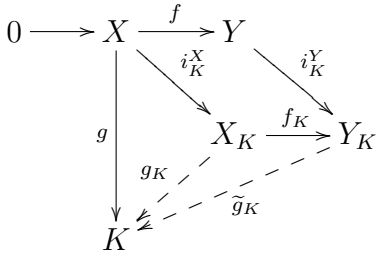
   

   es claro que no hay morfismo $\mathbb{Q} \to \mathbb{Z}$ que restringido a $\mathbb{Z}$ sea la identidad pues de hecho no hay ningún morfismo no nulo de $\mathbb{Q}$ en $\mathbb{Z}$.

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:

   Para esto recordemos que, en esa situación, si $f : X \to Y$ es un monomorfismo, entonces $f_S : X_S \to Y_S$ es un monomorfismo, para cualquier subconjunto multiplicativo S de A. Tomando $S = A - \{0\}$, llamemos $X_K := X_{A-\{0\}}$, análogamente Y_K. Si $g : X \to K$ es un morfismo cualquiera de A-módulos, tenemos el siguiente diagrama:



   Las flechas llenas f y g son los datos originales, $i_K^X : X \to X_K$ es la flecha canónica de localización $x \mapsto \frac{x}{1}$, idem i_K^Y. Como los elementos de $A - \{0\}$ son inversibles en K, el morfismo $g : X \to K$ se factoriza a través de X_K mediante g_K. Si ahora sólo consideramos X_K, Y_K y K, el diagrama está en la categoría de K-espacios vectoriales, en donde todos los objetos son inyectivos, de ahi la existencia de $\widetilde{g}_K$. Tomamos entonces $\widetilde{g} : Y \to K$ definida por $\widetilde{g} = \widetilde{g}_K \circ i_K^Y$. Como en el diagrama anterior, todos los cuadrados y/o 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 de inyectivos, que se demuestran muchas veces dualizando las demostraciones anteriores:

Proposición 5.4.2. *Sea A un anillo y $(M_i)_{i\in I}$ una familia de A-módulos. Entonces:*

1. $\prod_{i\in I} M_i$ *es inyectivo si y sólo si cada* M_i *es inyectivo.*
2. *Si* $\oplus_{i\in I} M_i$ *es inyectivo entonces cada* M_i *es inyectivo. La recíproca no es necesariamente cierta.*

Demostración: 1. Sea $f : X \to Y$ un monomorfismo y consideremos el cuadrado conmutativo

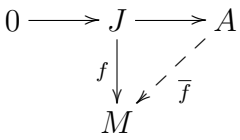
$$\begin{array}{ccc} \mathrm{Hom}_A(Y, \prod_{i\in I} M_i) & \xrightarrow{f^*} & \mathrm{Hom}_A(X, \prod_{i\in I} M_i) \\ \| & & \| \\ \prod_{i\in I} \mathrm{Hom}_A(Y, M_i) & \xrightarrow{\prod f_i^*} & \prod_{i\in I} \mathrm{Hom}_A(X, M_i) \end{array}$$

Luego la flecha de arriba (f^*) es un epimorfismo si y sólo si la flecha de abajo ($\prod f_i^*$) lo es. Y $\prod f_i^*$ es un epimorfismo si y sólo si todas las f_i^* lo son, lo que demuestra 1.

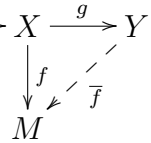
2. Dado $M = \oplus_{i\in I} M_i$ y M_{i_0}, entonces $M = \left(\oplus_{i\in I-\{i_0\}} M_i\right) \prod M_{i_0}$. Por 1., al ser M inyectivo resulta M_{i_0} inyectivo también.

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 5.4.3. *(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 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 $\overline{f}$.

Podemos suponer que X es un submódulo de Y y que g es la inclusión, si no se reemplaza X por $g(X)$ y f por $f \circ g^{-1}$.

Se define $Y = \{(Y', f') \ / Y' \subseteq Y$ es un submódulo, f' es un morfismo de A-módulos con $f'|_X = f\}$. Se ordena parcialmente a Y a través de

$$(Y', f') \leq (Y'', f'') \ \Leftrightarrow Y' \subseteq Y'' \text{ y } f''|_{Y'} = f'$$

Se verifica que $(Y, \leq)$ es un conjunto inductivo superiormente, luego tiene algún elemento maximal, que llamaremos (Y_0, f_0). Supongamos que Y_0 está incluído estrictamente en Y, sea entonces $y \in Y - Y_0$, luego $\langle y, Y_0 \rangle$ contiene estrictamente a Y_0. Sea $J = \{a \in A \ / \ ay \in Y_0\}$; como Y_0 es un submódulo de Y, J resulta un ideal de A (ejercicio: verificarlo!). Sea entonces $\phi : J \to M$ definida por $\phi(a) := f_0(ay)$. Por hipótesis, ϕ se puede extender a $\overline{\phi} : A \to M$. Veamos que f_0 se puede extender a $\langle y, Y_0 \rangle$.

Sea $x = ay + y_0$ donde $a \in A$ e $y_0 \in Y_0$, definimos

$$f_1(x) := \overline{\phi}(a) + f_0(y_0)$$

Esta función $f_1 : \langle y, Y_0 \rangle \to M$ está bien definida pues si $ay + y_0 = a'y + y_0'$, entonces $(a - a')y = y_0' - y_0 \in Y_0$, es decir, que $(a - a') \in J$, por lo tanto

$$\begin{array}{rcccl} \overline{\phi}(a) - \overline{\phi}(a') & = & \overline{\phi}(a - a') & = & \phi(a - a') = \\ & = & f_0((a - a')y) & = & f_0(y_0' - y_0) = \\ & = & f_0(y_0') - f_0(y_0) & & \end{array}$$

Reordenando los términos de estas igualdades obtenemos que $\overline{\phi(a)} + f_0(y_0) = \overline{\phi(a')} + f_0(y_0')$. Por lo tanto la función está bien definida, y es claro que $(Y_0, f_0) < (\langle y, Y_0 \rangle, f_1)$, lo que contradice la maximalidad de (Y_0, f_0), luego Y_0 debe ser igual a Y.

Ejercicio: Utilizando el teorema anterior, demostrar nuevamente 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.

Para obtener más ejemplos de módulos inyectivos, probaremos los siguientes dos lemas:

Lema 5.4.4. *Un grupo abeliano G es divisible si y sólo si es un $\mathbb{Z}$-módulo inyectivo.*

Demostración: $\Rightarrow$) Utilizaremos el Teorema de Baer, es decir, probaremos que todo diagrama de grupos abelianos $\begin{array}{ccccc} 0 & \longrightarrow & I & \longrightarrow & \mathbb{Z} \\ & & \downarrow{\scriptstyle h} & & \\ & & G & & \end{array}$ (donde I es un ideal de $\mathbb{Z}$) se completa con una flecha $\mathbb{Z} \to G$.

Recordamos ahora que todos los ideales de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$ para algún $n \in \mathbb{N}_0$. Luego, dado $I \subseteq \mathbb{Z}$, consideremos el n tal que $I = n\mathbb{Z}$. Si $n = 0$ se puede extender siempre el morfismo 0 por 0. Si $n \neq 0$, como G es un grupo abeliano divisible existe $v \in G$ tal que $h(n) = n.v$. Por linealidad, tenemos que $h(j.n) = j.n.v$ para todo $j.n \in n\mathbb{Z}$. Basta definir $\overline{h} : \mathbb{Z} \to G$ de la forma $\overline{h}(m) := m.v$.

$\Leftarrow$) Supongamos que G es un $\mathbb{Z}$-módulo inyectivo. Dado $g \in G$, $n \in \mathbb{Z}$, $n \neq 0$, queremos ver que existe $g' \in G$ tal que $g = n.g'$.

Definamos un morfismo $h_g : \mathbb{Z} \to G$ por $h_g(m) = mg$ y consideremos el monomorfismo $.n : \mathbb{Z} \to \mathbb{Z}$ (la multiplicación por n).

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{.n} & \mathbb{Z} \\ & & \downarrow{\scriptstyle h_g} & \swarrow{\scriptstyle \overline{h_g}} & \\ & & G & & \end{array}$$

Como G es inyectivo, existe $\overline{h_g} : \mathbb{Z} \to G$ que hace del diagrama anterior un diagrama conmutativo, i.e. $\overline{h_g}(n.m) = h_g(m) = mg \ \forall \ \ m \in \mathbb{Z}$. Si tomamos el elemento $g' := \overline{h_g}(1)$, éste verifica que

$$ng' = n\overline{h_g}(1) = \overline{h_g}(n) = h_g(1) = g$$

Proposición 5.4.5. *Si G es un grupo abeliano divisible, entonces el A-módulo* $\mathrm{Hom}_{\mathbb{Z}}(A, G)$ *es A-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. Recordamos 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 que si $\phi \in \mathrm{Hom}_{\mathbb{Z}}(A, G)$ y a, a' perteneces a A, entonces $(a.\phi)(a') := \phi(a'a)$.

Se define $f : N \to G$ por:

$$f(n) := h(n)(1) \quad \forall \quad n \in N$$

Como G es $\mathbb{Z}$-inyectivo, existe un morfismo de grupos abelianos $\overline{f} : M \to G$ que extiende a f. Se define una extensión de h como

$$\begin{aligned} \overline{h} &: M \to \mathrm{Hom}_{\mathbb{Z}}(A, G) \\ \overline{h}(m)(a) &:= \overline{f}(am) \end{aligned}$$

De esta manera $\overline{h}$ resulta A-lineal a izquierda (verificarlo!), y el diagrama conmuta porque dado $n \in N$,

$$\overline{h}(n)(a) = \overline{f}(an) = f(an) = h(an)(1)$$

por otro lado, como h es A-lineal,

$$h(an)(1) = (ah(n))(1) = h(n)(a)$$

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, es decir: 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:

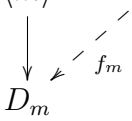
Lema 5.4.6. *Sea M un grupo abeliano cualquiera, entonces existe un grupo abeliano divisible D y un monomorfismo $M \to D$.*

Demostración: Primero supongamos 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 caso $M \cong \mathbb{Z}_n \hookrightarrow \mathbb{Q}/\mathbb{Z}$ donde el monomorfismo de $\mathbb{Z}_n$ en $\mathbb{Q}/\mathbb{Z}$ está definido por $\overline{1} \mapsto \frac{\overline{1}}{n}$.

Si ahora M es cualquiera y $m \in M$, $\langle m \rangle$ es cíclico y existe un monomorfismo $\langle m \rangle \hookrightarrow D_m$ donde D_m es un grupo abeliano divisible. Como los módulos

divisibles son inyectivos, se puede definir, para cada $m \in M$, un morfismo $M \to D_m$ que extienda al monomorfismo anterior: $0 \longrightarrow \langle m \rangle \longrightarrow M$



El morfismo f_m no tiene por qué ser inyectivo, sin embargo uno siempre sabe que $m \notin \mathrm{Ker}(f_m)$.

Se considera ahora $D := \prod_{m \in M-\{0\}} D_m$ y el morfismo

$$\begin{aligned} f : M &\to \prod_{m \in M-\{0\}} D_m \\ x &\mapsto \{f_m(x)\}_{m \in M-\{0\}} \end{aligned}$$

Como todos los D_m son $\mathbb{Z}$-módulos inyectivos, D resulta un $\mathbb{Z}$-módulo inyectivo, además

$$\mathrm{Ker}(f) = \cap_{m \in M-\{0\}} \mathrm{Ker}(f_m)$$

Pero dado $m \in M$, $m \notin \mathrm{Ker}(f_m) \supseteq \cap_{x \in M-\{0\}} \mathrm{Ker}(f_x)$, luego $\mathrm{Ker}(f) = 0$, es decir, f es un monomorfismo.

Proposición 5.4.7. *Sea M un A-módulo cualquiera, entonces 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 $M \to D$, donde D es un grupo abeliano divisible. A partir de este monomorfismo tenemos la siguiente cadena de monomorfismos:

$$M \cong \mathrm{Hom}_A(A, M) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(A, M) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(A, D)$$

Si llamamos $I := \mathrm{Hom}_{\mathbb{Z}}(A, D)$, resulta de la proposición 5.4.5que I es A-inyectivo.

Recordamos 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 5.4.8. *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 $M \cong \mathbb{Z}$, se puede definir

$$\begin{aligned} &\mathbb{Z} \to (\mathbb{Q}/\mathbb{Z})^{\mathbb{N}} \\ &1 \mapsto \left\{\frac{1}{n}\right\}_{n\in\mathbb{N}} \end{aligned}$$

y resulta inyectiva. Ahora un argumento similar al exhibido en la demostración del lema 5.4.6 (utilizando el hecho de que $\mathbb{Q}/\mathbb{Z}$ es inyectivo) muestra que siempre hay un monomorfismo de M en un producto 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 del de cogenerador es el de generador, donde la definición de generador es la siguiente: un A-módulo es generador si, para todo A-módulo X existe un conjunto deíndices J y un epimorfismo $M^{(J)} \to X$. Por ejemplo el A-módulo ${}_AA$ es generador, y cualquier módulo libre también, aunque un generador no es necesariamente libre.

Proposición 5.4.9. *Sea M un A-módulo, son equivalentes:*

1. *M es inyectivo.*
2. *Toda sucesión exacta corta del tipo $0 \to M \to X \to Y \to 0$ se parte.*

Además, cualquiera de las dos anteriores implica que M es un sumando directo de un cogenerador.

Demostración: 1. $\Rightarrow$ 2. Considerando en particular el diagrama

$$\begin{array}{ccccc} 0 & \longrightarrow & M & \longrightarrow & X \\ & & {\scriptstyle Id_M}\downarrow & \swarrow & \\ & & M & & \end{array}$$

sabemos que existe la flecha punteada que hace conmutar el diagrama debido a la inyectividad de M, esto dice que la sucesión

$$0 \to M \to X \to Y \to 0$$

se parte.

$2 \Rightarrow 1$. Dado M, sabemos que existe un monomorfismo $f : M \to I$ donde I es inyectivo. Consideramos la sucesión exacta corta $0 \to M \to I \to \mathrm{Coker}(f) \to 0$. Sabemos que esta sucesión se parte, luego M es un sumando directo de un inyectivo, luego un factor directo, por lo tanto M es inyectivo.

Veamos finalmente que 2. implica que M es sumando directo de un cogenerador:

Sabemos que $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$ es un cogenerador en la categoría de A-módulos. En particular, dado M, existe un conjunto I y un monomorfismo $f : M \to \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})^I$. Considerando la sucesión exacta

$$0 \to M \to \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})^I \to \mathrm{Coker}(f) \to 0$$

sabemos que se parte, luego M es un sumando directo de $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})^I$, y está claro que si un A-módulo X es cogenerador, también lo es X^I para cualquier conjunto no vacío I.

Observación: el A-módulo $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$ además de ser cogenerador, es inyectivo, luego todo sumando directo de $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})^I$ también será inyectivo.

5.5. Ejercicios

1. Sea k un cuerpo y G un grupo finito tal que $\frac{1}{|G|} \in k$. Demostrar que todo $k[G]$-módulo es proyectivo e inyectivo (sug: usar el hecho de que todo submódulo es un s.d.). ¿Es todo $k[G]$-módulo libre?

2. Sea $(\mathbb{R}^n, \phi)$ el $\mathbb{R}[x]$-módulo que tiene a $\mathbb{R}^n$ como espacio vectorial subyacente y la multiplicación por x está definida a través de la transformación lineal ϕ.

   a) Supongamos que o bien ϕ (en la base canónica) es una matriz simétrica o bien es una matriz ortogonal. Demostrar que todo $\mathbb{R}[x]$-submódulo de $(\mathbb{R}^n, \phi)$ es un sumando directo.

   b) Dar ejemplos de $(\mathbb{R}^n, \phi)$ que admitan $\mathbb{R}[x]$-submódulos que no sean sumandos directos.

3. 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?

4. Sea A un anillo conmutativo, M y N dos A-módulos a izquierda. Si consideramos a M y N como A-bimódulos simétricos (i.e. $m.a := a.m \; \forall \; a \in A, \; m \in M$, idem N), Decir todas maneras en que se puede dar a $\mathrm{Hom}_A(M,N)$ una estructura de A-módulo a derecha o a izquierda. Ver que todas coinciden y por lo tanto $\mathrm{Hom}_A(M,N)$ es un$A$-módulo simétrico. Probar:

   a) M divisible $\Rightarrow \mathrm{Hom}_A(M,N)$ no tiene torsión.

   b) N no tiene torsión $\Rightarrow \mathrm{Hom}_A(M,N)$ no tiene torsión.

5. Probar que no existe un epimorfismo de grupos

   a) de G_{p^∞} en $G_{p^\infty} \oplus G_p$.

   b) de $\mathbb{Q}$ en $G_{p^\infty} \oplus G_{p^\infty}$.

   c) de $\mathbb{Q}/\mathbb{Z}$ en $G_{p^\infty} \oplus G_n$.

6. Describir *todos* los $\mathbb{Z}$-módulos proyectivos de tipo finito y *todos* los $k[x]$-módulos proyectivos de tipo finito (k un cuerpo).

7. Probar que si existe un epimorfismo $\mathbb{Z}^n \to \mathbb{Z}^m$ entonces $n \geq m$. Probar también que si existe un monomorfismo $\mathbb{Z}^n \to \mathbb{Z}^m$ entonces $n \leq m$.

8. 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.

9. 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.

10. Probar que M es un A-módulo finitamente generado y proyectivo si y solo si pueden encontrarse $x_1, \ldots, x_r \in M$ y $\phi_1, \ldots, \phi_r \in M^*$ tal que para todo $m \in M$ vale $m = \sum_{i=1}^r \phi_i(m).x_i$.

11. 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^*?

12. 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 $\mathrm{Hom}_k(P_A, k)$ es un A-módulo 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.

13. 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

$$x.x = 0 \ ; \ y.y = 0 \ ; \ x.y = xy \ ; \ y.x = -xy$$

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. Demostrar el isomorfismo de A-módulos $M := \mathrm{Hom}_k(I, k) \cong \mathrm{Hom}_k(A, k)/I^{\perp}$ donde $I^{\perp} = \{f : A \to k \ / \ f|_I = 0\}$. Ver que M no es inyectivo.

