

Una introducción a la teoría de módulos sobre
anillos no conmutativos
Volumen I

Mauricio Medina-Bárcenas

Introducción

Este texto es un re-acomodo de las notas que he estado escribiendo sobre teoría de módulos que se pueden encontrar en mi página personal. Las notas originales surgieron como un trabajo social por el año 2009 basandome en los cursos de Algebra Moderna 3 y Algebra Moderna 4 impartidos por el Dr. Alejandro Alvarado García en la Facultad de Ciencias de la UNAM.

El escrito aquí presentado, es en gran parte (algunos resultados no se vieron en clase) el curso de Algebra Moderna 3 que impartí en la Facultad de Ciencias en el semestre 2023-2. La intención de re-escribir estas notas y no presentar a los alumnos las notas originales mencionadas arriba, es que quise dar un curso que incluyera, en mi opinión personal, lo que un alumno de licenciatura necesita de la teoría de módulos para poder adentrarse en otras áreas del álgebra o continuar con esta línea. Estas notas buscan que el alumno tenga una formación que le permita entender textos básicos de teoría de representaciones o de álgebra homológica.

El contenido de estas notas comprende desde la definición de R -módulo hasta las definiciones de módulo inyectivo y proyectivo. En este camino se presentan construcciones generales como el producto directo y suma directa de módulos. También se incluyen en estas notas el producto tensorial de módulos, necesario para otras áreas afines. Se hace una breve exposición de módulos semisimples y se introducen los conceptos de radical y zoclo. Para finalizar, se definen módulos proyectivos e inyectivos, pasando por módulos libres y grupos divisibles.

La exposición de este escrito trata de ser la más clara posible. Se buscó no dejar ningún concepto sin un adecuado ejemplo. También, a lo largo del texto se dan contraejemplos a distintas situaciones que me parecieron importantes de resaltar. Por último, cada capítulo termina con una sección de ejercicios, los cuales busqué que fueran adecuados para alumnos de licenciatura que ven por primera vez estos temas.

Como menciono arriba, no todos los resultados puestos en estas notas se vieron en clase, así que a continuación doy una lista de los resultados que pueden ser omitidos en un primer curso y así no tener que dar clases muy rápidas y que puedan abrumar a los estudiantes. Por supuesto, el profesor del curso tiene la última palabra sobre los resultados que quiera dar a sus alumnos. Los resultados listados abajo, son precisamente los que yo omití en mi curso.

Resultados que pueden ser omitidos: Sección 1.1, Lemma 3.2.7, Teorema 5.1.16, Teorema 5.3.12, Lemma 5.3.17, Teorema 5.3.18, Teorema 5.3.19, Teorema 6.1.7, Proposición 6.1.11, Corolario 6.1.12; y del Teorema 6.2.28 al Corolario 6.2.34.

Para terminar, quisiera dar una disculpa anticipada por los errores, principalmente de ortografía, que estas notas puedan contener. Estoy abierto a cualquier

II

sugerencia y/o comentario que me lo pueden hacer llegar a mi correo mmedina@ciencias.unam.mx

Dr. Mauricio Medina-Bárceñas
Ciudad de México, Mayo 2023

Índice general

Introducción	I
Notación	V
1. Definición de R-Módulo	1
1.1. Repaso de anillos	1
1.2. Definición de R -módulo	4
1.3. Ejercicios	7
2. Submódulos y Cocientes	9
2.1. Submódulos	9
2.2. Cocientes	13
2.3. Ejercicios	15
3. R-morfismos	17
3.1. R -morfismos	17
3.2. Teoremas de Isomorfismo	22
3.3. Sucesiones Exactas	25
3.4. El grupo de R -morfismos Hom_R	28
3.5. Ejercicios	31
4. Construcciones de módulos	35
4.1. Producto y Coproducto	35
4.2. Producto Fibrado y Coproducto Fibrado	41
4.3. Producto Tensorial	45
4.4. Ejercicios	52
5. Módulos semisimples y el Radical	55
5.1. Submódulos esenciales y superfluos	55
5.1.1. Submódulos esenciales	55
5.1.2. Submódulos superfluos	58
5.2. Módulos semisimples	60
5.3. Radical y zoclo	63
5.4. Ejercicios	69
6. Módulos Proyectivos e Inyectivos	71
6.1. Módulos libres	71
6.2. Módulos Inyectivos y Proyectivos	76
6.3. Ejercicios	86

A. Nociones Básicas de Categorías	89
A.1. Definición de Categoría	89
A.2. Funtores	92
A.3. Producto y Coproducto	93
A.4. Producto Fibrado y Coproducto Fibrado	95
Índice	98

Notación

\mathbb{N}	Números naturales.
\mathbb{Z}	Números enteros.
\mathbb{P}	Conjunto de números primos.
\mathbb{Q}	Números racionales.
\mathbb{R}	Números reales.
\mathbb{C}	Números complejos.
\mathbb{Z}_n	Números módulo n .
\mathbb{Z}_{p^∞}	p -Grupo de Prüfer.
Ab	Categoría de grupos abelianos.
R^{op}	Anillo opuesto.
$R[x_1, \dots, x_n]$	Anillo de polinomios en indeterminadas x_1, \dots, x_n con coeficientes en R .
$R\text{-Mod}$	Categoría de R -módulos izquierdos.
$R\text{-Simp}$	Conjunto de representantes de clases de isomorfismo de R -módulos simples.
${}_R M$ (resp. M_R)	M es un R -módulo izquierdo (resp. derecho).
$N \leq M$	N es submódulo de M .
$N < M$	N es submódulo propio de M .
$M_{n \times k}(R)$	Grupo de matrices de $n \times k$ con coeficientes en R .
$M_n(R)$	Anillo de matrices de $n \times n$ con coeficientes en R .
$TL_n(R)$	Anillo de matrices triangulares inferiores de $n \times n$ con coeficientes en R .
M/N	Módulo cociente.
$Sub(M)$	Conjunto de submódulos del módulo M .
$\ell(X)$	Submódulo generado por el conjunto X .
$(N : x)$	Trasladado por la izquierda de x a N .
$(N : L)$	Trasladado por la izquierda de L a N .
$(0 : x)$	Ideal anulador izquierdo de x .
$Zoc(M)$	Zoclo del módulo M .
$Rad(M)$	Radical del módulo M .
$N \ll M$	N es superfluo en M .
$N \leq_e M$	N es esencial en M .
$M^{(I)}$	Suma directa de copias del módulo M indicadas en el conjunto I .
M^I	Producto directo de copias del módulo M indicadas en el conjunto I .
$E(M)$	Cápsula inyectiva del módulo M .
$M \oplus N$	Suma directa de los módulos M y N .
$A \times B$	Producto cartesiano de A y B .
\bigoplus	Suma directa.

\prod	Producto directo
\coprod	Coproducto.
$\text{Hom}_R(M, N)$	Conjunto de R -morfismos de M en N .
$\text{End}_R(M)$	Anillo de endomorfismos del R -módulo M .
Id_M	Morfismo identidad del módulo M .
\ggrightarrow	Monomorfismo.
\longrightarrow	Epimorfismo.
\hookrightarrow	Inclusión.
$\text{Ker } \varphi$	Núcleo del morfismo φ .
$\text{Im } \varphi$	Imagen del morfismo φ .
$M \otimes_R N$	Producto tensorial de los módulos M y N sobre el anillo R .
$\text{Coker } \varphi$	Conúcleo del morfismo φ .
$(- \cdot x)$	Morfismo multiplicar por x por la izquierda.
$\bigvee X$	Supremo del conjunto X .
$\bigwedge X$	Infimo del conjunto X .
$\mathcal{O}(X)$	Marco de conjuntos abiertos del espacio topológico X .
$\text{Obj}(\mathcal{C})$	Objetos de la categoría \mathcal{C} .
$\text{Hom}_{\mathcal{C}}(A, B)$	Morfismos en la categoría \mathcal{C} entre los objetos A y B .

Capítulo 1

Definición de R -Módulo

1.1. Repaso de anillos

Definición 1.1.1. Un *anillo* con uno es una quinteta $(R, +, *, 0, 1)$ donde R es un conjunto y se satisface lo siguiente:

1. $(R, +, 0)$ es un grupo abeliano
2. $(R, *, 1)$ es un monoide
3. $r * (s + t) = r * s + r * t$
 $(s + t) * r = s * r + t * r$

Ejemplo 1.1.2. (i) Los conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y \mathbb{C} son anillos las operaciones usuales de suma y producto.

(ii) Para cada $n > 0$, los conjuntos \mathbb{Z}_n son anillos.

(iii) Sea K un campo. Entonces $M_n(K)$ es un anillo con las operaciones usuales de matrices.

(iv) Sea R un anillo conmutativo y G un grupo finito. Se define el *álgebra de grupo* RG como el conjunto de sumas formales

$$RG = \left\{ \sum_{g \in G} r_g g \mid r_g \in R \right\}$$

con operaciones

- $\sum_{g \in G} r_g g + \sum_{g \in G} s_g g = \sum_{g \in G} (r_g + s_g) g$
- $\left(\sum_{g \in G} r_g g \right) * \left(\sum_{h \in G} s_h h \right) = \sum_{gh \in G} r_g s_h gh$

Definición 1.1.3. Sea R un anillo y S un subconjunto de $(R, +, *, 0, 1)$. Decimos que S es un *subanillo* de R si:

1. $(S, +, 0)$ es un subgrupo de $(R, +, 0)$.
2. $rs \in S$ para todo $r, s \in S$.

3. $1 \in S$.

Ejemplo 1.1.4. (I) Se tiene que \mathbb{Z} es un subanillo de \mathbb{Q} que es un subanillo de \mathbb{R} que es un subanillo de \mathbb{C} .

(II) Sea K un campo. El subconjunto de matrices triangulares inferiores $\text{TI}_n(K)$ de $M_n(K)$ es un subanillo.

(III) El conjunto $\begin{pmatrix} \mathbb{Q} & 0 \\ \mathbb{R} & \mathbb{R} \end{pmatrix}$ es un subanillo de $\text{TI}_2(\mathbb{R})$.

(IV) Sea K un campo y G un grupo finito. Si H es un subgrupo de G , entonces KH es un subanillo de KG .

Definición 1.1.5. Sea $(R, +, *, 0, 1)$ un anillo. Un *ideal izquierdo* (resp. *derecho*, *bilateral*) es un subconjunto I de R tal que:

- $(I, +, 0)$ es un subgrupo de $(R, +, 0)$.
- $ra \in I$ (resp. $ar \in I$, $ra, ar \in I$) para todo $a \in I$ y $r \in R$.

Ejemplo 1.1.6. (I) 0 y R son ideales bilaterales.

(II) Sea K un campo. Entonces $\begin{pmatrix} K & 0 \\ K & 0 \end{pmatrix}$ y $\begin{pmatrix} 0 & 0 \\ 0 & K \end{pmatrix}$ son ideales izquierdos de $\text{TI}_2(K)$.

(III) Sea ${}_K V$ un K -espacio vectorial de dimensión infinita. Sea R el anillo de transformaciones lineales de V en V . Entonces

$$I = \{f \in R \mid \dim_K(\text{Im } f) < \infty\}$$

es un ideal bilateral de R .

Dado un anillo R y un ideal bilateral I de R , se define el cociente R/I como el conjunto de clases de equivalencia dadas por la relación:

$$r \equiv s \Leftrightarrow r - s \in I.$$

Las clases de equivalencia se pueden ver como

$$r + I = \{r + a \mid a \in I\}$$

para cada $r \in R$. Así, R/I es un anillo asociativo con uno, con las operaciones:

$$(r + I) + (s + I) = (r + s) + I$$

$$(r + I)(s + I) = (rs) + I$$

para todo $r, s \in R$.

Proposición 1.1.7. Sea R un anillo e I un ideal bilateral de R . Entonces hay una biyección entre los ideales izquierdos (resp. derechos, bilaterales) de R/I y los ideales izquierdos (resp. derechos, bilaterales) de R que contienen a I .

Definición 1.1.8. Si $(R, +, \cdot, 0_R, 1_R)$ y $(S, \overline{+}, *, 0_S, 1_S)$ son anillos con uno, una función $\varphi : R \rightarrow S$ es un *morfismo de anillos* si:

1. $\varphi(r + s) = \varphi(r) + \varphi(s)$
2. $\varphi(rs) = \varphi(r) * \varphi(s)$
3. $\varphi(1_R) = 1_S$

Si φ es biyectiva, decimos que φ es un *isomorfismo de anillos*.

Ejemplo 1.1.9. (I) Si S es un subanillo de R , entonces el morfismo inclusión $\iota : S \rightarrow R$ dado por $\iota(s) = s$ es un morfismo de anillos.

(II) Sea R un anillo conmutativo y $a \in R$. La función evaluar en a , $ev_a : R[x] \rightarrow R$ es un morfismo de anillos.

(III) Sea R un anillo. La función $\varphi : R \rightarrow M_2(R)$ definida como $\varphi(r) = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$ es un morfismo de anillos.

(IV) Sea R un anillo e I un ideal bilateral. Entonces la función $\pi : R \rightarrow R/I$ dada por $\pi(r) = r + I$ es un morfismo de anillos.

Definición 1.1.10. Sea $\varphi : R \rightarrow S$ un morfismo de anillos. Se definen el *kernel* y la *imagen* de f como:

$$\text{Ker } \varphi = \{r \in R \mid \varphi(r) = 0\} \text{ y}$$

$$\text{Im } \varphi = \{\varphi(r) \in S \mid r \in R\}$$

respectivamente.

Proposición 1.1.11. Sea $\varphi : R \rightarrow S$ un morfismo de anillos. Entonces:

1. $\text{Ker } \varphi$ es un ideal bilateral de R .
2. $\text{Im } \varphi$ es un subanillo de S .
3. φ es inyectiva si y solo si $\text{Ker } \varphi = \{0\}$.
4. φ induce un isomorfismo de anillos entre $R/\text{Ker } \varphi$ y $\text{Im } \varphi$.
5. Si J es un ideal izquierdo (resp. derecho, bilateral) de S , entonces $\varphi^{-1}(J)$ es un ideal izquierdo (resp. derecho, bilateral) de R .

1.2. Definición de R -módulo

A partir de aquí R denotará a un anillo asociativo con uno

Definición 1.2.1. Sea $(M, +, 0)$ un grupo abeliano. Un endomorfismo de M es un morfismo de grupos abelianos $\varphi : M \rightarrow M$. Denotemos $\text{End}_{\mathbb{Z}}(M) = \{\varphi \mid \varphi \text{ endomorfismo de } M\}$.

Sean $\varphi, \psi \in \text{End}_{\mathbb{Z}}(M)$.

$$\begin{array}{ccc}
 \widehat{\varphi + \psi} : & M \longrightarrow M & -\varphi : & M \longrightarrow M \\
 & m \longmapsto \varphi(m) + \psi(m) & & m \longmapsto -\varphi(m) \\
 \\
 \widehat{0} : & M \longrightarrow M & \varphi \circ \psi : & M \longrightarrow M \\
 & m \longmapsto 0 & & m \longmapsto \varphi(\psi(m)) \\
 \\
 1_M : & M \longrightarrow M & & \\
 & m \longmapsto m & &
 \end{array}$$

Entonces $(\text{End}_{\mathbb{Z}}(M), \widehat{+}, \circ, \widehat{0}, 1_M)$ es un anillo.

Definición 1.2.2. Sea R un anillo. La pareja (M, λ) es un R -módulo izquierdo denotado ${}_R M$, si $(M, \overline{+}, \overline{0})$ es un grupo abeliano y $\lambda : R \rightarrow \text{End}_{\mathbb{Z}}(M)$ es un morfismo de anillos.

Sea R un anillo y (M, λ) un R -módulo. Para cada $r \in R$, $\lambda(r) : M \rightarrow M$ es un endomorfismo de M . Denotemos $rm := \lambda(r)(m)$, es decir,

$$\lambda(r) : M \longrightarrow M$$

$$m \longmapsto \lambda(r)(m) := rm.$$

Entonces se satisface lo siguiente:

1. $\lambda(r + s) = \lambda(r) \widehat{+} \lambda(s)$
 $\forall m \in M, (r + s)m := \lambda(r + s)(m) = \lambda(r)(m) \overline{+} \lambda(s)(m) := rm \overline{+} sm.$
2. $\lambda(r * s) = \lambda(r) \circ \lambda(s)$
 $\forall m \in M, (r * s)m := \lambda(r * s)(m) = \lambda(r)(\lambda(s)(m)) := r(sm).$
3. $\lambda(r)(m \overline{+} n) = \lambda(r)(m) \overline{+} \lambda(r)(n)$
 $\forall m, n \in M, r(m \overline{+} n) := \lambda(r)(m \overline{+} n) = \lambda(r)(m) \overline{+} \lambda(r)(n) := rm \overline{+} rn.$

$$4. \lambda(1_R) = Id_M \\ \forall m \in M, 1_R m := \lambda(1_R)(m) = 1_M(m) = m.$$

Ejemplo 1.2.3. (i) Como ejemplos básicos de R -módulos están los siguientes. Tomemos

$$\varphi : R \longrightarrow \text{End}_{\mathbb{Z}}(R_+)$$

$$r \longmapsto \varphi(r) : R_+ \longrightarrow R_+$$

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

donde R_+ es la parte aditiva del anillo $(R, +, 0)$. Con esta φ tenemos que R es un R -módulo sobre si mismo ${}_R R$.

(ii) Si $R = \mathbb{Z}$ y S es un anillo existe un único morfismo de anillos

$$\mathbb{Z} \longrightarrow S$$

$$1 \longmapsto 1_S$$

$$n \longmapsto 1_S + 1_S + \dots + 1_S \text{ (} n \text{ veces)}$$

Como $n = 1 + 1 + \dots + 1$ el morfismo es único por que ya está determinado en 1.

Si M es un grupo abeliano

$$\lambda : \mathbb{Z} \longrightarrow \text{End}_{\mathbb{Z}}(M)$$

$$1 \longmapsto Id_M$$

$$n \longmapsto \lambda(n) : M \longrightarrow M$$

$$m \longmapsto \lambda(n)(m) := nm$$

Como λ es único y $\lambda(n)(m) = (Id_M + \dots + Id_M)(m) = m + \dots + m := nm$, entonces todo grupo abeliano es un \mathbb{Z} -módulo.

Dado un R -módulo (M, λ) , por la Proposición 1.1.11 tenemos que $\text{Ker } \lambda$ es un ideal bilateral de R . Notemos que

$$\text{Ker } \lambda = \{r \in R \mid \lambda(r) = 0\} = \{r \in R \mid \lambda(r)(m) = 0 \forall m \in M\} = \{r \in R \mid rm = 0 \forall m \in M\}$$

Definición 1.2.4. Sea (M, λ) un R -módulo. Al núcleo de λ se le llama *el anulador de M* y se denota $\text{Ann}_R(M)$. Si $\text{Ann}_R(M) = 0$ se dice que M es *fiel*.

Proposición 1.2.5. Sea (M, λ) un R -módulo. Entonces M es un $R/\text{Ann}_R(M)$ -módulo fiel.

Demostración. Tenemos el morfismo de anillos $\lambda : R \rightarrow \text{End}_{\mathbb{Z}}(M)$. Por definición $\text{Ann}_R(M) = \text{Ker } \lambda$. Se sigue de la Proposición 1.1.11 que λ induce un morfismo de anillos inyectivo $\bar{\lambda} : R/\text{Ann}_R(M) \rightarrow \text{End}_{\mathbb{Z}}(M)$. Por lo tanto M es un $R/\text{Ann}_R(M)$ -módulo fiel. \square

Es posible dar otra definición de R -módulo izquierdo, enfocandonos sólo en la acción del anillo R en el grupo abeliano M .

Definición 1.2.6. Sea R un anillo y $(M, \bar{+}, 0)$ un grupo. Se dice que M es un R -módulo izquierdo, denotado ${}_R M$, si existe una acción

$$R \times M \longrightarrow M$$

$$(r, m) \longrightarrow rm$$

que cumple:

1. $r(m\bar{+}n) = rm\bar{+}rn$
2. $(r + s)m = rm\bar{+}sm$
3. $(r * s)m = r(sm)$
4. $1m = m$

Ejemplo 1.2.7. (I) Sea K un campo. Entonces todo espacio vectorial sobre K es un K -módulo.

(II) Consideremos el anillo $R = \begin{pmatrix} \mathbb{Q} & 0 \\ \mathbb{R} & \mathbb{R} \end{pmatrix}$ con las operaciones de matrices. Entonces

$$\begin{pmatrix} 0 & 0 \\ \mathbb{R} & \mathbb{R} \end{pmatrix} \begin{pmatrix} \mathbb{R} & 0 \\ \mathbb{R} & \mathbb{R} \end{pmatrix}$$

Son R -módulos izquierdos.

(III) Sea $R = C(\mathbb{R}, \mathbb{R})$ el anillo de funciones continuas de \mathbb{R} en \mathbb{R} , con producto la composición de funciones. Sea X un espacio topológico y sea $C(X, \mathbb{R})$ las funciones continuas de X en \mathbb{R} .

Sea $g \in C(X, \mathbb{R})$ y $f \in R$ entonces $f \circ g \in C(X, \mathbb{R})$. Con esta operación $C(X, \mathbb{R})$ es un R -módulo izquierdo.

(IV) Sean R y S anillos y sea $f : R \rightarrow S$ un morfismo de anillos. Con el morfismo f podemos darle estructura de R -módulo izquierdo a S de la siguiente manera:

Como S es un anillo, en particular es un grupo abeliano. Ahora si $r \in R$ y $s \in S$ definimos $r \cdot s = f(r)s$.

A esta estructura que le damos a S se le llama *restricción de escalares*.

1.3. Ejercicios

1. Sea $\{R_i\}_I$ una familia de anillos. Demuestre que el producto cartesiano $\prod_I R_i$ es un anillo con las operaciones coordenada a coordenada.
2. Sea ${}_K V$ un K -espacio vectorial (de cualquier dimensión). Sea

$$\text{End}_K(V) = \{f : V \rightarrow V \mid f \text{ es una transformación lineal}\}.$$

Demuestre que $\text{End}_K(V)$ es un anillo con la suma puntual y la composición.

3. De un K -espacio vectorial V tal que $\text{End}_K(V)$ no sea un anillo conmutativo.
4. Sea K un campo. Demuestre que $\begin{pmatrix} 0 & 0 \\ 0 & K \end{pmatrix}$ no es un ideal bilateral de $\text{TI}_2(K)$.
5. Sea K un campo. Demuestre que $\begin{pmatrix} K & 0 \\ K & 0 \end{pmatrix}$ es un ideal bilateral de $\text{TI}_2(K)$ pero no de $M_n(K)$.
6. Sea I el ideal del ejercicio anterior. Demuestre que $\text{TI}_2(K)/I$ es isomorfo a K .
7. Demuestre la Proposición 1.1.7
8. Sea K un campo. Demuestre que el anillo $M_n(K)$ no tiene ideales bilaterales distintos de 0 y $M_n(K)$.
9. Sean R un anillo conmutativo, G y H grupos finitos. Suponga que $f : G \rightarrow H$ es un morfismo de grupos. Demuestre que $\bar{f} : R[G] \rightarrow R[H]$ definida como $\bar{f}\left(\sum_{g \in G} r_g g\right) = \sum_{g \in G} r_g f(g)$ es un morfismo de anillos.
10. Demuestre la Proposición 1.1.11.
11. De un ejemplo en el que la imagen de un ideal bajo un morfismo de anillos no sea un ideal.
12. Demuestre que la operación $\bar{\mp}$ de M en la Definición 1.1.8 es conmutativa usando las condiciones de la acción de R en M .
13. Demuestre que las Definiciones 1.1.1 y 1.1.8 son equivalentes.
14. Demuestre que si R es un anillo conmutativo con unidad y M es un R -módulo izquierdo, entonces M es un R -módulo derecho. ¿Qué pasa si R no es conmutativo?
15. Sea R un anillo y $M_{n \times k}(R)$ las matrices de tamaño $n \times k$ con coeficientes en R . Demuestre que $M_{n \times k}(R)$ es un $M_n(R)$ -módulo izquierdo para todo $n, k > 0$.
16. Sea R un anillo conmutativo, M un R -módulo y x una indeterminada. Definimos

$$M[x] = \left\{ \sum_{i=0}^n m_i x^i \mid m_i \in M, n \geq 0 \right\}.$$

Demuestre que $M[x]$ es un $R[x]$ -módulo con las operaciones de polinomios.

17. Demuestre que todo K -espacio vectorial V es fiel.
18. Sea R un anillo y M un R -módulo. Demuestre que las siguientes afirmaciones son equivalentes:
 - (a) M es fiel.
 - (b) R es (isomorfo a) un subanillo de $\text{End}_{\mathbb{Z}}(M)$.
 - (c) Si $rm = 0$ para todo $m \in M$ entonces $r = 0$.

Capítulo 2

Submódulos y Cocientes

2.1. Submódulos

Definición 2.1.1. Un subconjunto N de M es un *submódulo* (lo denotaremos $N \leq {}_R M$) si

1. N es un subgrupo de M , y
2. $rx \in N$ para todo $r \in R$ y $x \in N$.

Denotemos $Sub({}_R M) := \{N \mid N \leq {}_R M\}$ al conjunto de submódulos de M .

Ejemplo 2.1.2. (i) Para todo R -módulo M , $\{0\} \leq M$ y $M \leq M$.

(ii) En ${}_R R$, $I \leq {}_R R$ si I es un ideal izquierdo de R

Definición 2.1.3. Un módulo M es *simple* si sus únicos submódulos son los triviales, es decir, 0 y M .

Ejemplo 2.1.4. (i) Si p es un número primo entonces los \mathbb{Z} -módulos \mathbb{Z}_p son simples.

(ii) Si $M_n(K)$ es el anillo de matrices cuadradas de $n \times n$ con coeficientes en un anillo con división (por ejemplo un campo) entonces para cada $1 \leq l \leq n$

$$S_l = \{(a_{ij}) \in M_n(K) \mid a_{ij} = 0 \text{ para todo } j \neq l\}$$

es simple como $M_n(K)$ -módulo.

Definición 2.1.5. Si $A \subseteq R$ y $X \subseteq M$, $AX = \{a_1x_1 + a_2x_2 + \dots + a_nx_n \mid a_i \in A, x_i \in X, n \in \mathbb{N}\}$ es el conjunto de *combinaciones lineales* de A y X .

Lema 2.1.6. Sea M un R -módulo izquierdo y $\emptyset \neq X \subseteq M$. Entonces $RX \leq {}_R M$.

Demostración. Es claro que la suma de dos combinaciones lineales de X con coeficientes en R , es una combinación lineal de X con coeficientes en R . Ahora, sea $x \in RX$ y $s \in R$. Entonces $x = r_1x_1 + \dots + r_nx_n$ y $sx = sr_1x_1 + \dots + sr_nx_n \in RX$. Por lo tanto $RX \leq M$. \square

Proposición 2.1.7. Sea $\phi \neq N \subseteq {}_R M$. Son equivalentes:

- (a) $N \leq M$
- (b) $RN = N$
- (c) $\forall a \in R$ y $\forall x, y \in N$, $ax + y \in N$

Demostración. (a) \Rightarrow (b). Es claro que $N \subseteq RN$ ya que todo elemento de N es una combinación lineal en RN . Ahora sea $z \in RN$ entonces $z = a_1x_1 + a_2x_2 + \dots + a_nx_n$ con $a_i \in R$ y $x_i \in N$ como $N \leq {}_R M$ entonces $a_i x_i \in N$ y $a_i x_i + a_{i+1} x_{i+1} \in N$ por lo tanto $a_1 x_1 + \dots + a_n x_n \in N$ así $RN \subseteq N$ demostrando 2.

(b) \Rightarrow (c). Sean $a, b \in R$ y $x, y \in N$ entonces $ax + by \in RN$ y por 2, tenemos que $RN = N$. Así que $ax + by \in N$.

(c) \Rightarrow (a). Tomemos $a = 1$ y $x, y \in N$. Entonces $x + y \in N$. Ahora sea $a = -1$ y $x \in N$. Entonces, $(-1)x + x = 0 \in N$. Por lo anterior, podemos tomar $a \in R$ y $x, 0 \in N$. Así $ax = ax + 0 \in N$. Por lo tanto $N \leq {}_R M$. \square

El Ejercicio 2.3.3 nos dice que existe el menor submódulo (con respecto a la inclusión) de ${}_R M$ que contiene a X al cual se le llama el *generado por X* y se denota $\ell(X)$.

Lema 2.1.8. 1. Si $X \subseteq Y \subseteq {}_R M$ entonces $\ell(X) \leq \ell(Y)$.

2. $\ell(\phi) = \{0\}$

3. $\ell(X) = RX$

Demostración. 1 y 2 Son claras.

3. Como $RX \leq {}_R M$ y $X \subseteq RX$, $\ell(X) \subseteq RX$ por que $\ell(X)$ es el menor submódulo que contiene a X . Ahora si $a_1, \dots, a_n \in R$ y $x_1, \dots, x_n \in X$ entonces $a_1 x_1 + \dots + a_n x_n \in \ell(X)$ así que $RX \subseteq \ell(X)$. \square

Observación 2.1.9. Por el lemma anterior tenemos que

$$\ell\left(\bigcup_{\alpha \in X} M_\alpha\right) = \{x_1 + \dots + x_n \mid x_i \in M_{\alpha_i}\}$$

el cual denotamos por $\sum_{\alpha \in X} M_\alpha$.

Lema 2.1.10. Si H, K, L son submódulos de ${}_R M$ entonces

$$H \cap (K + L) \geq (H \cap K) + (H \cap L)$$

Demostración. Tenemos que $H \cap K \leq H$ y $H \cap K \leq K \leq K + L$ también $H \cap L \leq H$ y $H \cap L \leq L \leq K + L$ entonces $H \cap K \leq H \cap (K + L)$ y $H \cap L \leq H \cap (K + L)$ por lo tanto $(H \cap K) + (H \cap L) \leq H \cap (K + L)$. \square

Observación 2.1.11. Notemos que la igualdad en la observación anterior no es cierta en general. Consideremos \mathbb{R}^2 como \mathbb{R} -módulo. Sean $H = \{(x, 0) \mid x \in \mathbb{R}\}$, $K = \{(0, y) \mid y \in \mathbb{R}\}$ y $L = \{(x, x) \mid x \in \mathbb{R}\}$. Es claro que H, K y L son submódulos de \mathbb{R}^2 y $H \cap (K + L) = H \cap \mathbb{R}^2 = H$. Por otro lado $(H \cap K) + (H \cap L) = \bar{0} + \bar{0} = \bar{0}$.

Lema 2.1.12 (Ley Modular). Sean H, L, K submódulos de ${}_R M$. Si $K \leq H \leq L$ entonces

$$H \cap (K + L) = K + (H \cap L)$$

Demostración. \supseteq Es la Observación 2.1.10.

\subseteq Sea $x \in H \cap (K + L)$ entonces $x \in H$ y $x = k + l$ con $k \in K$ y $l \in L$ entonces $l = x - k$ y como $k \in K \leq H$ y $x \in H \Rightarrow l \in H$ por lo tanto $x \in K + (H \cap L)$. Quedando demostrada la Ley Modular. \square

A partir de este momento denotaremos ${}_R M$ simplemente por M siempre y cuando esté claro sobre que anillo estamos trabajando.

Definición 2.1.13. Sea M un R -módulo.

1. Decimos que $X \subseteq M$ genera a M si $RX = M$.
2. Si X genera a M y X es finito, decimos que M es *finitamente generado*.
3. Si $X = \{x\}$ y genera a M , decimos que M es *cíclico* $M = Rx$.

Proposición 2.1.14. Un módulo M es finitamente generado (f.g.) si y solo si para cada familia $\{M_i\}_{i \in I}$ de submódulos de M tales que $\sum_{i \in I} M_i = M$, existe $F \subseteq I$ finito tal que $M = \sum_{j \in F} M_j$.

Demostración. Supongamos que M es f.g. entonces $M = RX$ para algún $X \subseteq M$ finito. Notemos que $RX = Rx_1 + Rx_2 + \dots + Rx_n$. Si $M = \sum_{i \in I} M_i$ entonces para cada $i \in \{1, \dots, n\}$, x_i está en una suma finita de submódulos en la familia $\{M_i\}_{i \in I}$. Entonces $X = \{x_1, \dots, x_n\}$ está incluido en una suma finita de submódulos $\{M_j\}_{j \in F}$. Así se tiene que $M \subseteq \sum_{j \in F} M_j \subseteq \sum_{i \in I} M_i \subseteq M$. Recíprocamente tenemos que $M = \sum_{m \in M} Rm$ entonces existe $X = \{x_1, \dots, x_n\} \subseteq M$ tal que $M = \sum_{i=1}^n Rx_i = RX$ por lo tanto M es f.g. \square

Definición 2.1.15. Decimos que $N \leq M$ es *máximo* en M si $N < M$ y siempre que $N < L \leq M$ se tiene que $L = M$.

Proposición 2.1.16. Son equivalentes para $N < M$:

- (a) N es máximo en M .
- (b) Si $m \notin N$, entonces $N + Rm = M$

Demostración. (a) \Rightarrow (b). Sup. que $m \notin N$ entonces $N < N + Rm$ y como N es máximo entonces $N + Rm = M$.

(b) \Rightarrow (a). Supongamos que $N < L \leq M$ como $N < L$ tomamos $m \in L - N$ entonces $N + Rm = M$ por hipótesis, pero $N + Rm \subseteq L$ entonces $L = M$. \square

Teorema 2.1.17. Si ${}_R M$ es finitamente generado entonces todo submódulo propio de ${}_R M$ está incluido en un submódulo máximo.

Demostración. Sea $K < M$ submódulo propio de M , entonces existe un conjunto $\{x_1, \dots, x_n\}$ de M tal que $M = Rx_1 + \dots + Rx_n + K$ por la Proposition 2.1.14 y podemos suponer que n es el mínimo.

Sea $L = K + Rx_2 + \dots + Rx_n$. Entonces $L < M$. Sea $\mathbf{P} = \{N < {}_R M \mid L \leq N\}$ que es no vacío ya que $L \in \mathbf{P}$. Tenemos que (\mathbf{P}, \subseteq) es un COPO. Note que un submódulo T de M que incluya a L , no está en \mathbf{P} si y solo si $x_1 \in T$. Sea

$C = \{N_\alpha\}_{\alpha \in X}$ una cadena en \mathbf{P} no vacía, y sea $V = \bigcup C$. Sean $a, b \in V$, $r, s \in R$ P.D. $ra + sb \in V$. Si $a, b \in V$ entonces $a \in N_i$ p. a. $i \in X$ y $b \in N_j$ p. a. $j \in X$ y como $N_i \subseteq N_j$ o $N_j \subseteq N_i$ por ser C una cadena entonces $a, b \in N_i$ o $a, b \in N_j$ así que $ra + sb \in N_i$ o $ra + sb \in N_j$ por lo tanto $ra + sb \in V$. Como $x_1 \notin N_\alpha$ para toda $\alpha \in X$, $x_1 \notin V$ y así $V \in \mathbf{P}$. Por el lema de Zorn \mathbf{P} tiene elementos máximos. Sea N máximo en \mathbf{P} , si $N < T \leq M$ entonces $x_1 \in T$ ya que de lo contrario T estaría en \mathbf{P} contradiciendo la maximalidad de N . Por lo tanto $T = M$. \square

Corolario 2.1.18. *Un anillo R como R -módulo, tiene submódulos máximos. Es decir, todo anillo tiene ideales izquierdos (derechos) máximos.*

Corolario 2.1.19. *Si M es un R -módulo finitamente generado, entonces tiene submódulos máximos.*

Observación 2.1.20. Existen módulos que no tienen submódulos máximos; por ejemplo, el \mathbb{Z} -módulo \mathbb{Q} (Ejercicio 2.3.8). Por otro lado, pueden existir módulos que no sean finitamente generados pero que cada submódulo esté contenido en un máximo (Vea la Proposición 11.3.7 de las notas completas). También es posible tener un módulo que tenga submódulos máximos pero que no todo submódulo esté contenido en un máximo; por ejemplo el \mathbb{Z} -módulo $\mathbb{Z}_p \oplus \mathbb{Q}$ con p primo¹. En este módulo, el submódulo $0 \oplus \mathbb{Q}$ es máximo (Vea el Corolario 2.2.3 y el Corolario 3.2.5), sin embargo el submódulo $\mathbb{Z}_p \oplus 0$ no está contenido en ningún máximo (Vea el Corolario 3.2.5 y la Proposición 2.2.2).

Definición 2.1.21. Sea $\{N_\alpha\}_{\alpha \in X} \subseteq \text{Sub}(M)$ si:

1. $\sum_{\alpha \in X} N_\alpha = M$
2. $N_\alpha \cap \sum_{\beta \neq \alpha} N_\beta = 0$ para todo $\alpha \in X$

decimos que M es la *suma directa de la familia* $\{N_\alpha\}_{\alpha \in X}$ y lo denotamos como $\bigoplus_{\alpha \in X} \{N_\alpha\}$

Proposición 2.1.22. *Son equivalentes para $M = \sum_{\alpha \in X} N_\alpha$*

- (a) $N_\alpha \cap \sum_{\beta \neq \alpha} N_\beta = 0$ para todo $\alpha \in X$;
- (b) *todo elemento $m \in M$ se escribe de manera única como $m = n_{\alpha_1} + \dots + n_{\alpha_k}$ con $n_{\alpha_i} \in N_{\alpha_i}$.*

Demostración. (a) \Rightarrow (b) Sea $m \in M$ tal que $m = a_{\alpha_1} + \dots + a_{\alpha_k}$ y $m = b_{\alpha_1} + \dots + b_{\alpha_s}$ con $a_{\alpha_i}, b_{\alpha_i} \in N_{\alpha_i}$ dos representaciones distintas de m . Tomemos $a_{\alpha_j} \in N_{\alpha_j}$. Entonces $a_{\alpha_j} = b_{\alpha_1} + \dots + b_{\alpha_s} - a_{\alpha_1} - \dots - a_{\alpha_k}$ con $k \neq j$. Agrupando términos que estén en el mismo submódulo, nos da que $a_{\alpha_j} \in N_{\alpha_j} \cap \sum_{\beta \neq \alpha_j} N_\beta$, contradiciendo (a). Por lo tanto m se escribe de manera única.