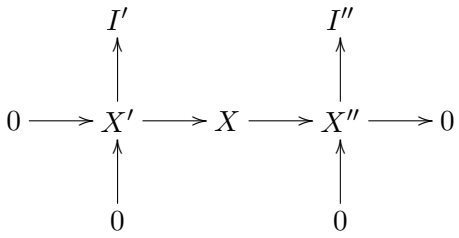
14. Ver que el siguiente diagrama de A-módulos

$$\begin{array}{ccccccccc} & & P' & & & & P'' & & \\ & & \downarrow & & & & \downarrow & & \\ 0 & \longrightarrow & X' & \longrightarrow & X & \longrightarrow & X'' & \longrightarrow & 0 \\ & & \downarrow & & & & \downarrow & & \\ & & 0 & & & & 0 & & \end{array}$$

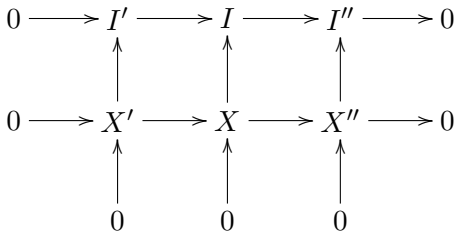
con P' y P'' proyectivos y la fila exacta, puede completarse al siguiente diagrama de filas exactas (con P también necesariamente proyectivo):

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P' & \longrightarrow & P & \longrightarrow & P'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & X' & \longrightarrow & X & \longrightarrow & X'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

15. Ver que el siguiente diagrama de A-módulos



con I' e I'' inyectivos y la fila exacta, puede completarse al siguiente diagrama de filas exactas (con I también necesariamente inyectivo):

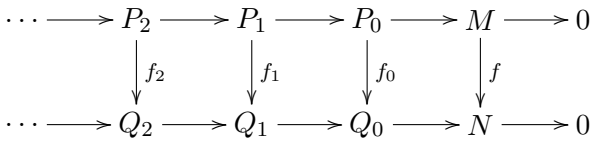


16. *a*) Sean

$$\cdots \to P_2 \to P_1 \to P_0 \to M \to 0$$

$$\cdots \to Q_2 \to Q_1 \to Q_0 \to N \to 0$$

dos sucesiones exactas de A-módulos en donde los P_i y los Q_i son proyectivos ($i \geq 0$) y sea $f : M \to N$ un morfismo de A-módulos. Demuestre entonces que f se levanta a un morfismo de sucesiones exactas, es decir que existe una familia de morfismos $\{f_i\}_{i\geq 0}$, $f_i : P_i \to Q_i$ tales que el siguiente diagrama es conmutativo:



b) Sean

$$0 \to M \to I_0 \to I_1 \to I_2 \to \dots$$

$$0 \to N \to J_0 \to J_1 \to J_2 \to \dots$$

dos sucesiones exactas de A-módulos en donde los I_i y los J_i son inyectivos ($i \geq 0$) y sea $f : M \to N$ un morfismo de A-módulos. Demuestre entonces que f se levanta a un morfismo de sucesiones exactas, es decir, a $\{f_i\}_{i\geq 0}$, $f_i : I_i \to J_i$ tales que el siguiente diagrama es conmutativo:

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & M & \longrightarrow & I_0 & \longrightarrow & I_1 & \longrightarrow & I_2 & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \\ 0 & \longrightarrow & N & \longrightarrow & J_0 & \longrightarrow & J_1 & \longrightarrow & J_2 & \longrightarrow & \cdots \end{array}$$

17. Sea A un anillo conmutativo y M, N dos A-módulos finitamente generados y proyectivos. Probar entonces que $\mathrm{Hom}_A(M, N)$ es un A-módulo finitamente generado y proyectivo.

18. Sea $M = k[x]$, $f \in k[x]$ y $S = \langle f \rangle$. Demuestre que $S^0 \cong (k[x]/\langle f \rangle)^*$ (dual respecto de k).

19. Sea M un A-módulo y $S \subseteq M$ un submódulo. Sea $S^0 = \{f \in M^* \text{ tal que } f(s) = 0 \ \forall \ s \in S\}$.

    a) Probar que S^0 es un submódulo (a izquierda de M^*) y $S^0 \cong (M/S)^*$.

    b) Supongamos que S es un sumando directo, probar entonces que:

    1) $S^* \cong M^*/S^0$.
    2) $(S^0)^0 \cong S \oplus (M^*)^0$.

20. Sea $\mathcal{S}$ el espacio vectorial formado por las sucesiones de números reales que tienen límite, sea $\mathcal{S}_0$ el subespacio formado por las sucesiones que tienden a cero. Encuentre isomorfismos explícitos $\mathcal{S}/\mathcal{S}_0 \cong \mathbb{R}$, $\mathcal{S} \cong \mathbb{R} \oplus \mathcal{S}_0$, $\mathcal{S}^* \cong \mathcal{S}_0^* \oplus \mathbb{R}$.

21. Dado un A-módulo cualquiera M, ver que M^* es siempre (via el morfismo canónico) un sumando directo de M^{***}.

6

Teoremas de estructura

Este capítulo tratará dos situaciones diferentes en donde hay una clasificación completa de la categoría de módulos (o 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 espacios vectoriales como caso de categoría semisimple, e indicamos como obtener la representación matricial de las formas de Jordan como aplicación del teorema de estructura sobre un dominio principal.

6.1. 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.

6.2. Módulos y anillos semisimples

Recordamos que un A-módulo M se dice simple si los 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 para la propiedad: " $b \in B \Leftrightarrow \langle b \rangle$ es simple, y $\langle b \rangle \cap \langle b' \rangle = 0$ para todo $b' \in B$, $b' \neq b$". Sea $M = \oplus_{b \in B} \langle b \rangle$, veamos que $M = A$:

Supongamos que no, luego existe un ideal a izquierda I maximal tal que $M \subset I$. Como A/I es un A-módulo simple y A/I es (por hipótesis) un A-módulo proyectivo, entonces $A \cong I \oplus A/I$. Pero entonces $A/I \subset M \subset I$, lo que es un absurdo, luego $M = A$. Resulta entonces que el A-módulo ${}_AA$ es suma directa de submódulos simples.

Definición 6.2.1. *1. Un A-módulo M se dice* **semisimple** *si y sólo si M es suma directa de submódulos simples.*

2. Un anillo A se dice **semisimple** *si y sólo si ${}_AA$ es un A-módulo semisimple.*

Ejemplos:

1. Todo módulo simple es semisimple (en particular $\{0\}$ es semisimple).

2. Si k es un cuerpo, todo k-espacio vectorial es semisimple.

3. Si k es un cuerpo, y $A = k \times \cdots \times k$ (n-veces), 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. G es un grupo abeliano simple si y sólo si $G \cong \mathbb{Z}_p$ con p un número primo. G es semisimple si y sólo si $G \cong \bigoplus_{p \text{ primo}} \mathbb{Z}_p^{(I_p)}$.

6. Sea $\mathcal{M} \subset A$ un ideal a izquierda maximal, entonces $A/\mathcal{M}$ es un A-módulo simple.

Observación: Si M es un A-módulo simple, entonces M es cíclico, y está generado por cualquiera de sus elementos no nulos, pues 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 $\mathcal{M} \subset A$ ideal a izquierda maximal tal que $M \cong A/\mathcal{M}$.

Vimos antes que un anillo A tal que todo A-módulo es proyectivo es semisimple. La afirmación recíproca se demostrará en la siguiente proposición.

Proposición 6.2.2. *Sea A un anillo semisimple, entonces todo A-módulo es proyectivo.*

Demostración: Sea M un A-módulo y sea $A = \oplus_{i\in I} A_i$ donde los A_i son A-módulos simples. El conjunto I es necesariamente finito pues $1 \in A$, $1 = \sum_{k=1}^{n} a_{i_k}$ con $a_{i_k} \in A_{i_k}$. Si $x \in A$, $x = x,1 = \sum_{k=1}^{n} x a_{i_k} \in \oplus_{k=1}^{n} A_{i_k}$.

Sea B un subconjunto de M maximal con respecto a la propiedad: "$b \in B \Leftrightarrow \langle b\rangle$ es simple, y $\langle b\rangle \cap \langle b'\rangle = 0$ para todo $b' \in B$, $b' \neq b$". Sea $N = \oplus_{b\in B}\langle b\rangle$, veamos que $N = M$:

Como B es maximal, entonces N tiene que contener a todo submódulo simple de M, y por lo tanto a todo submódulo semisimple. Pero como $A = \oplus_{i\in I} A_i$ con A_i simple, entonces todo cociente de A es semisimple, luego todo A-módulo cíclico es semisimple. Por lo tanto N contiene a todo elemento de M, luego $N = M$, con lo que resulta M semisimple.

Observación: Esta proposición muestra que en particular, todo anillo semisimple es hereditario.

Proposición 6.2.3. *Sea M un A-módulo, 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, queremos ver que M es semisimple.

Sea S la familia de submódulos simples de M, queremos probar que $M = \oplus_{S\in S} S$. Llamamos $N := \oplus_{S\in S} S$, por hipótesis N es un sumando directo. Sea N' un complemento, es decir, $N' \subseteq M$ y $M = N' \oplus N$. Veamos que si $N' \neq 0$ entonces contiene algún submódulo simple, lo que sería absurdo.

Podemos suponer que N' es de tipo finito, entonces tiene algún submódulo maximal $\mathcal{M}$. Consideremos la sucesión exacta corta

$$0 \to \mathcal{M} \to N' \to N'/\mathcal{M} \to 0$$

Al ser $\mathcal{M}$ maximal en N', el cociente $N'/\mathcal{M}$ es simple. Veamos que $N'/\mathcal{M}$ es isomorfo a un sumado directo de N', y para esto veremos que la propiedad de que "todo submódulo es un sumando directo" es hereditaria. Más precisamente: si X es tal que todo submódulo es un sumando directo e $Y \subseteq X$ un submódulo, entonces todo submódulo de Y es un sumando directo de Y.

Consideremos $Y' \subseteq Y$ un submódulo, entonces es un submódulo de X, luego sumando directo de X, y por lo tanto existe $p : X \to Y'$ tal que $p|_{Y'} = Id_{Y'}$. Llamemos $\pi := p|_Y$. Es claro que $\pi : Y \to Y'$ y verifica $\pi|_{Y'} = Id_{Y'}$, luego Y' se complementa en Y.

Supongamos ahora que M es semisimple y sea T un submódulo propio de M, sabemos que $M = \oplus_{i\in I} M_i$ con M_i simples. Sea $F = \{J \subseteq I \ / \ \oplus_{i\in J} M_i \cap T = 0\}$, tenemos que $F \neq \emptyset$ pues existe $i \in I$ tal que $M_i \not\subseteq T$, por lo tanto $M_i \cap T = 0$. Además F es inductivo superiormente, luego admite un elemento maximal, que llamamos J_0.

Es claro que $\langle \oplus_{i\in J_0} M_i, T\rangle = (\oplus_{i\in J_0} M_i) \oplus T$, veamos que además es igual a M.

Por la maximalidad de J_0, si $k \in I$, $M_k \cap ((\oplus_{i\in J_0} M_i) \oplus T) \neq 0$, luego $M_k \cap ((\oplus_{i\in J_0} M_i) \oplus T) = M_k$ pues M_k es simple. Esto dice que todos los submódulos simples de M están contenidos en $(\oplus_{i\in J_0} M_i) \oplus T$, y como M es semisimple, la suma de los submódulos simples es todo M.

Corolario 6.2.4. *Sea M un A-módulo semisimple y N un submódulo, entonces N y M/N son también semisimples.*

Demostración: de la prueba de la proposición anterior, si N es un submódulo de M con M semisimple, entonces todo submódulo de N es un sumando directo, luego 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, luego 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, y tal que además M/N es semisimple, no es cierto en general que M tenga que ser semisimple. Un (contra)ejemplo de esta situación es la extensión $0 \to \mathbb{Z}_p \to \mathbb{Z}_{p^2} \to \mathbb{Z}_p \to 0$.

Proposición 6.2.5. *Sea A un anillo, son equivalentes:*

1. *A es semisimple.*
2. *Todo A-módulo es semisimple.*
3. *Todo A-módulo libre es semisimple.*

4. *Todo A-módulo es proyectivo.*

5. *Toda extensión de A-módulos es trivial.*

6. *Todo A-módulo es inyectivo.*

7. *Todo ideal (a izquierda) de A es inyectivo.*

8. *Todo cociente de A es proyectivo.*

Demostración: $1 \Rightarrow 2$). Todo A-módulo es suma de submódulos cíclicos, por lo tanto basta ver que todo A-módulo cíclico es semisimple. Si M es cíclico, $M \cong A/I$ para algún ideal (a izquierda) I, por ser A semisimple, M resulta semisimple pues por el Corolario 6.2.4 todo cociente de un semisimple es semisimple.

$2 \Rightarrow 3$). es trivial.

$3 \Rightarrow 4$). Sea M un A-módulo cualquiera, entonces M es cociente de un libre. Considerando un epimorfismo $p : L \to M$ donde L es libre, $\operatorname{Ker}(p)$ es (Proposición 6.2.3) un sumando directo de L, luego $L/\operatorname{Ker}(p) \cong M$ también es isomorfo a un sumando directo de L, luego M es proyectivo.

$4 \Rightarrow 5$). Consideramos una extensión de A-módulos cualquiera $0 \to X \to Y \to Z \to 0$. Como en particular Z es proyectivo, esta sucesión se parte.

$5 \Rightarrow 6$). Sea M un A-módulo, como en particular toda sucesión exacta $0 \to M \to X \to Y \to 0$ se parte, M resulta inyectivo.

$6 \Rightarrow 7$). es trivial

$7 \Rightarrow 8$). Sea I un ideal, que sabemos que es inyectivo, luego la sucesión exacta

$$0 \to I \to A \to A/I \to 0$$

se parte. Esto dice que A/I es isomorfo a un sumando directo de A, luego A/I es proyectivo.

$8 \Rightarrow 1$). Por la Proposición 6.2.3 basta ver que todo ideal I de A es un sumando directo. Considerando de nuevo la sucesión $0 \to I \to A \to A/I \to 0$, como A/I es proyectivo, esta sucesión se parte, luego I es un sumando directo, como se quería ver.

Observación: Si A es semisimple, entonces A es artiniano y noetheriano. Para ver que es noetheriano, basta ver que todo ideal es finitamente generado, pero como todo ideal es un sumando directo, entonces todo ideal es isomorfo a un cociente de A, luego cíclico, luego finitamente generado. Para ver que es artiniano consideremos una cadena descendente de ideales

$$I_1 \supset I_2 \supset I_3 \supset \dots$$

Como I_2 es un sumando directo de I_1, $I_1 \cong C_1 \oplus I_2$. A su vez, I_3 es un sumando directo de I_2, luego $I_2 = I_3 \oplus C_2$ y consecuentemente $I_1 = I_3 \oplus C_1 \oplus C_2$. Si consideramos la cadena creciente de ideales $C_1 \subset (C_1 \oplus C_2) \subset (C_1 \oplus C_2 \oplus C_3) \subset \dots$, como A es noetheriano se estaciona, luego existe un n_0 tal que $C_n = 0 \ \forall \ n \geq n_0$, lo que significa que $I_n \cong I_{n+1} \ \forall \ n \geq n_0$.

Ejemplos:
1. (Teorema de Maschke) Sea G un grupo finito, k un cuerpo tal que $\frac{1}{|G|} \in k$, entonces $k[G]$ es un anillo semisimple.
Demostración: Sea M un $k[G]$-módulo y $S \subseteq M$ un submódulo, queremos ver que S es un sumando directo. Como k es un cuerpo, existe una transformación k-lineal $\pi : M \to S$ tal que $\pi|_S = Id_S$. Si π fuera $k[G]$-lineal, entonces S sería un $k[G]$-sumando directo. Definamos $\phi : M \to S$ a través de

$$\phi(m) := \frac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}.m)$$

Veamos que $\phi|_S = Id_S$ y que es $k[G]$-lineal:
Si $s \in S$, entonces $g^{-1}.s \in S$ y $\pi(g^{-1}.s) = g^{-1}.s$, luego

$$\phi(s) = \frac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}.s) \frac{1}{|G|} \sum_{g \in G} gg^{-1}.s = \frac{1}{|G|} \sum_{g \in G} s = \frac{|G|}{|G|} s = s$$

Si $h \in G$, $\phi(h.m) = \frac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}hm)$. Llamando $g' = hg$, tenemos que

$$\begin{array}{rcccl} \phi(h.m) & = & \frac{1}{|G|} \sum_{g \in G} g\pi(g^{-1}hm) & = & \frac{1}{|G|} \sum_{g' \in G} g'\pi((g')^{-1}hm) = \\ & = & \frac{1}{|G|} \sum_{g' \in G} hg\pi(g^{-1}h^{-1}hm) & = & \frac{1}{|G|} h.\left(\sum_{g' \in G} g\pi(g^{-1}m)\right) = \\ & = & h\phi(m) & & \end{array}$$

2. Sea D un anillo de división y $A = M_2(D)$.
Llamemos $I_1 := \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \ / \ a, b \ \in D \right\}$ e $I_2 := \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \ / \ a, b \ \in D \right\}$.
Es claro que, como A-módulos a izquierda, $A \cong I_1 \oplus I_2$. Además son simples, por ejemplo basta ver que cualquier elemento de I_1 genera a I_1, (con I_2 es la misma cuenta).
Si $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \neq 0$, supongamos que $a \neq 0$, entonces $\begin{pmatrix} a^{-1} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.
A su vez $\begin{pmatrix} 0 & 0 \\ a^{-1} & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Luego $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ genera I_1. Si $a = 0$ entonces necesariamente $b \neq 0$, se deja como ejercicio ver que en este caso $\begin{pmatrix} 0 & 0 \\ b & 0 \end{pmatrix}$ también genera I_1. Por lo tanto $M_2(D)$ es semisimple. Análogamente, $M_n(D)$ es semisimple para cualquier $n \in \mathbb{N}$.

Ejercicio: (Lema de Schur). Sea M un A-módulo simple, entonces el anillo $\mathrm{End}_A(M)$ es un anillo de división, i.e. todo morfismo A-lineal $f : M \to M$ o bien es cero, o bien es un isomorfismo.

Teorema 6.2.6. *(Wedderburn) Sea A un anillo semisimple, entonces*

$$A^{op} \cong \prod_{i=1}^{N} M_{r_i}(D_i)$$

donde D_i son los anillos de división $D_i = \mathrm{End}_A(L_i)$ con L_i ideales simples de A.

Demostración: Como A es semisimple, entonces existen $L_1, \ldots, L_N$ ideales simples tales que $A \cong \oplus_{i=1}^{N}(L_i)^{r_i}$. Llamamos $A_i := (L_i)^{r_i}$, afirmamos que son ideales biláteros:

Es claro que son ideales a izquierda, calculemos $A_i.A$:

$$A_i.A = \sum_{j=1}^{N} A_i.A_j$$

Supongamos que $i \neq j$, entonces $L_i.L_j = 0$. Si no, sea $x \in L_j$ tal que $L_i.x \neq 0$. Como L_i y L_j son simples, y el morfismo $L_i \to L_j$ definido por $a \mapsto a.x$ es no nulo, entonces son isomorfos, lo que es una contradicción. Esto implica que $A_i.A_j = 0$ cuando $i \neq j$, por lo tanto $A_i.A \subseteq A_i.A_i \subseteq A_i$, luego A_i es también ideal a derecha. Tenemos la siguiente cadena de isomorfismos de anillos:

$$A^{op} \cong \mathrm{Hom}_A({}_AA, {}_AA) = \mathrm{Hom}_A(\oplus_{i=1}^{N} A_i, \oplus_{j=1}^{N} A_j) \cong \oplus_{i,j=1}^{N} \mathrm{Hom}_A(A_i, A_j)$$

Pero si $i \neq j$, $\mathrm{Hom}_A(A_i, A_j) = 0$ porque si no habría algún morfismo no nulo de L_i en L_j (y por lo tanto un isomorfismo), entonces

$$\bigoplus_{i,j=1}^{N} \mathrm{Hom}_A(A_i, A_j) = \prod_{i=1}^{N} \mathrm{End}_A(A_i)$$

Calculemos ahora $\mathrm{End}_A(A_i)$:

Como $A_i \cong (L_i)^{r_i}$,

$$\mathrm{End}_A(A_i) \cong \mathrm{Hom}_A((L_i)^{r_i}, (L_i)^{r_i}) \cong M_{r_i}(\mathrm{End}_A(L_i)) = M_{r_i}(D_i)$$

En general, el isomorfismo $\mathrm{End}_A(X^n) \cong M_n(\mathrm{End}_A(X))$ está dado por:

Dada $\phi : X^n \to X^n$, $(x_1, \ldots, x_n) \mapsto (\phi_1(x_1, \ldots, x_n), \ldots, \phi_n(x_1, \ldots, x_n))$ se asigna $||\phi|| \in M_n(\mathrm{End}_A(X))$ definida por

$$||\phi||_{ij}(x) := \phi_j(0, \ldots, 0, x, 0 \ldots, 0) \quad \text{con } x \text{ en el lugar } i.$$

Se deja como ejercicio ver que siempre esa asignación es un isomorfismo de anillos.

Corolario 6.2.7. *Sea A un anillo semisimple tal que no tiene ideales biláteros propios. Entonces A es isomorfo a un anillo de matrices con coeficientes en un anillo de división.*

Corolario 6.2.8. *Sea A un anillo, entonces A es semisimple a izquierda si y sólo si es semisimple a derecha.*

Demostración: Es claro utilizando el Teorema de Wedderburn, y notando que la trasposición de matrices da un isomorfismo de anillos:

$$M_n(D)^{op} \cong M_n(D^{op})$$

Finalmente D es un anillo de division si y sólo si D^{op} es un anillo de división.

Ejercicio: Descomponer a $\mathbb{R}[\mathbb{Z}_2]$, $\mathbb{R}[\mathbb{Z}_3]$ y $\mathbb{C}[\mathbb{Z}_3]$ como producto de matrices sobre álgebras de división, (como dice el Teorema de Wedderburn). Sug.: Encontrar módulos simples sobre los respectivos anillos. (nombre: módulos simples = representaciones irreducibles). 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?

Ejercicio: Sea A semisimple, probar que $\mathrm{rad}(A) = 0$, donde $\mathrm{rad}(A)$ es la intersección de todos los ideales a izquierda maximales de A.

Proposición 6.2.9. *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 $\mathrm{rad}(A) = 0$, veamos que todo ideal de A es un sumando directo:

Sea $I \subset A$ un ideal de A, consideremos $J = \{J \subset A$ ideal a izquierda de A tal que $I + J = A\}$. El conjunto J es no vacío pues $A \in J$, está ordenado

por la inclusión, y por ser A artiniano, admite un elemento minimal. Sea $J \in J$ un elemento minimal, es claro que $I + J = A$, veamos que $I \cap J = 0$.

Supongamos que $I \cap J \neq 0$, entonces, dentro del conjunto de los ideales (a izquierda) no nulos contenidos en $I \cap J$ existe uno minimal, que llamamos B.

Como $\text{rad}(A) = 0$, existe un ideal maximal $\mathcal{M}$ tal que $B \not\subseteq \mathcal{M}$, y por lo tanto $A = B + \mathcal{M}$. Como $B \subset J$, resulta que $J \not\subseteq \mathcal{M}$, sea entonces $J' = \mathcal{M} \cap J \subset J$. Entonces

$$A = I + J = I + (B + \mathcal{M}) \cap J \subseteq I + B + J' = I + J'$$

pues $B \subseteq I$. Esto dice que $J' \in J$, lo que contradice la minimalidad de J.

Ejercicio: demostrar que $\text{rad}(A)$ es un ideal bilátero.

Corolario 6.2.10. *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).*

Ejercicio: Sea G un grupo finito y k un cuerpo. Demostrar que la función $\epsilon k[G] \to k$ (definida por $\epsilon(g) = 1 \ \forall g \in G$) es un morfismo de anillos, luego $k[G]$ siempre tiene por lo menos un ideal bilátero propio.

Corolario 6.2.11. *Si A es artiniano, entonces $A/\text{rad}(A)$ es semisimple.*

Demostración: basta demostrar que $\text{rad}(A/\text{rad}(A)) = 0$, que se deja como ejercicio.

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* $A_1(k)$ está definida como la subálgebra de $\text{End}_k(k[x])$ generada por la multiplicación por la variable x, que denotaremos q, y la derivada con respecto a x, que denotaremos p. Como se verifica la relación de conmutación $[p, q] = 1$ (verficar!), todo elemento del álgebra de Weyl se puede escribir como combinación k-lineal de monomios de la forma $p^i q^j$ con i y j mayores o iguales que cero. 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, el polinomio f_n se llamará coeficiente principal de P.

Ejemplo / Ejercicio:

1. Si P es un elemento del álgebra de Weyl de grado n, con coeficiente principal f_n, entonces $[P, q]$ es un elemento de grado $n-1$, y su coeficiente principal es $n.f_n$.

2. Si f es un polinomio en q, entonces $[p, f] = f'$.

A partir del cálculo anterior, es fácil ver que $A_1(k)$ no tiene ideales biláteros propios:

Sea I un ideal bilátero no nulo, y $0 \neq P \in I$. Como $[P, q] \in I$, si el grado de P es positivo, haciendo el corchete iteradamente uno puede suponer que I contiene un elemento de grado cero no nulo, es decir, un polinomio en q, digamos $f(q)$. Si f fuera una constante, entonces I contiene una unidad, luego $I = A$. Si f no es una constante, entonces $[p, f(q)] = f'(q) \neq 0$ y $f'(q) \in I$. Si f' es una constante terminamos, si no volvemos a calcular conmutadores sucesivos hasta obtener una constante.

6.3. Ejercicios

1. Demuestre que $\mathrm{rad}(A/\mathrm{rad}(A)) = 0$.

2. Demuestre que $\mathrm{rad}(A) = \{a \in A \ / \ 1 - x.a$ es inversible a izquierda para todo $x\}$.

3. Sea A un anillo, probar que si $r \in \mathrm{rad}(A)$ entonces $1 - r$ es una unidad de A.

4. Probar que si A es semisimple y L es un ideal a izquierda de A entonces,

   - existe $e \in A$ idempotente (i.e. $e^2 = e$) tal que $L = A.e$.
   - A no tiene ideales a izquierda nilpotentes.
   - Si L es simple entonces el idempotente es primitivo (i.e. si $e = e_1 + e_2$ con $e_i^2 = e_i$ y $e_1.e_2 = 0 = e_2.e_1$ entonces alguno de los e_i es cero).

5. Sea M un A-módulo simple con A semisimple, demostrar que M es isomorfo a un ideal de A.

6. Encontar un ejemplo de anillo (necesariamente no semisimple) tal que exista un módulo simple que no sea isomorfo a ningún ideal de A.

7. Sea k un cuerpo y $T_2(k) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} / \ a,\ b,\ c \in k \right\}$ no es un anillo semisimple. Calcular $\mathrm{rad}(T_2(k))$ y $T_2(k)/\mathrm{rad}(T_2(k))$.

8. Sea k un cuerpo, $A = k \times k$ con el producto coordenada a coordenada. Ver que A es semisimple pero no simple. Quiénes son los idempotentes ortogonales que suman uno?

9. 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.

10. Sea $v = (v_1, \ldots, v_n)$ un vector no nulo en k^n (k cuerpo). Probar que el conjunto de las matrices de la forma

$$\begin{pmatrix} a_1v_1 & a_1v_2 & a_1v_3 & \ldots & a_1v_n \\ a_2v_1 & a_2v_2 & a_2v_3 & \ldots & a_2v_n \\ a_3v_1 & a_3v_2 & a_3v_3 & \ldots & a_3v_n \\ . & . & . & \ldots & . \\ a_nv_1 & a_nv_2 & a_nv_3 & \ldots & a_nv_n \end{pmatrix}$$

con los $a_i \in k$, forman un ideal (a izquierda) simple.

11. Encontrar en $M_n(A)$ una familia $\{e_1, \ldots, e_n\}$ de elementos tales que $e_ie_j = 0$ si $i \neq j$, $e_i^2 = e_i$ y $\sum_{i=1}^n e_i = 1_{M_n(A)}$.

12. 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 $D_i = \mathrm{End}_A(L_i)^{op}$ 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.

13. 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.

14. 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, "tomar dimensión" para 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.

15. Sea $\mathcal{S}_3$ el grupo de permutaciones de tres elementos.

    a) Ver que existe una sucesión exacta de grupos $1 \to \mathbb{Z}_3 \to \mathcal{S}_3 \to \mathbb{Z}_2 \to 1$, más aún, $\mathcal{S}_3 \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_2$ donde la acción de $\mathbb{Z}_2$ en $\mathbb{Z}_3$ es "cambiar de signo". Ayuda eso para encontrar representaciones de $\mathbb{R}[\mathcal{S}_3]$ a partir de representaciones de $\mathbb{R}[\mathbb{Z}_3]$ y de $\mathbb{R}[\mathbb{Z}_2]$?

    b) Calcular el centro de $\mathbb{R}[\mathcal{S}_3]$. Qué posibilidades de descomposición en producto de matrices tiene $\mathbb{R}[\mathcal{S}_3]$?

    c) Sea M una representación irreducible de $\mathbb{R}[\mathcal{S}_3]$ con $dim_{\mathbb{R}}(M) = 2$ (cuántas hay?). Calcular el álgebra de división $\mathrm{End}_{\mathbb{R}[\mathcal{S}_3]}(M)$.

16. Sea k un cuerpo, G un grupo tal que $k[H]$ es semisimple para todo subgrupo H de G finitamente generado. Probar que $k[G]$ es semisimple.

17. (Una versión del Lema de Schur) Sea k un cuerpo algebraicamente cerrado, G un grupo finito tal que $|G|$ es inversible en k. Sea M un $k[G]$-módulo simple no nulo. Probar que $\mathrm{End}_{k[G]}(M) \cong k$, es decir, los únicos morfismos G-lineales son las homotecias. (Sugerencia: pensar en autovalores)

18. Sea k un cuerpo algebraicamente cerrado, G un grupo finito tal que $|G|$ es inversible en k. Entnces $k[G] \cong \bigoplus_{i=1}^{r} M_{n_1}(k)$ (por qué aparece k en las matrices en vez de álgebras de división cualesquiera?). Probar que $r = \#\langle G\rangle$, es decir, la cantidad de clases de isomorfismo de representaciones irreducibles de $k[G]$ es la misma que la cantidad de clases de conjugación de G. Sugerencia: $r = dim_k(\mathcal{Z}(k[G]))$ ($\mathcal{Z}(..)$= centro de ...).

19. Con las mismas notaciones del ejercicio anterior, demostrar que $dim_k(\mathcal{Z}(k[G]) = \#\langle G\rangle$ sin usar la hipótesis de k algebraicamente cerrado.

20. Es $\mathbb{Z}_2[\mathbb{Z}_2]$ una $\mathbb{Z}_2$-álgebra semisimple?

6.4. Dominios principales

El teorema principal de esta sección es el teorema 6.4.7, que caracteriza completamente los módulos finitamente generados sobre dominios a ideales principales (dip).

6.4.1. Anillos euclideanos, principales y de factorización

Comenzaremos recordando algunas definiciones generales y daremos algunas propiedades básicas de los dominios principales que se utilizarán luego.

Definición 6.4.1. *Sea A un dominio íntegro, diremos que A es* **euclídeo** *si existe una función $d : A - \{0\} \to \mathbb{N}_0$ tal que*

- $d(r) \leq d(r.s)\ \forall\ \ r,\ \forall\ s \neq 0.$
- *Dados a, b en A, $b \neq 0$, entonces existen (no necesariamente únicos) q, r en A tales que $a = bq + r$ con $r = 0$ ó $d(r) < d(b)$.*

Ejemplos:

1. k un cuerpo con $d \equiv 0$.
2. $\mathbb{Z}$, con $d(m) = |m|$.
3. $k[x]$ con k un cuerpo y $d = gr$.
4. $\mathbb{Z}_{\mathcal{P}}$ donde $\mathcal{P} = p\mathbb{Z}$ (p un número primo) con $d\left(\frac{m}{n}\right) = p^q$ si $m = p^q m'$ y $(m : m') = 1$.
5. Ejercicio: $k[x, x^{-1}]$ es euclídeo.
6. $\mathbb{Z}[i]$ con $d(a + bi) = a^r + b^2$.

Proposición 6.4.2. *Si A es euclideano entonces A es principal.*

Demostración: Sea $I \subset A$ un ideal no nulo, llamemos d a la función euclídea de A y sea $n \in \mathbb{N}_0 = min\{d(x)\ :\ x \in I - 0\}$. Sea $y \in I$ tal que $d(y) = n$, es claro que $\langle y \rangle \subseteq I$, dado $x \in I$, si $x \neq 0$ se tiene que existen q y r en A con $x = qy + r$, donde o bien $r = 0$ o bien $d(r) < d(y)$. Como $r = x - qy$ tenemos que $r \in I$, luego $d(r) \leq d(y)$ por la minimalidad de y, esto es un absurdo a menos que $r = 0$, es decir que $x \in \langle y \rangle$.

Recordamos que un elemento p en un anillo A se dice **primo** si y sólo si $p \notin \mathcal{U}(A)$ y $a.b \in \langle p \rangle \Rightarrow a \in \langle p \rangle$ ó $b \in \langle p \rangle$, equivalentemente p es primo si y sólo si $A/\langle p \rangle$ es un dominio íntegro. Recordamos también que un elemento $q \in A$ se llama **irreducible** si y sólo si $q \neq 0$, $q \notin \mathcal{U}(A)$ y si $q = b.c$ entonces o bien b o bien c son unidades. Si q es irreducible y u es una unidad, claramente uq es también irreducible, diremos que uq es un irreducible **asociado** a q.

Ejercicio: Si p es primo, entonces es irreducible.

Un dominio íntegro A se dice de **factorización única** (dfu) si satisface: para todo $0 \neq a \in A$, existen $q_1, \ldots q_r$ elementos irreducibles de A 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 dfu y $q \in A$ es irreducible, entonces q es primo.

Proposición 6.4.3. *Sea A un dominio principal, entonces A es un dominio de factorización única.*

Demostración: Sea $a \in A$, $a \neq 0$, $a \notin \mathcal{U}(A)$ y supongamos que a no se escribe como producto de irreducibles (en particular a no es irreducible). Entonces existen a_1 y b_1 que no son unidades tales que $a = a_1b_1$ y además alguno de los dos no es producto de irreducibles, por ejemplo a_1. Como $a_1|a$ y $b_1 \notin \mathcal{U}(A)$, entonces $\langle a\rangle \subset \langle a_1\rangle$ y la inclusión es estricta. A su vez, como el a_1 no es irreducible, se repite el razonamiento anterior y se obtiene una cadena de ideales estrictamente creciente, lo que es absurdo porque si A es principal entonces debe ser noetheriano.

La unicidad se demuestra de la misma manera que se demuestra que todo número entero se factoriza como un producto de primos. La mecánica de la demostración es la misma usando que, como se está en un dip, todo irreducible es primo.

Ejercicio: Mostrar (sin usar que dip $\Rightarrow$ dfu) que en un dip, todo elemento irreducible es primo.

Ejemplos: todos los dominios euclídeos son de factorización única, como $\mathbb{Z}$, y $k[x]$ con k cuerpo. También $k[x, x^{-1}]$ es un dfu, más generalmente, toda localización de un dfu es dfu.

Como resultado folklórico, mencionamos que en los dfu se tiene existencia de máximo común divisor, donde, dados $a_1, \ldots, a_r$, el máximo común divisor está definido como un elemento que divide a todos los a_i, y que es máximo con esa propiedad (máximo con respecto al orden de la divisibilidad). En un anillo arbitrario, en caso de existir un máximo común divisor, éste está univocamente determinado a menos de multiplicación por unidades. Observamos que como la noción de dominio euclideano implica dip, que a su vez implica dfu, en todos estos tipos de anillos hay existencia de máximo común divisor.

Teorema 6.4.4. *Sea A un dfu, entonces $A[x]$ también es dfu.*

Demostración: Dado $f \in A[x]$, $f \neq 0$, escribimos $f = c.g$ con $c \in A$ y g es tal que el máximo común divisor de todos sus coeficientes es uno.

Si consideramos $g \in A[x] \subset F[x]$, donde F es el cuerpo de fracciones de A, como $F[x]$ es dfu (ya que es euclideano, luego dip, luego dfu), entonces existe una descomposición $g = \frac{a}{b}h_1 \dots h_k$ donde $a,\ b \in A$, $b \neq 0$ y $h_i \in F[x]$ son polinomios irreducibles. Cambiando eventualmente los elementos a y b se puede suponer que los $h_i \in A[x]$ y que el máximo común divisor de los coeficientes de cada h_i es uno. Pero entonces cada h_i es irreducible en $A[x]$, luego $bg = ah_1 \dots h_k$, y como $h_1 \dots h_k$ es un polinomio tal que el máximo común divisor de sus coeficientes es uno, resulta que $a = bu$ con $u \in \mathcal{U}(A)$ y entonces $g = uh_1 \dots h_k$. Por lo tanto $f = u.c.h_1 \dots h_k$. Factorizando c como producto de irreducibles en A se obtiene una factorización completa de f. La unicidad se sigue de la unicidad de la factorización en $F[x]$ (para la parte de los h_i) y de la unicidad de la factorización en A (para el c).

Ejemplo: $\mathbb{Z}[x]$ es un dfu, y no es principal. Similarmente, si k es un cuerpo, $k[x_1, \dots, x_n]$ es un dfu, y no es principal a menos que $n = 1$.

6.4.2. Módulos finitamente generados sobre un dip

Hemos visto en la sección de módulos libres que si M es un módulo finitamente generado sobre un dominio principal A entonces $M \cong t(M) \oplus A^r$ para un r dado. El objetivo de esta sección es describir completamente los módulos sobre un dominio principal que son finitamente generados y de torsión.

Lema 6.4.5. *Sea A un dip, si L es un A-módulo libre y $M \subseteq L$ es un submódulo no nulo, entonces existen $0 \neq z \in L$, un submódulo S de L, y $c \in A$ tales que*

- $L = \langle z \rangle \oplus S$
- $M = \langle cz \rangle \oplus (S \cap M)$
- *Si $f : L \to A$ es una función lineal tal que $f(z) = 1$, entonces $f(M) = \langle c \rangle$.*

Demostración: Sea $I = \{I$ ideal no nulo de A tal que $I = f(M)$ para alguna $f \in \mathrm{Hom}_A(L, A)\}$. Este conjunto es no vacío pues en I están las imágenes de las funciones coordenadas de L en A, y alguna coordenada de los elementos

de M es no nula pues $M \neq 0$. Como A es noetheriano, I tiene un elemento maximal que llamamos I_0. Sea $h : L \to A$ tal que $h(M) = I_0$; como A es principal, existe $c \in A$ tal que $I_0 = c.A$. Llamemos $u \in M$ a un elemento tal que $h(u) = c$, afirmamos que u es divisible por c en L.

En efecto, veremos que $f_i(u)$ es divisible por c para todo i, donde f_i son las funciones coordenadas de L. Dado i, sea d_i el máximo comun divisor entre c y $f_i(u)$, sean $r,\ s \in A$ tales que $d_i = rc+sf_i(u) = rh(u)+sf_i(u) = (rh+sf_i)(u)$. Definimos $\phi = (rh + sf_i)$, la cuenta anterior muestra que $\phi(M)$ contiene al ideal generado por d_i, que a su vez contiene al ideal generado por c, esto contradice la maximalidad de I_0 a menos que $d_i = c$. De esta manera vemos que c divide a $f_i(u)$ para todo i, por lo tanto c divide a $h(u)$ (dado que h es una combinación lineal de las funciones coordenadas). Llamamos z al elemento de L tal que $u = c.z$, es claro que $h(z) = 1$ (recordar que A es íntegro).

Sea ahora $S = \mathrm{Ker}(h)$:

- considerando la sucesión exacta $0 \to \mathrm{Ker}(h) \to L \to \mathrm{Im}(h) \to 0$, como $\mathrm{Im}(h) = A$, la sucesión se parte, luego S es un sumando directo, y un complemento se obtiene a partir de una sección de h, que es por ejemplo enviar el 1 en z, luego $L = \langle z \rangle \oplus S$.

- La inclusión $\langle cz \rangle \oplus (S \cap M) \subseteq M$ es clara pues $c.z = u \in M$. En el otro sentido, si $x \in M$ entonces $h(x)z \in \langle cz \rangle \subset M$, luego se puede escribir $x = h(x).z + (x - h(x).z)$. Como el elemento $h(x).z \in M$ se sigue que $(x - h(x).z) \in M$, además $h(x - h(x).z) = h(x) - h(x).h(z) = 0$, luego $(x - h(x).z) \in M \cap S$.

- Sea $f : L \to A$ lineal tal que $f(z) = 1$. Entonces $f(u) = f(c.z) = cf(z) = c$, luego $\langle c \rangle \subset f(M)$, pero como $\langle c \rangle = I_0$ es un ideal maximal con respecto a esa propiedad, entonces son iguales.