(b) \Rightarrow (a) Si $N_\alpha \cap \sum_{\beta \neq \alpha} N_\beta \neq 0$ tomemos un elemento n_α en la intersección. Así, $n_\alpha = n_{\beta_1} + \dots + n_{\beta_k}$ con $n_{\beta_j} \in N_{\beta_j}$ y $\beta_j \neq \alpha$. Pero esto contradice que todo elemento de M se escriba de manera única. Por lo tanto, $n_\alpha = 0$. \square

¹Para la definición de suma directa vea la Sección 4.1

2.2. Cocientes

Sea ${}_R M$ un R -módulo y $N \leq M$ definimos la siguiente relación de equivalencia en M : Sean $x, y \in M$. Decimos que x y y son congruentes módulo N ($x \equiv y(N)$), si y solo si $x - y \in N$.

Para $x \in M$ consideremos su clase de equivalencia \bar{x} . Entonces

$$\bar{x} = \{y \in M \mid x \equiv y(N)\} = \{y \in M \mid y = x + n \text{ p.a. } n \in N\} = \{x + n \mid n \in N\}.$$

Así que denotamos a la clase de equivalencia de x por $x + N$ y denotamos al cociente de esta relación por $M/N := \{x + N \mid x \in M\}$.

Podemos definir en M/N las siguientes operaciones: Sean $y + N, x + N \in M/N$ y $r \in R$

$$\begin{aligned} (x + N) + (y + N) &:= (x + y) + N \\ r(x + N) &:= rx + N \end{aligned}$$

Proposición 2.2.1. *Con las operaciones anteriores M/N es un R -módulo.*

Proposición 2.2.2. *Sean M un R -módulo y $N \leq M$. Entonces existe una biyección entre los submódulos de M que contienen a N y los submódulos de M/N .*

Demostración. Sea $Sub(M)/N := \{L \leq M \mid N \subseteq L\}$. Definimos:

$$f_N : \quad Sub(M)/N \longrightarrow Sub(M/N)$$

$$H \longrightarrow H/N = \{h + N \mid h \in H\}$$

$$f_N^* : \quad Sub(M/N) \longrightarrow Sub(M)/N$$

$$T \longrightarrow \{x \in M \mid x + N \in T\} = f_N^*(T)$$

Si $x, y \in f_N^*(T)$ entonces $x + N, y + N \in T \Rightarrow (x + N) + (y + N) \in T \Rightarrow (x + y) + N \in T$ por lo tanto $x + y \in f_N^*(T)$ y si $r \in R$ entonces $rx + N = r(x + N) \in T$ por lo tanto $rx \in f_N^*(T)$

Por lo tanto $f_N^*(T) \in Sub(M)/N$.

Afirmamos que f_N^* es biyectiva.

Veamos que $f_N \circ f_N^* = Id_{Sub(M/N)}$ y $f_N^* \circ f_N = Id_{Sub(M)/N}$.

Sea $T \in Sub(M/N)$ entonces $f_N \circ f_N^*(T) = f_N(\{x \in M \mid x + N \in T\}) = \{x \in M \mid x + N \in T\}/N = T$.

Ahora sea $H \in Sub(M)/N$ entonces $f_N^* \circ f_N(H) = f_N^*(H/N) = \{x \in M \mid x + N \in H/N\} = H$. \square

Corolario 2.2.3. *Sea $N \leq M$. Entonces M/N es simple si y solo si N es máximo en M .*

Como ${}_R R$ es f.g. entonces tiene máximos y por lo tanto siempre hay módulos simples.

Proposición 2.2.4. *Sea M un módulo finitamente generado y $N \leq M$. Entonces M/N es finitamente generado.*

Demostración. Supongamos que M es finitamente generado, con generadores $m_1, \dots, m_n \in M$. Sea $x + N \in M/N$. Se tiene que $x = r_1 m_1 + r_2 m_2 + \dots + r_n m_n$. Entonces, $x + N = (r_1 m_1 + r_2 m_2 + \dots + r_n m_n) + N = r_1 m_1 + N + r_2 m_2 + N + \dots + r_n m_n + N$. Lo que implica que $m_1 + N, m_2 + N, \dots, m_n + N$ generan a M/N . \square

Observación 2.2.5. En general, submódulos de módulos finitamente generados no tienen por qué heredar la propiedad. Para ésto, consideremos el anillo

$$R = \begin{pmatrix} \mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix}$$

con las operaciones usuales de matrices. Es claro que ${}_R R$ es finitamente generado. Pero el ideal izquierdo

$$I = \begin{pmatrix} 0 & \mathbb{Q} \\ 0 & 0 \end{pmatrix}$$

no lo es. Notemos que la acción de R en I está dada por $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 0 & q \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & aq \\ 0 & 0 \end{pmatrix}$. Es decir, está determinada por la acción de \mathbb{Z} en \mathbb{Q} . Sabemos que ${}_{\mathbb{Z}} \mathbb{Q}$ no es finitamente generado (Ejercicio 2.3.7), por lo tanto ${}_R I$ tampoco.

2.3. Ejercicios

1. Considere el anillo R del Ejemplo 1.2.7.II. Demuestre que $\begin{pmatrix} 0 & 0 \\ 0 & \mathbb{R} \end{pmatrix}$ es un R -módulo simple.
2. Demuestre la afirmación del Ejemplo 2.1.4.II.
3. Demuestre que si $\{N_\alpha\}_{\alpha \in X}$ es una familia de submódulos de ${}_R M$ entonces $\bigcap \{N_\alpha\}_{\alpha \in X}$ es un submódulo de ${}_R M$.
4. Sea X un subconjunto no vacío de un R -módulo izquierdo M e I un ideal izquierdo de R . Demuestre que IX es un submódulo de M .
5. Demuestre 1 y 2 del Lemma 2.1.8.
6. Demuestre que cualquier submódulo finitamente generado de ${}_Z \mathbb{Q}$ es cíclico.
7. Sea $X \subseteq {}_Z \mathbb{Q}$ un subconjunto generador, es decir, $\mathbb{Z}X = {}_Z \mathbb{Q}$ y sea $x_0 \in X$. Demuestre que $\mathbb{Z}(X - \{x_0\}) = {}_Z \mathbb{Q}$. Concluya que ${}_Z \mathbb{Q}$ no es finitamente generado.
8. Demuestre que ${}_Z \mathbb{Q}$ no tiene submódulos máximos.
9. Demuestre que un módulo simple es cíclico.
10. Sea K un anillo con división. Demuestre que todo K -módulo tiene una base.
11. Muestre que \mathbb{Z}_4 como \mathbb{Z} -módulo no tiene una base.

Definición 2.3.1. Una *retícula* (L, \leq, \wedge, \vee) es un COPO (conjunto parcialmente ordenado) con orden \leq donde cada pareja de elementos $x, y \in L$ tiene supremo denotado $x \vee y$ e ínfimo denotado $x \wedge y$. Decimos que una retícula es *completa* si todo subconjunto $X \subseteq L$ tiene supremo $\bigvee X$ e ínfimo $\bigwedge X$.

12. Sea X un conjunto y $\mathbf{P}(X)$ el conjunto potencia de X . Demuestre que $\mathbf{P}(X)$ es una retícula completa, donde el orden está dado por la contención de conjuntos y el supremo e ínfimo son la unión y la intersección de conjuntos respectivamente.
13. Sea X un espacio topológico. Denotemos por $\mathcal{O}(X)$ al conjunto de subconjuntos abiertos de X . Demuestre que $\mathcal{O}(X)$ es una retícula completa donde el orden está dado por la contención y el supremo e ínfimo quedan descritos por la unión y tomar el interior de la intersección de una familia de conjuntos abiertos respectivamente.
14. Demuestre que $Sub({}_R M)$ es una retícula completa donde \leq está dado por \subseteq . Además, dada una familia de submódulos de ${}_R M$, $\{N_\alpha\}_{\alpha \in X}$, el ínfimo de la familia está dado por $\bigwedge_{\alpha \in X} N_\alpha = \bigcap_{\alpha \in X} N_\alpha$ y el supremo por $\bigvee_{\alpha \in X} N_\alpha = \ell(\bigcup_{\alpha \in X} N_\alpha)$.

Definición 2.3.2. Un subconjunto X de una retícula L es *dirigido* (resp. *codirigido*) si dados $x, y \in X$ existe $z \in X$ tal que $x \vee y \leq z$ (resp. $z \leq x \wedge y$).

Definición 2.3.3. Sea (L, \leq, \wedge, \vee) una retícula completa. Decimos que L es *superiormente continua* si

$$a \wedge \bigvee X = \bigvee \{a \wedge x \mid x \in X\}$$

para todo conjunto dirigido $X \subseteq L$.

15. Sea ${}_R M$ un R -módulo. Demuestre que $Sub({}_R M)$ es una retícula superiormente continua.
16. Sea $N \leq M$. Demuestre que la relación $\equiv (N)$ es de equivalencia.
17. Demuestre la Proposición 2.2.1.
18. Demuestre que si M es un módulo cíclico entonces todo cociente de M es cíclico.
19. Sea R un anillo, I un ideal bilateral y M un R -módulo izquierdo. Suponga que $IM = 0$. Demuestre que M es un R/I -módulo izquierdo.
20. Sea D un dominio entero y M un D -módulo. Considere el siguiente subconjunto de M :

$$t(M) = \{m \in M \mid rm = 0 \text{ para algún } r \in D\}.$$

Demuestre que $t(M)$ es un submódulo de M . A $t(M)$ se le llama el *submódulo de torsión* de M .

Capítulo 3

R -morfismos

3.1. R -morfismos

Definición 3.1.1. Si ${}_R M$ y ${}_R N$ son R -módulos una función $\varphi : M \rightarrow N$ es un R -morfismo si:

1. $\varphi(x + y) = \varphi(x) + \varphi(y)$
2. $\varphi(rx) = r\varphi(x)$

para todo $x, y \in M$ y todo $r \in R$.

Observación 3.1.2. $\varphi : {}_R M \rightarrow {}_R N$ es un R -morfismo si y solo si $\varphi(rx + y) = r\varphi(x) + \varphi(y)$ para todo $x, y \in M$ y todo $r \in R$.

Ejemplo 3.1.3. (i) Para cualesquiera dos módulos M y N tenemos el morfismo cero:

$$\begin{aligned} \bar{0} : \quad M &\longrightarrow N \\ m &\longmapsto 0 \quad \forall m \in M \end{aligned}$$

(ii) Sea ${}_R N \leq {}_R M$ y consideremos la función:

$$\begin{aligned} i : \quad N &\longrightarrow M \\ n &\longmapsto n \quad \forall n \in N \end{aligned}$$

Si $N = M$, entonces i es la identidad denotada Id_M . Si N es propio en M a i se le llama la *inclusión canónica* y se denotará con la flecha \hookrightarrow .

(iii) Si $N \leq {}_R M$, la función

$$\begin{aligned} \pi : \quad M &\longrightarrow M/N \\ m &\longmapsto m + N \end{aligned}$$

es R -morfismo al cual llamamos la *proyección canónica*. Para ver esto, sean $x, y \in M$ y $r \in R$

$$\begin{aligned}\pi(rx + y) &= (rx + y) + N = (rx + N) + (y + N) \\ &= r(x + N) + (y + N) = r\pi(x) + \pi(y)\end{aligned}$$

Lema 3.1.4. 1. *Composición de R -morfismos es un R -morfismo.*

2. *Si $\varphi : M \rightarrow N$ es un R -morfismo biyectivo entonces la función inversa de φ es un R -morfismo dado por $\varphi^{-1}(x) = u$ si $\varphi(u) = x$.*

Demostración. 1. Sean M, N, L R -módulos, $\varphi : M \rightarrow N$ y $\psi : N \rightarrow L$ R -morfismos $x, y \in M$ y $r \in R$ entonces

$$\psi\varphi(rx + y) = \psi(r\varphi(x) + \varphi(y)) = r\psi\varphi(x) + \psi\varphi(y)$$

2. Supongamos que φ es biyectiva con inversa φ^{-1} . Entonces

$$\begin{aligned}\varphi^{-1}(rn + l) &= \varphi^{-1}(r\varphi(x) + \varphi(y)) = \varphi^{-1}(\varphi(rx + y)) = rx + y \\ &= r\varphi^{-1}(n) + \varphi^{-1}(l)\end{aligned}$$

□

Observación 3.1.5. Sea $\varphi : M \rightarrow N$ un R -morfismo. Usaremos el termino *monomorfismo* para referirnos a que φ es inyectivo y usaremos el termino *epimorfismo* si φ es suprayectivo. Los terminos monomorfismo (resp. epimorfismo) y morfismo inyectivo (resp. suprayectivo) no son sinónimos, sin embargo en la teoría de módulos los conceptos coinciden (Vea la Definición A.1.3 y el Teorema A.1.5).

Definición 3.1.6. Sea $\varphi : M \rightarrow N$ un R -morfismo. Si φ es biyectivo, es decir, inyectivo y suprayectivo lo llamamos *isomorfismo*. Decimos que M es isomorfo a N y lo denotamos $M \cong N$ si existe un isomorfismo $\varphi : M \rightarrow N$.

Ejemplo 3.1.7. Consideremos \mathbb{Z} como \mathbb{Z} -módulo y sea $0 \neq n \in \mathbb{Z}$. Entonces $\mathbb{Z} \cong n\mathbb{Z}$ donde el isomorfismo está dado por $x \mapsto nx$.

Lema 3.1.8. *Sean M, N y L R -módulos. Entonces*

1. $M \cong M$.
2. si $M \cong N$ entonces $N \cong M$.
3. si $M \cong N$ y $N \cong L$ entonces $M \cong L$.

Lema 3.1.9. *Sea $\varphi : M \rightarrow N$ R -morfismo, $U \leq M$ y $V \leq N$ entonces:*

1. $\varphi(U) \leq N$.
2. $\varphi^{-1}(V) \leq M$

Demostración. 1. Sean $x, y \in U$ y $r \in R$ entonces $x = \varphi(u_1)$ y $y = \varphi(u_2)$ con $u_1, u_2 \in U$ así $rx + y = r\varphi(u_1) + \varphi(u_2) = \varphi(ru_1 + u_2) \in \varphi(U)$ por lo tanto $\varphi(U) \leq N$.

2. Sean $x, y \in \varphi^{-1}(V)$ y $r \in R$ entonces $\varphi(x) \in V$ y $\varphi(y) \in V$ así que $\varphi(rx + y) = r\varphi(x) + \varphi(y) \in V$ por lo tanto $rx + y \in \varphi^{-1}(V)$. \square

Definición 3.1.10. Sea $\varphi : M \rightarrow N$ es un *R*-morfismo.

1. El *núcleo* de φ se define como:

$$\text{Ker } \varphi = \varphi^{-1}(\{0\}) \leq M.$$

2. La *imagen* de φ se define como:

$$\text{Im } \varphi = \varphi(M) = \{n \in N \mid n = \varphi(m) \text{ para algún } m \in M\}.$$

3. El *conúcleo* de φ se define como:

$$\text{Coker } \varphi = N / \text{Im } \varphi.$$

Lema 3.1.11. Sea $\varphi : M \rightarrow N$ un *R*-morfismo.

1. Si $U \leq M$, entonces $\varphi^{-1}(\varphi(U)) = U + \text{Ker } \varphi$.

2. Si $V \leq N$, entonces $\varphi(\varphi^{-1}(V)) = V \cap \text{Im } \varphi$.

3. Si $\psi : N \rightarrow L$ es un *R*-morfismo, entonces:

a) $\text{Ker } \psi\varphi = \varphi^{-1}(\text{Ker } \psi)$.

b) $\text{Im } \psi\varphi = \psi(\text{Im } \varphi)$.

Demostración. 1. Sea $x \in \varphi^{-1}(\varphi(U))$, es decir, $\varphi(x) \in \varphi(U)$. Entonces existe $u \in U$ tal que $\varphi(u) = \varphi(x)$ y así $u - x \in \text{Ker } \varphi$. Por lo tanto $x = x + (u - x) \in U + \text{Ker } \varphi$. Recíprocamente, si $x \in U + \text{Ker } \varphi$, entonces $x = u + k$ con $u \in U$ y $k \in \text{Ker } \varphi$. Así $\varphi(x) = \varphi(u + k) = \varphi(u) + \varphi(k) = \varphi(u) + 0 = \varphi(u)$ lo que implica que $\varphi(x) \in \varphi(U)$. Por lo tanto $x \in \varphi^{-1}(\varphi(U))$.

2. Si $y \in \varphi(\varphi^{-1}(V))$ entonces $y = \varphi(x)$ para algún $x \in \varphi^{-1}(V)$, lo que implica que $y = \varphi(x) \in V$. Por lo tanto $y \in \text{Im } \varphi$ y $y \in V$, es decir, $y \in V \cap \text{Im } \varphi$. Recíprocamente, si $y \in V \cap \text{Im } \varphi$ entonces $y \in V$ y $y = \varphi(x)$ para algún $x \in M$. Entonces $x \in \varphi^{-1}(V)$ y por lo tanto $y \in \varphi(\varphi^{-1}(V))$.

3a) $x \in \text{Ker } \psi\varphi \Leftrightarrow \psi\varphi(x) = 0 \Leftrightarrow \varphi(x) \in \text{Ker } \psi \Leftrightarrow x \in \varphi^{-1}(\text{Ker } \psi)$.

3b) $x \in \text{Im } \psi\varphi \Leftrightarrow x = \psi\varphi(y)$ p. a. $y \in M \Leftrightarrow x \in \psi(\varphi(y)) \Leftrightarrow x \in \psi(\text{Im } \varphi)$. \square

Corolario 3.1.12. Sean A, B, C , y D *R*-módulos. Si el cuadrado

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ \downarrow \gamma & & \downarrow \beta \\ C & \xrightarrow{\delta} & D \end{array}$$

es conmutativo con γ sobre y β inyectivo, entonces:

1. $\text{Im } \alpha = \beta^{-1}(\text{Im } \delta)$
2. $\text{Ker } \delta = \gamma(\text{Ker } \alpha)$

Demostración. 1. Por el Lema 3.1.11, $\text{Im } \delta\gamma = \delta(\text{Im } \gamma) = \delta(C) = \text{Im } \delta$ pero también tenemos que $\text{Im } \delta\gamma = \text{Im } \beta\alpha = \beta(\text{Im } \alpha)$ por lo tanto $\text{Im } \delta = \beta(\text{Im } \alpha)$ entonces $\beta^{-1}(\text{Im } \delta) = \beta^{-1}\beta(\text{Im } \alpha) = \text{Im } \alpha$

2. Usando el Lema 3.1.11, $\text{Ker } \beta\alpha = \alpha^{-1}(\text{Ker } \beta) = \alpha^{-1}(0) = \text{Ker } \alpha$ pero $\text{Ker } \beta\alpha = \text{Ker } \delta\gamma = \gamma^{-1}(\text{Ker } \delta)$ así que $\text{Ker } \alpha = \gamma^{-1}(\text{Ker } \delta)$ entonces $\gamma(\text{Ker } \alpha) = \gamma\gamma^{-1}(\text{Ker } \delta) = \text{Ker } \delta$. \square

Proposición 3.1.13. *Son equivalentes para un R -morfismo $\varphi : M \rightarrow N$:*

- (a) φ es inyectiva.
- (b) $\text{Ker } \varphi = 0$

Demostración. (a) \Rightarrow (b). Sea $x \in \text{Ker } \varphi$ entonces $\varphi(x) = 0$ pero también $\varphi(0) = 0$ por ser φ R -morfismo y como φ es inyectiva entonces $x = 0$.

(b) \Rightarrow (a). Si $\varphi(x) = \varphi(y)$ se tiene que $\varphi(x - y) = 0$ entonces $x - y \in \text{Ker } \varphi$ por lo tanto $x = y$ y φ es inyectiva. \square

Proposición 3.1.14. *Son equivalentes para un R -morfismo $\varphi : M \rightarrow N$:*

- (a) φ es suprayectiva.
- (b) $\text{Coker}(\varphi) = 0$

Demostración. Solo hay que notar que φ es sobre si y sólo si $\text{Im } \varphi = N$ si y sólo si $N/\text{Im } \varphi = 0$. \square

Proposición 3.1.15. *Si $\varphi : A \rightarrow B$ es un R -morfismo, $\{A_i\}_{i \in I}$ es una familia de submódulos de A y $\{B_j\}_{j \in J}$ es una familia de submódulos de B , entonces:*

1. $\varphi\left(\sum_{i \in I} A_i\right) = \sum_{i \in I} \varphi(A_i)$.
2. $\varphi^{-1}\left(\bigcap_{j \in J} B_j\right) = \bigcap_{j \in J} \varphi^{-1}(B_j)$.
3. $\sum_{j \in J} \varphi^{-1}(B_j) \subseteq \varphi^{-1}\left(\sum_{j \in J} B_j\right)$. Si $B_j \subseteq \text{Im } \varphi$ para todo $j \in J$, entonces se da la igualdad.
4. $\varphi\left(\bigcap_{i \in I} A_i\right) \subseteq \bigcap_{i \in I} \varphi(A_i)$. Si $\text{Ker } \varphi \subseteq A_i$ para todo $i \in I$, entonces se da la igualdad.

Demostración. 1 y 2 se dejan como ejercicio.

3. $x \in \sum_{j \in J} \varphi^{-1}(B_j) \Leftrightarrow x = x_{j_1} + \dots + x_{j_n}$ con $x_{j_k} \in \varphi^{-1}(B_{j_k})$ entonces $\varphi(x) = \varphi(x_{j_1}) + \dots + \varphi(x_{j_n})$ con $\varphi(x_{j_k}) \in B_{j_k}$ así que $\varphi(x) \in \sum_{j \in J} B_j$ lo que implica que $x \in \varphi^{-1}\left(\sum_{j \in J} B_j\right)$. Ahora, si suponemos que $B_j \subseteq \text{Im } \varphi$ para toda $j \in J$ tenemos que

$$\varphi^{-1}\left(\sum_{j \in J} B_j\right) = \varphi^{-1}\left(\sum_{j \in J} (B_j \cap \text{Im } \varphi)\right) = \varphi^{-1}\left(\sum_{j \in J} \varphi(\varphi^{-1}(B_j))\right)$$

$$= \varphi^{-1} \left(\varphi \left(\sum_{j \in J} \varphi^{-1}(B_j) \right) \right) = \sum_{j \in J} \varphi^{-1}(B_j) + \text{Ker } \varphi = \sum_{j \in J} \varphi^{-1}(B_j).$$

4. $x \in \varphi(\bigcap_{i \in I} A_i) \Leftrightarrow x = \varphi(y)$ con $y \in \bigcap_{i \in I} A_i$ entonces $x \in \varphi(A_i)$ para toda $i \in I$, por lo tanto $x \in \bigcap_{i \in I} \varphi(A_i)$. Ahora, si suponemos que $\text{Ker } \varphi \subseteq A_i$ para toda $i \in I$ tenemos que

$$\begin{aligned} \varphi \left(\bigcap_{i \in I} A_i \right) &= \varphi \left(\left(\bigcap_{i \in I} A_i \right) + \text{Ker } \varphi \right) = \varphi \left(\bigcap_{i \in I} \varphi^{-1}(\varphi(A_i)) \right) \\ &= \varphi \left(\varphi^{-1} \left(\bigcap_{i \in I} \varphi(A_i) \right) \right) = \bigcap_{i \in I} \varphi(A_i) \cap \text{Im } \varphi = \bigcap_{i \in I} \varphi(A_i). \end{aligned}$$

□

3.2. Teoremas de Isomorfismo

Teorema 3.2.1. *Todo R -morfismo $\varphi : M \rightarrow N$ se puede factorizar como $\varphi = \varphi_1\varphi_2$ donde φ_1 es monomorfismo y φ_2 es epimorfismo.*

Demostración. Tomemos el módulo $M/\text{Ker } \varphi$ y $\varphi_2 = \pi : M \rightarrow M/\text{Ker } \varphi$ la proyección canónica. Definimos $\varphi_1 : M/\text{Ker } \varphi \rightarrow N$ como $\varphi_1(m + \text{Ker } \varphi) = \varphi(m)$. Notemos que

$$\begin{aligned} m + \text{Ker } \varphi = m' + \text{Ker } \varphi &\Leftrightarrow m - m' \in \text{Ker } \varphi \Leftrightarrow \varphi(m - m') = 0 \\ &\Leftrightarrow \varphi(m) - \varphi(m') = 0 \Leftrightarrow \varphi(m) = \varphi(m'). \end{aligned}$$

Por lo tanto φ_1 está bien definida y es inyectiva. Además, φ_1 es R -morfismo ya que $\varphi_1(r(m + \text{Ker } \varphi) + (n + \text{Ker } \varphi)) = \varphi_1((rm + n) + \text{Ker } \varphi) = \varphi(rm + n) = r\varphi(m) + \varphi(n) = r\varphi_1(m + \text{Ker } \varphi) + \varphi_1(n + \text{Ker } \varphi)$. Más aún, como $\text{Im } \varphi = \text{Im } \varphi_1$ se tiene que φ es epi si y solo si φ_1 es un isomorfismo. \square

Teorema 3.2.2 (1er Teorema de Isomorfismo). *Si $\varphi : M \rightarrow N$ es un R -morfismo entonces $M/\text{Ker } \varphi \cong \text{Im } \varphi$.*

Demostración. Por el Teorema 3.2.1. \square

Teorema 3.2.3 (2do Teorema de Isomorfismo). *Sean $H, K \leq M$. Entonces $(H + K)/K \cong H/(H \cap K)$.*

Demostración. Tomemos $f : H \rightarrow (H + K)/K$ definida como $f(h) = h + K$. Entonces $\text{Ker } f = \{h \in H \mid h + K = K\} = H \cap K$. Por 1er Teorema de isomorfismo (Teorema 3.2.2) $(H + K)/K \cong H/(H \cap K)$. \square

Teorema 3.2.4 (3er Teorema de Isomorfismo). *Sean $K \leq L \leq M$. Entonces $M/L \cong (M/K)/(L/K)$.*

Demostración. Tomemos $f : M/K \rightarrow M/L$ definida como $f(m + K) = m + L$. Notemos que

$$m + K = m' + K \Leftrightarrow m - m' \in K \Rightarrow m - m' \in L \Leftrightarrow m + L = m' + L.$$

Por lo tanto f está bien definida y es sobre. Además $m + K \in \text{Ker } f \Leftrightarrow f(m + K) = L \Leftrightarrow m + L = L \Leftrightarrow m \in L$ así que $\text{Ker } f = \{m + K \mid m \in L\} = L/K$. Por el 1er Teorema de isomorfismo (Teorema 3.2.2) $M/L = (M/K)/(L/K)$. \square

Corolario 3.2.5. 1. *Si $M = N \oplus L$ entonces $M/N \cong L$.*

2. *Un R -módulo M es cíclico si y solo si M es cociente de R .*

Demostración. 1. $M/N \cong (N \oplus L)/N \cong L/(N \cap L) \cong L/0 \cong L$.

2 \Rightarrow . Supongamos que $M = Rx$ para algún $x \in M$. Consideremos el R -morfismo $(\cdot x) : R \rightarrow Rx$ multiplicar por x por la izquierda. Por el 1er Teorema de isomorfismo (Teorema 3.2.2) $M = Rx \cong R/\text{Ker}(\cdot x)$.

3 \Leftarrow . Si $M \cong R/I$ para algún ideal izquierdo I de R , entonces $R(1+I) = R/I$. Por lo tanto M es cíclico. \square

Definición 3.2.6. Dado un módulo M is $x \in M$, el anulador de x se define como $\text{Ker}(\cdot \cdot x) = \{r \in R \mid rx = 0\}$ y lo denotaremos $(0 : x)$.

Lema 3.2.7 (Zassenhaus). Sea M un R -módulo y $U, U', V, V' \leq M$ tales que $U' \leq U \leq M$ y $V' \leq V \leq M$ entonces $\frac{U'+(U \cap V)}{U'+(U \cap V')} \cong \frac{V'+(U \cap V)}{V'+(U \cap V)}$.

Demostración. Tenemos que $U \cap V' \leq U \cap V$. Entonces

$$\frac{U' + (U \cap V)}{U' + (U \cap V')} = \frac{(U \cap V) + (U' + (U \cap V'))}{U' + (U \cap V')} \cong \frac{U \cap V}{(U \cap V) \cap (U' + (U \cap V'))},$$

por el 2do Teorema de isomorfismo. Pero por la ley modular 2.1.12,

$$(U \cap V) \cap U' + (U \cap V') = U \cap V \cap U' + U \cap V' = V \cap U' + U \cap V'.$$

Por lo tanto $\frac{U \cap V}{(U \cap V) \cap (U' + (U \cap V'))} = \frac{U \cap V}{V \cap U' + U \cap V'}$. Análogamente se tiene que

$$\frac{V' + (U \cap V)}{V' + (U' \cap V)} \cong \frac{U \cap V}{V' \cap U + U' \cap V}.$$

□

Proposición 3.2.8. Sea $\varphi : M \rightarrow N$ un R -morfismo.

1. Sea $\alpha : M \rightarrow M'$ un epimorfismo tal que $\text{Ker } \alpha \subseteq \text{Ker } \varphi$. Entonces existe un único R -morfismo $\beta : M' \rightarrow N$ tal que $\varphi = \beta\alpha$.
2. Sea $\gamma : N' \rightarrow N$ un monomorfismo tal que $\text{Im } \varphi \subseteq \text{Im } \gamma$. Entonces existe un único $\delta : M \rightarrow N'$ tal que $\varphi = \gamma\delta$.

Demostración. 1. Definimos $\beta : M' \rightarrow N$ como $\beta(y) = \varphi(x)$ si $\alpha(x) = y$. Notemos que si $\alpha(x) = \alpha(x')$, entonces $x - x' \in \text{Ker } \alpha \subseteq \text{Ker } \varphi$. Así que $\varphi(x) = \varphi(x')$. Por lo tanto β esta bien definida. Ahora, veamos que β es un R -morfismo. Sean $y_1, y_2 \in M'$ tales que $\alpha(x_1) = y_1$ y $\alpha(x_2) = y_2$ y sea $r \in R$. Entonces $r\beta(y_1) + \beta(y_2) = r\varphi(x_1) + \varphi(x_2) = \varphi(rx_1 + x_2)$. Como $\alpha(rx_1 + x_2) = ry_1 + y_2$, $\beta(ry_1 + y_2) = \varphi(rx_1 + x_2) = r\beta(y_1) + \beta(y_2)$. Por la forma de definir β , ésta es única y $\varphi = \beta\alpha$. Además β es mono si y solo si $\text{Ker } \alpha = \text{Ker } \varphi$, y β es epi si y solo si φ es epi.

2. Definimos $\delta : M \rightarrow N'$ como $\delta(x) = y$ donde $\gamma(y) = \varphi(x)$. Notemos que si $\varphi(x) = \gamma(y')$ entonces $\gamma(y) = \gamma(y') \Leftrightarrow y - y' \in \text{Ker } \gamma = \{0\}$ entonces $y = y'$. Por lo tanto δ esta bien definida y es única. Claramente, $\gamma\delta = \varphi$. Además δ es mono si y solo si φ es mono, y δ es epi si y solo si $\text{Im } \varphi = \text{Im } \gamma$. □

Definición 3.2.9. 1. $N \leq M$ se llama *sumando directo* de M , si existe $L \leq M$ tal que $N \oplus L = M$

2. Decimos que un monomorfismo $\alpha : M \rightarrow N$ se *escinde* si $\text{Im } \alpha$ es un sumando directo de N .
3. Decimos que un epimorfismo $\beta : M \rightarrow N$ se *escinde* si $\text{Ker } \beta$ es un sumando directo de M .

Lema 3.2.10. Si el siguiente diagrama

$$\begin{array}{ccc} L & \xrightarrow{\alpha} & N \\ & \searrow \lambda & \downarrow \beta \\ & & M \end{array}$$

es conmutativo, entonces:

1. $\text{Im } \alpha + \text{Ker } \beta = \beta^{-1}(\text{Im } \lambda)$.
2. $\text{Im } \alpha \cap \text{Ker } \beta = \alpha(\text{Ker } \lambda)$.

Demostración. 1. $\text{Im } \lambda = \text{Im } \beta\alpha = \beta(\text{Im } \alpha)$, entonces $\beta^{-1}(\text{Im } \lambda) = \beta^{-1}(\beta(\text{Im } \alpha)) = \text{Im } \alpha + \text{Ker } \beta$.

2. $\text{Ker } \lambda = \text{Ker } \beta\alpha = \alpha^{-1}(\text{Ker } \beta)$, entonces $\alpha(\text{Ker } \lambda) = \alpha(\alpha^{-1}(\text{Ker } \beta)) = \text{Ker } \beta \cap \text{Im } \alpha$. □

Corolario 3.2.11. Con el diagrama del lema anterior.

1. Si λ es un epimorfismo, entonces $\text{Im } \alpha + \text{Ker } \beta = N$.
2. Si λ es un monomorfismo, entonces $\text{Im } \alpha \cap \text{Ker } \beta = 0$.
3. Si λ es un isomorfismo, entonces $\text{Im } \alpha \oplus \text{Ker } \beta = N$.

Corolario 3.2.12. Son equivalentes para $\alpha : M \rightarrow N$:

- (a) α es mono y se escinde.
- (b) Existe $\beta : N \rightarrow M$ tal que $\beta\alpha = \text{Id}_M$

Demostración. (a) \Rightarrow (b). Supongamos que α es un monomorfismo y que $\text{Im } \alpha \oplus N' = N$ para $N' \leq N$. Sea $\alpha_0 : M \rightarrow \text{Im } \alpha$ la corresticción de α a su imagen. Como α es mono, α_0 es un isomorfismo. Sea $\rho : N \rightarrow \text{Im } \alpha$ la proyección canónica y sea $\beta = \alpha_0\rho$. Entonces, para todo $m \in M$ se tiene que

$$\beta\alpha(m) = \alpha_0\rho\alpha(m) = \alpha_0\rho(\alpha(m)) = \alpha_0(\alpha(m)) = m.$$

Por lo tanto $\beta\alpha = \text{Id}_M$.

(b) \Rightarrow (a). Por hipótesis tenemos el siguiente diagrama conmutativo

$$\begin{array}{ccc} M & \xrightarrow{\alpha} & N \\ & \searrow \text{Id} & \downarrow \beta \\ & & M \end{array}$$

Por el corolario anterior $N = \text{Im } \alpha \oplus \text{Ker } \beta$. Además α es mono ya que Id_M es mono. □

Corolario 3.2.13. Son equivalentes para $\gamma : N \rightarrow L$:

- (a) γ es epi y se escinde.
- (b) Existe $\delta : L \rightarrow N$ tal que $\gamma\delta = \text{Id}_L$.

3.3. Sucesiones Exactas

Definición 3.3.1. Una *sucesión exacta* de R -módulos, es una sucesión de R -morfismos

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \cdots \longrightarrow M_j \xrightarrow{f_j} M_{j+1}$$

tal que $\text{Ker } f_{i+1} = \text{Im } f_i$ para todo $i > 0$. Si la sucesión

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

es exacta decimos que es una *sucesión exacta corta*.

Observación 3.3.2. Sea

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

una sucesión exacta corta. Entonces:

1. f es un monomorfismo.
2. g es un epimorfismo.

Lema 3.3.3. *Sea*

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C \\ \alpha \downarrow & & \beta \downarrow & & \gamma \downarrow \\ A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' \end{array}$$

conmutativo y con renglones exactos.

1. Si γ, α, f' son monomorfismos, entonces β es monomorfismo.
2. Si α, γ, g son epimorfismos, entonces β es epi.
3. Si β es monomorfismo y α, g epimorfismos, entonces γ es monomorfismo.
4. Si β es epimorfismo y f', γ monomorfismos, entonces α es epi.

Demostración. 1. Sea $b \in B$ tal que $\beta(b) = 0$. Como el diagrama es conmutativo entonces $\gamma(g(b)) = 0$ pero γ es monomorfismo entonces $g(b) = 0$, i.e. $b \in \text{Ker } g = \text{Im } f$. Entonces existe $a \in A$ tal que $f(a) = b$. Por la conmutatividad del diagrama $f'(\alpha(a)) = \beta(f(a)) = \beta(b) = 0$ pero α y f' son monomorfismos, así que $a = 0$ y $f(a) = 0$. Por lo tanto $b = 0$ y β es un monomorfismo.

2. Sea $x \in B'$ y tomemos $g'(x) \in C'$. Como γ es sobre existe $c \in C$ tal que $\gamma(c) = g'(x)$ y como g también es sobre existe $b \in B$ tal que $g(b) = c$. Entonces $\gamma(g(b)) = g'(x) = g'(\beta(b))$ ya que el diagrama conmuta. Tomemos $x - \beta(b) \in B'$. Entonces $g'(x - \beta(b)) = 0$, es decir, $x - \beta(b) \in \text{Ker } g' = \text{Im } f'$ por lo que existe $w \in A'$ tal que $f'(w) = x - \beta(b)$. Como α es sobre existe $a \in A$ tal que $\alpha(a) = w$, lo que implica $\beta(f(a)) = f'(\alpha(a)) = f'(w) = x - \beta(b)$. Tomemos $f(a) + b \in B$. Así $\beta(f(a) + b) = \beta(f(a)) + \beta(b) = x - \beta(b) + \beta(b) = x$. Por lo tanto β es un epimorfismo.

3. Sea $c \in C$ tal que $\gamma(c) = 0$. Como g es sobre existe $b \in B$ tal que $g(b) = c$, entonces $g'(\beta(b)) = \gamma(g(b)) = 0$ lo que implica que $\beta(b) \in \text{Ker } g' = \text{Im } f'$. Así que existe $x \in A'$ tal que $f'(x) = \beta(b)$. Como α es sobre existe $a \in A$

tal que $\alpha(a) = x$ y así $f'(\alpha(a)) = \beta(f(a)) = \beta(b)$ pero β es monomorfismo, entonces $f(a) = b$. Entonces, $0 = g(f(a)) = g(b) = c$ y por lo tanto γ es un monomorfismo.