Corolario 6.4.6. *Sea A un dip, L un A-módulo libre y M un submódulo de tipo finito, entonces existe una base $\{e_i\}_{i \in I}$, una subfamila finita $\{e_{i_j}\ j = 1, \ldots, n\}$ de $\{e_i\}_{i \in I}$ y elementos $a_1, \ldots a_n \in A$ tales $a_j | a_{j+1}$ $(j = 1, \ldots, n-1)$ y $M = \oplus_{j=1}^{n} \langle a_j e_{i_j} \rangle$.*

Demostración: Es por inducción en el rango de M. Por la proposición anterior, si $M \neq 0$, existe $z \in L$, $c \in A$ y S un submódulo 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. Aplicamos la hipótesis inductiva a $M \cap S \subseteq S$,

que es libre por ser submódulo de un libre, luego existe una base $\{x_k\}_{k\in\mathcal{K}}$ de S, una subfamilia finita $\{x_{k_l} \ : \ l = 2, \dots n\}$ y una sucesión $a_2|a_3|\dots a_n$ de elementos de A tales que $S \cap M = \oplus_{j=2}^{n}\langle a_j x_{k_j}\rangle$. Llamamos $a_1 := c$, $x_{k_1} := z$, entonces obtenemos que $M = \oplus_{j=1}^{n}\langle a_j x_{k_j}\rangle$. Falta ver que $a_1|a_2$. Se define $f : L \to A$ como $f(e_i) = \begin{cases} 1 & \text{si } \exists\ j \ / \ i = i_j \\ 0 & \text{si no} \end{cases}$. Para todo $j = 1, \dots, n$, $a_j = f(a_j e_{i_j}) \in f(M)$, por el último ítem de la proposición anterior, al ser $f(z) = 1$ tenemos que $f(M) = \langle c\rangle = \langle a_1\rangle$, por lo tanto $a_j \in \langle a_1\rangle$ para todo j, en particular $a_1|a_2$.

Teorema 6.4.7. *(De estructura de módulos f.g. sobre un dip) Sea M un A-módulo de tipo finito, entonces*

1. *Existe una sucesión $d_1|d_2|\dots d_n$ de elementos no inversibles de A tales que $M \cong \oplus_{i=1}^{n} A/d_i A$*

2. *Si $\{d_i\}_{i=1}^{n}$ y $\{d'_i\}_{i=1}^{n'}$ son dos familias de elementos de A que verifican 1, entonces $n = n'$ y existen unidades de A, $u_1, \dots, u_n$ tales que $d_i = u_i d'_i$ para todo $i = 1, \dots n$.*

Demostración: Veamos primero la primer parte, la segunda la demostraremos luego de exhibir diversos corolarios.

Sea L un A-módulo libre de tipo finito con un epimorfismo $p : L \to M$, luego $M \cong L/\operatorname{Ker}(p)$.

Por diversas razones (por ejemplo noetherianidad, o Teorema 5.1.15), $\operatorname{Ker}(p)$ es de tipo finito. Por el corolario anterior existen $\{e_i\}_{i=1,\dots,r}$ ($r = rg(L)$) una base de L, $d_j|d_{j+1}$, $j = 1, \dots s-1$ ($s = rg(\operatorname{Ker}(p)) \leq r$) una sucesión de elementos de A tales que $\{d_i e_i\}_{i=1,\dots s}$ es una base de $\operatorname{Ker}(p)$. Entonces

$$M \cong L/\operatorname{Ker}(p) \cong \frac{\bigoplus_{i=1}^{r}\langle e_i\rangle}{\bigoplus_{i=1}^{s}\langle d_i e_i\rangle} \cong \bigoplus_{i=1}^{r} A/\langle d_i\rangle$$

donde $d_i = 0$ si $i = s+1, \dots, r$.

Sea $m = max\{i \ / \ d_i \in \mathcal{U}(A)\}$ (o $m = 0$ si el conjunto anterior es vacío). Luego $M \cong \bigoplus_{i=m+1}^{r} A/\langle d_i\rangle$, ya que si d es una unidad, entonces $A/A.d = 0$. Renumerando los d_i y tomando $n = r - m$, obtenemos que los d_i no son unidades que se dividen consecutivamente y que $M \cong \oplus_{i=1}^{n} A/d_i A$.

Corolario 6.4.8. *Sea A un dip. Un A-módulo M es de tipo finito si y sólo si existe una familia C_i con $i = 1, \dots, n$ de A-módulos cíclicos tales que $M \cong \oplus_{i=1}^{n} C_i$.*

Observaciones: 1. La recíproca es cierta para cualquier anillo, no necesariamente un dip.

2. Con las notaciones del teorema de estructura:

$$t(M) = \bigoplus_{\substack{i=1,\dots,n \\ d_i \neq 0}} A/d_i A$$

Corolario 6.4.9. *Sea A un dip, M un A-módulo finitamente generado, entonces existe $n \in \mathbb{N}_0$, una familia $\{p_1, \dots p_r\}$ de primos de A, y números enteros no negativos $n_i^1 \leq \cdots \leq n_i^r$ $(i = 1, \dots r)$ tales que*

$$M \cong \bigoplus_{i=1}^{r} \left(\bigoplus_{j=1}^{r} A/\langle p_i^{n_i^j} \rangle \right) \oplus A^n$$

Demostración: el n se elige como el rango de la parte libre de M, para la parte de torsión sabemos que $t(M) = \oplus_{i=1}^{m} A/\langle d_i A \rangle$. Lo que hacemos ahora es escribir a cada d_i como producto de primos, de hecho, como $d_1 | d_2 | \dots | d_m$, basta factorizar $d_m = \prod_{i=1}^{r} p_i^{n_i^r}$, 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 6.4.10. *Sea A un dip y M un A-módulo finitamente generado de torsión, entonces existe una familia finita de A-módulos cíclicos $\{C_i\}_{i \in I}$, con cada C_i p_i-primario (donde los p_i primos, que en este caso es lo mismo que irreducibles).*

Observación: 1. La condición de ser "de tipo finito" es esencial en la demostración del teorema, como lo muestra el siguiente ejemplo:

Sea $A = \mathbb{Z}$ 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. Recordamos

que $\mathbb{Q}$ 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 $d_i|d_{i+1}$ 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" del teorema de estructura.

Demostración de la parte de unicidad del Teorema 6.4.7.

Sean $\{I_i\}_{1\leq i\leq n}$, $\{J_j\}_{1\leq j\leq m}$ sucesiones decrecientes de ideales propios de A tales que $\oplus_{i=1}^n A/I_i \cong \oplus_{j=1}^m A/J_j$. Sea $\mathcal{M}$ un ideal maximal cualquiera de A, a partir de $\oplus_{i=1}^n A/I_i \cong \oplus_{j=1}^m A/J_j$ obtenemos

$$\mathrm{Hom}_A(\oplus_{i=1}^n A/I_i, A/\mathcal{M}) \cong \mathrm{Hom}_A(\oplus_{j=1}^m A/J_j, A/\mathcal{M})$$

o bien,

$$\bigoplus_{i=1}^n \mathrm{Hom}_A(A/I_i, A/\mathcal{M}) \cong \bigoplus_{j=1}^m \mathrm{Hom}_A(A/J_j, A/\mathcal{M})$$

Consideramos los ideales transportadores $(\mathcal{M} : I_i) = \{a \in A \ / \ aI_i \subset \mathcal{M}\}$. Sea

$$\begin{aligned} \phi : (\mathcal{M} : I_i) &\to \mathrm{Hom}_A(A/I_i, A/\mathcal{M}) \\ a &\mapsto f_a = (\overline{x} \mapsto \overline{ax}) \end{aligned}$$

Es un ejercicio sencillo ver que es un epimorfismo, con núcleo $\mathcal{M}$, y por lo tanto que hay un isomorfismo $\mathrm{Hom}_A(A/I_i, A/\mathcal{M}) \cong (\mathcal{M} : I_i)/\mathcal{M}$.

Tomando $\mathcal{M}$ un ideal maximal que contenga a I_1, como los I_i estaban encajados, $\mathcal{M}$ contiene a todos los I_i, por lo tanto $(\mathcal{M} : I_i) = A \ \forall \ i = 1, \dots n$, y

$$(A/\mathcal{M})^n \cong \oplus_{j=1}^m (\mathcal{M} : J_j)/\mathcal{M}$$

Como $\mathcal{M} \subseteq (\mathcal{M} : J_j)$, esto implica que $(\mathcal{M} : J_j)$ o bien es $\mathcal{A}$ o bien es $\mathcal{M}$. Sea $q = \#\{j \ / \ (\mathcal{M} : J_j) = A\}$, entonces $(A/\mathcal{M})^n \cong (A/\mathcal{M})^q$ como A-módulo, luego son isomorfos como $A/\mathcal{M}$-espacios vectoriales, lo que implica $n = q \leq m$. Análogamente $m \leq n$, y por lo tanto son iguales.

Partimos ahora de $\oplus_{i=1}^n A/I_i \cong \oplus_{i=1}^n A/J_i$, con $I_i \supseteq I_{i+1}$ y $J_i \supseteq J_{i+1}$, para todo $i = 1, \dots n-1$.

Para cualquier elemento c de A, el isomorfismo anterior implica $\bigoplus_{i=1}^n c.A/I_i \cong \bigoplus_{i=1}^n c.A/J_i$. Utilizaremos el siguiente Lema:

Lema 6.4.11. *Sea A un anillo arbitrario, I un ideal de A y $c \in A$, entonces*

$$c.(A/I) \cong A/(I : c.A)$$

Demostración: Ejercicio.

Como los I_i formaban una sucesión decreciente, $(I_i : c.A) \supseteq (I_{i+1} : c.A)$, idem con los J_i. Sea $i_{\mathcal{A}} = max\{i \ / \ c \in I_i\}$ y sea $i_{\mathcal{B}} = max\{i \ / \ c \in J_i\}$, entonces

$$\bigoplus_{i=i_{\mathcal{A}}+1}^{n} A/(I_i : c.A) \cong \bigoplus_{i=i_{\mathcal{B}}+1}^{n} A/(J_i : c.A)$$

Por la primer parte de la demostración resulta que $i_{\mathcal{A}} = i_{\mathcal{B}}$, por lo tanto $I_i = J_i$ para todo i.

6.5. Ejercicios

1. Sea V un espacio vectorial sobre un cuerpo k, $dim_k(V) < \infty$ y $\phi : V \to V$ una transformación lineal. Convencerse del siguiente "diccionario":

Pares (V, ϕ)	$k[x]$-módulos
$\psi = \alpha\phi\alpha^{-1}$	$(V, \phi) \cong (V, \psi)$ (iso en ${}_{k[x]}mod$)
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
No existe ninguna base en la que ϕ se escriba en bloques	(V, ϕ) es un $k[x]$-módulo indescomponible, luego cíclico (por qué?)

2. **Teorema chino del resto**. Sea A un anillo conmutativo, $a_1, \ldots, a_n$ elementos de A. Llamemos $b_i = a_1.a_2 \ldots \widehat{a_i} \ldots a_n$ y supongamos que $1 = \sum_{i=1}^{n} t_i.b_i$ para ciertos elementos t_i. Sea $I = a_1.a_2 \ldots a_n.A$, $I_i = a_i.A$. $I \subseteq I_i$ luego A/I_i es un A/I-módulo para todo $i = 1, \ldots, n$. Demuestre que $A/I \cong \oplus A/I_i$.

3. Escribir el Teorema chino del resto en el caso $A = \mathbb{Z}$.

4. Sea (V, ϕ) un $k[x]$-módulo indescomponible, luego cíclico (¿porqué?), $(V, \phi) \cong k[x]/\langle p \rangle$. Si escribimos a $p = q_1^{\alpha_1} \ldots q_s^{\alpha_s}$ 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 $k[x]/\langle a_i \rangle$.

5. 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. Calcular $(\mathbb{Z} \oplus \mathbb{Z})/H$ donde $H = \{(x, y) \in \mathbb{Z} \oplus \mathbb{Z} \text{ tales que } 3x + 6y = 0\}$ (sugerencia: calcular una base de H que sea "múltiplo" de alguna base de $\mathbb{Z} \oplus \mathbb{Z}$).

7. Hallar una base de $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ que permita calcular $(\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z})/H$ donde $H = \{(x, y, z) \in \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \text{ tales que } 3x + 6y + 2z = 0, \text{ y } 2x - 4y = 0\}$. Calcule $(\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z})/H$. Encuentre "a ojo" algún morfismo de grupos con dominio $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ y núcleo H.

8. Listar las clases de isomorfismo de los grupos abelianos de orden 16, 18, 20, 189.

9. 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.

10. 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 esto se sugieren las siguientes cosas:

    a) 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.

    b) Considerar el grupo abeliano $G = (k - \{0\}, .)$, usar el teorema de estructura dar todas las posibilidades de G. A través de la traducción de la notación aditiva a la multiplicativa, relacione la cantidad de ceros que pueden tener en k los polinomios, y los órdenes de los elementos de G.

6.6. Formas de Jordan

Sea k un cuerpo algebraicamente cerrado y sea (V, ϕ) un $k[x]$-módulo. Sabiendo que los polinomios irreducibles son todos de la forma $(x-\lambda)$, a partir del teorema chino del resto en el contexto de polinomios (ejercicio 4 más arriba) se puede fácilmente demostrar que existe una base en la que ϕ se escribe en bloques de Jordan, es decir, en bloques de la forma $\begin{pmatrix} \lambda & 0 & 0 & \dots & 0 & 0 \\ 1 & \lambda & 0 & \dots & 0 & 0 \\ 0 & 1 & \lambda & \dots & \cdot & \cdot \\ 0 & 0 & 1 & \cdot & \cdot & \\ \cdot & \cdot & & & & \\ \cdot & \cdot & \dots & \dots & \lambda & 0 \\ 0 & 0 & \dots & \dots & 1 & \lambda \end{pmatrix}$.

En efecto, esto se consigue calculando en $k[x]/\langle (x-\lambda)^n \rangle$ la matriz del endomorfismo "multiplicar por x" en la base $\{\overline{1}, \overline{(x-\lambda)}, \overline{(x-\lambda)^2}, \dots, \overline{(x-\lambda)^{n-1}}\}$.

Ejercicios:

1. Exhibir un ejemplo de matrices de dos por dos tales que sus polinomios característicos coincidan, pero que no sean conjugadas.

2. Hallar *todos* los $\mathbb{C}[x]$-módulos M tales que $dim_{\mathbb{C}}(M) = 1, 2, 3$. Decir cuáles de ellos son cíclicos, indescomponibles, simples, suma de simples o suma de indescomponibles.

3. Hallar *todos* los $\mathbb{R}[x]$-módulos M tales que $dim_{\mathbb{R}}(M) = 1, 2, 3$. Decir cuáles de ellos son cíclicos, indescomponibles, simples, suma de simples o suma de indescomponibles.

4. 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 $DN = ND$.

7

Producto tensorial

7.1. Existencia y unicidad del producto tensorial

El producto tensorial de módulos es una construcción que permite "linealizar" funciones bilineales (o multilineales), más precisamente, dados dos A-módulos M_A y ${}_AN$ y un grupo abeliano P, consideramos las funciones $\phi : M \times N \to P$ tales que:

- ϕ es lineal en la primera variable: $\phi(m + m', n) = \phi(m, n) + \phi(m', n)$ para todo $m, m' \in M$, $n \in N$.
- ϕ es lineal en la segunda variable: $\phi(m, n + n') = \phi(m, n) + \phi(m, n')$ para todo $m \in M$, $n, n' \in N$.
- ϕ es A-balanceada: $\phi(ma, n) = \phi(m, an)$ para todo $a \in A$, $m \in M$ y $n \in N$.

Una tal función se llamará **bilineal A-balanceada**.

Los ejemplos básicos de este tipo de funciones son:

1. $M = N = P = A$, $\phi(a, b) = ab$ (producto en el anillo).
2. $M = A^{1\times n}$, $N = A^{n\times 1}$, $P = A$, $\phi((a_1, \ldots, a_n), (b_1, \ldots, b_n)) = \sum_{i=1}^{n} a_i b_i$.
3. $M = N = C(X)$ donde X es una subvariedad compacta de $\mathbb{R}^n$ y $P = \mathbb{R}$, $\phi(f, g) = \int_X f.g$.

4. N un A-módulo a izquierda, $M = N^*$, $\phi(f, m) = f(m)$.

5. Como subejemplo del anterior, si k es un anillo cualquiera y $N = k[x]$, tomamos $M = k^{\mathbb{N}_0}$ y en este caso $\phi(\{a_n\}, p) = \sum_{i=0}^{gr(p)} \lambda_i x^i = \sum_{i=1}^{gr(p)} a_i.\lambda_i$ es bilineal, A-balanceada.

El objetivo al construir el producto tensorial $M \otimes_A N$ es encontrar un objeto de tipo universal tal que sea lo mismo 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, que se busca un objeto $M \otimes_A N$ que verifique

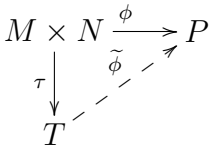
$$Bil^A(M \times N, P) \cong \mathrm{Hom}_{\mathbb{Z}}(M \otimes_A N, P)$$

donde $Bil^A(M \times N, P)$ denota precisamente a las funciones bilineales A-balanceadas de $M \times N$ en P.

Nos proponemos entonces mostrar que tal objeto existe y es único salvo isomorfismos de grupos abelianos.

Proposición 7.1.1. *Dados un A-módulo a derecha M_A y un A-módulo a izquierda ${}_AN$, existe un grupo abeliano T y una función $\tau : M \times N \to T$ con las siguientes propiedades:*

- *τ es bilineal y A-balanceada.*
- *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 $\phi = \widetilde{\phi}\tau$, es decir, se completa el siguiente diagrama en forma conmutativa:*



- *Si (T', τ') es un par con la misma propiedad, entonces $T \cong T'$ (isomorfismo de grupos abelianos).*

Demostración: *Existencia.* Construimos el objeto (T, τ) de la siguiente manera:

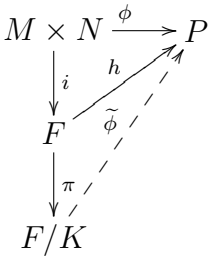
Sea $F = \mathbb{Z}^{(M\times N)}$ el $\mathbb{Z}$-módulo libre con base el conjunto $M \times N$ y sea K el subgrupo generado por los elementos de la forma

$$(m+m', n)-(m, n)-(m', n) \ ; \ (m, n+n')-(m, n)-(m, n') \ ; \ (ma, n)-(m, an)$$

donde $m, m' \in M$, $n, n' \in N$ y $a \in A$.

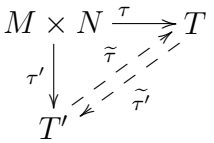
Definimos $T := F/K$ y denotamos por $m \otimes n$ a la clase de (m, n) en T. Definimos $\tau : M \times N \to T$ como $\tau(m, n) = m \otimes n$. Es claro, a partir de cómo se definió K, que τ es bilineal y A-balanceada, veamos que τ verifica además las otras propiedades:

Sea P un grupo abeliano y $\phi : M \times N \to P$ una función bilineal A-balanceada. Como F es libre con base $M \times N$, existe un único morfismo de $\mathbb{Z}$-módulos $h : F \to P$ (propiedad universal de la base) tal que el siguiente diagrama de líneas llenas conmuta:



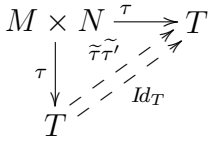
Como ϕ es bilineal y balanceada entonces ϕ se anula en K, por lo tanto induce una flecha $\widetilde{\phi}$ definida sobre el cociente, que verifica $\phi = \widetilde{\phi}\pi i = \widetilde{\phi}\tau$. Notar que $\widetilde{\phi}$ queda unívocamente determinada.

Unicidad. Sea (T', τ') un objeto con las mismas propiedades de (T, τ). Consideremos el siguiente diagrama



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, tenemos entonces que $\widetilde{\tau}\widetilde{\tau'} = Id_T$, análogamente se demuestra que $\widetilde{\tau'}\widetilde{\tau} = Id_{T'}$.

Notación: el grupo abeliano T se llama **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 con un conjunto de generadores $\{m \otimes n\}_{(m,n)\in M\times N}$ que verifican las relaciones

$$\begin{aligned}(m + m') \otimes n &= m \otimes n + m' \otimes n\\ m \otimes (n + n') &= m \otimes n + m \otimes n'\\ ma \otimes n &= m \otimes an\end{aligned}$$

Notar 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 en general una combinación lineal finita de ellos con coeficientes en $\mathbb{Z}$; los elementos de $M \otimes_A N$ de la forma $m \otimes n$ se denominan **tensores elementales**. Además, dado un elemento de $M \otimes_A N$, su escritura en términos de tensores elementales no es necesariamente única (por ejemplo $x' \otimes y + x \otimes y = (x + x') \otimes y$!).

Observación: Para todo $x \in M$, $x \otimes 0 = 0$, y análogamente $0 \otimes y = 0$ para todo $y \in N$. Veremos incluso que puede suceder $x \otimes y = 0$ sin que x sea cero ni que y sea cero, ya que por ejemplo $M \otimes_A N$ puede ser cero sin que M ni N lo sean (ver por ejemplo el caso $M = \mathbb{Z}_n$, $N = \mathbb{Q}/\mathbb{Z}$, $A = \mathbb{Z}$, descripto más adelante). Un ejemplo concreto es tomar un anillo A en donde exista un elemento x tal que $x^2 = 0$ sin que x sea cero, tomamos $M = N = A$, y es claro que $x \otimes x = 1.x \otimes x = 1 \otimes x^2 = 1 \otimes 0 = 0$.

Ejemplos:

1. $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}_n$ mediante la aplicación $\overline{x} \otimes y \mapsto \overline{xy}$, con inversa $\overline{x} \mapsto \overline{x} \otimes 1$. Observar que la buena definición de esta aplicación se sigue de la propiedad universal del producto tensorial aplicada a la función bilineal $\mathbb{Z}$-balanceada $\mathbb{Z}_n \times \mathbb{Z} \to \mathbb{Z}_n$ dada por $(\overline{x}, y) \mapsto \overline{xy}$.

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 la misma demostración que el ejemplo 1, tenemos que $M \otimes_A A \cong M$ (isomorfismo de grupos abelianos) bajo la aplicación que proviene de $(m, a) \mapsto m.a$, que tiene inversa $m \mapsto m \otimes 1$.

4. $k[x] \otimes_k k[y] \cong k[x, y]$ mediante la aplicación $p(x) \otimes q(y) \mapsto p(x)q(y)$. 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, si no, todo polinomio en dos variables sería un producto de dos polinomios, uno que depende de x y otro que depende de y. Sin embargo 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 $M \otimes_A N = 0$. Un ejemplo de este tipo es $\mathbb{Z}_{p^\infty} \otimes_{\mathbb{Z}} \mathbb{Z}_{p^\infty} = 0$.

6. Dados m y n naturales, $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m = \mathbb{Z}_{(m;n)}$ donde $(m; n)$ denota el máximo común divisor, en particular, si $(m; n) = 1$ tenemos que $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m = 0$.

Observación: dados M_A y ${}_AN$, dos A-módulos, y $M' \subseteq M$, $N' \subseteq N$ dos A-submódulos, se puede considerar $M \otimes_A N$ y $M' \otimes_A N'$, más aún, se tiene un morfismo de grupos abelianos inducido por las inclusiones $M' \otimes_A N' \to M \otimes_A N$, 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 $\mathbb{Q}/\mathbb{Z}$ bajo la inyección $\overline{1} \mapsto \overline{\frac{1}{2}}$. Sabemos que $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_2 \cong \mathbb{Z}_2$, por otro lado, $\mathbb{Q}/\mathbb{Z}$ es divisible y de torsión simultáneamente, por lo tanto $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$, luego ninguna aplicación $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_2 \to \mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}$ puede ser inyectiva.

Observación: Si A es un anillo, queda definido otro anillo A^{op}, cuyos elementos son los mismos que los de A, con operación suma también igual a la de A, pero con producto definido por $a._{op}b := ba$.

Se verifica sin dificultad (verificarlo!) que A^{op} resulta un anillo (con el mismo 1). Es claro que si A es conmutativo, $A = A^{op}$, también si M es un A-módulo a derecha, entonces es un A^{op}-módulo a izquierda (definiendo $a.m := ma$) y viceversa.

Proposición 7.1.2. *Si M es un A-módulo a derecha y N es un A-módulo a izquierda, entonces, con las estructuras de A^{op}-módulo comentadas anteriormente:*

$$\begin{aligned} M \otimes_A N &\cong N \otimes_{A^{op}} M \\ m \otimes n &\mapsto n \otimes m \end{aligned}$$

Demostración: Basta verificar que la función $f : M \times N \to N \otimes_{A^{op}} M$ definida por $f(m,n) = n \otimes m$ es bilineal y A-balanceada; análogamente la función $g : N \times M \to M \otimes_A N$ definida por $g(n,m) = m \otimes n$ 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, i.e. $n.g = n$ 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 $\phi(-).w$ aplicada a un vector v no es otra cosa que $\phi(v).w$, es bilineal y k-balanceada, por lo tanto induce un morfismo de grupos abelianos $V^* \otimes_k W \to \mathrm{Hom}_k(V,W)$. La imagen de $\phi \otimes w$ es $\phi(-)w$, que es una transformación lineal cuya imagen tiene dimensión 1 (siendo por ejemplo $\{w\}$ una base de la imagen). Vemos de esta manera 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, 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.

Si bien, dados M_A y ${}_AN$, $M \otimes_A N$ es sólo un grupo abeliano, en ciertos casos, este objeto tiene más estructura. En el ejemplo precedente, $V^* \otimes_k W$ resulta 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, veremos ahora como caso particular

que $M \otimes_A A$ tiene una estructura natural de A-módulo a derecha ($A \otimes_A N$ tiene una estructura natural de A-módulo a izquierda) y que los isomorfismos anteriores son de hecho isomorfismos de A-módulos.

Proposición 7.1.3. *Sean A, B, C tres anillos, ${}_AM_B$ 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

$$a(m \otimes n)c := (am) \otimes (nc)$$

y extendida por $\mathbb{Z}$-linealidad en $M \otimes_B N$. Es claro que esta aplicación está bien definida porque fijados a y c, la aplicación $M \times N \to M \otimes_B N$ definida por $(m, n) \mapsto (am) \otimes (nc)$ es bilineal B-balanceada. Se verifica 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 la estructura de A-C-bimódulo buscada.

Además, dados morfismos A-lineales $f : M \to M'$ y $g : N \to N'$, 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, luego determina un único morfismo de grupos abelianos, que llamamos $f \otimes g$, caracterizado por la igualdad $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$.

Ejemplos: Ver que los isomorfismos de grupos abelianos son de A-C-bimódulos para cada A y C convenientemente señalado:

1. Si M es un A-módulo a derecha, entonces $M \otimes_A A \cong M$, isomorfismo de $\mathbb{Z}$-A-bimódulos (idem con $A \otimes_A N \cong N$).

2. Si M es un A-módulo a derecha y N un A módulo a izquierda, se considera entonces 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 $M \otimes_A N \cong N \otimes_{A^{op}} M$ es un isomorfismo de $\mathcal{Z}(A)$-bimódulos. También $M \otimes_{\mathcal{Z}(A)} N \cong N \otimes_{\mathcal{Z}(A)} M$ 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 para cada par de números naturales r, s, el conjunto $A^{r\times s}$, con la suma y multiplicación usual de matrices tiene una estructura de $M_r(A) := A^{r\times r}$-módulo a izquierda y de $M_s(A)$-módulo a derecha. En particular, $A^{n\times 1}$ es un $M_n(A)$-A-bimódulo y $A^{1\times n}$ es un A-$M_n(A)$-bimódulo, y se tienen los siguientes isomorfismos:

   a) $A^{n\times 1} \otimes_A A^{1\times n} \cong A^{n\times n}$ como $M_n(A)$-$M_n(A)$-bimódulo.

   b) $A^{1\times n} \otimes_{M_n(A)} A^{n\times 1} \cong A$ como A-A-bimódulo.

   c) En general, $A^{n\times r} \otimes_{M_r(A)} A^{r\times s} \cong A^{n\times s}$ como $M_n(A)$-$M_s(A)$-bimódulo.

5. Si A es un anillo conmutativo y L es un A-módulo libre finitamente generado, M un A-módulo cualquiera, entonces $L^* \otimes_A M \cong \mathrm{Hom}_A(L, M)$.

7.2. Funtorialidad de $\otimes$

Dado un bimódulo ${}_AM_B$, se pueden definir dos funtores asociados a M:

$$\begin{array}{cc} - \otimes_A M : {}_C\mathrm{Mod}_A \to {}_C\mathrm{Mod}_B & M \otimes_B - : {}_B\mathrm{Mod}_C \to {}_A\mathrm{Mod}_C \\ X \mapsto X \otimes_A M & Z \mapsto M \otimes_B Z \\ f \mapsto f \otimes Id_M & g \mapsto Id_M \otimes g \end{array}$$

Como primer ejemplo, 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. En caso de ser X un A-B-bimódulo, entonces el isomorfismo precedente es también isomorfismo de A-B-bimódulos.

Como segundo ejemplo, 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, se tiene un isomorfismo

$$\begin{array}{c} A_S \otimes M \cong M_S \\ \dfrac{a}{s} \otimes m \mapsto \dfrac{am}{s} \end{array}$$

con inverso $\frac{am}{s} \mapsto \frac{1}{s} \otimes am$.

Como tercer ejemplo, si V es un $\mathbb{R}$-espacio vectorial, podemos considerar su complexificación: $V \oplus i.V$, que tiene una estructura obvia de $\mathbb{C}$-espacio vectorial (definiendo, para $a+bi \in \mathbb{C}$, $v+iw \in V \oplus i.V$, $(a+bi)(v+iw) := av - bw + i(bv+aw)$). 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 $a.b := f(a)b$ (idem para $b.a$), por lo tanto podemos 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 **extensión de escalares**. Si M es un A-módulo, $B \otimes_A M$ se llama el B-módulo extendido o inducido.

Enunciamos y demostramos algunas de las propiedades del funtor $M \otimes_A -$:

Proposición 7.2.1. *Dado un A-módulo derecha M, el funtor $M \otimes_A -$ preserva epimorfismos.*

Demostración: Sea $f : N \to N'$ un epimorfismo de A-módulos a izquierda, entonces $Id \otimes f : M \otimes_A N \to M \otimes_A N'$ es un epimorfismo pues todos los tensores elementales de $M \otimes_A N'$ están en la imagen $Id \otimes f$, y $M \otimes_A N'$ está generado por tensores elementales.

Observación: El funtor $M \otimes_A -$ no siempre preserva monomorfismos. Para ver esto exhibimos un contraejemplo:

Sea $f : \mathbb{Z}_2 \to \mathbb{Z}_4$ definido por $f(\overline{1}) = \overline{2}$. Consideramos el funtor $\mathbb{Z}_2 \otimes -$, y tenemos las siguientes identificaciones:

$$\begin{array}{ccc} \mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_2 & \xrightarrow{Id \otimes f} & \mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_4 \\ \| & & \| \\ \mathbb{Z}_2 & \xrightarrow{\quad g \quad} & \mathbb{Z}_2 \end{array}$$

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 $\overline{a} \otimes \overline{b} \mapsto \overline{ab}$. Obtenemos entonces

$$g(\overline{1}) = \mu((id \otimes f)(\overline{1} \otimes \overline{1})) = \mu(\overline{1} \otimes \overline{2}) = \overline{2} = 0$$

Esto dice que $Id \otimes f = 0$, que dista de ser monomorfismo. Sin embargo, se tiene la siguiente propiedad de exactitud a derecha:

Proposición 7.2.2. *Sea $N_1 \to^f N_2 \to^g N_3 \to 0$ una sucesión exacta de A-módulos a izquierda, entonces, para cualquier A-módulo a derecha M la sucesión de grupos abelianos*

$$M \otimes_A N_1 \xrightarrow{Id\otimes f} M \otimes_A N_2 \xrightarrow{Id\otimes g} M \otimes_A N_3 \longrightarrow 0$$

es exacta.

Demostración: Ya vimos que $Id\otimes g$ es un epimorfismo, también es claro que $(Id\otimes g)\circ(Id\otimes f) = 0$ pues $(Id\otimes g)\circ(Id\otimes f)(m\otimes n) = m\otimes g(f(n)) = m\otimes 0 = 0$, luego $\mathrm{Im}(Id\otimes f) \subseteq \mathrm{Ker}(Id\otimes g)$. Falta ver que $\mathrm{Ker}(Id\otimes g) \subseteq \mathrm{Im}(Id\otimes f)$.

Sea $\sum_i m_i\otimes n_i \in M\otimes N_2$ tal que $\sum_i m_i\otimes g(n_i) = 0$, esto no permite afirmar que cada $g(n_i) = 0$!. Sin embargo, podemos considerar $M\otimes_A N_2/\mathrm{Im}(Id\otimes f) = M\otimes_A N_2/\langle m\otimes f(n)\rangle$ y definimos $\widetilde{\phi} : M\times N_3 \to M\otimes_A N_2/\mathrm{Im}(Id\otimes f)$ por $\widetilde{\phi}(m,x) := \overline{m\otimes x'}$ donde $x'\in N_2$ es un elemento tal que $g(x') = x$ (recordar que g es epimorfismo). $\widetilde{\phi}$ está bien definida porque si x'' es otro elemento de N_2 tal que $g(x'') = x$, entonces $x' - x'' \in \mathrm{Ker}(g) = \mathrm{Im}(f)$, esto dice que existe $y\in N_1$ tal que $x' - x'' = f(y)$ y por lo tanto

$$\overline{m\otimes x''} = \overline{m\otimes x'' + m\otimes f(y)} = \overline{m\otimes x'' + m\otimes (x' - x'')} = \overline{m\otimes x'}$$

Ahora que sabemos que está bien definida, es claro que $\widetilde{\phi}$ es bilineal y A-balanceada, luego define un morfismo de grupos abelianos $\phi : M\otimes N_3 \to \frac{M\otimes_A N_2}{\mathrm{Im}(Id\otimes f)}$ que verifica, por construcción, que $\phi(m\otimes g(x')) = \overline{m\otimes x'}$, es decir, que $\phi\circ(\overline{Id\otimes g}) = Id_{\frac{M\otimes_A N_2}{\mathrm{Im}(Id\otimes f)}}$. Si ahora $w\in\mathrm{Ker}(Id\otimes g)$, entonces $w\in\mathrm{Im}(Id\otimes f)$ si y sólo si $\overline{w} = 0$ en $M\otimes_A N_2/\mathrm{Im}(Id\otimes f)$. Pero usando que $\phi\circ(\overline{Id\otimes g}) = Id_{\frac{M\otimes_A N_2}{\mathrm{Im}(Id\otimes f)}}$ tenemos que $\overline{w} = \phi(\overline{Id\otimes g}(\overline{w})) = \phi(\overline{(Id\otimes g)(w)}) = \phi(0) = 0$ 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*

$$N_1 \to^f N_2 \to^g N_3 \to 0$$

y una sucesión exacta de A-módulos a izquierda

$$M_1 \to^h M_2 \to^k M_3 \to 0$$

entonces la siguiente es una sucesión exacta de grupos abelianos

$$\mathrm{Im}(f)\otimes_A M_2 + N_2\otimes_A \mathrm{Im}(h) \xrightarrow{\gamma} N_2\otimes_A M_2 \xrightarrow{g\otimes k} N_3\otimes_A M_3 \longrightarrow 0$$

Demostración: es análoga al caso anterior, se deja como ejercicio (también queda como ejercicio ver la definición del morfismo γ).

Observación: Supongamos ahora que dada una sucesión exacta de A-módulos a izquierda $N_1 \to^f N_2 \to^g N_3 \to 0$ sabemos que para todo A-módulo a derecha M, la sucesión correspondiente $M \otimes_A N_1 \to M \otimes_A N_2 \to M \otimes_A N_3 \to 0$ es exacta. En particular, tomando $M = A$, la sucesión de grupos abelianos $A \otimes_A N_1 \to A \otimes_A N_2 \to A \otimes_A N_3 \to 0$ es exacta; pero sabemos que $A \otimes_A N_i \cong N_i$ como A-módulos a izquierda, y bajo esta identificación $Id \otimes f$ se corresponde con f (resp. g), luego la sucesión original es exacta.

Hay otra manera de demostrar estas propiedades de exactitud, que provienen de la relación entre el funtor producto tensorial y el Hom, que es lo que se llama *adjunción*, que veremos en la sección que viene. Esta propiedad tiene además la ventaja de poder 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. Se tiene 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: 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, entonces, para cada $y \in Y$, la aplicación $x \mapsto g(x \otimes y)$ es un morfismo de A-módulos de X en Z, por lo tanto se tiene definida 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, si $f : Y \to \mathrm{Hom}_A(X, Z)$, la fórmula $f(y)(x)$ depende linealmente tanto de y como de x, luego define una función bilineal $(x, y) \mapsto f(y)(x)$. Esta aplicación también verifica (ejercicio) $f(by)(x) = f(y)(xb)$, es decir es B-balanceada y por lo tanto define un único morfismo de grupos con dominio el producto tensorial $X \otimes_B Y$. Sigue como ejercicio la verificación de que esta aplicación es A-lineal, quedando entonces definida una función

$$\begin{aligned} \psi : \mathrm{Hom}_B(Y, \mathrm{Hom}_A(X, Z)) &\to \mathrm{Hom}_A(X \otimes_B Y, Z) \\ f &\mapsto ((x \otimes y) \mapsto f(y)(x)) \end{aligned}$$

Finalmente, queda como ejercicio ver que ϕ y ψ son uno el inverso del otro, y que además son C-lineales a derecha.

El segundo isomorfismo es completamente análogo.

Ejemplo: Sea A un anillo conmutativo, L un A-módulo libre finitamente generado, entonces (ejemplo precedente) $L^* \otimes_A M^* \cong \mathrm{Hom}_A(L, M^*)$, y a su vez

$$\mathrm{Hom}_A(L, M^*) = \mathrm{Hom}_A(L, \mathrm{Hom}_A(M, A)) \cong \mathrm{Hom}_A(M \otimes_A L, A) = (M \otimes_A L)^*.$$

A partir del teorema de adjunción, se obtiene una bonita 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 se tiene un isomorfismo de A-D-bimódulos $(M \otimes_B N) \otimes_C P \cong M \otimes_B (N \otimes_C P)$.*

Demostración: utilizaremos el hecho de que si se tienen dos A-D-bimódulos X e Y tales que para todo A-módulo Z, $\mathrm{Hom}_A(X, Z) \cong \mathrm{Hom}_A(Y, Z)$ (isomorfismo de D-módulos a derecha), entonces $X \cong Y$ (dejamos la demostración de este hecho como ejercicio).