4. Sea $x \in A'$. Entonces $g'(f'(x)) = 0$. Como β es sobre existe $b \in B$ tal que $\beta(b) = f'(x)$. Así $\gamma(g(b)) = g'(\beta(b)) = g'(f'(x)) = 0$ pero γ es monomorfismo, lo que implica que $g(b) = 0$, es decir, $b \in \text{Ker } g = \text{Im } f$. Entonces existe $a \in A$ tal que $f(a) = b$, lo que implica que $f'(\alpha(a)) = \beta(f(a)) = \beta(b) = f'(x)$ pero f' es monomorfismo así que $\alpha(a) = x$. Por lo tanto α es un epimorfismo. \square

Lema 3.3.4 (del quinto). *Considere el siguiente diagrama conmutativo*

$$\begin{array}{ccccccccc} A & \xrightarrow{f_1} & B & \xrightarrow{f_2} & C & \xrightarrow{f_3} & D & \xrightarrow{f_4} & E \\ \alpha \downarrow & & \beta \downarrow & & \gamma \downarrow & & \delta \downarrow & & \epsilon \downarrow \\ A' & \xrightarrow{g_1} & B' & \xrightarrow{g_2} & C' & \xrightarrow{g_3} & D' & \xrightarrow{g_4} & E' \end{array}$$

con renglones exactos.

1. Si α es epimorfismo y β, δ monomorfismos, entonces γ es un monomorfismo.
2. Si ϵ es monomorfismo y β, δ son epimorfismos, entonces γ es un epimorfismo.
3. Si ϵ es monomorfismo, α epimorfismo y β, δ isomorfismos, entonces γ es un isomorfismo.

Demostración. 1. Sea $c \in C$ tal que $\gamma(c) = 0$. Entonces $\delta(f_3(c)) = g_3(\gamma(c)) = g_3(0) = 0$ pero δ es monomorfismo así que $f_3(c) = 0$. Entonces $c \in \text{Ker } f_3 = \text{Im } f_2$ por lo que existe $b \in B$ tal que $f_2(b) = c$. Ahora, $g_2(\beta(b)) = \gamma(f_2(b)) = \gamma(c) = 0$ entonces $\beta(b) \in \text{Ker } g_2 = \text{Im } g_1$. Así, existe $x \in A'$ tal que $g_1(x) = \beta(b)$. Como α es epimorfismo existe $a \in A$ tal que $\alpha(a) = x$. Tenemos que $\beta(f_1(a)) = g_1(\alpha(a)) = g_1(x) = \beta(b)$ pero β es monomorfismo, entonces $f_1(a) = b$. Así que $c = f_2(b) = f_2(f_1(a)) = 0$ y por lo tanto γ es un monomorfismo.

2. Sea $c' \in C'$. Entonces $g_4(g_3(c')) = 0$. Como δ es epimorfismo, existe $d \in D$ tal que $\delta(d) = g_3(c')$, Así, $\epsilon(f_4(d)) = g_1(\delta(d)) = g_4(g_3(c')) = 0$ pero ϵ es monomorfismo, así que $f_4(d) = 0$ i.e. $d \in \text{Ker } f_4 = \text{Im } f_3$. Por lo tanto existe $c \in C$ tal que $f_3(c) = d$ y se sigue que $g_3(\gamma(c)) = \delta(f_3(c)) = \delta(d) = g_3(c')$. Entonces $g_3(c' - \gamma(c)) = 0$ i.e. $c' - \gamma(c) \in \text{Ker } g_3 = \text{Im } g_2$ por lo que existe $w \in B'$ tal que $g_2(w) = c' - \gamma(c)$. Como β es epimorfismo, existe $b \in B$ tal que $\beta(b) = w$. Entonces $\gamma(f_2(b)) = g_2(\beta(b)) = g_2(w) = c' - \gamma(c)$. Tomando $c + f_2(b)$ tenemos que $\gamma(c + f_2(b)) = \gamma(c) + \gamma(f_2(b)) = \gamma(c) + c' - \gamma(c) = c'$. Por lo tanto γ es un epimorfismo.

3. Se sigue de 1 y 2. \square

Corolario 3.3.5. *Si tenemos el siguiente diagrama conmutativo*

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow \cong & & \downarrow & & \downarrow \cong & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

con renglones exactos y se tiene que $A \cong A'$ y $C \cong C'$, entonces $B \cong B'$.

Definición 3.3.6. Decimos que la sucesión exacta corta

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

se escinde si $\text{Im } f = \text{Ker } g$ es un sumando directo de B .

Ejemplo 3.3.7. (I) Dada una suma directa $M = N \oplus L$ siempre hay una sucesión exacta corta canónica que se escinde:

$$0 \longrightarrow N \xrightarrow{i} M \xrightarrow{\pi} L \longrightarrow 0$$

donde $i : N \rightarrow M$ es la inclusión canónica dada por $i(n) = n + 0$ y $\pi : M \rightarrow L$ es la proyección canónica dada por $\pi(n + l) = l$.

(II) Sea K un campo y considere el anillo de matrices de 2×2 triangulares inferiores con coeficientes en K , i.e.,

$$R = \begin{pmatrix} K & 0 \\ K & K \end{pmatrix}.$$

Considere la sucesión exacta corta

$$0 \rightarrow \begin{pmatrix} 0 & 0 \\ K & 0 \end{pmatrix} \xrightarrow{f} R \xrightarrow{g} \begin{pmatrix} K & 0 \\ K & 0 \end{pmatrix} \rightarrow 0$$

donde $f \begin{pmatrix} 0 & 0 \\ a & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix}$ y $g \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$. Entonces esta sucesión se escinde.

Las pruebas de las siguientes proposiciones se siguen de las definiciones.

Proposición 3.3.8. Son equivalentes para un monomorfismo $\varphi : M \rightarrow N$:

- (a) φ se escinde.
- (b) La sucesión exacta $0 \rightarrow M \xrightarrow{\varphi} N \rightarrow \text{Coker } \varphi \rightarrow 0$ se escinde.

Proposición 3.3.9. Son equivalentes para un epimorfismo $\varphi : M \rightarrow N$:

- (a) φ se escinde.
- (b) La sucesión exacta $0 \rightarrow \text{Ker } \varphi \rightarrow M \xrightarrow{\varphi} N \rightarrow 0$ se escinde.

3.4. El grupo de R -morfismos Hom_R

Definición 3.4.1. Dados ${}_R M$ y ${}_R N$ R -módulos definimos $\text{Hom}_R(M, N) := \{f : M \rightarrow N \mid f \text{ es } R\text{-morfismo}\}$.

Lema 3.4.2. Sean M y N R -módulos. Entonces $\text{Hom}_R(M, N)$ es un grupo abeliano.

Demostración. Para $f, g \in \text{Hom}_R(M, N)$ definimos su suma como el morfismo $f + g : M \rightarrow N$ $(f + g)(x) = f(x) + g(x)$. Entonces $f + g \in \text{Hom}_R(M, N)$ y se tiene que $(\text{Hom}_R(M, N), +, \bar{0})$ es un grupo abeliano. \square

Observación 3.4.3. Dado $f \in \text{Hom}_R(M, N)$ y $r \in R$, si consideramos $rf : M \rightarrow N$ como $(rf)(x) = rf(x)$ no siempre se tiene que rf sea un R -morfismo ya que para $s \in R$, $(rf)(sx) = rf(sx) = rsf(x)$ el cual es distinto de $sr f(x) = s(rf)(x)$ si $sr \neq rs$.

Definición 3.4.4. Sean R y S anillos y M un grupo abeliano. Se dice que M es un R - S -bimódulo (${}_R M_S$) si M es un R -módulo izquierdo y M es un S -módulo derecho tal que $(rx)s = r(xs)$ para todo $r \in R$, todo $s \in S$ y todo $x \in M$.

Ejemplo 3.4.5. (I) Un anillo R es un R - R -bimódulo canónicamente con la multiplicación.

(II) Si R es un anillo conmutativo y M es un R -módulo izquierdo, entonces M es un R - R -bimódulo con la siguiente acción derecha: $m \cdot r = rm$ para todo $r \in R$ y todo $m \in M$ (Ejercicio 1.3.14).

(III) Sean $n, \ell > 0$ y K un campo. Entonces el grupo abeliano $M_{n \times \ell}(K)$ es un $M_n(K)$ - $M_\ell(K)$ -bimódulo con la multiplicación de matrices.

Proposición 3.4.6. Sea ${}_R M_S$ un R - S -bimódulo y ${}_R N$ un R -módulo. Entonces $\text{Hom}_R(M, N)$ es un S -módulo izquierdo.

Demostración. Sean M un R - S -bimódulo y que N es un R -módulo. Para cada $s \in S$ y $f \in \text{Hom}_R(M, N)$, definimos $sf : M \rightarrow N$ como $(sf)(x) = f(xs)$. Entonces $(sf)(rx + y) = f((rx + y)s) = f(rxs + ys) = f(rxs) + f(ys) = rf(xs) + f(ys) = r(sf)(x) + (sf)(y)$ por lo tanto $sf \in \text{Hom}_R(M, N)$. Por lo tanto ${}_S \text{Hom}({}_R M_S, {}_R N)$ es un S -módulo izquierdo. \square

Teorema 3.4.7. Para todo R -módulo M , ${}_R M \cong {}_R \text{Hom}(R, M)$.

Demostración. Como R es un R - R -bimódulo, $\text{Hom}_R(R, M)$ es un R -módulo izquierdo. Definimos $\rho : M \rightarrow \text{Hom}_R(R, M)$ de la siguiente manera: dado $m \in M$, $\rho(x) : R \rightarrow M$ está dado por $\rho(m)(r) = rm$ para todo $r \in R$. Veamos que ρ es un R -morfismo. Sean $r, s \in R$ y $m, n \in M$. Entonces

$$\begin{aligned} \rho(rm + n)(s) &= s(rm + n) = srm + sn = \rho(m)(sr) + \rho(n)(s) \\ &= (r\rho)(m)(s) + \rho(n)(s) = (r\rho(m) + \rho(n))(s). \end{aligned}$$

Además, si $f \in \text{Hom}_R(R, M)$, tomando $f(1) = x$, se tiene que $f(r) = f(r1) = rf(1) = rx$. Por lo tanto ρ es un epimorfismo. Ahora, si $\rho(x) = \bar{0}$, entonces $rx = \rho(x)(r) = 0$ para todo $r \in R$. En particular $0 = 1x = x$. Por lo tanto ρ es un monomorfismo. Entonces ρ es un isomorfismo. \square

Observación 3.4.8. Para todo R -módulo M , el grupo $\text{Hom}_R(M, M)$ es un anillo no trivial, con multiplicación la composición si y solo si $M \neq 0$. A este anillo lo llamamos el *anillo de endomorfismos* de M y lo denotamos por $\text{End}_R(M)$.

Proposición 3.4.9. Sean M y N R -módulos simples. Entonces todo elemento no cero de $\text{Hom}_R(M, N)$ es un isomorfismo. En particular, si S es simple, $\text{End}_R(S)$ es un anillo con división.

Demostración. Supongamos que M y N son R -módulos simples, si $\varphi : M \rightarrow N$ es un R -morfismo y $\varphi \neq \bar{0}$ entonces $\text{Ker } \varphi = 0$ ya que $\text{Ker } \varphi < M$. Por lo tanto φ es un monomorfismo. Además $0 \neq \varphi(M) \leq N$, así que $\varphi(M) = N$. Esto implica que φ es un epimorfismo. Por lo tanto φ es un isomorfismo. Se sigue que el anillo de endomorfismos $\text{End}_R(S)$ de un R -módulo simple ${}_R S$ es un anillo con división. \square

Observación 3.4.10. Notemos que si M es un R -módulo tal que $\text{End}_R(M)$ es un anillo con división no implica que M sea un R -módulo simple. Para ver esto, consideremos el \mathbb{Z} -módulo \mathbb{Q} el cual no es simple pero $\text{End}_{\mathbb{Z}}(\mathbb{Q}) \cong \mathbb{Q}$ (Ejercicio 3.5.4).

Observación 3.4.11. Por el Teorema 3.4.7, ${}_R R \cong \text{End}_R(R)$. Se puede ver que este isomorfismo cumple que si $f, g \in \text{End}_R(R)$ entonces $\rho(fg) = \rho(g)\rho(f)$. Dado un anillo R , se define el *anillo opuesto* de R , denotado R^{op} , como el anillo con la misma suma que R pero con producto $a \cdot b = ba$ para todo $a, b \in R^{op}$. Así, tenemos un isomorfismo de anillos $R^{op} \cong \text{End}_R(R)$.

Proposición 3.4.12. Sea $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$ una sucesión exacta corta y N cualquier R -módulo. Entonces la sucesión

$$0 \rightarrow \text{Hom}_R(C, N) \xrightarrow{g^*} \text{Hom}_R(B, N) \xrightarrow{f^*} \text{Hom}_R(A, N)$$

con $f^*(\psi) = \psi f$ y $g^*(\varphi) = \varphi g$, es una sucesión exacta de \mathbb{Z} -módulos.

Demostración. Sea

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

una sucesión exacta corta, apliquemos el funtor $\text{Hom}_R(-, N)$ a la sucesión

$$0 \longrightarrow \text{Hom}_R(C, N) \xrightarrow{g^*} \text{Hom}_R(B, N) \xrightarrow{f^*} \text{Hom}_R(A, N)$$

donde $f^* = \text{Hom}_R(f, N)$ y $g^* = \text{Hom}_R(g, N)$. Si $g^*(\varphi) = 0$ entonces $\varphi g = 0$. Como g es sobre, $\varphi = 0$. Lo que implica que g^* es monomorfismo. Sea $\varphi \in \text{Ker } f^*$, i.e., $\varphi f = 0$. Podemos definir $\psi : C \rightarrow N$ como $\psi(g(x)) = \varphi(x)$ y así $\varphi = g^*(\psi)$. Ahora si $\varphi \in \text{Im } g^*$ se tiene que $\varphi = \psi g$ para algún $\psi : C \rightarrow N$ lo que implica que $\varphi f = \psi g f = 0$. Por lo tanto $\text{Ker } f^* = \text{Im } g^*$. \square

Proposición 3.4.13. Sea $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$ una sucesión exacta corta y M cualquier R -módulo. Entonces la sucesión

$$0 \rightarrow \text{Hom}_R(M, A) \xrightarrow{f_*} \text{Hom}_R(M, B) \xrightarrow{g_*} \text{Hom}_R(M, C)$$

con $f_*(\varphi) = f\varphi$ y $g_*(\psi) = g\psi$, es una sucesión exacta de \mathbb{Z} -módulos.

Ejemplo 3.4.14. Sea $n > 0$. Considere la sucesión exacta canónica

$$0 \rightarrow n\mathbb{Z} \xrightarrow{\iota} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_n \rightarrow 0.$$

Por la Proposición 3.4.13, hay una sucesión exacta

$$0 \rightarrow \mathrm{Hom}_R(\mathbb{Z}_n, n\mathbb{Z}) \xrightarrow{\iota_*} \mathrm{Hom}_R(\mathbb{Z}_n, \mathbb{Z}) \xrightarrow{\pi_*} \mathrm{Hom}_R(\mathbb{Z}_n, \mathbb{Z}_n).$$

En este caso $\mathrm{Hom}_R(\mathbb{Z}_n, \mathbb{Z}) = 0$ pero $\mathrm{Hom}_R(\mathbb{Z}_n, \mathbb{Z}_n) \neq 0$ lo que implica que π_* no es suprayectiva.

3.5. Ejercicios

1. Sean ${}_K V$ y ${}_K W$ espacios vectorial sobre el campo K . Entonces $f : V \rightarrow W$ es una transformación lineal si y solo si f es un K -morfismo.
2. Demuestre el Lemma 3.1.8.
3. Demuestre 1 y 2 de la Proposición 3.1.15.
4. Demuestre que $\text{End}_{\mathbb{Z}}(\mathbb{Q}) \cong \mathbb{Q}$ (como anillos).
5. Sea $n \in \mathbb{Z}$. Demuestre que $\text{End}_R(\mathbb{Z}_n) \cong \mathbb{Z}_n$ (como anillos).
6. Sea M un R -módulo y $x, y \in M$. Demuestre que son equivalentes:
 - (a) $Rx \cong Ry$.
 - (b) $(0 : x) = (0 : y)$.
7. Si $m, n \in \mathbb{Z}$ son enteros no cero ¿Cuántos \mathbb{Z} -morfismos hay de \mathbb{Z}_n a \mathbb{Z}_m ?
8. Sean $K, L \leq M$ tales que $M = K \oplus L$. Suponga que existen R -morfismos $\varphi_1 : K \rightarrow N$ y $\varphi_2 : L \rightarrow N$. Demuestre que existe un único R -morfismo $\varphi : M \rightarrow N$ tal que $\varphi|_K = \varphi_1$ y $\varphi|_L = \varphi_2$.
9. Sean $N, L \leq M$. Demuestre que si $N \cap L = 0$ entonces M/N tiene un submódulo isomorfo a L .
10. Demuestre el Corolario 3.2.13.
11. **Propiedad universal del núcleo.** Sea $\varphi : M \rightarrow N$ un R -morfismo. Suponga que existe $\psi : M' \rightarrow M$ tal que $\varphi\psi = 0$. Demuestre que existe un único R -morfismo $\bar{\psi} : M' \rightarrow \text{Ker } \varphi$ tal que $i\bar{\psi} = \psi$ donde $i : \text{Ker } \varphi \rightarrow M$ es la inclusión.

$$\begin{array}{ccccc}
 & & M' & & \\
 & \swarrow \bar{\psi} & \downarrow \psi & \searrow 0 & \\
 \text{Ker } \varphi & \xrightarrow{\varphi} & M & \xrightarrow{\varphi} & N
 \end{array}$$

12. **Propiedad universal del conúcleo.** Sea $\varphi : M \rightarrow N$ un R -morfismo. Suponga que existe $\psi : N \rightarrow N'$ tal que $\psi\varphi = 0$. Demuestre que existe un único R -morfismo $\bar{\psi} : \text{Coker } \varphi \rightarrow N'$ tal que $\bar{\psi}\pi = \psi$ donde $\pi : N \rightarrow \text{Coker } \varphi$ es la proyección canónica.

$$\begin{array}{ccccc}
 M & \xrightarrow{\varphi} & N & \twoheadrightarrow & \text{Coker } \varphi \\
 & \searrow 0 & \downarrow \psi & \swarrow \bar{\psi} & \\
 & & N' & &
 \end{array}$$

13. Demuestre la Observación 3.3.2.

14. **Lema del 3×3 .** Suponga que tiene el siguiente diagrama con columnas exactas

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & A'' & \longrightarrow & B'' & \longrightarrow & C'' \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
 \end{array}$$

Demuestre que si los dos renglones de arriba son exactos entonces el renglón de abajo también lo es. Demuestre que si los dos renglones de abajo son exactos, entonces el renglón de arriba también lo es.

15. **Lema de la serpiente.** Considere el siguiente diagrama con columnas exactas y los dos renglones intermedios exactos

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & \text{Ker } f & & \text{Ker } g & & \text{Ker } h \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C \longrightarrow 0 \\
 & & \downarrow f & & \downarrow g & & \downarrow h \\
 0 & \longrightarrow & A' & \xrightarrow{\alpha'} & B' & \xrightarrow{\beta'} & C' \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & \text{Coker } f & & \text{Coker } g & & \text{Coker } h \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
 \end{array}$$

Demuestre que hay una sucesión exacta

$$0 \rightarrow \text{Ker } f \rightarrow \text{Ker } g \rightarrow \text{Ker } h \xrightarrow{\delta} \text{Coker } f \rightarrow \text{Coker } g \rightarrow \text{Coker } h \rightarrow 0.$$

16. Sea $0 \rightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \rightarrow 0$ una sucesión exacta corta. Demuestre que son equivalentes:
- La sucesión se escinde.
 - Existe un R -morfismo $\alpha : B \rightarrow A$ tal que $\alpha\varphi = Id_A$.
 - Existe un R -morfismo $\beta : C \rightarrow B$ tal que $\psi\beta = Id_C$.

(d) Existen R -morfismos $\alpha : B \rightarrow A$, $\beta : C \rightarrow B$ tales que la sucesión

$$0 \rightarrow C \xrightarrow{\beta} B \xrightarrow{\alpha} A \rightarrow 0$$

es exacta corta y se cumple que $\alpha\varphi = Id_A$ y $\psi\beta = Id_C$.

17. Sea R un anillo. Suponga que hay una sucesión exacta corta de R -módulos

$$0 \rightarrow A \rightarrow B \rightarrow R \rightarrow 0.$$

Demuestre que la sucesión se escinde.

18. Sean R y S anillos. Demuestre que si M es un R -módulo izquierdo y N es un R - S -bimódulo, entonces $\text{Hom}_R(M, N)$ es un S -módulo derecho.

19. Demuestre la Proposición 3.4.13.

20. Sean $f : A \rightarrow B$ y $g : B \rightarrow C$ R -morfismos. Si para todo R -módulo M se tiene que la sucesión

$$0 \longrightarrow \text{Hom}_R(C, M) \xrightarrow{g^*} \text{Hom}_R(B, M) \xrightarrow{f^*} \text{Hom}_R(A, M)$$

es exacta, demuestre que la sucesión

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

es exacta.

Definición: Sea R un anillo. Decimos que $e \in R$ es un *idempotente* si $e^2 = e$.

21. Sea M un R -módulo y $S = \text{End}_R(M)$. Demuestre que si $e^2 = e \in S$ es un idempotente, entonces $M = eM \oplus (1 - e)M = \text{Im } e \oplus \text{Im}(1 - e)$.

22. Sea R un anillo y $e^2 = e \in R$ un idempotente. Demuestre que $eRe = \{ere \mid r \in R\}$ es un anillo con uno.

23. Sea M un R -módulo, $S = \text{End}_R(M)$ y $e^2 = e \in S$ un idempotente. Demuestre que $\text{End}_R(eM) \cong eSe$.

Definición. Sea M un R -módulo y $N \leq M$. Decimos que N es *totalmente invariante* si $\varphi(N) \subseteq N$ para todo $\varphi \in \text{End}_R(M)$.

24. Considere un anillo R como R -módulo izquierdo. Demuestre que un submódulo de R es totalmente invariante si y solo si es un ideal bilateral.

25. Sea M un R -módulo y $\{N_i\}_I$ una familia de submódulos totalmente invariantes de M . Demuestre que $\bigcap_{i \in I} N_i$ y $\sum_{i \in I} N_i$ son totalmente invariantes.

26. Sea M un R -módulo, $N \leq M$ y $\{A_i\}_I$ una familia de submódulos de M . Suponga que $M = \bigoplus_I A_i$. Si N es totalmente invariante entonces $N = \bigoplus_I (N \cap A_i)$.
27. Sean M y N dos R -módulos. Considere los siguientes submódulos de M y N respectivamente.

$$\text{Rej}_M(N) = \bigcap \{\text{Ker } \varphi \mid \varphi \in \text{Hom}_R(N, M)\}.$$

$$\text{Tr}^M(N) = \sum \{\varphi(M) \mid \varphi \in \text{Hom}_R(M, N)\}.$$

El primero es llamado el *rechazo* de N en M y el segundo la *traza* de M en N . Demuestre que $\text{Rej}_M(N)$ y $\text{Tr}^M(N)$ son submódulos totalmente invariantes de M y de N respectivamente.

28. Sea D un dominio entero y M un D -módulo. Demuestre que el submódulo de torsión $t(M)$ de M es totalmente invariante (Vea el Ejercicio 2.3.20).
29. Sean M y N dos D -módulos con D un dominio entero. Suponga que $t(M) = M$ y $t(N) = 0$. Demuestre que $\text{Hom}_D(M, N) = 0$.

Capítulo 4

Construcciones de módulos con propiedades universales

4.1. Producto y Coproducto

Sea $\{M_i\}_{i \in I}$ una familia de R -módulos izquierdos. Consideremos el producto cartesiano de la familia

$$\prod_I M_i := \left\{ f : I \rightarrow \bigcup_I M_i \mid f(i) \in M_i \right\}.$$

Dadas $f, g \in \prod_I M_i$ podemos definir la función $f + g : I \rightarrow \bigcup_I M_i$ de la siguiente manera:

$$(f + g)(i) = f(i) + g(i) \in M_i$$

y dado $r \in R$ podemos definir la función $rf : I \rightarrow \bigcup_I M_i$ de la siguiente manera:

$$(rf)(i) = rf(i) \in M_i.$$

Con estas operaciones $\prod_I M_i$ es un R -módulo izquierdo (Ejercicio 4.4.1).

Dada una función $f \in \prod_I M_i$, la podemos identificar con una sucesión de elementos $(x_i)_I$ indicados en I tales que $x_i := f(i) \in M_i$. Así, las operaciones en $\prod_I M_i$ quedan de la siguiente manera:

- $(x_i)_I + (y_i)_I := (x_i + y_i)_I$ para todo $(x_i)_I, (y_i)_I \in \prod_I M_i$.
- $r(x_i)_I := (rx_i)_I$ para todo $(x_i)_I \in \prod_I M_i$ y todo $r \in R$.

Definición 4.1.1. Sea $(x_i)_I \in \prod_I M_i$. Definimos el *soporte* de $(x_i)_I$, denotado $\text{sop}((x_i)_I)$, como el subconjunto de I dado por

$$\text{sop}((x_i)_I) = \{j \in I \mid x_j \neq 0\}.$$

Lema 4.1.2. Sea $\{M_i\}_I$ una familia de R -módulos. Considere el siguiente conjunto:

$$\prod_I M_i := \left\{ (x_i)_I \in \prod_I M_i \mid \text{sop}((x_i)_I) \text{ es finito} \right\}.$$

Entonces $\prod_I M_i$ es un submódulo de $\prod_I M_i$.

Demostración. Notemos que $0 = (0_i)_I \in \coprod_I M_i$ ya que $\text{sop}((x_i)_I) = \emptyset$. Ahora si $(x_i)_I, (y_i)_I \in \coprod_I M_i$ entonces

$$j \in \text{sop}((x_i)_I + (y_i)_I) \Leftrightarrow j \in \text{sop}((x_i + y_i)_I) \Leftrightarrow x_j + y_j \neq 0$$

así que $x_j \neq 0$ o $y_j \neq 0$, es decir, $j \in \text{sop}((x_i)_I) \cup \text{sop}((y_i)_I)$. Por lo tanto $\text{sop}((x_i)_I + (y_i)_I)$ es finito. Si $r \in R$ y $(x_i)_I \in \coprod_I M_i$ entonces

$$j \in \text{sop}(r(x_i)_I) \Leftrightarrow j \in \text{sop}((rx_i)_I) \Leftrightarrow rx_j \neq 0$$

así que $x_j \neq 0$, es decir, $j \in \text{sop}((x_i)_I)$ que es finito. \square

Dada una familia de R -módulos izquierdos $\{M_i\}_I$, para cada $j \in I$ tenemos un R -morfismo $\pi_j : \prod_I M_i \rightarrow M_j$ al que llamamos *la proyección canónica en M_j* definido como $\pi_j((x_i)_I) = x_j$.

Teorema 4.1.3 (Propiedad universal del producto). *Sea $\{M_i\}_I$ una familia de R -módulos. Consideremos $\prod_I M_i$ y las proyecciones canónicas $\{\pi_i\}_I$. Entonces para todo R -módulo C y toda familia de R -morfismos $\{\gamma_i : C \rightarrow M_i\}_I$, existe un único R -morfismo $\gamma : C \rightarrow \prod_I M_i$ tal que $\pi_i \gamma = \gamma_i$ para todo $i \in I$.*

$$\begin{array}{ccc} \prod_I M_i & \xrightarrow{\pi_j} & M_j \\ \uparrow \gamma_i & \nearrow \gamma_j & \\ C & & \end{array}$$

Demostración. Supongamos que C es un R -módulo y $\{\gamma_i : C \rightarrow M_i\}_I$ es una familia de R -morfismos. Definimos $\gamma : C \rightarrow \prod_I M_i$ como $\gamma(c) = (\gamma_i(c))_I$. Así, para $x, y \in C$ y $r \in R$, $\gamma(rx + y) = (\gamma_i(rx + y))_I = (r\gamma_i(x) + \gamma_i(y))_I = r(\gamma_i(x))_I + (\gamma_i(y))_I = r\gamma(x) + \gamma(y)$. Por lo tanto γ es un R -morfismo. Dada $j \in I$, $\pi_j(\gamma(c)) = \pi_j((\gamma_i(c))_I) = \gamma_j(c)$ lo que implica que $\pi_j \gamma = \gamma_j$. Por último, si $\gamma' : C \rightarrow \prod_I M_i$ es un R -morfismo tal que $\pi_j \gamma' = \gamma_j$ para toda $j \in I$ entonces $\pi_j(\gamma'(c)) = \gamma_j(c) = \pi_j(\gamma(c))$, así que $\forall j \in I$ la j -ésima coordenada de $\gamma'(c)$ es la misma que la de $\gamma(c)$. Entonces $\gamma'(c) = \gamma(c)$ y por lo tanto $\gamma' = \gamma$ \square

Dada una familia de R -módulos izquierdos $\{M_i\}_I$, para cada $j \in I$ tenemos un R -morfismo $\eta_j : M_j \rightarrow \prod_I M_i$ al que llamamos *la inclusión canónica de M_j* definido como $\eta_j(x) = (\hat{x}_i)_I$, donde $(\hat{x}_i)_I$ es el elemento del producto $(x_i)_I$ tal que $x_i = 0$ para toda $j \neq i$ y $x_i = x$ si $j = i$.

Teorema 4.1.4 (Propiedad universal del coproducto). *Sea $\{M_i\}_I$ una familia de R -módulos. Consideremos $\prod_I M_i$ y las inclusiones canónicas $\{\eta_i\}_I$. Entonces para todo R -módulo B y toda familia de R -morfismos $\{\alpha_i : M_i \rightarrow B\}_I$, existe un único R -morfismo $\alpha : \prod_I M_i \rightarrow B$ tal que $\alpha \eta_i = \alpha_i$ para todo $i \in I$.*

$$\begin{array}{ccc} M_j & \xrightarrow{\eta_j} & \prod_I M_i \\ & \searrow \alpha_j & \downarrow \alpha \\ & & M_j \end{array}$$

Demostración. Supongamos que $\{\alpha_i : M_i \rightarrow B\}_I$ es una familia de R -morfismos. Definimos $\alpha : \coprod_I M_i \rightarrow B$ como $\alpha((x_i)_I) = \sum\{\alpha_i(x_i) \mid i \in \text{sop}((x_i)_I)\}$. La suma está bien definida ya que $\text{sop}((x_i)_I)$ es finito. Notemos que

$$\begin{aligned} \alpha(r(x_i)_I + (y_i)_I) &= \alpha((rx_i + y_i)_I) \\ &= \sum\{\alpha_i(rx_i + y_i) \mid i \in \text{sop}((rx_i + y_i)_I)\} \\ &= \sum\{\alpha_i(rx_i + y_i) \mid i \in \text{sop}((rx_i)_I) \cup \text{sop}((y_i)_I)\} \\ &= \sum\{r\alpha_i(x_i) \mid i \in \text{sop}((x_i)_I)\} + \sum\{\alpha_i(y_i) \mid i \in \text{sop}((y_i)_I)\} \\ &= r\alpha((x_i)_I) + \alpha((y_i)_I). \end{aligned}$$

Por lo tanto α es un R -morfismo. Para cada $x \in M_j$ se tiene que $\alpha\eta_j(x) = \alpha((\hat{x}_j)_I) = \alpha_j(x_j) = \alpha_j(x)$. Por lo tanto $\alpha\eta_j = \alpha_j$ para toda $j \in I$. Ahora supongamos que existe $\alpha' : \coprod_{i \in I} M_i \rightarrow B$ tal que $\alpha'\eta_i = \alpha_i$ para todo $i \in I$. Notemos que, si $(a_i)_I \in \coprod_I M_i$, entonces $(a_i)_I = \sum\{(\hat{a}_i)_I \mid i \in \text{sop}((a_i)_I)\} = \sum\{\eta_i(a_i) \mid i \in \text{sop}((a_i)_I)\}$. Por lo que

$$\begin{aligned} \alpha'((a_i)_I) &= \alpha' \left(\sum\{(\hat{a}_i)_I \mid i \in \text{sop}((a_i)_I)\} \right) \\ &= \alpha' \left(\sum\{\eta_i(a_i) \mid i \in \text{sop}((a_i)_I)\} \right) \\ &= \sum\{\alpha'\eta_i(a_i) \mid i \in \text{sop}((a_i)_I)\} \\ &= \sum\{\alpha_i(a_i) \mid i \in \text{sop}((a_i)_I)\} \\ &= \sum\{\alpha\eta_i(a_i) \mid i \in \text{sop}((a_i)_I)\} \\ &= \alpha \left(\sum\{\eta_i(a_i) \mid i \in \text{sop}((a_i)_I)\} \right) \\ &= \alpha((a_i)_I). \end{aligned}$$

Por lo tanto $\alpha' = \alpha$. □

Proposición 4.1.5. *Sea $\{M_i\}_I$ una familia de R -módulos. Entonces existen submódulos $\widehat{M}_i \leq \coprod_I M_i$ para cada $i \in I$ tales que $M_i \cong \widehat{M}_i$ y $\coprod_I M_i = \bigoplus_I \widehat{M}_i$.*

Demostración. Sea $\{M_i\}_I$ una familia de R -módulos. Consideremos $\coprod_I M_i$ con las inclusiones canónicas $\eta_i : M_i \rightarrow \coprod_I M_i$. Definimos $\widehat{M}_i := \eta(M_i) = \{(\hat{x}_i)_I \mid x_i \in M_i\}$. Como η_i es inyectiva, $M_i \cong \widehat{M}_i$. Notemos que cada $(x_i)_I \in \coprod\{M_i\}_I$ es de la forma $\sum_{i \in \text{sop}(x_i)} (\hat{x}_i)_I = \sum_{i \in \text{sop}(x_i)} \eta_i(x_i)$ así que $(x_i)_I \in \sum_{i \in \text{sop}(x_i)} \widehat{M}_i \subseteq \sum_I \widehat{M}_i$. Por lo tanto $\coprod_I M_i \subseteq \sum_I \widehat{M}_i$. Ahora, como cada $\widehat{M}_i \leq \coprod\{M_i\}$, $\sum_I \widehat{M}_i \subseteq \coprod\{M_i\}$. Por lo tanto $\sum_I \widehat{M}_i = \coprod_I M_i$. Además, si $(x_i)_I \in \widehat{M}_j \cap \sum_{i \neq j} \widehat{M}_i$, entonces $x_k = 0$ para toda $k \neq j$ y también $x_j = 0$ ya que $(x_i)_I \in \sum_{i \neq j} \widehat{M}_i$. Así que $(x_i)_I = (0)$. Por lo tanto $\coprod_I M_i = \bigoplus_I \widehat{M}_i$. □

En general se usa la notación $\bigoplus_I M_i$ para el coproducto de la familia $\{M_i\}_I$ y se le llama la *suma directa* de la familia. Si todo los módulos M_i son iguales a un módulo M se usa la notación $M^{(I)}$ para el coproducto y M^I para el producto.

Proposición 4.1.6. *Sean $\{A_i\}_I$ y $\{B_i\}_I$ dos familias de R -módulos y $\{\alpha_i : A_i \rightarrow B_i\}_I$ una familia de R -morfismos. Entonces:*

1. Existe un único morfismo $\prod \alpha_i : \prod_I A_i \rightarrow \prod_I B_i$ dado por $\prod \alpha_i((a_i)_I) = (\alpha(a_i))_I$.
2. Existe un único morfismo $\bigoplus \alpha_i : \bigoplus_I A_i \rightarrow \bigoplus_I B_i$ dado por $\bigoplus \alpha_i((a_i)_I) = (\alpha_i(a_i))_I$.

Demostración. 1. Sean $\pi_i^A : \prod_I A_i \rightarrow A_i$ las proyecciones canónicas. Entonces para cada $j \in I$ tenemos un R -morfismo $\alpha_j \pi_j^A : \prod_I A_i \rightarrow B_j$.

$$\begin{array}{ccc} \prod_I B_i & \xrightarrow{\pi_j^B} & B_j \\ \uparrow & & \uparrow \alpha_j \\ \prod_I A_i & \xrightarrow{\pi_j^A} & A_j \end{array}$$

Por la Propiedad universal del producto (Teorema 4.1.3), existe un único R -morfismo $\prod \alpha_i : \prod_I A_i \rightarrow \prod_I B_i$ que se calcula como

$$\prod \alpha_i((a_i)_I) = (\alpha_i \pi_i^A((a_i)_I))_I = (\alpha_i(a_i))_I.$$

2. Sean $\eta_i^B : B_i \rightarrow \bigoplus_I B_i$ las inclusiones canónicas. Entonces para cada $j \in I$ tenemos un R -morfismo $\eta_j^B \alpha_j : A_j \rightarrow \bigoplus_I B_i$.

$$\begin{array}{ccc} A_j & \xrightarrow{\eta_j^A} & \bigoplus_I A_i \\ \alpha_j \downarrow & & \downarrow \\ B_j & \xrightarrow{\eta_j^B} & \bigoplus_I B_i \end{array}$$

Por la Propiedad universal de la suma direct (Teorema 4.1.4), existe un único R -morfismo $\bigoplus_I \alpha_i : \bigoplus_I A_i \rightarrow \bigoplus_I B_i$ que se calcula como

$$\bigoplus_I \alpha_i((a_i)_I) = \sum_I \eta_i^B \alpha_i(a_i) = (\alpha_i(a_i))_I.$$

□

Proposición 4.1.7. Sea I un conjunto. Sea $\{0 \rightarrow A_i \xrightarrow{\alpha_i} B_i \xrightarrow{\beta_i} C_i \rightarrow 0\}_I$ una familia de sucesiones exactas en $R\text{-Mod}$. Entonces las sucesiones

$$0 \longrightarrow \prod_I A_i \xrightarrow{\prod \alpha_i} \prod_I B_i \xrightarrow{\prod \beta_i} \prod_I C_i \longrightarrow 0$$

$$0 \longrightarrow \bigoplus_I A_i \xrightarrow{\bigoplus \alpha_i} \bigoplus_I B_i \xrightarrow{\bigoplus \beta_i} \bigoplus_I C_i \longrightarrow 0.$$

son exactas.