Dado ahora un A-módulo cualquiera Z, por la adjunción tenemos los siguientes isomorfismos:

$$\begin{aligned} \mathrm{Hom}_A((M \otimes_B N) \otimes_C P, Z) &\cong \mathrm{Hom}_C(P, \mathrm{Hom}_A(M \otimes_B N, Z)) \\ &\cong \mathrm{Hom}_C(P, \mathrm{Hom}_B(N, \mathrm{Hom}_A(M, Z))) \\ &\cong \mathrm{Hom}_B(N \otimes_C P, \mathrm{Hom}_A(M, Z)) \\ &\cong \mathrm{Hom}_A(M \otimes_B (N \otimes_C P), Z) \end{aligned}$$

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 $X \otimes_A (\oplus_{i\in I} M_i) \cong \oplus_{i\in I}(X \otimes_A M_i)$, isomorfismo de B-módulos.*

Demostración: Utilizamos la propiedad universal de la suma directa. Recordamos que $\oplus_{i\in I} M_i$ 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 $\oplus_{i\in I} M_i$ queda definido a partir de sus restricciones a cada M_i, es decir, que la flecha natural

$$\begin{aligned} \mathrm{Hom}_A(\oplus_{i\in I} M_i, X) &\cong \prod_{i\in I} \mathrm{Hom}_A(M_i, X) \\ f &\mapsto \{f|_{M_i}\}_{i\in I} \end{aligned}$$

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:

$$\begin{array}{rcl} \mathrm{Hom}_B(X \otimes_A (\oplus_{i\in I} M_i), Z) & \cong & \mathrm{Hom}_A(\oplus_{i\in I} M_i, \mathrm{Hom}_B(X, Z)) \\ & \cong & \prod_{i\in I} \mathrm{Hom}_A(M_i, \mathrm{Hom}_B(X, Z)) \\ & \cong & \prod_{i\in I} \mathrm{Hom}_B(X \otimes_A M_i, Z) \end{array}$$

Esto dice que la aplicación $\mathrm{Hom}_B(X \otimes_A (\oplus_{i\in I} M_i), Z) \to \prod_{i\in I} \mathrm{Hom}_B(X \otimes_A M_i, Z)$ es una biyección, por lo tanto $X \otimes_A (\oplus_{i\in I} M_i)$ verifica 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. *Sea M un A-módulo, entonces $A^{(I)} \otimes_A M \cong M^{(I)}$. En particular, $A^{(I)} \otimes A^{(J)} \cong A^{(I\times J)}$.*

Sin embargo, el producto tensorial no conmuta en general con productos arbitrarios, es decir, que $(\prod_i M_i) \otimes_A N$ en general es distinto a $\prod_i (M_i \otimes_A N)$. Por supuesto, si el producto es finito, es cierto; exhibimos un contraejemplo:

Sea $A = k$ un cuerpo, consideremos $N = k^{(\mathbb{N})}$ y $M = N^* \cong k^{\mathbb{N}}$. Se tiene un morfismo natural $N^* \otimes_k N \to \mathrm{Hom}_k(k^{(\mathbb{N})}, k^{(\mathbb{N})})$ dado por $(\phi \otimes v)(w) := \phi(w)v$ donde $v, w \in k^{(\mathbb{N})}$ y $\phi \in \left(k^{(\mathbb{N})}\right)^*$. Si el producto tensorial conmutara con productos arbitrarios, tendríamos que $k^{\mathbb{N}} \otimes k^{(\mathbb{N})} \cong \left(k^{(\mathbb{N})}\right)^{\mathbb{N}}$, es decir,

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 $\left(k^{(\mathbb{N})}\right)^* \otimes k^{(\mathbb{N})}$, justamente la imagen de $\left(k^{(\mathbb{N})}\right)^* \otimes k^{(\mathbb{N})}$ en $\mathrm{Hom}_k(k^{(\mathbb{N})}, k^{(\mathbb{N})})$ consiste de las transformaciones lineales cuya imagen tiene dimensión finita. Una de las transformaciones lineales que no está en esta imagen es por ejemplo la identidad.

7.4. Módulos Playos

Vimos anteriormente que si $0 \to X \to Y \to Z \to 0$ es una sucesión exacta de A-módulos a izquierda y M es un A-módulo a derecha, entonces la correspondiente sucesión $M \otimes_A X \to M \otimes_A Y \to M \otimes_A Z \to 0$ 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* $0 \to X \to^f Y \to^g Z \to 0$ *una sucesión exacta corta de A-módulos a izquierda.*

- *Si* P *es un A-módulo a derecha libre, o más generalmente proyectivo, entonces* $0 \to P \otimes_A X \to P \otimes_A Y \to P \otimes_A Z \to 0$ *es exacta.*
- *Si la sucesión exacta se parte, y* M *es un A-módulo a derecha cualquiera, entonces la sucesión* $0 \to P \otimes_A X \to P \otimes_A Y \to P \otimes_A Z \to 0$ *se parte, y en particular es exacta.*

Demostración: 1. 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, entonces es un sumando directo de un libre, consideremos entonces Q tal que $P \oplus Q = L$ con L libre, entonces

$$\begin{array}{ccccccccc}
0 & \longrightarrow & L \otimes_A X & \longrightarrow & L \otimes_A Y & \longrightarrow & L \otimes_A Z & \longrightarrow & 0 \\
 & & \| & & \| & & \| & & \\
0 & \longrightarrow & (P \otimes_A X) \oplus (Q \otimes_A X) & \longrightarrow & (P \otimes_A Y) \oplus (Q \otimes_A Y) & \longrightarrow & (P \otimes_A Z) \oplus (Q \otimes_A Z) & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & P \otimes_A X & \xrightarrow{Id_P \otimes f} & P \otimes_A Y & \xrightarrow{Id_P \otimes g} & P \otimes_A Z & \longrightarrow & 0
\end{array}$$

Falta sólo ver que $Id_P \otimes f$ es monomorfismo, pero $Id_P \otimes f$ es la restricción a $(P \otimes_A X) \oplus (Q \otimes_A X)$ de $Id_L \otimes f$, que sabemos que es monomorfismo.
La parte 2. se deja como ejercicio.

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 esto identificamos el funtor $A_S \otimes_A -$ con el funtor de localización $(-)_S$. Consideremos entonces $f : M \to N$ un monomorfismo de A-módulos, queremos ver que $f_S : M_S \to N_S$ es un monomorfismo.

Sea $\frac{m}{s} \in \mathrm{Ker}(f_S)$, entonces $\frac{f(m)}{s} = 0$ en N_S, esto significa que existe $t \in S$ tal que $0.s = 0 = t.f(m)$ en N. Pero f es lineal, entonces $f(t.m) = 0$, lo que implica que $t.m = 0$ en M pues $f : M \to N$ es monomorfismo. Ahora bien, si $t.m = 0$ con $t \in S$, entonces $\frac{m}{s} = \frac{tm}{ts} = 0$ es M_S, luego $\mathrm{Ker}(f_S) = 0$ como queríamos ver.

Definición 7.4.2. *Un A módulo a derecha M se dice* **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 mas 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 restricción. 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

Definición: si k es un anillo conmutativo con uno, una *k-álgebra unitaria A*

es un anillo unitario A junto con un morfismo de anillos $k \to \mathcal{Z}(A)$. En particular A es un k-bimódulo simétrico.

1. *Algebra tensorial, simétrica y exterior*: Sea k un anillo conmutativo y V un k-módulo simétrico. Se define $T(V) = \oplus_{n\geq 0} V^{\otimes n}$ en donde se conviene que $V^{\otimes 0} := k$ y $V^{\otimes n+1} := V^{\otimes n} \otimes V$. Es obviamente un k-módulo, que resulta una k-álgebra con la multiplicación dada por la yuxtaposición (nombre: álgebra tensorial). Sea I_S el ideal bilátero generado por los elementos de la forma $v \otimes w - w \otimes v$ donde $v, w \in V$ y sea I_Λ el ideal bilátero generado por los elementos de la forma $v \otimes w + w \otimes v$. Se define $S(V) := T(V)/I_S$ y $\Lambda(V) = T(V)/I_\Lambda$, se llaman respectivamente el álgebra simétrica y el álgebra exterior. Notación: a la clase módulo I_S de $v_1 \otimes ... \otimes v_k$ se la denotará $v_1 ... v_k$ y a su clase módulo I_Λ se la denotará $v_1 \wedge ... \wedge v_k$. Ver 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

   $$\mathrm{Hom}_k(V, A) \cong \mathrm{Hom}_{k-alg}(T(V), A)$$

   si además A es conmutativa, entonces

   $$\mathrm{Hom}_k(V, A) \cong \mathrm{Hom}_{k-alg}(S(V), A)$$

   Si V es k-libre de base $\{x_1, ..., x_n\}$ demuestre que $S(V) \cong k[x_1, ..., x_n]$.

2. Sea k un cuerpo y $f : V \to V$ un endomorfismo de un espacio vectorial de dimensión finita, $dim_k(V) = n$. Ver que $\Lambda(V) = \oplus_{i=0}^{n} \Lambda^i(V)$ donde $\Lambda^i(V) = \mathrm{Im}(V^{\otimes i} \to \Lambda(V))$. Calcular la dimensión de cada $\Lambda^i(V)$, ver en particualar que $dim_k(\Lambda^n(V)) = 1$. Ver que $\Lambda(f) : \Lambda(V) \to \Lambda(V)$ (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, demuestre que $\Lambda^n(f) = det(f).Id_{\Lambda^n(V)}$. Deducir de lo anterior y de la funtorialidad de Λ^n que $det(g \circ f) = det(g).det(f)$.

3. Sea $S \subset A$ un subconjunto multiplicativamente cerrado de un anillo conmutativo A. Si M es un A_S-módulo a derecha y N es un A_S-módulo a izquierda (luego son también A-módulos), entonces $M \otimes_{A_S} N = M \otimes_A N$.

4. Sea M un A-módulo a derecha de torsión y N un A-módulo a izquierda divisible, entonces $M \otimes_A N = 0$. ¿Cuánto vale $G_{p^\infty} \otimes_{\mathbb{Z}} G_{p^\infty}$? Demuestre que el único producto (distributivo con respecto a la suma) que se puede definir en G_{p^∞} es $x.y = 0\ \forall x, y \in G_{p^\infty}$.

5. Si $(n;m) = 1$ entonces $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m = 0$.

6. Calcular $\mathbb{Z}_{p^n} \otimes_{\mathbb{Z}} \mathbb{Z}_{p^m}$.

7. Sea M un A-módulo proyectivo, entonces $A_S \otimes_A M$ es un A_S-módulo proyectivo.

8. Sea A un anillo conmutativo, M y N dos A-módulos playos (resp. proyectivos), entonces $M \otimes_A N$ es un A-módulo playo (resp. proyectivo).

9. Sea G un grupo y M un $\mathbb{Z}[G]$-módulo, es decir, un grupo abeliano con una acción de G sobre él. Sea $\mathbb{Z}$ el $\mathbb{Z}[G]$módulo definido por $g.n = n\ \forall n \in \mathbb{Z},\ g \in G$, entonces:

   a) $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M) \cong \{m \in M \ / \ g(m) = m \forall g \in G\} =: M^G$ (los invariantes).

   b) $\mathbb{Z} \otimes_{\mathbb{Z}[G]} M \cong M/\langle m - g(m) : \ m \in M,\ g \in G\rangle =: M_G$ (los coinvariantes) ($\langle \dots \rangle$ significa el generado como grupo abeliano).

   c) Deducir que $(-)^G$ y $(-)_G$ son dos funtores de $\mathbb{Z}[G]$-módulos en grupos abelianos, $(-)^G$ es exacto a izquierda y $(-)_G$ es exacto a derecha.

10. Demuestre que $\mathbb{Q}$ no es $\mathbb{Z}$-proyectivo.

11. Sea $0 \to M' \to M \to M'' \to 0$ una sucesión exacta de A-módulos.

    a) M' y M'' playos entonces M es playo.

    b) M y M'' playos entonces M' es playo.

    c) Dar un contraejemplo donde M' y M sean playos, pero que M'' no lo sea. (sugerencia: M' y M pueden incluso ser libres).

    Nota: 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.

12. Sea A un dominio íntegro,

    a) Probar que si M es un A-módulo playo, entonces M es sin torsión.

    b) Encuentre 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.

13. 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).

14. 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).

15. 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 $M_n(A) \otimes_k C \cong M_n(A \otimes C)$.

16. Sea A un anillo conmutativo, ver que si $A^{(I)} \cong A^{(J)}$ entonces el cardinal de I es igual al cardinal de J (sug.: usar $- \otimes_A A/\mathcal{M}$ donde $\mathcal{M}$ es algún ideal maximal de A).

17. Sea k un anillo conmutativo y sea $k - Algc$ la categoría de k-álgebras conmutativas (con morfismos los morfismos de anillos k-lineales). Si A y B son dos k-álgebras conmutativas, entonces $A \otimes_k B$ tiene estructura de k-álgebra definiendo $(a \otimes b)(c \otimes d) := ac \otimes bd$ y extendiendo por linealidad (para esto no hace falta que sean anillos conmutativos). Demostrar que las aplicaciones $i_A : A \to A \otimes_k B$ $(a \mapsto a \otimes 1_B)$ y $i_B : B \to A \otimes_k B$ $(b \mapsto 1_A \otimes b)$ hacen de $A \otimes_k B$ el coproducto de A y B en la categoría $k - Algc$.

18. Sean V y W dos k-módulos simétricos, demuestre que $S(V \oplus W) \cong S(V) \otimes_k S(W)$, en particular $k[x] \otimes_k k[y] \cong k[x,y]$.

19. Sea A una k-álgebra conmutativa, $M = A \otimes_k V$ donde V es un k-módulo. Demuestre que $T_A(M) \cong A \otimes T_k(V)$, $S_A(M) \cong A \otimes S_k(V)$ y $\Lambda_A(M) \cong A \otimes \Lambda_k(V)$, los isomorfismos son de k-álgebras.

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. Estos teoremas fueron demostrados por Kiiti 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

$$- \otimes_A P : \mathrm{Mod}_A \to \mathrm{Mod}_B \qquad ; \qquad - \otimes_B Q : \mathrm{Mod}_B \to \mathrm{Mod}_A$$

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 equivalencias. Componiéndolos, se obtienen funtores

$$\begin{array}{ll} \mathrm{Mod}_A \to \mathrm{Mod}_A & \mathrm{Mod}_B \to \mathrm{Mod}_B \\ \quad M \mapsto M \otimes_A (P \otimes_B Q) & \quad X \mapsto X \otimes_B (Q \otimes_A P) \end{array}$$

No hay ninguna razón *a priori* que permita 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 y ejercicio: 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 $G \circ F \cong Id_{\mathfrak{C}}$ y $F \circ G \cong Id_{\mathfrak{D}}$, 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 quasi-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 $F : \mathrm{Hom}_{\mathfrak{C}}(M, N) \cong \mathrm{Hom}_{\mathfrak{D}}(F(M), F(N))$. Esto es una consecuencia de que $G\circ F \cong Id_{\mathfrak{C}}$ y de que $F\circ G \cong Id_{\mathfrak{D}}$, 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 M un A-módulo cualquiera y X un B-módulo 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 $G(F(M)) \cong M$.

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 conserva objetos finitamente generados:

Sea 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 quasi-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 $J \subset I$ 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 sobreyectiva, 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, $F : {}_A\mathrm{Mod} \to {}_B\mathrm{Mod}$ 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.*

En particular, F preserva epimorfismos y G preserva monomorfismos, propiedad que ya conocíamos a partir del teorema anterior.

Para demostrar este teorema vamos a hacer uso del Lema 5.2.2, 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 5.2.2, $0 \to \mathrm{Hom}_A(T, G(X)) \to \mathrm{Hom}_A(N, G(X)) \to \mathrm{Hom}_A(M, G(X))$ 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 de lema anterior 5.2.2 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 análoga (o mejor dicho 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 $Q \otimes_B P \cong B$. 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, $P = G(B)$ 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. Tenemos 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:*

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 $i_N : N \subseteq M$ un submódulo, le asignamos $\mathrm{Im}(F(i_N) : F(N) \to F(M)) \subseteq F(M)$. 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 igual utilizando G en vez de F.

5. M es simple si y sólo si el conjunto de sus submódulos está formado por $\{\{0\}, M\}$. En este caso el conjunto de submódulos de $F(M)$ (utilizando 1.) está formado por $\{\{0\}, F(M)\}$ 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* $M_n(A)$ *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.) $\Leftrightarrow$ todo A-módulo (a izq.) es proyectivo $\Leftrightarrow$ 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 (o bien inyectivos).

8.2. Teoremas de Morita

Por razones de comodidad, durante esta sección consideraremos módulos a derecha en vez de 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. Sea A un anillo y B otro anillo tal 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. Sea 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 se puede preguntar si $M_n(A) \cong M_m(B)$ (isomorfismo de anillos) para algun $n, m \in \mathbb{N}$. 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 (ver ejercicio 1 del final de este capítulo) que todo funtor entre categorías de módulos que admite un adjunto (de algún lado) 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, 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.

Sea $f \in \mathrm{Hom}_A(M, N)$, $\phi \in \mathrm{End}_A(M)$ 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

$$F(\phi.f.\psi) = F(\phi) \circ F(f) \circ F(\psi)$$

Pero 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 demostrada 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 la comodidad de considerar módulos a

derecha, si no $\mathrm{End}_B({}_BB, {}_BB) \cong B^{op}$). 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 ellos, pues si observamos las fórmulas para F y G del teorema 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 del teorema 8.2.4, se tienen isomorfismos de funtores:*

$$F \cong (-) \otimes_B P \qquad ; \qquad G \cong (-) \otimes_A Q$$

Demostración: a partir del teorema 8.2.4 sabemos que $F \cong \mathrm{Hom}_A({}_BQ_A, -)$ y que y $G \cong \mathrm{Hom}_B({}_AP_B, -)$. Por otro lado, para cualquier bimódulo se tienen transformaciones naturales

$$(-) \otimes_A (Q)^{*A} \to \mathrm{Hom}_A({}_BQ_A, -) \qquad ; \qquad (-) \otimes_B (P)^{*B} \to \mathrm{Hom}_B({}_AP_B, -)$$

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, y es la simetría en la definición de equivalencia Morita. Resulta en principio un poco molesto el hecho de 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 mediante 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 (${}_A\mathrm{Mod}_A$ indica la categoría de A-A-bimódulos, idem 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 esto hay que demostrar versiones análogas a los teoremas 8.2.4 y 8.2.5 para módulos a izquierda, las demostraciones son similares, cuidando algunos detalles como por ejemplo que $\mathrm{Hom}_A({}_AA, {}_AA) \cong A^{op}$ en vez de 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:

$$\begin{array}{rcccl} \mathcal{Z}(A) & \cong & \mathrm{Hom}_{A-A}(A,A) & \cong & \mathrm{Hom}_{B-B}(Q \otimes_A A \otimes_A P, Q \otimes_A A \otimes_A P) \\ & \cong & \mathrm{Hom}_{B-B}(Q \otimes_A P, Q \otimes_A P) & \cong & \mathrm{Hom}_{B-B}(B,B) \cong \mathcal{Z}(B) \end{array}$$

y todos estos isomorfismos son de anillos.

Para el segundo punto, observamos que la categoría ${}_A\mathrm{Mod}_A$ se identifica con la categoría de ${}_{A^e}\mathrm{Mod}$ y con la de Mod_{A^e}, donde $A^e = A \otimes_{\mathbb{Z}} A^{op}$ (idem 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

$$\begin{array}{rcccl} A/[A,A] & \cong & A \otimes_{A^e} A & \cong & (P \otimes_B Q) \otimes_{A^e} (P \otimes_B Q) \\ & \cong & (Q \otimes_A P) \otimes_{B^e} (Q \otimes_A P) & \cong & B \otimes_{B^e} B \cong B/[B,B] \end{array}$$

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, por lo tanto es el nucleo de algún elemento del dual. Es conocido que $tr(M.N - N.M) = 0$, por lo tanto $[M_n(k), M_n(k)] \subseteq \mathrm{Ker}(tr)$, pero como tienen la misma dimensión entonces son 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 i$p \otimes \phi \mapsto (x \mapsto p.\phi(x))$,
- y 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:*

$$v(p \otimes q).p' = p.u(q \otimes p') \qquad ; \qquad u(q \otimes p).q' = q.v(p \otimes q')$$

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 $v \circ s$:

$$\begin{array}{rll} s(v(p \otimes q)) = & \sum_{i=1}^r v(p \otimes q)p_i \otimes q_i & = \sum_{i=1}^r p.u(q \otimes p_i) \otimes q_i = \\ = & \sum_{i=1}^r p \otimes u(q \otimes p_i)q_i & = \sum_{i=1}^r p \otimes q.v(p_i \otimes q_i) = \\ = & (p \otimes q) \sum_{i=1}^r v(p_i \otimes q_i) & = p \otimes q \end{array}$$

$$v(s(a)) = \sum_{i=1}^{r} v(a.p_i \otimes q_i) = a.\sum_{i=1}^{r} v(p_i \otimes q_i) = a$$

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 $e = e^2$. Consideramos 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 (i.e. que no tiene ideales biláteros no triviales). 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 en 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, en anillos nos interesarán particularmente las acciones de grupos que respeten la estructura de anillo. Sea entonces A un anillo y G un grupo finito que actúa en A por automorfismos de anillos, es decir, se tiene una aplicación

$$G \times A \to A$$
$$(g, a) \mapsto g(a)$$

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 $A = k^X = Func(X, k)$ 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

$$x.(ag) := g^{-1}(xa) \quad (a, x \in A,\ g \in G)$$

Definimos ahora dos morfismos:

$$\mu : P \otimes_{A^G} Q \to A \rtimes G \qquad \tau : Q \otimes_{A \rtimes G} P \to A^G$$
$$\mu(a \otimes b) := \sum_{g \in G} ag(b)g \qquad \tau(a \otimes b) := \sum_{g \in G} g(a.b)$$

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

$$\begin{array}{rcccl} \tau(x(ah) \otimes y) = & \tau(h^{-1}(xa) \otimes y) & = & \sum_{g \in G} g(h^{-1}(xa).y) \\ = & \sum_{g \in G} g.h^{-1}(xa.h(y)) & = & \sum_{g' \in G} g'(xah(y)) = \tau(x \otimes (ah).y) \end{array}$$

Veamos ahora la compatibilidad de μ y τ: sean $x, y, z \in A$ entonces

$$\begin{array}{rcl} x\mu(y\otimes z) = & x\left(\sum_{g\in G} yg(z)g\right) & = \sum_{g\in G} g^{-1}(xyg(z)) = \\ = & \sum_{g\in G} g^{-1}(xy)z & = \left(\sum_{g\in G} g^{-1}(xy)\right) z = \tau(x\otimes y)z \end{array}$$

Por otro lado

$$\begin{array}{rcl} \mu(x\otimes y)z = & \left(\sum_{g\in G} xg(y)g\right) z & = \sum_{g\in G} xg(y)g(z) = \\ & = \sum_{g\in G} xg(yz) & = x\left(\sum_{g\in G} g(yz)\right) = x\tau(y\otimes z) \end{array}$$

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 sub-bimódulo 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. *Sea 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 $a_1, \ldots, a_s, b_1, \ldots, b_s \in A$ tales que*

$$\sum_{i=1}^{s} a_i.g(b_i) = \begin{cases} 1 & si\ g = 1_G \\ 0 & si\ g \neq 1_G \end{cases}$$

Si la acción de un grupo G sobre un anillo A es Galois y $a_1, \ldots, a_s, b_1, \ldots, b_s$ 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

1. Sea $F : {}_A\mathrm{Mod} \to {}_B\mathrm{Mod}$ un funtor cualquiera. Ver que:
   a) F preserva productos finitos si y sólo si F preserva sumas finitas.
   b) 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).
2. Sea $F : \mathfrak{C} \to \mathfrak{D}$ un funtor entre dos categorías $\mathfrak{C}$ y $\mathfrak{D}$. 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 $\mathfrak{D}$, y ese isomorfismo es natural (sugerencia: demostrar primero que el ejercicio es equivalente a probar que existe un isomorfismo natural $\mathrm{Hom}_{\mathfrak{C}}(M, G(X)) \cong \mathrm{Hom}_{\mathfrak{C}}(M, G'(X))$ para todo objeto X de $\mathfrak{D}$ y M de $\mathfrak{C}$).
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.
4. Probar que si $A \sim_M B$ y $A' \sim_M B'$ entonces $A \times A' \sim_M B \times B'$ y que $A \otimes_{\mathbb{Z}} A' \sim_M B \otimes_{\mathbb{Z}} B'$.
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?
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 $k \times k$?

7. Sea G un grupo finito que actúa en un anillo A.

   a) (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.

   b) Probar que si A es noetheriano entonces $A \rtimes G$ es noetheriano.

   c) Concluir que si $|G| \in A$ y la acción es Galois, entonces A semisimple (resp. noetheriano) implica A^G semisimple (resp. noetheriano).

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 $\mathbb{C}$?

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.

   a) 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.

   b) Si consideramos a A como un objeto de ${}_{A^G}\mathrm{Mod}_{A \rtimes G}$, entonces ver que $A \otimes_{A \rtimes G} M \cong M^G$.

   c) 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.

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 $n \in \mathbb{N}$.

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). Calcular $\mathcal{Z}(A \rtimes G)$.

9

Categorías: construcciones universales, límites y colímites

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, como excusa de notación, varios ejemplos ilustrando la definición.

Definición 9.1.1. *Definir una categoría* $\mathfrak{C}$ *es dar los siguientes datos:*

- *Una clase (no necesariamente un conjunto) de objetos, que se denotará* $\mathrm{Obj}(\mathfrak{C})$.
- *Para cada par de objetos* X *e* Y *de* $\mathfrak{C}$*, un conjunto de flechas de* X *en* Y*, que se denotará* $\mathrm{Hom}_{\mathfrak{C}}(X,Y)$ *(o a veces* $[X,Y]$*, o* $[X,Y]_{\mathfrak{C}}$*, o* $\mathfrak{C}(X,Y)$*, o* $Mor[X,Y]$*).*

Estos satisfacen los siguientes axiomas:

C1: Si X*,* X'*,* Y*,* Y' *son objetos de* $\mathfrak{C}$ *y o bien* $X \neq X'$ *o bien* $Y \neq Y'$*, entonces* $\mathrm{Hom}_{\mathfrak{C}}(X,Y) \neq \mathrm{Hom}_{\mathfrak{C}}(X',Y')$.

C2: Para cada terna de objetos X, Y, Z de $\mathfrak{C}$ está definida una función que llamaremos composición

$$\begin{aligned} \mathrm{Hom}_{\mathfrak{C}}(Y,Z) \times \mathrm{Hom}_{\mathfrak{C}}(X,Y) &\to \mathrm{Hom}_{\mathfrak{C}}(X,Z) \\ (f,g) &\longmapsto f \circ g \end{aligned}$$

que es asociativa (en el sentido obvio).

C3: Para cualquier objeto X, existe un elemento de $\mathrm{Hom}_{\mathfrak{C}}(X,X)$ 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.

Ejemplos: Damos a continuación la notación para categorías usuales, señalando primero los objetos, y luego las flechas:

$\mathfrak{Sets}$ 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-$\mathfrak{AlgC}$ k-álgebras conmutativas.

$\mathfrak{C}^{op}$ Dada una categoría $\mathfrak{C}$, si definimos $\mathrm{Obj}(\mathfrak{C}^{op}) = \mathrm{Obj}(\mathfrak{C})$ y para cada par de objetos X e Y: $\mathrm{Hom}_{\mathfrak{C}^{op}}(X, Y) := \mathrm{Hom}_{\mathfrak{C}}(Y, X)$, y la composición $f \circ_{op} g := g \circ f$. Entonces $\mathfrak{C}^{op}$ resulta también una categoría, que se denomina la **categoría opuesta**.

Otros 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

$$\mathrm{Hom}(i, j) = \begin{cases} \{*\} & \text{si } i \leq j \\ \emptyset & \text{si } i \text{ y } j \text{ no están relacionados} \end{cases}$$

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 las flechas definidas como $\mathrm{Hom}(\{*\}, \{*\}) := M$ 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 $\mathfrak{C}$ una categoría, dos objetos X e Y de $\mathfrak{C}$ se dirán* **isomorfos** *si existen morfismos $f : X \to Y$ y $g : Y \to X$ tales que $f \circ g = Id_Y$ y $g \circ f = Id_X$, 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 junto con 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, pero 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 los conjuntos ordenados como objetos y las funciones creciente como morfismos. Si $(X, \leq)$ es un conjunto ordenado con una relación de orden no trivial (es decir, 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 $\mathfrak{C}_M$ 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 enunciada 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 $\mathfrak{C}$, 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 $\mathfrak{C}$, entonces f es un monomorfismo si y sólo si, para todo objeto Z la función de conjuntos*

$$\begin{aligned} f_* : \mathrm{Hom}_{\mathfrak{C}}(Z, X) &\to \mathrm{Hom}_{\mathfrak{C}}(Z, Y) \\ h &\mapsto f \circ h \end{aligned}$$

es inyectiva.

La noción de monomorfismo categórico en la categoría de módulos, o de grupos, coincide con la noción de monomorfismo definida anteriormente. Como ejemplos extremos podemos comentar que todo isomorfismo es un monomorfismo (verificarlo!), y en categorías en 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 también 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 esto, 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 $\mathfrak{C}$ no es otra cosa que la misma definición pero enunciada en la categoría $\mathfrak{C}^{op}$.

Definición 9.1.6. *Sea $f : X \to Y$ un morfismo en una categoría $\mathfrak{C}$, 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 $\mathfrak{C}$. Son equivalentes:*

1. *f es un epimorfismo.*
2. *Para todo objeto Z, la función de conjuntos*

$$\begin{aligned} f^* : \mathrm{Hom}_{\mathfrak{C}}(X, Z) &\to \mathrm{Hom}_{\mathfrak{C}}(Y, Z) \\ h &\longmapsto h \circ f \end{aligned}$$

   es inyectiva.

3. *$f \in \mathrm{Hom}_{\mathfrak{C}}(X, Y) = \mathrm{Hom}_{\mathfrak{C}^{op}}(Y, X)$ en un monomorfismo en $\mathfrak{C}^{op}$.*

Todo isomorfismo es un epimorfismo. En la categoría de conjuntos, un epimorfismo es lo mismo que una función suryectiva (verificarlo!), lo mismo para la categoría de módulos (ver Proposición 3.4.4 del capítulo 3).

Ejemplos: / Ejercicios:

1. En la categoría de espacios métricos como objetos y funciones continuas como morfismos, las 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. La siguiente construcción puede utilizarse para mostrar que, en la categoría de grupos, un epimorfismo categórico es siempre una suryección:

   Sea G un grupo y H un subgrupo de G. Llamemos X al conjunto de clases a izquierda de G/H. La multiplicación a derecha por elementos de G permuta estas clases, luego X es un G espacio. Si llamamos $K := \mathbb{Z}_2^X$ al grupo aditivo de las funciones de X en $\mathbb{Z}_2$, entonces G actúa por automorfismos de grupo en K, y se puede formar el producto semidirecto de K con G a través de esta acción. Se tiene siempre definido un morfismo que llamaremos $\alpha : G \to K \rtimes G$ dado por $g \mapsto (0, g)$.

   Llamemos δ a la función que vale 1 en la clase de H y cero en las demás, definimos la función $\beta : G \to K \rtimes G$ a través de $g \mapsto (\delta - g(\delta), g)$.

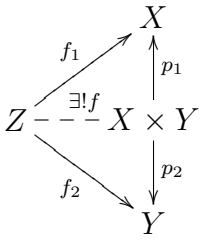
   Esta función es un morfismo de grupos (verificarlo!) y además los elementos de G en donde α es igual a β son exactamente los elementos en donde $\delta = g(\delta)$. Como g actúa permutando las clases a través de la multiplicación a derecha, la clase de H es igual a la clase de $H.g$ si y sólo si $g \in H$. Esto dice que si componemos α ó β con la inclusión $H \to G$, entonces estos morfismos coinciden. Si suponemos ahora que la inclusión $H \hookrightarrow G$ es un epimorfismo categórico, debería valer $\alpha = \beta$ sobre todo G, pero como α coincide con β exactamente en H resulta $G = H$.

4. 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 $f : Z \to X \times Y$, para un $z \in Z$, $f(z) \in X \times Y$, 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 $\mathfrak{C}$, obteniéndose:

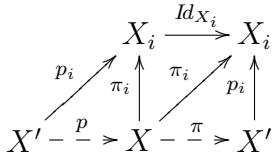
Definición 9.2.1. *Dados $\{X_i\}_{i \in I}$ una familia de objetos de una categoría $\mathfrak{C}$ indexados por un conjunto I, se define un* **producto directo** $\prod_{i \in I} X_i$ *como un objeto de $\mathfrak{C}$ con las siguientes dos propiedades:*

- *$\forall j \in I$, existe un morfismo $p_j : \prod_{i \in I} X_i \to X_j$.*
- *(Propiedad universal) Si $Z \in \mathrm{Obj}(\mathfrak{C})$ 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 $\{X_i\}_{i \in I} \in \mathfrak{C}$, si un objeto producto existe, entonces es único a menos de isomorfismo, por lo tanto uno puede hablar (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

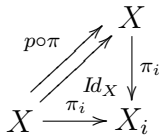
flechas $p_i : X' \to X_i$ queda definida una única flecha $p : X' \to X$ tal que $\pi_i \circ p = p_i$. Simétricamente, como X' también es un producto, usando las flechas $\pi_i : X \to X_i$ queda definida una única flecha $\pi : X \to X'$ tal que $p_i \circ \pi = \pi_i$.



Afirmamos que estos morfismos son isomorfismos, uno el inverso del otro. Para ver esto, consideramos la composición $p \circ \pi : X \to X$, al calcular la composición con las proyecciones tenemos las igualdades:

$$\pi_i \circ (p \circ \pi) = (\pi_i \circ p) \circ \pi = p_i \circ \pi = \pi_i = \pi_i \circ Id_X$$

Es decir, el diagrama siguiente con cualquiera de las dos flechas conmuta



Luego, por unicidad, tiene que ser $p \circ \pi = Id_X$. La otra composición es análoga.

Todo morfismo $f : X \to Y$ entre dos objetos de una categoría $\mathfrak{C}$ induce, por composición, para cada objeto Z de $\mathfrak{C}$, una función entre los conjuntos $f_* : \mathrm{Hom}_{\mathfrak{C}}(Z, X) \to \mathrm{Hom}_{\mathfrak{C}}(Z, Y)$. 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 $(p_j)_* : \mathrm{Hom}_{\mathfrak{C}}(Z, \prod_{i\in I} X_i) \to \mathrm{Hom}_{\mathfrak{C}}(Z, X_j)$. 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 $\mathfrak{C}$ 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* $\mathfrak{C}$ *si y sólo si la función natural*

$$\prod_{i\in I}(p_i)_* : \mathrm{Hom}_{\mathfrak{C}}(Z, \prod_{i\in I} X_i) \to \prod_{i\in I} \mathrm{Hom}_{\mathfrak{C}}(Z, X_i)$$
$$f \mapsto \{p_i \circ f\}_{i\in I}$$

es una biyección para todo $Z \in \mathrm{Obj}(\mathfrak{C})$.

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 los Hom sea inyectiva.

Ejemplos: En la categorías de conjuntos, módulos sobre un anillo, anillos, grupos (conmutativos o no), el producto categórico es el producto cartesiano, pero esto 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, dado $V = \oplus_{n\in\mathbb{Z}} V_n$ y $W = \oplus_{n\in\mathbb{Z}} W_n$ dos espacios vectoriales graduados, $\mathrm{Hom}_{\mathfrak{C}}(V, W) = \{f : V \to W$ transformaciones 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 $\oplus_{n\in\mathbb{Z}}(\prod_{i\in I} V^i_n)$ 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 $k^{(\mathbb{Z})}$.

Otro ejemplo en donde el producto no se calcula con 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

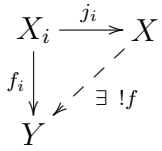
Definición 9.2.3. *Sea $\{j_i : X_i \to X\}_{i\in I}$ una familia de morfismos en una categoría $\mathfrak{C}$ indexada por un conjunto I, diremos que X (junto con los morfismos j_i) es el* **coproducto** *de los X_i si y sólo si la familia $\{j_i : X \to X_i\}_{i\in I}$ es un producto en la categoría $\mathfrak{C}^{op}$, se denotará $X := \coprod_{i\in I} X_i$.*

Con demostración obvia, se tiene la siguiente proposición:

Proposición 9.2.4. *Dada $\{X_i\}_{i\in I}$ una familia de objetos de $\mathfrak{C}$, 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 $\mathfrak{C}$, X un objeto de $\mathfrak{C}$ y $j_i : X_i \to X$ morfismos; son equivalentes:*

- *X es el coproducto de los X_i.*
- *Para cualquier objeto Y de $\mathfrak{C}$ 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 $\mathfrak{C}$, la función natural*

$$\prod_{i\in I} j_i^* : \mathrm{Hom}_{\mathfrak{C}}(X, Y) \to \prod_{i\in I} \mathrm{Hom}_{\mathfrak{C}}(X_i, Y)$$

es una biyección.

Demostración: se deja como ejercicio.

Ejemplos: / Ejercicios:

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.

9.2.3. Objeto inicial, objeto final, Ker y Coker

En una categoría $\mathfrak{C}$, un objeto I se denomina **inicial** en caso de que, dado cualquier otro objeto X de $\mathfrak{C}$, exista un único morfismo $I \to X$. Como es de esperar, un objeto inicial, si existe, es único salvo isomorfismo. Para ver esto, 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, $Id_I : I \to I$, luego por unicidad, $j \circ i = Id_I$. La cuenta para ver que $i \circ j = Id_J$ 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 conmutativos), $\mathbb{Z}$ 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 (que, naturalmente, podría no existir).

Dualmente, un objeto F en $\mathrm{Obj}(\mathfrak{C})$ se llama objeto **final** si, para cualquier otro objeto X de $\mathfrak{C}$ existe un único morfismo $X \to F$.

Ejercicio: Dada una categoría $\mathfrak{C}$, un objeto F es final si y sólo si F es un objeto inicial en $\mathfrak{C}^{op}$. Si una categoría $\mathfrak{C}$ 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, $\mathfrak{C}$ tiene objeto 0 si y sólo si $\mathfrak{C}^{op}$ tiene objeto cero, y el cero de $\mathfrak{C}$ sirve como cero de $\mathfrak{C}^{op}$.

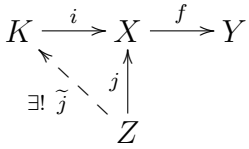
Observación: Si $\mathfrak{C}$ es una categoría con objeto cero, entonces, dado un par de objetos X e Y, el conjunto $\mathrm{Hom}_{\mathfrak{C}}(X, Y)$ nunca es vacío pues siempre existe el morfismo composición:

$$X \to 0 \to Y$$

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 $\mathfrak{C}$ 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 $ker(f)$.

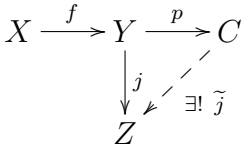
Comparando esta definición con la propiedad universal del núcleo en el contexto de grupos y de módulos, vemos que la noción de núcleo categórico dada aquí coincide, en estos casos, con la noción de núcleo habitual.

La noción de conúcleo es dual a la de núcleo:

Definición 9.2.7. *Sea $f : X \to Y$ un morfismo en una categoría $\mathfrak{C}$ 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 $\widetilde{j} \circ p = j$, en diagramas:*



Ejercicio: Dada $f : X \to Y$, un morfismo $p : Y \to C$ es un conúcleo de f si y sólo si $p : C \to Y$ es un núcleo, en $\mathfrak{C}^{op}$ de $f : Y \to X$. 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 $\pi : N \to N/\mathrm{Im}(f)$. En la categoría de grupos, si $f : G \to H$ es un morfismo de grupos, el conúcleo es la proyección al cociente $H \to H/N(\mathrm{Im}(f))$, donde $N(\mathrm{Im}(f))$ es el normalizador de $\mathrm{Im}(f)$ en H, es decir, el subgrupo normal más chico que contiene a $\mathrm{Im}(f)$ (que eventualmente puede contener estrictamente a $\mathrm{Im}(f)$).