Demostración. Sea $(a_i)_I \in \prod_I A_i$ tal que $\prod_I \alpha_i((a_i)_I) = 0$, es decir, $(\alpha_i(a_i))_I = 0$. Note que por la Observación 3.3.2, cada α_i es inyectiva. Esto implica que $a_i = 0$ para todo $i \in I$. Por lo tanto $\prod_I \alpha_i$ es inyectiva. Por la unicidad de los morfismos dados en la Proposición 4.1.6, $\prod_I \beta_i \prod_I \alpha_i = \prod_I \beta_i \alpha_i$. Por lo tanto,

$\prod_I \beta_i \prod_I \alpha_i = 0$, es decir, $\text{Im } \prod_I \alpha_i \subseteq \text{Ker } \prod_I \beta_i$. Ahora sea $(b_i)_I \in \text{Ker } \prod_I \beta_i$. Entonces $0 = \prod_I \beta_i((b_i)_I) = (\beta_i(b_i))_I$. Esto implica que para cada $j \in I$, $b_j \in \text{Ker } \beta_j$. Así, para cada $j \in I$, existe $a_j \in A_j$ tal que $\alpha_j(a_j) = b_j$. Por lo tanto $\prod_I \alpha_i((a_i)_I) = (b_i)_I$. Esto prueba que $\text{Im } \prod_I \alpha_i = \text{Ker } \prod_I \beta_i$. Sea $(c_i)_I \in \prod_I C_i$. Como $\beta_i : B_i \rightarrow C_i$ es suprayectiva para cada $i \in I$, existe $b_i \in B_i$ tal que $\beta_i(b_i) = c_i$ para toda $i \in I$. Por lo tanto $\prod_I \beta_i((b_i)_I) = (c_i)_I$, es decir, $\prod_I \beta_i$ es suprayectiva. Por lo tanto la sucesión de productos es exacta.

Que la sucesión de sumas directas es exacta, se prueba de manera similar (Ejercicio 4.4.8). \square

Proposición 4.1.8. *Sea $\{M_i\}_I$ una familia de R -módulos izquierdos y N un R -módulo. Entonces hay un isomorfismo de grupos abelianos:*

$$\text{Hom}_R \left(\bigoplus_I M_i, N \right) \cong \prod_I \text{Hom}_R(M_i, N).$$

Demostración. Sean $\eta_i : M_i \rightarrow \bigoplus_I M_i$ las inclusiones canónicas. Sea $\varphi \in \text{Hom}_R(\bigoplus_I M_i, N)$. Para cada $i \in I$ definimos el R -morfismo

$$\alpha_i : \text{Hom}_R \left(\bigoplus_I M_i, N \right) \rightarrow \text{Hom}_R(M_i, N)$$

como $\alpha_i(\varphi) = \varphi\eta_i$. Por el Teorema 4.1.3, existe un único R -morfismo

$$\alpha : \text{Hom}_R \left(\bigoplus_I M_i, N \right) \rightarrow \prod_I \text{Hom}_R(M_i, N)$$

dado por $\alpha(\varphi) = (\alpha_i(\varphi))_I = (\varphi\eta_i)_I$. Veamos que α es un isomorfismo. Sean $\varphi, \psi \in \text{Hom}_R(\bigoplus_I M_i, N)$. Entonces $\alpha(\varphi + \psi) = ((\varphi + \psi)\eta_i)_I = (\varphi\eta_i + \psi\eta_i)_I = (\varphi\eta_i)_I + (\psi\eta_i)_I = \alpha(\varphi) + \alpha(\psi)$. Por lo tanto α es un morfismo de grupos abelianos. Supongamos que $\alpha(\varphi) = 0$, that is, $(\varphi\eta_i)_I = 0$. Entonces $\varphi\eta_i = 0$ para todo $i \in I$. Por el Ejercicio 4.4.5, se sigue que $\varphi = 0$. Ahora sea $(\beta_i)_I \in \prod_I \text{Hom}_R(M_i, N)$. Entonces tenemos para cada $i \in I$, $\beta_i : M_i \rightarrow N$. Por la Propiedad universal de la suma directa (Teorema 4.1.4) existe un único morfismo $\beta \in \text{Hom}_R(\bigoplus_I M_i, N)$ tal que $\beta\eta_i = \beta_i$ para todo $i \in I$. Por lo tanto $\alpha(\beta) = (\beta_i)_I$. Así tenemos que α es un isomorfismo. \square

Observación 4.1.9. Por la prueba de la Proposición 4.1.8 se puede ver que dada una familia de R -módulos $\{M_i\}_I$ y un R -módulo N hay un R -morfismo

$$\alpha : \text{Hom}_R \left(\prod_I M_i, N \right) \rightarrow \prod_I \text{Hom}_R(M_i, N).$$

En general este R -morfismo no es un isomorfismo. Sea \mathbb{P} el conjunto de todos los números primos. Si consideramos $\prod_{p \in \mathbb{P}} \mathbb{Z}_p$ y \mathbb{Q} entonces $\text{Hom}_{\mathbb{Z}} \left(\prod_{p \in \mathbb{P}} \mathbb{Z}_p, \mathbb{Q} \right) \neq 0$ pero $\prod_{p \in \mathbb{P}} \text{Hom}_{\mathbb{Z}}(\mathbb{Z}_p, \mathbb{Q}) = 0$, es decir, $\alpha = 0$ no es un isomorfismo.

Proposición 4.1.10. *Sea $\{N_i\}_I$ una familia de R -módulos izquierdos y M un R -módulo. Entonces hay un isomorfismo de grupos abelianos:*

$$\text{Hom}_R \left(M, \prod_I N_i \right) \cong \prod_I \text{Hom}_R(M, N_i).$$

Ejemplo 4.1.11. En general, no es posible cambiar el producto directo en la Proposición 4.1.10 por suma directa. Sea p un número primo y pongamos $M = \bigoplus_{n>0} \mathbb{Z}_{p^n}$. Entonces

$$\text{Hom}_{\mathbb{Z}} \left(M, \bigoplus_{n>0} \mathbb{Z}_{p^n} \right) \not\cong \bigoplus_{n>0} \text{Hom}_{\mathbb{Z}}(M, \mathbb{Z}_{p^n}).$$

Para ver esto, primero tomemos un morfismo $\varphi : M \rightarrow \mathbb{Z}_{p^n}$ con n fijo. Entonces $p^n \varphi(m) = 0$ para todo $m \in M$. Ahora, dado $(\varphi_n)_{n>0} \in \bigoplus_{n>0} \text{Hom}_{\mathbb{Z}}(M, \mathbb{Z}_{p^n})$ podemos considerar $k = \max\{n \in \text{sop}((\varphi_n)_{n>0})\}$. Entonces $p^k (\varphi_n)_{n>0} = 0$. Es decir, todo elemento de $\bigoplus_{n>0} \text{Hom}_{\mathbb{Z}}(M, \mathbb{Z}_{p^n})$ tiene orden finito. Por otro lado, el morfismo identidad $Id : M \rightarrow \bigoplus_{n>0} \mathbb{Z}_{p^n}$ no tiene orden finito, ya que si $k \in \mathbb{Z}$ podemos encontrar $\ell > 0$ tal que $k < p^\ell$ y así $k Id((\widehat{1}_{p^\ell})_{n>0}) \neq 0$.

Proposición 4.1.12. 1. Sea R un anillo y pongamos que ${}_R R = \bigoplus_I A_i$ con $A_i \leq {}_R R$. Entonces:

- (I) Existe un subconjunto finito I_0 de I tal que ${}_R R = \bigoplus_{I_0} A_j$.
 (II) Existen elementos $e_i \in A_i$ con $i \in I_0$ tales que para todo $i, j \in I_0$ se tiene que $A_i = Re_i$, $\sum_{I_0} e_i = 1$ y $e_i e_j = \begin{cases} e_i & i = j \\ 0 & i \neq j \end{cases}$.

En éste caso decimos que el conjunto de los e_i 's es de idempotentes ortogonales.

- (III) Si cada A_i es bilateral entonces los e_i 's están en el centro de R . En este caso cada A_i es un anillo con uno.

2. Si $e_1, \dots, e_n \in R$ son idempotentes ortogonales tal que $\sum e_i = 1$ entonces ${}_R R = \bigoplus Re_i$. Si además los e_i 's son centrales entonces cada Re_i es bilateral.

Demostración. 1.(I). Si ${}_R R = \bigoplus_I A_i$ entonces $1 = e_{i_1} + \dots + e_{i_n}$ con $e_{i_j} \in A_{i_j}$ distintos de cero, así que para todo $r \in R$ $r = re_{i_1} + \dots + re_{i_n}$ por lo tanto $r \in \sum_{j=1}^n A_{i_j}$. Entonces $R = \bigoplus_{j=1}^n A_{i_j}$.

(II). Tenemos que $1 = e_1 + \dots + e_n$ con $e_i \in A_i$. Multiplicando por e_j , se tiene que $e_j = e_1 e_j + \dots + e_n e_j$. Así,

$$0 = e_j - e_j e_j = e_j e_1 + \dots + e_j e_{j-1} + e_j e_{j+1} + \dots + e_j e_n.$$

Como cada $e_j e_i \in A_i$ y la suma es directa, cada sumando tiene que ser cero, es

decir, $e_j e_i = \begin{cases} e_i & i = j \\ 0 & i \neq j \end{cases}$. Ahora, si $a_j \in A_j$ entonces $a_j = a_j e_1 + \dots + a_j e_n = a_j e_j$

así que $A_j \subseteq A_j e_j \subseteq Re_j \subseteq A_j$. Por lo tanto $A_j = Re_j$.

(III). Sea $r \in R$, tenemos que $r = \sum re_j = \sum e_j r$. Como A_j es bilateral $re_j, e_j r \in A_j$. Lo que implica que $re_j = e_j r$. Por otro lado, si e_i es central, entonces $Re_i = e_i Re_i$ que es un anillo con unidad.

2. Como $1 = \sum e_i$, para todo $r \in R$, $r = \sum re_i \in \sum Re_i$. Así que ${}_R R = \sum Re_i$. Supongamos que $r \in Re_i \cap \sum_{i \neq j} Re_j$ entonces $r = r e_i = \sum_{i \neq j} r_j e_j e_i$ lo que implica que $re_i = r e_i e_i = \sum_{i \neq j} r_j e_j e_i$. Como los e_i 's son idempotentes ortogonales $r = r e_i = 0$. Por lo tanto $\bigoplus Re_i = {}_R R$. Si cada e_i es central $(Re_i)r = Rre_i \subseteq Re_i$. Por lo tanto Re_i es ideal derecho. \square

4.2. Producto Fibrado y Coproducto Fibrado

Considere el siguiente diagrama conmutativo de R -morfismos

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ \varphi \downarrow & & \downarrow \beta \\ M & \xrightarrow{\psi} & N. \end{array}$$

Definición 4.2.1. 1. El par (φ, α) es llamado el *producto fibrado* del par (ψ, β) si para cualquier par (φ', α') con $\varphi' : Y \rightarrow M$, $\alpha' : Y \rightarrow B$ existe un único $\tau : Y \rightarrow A$ tal que $\varphi' = \varphi\tau$ y $\alpha' = \alpha\tau$.

$$\begin{array}{ccccc} & & Y & & \\ & & \swarrow \alpha' & & \\ & & A & \xrightarrow{\alpha} & B \\ & \swarrow \varphi' & \downarrow \varphi & & \downarrow \beta \\ & & M & \xrightarrow{\psi} & N \end{array}$$

2. El par (ψ, β) es llamado el *coproducto fibrado* del par (φ, α) si para cualquier par (ψ', β') con $\psi' : M \rightarrow X$, $\beta' : B \rightarrow X$ y $\psi'\varphi = \beta'\alpha$ existe un único $\sigma : N \rightarrow X$ tal que $\psi' = \sigma\psi$ y $\beta' = \sigma\beta$.

$$\begin{array}{ccccc} A & \xrightarrow{\alpha} & B & & \\ \varphi \downarrow & & \downarrow \beta & & \\ M & \xrightarrow{\psi} & N & & \\ & \searrow \psi' & \searrow \sigma & & \\ & & X & & \end{array}$$

Proposición 4.2.2. Sean M y N R -módulos. Entonces el producto de M con N junto con las proyecciones canónicas es el producto fibrado del par

$$\begin{array}{ccc} M & & \\ \downarrow 0 & & \\ N & \xrightarrow{0} & 0. \end{array}$$

Demostración. Sean $\pi_1 : M \times N \rightarrow M$ y $\pi_2 : M \times N \rightarrow N$ las proyecciones canónicas. Es claro que $0\pi_1 = 0\pi_2$. Ahora, si $\alpha : Y \rightarrow M$ y $\varphi : Y \rightarrow N$ son R -morfismos tales que $0\alpha = 0\varphi$. Por la propiedad universal del producto (Teorema 4.1.3) existe un único R -morfismo $\tau : Y \rightarrow M \times N$ tal que $\pi_1\tau = \alpha$ y $\pi_2\tau = \varphi$.

Por lo tanto (π_1, π_2) es el producto fibrado de $(0, 0)$.

$$\begin{array}{ccccc}
 Y & & & & \\
 \searrow \alpha & & & & \\
 & M \times N & \xrightarrow{\pi_1} & M & \\
 \searrow \tau & \downarrow \pi_2 & & \downarrow 0 & \\
 & N & \xrightarrow{0} & 0 & \\
 \searrow \varphi & & & & \\
 & & & &
 \end{array}$$

□

Teorema 4.2.3. Tomemos el ángulo (ψ, β)

$$\begin{array}{ccc}
 & B & \\
 & \downarrow \beta & \\
 M & \xrightarrow{\psi} & N.
 \end{array}$$

Sea $A := \{(m, b) \mid m \in M, b \in B \text{ y } \psi(m) = \beta(b)\}$ y sean $\varphi : A \rightarrow M$ y $\alpha : A \rightarrow B$ definidos como $\varphi(m, b) = m$ y $\alpha(m, b) = b$ respectivamente. Entonces (φ, α) es el producto fibrado de (ψ, β) .

Demostración. Tenemos que $A \leq M \oplus B$ y φ y α son las restricciones de las proyecciones canónicas, así que son R -morfismos. Sea Y un R -módulo y $\varphi' : Y \rightarrow M$ y $\alpha' : Y \rightarrow B$ morfismos tales que $\beta\alpha' = \psi\varphi'$. Definimos $\tau : Y \rightarrow A$ como $\tau(y) = (\varphi'(y), \alpha'(y)) \in A$ ya que $\psi\varphi' = \beta\alpha'$. Es claro que τ es un R -morfismo. Ahora, $\alpha\tau(y) = \alpha(\varphi'(y), \alpha'(y)) = \alpha'(y)$ y $\varphi\tau(y) = \varphi(\varphi'(y), \alpha'(y)) = \varphi'(y)$ así que $\alpha\tau = \alpha'$ y $\varphi\tau = \varphi'$.

Supongamos que tenemos $\tau' : Y \rightarrow A$ tal que $\varphi\tau' = \varphi'$ y $\alpha\tau' = \alpha'$. Sea $(\tau - \tau')(y) = (m, b)$ entonces $0 = \varphi(\tau - \tau')(y) = \varphi(m, b) = m$ y $0 = \alpha(\tau - \tau')(y) = \alpha(m, b) = b$. Como φ ni α son los morfismos 0 entonces $(\tau - \tau')(y) = 0$, por lo tanto $(\tau - \tau') = 0$. □

Teorema 4.2.4. Tomemos el ángulo (φ, α)

$$\begin{array}{ccc}
 A & \xrightarrow{\alpha} & B \\
 \varphi \downarrow & & \\
 M & &
 \end{array}$$

Sea $N = (M \oplus B)/U$ con $U := \{(\varphi(a), -\alpha(a)) \mid a \in A\}$ y sean $\psi : M \rightarrow N$ y $\beta : B \rightarrow N$ definidos como $\psi(m) = (m, 0) + U$ y $\beta(b) = (0, b) + U$ respectivamente. Entonces (ψ, β) es el coproducto fibrado de (φ, α) .

Demostración. Denotemos $\overline{(m, b)}$ a la clase $(m, b) + U$ en N . Es claro que U es submódulo de $M \oplus B$ y que ψ y β son R -morfismos. Ahora $\psi\varphi(a) = \overline{(\varphi(a), 0)}$ y $\beta\alpha(a) = \overline{(0, \alpha(a))}$. Como $(\varphi(a), 0) - (0, \alpha(a)) = (\varphi(a), -\alpha(a)) \in U$, se tiene que $\psi\varphi = \beta\alpha$. Sea X un módulo y $\psi' : M \rightarrow X$ y $\beta' : B \rightarrow X$ morfismos tales que $\beta'\alpha = \psi'\varphi$. Definimos $\sigma : N \rightarrow X$ como $\sigma(\overline{(m, b)}) = \psi'(m) + \beta'(b)$. Notemos que $\sigma(\overline{(\varphi(a), -\alpha(a))}) = \psi'\varphi(a) - \beta'\alpha(a) = 0$ ya que $\psi'\varphi = \beta'\alpha$. Por lo tanto σ

está bien definida. Por otro lado, $\sigma\psi(m) = \sigma(\overline{(m, 0)}) = \psi'(m) + \beta'(0) = \psi'(m)$ y $\sigma\beta(b) = \sigma(\overline{(0, b)}) = \psi'(0) + \beta'(b) = \beta'(b)$, i.e. $\sigma\psi = \psi'$ y $\sigma\beta = \beta'$.

Supongamos que tenemos $\sigma' : N \rightarrow X$ tal que $\psi' = \sigma'\psi$ y $\beta' = \sigma'\beta$. Entonces $(\sigma - \sigma')\psi = 0$ y $(\sigma - \sigma')\beta = 0$. Así que $0 = (\sigma - \sigma')\psi(m) = (\sigma - \sigma')(\overline{(m, 0)})$ y $0 = (\sigma - \sigma')\beta(b) = (\sigma - \sigma')(\overline{(0, b)})$ pero como $\{(m, 0), (0, b) \mid m \in M, b \in B\}$ generan N entonces $(\sigma - \sigma') = 0$. \square

Teorema 4.2.5. *Sea (ψ, β) el coproducto fibrado de (φ, α) . Entonces:*

1. *Si α es un monomorfismo (resp. epimorfismo), entonces ψ es monomorfismo (resp. epimorfismo).*
Si φ es un monomorfismo (resp. epimorfismo), entonces β es monomorfismo (resp. epimorfismo).
2. *Sea α un monomorfismo. Entonces $\text{Im } \psi$ es un sumando directo de N si y sólo si existe $\kappa : B \rightarrow M$ tal que $\varphi = \kappa\alpha$.*

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ \varphi \downarrow & \swarrow \kappa & \downarrow \beta \\ M & \xrightarrow{\psi} & N \end{array}$$

Demostración. 1. Sea α un monomorfismo y $\psi(m) = \overline{(m, 0)} = 0$, entonces existe un $a \in A$ tal que $(m, 0) = (\varphi(a), -\alpha(a))$. Así que $\alpha(a) = 0$, lo que implica que $a = 0$. Por lo tanto $m = \varphi(a) = 0$. Si φ es un monomorfismo la prueba es simétrica. Ahora supongamos que α es un epimorfismo. Sea $\overline{(m, b)} \in N$. Por hipótesis existe $a \in A$ tal que $\alpha(a) = b$. Entonces $\overline{(m + \varphi(a), 0)} - \overline{(m, b)} = \overline{(\varphi(a), -\alpha(a))} = 0$. Por lo tanto $\psi(m + \varphi(a)) = \overline{(m, b)}$. Es decir, ψ es suprayectivo. Si φ es un epimorfismo la prueba es simétrica.

$2 \Rightarrow$. Sean α un monomorfismo y supongamos que $N = \text{Im } \psi \oplus N_0$. Entonces ψ también es un monomorfismo, así que ψ induce un isomorfismo $\psi_0 : M \rightarrow \text{Im } \psi$. Sea $\pi : N \rightarrow \text{Im } \psi$ la proyección canónica. Definimos $\kappa := \psi_0^{-1}\pi\beta$. Entonces $\kappa\alpha(a) = \psi_0^{-1}\pi\beta\alpha(a) = \psi_0^{-1}\pi\psi\varphi(a) = \psi_0^{-1}\pi(\overline{(\varphi(a), 0)}) = \psi_0^{-1}(\overline{(\varphi(a), 0)}) = \varphi(a)$. Por lo tanto $\kappa\alpha = \varphi$.

\Leftarrow . Sea $\kappa : B \rightarrow M$ tal que $\kappa\alpha = \varphi$. Tomemos $\xi : N \rightarrow M$ como $\xi(\overline{(m, b)}) = m + \kappa(b)$. Como $\xi(\overline{(\varphi(a), -\alpha(a))}) = \varphi(a) - \kappa\alpha(a) = 0$, ξ está bien definido y es un R -morfismo. Se tiene que $\xi\psi(m) = \xi(\overline{(m, 0)}) = m$, es decir, $\xi\psi = \text{Id}_M$. Entonces por el Corolario 3.2.11.(3), $N = \text{Im } \psi \oplus \text{Ker } \xi$. \square

Teorema 4.2.6. *Sea (φ, α) el producto fibrado de (ψ, β) . Entonces:*

1. *Si β es un epimorfismo (resp. monomorfismo), entonces φ es epimorfismo (resp. monomorfismo).*
Si ψ es un epimorfismo (resp. monomorfismo), entonces α es epimorfismo (resp. monomorfismo).
2. *Sea ψ un epimorfismo. Entonces $\text{Ker } \alpha$ es un sumando directo de A si y sólo si existe $\kappa : B \rightarrow M$ tal que $\beta = \psi\kappa$.*

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ \varphi \downarrow & \swarrow \kappa & \downarrow \beta \\ M & \xrightarrow{\psi} & N \end{array}$$

Proposición 4.2.7. Sea $0 \rightarrow K \xrightarrow{\xi} M \xrightarrow{\psi} N \rightarrow 0$ una sucesión exacta corta y $\beta : B \rightarrow N$ un R -morfismo. Entonces hay un diagrama conmutativo con renglones exactos

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{\tau} & A & \xrightarrow{\alpha} & B & \longrightarrow & 0 \\ & & \downarrow 1 & & \downarrow \varphi & & \downarrow \beta & & \\ 0 & \longrightarrow & K & \xrightarrow{\xi} & M & \xrightarrow{\psi} & N & \longrightarrow & 0, \end{array}$$

tal que (φ, α) es el producto fibrado de (β, ψ) .

Demostración. Tomemos el producto fibrado del par (β, ψ) . Por la propiedad universal del producto fibrado, existe un único R -morfismo $\tau : K \rightarrow A$ tal que $\tau(k) = (\xi(k), 0)$. Por lo tanto $\varphi\tau = \xi$ y $\alpha\tau = 0$, lo que nos dice también que $\text{Im } \tau \subseteq \text{Ker } \alpha$. Sea $(m, b) \in A$ tal que $\alpha(m, b) = 0$. Entonces $b = 0$. Esto implica que $\psi(m) = 0$. Así que existe $k \in K$ tal que $\xi(k) = m$. Por lo tanto, $\tau(k) = (\xi(k), 0) = (m, 0)$, y así $\text{Ker } \alpha = \text{Im } \tau$. Ahora si $\tau(k) = 0$, es decir $(\xi(k), 0) = (0, 0)$, entonces $\xi(k) = 0$. Como ξ es inyectiva, $k = 0$. Por lo tanto τ es un monomorfismo. Por el Teorema 4.2.6, α es un epimorfismo y por lo tanto el renglón superior es exacto. \square

4.3. Producto Tensorial

Sea S un anillo y consideremos A_S un S -módulo derecho y ${}_S U$ un S -módulo izquierdo. Consideremos $A \times U$ (como conjunto) y tomemos el \mathbb{Z} -módulo $F = \mathbb{Z}^{(A \times U)}$. Sean $\{\eta_{(a,u)} : \mathbb{Z} \rightarrow F \mid (a,u) \in A \times U\}$ las inclusiones canónicas. Para cada $(a,u) \in A \times U$ denotemos $(a,u) = \eta_{(a,u)}(1) \in F$. Sea $x = (z_{(a,u)})_{A \times U} \in F$. Entonces $\text{sop}(x) = \{(a_1, u_1), (a_2, u_2), \dots, (a_n, u_n)\}$. Denotemos $z_i = z_{(a_i, u_i)}$ para $1 \leq i \leq n$. Así

$$x = \sum_{i=1}^n \eta_{(a_i, u_i)}(z_i) = \sum_{i=1}^n z_i \eta_{(a_i, u_i)}(1) = \sum_{i=1}^n z_i (a_i, u_i).$$

Más aún, el conjunto $\{(a,u) \in F \mid (a,u) \in A \times U\} = \{\eta_{(a,u)}(1) \mid (a,u) \in A \times U\}$ es una base de F , es decir, es un conjunto linealmente independiente sobre \mathbb{Z} y genera a F (Ejercicio 4.4.14). A F lo llamamos el \mathbb{Z} -módulo (o grupo abeliano) libre con base $A \times U$.

Definimos los siguientes subconjuntos de F :

$$\begin{aligned} D_1 &= \{(a_1 + a_2, u) - (a_1, u) - (a_2, u) \mid a_1, a_2 \in A, u \in U\} \\ D_2 &= \{(a, u_1 + u_2) - (a, u_1) - (a, u_2) \mid a \in A, u_1, u_2 \in U\} \\ T &= \{(as, u) - (a, su) \mid a \in A, u \in U, s \in S\} \end{aligned}$$

Tomamos el submódulo generado por estos subconjuntos

$$K = \langle D_1 \cup D_2 \cup T \rangle \leq F$$

Definición 4.3.1. Sean S un anillo, A_S un S -módulo derecho y ${}_S U$ un S -módulo izquierdo. Consideremos F y K como arriba. El *producto tensorial* de A con U (sobre S) es el grupo abeliano $A \otimes_S U := F/K$.

Observación 4.3.2. Dado un básico $(a,u) \in F$, a su clase de equivalencia en $A \otimes_S U$ la denotamos $a \otimes u$. Un elemento en F es una suma finita $\sum z_i (a_i, u_i)$ con $z_i \in \mathbb{Z}$, por lo que los elementos de $A \otimes_S U$ son sumas finitas de la forma $\sum z_i a_i \otimes u_i$. Por lo tanto, el conjunto $\{a \otimes u \mid a \in A, u \in U\}$ genera a $A \otimes_S U$.

Proposición 4.3.3. Sean $a, a_1, a_2 \in A$, $u, u_1, u_2 \in U$ y $s \in S$. Entonces:

1. $(a_1 + a_2) \otimes u = (a_1 \otimes u) + (a_2 \otimes u)$
2. $a \otimes (u_1 + u_2) = (a \otimes u_1) + (a \otimes u_2)$
3. $as \otimes u = a \otimes su$
4. $0 \otimes u = 0 = a \otimes 0$
5. $-(a \otimes u) = (-a) \otimes u = a \otimes (-u)$
6. Para todo $z \in \mathbb{Z}$, $z(a \otimes u) = (za) \otimes u = a \otimes zu$

Demostración. 1. Notemos que $(a_1 + a_2) \otimes u - (a_1 \otimes u) - (a_2 \otimes u) = 0$ ya que $(a_1 + a_2, u) - (a_1, u) - (a_2, u) \in K$. Análogamente se tienen 2 y 3. Los incisos 4 y 5 los dejamos como ejercicio 4.4.15. Para 6, si $z > 0$, entonces $z(a \otimes u) = (a \otimes u) + (a \otimes u) + \dots + (a \otimes u)$ (z veces). Aplicando 1, obtenemos

$(a + a + \cdots + a) \otimes u = (za) \otimes u$. Si aplicamos 2, obtenemos $a \otimes (u + u + \cdots + u) = a \otimes (zu)$. Ahora si $z < 0$, entonces $-z > 0$ y así

$$z(a \otimes u) = -(-z(a \otimes u)) = -(-za) \otimes u = (za) \otimes u$$

$$z(a \otimes u) = -(-z(a \otimes u)) = -(a \otimes (-zu)) = a \otimes (zu)$$

por el inciso 5. □

Ejemplo 4.3.4. Sea $0 \neq n \in \mathbb{Z}$. Consideremos los \mathbb{Z} -módulos \mathbb{Z}_n , \mathbb{Q} y el producto tensorial $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Q}$ sobre \mathbb{Z} . Entonces

$$a \otimes q = a \otimes \left(\frac{n}{n} q \right) = a \otimes \left(n \left(\frac{1}{n} \right) q \right) = an \otimes \left(\frac{1}{n} q \right) = 0 \otimes \left(\frac{1}{n} q \right) = 0.$$

Por lo tanto $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Q} = 0$.

Definición 4.3.5. Sean A_S un S -módulo derecho, ${}_S U$ un S -módulo izquierdo y M un grupo abeliano. Una función $\varphi : A \times U \rightarrow M$ es *biaditiva* si

$$\varphi(a_1 + a_2, u) = \varphi(a_1, u) + \varphi(a_2, u)$$

$$\varphi(a, u_1 + u_2) = \varphi(a, u_1) + \varphi(a, u_2).$$

Decimos que φ es *S-tensorial* si además

$$\varphi(as, u) = \varphi(a, su).$$

Dados A_S un S -módulo derecho y ${}_S U$ un S -módulo izquierdo, podemos considerar la siguiente función

$$A \times U \xrightarrow{i} F \xrightarrow{\pi} A \otimes_S U := F/K$$

donde i es la inclusión de la base y π es la proyección canónica. Denotemos a esta composición por $\tau : A \times U \rightarrow A \otimes_S U$.

Proposición 4.3.6. Sean A_S un S -módulo derecho y ${}_S U$ un S -módulo izquierdo. Entonces $\tau : A \times U \rightarrow A \otimes_S U$ es *S-tensorial*. Además, para todo \mathbb{Z} -morfismo $\lambda : A \otimes_S U \rightarrow M$ la función $\lambda\tau$ también es *S-tensorial*.

Demostración. Veamos que τ es *S-tensorial*. Sean $a, b \in A$, $u, v \in U$ y $s \in S$. Entonces

$$\tau(a + b, u) = (a + b) \otimes u = a \otimes u + b \otimes u = \tau(a, u) + \tau(b, u)$$

por la Proposición 4.3.3. De la misma manera $\tau(a, u + v) = \tau(a, u) + \tau(a, v)$. Ahora,

$$\tau(as, u) = as \otimes u = a \otimes su = \tau(a, su)$$

por la Proposición 4.3.3. El resto de la prueba se deja como ejercicio. □

Dados A_S un S -módulo derecho, ${}_S U$ un S -módulo izquierdo y M un grupo abeliano, denotemos por $\text{Tens}_S(A \times U, M)$ a la colección de funciones *S-tensoriales*.

Proposición 4.3.7. Sean A_S un S -módulo derecho, ${}_S U$ un S -módulo izquierdo y M un grupo abeliano. Entonces, $\text{Tens}_S(A \times U, M)$ es un \mathbb{Z} -módulo. Además, hay un isomorfismo

$$\text{Tens}_S(A \times U, M) \cong \text{Hom}_{\mathbb{Z}}(A \otimes_S U, M)$$

de \mathbb{Z} -módulos.

Demostración. Dados $\lambda, \zeta \in \text{Tens}_S(A \times U, M)$, definimos $(\lambda + \zeta)(a, u) = \lambda(a, u) + \zeta(a, u)$. Claramente esta operación hace a $\text{Tens}_S(A \times U, M)$ un grupo abeliano. Definimos $\Phi : \text{Hom}_{\mathbb{Z}}(A \otimes_S U, M) \rightarrow \text{Tens}_S(A \times U, M)$ como $\Phi(\lambda) = \lambda\tau$ la cual está bien definida por la Proposición 4.3.6. Sean $\lambda, \zeta \in \text{Hom}_{\mathbb{Z}}(A \otimes_S U, M)$. Entonces

$$\begin{aligned} \Phi(\lambda + \zeta)(a, u) &= (\lambda + \zeta)\tau(a, u) = (\lambda + \zeta)(a \otimes u) = \lambda(a \otimes u) + \zeta(a \otimes u) \\ &= \lambda\tau(a, u) + \zeta\tau(a, u) = \Phi(\lambda)(a, u) + \Phi(\zeta)(a, u). \end{aligned}$$

Supongamos que $\Phi(\lambda) = 0$, es decir, $0 = \Phi(\lambda)(a, u) = \lambda\tau(a, u)$ para todo $(a, u) \in A \times U$. Así $\lambda(\sum(a_i \otimes u_i)) = \sum(\lambda\tau(a_i, u_i)) = 0$. Por lo tanto $\lambda = 0$, es decir, Φ es inyectiva. Sea $\varphi \in \text{Tens}_S(A \times U, M)$. Como $A \times U$ es base de F entonces existe un único \mathbb{Z} -morfismo $\bar{\varphi} : F \rightarrow M$, dado como $\bar{\varphi}(\sum_{i=1}^n z_i(a_i, u_i)) = \sum_{i=1}^n z_i\varphi(a_i, u_i)$. Ahora, como φ es S -tensorial se tiene que $K \subseteq \text{Ker } \varphi$ (Definición 4.3.1), lo que implica que existe $\lambda : A \otimes_S U \rightarrow M$ tal que $\lambda\pi = \bar{\varphi}$. Por lo tanto $\lambda\tau = \varphi$ y así Φ es suprayectiva.

$$\begin{array}{ccc} A \times U & \xrightarrow{\quad} & F \xrightarrow{\pi} A \otimes_S U \\ \varphi \downarrow & \searrow \exists \bar{\varphi} & \searrow \exists \lambda \\ & & M \end{array}$$

Por lo tanto Φ es un isomorfismo. □

Corolario 4.3.8 (Propiedad universal del producto tensorial). Sean A_S un S -módulo derecho, ${}_S U$ un S -módulo izquierdo y M un grupo abeliano. Dada una función S -tensorial $\varphi : A \times U \rightarrow M$, existe un único \mathbb{Z} -morfismo $\lambda : T \rightarrow M$ tal que $\lambda\tau = \varphi$, donde τ es la función de la Proposición 4.3.6.

$$\begin{array}{ccc} A \times U & \xrightarrow{\tau} & {}_{\mathbb{Z}}T \\ \varphi \downarrow & \searrow \exists \lambda & \\ {}_{\mathbb{Z}}M & & \end{array}$$

Demostración. La prueba se sigue de la Proposición 4.3.7. □

Proposición 4.3.9. Dados $A_S, B_S, {}_S U$ y ${}_S V$ S -módulos, $\alpha \in \text{Hom}_S(A, B)$ y $\mu \in \text{Hom}_S(U, V)$ existe un único \mathbb{Z} -morfismo $\alpha \otimes \mu : A \otimes_S U \rightarrow B \otimes_S V$ tal que $(\alpha \otimes \mu)(a \otimes u) = \alpha(a) \otimes \mu(u)$

Demostración. Sean $A_S, B_S, {}_S U$ y ${}_S V$ S -módulos, $\alpha \in \text{Hom}_S(A, B)$ y $\mu \in \text{Hom}_S(U, V)$. Entonces la función $\varphi : A \times U \rightarrow B \otimes_S V$ definida como $\varphi(a, u) = \alpha(a) \otimes \mu(u)$ es S -tensorial (Ejercicio 4.4.17). Por lo tanto existe un único morfismo $\alpha \otimes \mu : A \otimes_S U \rightarrow B \otimes_S V$. □

Proposición 4.3.10. Sean $A_S, B_S, C_S, {}_S U, {}_S V$ y ${}_S W$ S -módulos, $\alpha \in \text{Hom}_S(A, B)$, $\mu \in \text{Hom}_S(U, V)$, $\beta \in \text{Hom}_S(B, C)$ y $\nu \in \text{Hom}_S(V, W)$. Entonces

1. $\text{Id}_A \otimes \text{Id}_U = \text{Id}_{A \otimes_S U}$.
2. $(\beta \otimes \nu)(\alpha \otimes \mu) = \beta\alpha \otimes \nu\mu$.
3. Si α y μ son isomorfismos entonces $\alpha \otimes \mu$ es isomorfismo.

Demostración. Ejercicio 4.4.18. □

Proposición 4.3.11. Sean A_S y ${}_S U$ S -módulos. Supongamos que además ${}_R A$ es un R - S -bimódulo. Entonces $A \otimes_S U$ es un R -módulo izquierdo.

Demostración. Sean $r \in R$ y $\sum a_i \otimes u_i \in A \otimes_S U$. Definimos

$$r \left(\sum a_i \otimes u_i \right) = \sum r a_i \otimes u_i.$$

Si $r_1, r_2 \in R$, entonces

$$r_1 \left(r_2 \left(\sum a_i \otimes u_i \right) \right) = r_1 \left(\sum r_2 a_i \otimes u_i \right) = \sum r_1 r_2 a_i \otimes u_i = (r_1 r_2) \left(\sum a_i \otimes u_i \right).$$

Además,

$$\begin{aligned} (r_1 + r_2) \left(\sum a_i \otimes u_i \right) &= \left(\sum (r_1 + r_2) a_i \otimes u_i \right) = \sum (r_1 a_i + r_2 a_i) \otimes u_i \\ &= \sum r_1 a_i \otimes u_i + \sum r_2 a_i \otimes u_i = r_1 \left(\sum a_i \otimes u_i \right) + r_2 \left(\sum a_i \otimes u_i \right) \end{aligned}$$

Es claro que $r \left(\sum a_i \otimes u_i + \sum a_j \otimes u_j \right) = r \left(\sum a_i \otimes u_i \right) + r \left(\sum a_j \otimes u_j \right)$ y que $1 \left(\sum a_i \otimes u_i \right) = \sum a_i \otimes u_i$. □

Observación 4.3.12. De forma análoga a la proposición anterior si ${}_S U_T$ es un S - T -bimódulo entonces $A \otimes_S U$ tienen estructura de T -módulo derecho (Ejercicio 4.4.19).

Proposición 4.3.13. Sean R y S anillos. Consideremos los módulos ${}_R A_S, {}_S U$ y ${}_R M$. Si $\varphi : A \times U \rightarrow M$ es una función S -tensorial tal que $\varphi(ra, u) = r\varphi(a, u)$ para todo $r \in R$ entonces existe un único R -morfismo $\lambda : A \otimes_S U \rightarrow M$ tal que $\lambda\tau = \varphi$.

Demostración. Por la propiedad universal del producto tensorial (Corolario 4.3.8) existe un único \mathbb{Z} -morfismo $\lambda : A \otimes_S U \rightarrow M$ tal que $\lambda\tau = \varphi$. Ahora, sea $r \in R$ y $\sum a_i \otimes u_i \in A \otimes_S U$. Entonces

$$\begin{aligned} \lambda \left(r \sum a_i \otimes u_i \right) &= \lambda \left(\sum r a_i \otimes u_i \right) = \sum \varphi(r a_i, u_i) = \sum (r \varphi(a_i, u_i)) \\ &= r \sum \varphi(a_i, u_i) = r \lambda \left(\sum a_i \otimes u_i \right). \end{aligned}$$

□

Teorema 4.3.14. Para todo S -módulo izquierdo U se tiene que ${}_S(S \otimes_S U) \cong {}_S U$.

Demostración. Definimos $\varphi : S \times U \rightarrow U$ como $\varphi(s, u) = su$ la cual es S -tensorial. Además $\varphi(ss', u) = (ss')u = s(s'u)$. Por la Proposición 4.3.13 existe un único S -morfismo $\lambda : S \otimes_S U \rightarrow U$ definido como

$$\lambda\left(\sum s_i \otimes u_i\right) = \sum s_i u_i.$$

Si $u \in U$, entonces $\lambda(1 \otimes u) = u$. Por lo tanto λ es sobre. Si $\lambda(\sum s_i \otimes u_i) = 0$, entonces $\sum s_i u_i = 0$. Así que

$$\sum s_i \otimes u_i = \sum 1 \otimes s_i u_i = 1 \otimes \sum s_i u_i = 1 \otimes 0 = 0.$$

Por lo tanto λ es inyectiva. \square

Observación 4.3.15. De forma análoga a la proposición anterior, si tenemos A_S un S -módulo derecho, entonces $A \otimes_S S \cong A_S$.

Proposición 4.3.16. *El producto tensorial es asociativo, es decir,*

$$(A \otimes_R M) \otimes_S U \cong A \otimes_R (M \otimes_S U)$$

para módulos A_R , ${}_R M_S$ y ${}_S U$.

Demostración. Sea $u_0 \in U$. Definimos la función

$$\varphi_{u_0} : A \times M \rightarrow A \otimes_R (M \otimes_S U)$$

como

$$\varphi_{u_0}(a, m) = a \otimes (m \otimes u_0)$$

Se puede ver fácilmente que esta función es R -tensorial. Por lo tanto existe un único morfismo $\lambda_{u_0} : A \otimes_R M \rightarrow A \otimes_R (M \otimes_S U)$ el cual se calcula como $\lambda_{u_0}(\sum a_i \otimes m_i) = \sum a_i \otimes (m_i \otimes u_0)$. Ahora definimos la función

$$\psi : (A \otimes_R M) \times U \rightarrow A \otimes_R (M \otimes_S U)$$

como

$$\psi\left(\sum (a_i \otimes m_i), u\right) = \lambda_u\left(\sum a_i \otimes m_i\right).$$

La función ψ es S -tensorial, así que existe un único morfismo $\zeta : (A \otimes_R M) \otimes_S U \rightarrow A \otimes_R (M \otimes_S U)$ definido como

$$\zeta\left(\sum (a_i \otimes m_i) \otimes u\right) = \sum a_i \otimes (m_i \otimes u_i).$$

De forma análoga podemos construir el inverso de ζ . \square

Proposición 4.3.17. *Sea $\{A_i\}_I$ una familia de S -módulos derechos y sea $\{U_j\}_J$ una familia de S -módulos izquierdos. Entonces*

$$\left(\bigoplus_I A_i\right) \otimes_S \left(\bigoplus_J U_j\right) \cong \bigoplus_I \bigoplus_J (A_i \otimes_S U_j).$$

Demostración. Sean $\iota_i : A_i \rightarrow \bigoplus_I A_i$ y $\eta_j : U_j \rightarrow \bigoplus_J U_j$ las inclusiones canónicas. Pongamos $A = \bigoplus_I A_i$ y $U = \bigoplus_J U_j$. Definimos la siguiente función S -tensorial

$$\varphi : A \times U \rightarrow \bigoplus_I (A_i \otimes U)$$

como

$$\varphi((a_i)_I, u) = (a_i \otimes u)_I.$$

Entonces existe un único morfismo $\lambda : A \otimes U \rightarrow \bigoplus_I (A_i \otimes U)$ definido como

$$\lambda((a_i)_I \otimes u) = (a_i \otimes u)_I.$$

Ahora para cada $i \in I$, usando la función S -tensorial definida como

$$(a_i, (u_j)_J) \mapsto \iota_i(a_i) \otimes (u_j)_J$$

tenemos un único morfismo $\lambda_i : A_i \otimes_S U \rightarrow A \otimes_S U$. Por la propiedad universal de la suma directa (Teorema 4.1.4), existe un único morfismo

$$\zeta : \bigoplus_I (A_i \otimes_S U) \rightarrow A \otimes_S U$$

dado por

$$\zeta((a_i \otimes u)_I) = \sum_I (\iota_i(a_i) \otimes u).$$

Sea $\sum((a_{i_k})_I)_k \otimes u \in A \otimes_S U$. Entonces

$$\begin{aligned} \zeta \lambda \left(\sum((a_{i_k})_I)_k \otimes u \right) &= \zeta \left(\sum((a_{i_k} \otimes u)_k) \right) \\ &= \sum \sum_I \iota_{i_k}(a_{i_k}) \otimes u = \sum((a_{i_k})_I)_k \otimes u. \end{aligned}$$

Por lo tanto $\zeta \lambda = Id_{A \otimes_S U}$. Por otro lado, si $(a_i \otimes u)_I \in \bigoplus_I (A_i \otimes_S U)$ entonces

$$\begin{aligned} \lambda \zeta((a_i \otimes u)_I) &= \lambda \left(\sum_I (\iota_i(a_i) \otimes u) \right) = \sum_I \lambda(\iota_i(a_i) \otimes u) \\ &= \sum_I \mu_i(a_i \otimes u) = (a_i \otimes u)_I \end{aligned}$$

donde $\mu_i : A_i \otimes_S U \rightarrow \bigoplus_I (A_i \otimes_S U)$ es la inclusión canónica. Por lo tanto λ es un isomorfismo. De la misma forma se puede ver que para cada $i \in I$

$$A_i \otimes_S U \cong \bigoplus_J (A_i \otimes_S U_j).$$

Por lo tanto

$$\bigoplus_I \bigoplus_J (A_i \otimes_S U_j) \cong A \otimes_S U.$$

□

En general el producto tensorial no conmuta con productos directos como se puede ver en el siguiente ejemplo.

Ejemplo 4.3.18. Sea \mathbb{P} es conjunto de números primos y consideremos $\prod_{p \in \mathbb{P}} \mathbb{Z}_p$. Por el Ejercicio 4.4.20, existe un único \mathbb{Z} -morfismo

$$\mathbb{Q} \otimes_{\mathbb{Z}} \prod_{p \in \mathbb{P}} \mathbb{Z}_p \rightarrow \prod_{p \in \mathbb{P}} \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

Por el Ejemplo 4.3.4, el codominio de esta función es 0. Veamos que el dominio no es 0. Por el Ejercicio 4.4.2 hay un monomorfismo $\varphi : \mathbb{Z} \rightarrow \prod_{p \in \mathbb{P}} \mathbb{Z}_p$. Afirmamos que

$$Id_{\mathbb{Q}} \otimes \varphi : \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z} \rightarrow \mathbb{Q} \otimes_{\mathbb{Z}} \prod_{p \in \mathbb{P}} \mathbb{Z}_p$$

es un monomorfismo. Sea $\sum_{i=1}^{\ell} \frac{a_i}{b_i} \otimes n_i \in \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}$ tal que $Id_{\mathbb{Q}} \otimes \varphi \left(\sum_{i=1}^{\ell} \frac{a_i}{b_i} \otimes n_i \right) = 0$, es decir, $\sum_{i=1}^{\ell} \frac{a_i}{b_i} \otimes \varphi(n_i) = 0$. Entonces

$$0 = \sum_{i=1}^{\ell} \frac{a_i}{b_i} \otimes n_i ([1]_p)_{\mathbb{P}}$$

donde $[1]_p$ es la clase de 1 módulo $p \in \mathbb{P}$. Existen enteros no cero, c_1, \dots, c_{ℓ} tales que

$$\begin{aligned} 0 &= \sum_{i=1}^{\ell} \frac{a_i}{b_i} \otimes n_i ([1]_p)_{\mathbb{P}} = \sum_{i=1}^{\ell} c_i a_i \otimes n_i ([1]_p)_{\mathbb{P}} = \sum_{i=1}^{\ell} 1 \otimes c_i a_i n_i ([1]_p)_{\mathbb{P}} \\ &= \sum_{i=1}^{\ell} 1 \otimes ([c_i a_i n_i]_p)_{\mathbb{P}} = \sum_{i=1}^{\ell} 1 \otimes \varphi(c_i a_i n_i) = 1 \otimes \varphi \left(\sum_{i=1}^{\ell} c_i a_i n_i \right). \end{aligned}$$

Por el Teorema 4.3.14, esto implica que $\varphi \left(\sum_{i=1}^{\ell} c_i a_i n_i \right) = 0 \in \prod_{p \in \mathbb{P}} \mathbb{Z}_p$. Como φ es un monomorfismo, $\sum_{i=1}^{\ell} c_i a_i n_i = 0 \in \mathbb{Z}$. Tomando el elemento inicial y usando el isomorfismo dado por el Teorema 4.3.14 obtenemos que

$$\sum_{i=1}^{\ell} \frac{a_i}{b_i} \otimes n_i = \sum_{i=1}^{\ell} c_i a_i \otimes n_i \mapsto \sum_{i=1}^{\ell} c_i a_i n_i = 0$$

Por lo tanto $\sum_{i=1}^{\ell} \frac{a_i}{b_i} \otimes n_i = 0$ y así $Id_{\mathbb{Q}} \otimes \varphi$ es un monomorfismo. Esto implica que $\mathbb{Q} \otimes_{\mathbb{Z}} \prod_{p \in \mathbb{P}} \mathbb{Z}_p \neq 0$.

4.4. Ejercicios

1. Pruebe que el producto de una familia de R -módulos izquierdos es un R -módulo izquierdos.
2. Sea \mathbb{P} el conjunto de números primos. Demuestre que hay un monomorfismo $\varphi : \mathbb{Z} \rightarrow \prod_{p \in \mathbb{P}} \mathbb{Z}_p$.
3. ¿Existe un monomorfismo $\varphi : \mathbb{Z} \rightarrow \bigoplus_{p \in \mathbb{P}} \mathbb{Z}_p$?
4. Sea $\varphi : M \rightarrow \prod_I N_i$ un R -morfismo. Demuestre que si $\pi_i \varphi = 0$ para todo $i \in I$, entonces $\varphi = 0$, donde $\pi_i : \prod_I N_i \rightarrow N_i$ son las proyecciones canónicas.
5. Sea $\varphi : \bigoplus_I M_i \rightarrow N$ un R -morfismo. Demuestre que si $\varphi \eta_i = 0$ para todo $i \in I$, entonces $\varphi = 0$, donde $\eta_i : M_i \rightarrow \bigoplus_I M_i$ son las inclusiones canónicas.
6. Sea $\{M_i\}_I$ una familia de R -módulos y para cada $i \in I$ tomemos un submódulo $N_i \leq M_i$. Demuestre que

$$\bigoplus_I M_i/N_i \cong \frac{\bigoplus_I M_i}{\bigoplus_I N_i}.$$

7. Sean M y N dos R -módulos finitamente generados. Demuestre que $M \oplus N$ es finitamente generado. Concluya que si $\{M_1, M_2, \dots, M_n\}$ es una familia finita de R -módulos finitamente generados, entonces $\bigoplus_{i=1}^n M_i$ es finitamente generado.
8. Complete la prueba de la Proposición 4.1.7.
9. Demuestre la Proposición 4.1.10.
10. Sean $L, N \leq M$. Consideremos las inclusiones canónicas $i : L \rightarrow M$ y $j : N \rightarrow M$. Demuestre que el producto fibrado del par (i, j) está dado por $L \cap N$ y su respectiva inclusión en L y N .
11. Sean M y N R -módulos. Demuestre que la suma directa $M \oplus N$ con sus inclusiones canónicas es el coproducto fibrado del siguiente ángulo:

$$\begin{array}{ccc} 0 & \longrightarrow & M \\ & & \downarrow \\ & & N \end{array}$$

12. Sea $0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\xi} C \rightarrow 0$ una sucesión exacta corta y $\varphi : A \rightarrow M$ un R -morfismo. Demuestre que el coproducto fibrado (ψ, β) de (φ, α) determina el siguiente diagrama conmutativo con renglones exactos

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\xi} & C & \longrightarrow & 0 \\ & & \downarrow \varphi & & \downarrow \beta & & \downarrow 1 & & \\ 0 & \longrightarrow & M & \xrightarrow{\psi} & N & \longrightarrow & C & \longrightarrow & 0. \end{array}$$

13. Demuestre el Teorema 4.2.6.
14. Demuestre que el conjunto $\{(a, u) \in F \mid (a, u) \in A \times U\} = \{\eta_{(a,u)}(1) \mid (a, u) \in A \times U\}$, dado al inicio de la Sección 4.3, es una base de F .
15. Complete la prueba de la Proposición 4.3.3.
16. Complete la prueba de la Proposición 4.3.6.
17. Sean $A_S, B_S, {}_S U$ y ${}_S V$ S -módulos, $\alpha \in \text{Hom}_S(A, B)$ y $\mu \in \text{Hom}_S(U, V)$. Demuestre que la función $\varphi : A \times U \rightarrow B \otimes_S V$ definida como $\varphi(a, u) = \alpha(a) \otimes \mu(u)$ es S -tensorial.
18. Demuestre la Proposición 4.3.10.
19. Demuestre la Proposición 4.3.12.
20. Sea N_S un S -módulo derecho y $\{M_i\}_I$ una familia de S -módulos izquierdos. Demuestre que existe un único \mathbb{Z} -morfismo

$$N \otimes_S \prod_I M_i \rightarrow \prod_I N \otimes_S M_i.$$

21. Sean $p, q \in \mathbb{P}$. Demuestre que $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Z}_q \neq 0$ si y solo si $p = q$.

Capítulo 5

Módulos semisimples y el Radical

5.1. Submódulos esenciales y superfluos

5.1.1. Submódulos esenciales

Definición 5.1.1. Sea M un módulo y $N \leq M$. Un *pseudocomplemento* (p.c.) de N en M es un submódulo $L \leq M$ que es máximo con la propiedad de $N \cap L = 0$.

Proposición 5.1.2. Sea M un módulo y $N \leq M$. Entonces N tiene pseudocomplementos en M .

Demostración. Sea $\mathbb{A} = \{L \leq M \mid L \cap N = 0\}$, $\mathbb{A} \neq \emptyset$ ya que $\{0\} \in \mathbb{A}$, además (\mathbb{A}, \subseteq) es un COPO. Si \mathcal{C} es una cadena en \mathbb{A} , entonces $\bigcup \mathcal{C}$ es una cota superior de \mathcal{C} . Sea $x \in N \cap \bigcup \mathcal{C}$. Entonces $x \in N$ y existe $L \in \mathcal{C}$ tal que $x \in L$ lo que implica que $x \in N \cap L = 0$. Así que $x = 0$. Por lo tanto $\bigcup \mathcal{C} \in \mathbb{A}$. Por el Lema de Zorn \mathbb{A} tiene máximos. \square

Definición 5.1.3. Sea $N \leq M$. Decimos que N es *esencial* en M ($N \leq_e M$) si siempre que $N \cap L = 0$ con $L \leq M$ se tiene que $L = 0$, equivalentemente si $0 \neq L \leq M$ entonces $N \cap L \neq 0$.

Ejemplo 5.1.4. 1. En \mathbb{Z} si $n \cdot m \neq 0$ entonces $\mathbb{Z}m \cap \mathbb{Z}n = \mathbb{Z}[m; n] \neq 0$ donde $[m; n]$ denota el mínimo común múltiplo. Por lo tanto todo $0 \neq \mathbb{Z}n$ es esencial en \mathbb{Z} .

2. Sea $p \in \mathbb{P}$ y $n > 0$. Entonces todo submódulo no cero de \mathbb{Z}_p^n es esencial.

Proposición 5.1.5. Son equivalentes para $N \leq M$:

(a) $N \leq_e M$

(b) Para todo $0 \neq m \in M$, existe $r \in R$ tal que $0 \neq rm \in N$

Demostración. (a) \Rightarrow (b) Sea $0 \neq m \in M$. Entonces $0 \neq Rm \leq M$. Como N es esencial, $Rm \cap N \neq 0$ así que existe $r \in R$ tal que $0 \neq rm \in N$.

(b) \Rightarrow (a) Sea $0 \neq L \leq M$ y $0 \neq l \in L$. Por hipótesis existe $r \in R$ tal que $0 \neq rl \in N$. Entonces $rl \in N \cap L$ y por lo tanto $N \leq_e M$. \square

Proposición 5.1.6. *Sea M un módulo y $N \leq M$. Si U es un p.c. de N en M entonces $N \oplus U \leq_e M$*

Demostración. Sea $L \leq M$ tal que $(N \oplus U) \cap L = 0$. En particular $N \cap L = 0$ y $L \cap U = 0$. Tomemos $n \in N \cap (U \oplus L)$. Entonces $n = u + l$ con $u \in U$ y $l \in L$. Así $l = n - u$ lo que implica que $l = 0$. Entonces $n = u$, es decir, $n \in U \cap N$. Por lo tanto $n = 0$. Por la maximalidad de U , $U + L = U$. Entonces $L = 0$ y por lo tanto $U \oplus N \leq_e M$. \square

Lema 5.1.7. 1. *Si $A \leq B \leq M \leq N$ y $A \leq_e N$ entonces $B \leq_e M$.*

2. *Si $\{A_i\}_{i=1}^n$ con $A_i \leq_e M$ entonces $\bigcap_{i=1}^n A_i \leq_e M$*

3. *Si $B \leq_e N$ y $\varphi : M \rightarrow N$ entonces $\varphi^{-1}(B) \leq_e M$.*

Demostración. 1. Si $U \leq M$ y $B \cap U = 0$ entonces $A \cap U = 0$. Como $U \leq M \leq N$ y $A \leq_e N$ entonces $U = 0$.

2. Por inducción. Si $n = 1$ es claro. Supongamos que vale para $n > 1$ i.e., $\bigcap_{i=1}^{n-1} A_i \leq_e M$. Sea $U \leq M$ tal que $(\bigcap_{i=1}^n A_i) \cap U = 0$. Así $0 = (\bigcap_{i=1}^{n-1} A_i \cap A_n) \cap U$. Por hipótesis de inducción se tiene que $A_n \cap U = 0$, pero $A_n \leq_e M$. Por lo tanto $U = 0$.

3. Sea $U \leq M$ tal que $\varphi^{-1}(B) \cap U = 0$. Si $\varphi(U) \cap B \neq 0$ entonces existe $b \in B$ tal que $b = \varphi(u)$ p.a. $0 \neq u \in U$. Así $u \in \varphi^{-1}(B) \cap U = 0$. Por lo tanto $\varphi(B) \cap U = 0$. Como $B \leq_e N$, $\varphi(U) = 0$ lo que implica que $U \subseteq \text{Ker } \varphi \subseteq \varphi^{-1}(0) \subseteq \varphi^{-1}(B)$. Así $U = \varphi^{-1}(B) \cap U = 0$ y por lo tanto $\varphi^{-1}(B) \leq_e M$. \square

Proposición 5.1.8. *Supongamos que $M = \sum_I M_i$ con $M_i \leq M$. Si $A_i \leq_e M_i$ y $\sum_I A_i = \bigoplus_I A_i$, entonces $\bigoplus_I A_i \leq_e M$ y $\sum_I M_i = \bigoplus_I M_i$.*

Demostración. Para cada $m \in M$ tenemos que $m = m_{i_1} + \dots + m_{i_k}$ con $m_{i_j} \in M_{i_j}$. Hagamos el caso para dos submódulos, es decir, supongamos que $m = m_1 + m_2$ con $0 \neq m_1 \in M_1$ $0 \neq m_2 \in M_2$ y que $A_1 \leq_e M_1$ $A_2 \leq_e M_2$ y $A_1 + A_2 = \bigoplus_I A_i$. Entonces existe $0 \neq r \in R$ tal que $0 \neq rm_1 \in A_1$ por la Proposición 5.1.5. Si $rm_2 = 0$, entonces $rm = rm_1$ y así $rm \in A_1 \oplus A_2$. Si $rm_2 \neq 0$ entonces existe $s \in R$ tal que $0 \neq srm_2 \in A_2$. Por lo tanto $srm = srm_1 + srm_2 \in A_1 \oplus A_2$. Lo que implica que $A_1 \oplus A_2 \leq_e M$. Para el caso general, como cada $m \in M$ se escribe como una suma finita, por inducción tenemos que $\bigoplus_I A_i \leq_e M$. Ahora, supongamos que $m_i = m_1 + \dots + m_{i-1}$ con $m_j \in M_j$. Entonces existe $0 \neq r \in R$ tal que $0 \neq r(m_1 + \dots + m_{i-1}) \in A_1 + \dots + A_{i-1}$. Así $rm_i \in M_i \cap (A_1 \oplus \dots \oplus A_{i-1})$. Entonces, existe $0 \neq s \in R$ tal que $0 \neq srm_i \in A_i$ lo que implica que $srm_i \in A_i \cap A_1 \oplus \dots \oplus A_{i-1}$. Así $srm_i = 0$ que es una contradicción. Por lo tanto $m_i = 0$. Esto implica que $\sum_I M_i = \bigoplus_I M_i$. \square

Corolario 5.1.9. *Si $M = \bigoplus_I M_i$ con $A_i \leq_e M_i \leq M$, entonces $\sum_I A_i = \bigoplus_I A_i$ y $\bigoplus_I A_i \leq_e M$.*

Demostración. Como $\sum_I M_i = \bigoplus_I M_i$ y $A_i \leq M_i$ entonces $\sum_I A_i = \bigoplus_I A_i$ por lo que estamos en las hipótesis de la Proposición 5.1.8. Por lo tanto $\bigoplus_I A_i \leq_e M$. \square

Corolario 5.1.10. *Sea $M = \bigoplus_I M_i$ y $B \leq M$. Son equivalentes:*

- (a) $B \cap M_i \leq_e M_i$ para cada $i \in I$;

$$(b) \bigoplus_I (B \cap M_i) \leq_e M;$$

$$(c) B \leq_e M$$

Demostración. (a) \Rightarrow (b). Se tiene por el Corolario 5.1.10.

(b) \Rightarrow (c). Para cada $i \in I$, $B \cap M_i \subseteq B$ así que $\bigoplus (B \cap M_i) \subseteq B \subseteq M$. Por lo tanto $B \leq_e M$.

(c) \Rightarrow (a). Tomemos $0 \neq m_i \in M_i$, entonces existe $0 \neq r \in R$ tal que $0 \neq rm_i \in B$ y así $rm_i \in B \cap M_i$. Por lo tanto $B \cap M_i \leq_e M$. \square

Observación 5.1.11. Dados $L, N \leq M$ tales que $N \cap L = 0$ entonces, siguiendo la prueba de la Proposición 5.1.2, se puede ver que N tiene pseudocomplementos en M que contienen a L .

Definición 5.1.12. Sean $L, N \leq M$. Decimos que L es *extensión esencial* de N si $N \leq_e L$. Si L es máximo con esta propiedad entonces L es una *extensión esencial máxima*.

Proposición 5.1.13. Si $N \leq M$ y U un p.c. de N en M y V un p.c. de U en M que incluye a N , entonces $N \leq_e V$ y V es extensión esencial máxima.

Demostración. Sea $L \leq V$ tal que $L \cap N = 0$. Entonces

$$N \cap (U + L) = (N \cap V) \cap (U + L) = N \cap (V \cap (U + L))$$

Como $L \subseteq V$, por la ley modular $N \cap (V \cap (U + L)) = N \cap (L + (V \cap U)) = N \cap L = 0$. Por hipótesis, U es máximo tal que $U \cap N = 0$ así que $U + L = U$ lo que implica $L \subseteq U$. Como $L \subseteq V$ y $U \cap V = 0$ se tiene que $L = 0$. Por lo tanto $N \leq_e V$. Además, si $V' \leq M$ es tal que $V \subseteq V'$, la maximidad de V se tiene que $V' \cap U \neq 0$, pero $(V' \cap U) \cap N = V' \cap (U \cap N) = 0$. Por lo tanto N no es esencial en V' . \square

Observación 5.1.14. Sea $N \leq M$. Si U es un p.c. de N en M , V un p.c. de U en M que incluye a N y W es un p.c. de V que incluye a U entonces $W = U$.

Definición 5.1.15. Un submódulo $N \leq M$ se llama *esencialmente cerrado* (o simplemente *cerrado*) en M si no tiene extensiones esenciales distintas de N en M .

Teorema 5.1.16. La colección de los submódulos de M que son p.c. en M son exactamente los submódulos cerrados de M .

Demostración. Si N es un p.c. en M entonces existe $L \leq M$ tal que N es p.c. de L en M . Supongamos que $N \leq_e N'$. Por ser N p.c., se tiene que $N' \cap L \neq 0$. Como $N \leq_e N'$, $0 \neq N \cap (L \cap N')$. Lo que implica que $0 \neq N \cap L$. Esto es una contradicción y por lo tanto N es cerrado. Recíprocamente si N no tiene extensiones esenciales distintas de N dentro de M , entonces N es un p.c. de un p.c. de él. \square

Proposición 5.1.17. Sean $A, B \leq M$ tales que $A \cap B = 0$. Entonces B es un p.c. de A en M si y sólo si $(A + B)/B \leq_e M/B$.

Demostración. \Rightarrow . Supongamos que $((A+B)/B) \cap (U/B) = 0$. Entonces $(A+B) \cap U = B$ pero $(A+B) \cap U = B + (A \cap U)$ por lo tanto $(A \cap U) \subseteq B$, lo que implica que $A \cap U \subseteq A \cap B = 0$ y así $A \cap U = 0$ pero B es p.c. de A en M entonces $B = U$. Por lo tanto $U/B = 0$ lo que implica que $(A+B)/B \leq_e M/B$.

\Leftarrow . Supongamos que $B \leq U \leq M$ tal que $A \cap U = 0$

Si $x \in (A+B) \cap U$ entonces $x = a + b$ con $a \in A$, $b \in B$ y $x \in U$ así que $a = x - b \in A \cap U$ lo que implica que $a = 0$ y por lo tanto $x \in B$. Entonces $(A+B) \cap U \subseteq B$ así que $(A+B) \cap U = B$, i.e. $((A+B)/B) \cap (U/B) = 0$ pero como $(A+B)/B \leq_e M/B$ entonces $U = B$. Por lo tanto B es p.c. de A en M . \square

5.1.2. Submódulos superfluos

Definición 5.1.18. Sea $A \leq M$. Decimos que $A' \leq M$ es un *suplemento de A en M* , si es mínimo con la propiedad de que $A + A' = M$.

En general los suplementos no tienen por qué existir.

Ejemplo 5.1.19. Consideremos a \mathbb{Z} como \mathbb{Z} -módulo. Supongamos que $n\mathbb{Z}$ tiene un suplemento $m\mathbb{Z}$. Entonces $\mathbb{Z} = n\mathbb{Z} + m\mathbb{Z}$. Esto implica que m y n son primos relativos, así que existe un primo p tal que $p|m$ y no a n . Sea $\ell > 0$ la máxima potencia de p tal que $p^\ell k = m$. Entonces $\mathbb{Z} = n\mathbb{Z} + (p^{\ell+i}k)\mathbb{Z}$ and $(p^{\ell+i}k)\mathbb{Z} \subset m\mathbb{Z}$ for all $i > 0$ contradiciendo la minimalidad de $m\mathbb{Z}$. Por lo tanto ningún submódulo propio de \mathbb{Z} tiene suplemento.

Definición 5.1.20. Un submódulo $N \leq M$ es *superfluo* en M ($N \ll M$) si siempre que $N + L = M$ con $L \leq M$, se tiene que $L = M$.

Lema 5.1.21. *Supongamos que $M = A + B$. Entonces B es suplemento de A en M si y solo si $A \cap B \ll B$.*

Demostración. \Rightarrow . Sea $U \leq B$ tal que $B = U + (A \cap B)$. Tenemos que

$$M = A + B = A + U + (A \cap B) = A + U.$$

Entonces $B = U$ por la minimidad de B .

\Leftarrow . Sea $U \leq B$ tal que $M = A + U$. Entonces, usando la ley modular

$$B = M \cap B = B \cap (U + A) = U + (B \cap A)$$

Como $A \cap B \ll B$, $U = B$. Por lo tanto B es mínimo con la propiedad de que $M = A + B$. \square

Lema 5.1.22. *Sea $A \leq M$. Si A^\bullet es suplemento de A y $A^{\bullet\bullet}$ es suplemento de A^\bullet , entonces A^\bullet también es suplemento de $A^{\bullet\bullet}$.*

Demostración. Por hipótesis $M = A^\bullet + A^{\bullet\bullet}$. Sea $U \leq A^\bullet$ tal que $M = U + A^{\bullet\bullet}$. Entonces

$$A^\bullet = M \cap A^\bullet = (U + A^{\bullet\bullet}) \cap A^\bullet = U + (A^\bullet \cap A^{\bullet\bullet})$$

Como $M = A + A^\bullet$, $M = A + U + (A^\bullet \cap A^{\bullet\bullet})$. Por el Lemma 5.1.21 $(A^\bullet \cap A^{\bullet\bullet}) \ll A^{\bullet\bullet} < M$. Entonces $(A^\bullet \cap A^{\bullet\bullet}) \ll M$ lo que implica que $M = A + U$. Pero $U \leq A^\bullet$ así que $U = A^\bullet$. Por lo tanto A^\bullet es suplemento de $A^{\bullet\bullet}$. \square

Observación 5.1.23. Si $M = A \oplus B$ entonces B es pseudocomplemento y suplemento de A en M .

Ejemplo 5.1.24. 1. En ${}_Z\mathbb{Q}$ si $(\mathbb{Z}q_1 + \dots + \mathbb{Z}q_n) + U = \mathbb{Q}$ entonces $\{q_1, \dots, q_n\} \cup U$ es un generador de \mathbb{Q} . Por el Ejercicio 2.3.7 U es generador, así que $U = \mathbb{Q}$. Por lo tanto todo submódulo f.g. de \mathbb{Q} es superfluo.

2. Sea $p \in \mathbb{Z}$ un número primo y consideremos el siguiente subgrupo de ${}_Z\mathbb{Q}$:

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid p \nmid b \right\}.$$

Entonces $\mathbb{Z}_{(p)}$ tiene un único submódulo máximo $p\mathbb{Z}_{(p)}$. Esto implica que todo submódulo de $\mathbb{Z}_{(p)}$ es superfluo.

Lema 5.1.25. 1. Si $A \leq B \leq M \leq N$ y $B \ll M$ entonces $A \ll N$.

2. Si $\{A_i\}_{i=1}^n$ con $A_i \ll M$ entonces $\sum_{i=1}^n A_i \ll M$.

3. Si $A \ll M$ y $\varphi \in \text{Hom}_R(M, N)$ entonces $\varphi(A) \ll N$.

Demostración. 1. Supongamos que $A + U = N$ con $U \leq N$. Entonces $B + U = N$. Así $M = N \cap M = M \cap (B + U)$, como $B \leq M$, $M \cap (B + U) = B + (M \cap U)$. Por hipótesis $B \ll M$ así que $M \cap U = M$ lo que implica que $M \subseteq U$ pero $A \subseteq M \subseteq U$. Por lo tanto $A + U = U = N$, i.e., $A \ll N$.

2. Por inducción. Si $n = 1$, se tiene el resultado por hipótesis. Supongamos que la afirmación es válida para $n > 1$ y que $A_1 + \dots + A_{n-1} \ll M$. Si $(A_1 + \dots + A_{n-1} + A_n) + U = M$ con $U \leq M$ entonces $(A_1 + \dots + A_{n-1}) + (A_n + U) = M$. Por hipótesis de inducción, $A_n + U = M$ y como $A_n \ll M$ entonces $U = M$.

3. Sea $U \leq M$ tal que $\varphi(A) + U = N$. Dado $m \in M$ se tiene que $\varphi(m) = \varphi(a) + u$ con $a \in A$ y $u \in U$. Entonces $u = \varphi(m - a)$, por lo tanto $m - a \in \varphi^{-1}(U)$. Esto implica que $m \in \varphi^{-1}(U) + A$. Por lo tanto $M = \varphi^{-1}(U) + A$. Como $A \ll M$, $\varphi^{-1}(U) = M$ lo que implica que $\varphi(M) = \varphi\varphi^{-1}(U) = U \cap \text{Im } \varphi$, así que $\varphi(A) \subseteq U$. Entonces $N = \varphi(A) + U = U$ y por lo tanto $\varphi(A) \ll N$. \square

Lema 5.1.26. Sea M un módulo. Para todo $a \in M$ se tiene que Ra no es superfluo en M si y solo si existe $C \leq M$ máximo tal que $a \notin C$.

Demostración. \Rightarrow] Supongamos que Ra no es superfluo en M . Sea $\Gamma = \{N < M \mid N + Ra = M\}$. Como Ra no es superfluo en M , $\Gamma \neq \emptyset$. Sea \mathcal{C} una cadena en Γ , entonces $\bigcup \mathcal{C} \in \Gamma$ ya que para cada $N \in \mathcal{C}$, $a \notin N$ porque en caso contrario $Ra \leq N$ y $N + Ra = M$ lo que implica que $N = M$, contradiciendo que N era propio en M . Así, $a \notin \bigcup \mathcal{C}$, y claramente $\bigcup \mathcal{C} + Ra = M$. Entonces, por el lema de Zorn, Γ tiene máximos. Sea C un máximo en Γ entonces $a \notin C$. Si $C < U \leq M$ entonces $U \notin \Gamma$. Como $C + Ra = M$, $U + Ra = M$ así que $U = M$. Por lo tanto C es máximo en M .

\Leftarrow] Si existe $C < M$ máximo tal que $a \notin C$ entonces $C + Ra = M$. Como C es propio en M , Ra no es superfluo en M . \square

5.2. Módulos semisimples

Lema 5.2.1. *Sea M un módulo tal que todo submódulo es sumando directo. Entonces todo submódulo no cero de M contiene un simple.*

Demostración. Sea $0 \neq U \leq M$ y sin pérdida de generalidad supongamos que U es f.g.. Entonces U tiene submódulos máximos. Sea $V \leq U$ un máximo. Por hipótesis existe $L \leq M$ tal que $M = V \oplus L$, aplicando la ley modular obtenemos $U = M \cap U = (V \oplus L) \cap U = V \oplus (L \cap U)$. Así $U/V \cong L \cap U$. Por lo tanto $L \cap U$ es simple. \square

Lema 5.2.2. *Supongamos que $M = \sum_I S_i$ con S_i simple para cada $i \in I$. Si $U \leq M$ entonces:*

1. *Existe $J \subseteq I$ tal que $M = U \oplus (\bigoplus_J S_i)$.*
2. *Existe $K \subseteq I$ tal que $U \cong \bigoplus_K S_i$*

Demostración. 1. Sea $\Gamma = \{L \subseteq I \mid U + (\sum_L S_i) = U \oplus (\bigoplus_L S_i)\}$. Γ es no vacío ya que $\emptyset \in \Gamma$. Usando el lema de Zorn, sea $L \in \Gamma$ un máximo y $N = U \oplus (\bigoplus_L S_i)$. Sea $i_0 \in I - L$ entonces por la maximalidad de L se tiene que $N \cap S_{i_0} \neq 0$ pero S_{i_0} es simple así que $S_{i_0} \leq N$. Por lo tanto $M = \sum_I S_i \subseteq N \subseteq M$, es decir, $M = N$.

2. Tenemos que $M = U \oplus (\bigoplus_J S_i)$, aplicando (1) a $\bigoplus_J S_i$ se tiene que existe $K \subseteq I$ tal que $M = (\bigoplus_J S_i) \oplus (\bigoplus_K S_i)$. Por lo tanto $U \cong \bigoplus_K S_i$. \square

Teorema 5.2.3. *Son equivalentes para un módulo:*

- (a) *Todo submódulo $U \leq M$ es suma de submódulos simples.*
- (b) *M es suma de submódulos simples.*
- (c) *M es suma directa de submódulos simples.*
- (d) *Todo submódulo es sumando directo.*

Demostración. (a) \Rightarrow (b). Es clara.

(b) \Rightarrow (c). Aplicando el Lema 5.2.2 con $U = 0$.

(c) \Rightarrow (d). Aplicando el Lema 5.2.2.

(d) \Rightarrow (a). Sea $U \leq M$ y U_0 la suma de todos los submódulos simples de U . Por hipótesis $M = U_0 \oplus V$, usando la ley modular $U = U \cap M = U \cap U_0 \oplus V = U_0 \oplus (U \cap V)$. Si $U \cap V \neq 0$ por el Lema 5.2.1 existe $S \leq U \cap V$ simple, pero por la forma que se tomó U_0 esto implica que $U_0 \cap (U \cap V) \neq 0$, contradicción. Por lo tanto $U \cap V = 0$ lo que implica que $U = U_0$. \square

Definición 5.2.4. Un módulo M se llama *semisimple* si satisface alguna de las condiciones del Teorema 5.2.3. Decimos que un anillo R es *semisimple* si es semisimple como R -módulo.

Observación 5.2.5. Por el Teorema 5.2.12, no es necesario especificar el lado en la definición anterior.