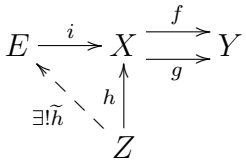
Si $f : (X, x_0) \to (Y, y_0)$ es un morfismo en la categoría $\mathfrak{Sets}_0$ (es decir, $f : X \to Y$ es una función tal que $f(x_0) = y_0$), se puede comprobar fácilmente que $\mathrm{Ker}(f) = (\{x \in X \ / \ f(x) = y_0\}, x_0)$, y $\mathrm{Coker}(f) = (Y/\sim, \overline{y_0})$ donde la relación 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 $\mathfrak{C}$. 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* $h = i \circ \widetilde{h}$



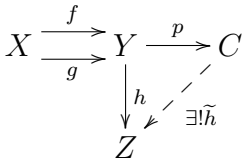
Ejercicios:

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* $\mathfrak{C}$*. Llamaremos un* **coegalizador** *de* f *y* g *a un objeto* C *provisto de un morfismo* $p : Y \to C$ *tal que* $p \circ f = p \circ g$*, 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 $y \sim y' \Leftrightarrow \exists\ x \in X$ 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 $(m_1, m_2) \in M_1 \oplus M_2$ va a parar a cero en M, significa que $m_1 + m_2 = 0$, o lo que es lo mismo $m_1 = -m_2$, y 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 $(f_1 \oplus f_2)(m, -m) = 0 \ \forall \ m \in M_1 \cap M_2 \quad \Leftrightarrow \quad f_1(m) + f_2(-m) = 0 \ \forall \ m \in M_1 \cap M_2$, o lo que es equivalente, que f_1 y f_2 coincidan en donde coinciden sus dominios.

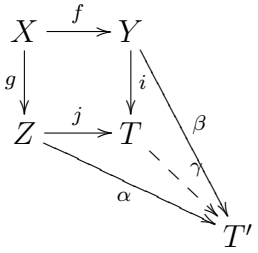
Esta noción, de construir un objeto a través de dos partes, pero que pueden tener relaciones entre ellas, es la que se formaliza categóricamente a través de la definición de push-out:

Definición 9.2.10. *Sean $f : X \to Y$ y $g : X \to Z$ dos morfismos (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 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:*



Notación: 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 $\mathfrak{C}$ con coproductos, X e Y dos objetos de $\mathfrak{C}$, entonces el pushout de $\begin{array}{ccc} I & \longrightarrow & X \\ \downarrow & & \\ Y & & \end{array}$ es $X \coprod Y$.

3. Sea $\mathfrak{C}$ 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 sucesión $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$ es exacta.

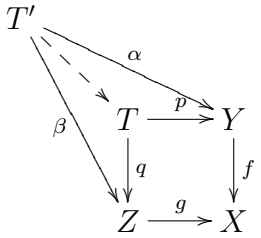
6. Describir al coegalizador como la "composición" de dos push-outs.

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 (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 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:*



Notación: 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 $\mathfrak{C}$ 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 $\mathfrak{C}$. Ver que es un cuadrado push-out (respectivamente pull-back) si y sólo si para todo objeto W en $\mathfrak{C}$, aplicando $\mathrm{Hom}_{\mathfrak{C}}(-, W)$ (respectivamente $\mathrm{Hom}_{\mathfrak{C}}(W, -)$) 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 $\begin{array}{ccc} X & \xrightarrow{Id} & X \\ {\scriptstyle Id}\downarrow & & \downarrow{\scriptstyle f} \\ X & \xrightarrow{f} & Y \end{array}$ es un pull-back.

6. Enunciar y demostrar la versión dual del ejercicio anterior, con epimorfismos y push-outs.

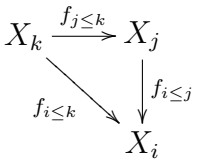
9.2.6. Límites

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 a la noción de coproducto, coegalizador y objeto inicial.

Para fijar ideas, comenzamos con la construcción del límite en la categoría de conjuntos:

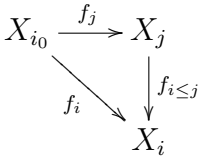
Consideremos un conjunto parcialmente ordenado $(I, \leq)$ (que puede ser vacío), una familia de conjuntos $\{X_i\}_{i \in I}$ y por cada $i \leq j$ una función $f_{i \leq j} : X_j \to X_i$. A estos datos les pedimos la siguiente condición de compatibilidad: si $i \leq j \leq k$, entonces $f_{i \leq j} \circ f_{j \leq k} = f_{i \leq k}$ 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:

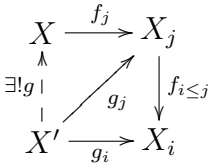


A un conjunto de datos con esas propiedades se lo llamará un **sistema proyectivo**. Notemos que si elegimos una familia de funciones entre varios conjuntos, esta familia siempre está parcialmente ordenada diciendo que una función f es menor o igual que otra función g si y sólo si son "componibles", 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

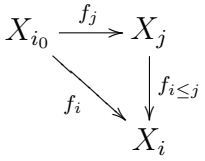


sean conmutativos, y además, que este conjunto X_{i_0} sea lo más grande posible, es decir, que si un conjunto X' tiene definidas funciones $g_i : X' \to X_i$ compatibles con la relación de orden de I, entonces estas funciones se factoricen a través de X (ver diagrama).



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 $\varprojlim_{\leftarrow I} X_i$ a este subconjunto del producto, y definimos $f_i : \varprojlim_{\leftarrow I} X_i \to X_i$ a la composición de la inclusión del límite en el producto con la proyección en la coordenada i-ésima:

$$\varprojlim_{\leftarrow I} X_i \hookrightarrow \prod_{i\in I} X_i \longrightarrow X_i$$

Por construcción, queda demostrada la siguiente proposición:

Proposición 9.2.12. *(Propiedad universal del límite) Sea 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 $f_i : \varprojlim_{\leftarrow I} X_i \to X_i$ 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 $g : Y \to \varprojlim_{\leftarrow I} X_i$ 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. *Dado 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, $\mathrm{Hom}_{\mathfrak{C}}(Y, X)$ es el límite (en la categoría de conjuntos) del sistema proyectivo $\{(f_{i\leq j})_* : \mathrm{Hom}_{\mathfrak{C}}(Y, X_j) \to \mathrm{Hom}_{\mathfrak{C}}(Y, X_i)\}$.*

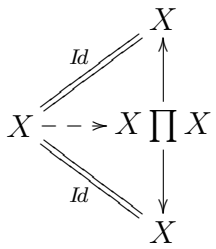
Ejemplos: / Ejercicios:

1. Consideremos, en una categoría cualquiera, un diagrama $\begin{array}{ccc} & & X_1 \\ & & \downarrow{\scriptstyle f} \\ X_2 & \xrightarrow{g} & X_3 \end{array}$.
   Definimos 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 $\mathfrak{C}$ 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 $Id_i = f_{i\leq i}$. Entonces el límite de este sistema proyectivo coincide con el producto de los X_i.

3. Sea I el conjunto vacío, entonces $\lim\limits_{\leftarrow \emptyset}$ es un objeto final.

4. Los coegalizadores pueden calcularse a partir de dos límites consecutivos, de hecho, a partir de dos pull-backs consecutivos:
   Sean $f, g : X \to Y$ y consideremos el pull back $\begin{array}{ccc} X \prod_Y X & \longrightarrow & X \\ \downarrow & & \downarrow{\scriptstyle g} \\ X & \xrightarrow{f} & Y \end{array}$.
   Si estuvieramos 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 egal-

izador 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 también 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 los naturales con el orden usual. En la categoría de anillos llamamos $k[x]_{\leq n} := k[x]/\langle x^{n+1}\rangle$ a los polinomios truncados en grado n. Si $n \leq m$, $f_{n\leq m:}k[x]_{\leq m} \to k[x]_{\leq n}$ denota la proyección canónica, probar que $\lim\limits_{\leftarrow n} k[x]_{\leq n} = k[|x|]$, las series de potencias formales con coeficientes en k.

7. Sea I un conjunto parcialmente ordenado que tiene máximo, es decir que existe $i_0 \in I$ tal que i_0 es comparable con todo elemento de I y además $i_0 \leq i \; \forall \; i \in I$. 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. *Sea I un conjunto parcialmente ordenado, $\{X_i\}_{i\in I}$ una familia de objetos de una categoría dada $\mathfrak{C}$, 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 junto con los morfismos $f_{i\leq j}$ se denominará un* **sistema inductivo** *en caso de que verifiquen 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 y* $\{f_{i\leq j} : X_i \to X_j\}$ *un sistema inductivo en una categoría* $\mathfrak{C}$.

1. *Si un límite directo existe, es único salvo isomorfismo.*
2. *Un límite directo en una categoría* $\mathfrak{C}$ *es lo mismo que un límite inverso en la categoría opuesta.*
3. *Dado un objeto cualquiera* Y, *el sistema* $\{(f_{i\leq j})^* : \mathrm{Hom}_{\mathfrak{C}}(X_j, Y) \to \mathrm{Hom}_{\mathfrak{C}}(X_i, Y)\}$ *es un sistema proyectivo. Un objeto* X *es un límite directo de los* X_i *si y sólo si* $\mathrm{Hom}_{\mathfrak{C}}(X, Y)$ *es el límite inverso (en la categoría de conjuntos) de los* $\mathrm{Hom}_{\mathfrak{C}}(X_i, Y)$ *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 la inclusión, y se consideran como morfismos también las inclusiones, entonces $\lim\limits_{\to I} X_i = \cup_{i\in I} X_i$.

9.3. Funtores

9.3.1. Definición y ejemplos

Una vez definido el concepto de categoría, en donde se tiene 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* $\mathfrak{C}$ *y* $\mathfrak{D}$ *dos categorías, un* **funtor** F *de* $\mathfrak{C}$ *en* $\mathfrak{D}$, *que denotaremos* $F : \mathfrak{C} \to \mathfrak{D}$, *es el siguiente par de datos:*

- *Una asignación, para cada objeto X de $\mathfrak{C}$, de un objeto $F(X)$ de $\mathfrak{D}$.*
- *Para cada par de objetos X e Y de $\mathfrak{C}$, una función*

$$F_{X,Y} : \mathrm{Hom}_{\mathfrak{C}}(X, Y) \to \mathrm{Hom}_{\mathfrak{D}}(F(X), F(Y)).$$

Verificando los siguientes dos axiomas:

F1: Si $g : X \to Y$ y $f : Y \to Z$ son dos morfismos en $\mathfrak{C}$, entonces $F(f \circ g) = F(f) \circ F(g)$.

F2: Para todo objeto X de $\mathfrak{C}$, $F(Id_X) = Id_{F(X)}$.

Nombres: 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 $F_{X,Y} : \mathrm{Hom}_{\mathfrak{C}}(X, Y) \to \mathrm{Hom}_{\mathfrak{D}}(F(Y), F(X))$ 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:

- $\mathcal{O} : \mathfrak{G} \to \mathfrak{Sets}$, 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.
- $\mathcal{O} : {}_A\mathrm{Mod} \to \mathfrak{Sets}$, 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, $\mathcal{O}(f) = f$.
- 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.
- 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 está bien definida la aplicación de grupos (abelianos) $\overline{f} : G/[G, G] \to G'/[G', G']$. Queda como ejercicio demostrar la funtorialidad de Ab (es decir, que $\overline{f \circ g} = \overline{f} \circ \overline{g}$ y que $\overline{Id_G} = Id_{G/[G,G]}$).

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?

Más ejemplos:

1. Si X es un objeto fijo en una categoría $\mathfrak{C}$, entonces se tienen dos funtores en la categoría de conjuntos:

   - $\mathrm{Hom}_{\mathfrak{C}}(X, -) : \mathfrak{C} \to \mathfrak{Sets}$ (covariante)

   $$\begin{aligned} Y &\mapsto \mathrm{Hom}_{\mathfrak{C}}(X, Y) \\ (f : Y \to Z) &\mapsto \big(f_* : \mathrm{Hom}_{\mathfrak{C}}(X, Y) \to \mathrm{Hom}_{\mathfrak{C}}(X, Z)\big) \end{aligned}$$

   donde, si $\phi : X \to Y$, $f_*(\phi) : X \to Z$ está definido por $f \circ \phi$.

   - $\mathrm{Hom}_{\mathfrak{C}}(-, X) : \mathfrak{C} \to \mathfrak{Sets}$ (contravariante)

   $$\begin{aligned} Y &\mapsto \mathrm{Hom}_{\mathfrak{C}}(Y, X) \\ (f : Y \to Z) &\mapsto \big(f^* : \mathrm{Hom}_{\mathfrak{C}}(Z, X) \to \mathrm{Hom}_{\mathfrak{C}}(Y, X)\big) \end{aligned}$$

   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 $\mathfrak{Top}$ se pueden definir dos funtores "extremos", usando la topología discreta: $X \mapsto (X, \mathcal{P}(X))$, o la indiscreta: $X \mapsto (X, \{\emptyset, X\})$.

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 $F_1, F_2 : \mathfrak{C} \to \mathfrak{D}$ dos funtores (covariantes) entre dos categorías $\mathfrak{C}$ y $\mathfrak{D}$. Dar un* **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 $\mathfrak{C}$, con la propiedad siguiente:*
Si $f : X \to Y$ es un morfismo en $\mathfrak{C}$ 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.

Nota: si los funtores F_1, F_2 son contravariantes, se dirá que $\eta : F_1 \to F_2$ es una transformación natural si es conmutativo el diagrama

$$\begin{array}{ccc} F_1(X) & \xleftarrow{F_1(f)} & F_1(Y) \\ {\scriptstyle \eta_X}\downarrow & & \downarrow{\scriptstyle \eta_Y} \\ F_2(X) & \xleftarrow{F_2(f)} & F_2(Y) \end{array}$$

para todo morfismo $f : X \to Y$. Si η_X es un isomorfismo para todo objeto X de $\mathfrak{C}$ (sea caso contravariante o 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 $F_1 = Id$ y $F_2 = (-)^{**}$.

2. Sabemos que dados dos anillos A, B y (bi)módulos ${}_AX_B$, ${}_BY$, ${}_AZ$ 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 X e Y y consideramos 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. Sea 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 los funtores $Z \otimes_A -$ 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 $sq : \mathfrak{Sets} \to \mathfrak{Sets}$ y $\mathrm{Hom}_{\mathfrak{Sets}}(2, -)$ definidos por $sq(E) = E \times E$ y $\mathrm{Hom}_{\mathfrak{Sets}}(2, -)(E) = \mathrm{Hom}_{\mathfrak{Sets}}(2, E)$, donde 2 denota al conjunto de dos elementos $\{0, 1\}$. Probar 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* $\mathfrak{C}$ *y* $\mathfrak{D}$ *dos categorías,* $F : \mathfrak{C} \to \mathfrak{D}$ *y* $G : \mathfrak{D} \to \mathfrak{C}$ *dos funtores tales que para todo par de objetos* $M \in \mathrm{Obj}(\mathfrak{C})$ *y* $X \in \mathrm{Obj}(\mathfrak{D})$ *existe un isomorfismo* $\mathrm{Hom}_{\mathfrak{D}}(F(M), X) \cong \mathrm{Hom}_{\mathfrak{C}}(M, G(X))$ *que es natural con respecto a las dos variables. En este caso diremos que* F *es* **adjunto a izquierda** *de* G *y que* G *es* **adjunto a derecha** *de* F*.*

Ejemplos:

1. Sea ${}_AX_B$ 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. Sea A un anillo, 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 $S \subset A$ 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 $f^{\rightarrow} : \mathcal{P}(A) \to \mathcal{P}(B)$ el funtor imagen y $f^{\leftarrow} : \mathcal{P}(B) \to \mathcal{P}(A)$ el funtor imagen inversa. Demuestre que $f^{\rightarrow}$ es adjunto a izquierda de $f^{\leftarrow}$.

2. 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. 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. 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. 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 $G : \mathfrak{C} \to \mathfrak{D}$ un funtor que admite un adjunto a derecha $F : \mathfrak{D} \to \mathfrak{C}$, 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 $\{f_{i\leq j} : X_j \to X_i\}$ un sistema proyectivo en $\mathfrak{D}$ que admite límite $(X, p_i : X \to X_i)$, queremos ver entonces que el sistema proyectivo $\{F(f_{i\leq j}) : F(X_j) \to F(X_i)\}$ también admite límite, y que coincide con $(F(X), F(p_i) : F(X) \to F(X_i))$. Para esto, recordemos que X es límite de los X_i si y sólo si la función natural

$$\mathrm{Hom}_{\mathfrak{D}}(Y, X) \to \lim_{\leftarrow I} \mathrm{Hom}_{\mathfrak{D}}(Y, X_i)$$

es una biyección para todo objeto Y. Si C es un objeto de $\mathfrak{C}$, entonces se tienen las siguientes biyecciones naturales:

$$\mathrm{Hom}_{\mathfrak{C}}(C, F(X)) \cong \mathrm{Hom}_{\mathfrak{D}}(G(C), X) \cong \lim_{\leftarrow I} \mathrm{Hom}_{\mathfrak{D}}(G(Y), X_i) \cong \lim_{\leftarrow I} \mathrm{Hom}_{\mathfrak{C}}(Y, F(X_i))$$

Lo que demuestra el teorema. La parte dual puede demostrarse de manera directa, o bien notando que $F : \mathfrak{C} \to \mathfrak{D}$ es adjunto a derecha de G si y sólo si $F : \mathfrak{C}^{op} \to \mathfrak{D}^{op}$ es adjunto a izquierda de $G : \mathfrak{D}^{op} \to \mathfrak{C}^{op}$, y los colímites en $\mathfrak{D}$ coinciden con los límites en $\mathfrak{D}^{op}$.

Si $G : \mathfrak{C} \to \mathfrak{D}$ un funtor que admite un adjunto a derecha $F : \mathfrak{D} \to \mathfrak{C}$, 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 $G : \mathfrak{C} \to \mathfrak{D}$ un funtor que admite un adjunto a derecha $F : \mathfrak{D} \to \mathfrak{C}$.*

- *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 ítem 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 $\mathfrak{D}$, consideremos $F(I)$ y un monomorfismo $g : M \to N$ en la categoría $\mathfrak{C}$. La definición de inyectivo se esquematiza mediante el diagrama

$$\begin{array}{ccc} M & \xrightarrow{g} & N \\ {\scriptstyle f}\downarrow & \swarrow_{?} & \\ F(I) & & \end{array}$$

Es decir, dada una $f \in \mathrm{Hom}_{\mathfrak{C}}(M, F(I))$ se quiere saber si se "extiende" a N, o sea si existe alguna $\widetilde{f} : N \to F(I)$ tal que $f = \widetilde{f} \circ g$. La manera de reescribir este párrafo en términos del funtor $\mathrm{Hom}_{\mathfrak{C}}(-, F(I))$ es decir si $g_* : \mathrm{Hom}_{\mathfrak{C}}(N, F(I)) \to \mathrm{Hom}_{\mathfrak{C}}(M, F(I))$ 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:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathfrak{C}}(N, F(I)) & \xrightarrow{g_*} & \mathrm{Hom}_{\mathfrak{C}}(M, F(I)) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathfrak{D}}(G(N), I) & \xrightarrow{G(g)_*} & \mathrm{Hom}_{\mathfrak{D}}(G(M), I) \end{array}$$

Por hipótesis, G preserva monomorfismos, luego $G(g) : G(M) \to G(N)$ es un monomorfismo, al ser I inyectivo en $\mathfrak{C}$ 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.

Ejemplos: El funtor olvido $\mathcal{O} : {}_A\mathrm{Mod} \to \mathfrak{Sets}$ claramente conserva epimorfismos, usando el teorema re-encontramos 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.

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.

11

Índice alfabético