Ejemplo 5.2.6. Sea K un campo. Entonces $M_2(K)$ es semisimple. De hecho $M_2(K) = \begin{pmatrix} K & 0 \\ 0 & K \end{pmatrix} \oplus \begin{pmatrix} 0 & K \\ 0 & 0 \end{pmatrix}$ (Ejemplo 2.1.4.II.). Por otro lado $TI_2(K)$ no es semisimple, el ideal izquierdo $\begin{pmatrix} 0 & 0 \\ K & 0 \end{pmatrix}$ no es un sumando directo.

Corolario 5.2.7. 1. Todo submódulo de un semisimple es semisimple.

2. Todo cociente de un semisimple es semisimple.

3. Suma de semisimples es semisimple.

Demostración. 1. Por el Lema 5.2.2.

2. Sea M semisimple y $\varphi : M \rightarrow N$ un morfismo suprayectivo. Como $M = \sum S_i$ con cada S_i simple entonces $\varphi(S_i) = 0$ o $\varphi(S_i) \cong S_i$. Por lo tanto $N = \varphi(M) = \varphi(\sum S_i) = \sum \varphi(S_i)$ que es suma de simples.

3. Es clara. \square

Definición 5.2.8. Un módulo M es *finitamente cogenerado* (f.c.) si para toda familia $\{A_i\}_I$ de submódulos de M tales que $\bigcap_I A_i = 0$ entonces existe $I_0 \subseteq I$ finito tal que $\bigcap_{I_0} A_i = 0$.

Teorema 5.2.9. Son equivalentes para un módulo M semisimple:

(a) $M = \sum_F S_i$ con F finito y S_i simple.

(b) $M = \bigoplus_{i=1}^n S_i$ con S_i simple.

(c) M es f.g.

(d) M es finitamente cogenerado.

Demostración. (a) \Leftrightarrow (b) Es clara.

(b) \Rightarrow (c) Cada submódulo simple S_i es cíclico, así que existe $x_i \in M$ tal que $S_i = Rx_i$ para cada $1 \leq i \leq n$. Entonces $M = \sum_{i=1}^n S_i = \sum_{i=1}^n Rx_i$. Por lo tanto M es finitamente generado.

(c) \Rightarrow (b) Supongamos que $M = Rx_1 + Rx_2 + \dots + Rx_n$. Como M es semisimple, cada Rx_i también lo es. Si $Rx_i = \bigoplus_J S_j$ con S_j simple, escribimos $x_i = x_{j_1} + \dots + x_{j_\ell}$ con $x_{j_k} \in S_{j_k}$. Esto implica que $Rx_i = \sum_{k=1}^{\ell} S_{j_k}$. Como esto para cada $1 \leq i \leq n$, se tiene que $M = \bigoplus_F S_i$ con F un conjunto finito.

(c) \Rightarrow (d) Sea $\{A_i\}_I$ una familia de submódulos de M tal que $\bigcap_I A_i = 0$ y supongamos que toda intersección finita es distinta de cero. Como M es semisimple y finitamente generado, por (b) y el lemma 5.2.2, cada $A_i = \bigoplus_{k=1}^{\ell_i} S_{i_k}$ con S_{i_k} simple para todo $i \in I$ y todo $1 \leq k \leq \ell_i$. Tenemos la cadena descendente $A_1 \supseteq A_1 \cap A_2 \supseteq \dots \supseteq \bigcap_{i=1}^n A_i \supseteq \dots$. Por el Lemma 5.2.2, $A_1 = (A_1 \cap A_2) \oplus \bigoplus_{k=1}^{l_1} S_{1_k}$ con $1 \leq l_1 \leq \ell_1$. Ahora, existe $1 \leq l_2 \leq \ell_2$ tal que

$$A_1 = (A_1 \cap A_2 \cap A_3) \oplus \bigoplus_{k=1}^{l_2} S_{2_k} \oplus \bigoplus_{k=1}^{l_1} S_{1_k}.$$

Continuando de esta manera, para cada $n > 0$ existen $l_1, \dots, l_n > 0$ tales que

$$A_1 = \left(\bigcap_{i=1}^{n+1} A_i \right) \oplus \bigoplus_{k=1}^{l_n} S_{n_k} \oplus \dots \oplus \bigoplus_{k=1}^{l_1} S_{1_k}.$$

Esto implica que $\bigoplus_{i>0} S_{i_1} \leq A_1$ lo que es una contradicción.

(d) \Rightarrow (b). Supongmos que M es f.c. y $M = \bigoplus_I S_i$ con cada S_i simple e I infinito. Entonces M tiene un submódulo de la forma $\bigoplus_{\mathbb{N}} S_i$. Tomemos para cada $i \in \mathbb{N}$ $A_i = \bigoplus_{j>i} S_j$. Si $0 \neq x \in \bigoplus_{\mathbb{N}} S_i$ $x = s_{i_1} + \dots + s_{i_k}$ así que $x \in \bigoplus_{i=1}^k S_i$

(reordenando si hace falta) entonces $x \notin A_{l+1}$ lo que implica que $\bigcap_{\mathbb{N}} A_i = 0$. Como M es f.c. existe una subfamilia finita $\{i_1, \dots, i_m\}$ tal que $\bigcap_{j=1}^m A_{i_j} = 0$, contradicción. Por lo tanto I es finito. \square

Definición 5.2.10. Sea M semisimple y $\{\Omega_j\}_J$ las clases de isomorfismo de submódulos simples de M . A $\sum_{S \in \Omega_j} S$ se le llama *componente homogénea* de M .

Lema 5.2.11. Sea M semisimple, $\{\Omega_j\}_J$ las clases de isomorfismo de submódulos simples de M y $B_j = \sum_{S \in \Omega_j} S$.

1. Si S es simple y $S \leq B_j$ entonces $S \in \Omega_j$.
2. $M = \bigoplus_J B_j$

Demostración. 1. Por el Lema 5.2.2.

2. Como M es suma de simples y cada simple está en algún Ω_j entonces $M = \sum_J B_j$. Sea $j_0 \in J$ y supongamos $D := B_{j_0} \cap \bigoplus_{j \neq j_0} B_j \neq 0$. Por el Lema 5.2.1 existe un simple $S \leq D$, es decir, $S \leq B_{j_0}$ y $S \leq \bigoplus_{j \neq j_0} B_j$ así que por un lado $S \in \Omega_{j_0}$ y por otro, con el Lema 5.2.2, tenemos que existe $j_1 \neq j_0$ tal que $S \in \Omega_{j_1}$. Lo que implica que $\Omega_{j_0} \cap \Omega_{j_1} \neq \emptyset$, contradicción. \square

Teorema 5.2.12. Son equivalentes para un anillo R :

- (a) ${}_R R$ es semisimple.
- (b) R_R es semisimple.

Demostración. Es suficiente demostrar sólo (a) \Rightarrow (b). Tenemos que ${}_R R = \bigoplus_{i=1}^n S_i$ con S_i simple. Por la Proposición 4.1.12 ${}_R R = \bigoplus_{i=1}^n R e_i$ con los e_i idempotentes ortogonales. Ahora $1 = e_1 + \dots + e_n$, entonces $r = e_1 r + \dots + e_n r$ para cada $r \in R$. Así que $\sum_{i=1}^n e_i R = R$. Si $e_i r_i = \sum_{j \neq i} e_j r_j$ al multiplicar por e_i , como los e_i son idempotentes ortogonales obtenemos $e_i e_i r_i = e_i r_i = 0$ por lo tanto $R = \bigoplus_{i=1}^n e_i R$.

Sea e uno de los e_i y sea $0 \neq a \in eR$, entonces $a = e r_1$ para algún $r_1 \in R$. Definimos $\varphi : Re \rightarrow Ra$ como $\varphi(re) = ra$ el cual está bien definido ya que si $se = 0$ entonces $sa = s(er_1) = (se)r_1 = 0$, además φ es un isomorfismo. Como ${}_R R$ es semisimple ${}_R R = Ra \oplus U$ para algún $U \leq R$. Sea $\psi : Ra \oplus U \rightarrow R$ como $\psi(ra + u) = \varphi^{-1}(ra)$ que es morfismo y $\psi(a) = e$. Como $\psi \in \text{End}({}_R R)$ entonces existe $b \in R$ tal que $\psi = (- \cdot b)$. Así que $e = \psi(a) = (- \cdot b)(a) = ab$ lo que implica que $e \in aR$. Entonces $eR = aR$, por lo tanto eR es simple. \square

5.3. Radical y zoclo

Teorema 5.3.1. *Sea M un R -módulo. Entonces*

1.

$$\begin{aligned} \sum_{A \ll M} A &= \bigcap \{B < M \mid B \text{ máximo}\} \\ &= \bigcap \{\text{Ker } \varphi \mid \varphi \in \text{Hom}_R(M, N) \text{ con } N \text{ semisimple}\}. \end{aligned}$$

2.

$$\begin{aligned} \bigcap_{A \leq_e M} A &= \sum \{B \leq M \mid B \text{ simple}\} \\ &= \sum \{\text{Im } \varphi \mid \varphi \in \text{Hom}_R(N, M) \text{ con } N \text{ semisimple}\}. \end{aligned}$$

Demostración. 1. Si $m \in \bigcap \{B < M \mid B \text{ máximo}\}$ entonces por el Lema 5.1.26, $Rm \ll M$ lo que implica que $m \in \sum_{A \ll M} A$. Por lo tanto

$$\bigcap \{B < M \mid B \text{ máximo}\} \subseteq \sum_{A \ll M} A.$$

Sea $B < M$, con B máximo. Entonces M/B es simple y tenemos la proyección canónica $\pi : M \rightarrow M/B$ con $B = \text{Ker } \pi$. Entonces, si denotamos π_B a la proyección canónica al cociente para cada submódulo B máximo tenemos que

$$\begin{aligned} \bigcap \{\text{Ker } \varphi \mid \varphi \in \text{Hom}_R(M, N) \text{ con } N \text{ semisimple}\} &\subseteq \bigcap \{\text{Ker } \pi_B \mid B \text{ máximo}\} \\ &= \bigcap \{B < M \mid B \text{ máximo}\}. \end{aligned}$$

Si $A \ll M$ y $\varphi : M \rightarrow N$ es un morfismo, entonces $\varphi(A) \ll N$. Si N es semisimple, el único submódulo superfluo de N es 0. Por lo tanto, si N es semisimple, entonces $\varphi(A) = 0$. Esto implica que

$$\sum_{A \ll M} A \subseteq \bigcap \{\text{Ker } \varphi \mid \varphi \in \text{Hom}_R(M, N) \text{ con } N \text{ semisimple}\}.$$

Así hemos probado 1.

2. Si $B \leq M$ con B simple y $A \leq_e M$ entonces $A \cap B = B$, lo que implica que $B \subseteq A$. Por lo tanto

$$\sum \{B \leq M \mid B \text{ simple}\} \subseteq \bigcap_{A \leq_e M} A.$$

Si $\varphi : N \rightarrow M$ es un morfismo con N semisimple entonces $\varphi(N)$ es semisimple. Por lo tanto

$$\sum \{\text{Im } \varphi \mid \varphi \in \text{Hom}_R(N, M) \text{ con } N \text{ semisimple}\} \subseteq \sum \{B \leq M \mid B \text{ simple}\}.$$

Sean $C \leq \bigcap \{A \mid A \leq_e M\}$ y C' un p.c. de C en M . Entonces $C \oplus C' \leq_e M$ así que $\bigcap \{A \mid A \leq_e M\} \subseteq C \oplus C'$. Usando el Lema 2.1.12 se tiene que

$$\bigcap_{A \leq_e M} A = \left(\bigcap_{A \leq_e M} A \right) \cap (C \oplus C') = C \oplus \left(\left(\bigcap_{A \leq_e M} A \right) \cap C \right).$$

Por lo tanto C es sumando directo de $\bigcap\{A \mid A \leq_e M\}$ lo que implica que $\bigcap\{A \mid A \leq_e M\}$ es semisimple. Por lo tanto

$$\bigcap_{A \leq_e M} A \subseteq \sum \{\text{Im } \varphi \mid \varphi \in \text{Hom}_R(N, M) \text{ con } N \text{ semisimple}\}.$$

De estas contenciones obtenemos 2. □

Definición 5.3.2. Sea M un R -módulo.

1. El submódulo dado en el Teorema 5.3.1.1 es llamado el *radical* de M y se denota $\text{Rad}(M)$.
2. El submódulo dado en el Teorema 5.3.1.2 es llamado el *zoclo* de M y se denota $\text{Zoc}(M)$.

Corolario 5.3.3. Para $m \in M$ se tiene que:

1. $Rm \ll M$ si y sólo si $m \in \text{Rad}(M)$.
2. $\text{Zoc}(M)$ es el mayor submódulo semisimple de M .

Demostración. Para 1 hay que usar la definición y la contrapositiva del Lema 5.1.26. El inciso 2 se sigue de la definición. □

Ejemplo 5.3.4. 1. Se sigue del Ejemplo 5.1.24.1 que $\text{Rad}(\mathbb{Q}) = \mathbb{Q}$. Es decir, \mathbb{Q} no tiene submódulos máximos. Por otro lado, $\text{Zoc}(\mathbb{Q}) = 0$.

2. Si consideramos el \mathbb{Z} -módulo $M = \mathbb{Z}_4$, entonces $\text{Zoc}(M) = 2\mathbb{Z}_4 = \text{Rad}(M)$.

3. Si M es un R -módulo semisimple, entonces $\text{Zoc}(M) = M$.

Proposición 5.3.5. Sea M un R -módulo. Entonces M es finitamente generado si y solo si $\text{Rad}(M) \ll M$ y $M/\text{Rad}(M)$ es f.g.

Demostración. Supongamos que M es finitamente generado. Por la Proposición 2.2.4, $M/\text{Rad}(M)$ es f.g.. Supongamos que $M = \text{Rad}(M) + A$ con $A < M$. Como M es f.g. existe un submódulo máximo C de M , tal que $A \subseteq C$. Entonces $M = \text{Rad}(M) + A \subseteq C < M$. Contradicción. Recíprocamente, considere $\{m_1 + \text{Rad}(M), \dots, m_n + \text{Rad}(M)\}$ un conjunto generador de $M/\text{Rad}(M)$. Sea $x \in M$. Si $x \notin \text{Rad}(M)$, entonces $x + \text{Rad}(M) \neq 0$. Esto implica que $x + \text{Rad}(M) = \sum_{i=1}^n r_i m_i + \text{Rad}(M)$. Así que existe $y \in \text{Rad}(M)$ tal que $x = \sum_{i=1}^n r_i m_i + y$ y por lo tanto $x \in Rm_1 + \dots + Rm_n + \text{Rad}(M)$. On the other hand, si $x \in \text{Rad}(M)$ entonces $x \in Rm_1 + \dots + Rm_n + \text{Rad}(M)$. Por lo tanto $M = Rm_1 + \dots + Rm_n + \text{Rad}(M)$. Se sigue por la hipótesis que $M = Rm_1 + \dots + Rm_n$, es decir, M es finitamente generado. □

Teorema 5.3.6. Sean M y N R -módulos.

1. Si $\varphi : M \rightarrow N$ es un morfismo, entonces:

$$I. \varphi(\text{Rad}(M)) \subseteq \text{Rad}(N)$$

$$II. \varphi(\text{Zoc}(M)) \subseteq \text{Zoc}(N)$$

2. $\text{Rad}\left(\frac{M}{\text{Rad}(M)}\right) = 0$ y para todo $C \leq M$ tal que $\text{Rad}(M/C) = 0$ se tiene que $\text{Rad}(M) \subseteq C$.

3. $\text{Zoc}(\text{Zoc}(M)) = \text{Zoc}(M)$ y para todo $C \leq M$ tal que $\text{Zoc}(C) = C$ se tiene que $C \subseteq \text{Zoc}(M)$.

Demostración. 1.I. Tenemos que $\text{Rad}(M) = \sum\{A \mid A \ll M\}$. Entonces $\varphi(\text{Rad}(M)) = \varphi(\sum\{A \mid A \ll M\}) = \sum\{\varphi(A) \mid A \ll M\}$ y como bajo morfismos, superflos van a dar a superfluos, $\text{Rad}(M) \subseteq \text{Rad}(N)$.

1.II. Es claro ya que la imagen de un semisimple es semisimple.

2. Por la Proposición 2.2.2, si $A \leq M/\text{Rad}(M)$ es un submódulo máximo entonces $A = B/\text{Rad}(M)$ con B máximo en M , así:

$$\begin{aligned} \text{Rad}\left(\frac{M}{\text{Rad}(M)}\right) &= \bigcap\{B/\text{Rad}(M) \mid B \leq M \text{ máximo}\} \\ &= \frac{\bigcap\{B \mid B \text{ máximo}\}}{\text{Rad}(M)} = \frac{\text{Rad}(M)}{\text{Rad}(M)} = 0. \end{aligned}$$

Ahora, sea $C \leq M$ tal que $\text{Rad}(M/C) = 0$. Si $\pi : M \rightarrow M/C$ es la proyección canónica, entonces $\pi(\text{Rad}(M)) \subseteq \text{Rad}(M/C) = 0$. Por lo tanto $\text{Rad}(M) \subseteq \text{Ker } \pi = C$.

3. Por el Corolario 5.3.3.2. □

Corolario 5.3.7. 1. Si $C \leq M$ entonces

I. $\text{Rad}(C) \leq \text{Rad}(M)$

II. $\text{Zoc}(C) \leq \text{Zoc}(M)$

2. Si $M = \bigoplus_I M_i$ entonces

I. $\text{Rad}(M) = \bigoplus_I \text{Rad}(M_i)$

II. $\text{Zoc}(M) = \bigoplus_I \text{Zoc}(M_i)$

III. $M/\text{Rad}(M) \cong \bigoplus_I (M_i/\text{Rad}(M_i))$

Demostración. 1 Se sigue del Teorema 5.3.6 tomando la inclusión canónica.

2.I. Para cada $i \in I$ tenemos que $\text{Rad}(M_i) \subseteq \text{Rad}(M)$, así que $\bigoplus_I \text{Rad}(M_i) \subseteq \text{Rad}(M)$. Sea $m \in \text{Rad}(M)$. Entonces m es una suma finita $\sum m_i$ con $m_i \in M_i$. Consideremos $\pi_i : M \rightarrow M_i$ las proyecciones canónicas. Como $\pi(\text{Rad}(M)) \subseteq \text{Rad}(M_i)$, cada $m_i \in \text{Rad}(M_i)$. Por lo tanto $m \in \bigoplus_I \text{Rad}(M_i)$.

2.II. Es análoga a la anterior.

2.III. Definimos el siguiente morfismo

$$\varphi : M/\text{Rad}(M) \rightarrow \bigoplus_I (M_i/\text{Rad}(M_i))$$

como $\varphi(m + \text{Rad}(M)) = \varphi(\sum m_i + \text{Rad}(M)) = \sum(m_i + \text{Rad}(M_i))$. Claramente φ es sobre. Supongamos que $\varphi(\sum m_i + \text{Rad}(M)) = 0$, es decir, $\sum(m_i + \text{Rad}(M_i)) = 0$. Entonces $m_i + \text{Rad}(M_i) = 0$ para cada $i \in I$. Por lo tanto $m_i \in \text{Rad}(M_i)$ para cada $i \in I$ y entonces $\sum m_i + \text{Rad}(M) = 0$ ya que $\text{Rad}(M_i) \subseteq \text{Rad}(M)$. □

Proposición 5.3.8. 1. Si M es semisimple entonces $\text{Rad}(M) = 0$.

2. $\text{Rad}(R)M \subseteq \text{Rad}(M)$.

3. $\text{Rad}(R)$ es un ideal bilateral.
4. Si M es f.g. entonces $\text{Rad}(M) \ll M$.
5. Si M es f.g. y $A \subseteq \text{Rad}(R)$ entonces $AM \ll M$. (Nakayama)
6. Si $0 \neq M$ es f.g. entonces $\text{Rad}(M) < M$.
7. Si $C \leq M$ entonces $\frac{C+\text{Rad}(M)}{C} \subseteq \text{Rad}(M/C)$.

Demostración. 1. Es clara por el Corolario 5.3.7.2.I.

2. Sea $m \in M$. Definimos $f_m : R \rightarrow M$ como $f_m(r) = rm$. Por el Teorema 5.3.6 $f_m(\text{Rad}(R)) \subseteq \text{Rad}(M)$. Por lo tanto

$$\text{Rad}(R)M = \sum_{m \in M} \text{Rad}(R)m \subseteq \text{Rad}(M).$$

3. Es inmediata del inciso 2.
4. Por la Proposición 5.3.5.
5. Sea $A \subseteq \text{Rad}(R)$. Entonces

$$AM \subseteq \text{Rad}(R)M \subseteq \text{Rad}(M) \ll M.$$

6. Como M es f.g. tenemos que $\text{Rad}(M) \ll M$.

7. Tomemos $\pi : M \rightarrow M/C$ la proyección canónica. Entonces $\pi(\text{Rad}(M)) = \frac{C+\text{Rad}(M)}{C} \subseteq \text{Rad}(M/C)$. \square

Observación 5.3.9. Note que en el inciso (4) de la Proposición 5.3.8 la hipótesis de que M sea f.g. es necesaria. Considere el \mathbb{Z} -módulo $\mathbb{Z} \oplus \mathbb{Q}$. Entonces

$$\text{Rad}(\mathbb{Z} \oplus \mathbb{Q}) = \text{Rad}(\mathbb{Z}) \oplus \text{Rad}(\mathbb{Q}) = 0 \oplus \mathbb{Q}$$

que no es superfluo.

Teorema 5.3.10. *Sea M un R -módulo. Entonces, M es s.s. si y solo si todo $N \leq M$ tiene suplemento en M y $\text{Rad}(M) = 0$.*

Demostración. \Rightarrow . Por la Proposición 5.3.8, $\text{Rad}(M) = 0$. En un módulo s.s. todo submódulo es sumando directo.

\Leftarrow . Sea $C \leq M$. Por hipótesis existe $B \leq M$ suplemento de C en M . Por el Lema 5.1.21, $B \cap C \ll B$ así que $B \cap C \ll M$. Tenemos que $\text{Rad}(M) = 0$, entonces $B \cap C = 0$. Por lo tanto $M = C \oplus B$. Es decir, todo submódulo es sumando directo. \square

Definición 5.3.11. Un anillo que R se llama *bueno izquierdo* si $\text{Rad}(R)M = \text{Rad}(M)$ para todo R -módulo M .

Teorema 5.3.12. *Sea R un anillo y denotemos $\bar{R} := R/\text{Rad}(R)$. Son equivalentes:*

- (a) $\text{Rad}(R)M = \text{Rad}(M)$ para todo R -módulo M .
- (b) Sea M un R -módulo. Si $\text{Rad}(R)M = 0$ entonces $\text{Rad}(M) = 0$.
- (c) $\text{Rad}(\bar{M}) = 0$ para todo \bar{R} -módulo \bar{M} .

Demostración. (a) \Rightarrow (b). Es clara.

(b) \Rightarrow (c). Sea $\bar{M} \in \bar{R}\text{-Mod}$. Consideremos el morfismo canónico de anillos $\rho : R \rightarrow \bar{R}$. Entonces \bar{M} es un R -módulo, así $\text{Rad}(R)\bar{M} = 0$ lo que implica que $\text{Rad}(\bar{R}\bar{M}) = 0$ pero $0 = \text{Rad}(\bar{R}\bar{M}) = \text{Rad}(\bar{R}\bar{M})$.

(c) \Rightarrow (a). Sea M un R -módulo y consideremos el R -módulo $\frac{M}{\text{Rad}(R)M}$. Como $\text{Rad}(R)(\frac{M}{\text{Rad}(R)M}) = 0$ entonces $\frac{M}{\text{Rad}(R)M}$ es un \bar{R} -módulo y tiene los mismos submódulos que como R -módulo. Por hipótesis, $\text{Rad}(\bar{R}\frac{M}{\text{Rad}(R)M}) = 0$ así que $\text{Rad}(R(\frac{M}{\text{Rad}(R)M})) = 0$. Por el Teorema 5.3.6.2, $\text{Rad}(M) \subseteq \text{Rad}(R)M$. \square

Lema 5.3.13. *Son equivalentes para $A \leq R$:*

1. $A \ll R$
2. $A \subseteq \text{Rad}(R)$
3. Para todo $a \in A$ se tiene que $1 - a$ tiene inverso por la izquierda.
4. Para todo $a \in A$ se tiene que $1 - a$ tiene inverso.

Demostración. 1 \Rightarrow 2. Es clara.

2 \Rightarrow 1. Por la Proposición 5.3.8.4, $\text{Rad}(R) \ll R$ y como $A \subseteq \text{Rad}(R)$ entonces $A \ll R$.

1 \Rightarrow 3. Sea $a \in A$. Entonces $r = ra + r(1 - a)$, lo que implica que $R = A + R(1 - a)$, pero $A \ll R$ así que $R = R(1 - a)$. Por lo tanto $1 - a$ tiene inverso izquierdo.

3 \Rightarrow 4. Sean $a \in A$ y $r \in R$ tal que $r(1 - a) = 1$. Entonces $r = 1 - (-ra)$. Como $-ra \in A$ existe $s \in R$ tal que $s(1 - (-ra)) = 1$, es decir, $sr = 1$. Por lo tanto r tiene inverso derecho e izquierdo, lo que implica que $s = 1 - a$. Por lo tanto r es el inverso de $1 - a$.

4 \Rightarrow 1. Supongamos que $R = A + B$. Entonces $1 = a + b$ con $a \in A$ y $b \in B$. Por hipótesis existe $r \in R$ tal que $rb = r(1 - a) = 1$ lo que implica que $1 \in B$. Por lo tanto $B = R$ y $A \ll R$. \square

Observación 5.3.14. También se tiene la versión para ideales derechos del lema anterior.

Teorema 5.3.15. *Sea R un anillo. Entonces $\text{Rad}({}_R R) = \text{Rad}(R_R)$.*

Demostración. Por la Proposición 5.3.8.4, $\text{Rad}({}_R R) \ll {}_R R$, así que por el Lema 5.3.13, para todo $a \in \text{Rad}({}_R R)$ $1 - a$ tiene inverso. Como $\text{Rad}({}_R R)$ es un ideal bilateral, por la Observación 5.3.14, $\text{Rad}({}_R R) \ll R_R$. Por lo tanto $\text{Rad}({}_R R) \subseteq \text{Rad}(R_R)$. Por simetría se tiene la igualdad. \square

Observación 5.3.16. En la literatura, el ideal $\text{Rad}(R)$ es conocido como el *radical de Jacobson* del anillo R .

Lema 5.3.17. *Sea $\varphi : R \rightarrow S$ un morfismo de anillos suprayectivo y sea ${}_S M$ un S -módulo. Entonces M es un R -módulo y los R -submódulos de M coinciden con los S -submódulos.*

Demostración. Sea ${}_S M$ un S -módulo. Sean $m \in M$ y $r \in R$, definimos $rm := \varphi(r)m$. Con esta operación M es un R -módulo. Claramente si ${}_S N \leq {}_S M$, entonces ${}_R N \leq {}_R M$. Ahora si ${}_R L \leq {}_R M$, dado $s \in S$ y $l \in L$ entonces $sl = rl \in L$ donde $r \in R$ es tal que $\varphi(r) = s$. \square

Teorema 5.3.18. Sea R un anillo tal que $\frac{R}{\text{Rad}(R)}$ es s.s. Entonces:

1. Todo simple izq. (resp. der.) es isomorfo a un submódulo izq. (resp. der.) de $\frac{R}{\text{Rad}(R)}$.
2. El número de bloques de $\frac{R}{\text{Rad}(R)}$ es finito e igual al número de clases de isomorfismo de módulos simples izq. (resp. der.).

Demostración. 1. Sea ${}_R S$ simple, entonces existe $\mathcal{M} \leq R$ ideal máximo tal que $S \cong R/\mathcal{M}$. Tenemos que $\text{Rad}(R) \subseteq \mathcal{M}$ entonces

$$S \cong \frac{R}{\mathcal{M}} \cong \frac{R/\text{Rad}(R)}{\mathcal{M}/\text{Rad}(R)}$$

Como $R/\text{Rad}(R)$ es s.s. entonces $\mathcal{M}/\text{Rad}(R)$ es sumando directo, es decir, $R/\text{Rad}(R) = (\mathcal{M}/\text{Rad}(R)) \oplus (A/\text{Rad}(R))$. Por lo tanto

$$A/\text{Rad}(R) \cong \frac{R/\text{Rad}(R)}{\mathcal{M}/\text{Rad}(R)} \cong S$$

2. Por el Lemma 5.3.17 los R -submódulos de ${}_R(\frac{R}{\text{Rad}(R)})$ coinciden con los ideales izquierdos de $R/\text{Rad}(R)$. Entonces $R/\text{Rad}(R)$ es semisimple como $\frac{R}{\text{Rad}(R)}$ -módulo. Lo que implica que los bloques de $R/\text{Rad}(R)$ son finitos. Además por (1), $R/\text{Rad}(R)$ contiene una copia de cada R -módulo simple. \square

Teorema 5.3.19. Sea R un anillo tal que $R/\text{Rad}(R)$ es s.s. Entonces para todo R -módulo M :

1. $\text{Rad}(M) = \text{Rad}(R)M$
2. $\text{Zoc}(M) = \{m \in M \mid \text{Rad}(R)m = 0\}$

Demostración. 1. Tenemos que $\text{Rad}(R)(\frac{M}{\text{Rad}(R)M}) = 0$, así que $\frac{M}{\text{Rad}(R)M}$ es un $R/\text{Rad}(R)$ -módulo. Como $R/\text{Rad}(R)$ es semisimple entonces $\frac{M}{\text{Rad}(R)M}$ es s.s. como $\frac{R}{\text{Rad}(R)}$ -módulo. Por el Lema 5.3.17 $\frac{M}{\text{Rad}(R)M}$ es s.s. como R -módulo. Por lo tanto $\text{Rad}(\frac{M}{\text{Rad}(R)M}) = 0$. Así $\text{Rad}(M) \subseteq \text{Rad}(R)M$.

2. Todo s.s. tiene radical cero y $\text{Rad}(R)M \subseteq \text{Rad}(M)$. Entonces, si $A := \{m \in M \mid \text{Rad}(R)m = 0\}$, tenemos que $\text{Zoc}(M) \subseteq A$. Por otra parte, $\text{Rad}(R)A = 0$, así que A es un $\frac{R}{\text{Rad}(R)}$ -módulo y tiene los mismos submódulos que ${}_R A$. Pero A como $\frac{R}{\text{Rad}(R)}$ -módulo es s.s. lo que implica que ${}_R A$ es s.s.. Por lo tanto $A \subseteq \text{Zoc}(M)$. \square

5.4. Ejercicios

1. Sea $p \in \mathbb{P}$ y $n > 0$. Demuestre que los submódulos de \mathbb{Z}_{p^n} forman una cadena, es decir, si $N, L \leq \mathbb{Z}_{p^n}$ entonces $N \leq L$ o $L \leq N$. Concluya que en \mathbb{Z}_{p^n} todo elemento es esencial y superfluo.
2. Considere \mathbb{Z}_2 como campo con dos elementos. Sea $R = \prod_{i>0} \mathbb{F}_i$ con $\mathbb{F}_i = \mathbb{Z}_2$ para todo $i > 0$. Demuestre que $\bigoplus_{i>0} \mathbb{F}_i$ es un ideal esencial de R .

Definición 5.4.1. Sea (L, \leq, \wedge, \vee) una retícula completa (Definición 2.3.1). Decimos que L es *inferiormente continua* si

$$a \vee \bigwedge X = \bigwedge \{a \vee x \mid x \in X\}$$

para todo conjunto codirigido (Definición 2.3.2) $X \subseteq L$.

3. Sea M un R -módulo y suponga que $Sub(M)$ es una retícula inferiormente continua. Demuestre que todo submódulo de M tiene suplemento.
4. Sea M un módulo tal que no tiene submódulos esenciales propios. Demuestre que M es semisimple.
5. Considere el diagrama

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ \varphi \downarrow & & \downarrow \beta \\ M & \xrightarrow{\psi} & N \end{array}$$

con B y M semisimples.

- a) Demuestre que si (α, φ) es el producto fibrado de (β, ψ) entonces A es semisimple.
 - b) Demuestre que si (β, ψ) es el coproducto fibrado de (α, φ) entonces N es semisimple.
6. De un ejemplo de una sucesión exacta corta

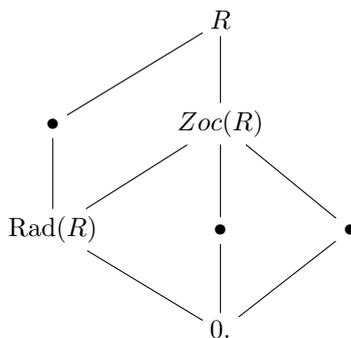
$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

tal que A y C sean semisimples pero B no.

7. Demuestre que $\prod_{p \in \mathbb{P}} \mathbb{Z}_p$ no es un \mathbb{Z} -módulo semisimple.
8. Demuestre que el ideal izquierdo $\begin{pmatrix} 0 & 0 \\ K & 0 \end{pmatrix}$ no es un sumando directo de $TI_2(K)$.
9. Demuestre que si S es un R -módulo simple, entonces $\text{Rad}(S) = 0$.
10. De un ejemplo de un R -módulo M tal que $\text{Zoc}(M/\text{Zoc}(M)) \neq 0$.
11. De un ejemplo de un R -módulo M tal que $\text{Rad}(\text{Rad}(M)) \neq \text{Rad}(M)$.
12. Sea $N \leq M$. Demuestre que $\text{Zoc}(N) = N \cap \text{Zoc}(M)$.

13. ¿Es cierto para $N \leq M$ que $\text{Rad}(N) = N \cap \text{Rad}(M)$.
14. Considere la sucesión exacta $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$. Demuestre que si $\text{Rad}(A) = A$ y $\text{Rad}(C) = C$ entonces $\text{Rad}(B) = B$.
15. Sea $\{M_i\}_I$ una familia de R -módulos. Demuestre que:
- $\text{Rad}(\prod_I M_i) \leq \prod_I \text{Rad}(M_i)$.
 - $\text{Zoc}(\prod_I M_i) \leq \prod_I \text{Zoc}(M_i)$.
16. Sea \mathbb{F}_2 el campo con dos elementos. Considere $R = \text{TI}_2(\mathbb{F}_2)$. Demuestre que
- los ideales izquierdos de R son

$$\left\{0, R, \begin{pmatrix} \mathbb{F}_2 & 0 \\ \mathbb{F}_2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ \mathbb{F}_2 & \mathbb{F}_2 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ \mathbb{F}_2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & \mathbb{F}_2 \end{pmatrix}, \left\{0, \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}\right\}\right\}.$$



- $\text{Rad}(R) = \begin{pmatrix} 0 & 0 \\ \mathbb{F}_2 & 0 \end{pmatrix}$ y $\text{Zoc}(R) = \begin{pmatrix} 0 & 0 \\ \mathbb{F}_2 & \mathbb{F}_2 \end{pmatrix}$.
- $R/\text{Rad}(R)$ es semisimple.
- R es un R -submódulo esencial en $M_2(\mathbb{F}_2)$.

Capítulo 6

Módulos Projectivos e Inyectivos

6.1. Módulos libres

Definición 6.1.1. Un subconjunto X de un R -módulo M es una *base* si

1. X genera a M , es decir, $M = \sum_{x \in X} Rx$, y
2. siempre que $r_1x_1 + \cdots + r_nx_n = 0$ con $r_i \in R$, $x_i \in X$ y $n > 0$ se tiene que $r_1 = r_2 = \cdots = r_n = 0$.

Definición 6.1.2. Un R -módulo ${}_R F$ es *libre* si tiene una base.

Proposición 6.1.3. Las siguientes condiciones son equivalentes para un módulo ${}_R F$:

- (a) F es libre;
- (b) $F = \bigoplus_I A_i$ con $A_i \cong {}_R R$ para toda $i \in I$.

Demostración. Notemos que 1 y 2 se satisfacen si $F = 0$ con \emptyset como base e $I = \emptyset$. Por convención la suma sobre el conjunto vacío es 0. Supongamos que $F \neq 0$.

$1 \Rightarrow 2$ Sea X una base de F y $a \in X$. Consideremos el R -morfismo $\varphi : R \rightarrow Ra$ dado por $\varphi(r) = ra$. Claramente φ es un epimorfismo, y por la propiedad de base $ra = 0$ implica $r = 0$. Por lo tanto φ es un isomorfismo. Como X es una base, X es un conjunto generador, es decir, $F = \sum_{a \in X} Ra$. Tomemos $a_0 \in X$ y $c \in Ra_0 \cap \sum_{a \neq a_0} Ra$. Entonces existen distintos $a_1, \dots, a_n \in X$ con $a_i \neq a_0$ y $r_0, r_1, \dots, r_n \in R$ tales que $c = r_0a_0 = \sum_{i=1}^n r_i a_i$. Así $r_0a_0 + \sum (-r_i)a_i = 0$. Como X es base, $r_0 = r_1 = \dots = r_n = 0$. Entonces $Ra_0 \cap \sum Ra = 0$ y por lo tanto $F = \bigoplus_{a \in X} Ra$.

$2 \Rightarrow 1$ Por hipótesis existe un isomorfismo $\varphi_i : R \rightarrow A_i$ para cada $i \in I$. Sea $X = \{\varphi_i(1) \mid i \in I\}$. Entonces $A_i = \varphi_i(R) = \varphi_i(R1) = R\varphi_i(1)$. Así que $F = \bigoplus_I A_i = \bigoplus_I R\varphi_i(1)$ y por lo tanto X genera. Ahora, tomemos una suma finita tal que $\sum r_i \varphi_i(1) = 0$. Como $F = \bigoplus A_i$, todo elemento de F se escribe de manera única, así que $r_i \varphi_i(1) = \varphi_i(r_i) = 0$. Esto implica que $r_i = 0$ para todo i . Por lo tanto X es una base de F . \square

Lema 6.1.4. *Sea I un conjunto. Entonces $R^{(I)}$ es un módulo libre con una base de tamaño el cardinal de I .*

Demostración. Consideremos la familia $\{A_i \mid i \in I\}$ con $A_i = R$ para toda i . Entonces $R^{(I)} = \coprod\{A_i\}_I = \bigoplus\{\widehat{A_i}\}_I$ con $R = A_i \cong \widehat{A_i}$. Por lo tanto $R^{(I)}$ es un módulo libre y tiene al conjunto $\{\eta_i(1) \mid i \in I\}$ como base, donde η_i son las inclusiones canónicas. \square

Proposición 6.1.5. *Todo módulo M es imagen epimorfica de un módulo libre. Si M es f.g. entonces M es imagen epimorfica de un módulo libre con base finita.*

Demostración. Sea Y un conjunto generador de M . Consideremos el módulo libre $R^{(Y)}$. Definimos el R -morfismo $\varphi : R^{(Y)} \rightarrow M$ como $\varphi(\eta_y(1)) = y$. Claramente φ es suprayectivo. Ahora supongamos que M es f.g. con conjunto generador $\{m_1, m_2, \dots, m_n\}$. Definimos el siguiente epimorfismo $\varphi : R^{(n)} \rightarrow M$ como $\varphi(e_i) = m_i$ para todo $1 \leq i \leq n$, where $e_i = (\delta_{ij})_{j=1}^n \in R^{(n)}$. \square

Corolario 6.1.6. *Sea R un anillo. Entonces, R es semisimple si y sólo si todo R -módulo izquierdo y derecho es semisimple.*

Demostración. Se sigue del Corolario 5.2.7 y la Proposición 6.1.5. No importa el lado que se considere por el Teorema 5.2.12. \square

Teorema 6.1.7. *Sea R un anillo y denotemos $\overline{R} := R/\text{Rad}(R)$. Son equivalentes:*

- (a) R un anillo bueno izquierdo.
- (b) Si $\varphi : M \rightarrow N$ es un R -morfismo entonces $\varphi(\text{Rad}(M)) = \text{Rad}(\varphi(M))$.
- (c) Sea M un R -módulo y $U \leq M$ entonces $\frac{\text{Rad}(M)+U}{U} = \text{Rad}(M/U)$.
- (d) Sea M un R -módulo y $U \leq M$. Si $\text{Rad}(M) = 0$ entonces $\text{Rad}(M/U) = 0$.

Demostración. (a) \Rightarrow (b). Sea $\varphi : M \rightarrow N$ un R -morfismo. Entonces

$$\varphi(\text{Rad}(M)) = \varphi(\text{Rad}(R)M) = \text{Rad}(R)\varphi(M) = \text{Rad}(\varphi(M)).$$

(b) \Rightarrow (c). Sólo hay que considerar la proyección canónica $\pi : M \rightarrow M/U$.

(c) \Rightarrow (d). Es claro.

(d) \Rightarrow (a). Sea M un R -módulo. Por la Proposición 6.1.5 existe un módulo libre F y $U \leq F$ tal que $M \cong F/U$. Por la Proposición 5.3.8.7, $\text{Rad}(F) = \text{Rad}(R)F$. Como $\text{Rad}(F/\text{Rad}(F)) = \text{Rad}(R/\text{Rad}(R)F) = 0$, por hipótesis:

$$\text{Rad} \left(\frac{\left(\frac{F}{\text{Rad}(R)F} \right)}{\left(\frac{\text{Rad}(R)F+U}{\text{Rad}(R)F} \right)} \right) = 0$$

pero

$$\frac{\left(\frac{F}{\text{Rad}(R)F} \right)}{\left(\frac{\text{Rad}(R)F+U}{\text{Rad}(R)F} \right)} \cong \frac{F}{\text{Rad}(R)F+U} \cong \frac{\left(\frac{F}{U} \right)}{\left(\frac{\text{Rad}(R)F+U}{U} \right)}.$$

Por lo tanto

$$\text{Rad} \left(\frac{\left(\frac{F}{U} \right)}{\left(\frac{\text{Rad}(R)F+U}{U} \right)} \right) = 0$$

Por el Teorema 5.3.6,

$$\text{Rad}(F/U) \subseteq \frac{\text{Rad}(R)F+U}{U} \subseteq \text{Rad}(R)(F/U).$$

Por lo tanto $\text{Rad}(R)M = \text{Rad}(M)$. \square

Teorema 6.1.8. *Si $\varphi : M \rightarrow F$ es un epimorfismo y ${}_R F$ es libre entonces φ se escinde.*

Demostración. Sea X una base de F y para cada $x \in X$ sean $m_x \in M$ los elementos tales que $\varphi(m_x) = x$. Definimos $\varphi' : F \rightarrow M$ como $\varphi'(\sum r_x x) = \sum r_x m_x$. Entonces, $\varphi\varphi'(\sum r_x x) = \varphi(\sum r_x m_x) = \sum r_x \varphi(m_x) = \sum r_x x$, i.e., $\varphi\varphi' = \text{Id}_F$. Por lo tanto $M = \text{Im } \varphi' \oplus \text{Ker } \varphi'$ por el Corolario 3.2.11.3. \square

Observación 6.1.9. Es claro por la Proposición 6.1.5 que los cocientes de módulos libres no son libres en general. De la misma manera, no siempre se tiene que submódulos de libres sean libres. Considere el anillo del Ejemplo 1.2.7.(II) y el ideal $\begin{pmatrix} 0 & 0 \\ 0 & \mathbb{R} \end{pmatrix}$ que es simple. Entonces este ideal no puede ser libre.

Recordemos que un anillo R es un *dominio* si $rs = 0$ implica que $r = 0$ o $s = 0$ para elementos $r, s \in R$. Si R es un dominio conmutativo, lo llamaremos *dominio entero*.

Proposición 6.1.10. *Sea R un dominio de ideales principales (DIP) izquierdos. Entonces todo submódulo de un módulo libre izquierdo es libre.*

Demostración. Sea F un R -módulo libre y $H \leq F$. Entonces F es de la forma $\bigoplus_K R x_k$ con $R x_k \cong R$. Supongamos que K está bien ordenado. Para cada $k \in K$ definimos $F_k = \bigoplus_{j \leq k} R x_j$ y $\overline{F}_k = \bigoplus_{j < k} R x_j$. Sea $H_k = H \cap F_k$ y $\overline{H}_k = H \cap \overline{F}_k$. Entonces $\bigcup_K F_k = F$ y $\bigcup_K H_k = H$ y además $\overline{H}_k = H \cap \overline{F}_k = H_k \cap \overline{F}_k$. Así

$$H_k / \overline{H}_k = H_k / (H_k \cap \overline{F}_k) \cong (\overline{F}_k + H_k) / \overline{F}_k \leq F_k / \overline{F}_k \cong R x_k \cong R.$$

Esto implica que H_k / \overline{H}_k es isomorfo a un ideal izquierdo de R . Como R es un DIP izquierdo, $H_k / \overline{H}_k = R \overline{h}_k$ con $\overline{h}_k \in H_k$. Como R es dominio, todo ideal de R es isomorfo a R , así que H_k / \overline{H}_k es libre. Por Teorema 6.1.8, la proyección canónica $\pi : H_k \rightarrow H_k / \overline{H}_k$ se escinde. Por lo tanto

$$H_k = \overline{H}_k \oplus R \overline{h}_k.$$

Afirmamos que $\{h_k\}_K$ es base de H . Como $F = \bigcup_K F_k$, para $h \in H$ existe $k \in K$ tal que $h \in F_k$. Sea $\mu(h)$ el menor índice l tal que $h \in F_l$ y sea H^* el subgrupo generado por $\{h_k\}_K$. Supongamos que H^* está contenido propiamente en H . Sea j el menor índice en el conjunto $\{\mu(h) \mid h \in H, h \notin H^*\}$ y sea h' tal que $\mu(h') = j$. Entonces $h' \in F_j \cap H = H_j$, así que $h' = a + r h_j$ para algún $a \in \overline{H}_k$, $r \in R$ y $a \in H$. Notemos que $a \notin H^*$. Como $a \in \overline{H}_j = H \cap \overline{F}_j$ entonces $a \in \overline{F}_j$, lo que implica que $a \in F_t$ para algún $t < j$. Por lo tanto $\mu(a) < j$ lo

que es una contradicción. Así $H = H^*$. Ahora, si $r_1 h_{k_1} + \dots + r_n h_{k_n} = 0$ con $k_1 < \dots < k_n$, entonces $r_n h_{k_n} \in Rh_{k_n} \cap \overline{H_{k_n}} = \{0\}$ lo que implica que $r_n = 0$. Haciendo esto para cada r_i , obtenemos que $\{h_k\}_K$ es base de H . \square

Proposición 6.1.11. *Si A_S es libre con base $\{x_\alpha\}_\Lambda$ entonces todo elemento de $A \otimes_S U$ se representa como una suma finita $\sum x_\alpha \otimes u_\alpha$ donde cada u_α está totalmente determinado.*

Demostración. Si A_S es libre con base $\{x_\alpha\}_\Lambda$ entonces $A = \bigoplus_\Lambda x_\alpha S$ con $x_\alpha S \cong S$. Por el Teorema 4.3.14 y la Proposición 4.3.17 se tiene que

$$\begin{aligned} A \otimes_S U &\cong \left(\bigoplus_\Lambda x_\alpha S \right) \otimes_S U \cong \bigoplus_\Lambda (x_\alpha S \otimes U) \\ &\cong \bigoplus_\Lambda (S \otimes_S U) \cong \bigoplus_\Lambda U. \end{aligned}$$

Si $a \in A$ entonces $a = \sum x_\alpha s_\alpha$ (una suma finita), así

$$\begin{aligned} \sum a_i \otimes u_i &= \sum \left(\sum x_{\alpha_i} s_{\alpha_i} \right) \otimes u_i = \sum \sum (x_{\alpha_i} s_{\alpha_i}) \otimes u_i \\ &= \sum \sum x_{\alpha_i} \otimes s_{\alpha_i} u_i = \sum x_\alpha \otimes u_\alpha \end{aligned}$$

Sea $a = \sum x_\alpha s_\alpha$ la representación de a en la base. Definimos la siguiente función S tensorial $A \times U \rightarrow U$ como: fijemos $\beta \in \Lambda$

$$(a, u) \mapsto \begin{cases} s_\beta u & \text{Si } \beta \text{ aparece en la representación de } a. \\ 0 & \text{En otro caso.} \end{cases}$$

Entonces existe un único morfismo $A \otimes_S U \rightarrow U$ definido como

$$\sum x_\alpha \otimes u_\alpha \mapsto \begin{cases} u_\beta & \text{Si } x_\beta \text{ aparece en la suma } \sum x_\alpha \otimes u_\alpha \\ 0 & \text{En otro caso.} \end{cases}$$

Como la imagen de este morfismo está únicamente determinada, se sigue la unicidad de los u_α . \square

Corolario 6.1.12. *Sea S un anillo conmutativo. Sean A_S un módulo libre con base x_1, \dots, x_m y ${}_S U$ un módulo libre con base z_1, \dots, z_n . Entonces $A \otimes_S U$ es un S -módulo libre con base $\{x_i \otimes z_j\}$.*

Demostración. Por la Proposición 6.1.11 cada elemento de $A \otimes_S U$ es de la forma $\sum x_i \otimes u_i$ donde los u_i están totalmente determinados. Esto implica que si $u_i = \sum s_{ij} z_{ij}$ entonces los s_{ij} están únicamente determinados. Por lo tanto los coeficientes de la representación

$$\sum x_i \otimes u_i = \sum x_i \otimes \left(\sum s_{ij} z_{ij} \right) = \sum \sum s_{ij} (x_i \otimes z_j)$$

son únicos. \square

Para terminar esta sección, a continuación damos un ejemplo de un ejemplo de un anillo R , tal que $R \cong R \oplus R$ como R -módulos. Es decir, en este anillo, las bases de un módulo libre no tienen porque tener la misma cardinalidad.

Ejemplo 6.1.13. Sea K un campo y ${}_K V$ un espacio vectorial de dimensión infinita (numerable). Sea $R = \text{End}_K(V)$. Fijemos una base $\{v_1, v_2, \dots, v_n, \dots\}$ de V . Consideremos los siguientes R -morfismos $\Theta_1, \Theta_2 : R \rightarrow R$ definidos como: Sea $\varphi, \psi \in R$,

$$\Theta_1(\varphi)(v_i) = \begin{cases} \varphi(v_n) & \text{si } i = 2n - 1 \\ 0 & \text{si } i = 2n \end{cases} \quad \Theta_2(\psi)(v_i) = \begin{cases} \psi(v_n) & \text{si } i = 2n \\ 0 & \text{si } i = 2n - 1 \end{cases}$$

Por la propiedad universal de la suma directa, existe un único R -morfismo $\Theta : R \oplus R \rightarrow R$ definido como $\Theta(\varphi, \psi) = \Theta_1(\varphi) + \Theta_2(\psi)$. Supongamos que $\Theta(\varphi, \psi) = 0$, es decir, $\Theta_1(\varphi) + \Theta_2(\psi) = 0$. Sea v_i un básico. Entonces $\varphi(v_i) = \Theta_1(\varphi)(v_{2i-1})$ y $\psi(v_i) = \Theta_2(\psi)(v_{2i})$. Por lo tanto

$$\varphi(v_i) = \Theta_1(\varphi)(v_{2i-1}) + 0 = \Theta_1(\varphi)(v_{2i-1}) + \Theta_2(\psi)(v_{2i-1}) = (\Theta_1(\varphi) + \Theta_2(\psi))(v_{2i-1}) = 0$$

$$\psi(v_i) = 0 + \Theta_2(\psi)(v_{2i}) = \Theta_1(\varphi)(v_{2i}) + \Theta_2(\psi)(v_{2i}) = (\Theta_1(\varphi) + \Theta_2(\psi))(v_{2i}) = 0.$$

Esto implica que $\varphi = 0 = \psi$. Por lo tanto Θ es inyectiva. Ahora sea $\alpha \in R$. Definimos $\varphi : R \rightarrow R$ como $\varphi(v_i) = \alpha(v_{2i-1})$ y definimos $\psi : R \rightarrow R$ como $\psi(v_i) = \alpha(v_{2i})$. Entonces $\Theta(\varphi, \psi) = \alpha$, es decir, Θ es suprayectiva. Por lo tanto $R \cong R \oplus R$.

6.2. Módulos Inyectivos y Projectivos

Definición 6.2.1. Se dice que un módulo ${}_R Q$ es *inyectivo* si para todo monomorfismo $\alpha : A \rightarrow B$ y para todo R -morfismo $\varphi : A \rightarrow Q$ existe un R -morfismo $\kappa : B \rightarrow Q$ tal que $\varphi = \kappa\alpha$.

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ \varphi \downarrow & \swarrow \kappa & \\ & & Q \end{array}$$

Teorema 6.2.2. Las siguientes condiciones son equivalentes para un módulo ${}_R Q$:

- (a) Q es inyectivo
- (b) Todo monomorfismo $\xi : Q \rightarrow B$ se escinde.

Demostración. 1. (a) \Rightarrow (b). Sea $\xi : Q \rightarrow B$ un monomorfismo. Considere Id_Q . Como Q es inyectivo, existe $\kappa : B \rightarrow Q$ tal que $\kappa\xi = Id_Q$. Se sigue que ξ se escinde por el Corolario 3.2.12.

(b) \Rightarrow (a). Sea (ψ, β) el coproducto fibrado de (α, φ) . Por el Teorema 4.2.5.(1), ψ es un monomorfismo. Por hipótesis ψ se escinde. Así que por el Teorema 4.2.5.(2) existe $\kappa : B \rightarrow Q$ tal que $\varphi = \kappa\alpha$. \square

Corolario 6.2.3. Sea Q un R -módulo y $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$ una sucesión exacta corta. Entonces la sucesión

$$0 \rightarrow \text{Hom}_R(C, Q) \xrightarrow{g^*} \text{Hom}_R(B, Q) \xrightarrow{f^*} \text{Hom}_R(A, Q) \rightarrow 0$$

es exacta.

Demostración. \Rightarrow Por el Proposición 3.4.12, basta probar que f^* es suprayectiva. Sea $\varphi : A \rightarrow Q$ cualquier R -morfismo. Como f es inyectivo y Q es un módulo inyectivo, existe $\kappa : B \rightarrow Q$ tal que $\varphi = \kappa f = f^*(\kappa)$. Es decir, f^* es suprayectiva.

\Leftarrow Sea $\varphi : A \rightarrow Q$ un R -morfismo y $f : A \rightarrow B$ un monomorfismo. Tenemos una sucesión exacta corta $0 \rightarrow A \rightarrow B \rightarrow \text{Coker } f \rightarrow 0$. Por hipótesis, $\text{Hom}_R(B, Q) \xrightarrow{f^*} \text{Hom}_R(A, Q)$ es suprayectiva. Entonces, para $\varphi \in \text{Hom}_R(A, Q)$ existe $\kappa \in \text{Hom}_R(B, Q)$ tal que $\varphi = f^*(\kappa) = \kappa f$. Por lo tanto, Q es inyectivo. \square

Definición 6.2.4. Se dice que un módulo ${}_R P$ es *projectivo* si para todo epimorfismo $\psi : B \rightarrow C$ y para todo R -morfismo $\beta : P \rightarrow C$ existe un R -morfismo $\lambda : P \rightarrow B$ tal que $\beta = \psi\lambda$.

$$\begin{array}{ccc} & & P \\ & \swarrow \lambda & \downarrow \beta \\ B & \xrightarrow{\psi} & C \end{array}$$

Teorema 6.2.5. *Las siguientes condiciones son equivalentes para un módulo ${}_R P$:*

- (a) P es proyectivo.
- (b) Todo epimorfismo $\xi : B \rightarrow P$ se escinde.

Demostración. (a) \Rightarrow (b). Sea $\xi : B \rightarrow P$ un epimorfismo. Considere Id_P . Como P es proyectivo, existe $\lambda : P \rightarrow B$ tal que $Id_P = \xi\lambda$. Por el Corolario 3.2.13, ξ se escinde.

(b) \Rightarrow (a). Tomemos el producto fibrado (φ, α) de (ψ, β) . Por el Teorema 4.2.6.(1), α es un epimorfismo. Por hipótesis α se escinde, lo que implica que existe $\lambda : P \rightarrow B$ tal que $\beta = \psi\lambda$ por el Teorema 4.2.6.(2). \square

Corolario 6.2.6. *Sea P un R -módulo y $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$ una sucesión exacta corta. Entonces Q es inyectivo si y solo si la sucesión*

$$0 \rightarrow \text{Hom}_R(P, A) \xrightarrow{f_*} \text{Hom}_R(P, B) \xrightarrow{g_*} \text{Hom}_R(P, C) \rightarrow 0$$

es exacta.

Demostración. \Rightarrow Por la Proposición 3.4.13, basta ver que g_* es suprayectiva. Sea $\beta \in \text{Hom}_R(P, C)$. Como g es suprayectiva y P es proyectivo, existe $\lambda : P \rightarrow B$ tal que $\beta = g\lambda = g_*(\lambda)$.

\Leftarrow Sea $g : B \rightarrow C$ un epimorfismo y $\beta : P \rightarrow C$ cualquier R -morfismo. Tenemos la sucesión exacta corta $0 \rightarrow \text{Ker } g \rightarrow B \rightarrow C \rightarrow 0$. Por hipótesis $g_* : \text{Hom}_R(P, B) \rightarrow \text{Hom}_R(P, C)$ es suprayectiva, así que existe $\lambda : P \rightarrow B$ tal que $\beta = g_*(\lambda) = g\lambda$. Por lo tanto P es proyectivo. \square

Proposición 6.2.7. *Las siguientes condiciones son equivalentes para un anillo R :*

- (a) R es semisimple.
- (b) Todo R -módulo izquierdo (resp. derecho) es inyectivo.
- (c) Todo R -módulo izquierdo (resp. derecho) es proyectivo.
- (d) Todo R -módulo simple (resp. derecho) es proyectivo.

Demostración. (a) \Rightarrow (b) y (c). Si R es semisimple entonces todo R -módulo es semisimple por el Corolario 6.1.6. Entonces todo monomorfismo y todo epimorfismo se escinde.

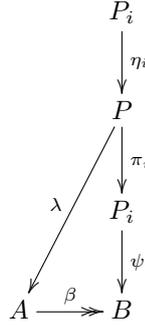
(b) y (c) \Rightarrow (a). Si $I \leq R$, entonces la inclusión se escinde por (b), es decir, I es sumando directo de R . Análogamente, si todo módulo es proyectivo la proyección canónica $R \rightarrow R/I$ se escinde, es decir, I es sumando directo de R . Por lo tanto R es semisimple.

(c) \Rightarrow (d) Es clara.

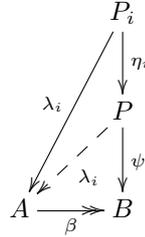
(d) \Rightarrow (a) Sea $\text{Zoc}(R) := \sum S_i$ con $S_i \leq R$, S_i simple. Si $\text{Zoc}(R) < R$, como R es f.g. entonces existe $\mathcal{M} \leq R$ máximo tal que $\text{Zoc}(R) \subseteq \mathcal{M}$. Como R/\mathcal{M} es simple y cada simple es proyectivo entonces la proyección canónica $\pi : R \rightarrow R/\mathcal{M}$ se escinde, es decir, $R = A \oplus \mathcal{M}$ con $A \cong R/\mathcal{M}$ simple. Contradicción ya que $\text{Zoc}(R)$ es la suma de todos los simples de R y $\text{Zoc}(R) \subseteq \mathcal{M}$. \square

Proposición 6.2.8. Sea $P = \bigoplus_I P_i$. Entonces P es proyectivo si y solo si cada P_i es proyectivo.

Demostración. \Rightarrow . Sea $\beta : A \rightarrow B$ un epimorfismo y $\psi : P_i \rightarrow B$. Como P es proyectivo, existe $\lambda : P \rightarrow A$ tal que $\beta\lambda = \psi\pi_i$ donde $\pi_i : P \rightarrow P_i$ es la proyección canónica. Sea $\eta_i : P_i \rightarrow \bigoplus_I P_i$ la inclusión canónica. Entonces $\beta\lambda\eta_i = \psi\pi_i\eta_i = \psi Id_{P_i} = \psi$.



\Leftarrow . Sean $\beta : A \rightarrow B$ un epimorfismo y $\psi : P \rightarrow B$. Como P_i es proyectivo para cada $i \in I$, existen morfismos $\lambda_i : P_i \rightarrow A$ tales que $\beta\lambda_i = \psi\eta_i$ donde η_i son las inclusiones canónicas de la suma directa. Por el Teorema 4.1.4, la familia $\{\lambda_i\}$ define un único morfismo $\lambda : P \rightarrow A$ tal que $\lambda\eta_i = \lambda_i$ para todo $i \in I$. Notemos que para cada $i \in I$, $\beta\lambda\eta_i = \psi\eta_i$. Por la unicidad que da el Teorema 4.1.4 tenemos que $\beta\lambda = \psi$.



□

En general el producto de módulos proyectivos no es proyectivo como lo muestra el siguiente ejemplo tomado del libro “Lectures on modules and rings” escrito por T.Y. Lam.

Lema 6.2.9. Sea $P = \mathbb{Z}^{(\mathbb{N})}$ y $M = \mathbb{Z}^{\mathbb{N}}$. Entonces $\text{Hom}_{\mathbb{Z}}(M/P, \mathbb{Z}) = 0$.

Demostración. Sea $\varphi \in \text{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$ tal que $\varphi(P) = 0$. Consideremos los siguientes dos subgrupos de M

$$A = \{(2a_1, 2^2a_2, \dots, 2^n a_n, \dots) \mid a_i \in \mathbb{Z}\}$$

$$B = \{(3b_1, 3^2b_2, \dots, 3^n b_n, \dots) \mid b_i \in \mathbb{Z}\}$$

Entonces $A + B = M$. Notemos que cada elemento de A se puede escribir de la forma

$$(2a_1, 2^2a_2, \dots, 2^{n-1}a_{n-1}, 0, 0, \dots) + 2^n x$$

para algún elemento $x \in M$. Como $\varphi(P) = 0$, $\varphi(A) \subseteq 2^n \mathbb{Z}$ para todo $n > 0$, es decir, $\varphi(A) \subseteq \bigcap_{n>0} 2^n \mathbb{Z} = 0$. Análogamente, $\varphi(B) = 0$. Por lo tanto $\varphi(M) = 0$. \square

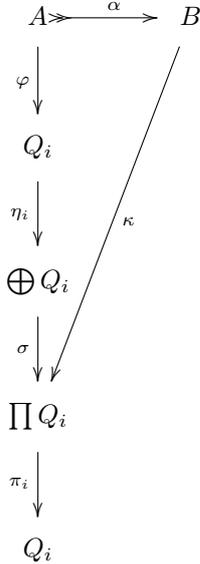
Proposición 6.2.10. *El \mathbb{Z} -módulo $\mathbb{Z}^{\mathbb{N}}$ no es proyectivo.*

Demostración. Supongamos que $M = \mathbb{Z}^{\mathbb{N}}$ es proyectivo. Entonces existe un \mathbb{Z} -módulo libre F con base $\{e_i \mid i \in I\}$ tal que $M \leq F$ (Teorema 6.2.13). Como $P = \mathbb{Z}^{(\mathbb{N})}$ es numerable, podemos descomponer el conjunto I en una unión ajena $I_1 \cup I_2$ con I_1 numerable y que además $P \subseteq \sum_{I_1} \mathbb{Z}e_i = F_1$. Notemos que M no está contenido en F_1 porque F_1 es numerable y M no lo es. Ahora, es posible tomar una proyección $\pi_i : F \rightarrow \mathbb{Z}e_i$ con $i \in I_2$ de tal manera que $\pi_i(M) \neq 0$ y $\pi_i(F_1) = 0$. Así, obtenemos un morfismo no cero $\varphi : M \rightarrow \mathbb{Z}$ tal que $\varphi(P) = 0$, contradiciendo el lema anterior. \square

Proposición 6.2.11. *Sea $Q = \prod_I Q_i$. Entonces, Q es inyectivo si y sólo si Q_i es inyectivo para todo $i \in I$.*

Demostración. \Rightarrow . Sean $\alpha : A \rightarrow B$ un monomorfismo y $\varphi : A \rightarrow Q_i$ un R -morfismo. Consideremos $\eta_i : Q_i \rightarrow \bigoplus Q_i$ la inclusión canónica, σ la inclusión de la suma directa en el producto y $\pi_i : \prod_I Q_i \rightarrow Q_i$ la proyección canónica. Como Q es inyectivo existe $\kappa : B \rightarrow Q$ tal que $\kappa\alpha = \sigma\eta_i\varphi$.

Entonces $\pi_i\kappa$ es el morfismo requerido ya que $\pi_i\kappa\alpha = \pi_i\sigma\eta_i\varphi = Id_{Q_i}\varphi = \varphi$.



\Leftarrow . Sea $\alpha : A \rightarrow B$ un monomorfismo y $\varphi : A \rightarrow Q$ un R -morfismo. Como Q_i es inyectivo para cada $i \in I$, existen morfismos $\kappa_i : B \rightarrow Q_i$ tales que $\kappa_i\alpha = \pi_i\varphi$ para toda $i \in I$, donde π_i son las proyecciones canónicas. Por el Teorema 4.1.3 tenemos que la familia de morfismos $\{\kappa_i\}$ definen un único morfismo $\kappa : B \rightarrow Q$ tal que $\pi_i\kappa = \kappa_i$. Entonces $\pi_i\kappa\alpha = \pi_i\varphi$ y por la unicidad de κ se tiene que $\kappa\alpha = \varphi$.

$$\begin{array}{ccc}
 A & \xrightarrow{\alpha} & B \\
 \varphi \downarrow & \swarrow \kappa & \\
 Q & & \\
 \pi_i \downarrow & \searrow \kappa_i & \\
 Q_i & &
 \end{array}$$

□

Ejemplo 6.2.12. Sea $R = \prod_{\mathbb{N}} K_i$ un producto directo de campos. Se sigue de los ejercicios 6.3.12 y 6.3.16 que todo R -módulo simple es inyectivo. No es difícil ver que cada K_i como ideal de R es un R -módulo simple. Sea $0 \neq (k_i)_{\mathbb{N}} \in R$ cualquier elemento. Entonces existe $i > 0$ tal que $k_i \neq 0$. Sea $e_i \in R$ el elemento tal que $e_i(j) = 0$ si $i \neq j$ y $e_i(i) = 1$. Entonces $0 \neq e_i(k_i)_{\mathbb{N}} \in \bigoplus_{\mathbb{N}} K_i$. Por la Proposición 5.1.5, $\bigoplus_{\mathbb{N}} K_i \leq_e R$. Es claro que $\bigoplus_{\mathbb{N}} K_i \neq R$. Por lo tanto $\bigoplus_{\mathbb{N}} K_i$ no puede ser un R -módulo inyectivo.

Teorema 6.2.13. *Un módulo es proyectivo si y solo si es isomorfo a un sumando directo de un módulo libre.*

Demostración. \Rightarrow . Sea P proyectivo. Por el Corolario 6.1.5, existe F libre y un epimorfismo $\alpha : F \rightarrow P$. Como P es proyectivo, α se escinde, es decir, $F = \text{Ker } \alpha \oplus K$. Pero $K \cong \text{Im } \alpha = P$, por lo tanto P es isomorfo a un sumando directo de un libre.

\Leftarrow . Por el Teorema 6.1.8, si F es libre entonces F es proyectivo. Por lo tanto, si P es isomorfo a un sumando directo de F , entonces por la Proposición 6.2.8, P es proyectivo. □

Corolario 6.2.14. *Sea R un DIP izquierdo. Entonces un R -módulo P es proyectivo si y solo si es libre.*

Demostración. \Rightarrow . Sea P proyectivo. Por el Teorema 6.2.13 P es isomorfo a un sumando directo de un libre, en particular es isomorfo a un submódulo de un libre. Usando la Proposición 6.1.10, tenemos que P es libre.

\Leftarrow . Todo libre es proyectivo. □

Teorema 6.2.15 (de la Base Dual). *Las siguientes condiciones son equivalentes para un módulo P :*

- (a) P es proyectivo.
- (b) Para toda familia $\{y_i\}_I$ de generadores de P , existe una familia de morfismos $\varphi_i \in \text{Hom}_R(P, R)$ tales que:
 - (1) Para todo $p \in P$, $\varphi_i(p) \neq 0$ sólo para un número finito de índices de I .
 - (2) Para todo $p \in P$, $p = \sum_I \varphi_i(p)y_i$

(c) Existe una familia $\{y_i\}_I$ de elementos de P y existe una familia $\{\varphi_i\}_I$ de elementos de $\text{Hom}_R(P, R)$ que satisfacen (1) y (2) del inciso (b).

Demostración. (a) \Rightarrow (b). Tenemos que existe $F = \bigoplus_I Rx_i$ libre y un epimorfismo $\xi : \bigoplus_I Rx_i \rightarrow P$ dado por $\xi(\sum r_i x_i) = \sum r_i y_i$. Como P es proyectivo existe $\lambda : P \rightarrow \bigoplus_I Rx_i$ tal que $\xi\lambda = \text{Id}_P$. Sea $\pi_i : \bigoplus_I Rx_i \rightarrow Rx_i \cong R$ la proyección canónica. Ahora si $a \in \bigoplus_I Rx_i$, entonces $a = \sum \pi_i(a)x_i$. Así que para cada $p \in P$,

$$p = \xi\lambda(p) = \xi\left(\sum \pi_i(\lambda(p))x_i\right) = \sum \pi_i(\lambda(p))\xi(x_i) = \sum \pi_i(\lambda(p))y_i.$$

Tomando $\varphi_i = \pi_i\lambda$ se tiene que $p = \sum \varphi_i(p)y_i$.

(b) \Rightarrow (c). Es claro.

(c) \Rightarrow (a). La condición (2) nos dice que $\{y_i\}_I$ es un conjunto generador de P . Sea $F = \bigoplus_I Rx_i$ donde $Rx_i \cong R$ para cada $i \in I$ y $\xi : F \rightarrow P$ el epimorfismo dado por $\xi(x_i) = y_i$. Usando (1) definimos $\tau : P \rightarrow F$ como $\tau(p) = \sum_I \varphi_i(p)x_i$. Entonces $\xi\tau(p) = \xi(\sum_I \varphi_i(p)x_i) = \sum_I \varphi_i(p)y_i = p$. Por lo tanto ξ se escinde, así que $F = \text{Ker } \xi \oplus \text{Im } \tau$. Como ξ es suprayectiva, $P \cong \text{Im } \tau$ y por lo tanto P es un sumando directo de un libre. Lo que implica que P es proyectivo. \square

Teorema 6.2.16 (Criterio de Baer). *Un R -módulo Q es inyectivo si y sólo si para todo $I \leq R$ ideal izq. y todo R -morfismo $\varphi : I \rightarrow Q$ existe $\eta : R \rightarrow Q$ tal que $\eta i = \varphi$, donde $i : I \rightarrow R$ es la inclusión canónica.*

Demostración. Sea $\alpha : A \rightarrow B$ un monomorfismo y $\psi : A \rightarrow Q$ un morfismo. Consideremos el conjunto $\Gamma = \{(C, \gamma) \mid C \leq B, \gamma : C \rightarrow Q \text{ tal que } \gamma\alpha = \psi\}$. Se tiene que $\Gamma \neq \emptyset$ ya que $(\text{Im } \alpha, \alpha_0) \in \Gamma$ con $\alpha_0 = \alpha$ correstringida a su imagen, que es un isomorfismo. Además Γ es un COPO, donde el orden está dado de la siguiente manera: $(C, \gamma) \leq (D, \eta)$ si y sólo si $C \leq D$ y $\eta|_C = \gamma$. Por el Lema de Zorn, Γ tiene máximos. Sea (C, γ) un máximo en Γ . Supongamos que existe $0 \neq b \in B - C$ y tomemos $C + Rb$. Si $C \cap Rb = 0$ se contradiría la maximalidad de (C, γ) ya que φ se podría extender a $C \oplus Rb$. Supongamos que $C \cap Rb \neq 0$ y consideremos $(C : b) = \{r \in R \mid rb \in C\} \leq R$ que es distinto de cero. Entonces tenemos un R -morfismo $(\cdot \cdot b) : (C : b) \rightarrow C$ dado por $(\cdot \cdot b)(r) = rb$. Por hipótesis existe $\tau : R \rightarrow Q$ tal que $\tau i = \gamma(\cdot \cdot b)$. Definimos $\gamma_1 : C + Rb \rightarrow Q$ como $\gamma_1(c + rb) = \gamma(c) + \tau(r)$. Notemos que $\gamma_1|_C = \gamma$. Entonces $(C + Rb, \gamma_1) \in \Gamma$ pero $(C, \gamma) < (C + Rb, \gamma_1)$ lo que es una contradicción. Por lo tanto $C = B$ y Q es inyectivo. El regreso es obvio. \square

Definición 6.2.17. Decimos que un grupo abeliano A es *divisible* si $zA = A$ para todo $0 \neq z \in \mathbb{Z}$.

Ejemplo 6.2.18. El \mathbb{Z} -módulo \mathbb{Q} es divisible, ya que si $0 \neq z \in \mathbb{Z}$ y $q \in \mathbb{Q}$, entonces $z(\frac{q}{z}) = q$. Por lo tanto $z\mathbb{Q} = \mathbb{Q}$.

Proposición 6.2.19. *La clase de los grupos divisibles es cerrada bajo imágenes homomorfas, bajo sumas directas y bajo productos.*

Demostración. Supongamos que ${}_Z D$ es divisible y $\varphi : D \rightarrow G$ es un homomorfismo. Entonces $z \text{Im } \varphi = z\varphi(D) = \varphi(zD) = \varphi(D) = \text{Im } \varphi$ para todo $0 \neq z \in \mathbb{Z}$. En particular las copias isomorfas de un divisible son divisibles.

Ahora, si $\{D_i\}_I$ es una familia de grupos divisibles entonces $z \prod_I D_i = \prod_I zD_i = \prod_I D_i$. De la misma forma $z \bigoplus_I D_i = \bigoplus_I zD_i = \bigoplus_I D_i$. \square

Teorema 6.2.20. *Todo grupo abeliano se inyecta en un grupo divisible.*

Demostración. Sea A un grupo abeliano. Sabemos que existe un grupo abeliano libre ${}_{\mathbb{Z}}F$ y un epimorfismo $\varphi : F \rightarrow A$ (Corolario 6.1.5). Entonces $F \cong \mathbb{Z}^{(I)}$ p.a. conjunto I . Consideremos ${}_{\mathbb{Z}}\mathbb{Q}$ que es divisible y como $\mathbb{Z} \hookrightarrow \mathbb{Q}$, tenemos un monomorfismo $i : \mathbb{Z}^{(I)} \hookrightarrow \mathbb{Q}^{(I)}$. Entonces hay un monomorfismo $\mathbb{Z}^{(I)} / \text{Ker } \varphi \hookrightarrow \mathbb{Q}^{(I)} / i(\text{Ker } \varphi)$ donde $\mathbb{Q}^{(I)} / i(\text{Ker } \varphi)$ es divisible. Por lo tanto A se sumerge en un divisible. \square

Teorema 6.2.21. *Un \mathbb{Z} -módulo es inyectivo si y sólo si es divisible.*

Demostración. \Rightarrow . Supongamos que ${}_{\mathbb{Z}}Q$ es inyectivo. Sean $0 \neq z_0 \in \mathbb{Z}$, $q_0 \in Q$ e $i : \mathbb{Z}z_0 \rightarrow \mathbb{Z}$ la inclusión canónica. Definimos $\varphi : \mathbb{Z}z_0 \rightarrow Q$ como $\varphi(nz_0) = nq_0$ que es un \mathbb{Z} -morfismo. Como Q es inyectivo, existe $\kappa : \mathbb{Z} \rightarrow Q$ tal que $\kappa i = \varphi$. Así que $z_0 \kappa(1) = \kappa(z_0) = \varphi(z_0) = q_0$. Por lo tanto $z_0 Q = Q$, lo que implica que Q es divisible.

\Leftarrow . Sea ${}_{\mathbb{Z}}D$ divisible y $\varphi : \mathbb{Z}n \rightarrow D$ un \mathbb{Z} -morfismo. Como D es divisible, para $\varphi(n) \in D$ y $n \in \mathbb{Z}$ existe $d' \in D$ tal que $nd' = \varphi(n)$. Entonces, definimos $\kappa : R \rightarrow D$ como $\kappa(m) = md'$. Así, $\kappa(tn) = tnd' = t\varphi(n) = \varphi(tn)$ para todo $tn \in \mathbb{Z}n$. Por el criterio de Baer (Teorema 6.2.16), D es inyectivo. \square

Observación 6.2.22. El concepto de módulo divisible puede ser dado para módulos sobre un dominio entero. En este caso, la Proposición 6.2.19 y la Proposición 6.2.20 permanecen ciertas (usando el Ejercicio 6.3.6). Para un dominio entero en general solo tenemos que inyectivo implica divisible. Si el dominio entero es de ideales principales, entonces obtenemos el Teorema 6.2.21.

Lema 6.2.23. *Sea R un anillo. Si ${}_{\mathbb{Z}}D$ es divisible, entonces el R -módulo izquierdo $\text{Hom}_{\mathbb{Z}}(R_R, D)$ es inyectivo.*

Demostración. Sean $\alpha : A \rightarrow B$ un R -monomorfismo y $\varphi : A \rightarrow \text{Hom}_{\mathbb{Z}}(R_R, D)$ cualquier R -morfismo. Definimos $\sigma : \text{Hom}_{\mathbb{Z}}(R_R, D) \rightarrow D$ como $\sigma(f) = f(1)$, el cual es un \mathbb{Z} -morfismo. Así que tenemos un \mathbb{Z} -morfismo $\sigma\varphi : A \rightarrow D$. Por lo tanto existe un \mathbb{Z} -morfismo $\tau : B \rightarrow D$ tal que $\tau\alpha = \sigma\varphi$.

Definimos $\kappa : B \rightarrow \text{Hom}_{\mathbb{Z}}(R_R, D)$ como $\kappa(b)(r) = \tau(rb)$ el cual es un R -morfismo. Entonces

$$\kappa\alpha(a)(r) = \tau(r\alpha(a)) = \tau(\alpha(ra)) = \sigma\varphi(ra) = \varphi(ra)(1) = r\varphi(a)(1) = \varphi(a)(r).$$

Por lo tanto $\kappa\alpha = \varphi$, lo que implica que $\text{Hom}_{\mathbb{Z}}(R_R, D)$ es inyectivo.

$$\begin{array}{ccc} {}_R A & \xrightarrow{\alpha} & {}_R B \\ \varphi \downarrow & \swarrow \kappa & \\ \text{Hom}_{\mathbb{Z}}({}_R R, {}_{\mathbb{Z}} D) & & \\ \sigma \downarrow & \swarrow \tau & \\ {}_{\mathbb{Z}} D & & \end{array}$$

\square

Teorema 6.2.24. *Para todo R -módulo M existe un monomorfismo $\varphi : M \rightarrow Q$ con Q un R -módulo inyectivo.*

Demostración. Sea M un R -módulo. Visto M como grupo abeliano existe un monomorfismo $\mu : {}_{\mathbb{Z}}M \rightarrow {}_{\mathbb{Z}}D$ con D divisible por el Teorema 6.2.20. Definimos $\rho : {}_R M \rightarrow {}_R \text{Hom}_{\mathbb{Z}}(R, D)$ como $\rho(m)(r) = \mu(rm)$ que es un R -morfismo. Además si $\rho(m) = 0$, entonces $\rho(m)(r) = 0$ para todo $r \in R$. Así $\mu(rm) = 0$ para todo $r \in R$, en particular $\mu(m) = 0$ pero μ es monomorfismo lo que implica que $m = 0$. Por lo tanto ρ es un monomorfismo. \square

Corolario 6.2.25. *Un módulo ${}_R Q$ es inyectivo si y sólo si Q es isomorfo a un sumando directo de $\text{Hom}_{\mathbb{Z}}(R, D)$ para algún ${}_{\mathbb{Z}}D$ divisible.*

Demostración. \Rightarrow . Por el Teorema 6.2.24 existe un monomorfismo de Q en $\text{Hom}_{\mathbb{Z}}(R, D)$ para algún ${}_{\mathbb{Z}}D$ divisible y este monomorfismo se escinde porque Q es inyectivo. Por lo tanto Q es isomorfo a un sumando directo de $\text{Hom}_{\mathbb{Z}}(R, D)$.

\Leftarrow . Se sigue por la Proposición 6.2.11. \square

Lema 6.2.26. *Si $\rho : M \rightarrow N$ es un monomorfismo entonces existen un R -módulo N' tal que $M \leq N'$ y $\tau : N' \rightarrow N$ un isomorfismo tal que si i es la inclusión de M en N' $\tau i = \rho$.*

Demostración. Sea L un conjunto tal que $|L| = |N - \rho(M)|$ y $L \cap M = \emptyset$. Sea $\beta : L \rightarrow N - \rho(M)$ una biyección. Definimos $N' = L \cup M$ y $\tau : N' \rightarrow N$ como $\tau(m) = \rho(m)$ si $m \in M$ y $\tau(l) = \beta(l)$ si $l \in L$.

Le damos estructura de R -módulo a N' de la siguiente manera: sean $x, y \in N'$ y $r \in R$ entonces $x + y = \tau^{-1}(\tau(x) + \tau(y))$ y $rx = \tau^{-1}(r\tau(x))$. Con estas operaciones τ es un isomorfismo. \square

Observación 6.2.27. Con el Lema 6.2.26 y el Teorema 6.2.24, tenemos que todo R -módulo es submódulo de un inyectivo.

Teorema 6.2.28. *Sea ${}_R Q$ un R -módulo inyectivo y $S = \text{End}_R(Q)$. Son equivalentes para $f \in S$:*

- (a) $f \in \text{Rad}(S)$
- (b) $\text{Ker } f \leq_e Q$

Demostración. (a) \Rightarrow (b). Sea $f \in \text{Rad}(S)$. Sea $U \leq Q$ tal que $U \cap \text{Ker } f = 0$. Entonces $f|_U$ es un monomorfismo. Como Q es inyectivo existe $g \in S$ tal que $g \circ f|_U = i$ donde $i : U \rightarrow Q$ es la inclusión canónica. Entonces para todo $u \in U$, $u = i(u) = gf(u)$ lo que implica que $U \subseteq \text{Ker}(Id_Q - gf)$. Como $f \in \text{Rad}(S)$, gf también. Así que $Id_Q - gf$ tiene inverso. Por lo tanto $U \subseteq \text{Ker}(Id_Q - gf) = 0$.

(b) \Rightarrow (a). Consideremos Sf y supongamos que $S = Sf + G$ para algún ideal izq. G de S . Entonces existen $g \in G$ y $h \in S$ tales que $Id_Q = hf + g$. Si $x \in \text{Ker } f \cap \text{Ker } g$ entonces $x = hf(x) + g(x) = 0$. Como $\text{Ker } f \leq_e Q$, $\text{Ker } g = 0$, es decir, g es un monomorfismo. Como Q es inyectivo existe $k \in S$ tal que $kg = Id_Q$ lo que implica que $Id_Q \in G$ y por lo tanto $G = S$. Entonces $Sf \ll S$ y así $f \in \text{Rad}(S)$. \square

Definición 6.2.29. Un anillo R se llama *regular de von Neumann* si para cada $r \in R$ existe $x \in R$ tal que $rxr = r$.

Corolario 6.2.30. Sea ${}_R Q$ inyectivo y $S := \text{End}_R(Q)$. Entonces $S/\text{Rad}(S)$ es un anillo regular de von Neumann, es decir, para cada $f \in S$ existe $g \in S$ tal que $fgf - f \in \text{Rad}(S)$.

Demostración. Sea $f \in S$. Sea $U \leq Q$ un p.c. de $\text{Ker } f$, entonces $\text{Ker } f \oplus U \leq_e Q$. Además $f|_U$ es un monomorfismo, así que existe $g \in S$ tal que $gf|_U = i$ donde $i : U \rightarrow Q$ es la inclusión canónica. Si $k + u \in \text{Ker } f \oplus U$ entonces

$$\begin{aligned} (fgf - f)(k + u) &= fgf(k + u) - f(k + u) = fgf(u) - f(u) \\ &= fgf(u) - f(gf(u)) = 0 \end{aligned}$$

Por lo tanto $\text{Ker } f \oplus U \subseteq \text{Ker}(fgf - f)$, así que $\text{Ker}(fgf - f) \leq_e Q$. Por el Teorema 6.2.28, $fgf - f \in \text{Rad}(S)$. \square

Teorema 6.2.31. Sea P proyectivo y $S := \text{End}_R(P)$. Son equivalentes para $f \in S$:

- (a) $f \in \text{Rad}(S)$
- (b) $\text{Im } f \ll P$

Demostración. (a) \Rightarrow (b). Sea $U \leq P$ tal que $\text{Im } f + U = P$. Consideremos $\pi : P \rightarrow P/U$ la proyección canónica. Entonces para cada $p \in P$ existen $f(x) \in \text{Im } f$ y $u \in U$ tales que $p + U = (f(x) + u) + U = f(x) + U$. Por lo tanto πf es suprayectiva. Como P es proyectivo, existe $g \in S$ tal que $\pi f g = \pi$. Entonces $\pi(\text{Id}_P - fg) = 0$ lo que implica que $\text{Im}(\text{Id}_P - fg) \subseteq \text{Ker } \pi = U$. Como $f \in \text{Rad}(S)$, $\text{Id}_P - fg$ tiene inverso. Por lo tanto $\text{Im}(\text{Id}_P - fg) = P = U$.

(b) \Rightarrow (a). Supongamos que $S = fS + G$ para algún ideal derecho G de S . Entonces existen $h \in S$ y $g \in G$ tales que $\text{Id}_P = fh + g$. Así, para todo $x \in P$, $x = (fh + g)(x) = f(h(x)) + g(x)$ lo que implica que $P = \text{Im } f + \text{Im } g$. Pero $\text{Im } f \ll P$ por lo que $\text{Im } g = P$, es decir, g es sobre. Como P es proyectivo existe $k \in S$ tal que $gk = \text{Id}_P$. Por lo tanto $G = S$. Entonces $fS \ll S$ y $f \in \text{Rad}(S)$. \square

Observación 6.2.32. Desafortunadamente no se puede dar directamente el resultado análogo al Corolario 6.2.30 para módulos proyectivos. Por ejemplo, si tomamos \mathbb{Z} como \mathbb{Z} -módulo, sabemos que \mathbb{Z} es proyectivo y $\text{End}_{\mathbb{Z}}(\mathbb{Z}) \cong \mathbb{Z}$ (Observación 3.4.11). Por otro lado, tenemos que $\text{Rad}(\mathbb{Z}) = 0$. Así que $\mathbb{Z} = \text{End}_{\mathbb{Z}}(\mathbb{Z})/\text{Rad}(\text{End}_{\mathbb{Z}}(\mathbb{Z}))$ que no es un anillo regular de von Neumann (Ejercicio 6.3.10).

Teorema 6.2.33. Si $0 \neq P$ es proyectivo entonces $\text{Rad}(P) \neq P$.

Demostración. Sea $S := \text{End}_R(P)$. Para cada $p \in P$ y $\varphi : P \rightarrow R$ definimos $\varphi_p : P \rightarrow P$ como $\varphi_p(x) = \varphi(x)p$. Sea $p \in \text{Rad}(P)$. Entonces $Rp \ll P$ así que $\text{Im } \varphi_p = \varphi(P)p \subseteq (Rp) \ll P$. Por lo tanto $\text{Im } \varphi_p \ll P$. Por el Teorema 6.2.31 $\varphi_p \in \text{Rad}(S)$.

Sea (φ_i, p_i) la familia dada por el Teorema 6.2.15. Entonces para todo $x \in P$ $x = \sum \varphi_i(x)p_i$. Por lo tanto $(\text{Id}_P - \varphi_{i p_i})(x) = 0$. Supongamos que $\text{Rad}(P) = P$. Si $0 \neq x \in P$, $x = \sum \varphi_i(x)p_i$. Como cada $p_i \in \text{Rad}(P)$ entonces $\varphi_{i p_i} \in \text{Rad}(S)$ para toda i . Lo que implica que $\sum \varphi_{i p_i} \in \text{Rad}(S)$ y por lo tanto $\text{Id}_P - \sum \varphi_{i p_i}$ tiene inverso. Contradicción. \square

Corolario 6.2.34. *Si P es proyectivo y $P = P_1 \oplus P_2$ con $P_2 \subseteq \text{Rad}(P)$ entonces $P_2 = 0$.*

Demostración. Consideremos $\pi : P \rightarrow P_2$ la proyección canónica. Entonces si $P_2 \subseteq \text{Rad}(P)$

$$P_2 = \pi(P_2) \subseteq \pi(\text{Rad}(P)) \subseteq \text{Rad}(P_2) \subseteq P_2$$

Así que $\text{Rad}(P_2) = P_2$. Como P_2 es proyectivo, $P_2 = 0$ por el Teorema 6.2.33. \square

6.3. Ejercicios

1. Demuestre que todo módulo sobre un anillo con división tiene base.
2. Sea R un anillo conmutativo. Si todo ideal de R es libre entonces R es un DIP.
3. Sea R un anillo conmutativo. Demuestre que $R \cong R \oplus R$ si y solo si $R = \{0\}$ (es trivial).
4. Sea K un campo y $R = K[x]$ el anillo de polinomios con coeficientes en K . Sea S el subanillo de R formado por los polinomios sin término lineal. Demuestre que R no es un S -módulo libre.
5. Sea R un anillo y M un R -módulo simple. Demuestre que M es proyectivo o para todo $0 \neq m \in M$ el ideal izquierdo $(0 : m) = \{r \in R \mid rm = 0\}$ es esencial en R .
6. Sea D un dominio entero. Siguiendo la Definición 6.2.17 podemos definir un D -módulo divisible. Demuestre que el campo de fracciones $K(D)$ de D es un D -módulo divisible.
7. Demuestre que $\prod_{p \in \mathbb{P}} \mathbb{Z}_p / \bigoplus_{p \in \mathbb{P}} \mathbb{Z}_p$ es un grupo divisible.
8. Sea $p \in \mathbb{P}$. Tomemos el \mathbb{Z} -módulo \mathbb{Q}/\mathbb{Z} y denotemos a sus elementos como $\left[\frac{a}{b}\right]$ con $\frac{a}{b} \in \mathbb{Q}$. Considere el siguiente subconjunto:

$$\mathbb{Z}_{p^\infty} = \left\{ \left[\frac{a}{p^n} \right] \in \mathbb{Q}/\mathbb{Z} \mid p \nmid a, n > 0 \right\}.$$

- a) Demuestre que \mathbb{Z}_{p^∞} es un subgrupo de \mathbb{Q}/\mathbb{Z} .
 - b) Demuestre que el conjunto $X = \left\{ \left[\frac{1}{p} \right], \left[\frac{1}{p^2} \right], \dots \right\}$ generan a \mathbb{Z}_{p^∞} .
 - c) Demuestre que, $\mathbb{Z} \left[\frac{1}{p^n} \right] \cong \mathbb{Z}_{p^n}$ para cada $n > 0$.
 - d) Demuestre que si $m \leq n$, entonces $\mathbb{Z} \left[\frac{1}{p^m} \right] \subseteq \mathbb{Z} \left[\frac{1}{p^n} \right]$.
 - e) Demuestre que $N \leq \mathbb{Z}_{p^\infty}$ si y solo si $N = \mathbb{Z} \left[\frac{1}{p^n} \right]$ para alguna $n > 0$. Concluya que todo submódulo de \mathbb{Z}_{p^∞} es esencial.
 - f) Demuestre que \mathbb{Z}_{p^∞} es divisible.
 - g) Demuestre que todo \mathbb{Z} -morfismo $\varphi : \mathbb{Z}_{p^\infty} \rightarrow \mathbb{Z}_{p^\infty}$ es suprayectivo.
 - h) Demuestre que $\mathbb{Q}/\mathbb{Z} = \bigoplus_{p \in \mathbb{P}} \mathbb{Z}_{p^\infty}$.
9. Sea K un campo y considere el anillo $R = \text{TI}_2(K)$.
 - a) Demuestre que $\text{Rad}(R)$ es un R -módulo proyectivo.
 - b) Demuestre que el R -módulo R/I donde $I = \text{Zoc}(R)$, es inyectivo.
 Veá el Ejercicio 5.4.16.
 10. Demuestre que \mathbb{Z} no es un anillo regular de von Neumann.

11. Sea $\{K_i\}_I$ una familia de campos. Demuestre que anillo $\prod_I K_i$ es un módulo inyectivo (sobre si mismo).
12. Sea $\{K_i\}_I$ una familia de campos. Demuestre que anillo $\prod_I K_i$ es un anillo regular de von Neumann.
13. Sea $\{K_i\}_I$ una familia de campos y considere el anillo $\prod_I K_i$. Sea $R = \{(a_i) \in \prod_I K_i \mid (a_i) \text{ es casi constante}\}$. Demuestre que R es un subanillo de $\prod_I K_i$ y que también es regular de von Neumann.
14. Sea M un R -módulo semisimple. Demuestre que $\text{End}_R(M)$ es un anillo regular de von Neumann.

Definición 6.3.1. Un anillo R es llamando *V-anillo izquierdo* si todo R -módulo izquierdo simple es inyectivo.

15. Demuestre que un anillo R es un V -anillo izquierdo si y solo si todo ideal izquierdo de R es intersección de ideales izquierdos máximos.
16. Demuestre que un anillo conmutativo R es V -anillo si y solo si R es regular de von Neumann.

Apéndice A

Nociones Básicas de Categorías

A.1. Definición de Categoría

Definición A.1.1. Una *categoría* \mathcal{C} consta de una clase de *objetos* que denotamos $Obj(\mathcal{C})$, y para cada pareja de objetos (A, B) de \mathcal{C} hay un conjunto, denotado $Hom_{\mathcal{C}}(A, B)$, cuyos elementos llamamos *morfismos* y que satisface:

1. Si $(A, B) \neq (C, D)$ entonces $Hom_{\mathcal{C}}(A, B) \cap Hom_{\mathcal{C}}(C, D) = \emptyset$
2. Para cada terna de objetos (A, B, C) en \mathcal{C} existe una función

$$Hom_{\mathcal{C}}(B, C) \times Hom_{\mathcal{C}}(A, B) \longrightarrow Hom_{\mathcal{C}}(A, C)$$

$$(\alpha, \beta) \longmapsto \alpha\beta$$

que llamamos *composición* y que cumple:

- a) $\gamma(\alpha\beta) = (\gamma\alpha)\beta$ (Asociatividad).
- b) Para todo objeto A de \mathcal{C} existe un morfismo $1_A \in Hom_{\mathcal{C}}(A, A)$ tal que $1_B\alpha = \alpha = \alpha 1_A$ para todo $\alpha \in Hom_{\mathcal{C}}(A, B)$ (Morfismo identidad).

Dada una categoría \mathcal{C} y $\varphi \in Hom_{\mathcal{C}}(A, B)$ se suele escribir al morfismo φ como una flecha con dominio A y codominio B

$$\varphi : A \rightarrow B$$

Ejemplo A.1.2. (i) La categoría de Conjuntos, $Sets$. $Obj(Sets) =$ Clase de los conjuntos

$$Hom_{Sets}(A, B) = \{f : A \rightarrow B \mid f \text{ es función}\}$$

- (ii) La categoría de grupos, Gps , donde los objetos son grupos y los morfismos son homomorfismos de grupos.

- (III) La categoría de groups Abelianos, Ab , donde los objetos son grupos abelianos y los morfismos son homomorfismos de grupos.
- (IV) La categoría de anillos, $Rings$, con objetos anillos y homomorfismos de anillos.
- (V) La categoría de R -módulos, $R-Mod$, con objetos módulos izquierdos y morfismos R -morfismos.
- (VI) Sea G un monoide y $*$ un objeto cualquiera. La categoría \widehat{G} tiene un solo objeto $\{*\}$ y $\text{Hom}_{\widehat{G}}(*, *) = G$.
- (VII) Espacios Topológicos, Top . $Obj(Top)$ =Espacios topológicos. Si X y Y son espacios topológicos $\text{Hom}_{Top}(X, Y)$ son las funciones continuas de X en Y .
- (VIII) Sea A un COPO. Vemos a A como categoría de la siguiente forma: $Obj(A) = A$. Si $x, y \in A$ entonces $\text{Hom}_A(x, y) = \{*\}$ si $x \leq y$ y $\text{Hom}_A(x, y) = \emptyset$ en otro caso.

Definición A.1.3. Sea \mathcal{C} una categoría y $\varphi \in \text{Hom}_{\mathcal{C}}(M, N)$. Decimos que:

1. φ es *monomorfismo* si siempre que $\varphi f = \varphi g$ para $f, g \in \text{Hom}_{\mathcal{C}}(L, M)$, se tiene que $f = g$.
2. φ es *epimorfismo* si siempre que $f\varphi = g\varphi$ para $f, g \in \text{Hom}_{\mathcal{C}}(N, L)$, se tiene que $f = g$.
3. φ es *bimorfismo* si es monomorfismo y epimorfismo.
4. φ es *isomorfismo* si existe $f \in \text{Hom}_{\mathcal{C}}(N, M)$ tal que $\varphi f = Id_N$ y $f\varphi = Id_M$

Ejemplo A.1.4. Sea $(\mathbb{N}, \cdot, 1)$ el monoide multiplicativo de los números naturales. Consideremos la categoría $\widehat{\mathbb{N}}$ la cual solo tiene un objeto $*$ y $\text{Hom}_{\widehat{\mathbb{N}}}(*, *) = \mathbb{N}$. Como \mathbb{N} tiene cancelación y la operación es conmutativa, entonces todo $n \in \text{Hom}_{\widehat{\mathbb{N}}}(*, *)$ es monomorfismo y epimorfismo. De este ejemplo vemos que bimorfismo no implica isomorfismo.

Teorema A.1.5. Sea $\varphi \in \text{Hom}_R(M, N)$ un morfismo en la categoría $R-Mod$. Entonces:

1. φ es monomorfismo $\Leftrightarrow \varphi$ es inyectiva.
2. φ es epimorfismo $\Leftrightarrow \varphi$ es suprayectiva o sobre.
3. φ es biyectiva $\Leftrightarrow \varphi$ es bimorfismo $\Leftrightarrow \varphi$ es isomorfismo.

Demostración. $1 \Rightarrow$. Sean $x, y \in M$ tales que $\varphi(x) = \varphi(y)$. Entonces $\varphi(x - y) = 0$. Tomemos $R(x - y)$ y consideremos la inclusión canónica $i : R(x - y) \hookrightarrow M$ y el morfismo cero $\bar{0} : R(x - y) \rightarrow M$. Se tiene que $\varphi i(r(x - y)) = r\varphi(x - y) = 0$ y $\varphi \bar{0}(r(x - y)) = \varphi(0) = 0$, es decir, $\varphi i = \varphi \bar{0}$. Por hipótesis, $i = \bar{0}$ lo que implica que $R(x - y) = 0$ y por lo tanto $x = y$.

\Leftarrow . Sean $f, g : L \rightarrow M$ tal que $\varphi f = \varphi g$ con φ inyectiva. Si $f \neq g$ entonces existe $x \in L$ tal que $f(x) \neq g(x)$ y como φ es inyectiva $\varphi f(x) \neq \varphi g(x)$. Por lo tanto $\varphi f \neq \varphi g$, contradicción.

2 \Rightarrow . Sea $I = \text{Im } \varphi$ y tomemos la proyección canónica $\pi : N \rightarrow N/I$ y el morfismo $\bar{0} : N \rightarrow N/I$. Sea $m \in M$. Entonces $\pi\varphi(m) = \pi(\varphi(m)) = 0$ y $\bar{0}\varphi(m) = 0$. Como φ es un epimorfismo, $\pi = \bar{0}$. Esto implica que $N \subseteq I$ y por lo tanto $N = I$.

\Leftarrow . Supongamos $f\varphi = g\varphi$ con $f \neq g$. Entonces existe $x \in N$ tal que $f(x) \neq g(x)$ pero φ es sobre, así que $x = \varphi(y)$ para algún $y \in M$. Así, $f\varphi(y) \neq g\varphi(y)$. Por lo tanto $f\varphi \neq g\varphi$, contradicción.

3. Es claro, por los incisos anteriores que φ es biyectiva $\Leftrightarrow \varphi$ es bimorfismo. Ahora, si φ es biyección por la Observación 2.1.8.2, φ^{-1} es un R -morfismo, entonces φ es isomorfismo. Por otro lado, si φ es isomorfismo entonces existe un R -morfismo $f : N \rightarrow M$ tal que $\varphi f = \text{Id}_N$ y $f\varphi = \text{Id}_M$. Lo que implica que φ es inyectiva y es suprayectiva por lo tanto φ es biyectiva. \square

Observación A.1.6. Notemos de la prueba del teorema anterior que siempre se tiene que función inyectiva (resp. suprayectiva) implica monomorfismo (resp. epimorfismo) sin embargo el regreso no se tiene en general. Consideremos la categoría *Rings*. Entonces el morfismo inclusión $\mathbb{Z} \hookrightarrow \mathbb{Q}$ es un epimorfismo pero claramente no es suprayectivo.

Demostración. Ejercicio. \square

Usando el Teorema A.1.5 y las Proposiciones 3.1.13 y 3.1.14 tenemos los siguientes resultados

Corolario A.1.7. *Son equivalentes para un R -morfismo $\varphi : M \rightarrow N$:*

- (a) φ es monomorfismo.
- (b) φ es inyectiva.
- (c) $\text{Ker } \varphi = 0$
- (d) Para todo L en $R\text{-Mod}$, si $\psi : L \rightarrow M$ es tal que $\varphi\psi = 0$ entonces $\psi = 0$.

Demostración. (a) \Leftrightarrow (b) es por el Teorema A.1.5 y (b) \Leftrightarrow (c) por la Proposición 3.1.13.

(a) \Rightarrow (d) Supongamos $\varphi\psi = 0$. Tenemos que $\varphi 0 = 0$ entonces $\varphi\psi = \varphi 0$. Como φ es monomorfismo se tiene que $\psi = 0$.

(d) \Rightarrow (c) Sean $K = \text{Ker } \varphi$ e $i : K \hookrightarrow M$ la inclusión. Entonces $\varphi i(K) = \varphi(K) = 0$ así que $\varphi i = 0$. Por hipótesis se tiene que $i = 0$ lo que implica que $K = 0$. \square

Corolario A.1.8. *Son equivalentes para un R -morfismo $\varphi : M \rightarrow N$:*

- (a) φ es epimorfismo.
- (b) φ es suprayectiva.
- (c) $\text{Coker}(\varphi) = 0$
- (d) Para todo L en $R\text{-Mod}$, si $\psi : N \rightarrow L$ es tal que $\psi\varphi = 0$ entonces $\psi = 0$.

Demostración. Ejercicio. \square

Regresemos al contexto general

Proposición A.1.9. Sea \mathcal{C} una categoría. Sean $\varphi \in \text{Hom}_{\mathcal{C}}(M, N)$ y $\psi \in \text{Hom}_{\mathcal{C}}(N, L)$ entonces:

1. φ, ψ monomorfismos $\Rightarrow \psi\varphi$ es monomorfismo.
2. φ, ψ epimorfismos $\Rightarrow \psi\varphi$ es epimorfismo.
3. $\psi\varphi$ es monomorfismo $\Rightarrow \varphi$ es monomorfismo.
4. $\psi\varphi$ es epimorfismo $\Rightarrow \psi$ es epimorfismo.

Demostración. Solo se demostrará 1 y 3, los incisos 2 y 4 son completamente análogos.

1. Supongamos que $(\psi\varphi)f = (\psi\varphi)g$. Como la composición es asociativa, $\psi(\varphi f) = \psi(\varphi g)$. Entonces $\varphi f = \varphi g$ porque ψ es monomorfismo. Como φ también es monomorfismo, $f = g$.

3. Supongamos que $\varphi f = \varphi g$. Entonces $\psi(\varphi f) = \psi(\varphi g)$, asociando $(\psi\varphi)f = (\psi\varphi)g$ lo que implica que $f = g$ ya que $\psi\varphi$ es monomorfismo. \square

A.2. Funtores

Definición A.2.1. Sean \mathcal{C} y \mathcal{D} categorías. Un *functor* $F : \mathcal{C} \rightarrow \mathcal{D}$ es una asignación de los $\text{Obj}(\mathcal{C})$ en $\text{Obj}(\mathcal{D})$ y una asignación de $\text{Hom}_{\mathcal{C}}(A, B)$ en $\text{Hom}_{\mathcal{D}}(F(A), F(B))$ para cada dos objetos A, B de \mathcal{C} de tal manera que se respeta la composición, es decir, si $f \in \text{Hom}_{\mathcal{C}}(B, E)$ y $g \in \text{Hom}_{\mathcal{C}}(A, B)$ entonces $F(fg) = F(f)F(g)$ y $F(1_A) = 1_{F(A)}$.

Observación A.2.2. En la definición anterior al functor F se le llama *functor covariante* o simplemente functor. Si dada $f \in \text{Hom}_{\mathcal{C}}(A, B)$ se tiene que $F(f) \in \text{Hom}_{\mathcal{D}}(F(B), F(A))$ entonces decimos que el functor es *contravariante*.

Ejemplo A.2.3. (I) Consideremos la categoría de grupos abelianos Ab y la categoría de conjuntos $Sets$. Hay un functor $U : Ab \rightarrow Sets$ tal que dado G un grupo abeliano $U(G)$ es solo G como conjunto, y dado un morfismo de grupos abelianos α , $U(\alpha)$ es α visto solo como función. A U se le llama *el functor que olvida*.

(II) Sean G, H grupos abelianos y consideremos las categorías \widehat{G} y \widehat{H} . Si $f : G \rightarrow H$ es un morfismo de grupos abelianos entonces f nos define un functor $\widehat{f} : \widehat{G} \rightarrow \widehat{H}$ definido como: $\widehat{f}(*) = *$ y para cada $g \in \text{Hom}_{\widehat{G}}(*, *) = G$, $\widehat{f}(g) = f(g) \in H = \text{Hom}_{\widehat{H}}(*, *)$. Claramente $\widehat{f}(gl) = \widehat{f}(g)\widehat{f}(l)$ y $\widehat{f}(1_{\widehat{G}}) = 1_{\widehat{H}}$.

(III) Sea X un espacio topológico y sea $\mathcal{O}(X)$ el COPO de abiertos de X . Definimos el functor $P : \mathcal{O}(X) \rightarrow Sets$ como: Dado un abierto $U \in \mathcal{O}(X)$ $P(U) = C(U, \mathbb{R})$ el conjunto de funciones continuas de U en \mathbb{R} . Ahora si $U \leq V$ i.e. $\text{Hom}_{\mathcal{O}(X)}(U, V) = \{*\}$ damos la siguiente función $r : P(V) \rightarrow P(U)$ (el functor P es contravariante) definida como $r(f) = f|_U$ la restricción de f a U .

(IV) El grupo fundamental de un espacio topológico nos define un functor $\pi_1 : Top \rightarrow Gps$.

- (v) Consideremos la categoría DE cuyos objetos son dominios enteros y los morfismos son homomorfismos inyectivos de anillos. Sea $Camp$ la categoría de campos. Si D es un dominio entero podemos construir su campo de fracciones $K(D)$. Entonces $K(-)$ nos define un funtor de DE en $Camp$.
- (vi) La asignación $[-x] : Rings \rightarrow Rings$ dada por $[-x](R) = R[x]$, el anillo de polinomios con coeficientes en R , y $[-x](f) : R[x] \rightarrow S[x]$ como $[-x](f)(\sum r_i x^i) = \sum f(r_i) x^i$ si $f : R \rightarrow S$ es un morfismo de anillos, nos define un funtor.

Ejemplo A.2.4. Dado un R -módulo M tenemos el siguiente funtor

$$\text{Hom}_R(M, -) : R\text{-Mod} \rightarrow Ab$$

Definido de la siguiente manera: Si N es un R -módulo entonces $\text{Hom}_R(M, N)$ es un grupo abeliano. Ahora, si $f : N \rightarrow L$ es un R -morfismo,

$$\text{Hom}_R(M, f) : \text{Hom}_R(M, N) \rightarrow \text{Hom}_R(M, L)$$

es un morfismo de grupos abelianos que se calcula como $\text{Hom}_R(M, f)(g) = fg$. De forma análoga tenemos el funtor

$$\text{Hom}_R(-, M) : R\text{-Mod} \rightarrow Ab$$

solo que este funtor es contravariante, es decir, si $f : N \rightarrow L$ es un R -morfismo entonces

$$\text{Hom}_R(f, M) : \text{Hom}_R(L, M) \rightarrow \text{Hom}_R(N, M)$$

calculado como $\text{Hom}_R(f, M)(h) = hf$.

A.3. Producto y Coproducto

Definición A.3.1. Sea \mathcal{C} una categoría y $\{A_i\}_{i \in I}$ una familia de objetos de \mathcal{C} .

1. Un *producto* de la familia $\{A_i\}_{i \in I}$ es una pareja $(P, \{\pi_i\}_{i \in I})$ tal que:
 - a) $P \in \text{Obj}(\mathcal{C})$
 - b) $\{\pi_i\}_I$ es una familia de morfismos de \mathcal{C} tale que $\pi_i \in \text{Hom}_{\mathcal{C}}(P, A_i)$.
 - c) Para toda familia de morfismos $\gamma_i \in \text{Hom}_{\mathcal{C}}(C, A_i)$ $i \in I$ y $C \in \text{Obj}(\mathcal{C})$ existe una única $\gamma \in \text{Hom}_{\mathcal{C}}(C, P)$ tal que $\gamma_i = \pi_i \gamma \forall i \in I$
2. Un *coproducto* de la familia $\{A_i\}_{i \in I}$ es una pareja $(Q, \{\eta_i\}_{i \in I})$ tal que:
 - a) $Q \in \text{Obj}(\mathcal{C})$
 - b) $\{\eta_i\}_I$ es una familia de morfismos de \mathcal{C} tale que $\eta_i \in \text{Hom}_{\mathcal{C}}(A_i, Q)$.
 - c) Para toda familia de morfismos $\alpha_i \in \text{Hom}_{\mathcal{C}}(A_i, B)$ $i \in I$ y $B \in \text{Obj}(\mathcal{C})$ existe una única $\alpha \in \text{Hom}_{\mathcal{C}}(Q, B)$ tal que $\alpha_i = \alpha \eta_i \forall i \in I$

Teorema A.3.2. Sea $(P, \{\pi_i\}_I)$ un producto de la familia $\{A_i\}$ en la categoría \mathcal{C} . Entonces una pareja $(P', \{\pi'_i\}_I)$, donde $\pi'_i \in \text{Hom}_{\mathcal{C}}(P', A_i)$ es también un

producto de la familia si y solo si existe un isomorfismo $\varphi \in \text{Hom}_{\mathcal{C}}(P', P)$ tal que:

$$\begin{array}{ccc} P' & \xrightarrow{\varphi} & P \\ \pi'_i \downarrow & \cong \nearrow & \downarrow \pi_i \\ P_i & & P_i \end{array}$$

conmuta para todo $i \in I$. Es decir el producto de una familia, si existe, es único salvo isomorfismo.

Demostración. Como $(P, \{\pi_i\}_I)$ es un producto entonces para la familia $\{\pi'_i\}_I$ existe un único $\varphi \in \text{Hom}_{\mathcal{C}}(P', P)$ tal que $\pi_i \varphi = \pi'_i$ para todo $i \in I$.

\Rightarrow . Supongamos que $(P', \{\pi'_i\}_I)$ es un producto entonces existe un único $\varphi' \in \text{Hom}_{\mathcal{C}}(P, P')$ tal que $\pi'_i \varphi' = \pi_i$, entonces $\pi_i(\varphi \varphi') = \pi_i$ pero $\pi_i \text{Id}_M = \pi_i$ para toda $i \in I$. Entonces por la unicidad del morfismo tenemos que $\varphi \varphi' = \text{Id}_M$. Análogamente se tiene que $\varphi' \varphi = \text{Id}_{M'}$. Por lo tanto φ es un isomorfismo.

\Leftarrow . Sea $\varphi : P' \rightarrow P$ un isomorfismo y $\{f_i\}_I$ una familia de morfismos $f_i \in \text{Hom}_{\mathcal{C}}(C, A_i)$ para toda $i \in I$. Entonces existe un único $h : C \rightarrow P$ tal que $\pi_i h = f_i$ para todo $i \in I$. Sea $\gamma = \varphi^{-1} h$ de C en P' , entonces $\pi'_i \gamma = \pi'_i \varphi^{-1} h = \pi_i h = f_i$. Además si $\gamma' : C \rightarrow P'$ es tal que $\pi'_i \gamma' = f_i$ para toda $i \in I$, entonces $\pi_i(\varphi \gamma') = \pi'_i \gamma' = f_i$. Por la unicidad de h , $\varphi \gamma' = h$ así que $\gamma' = \varphi^{-1} h = \gamma$. Por lo tanto $(P', \{\pi'_i\}_I)$ es un producto. \square

Teorema A.3.3. Sea $(Q, \{\eta_i\}_I)$ un coproducto de la familia $\{Q_i\}_I$ en la categoría \mathcal{C} . Entonces, $(Q', \{\eta'_i\}_I)$ donde $\eta_i \in \text{Hom}_{\mathcal{C}}(Q_i, Q')$ es también un coproducto de la familia si y solo si existe un único isomorfismo $\psi \in \text{Hom}_{\mathcal{C}}(Q, Q')$ tal que:

$$\begin{array}{ccc} Q & \xrightarrow{\psi} & Q' \\ \eta_i \uparrow & \cong \nearrow & \uparrow \eta'_i \\ Q_i & & Q_i \end{array}$$

conmuta $\forall i \in I$. Es decir el coproducto de una familia, si existe, es único salvo isomorfismo.

Demostración. Como $(Q, \{\eta_i\}_I)$ es un coproducto entonces para la familia de morfismos $\{\eta'_i\}_I$ existe un único morfismo $\psi : Q \rightarrow Q'$ tal que $\psi \eta_i = \eta'_i$ para toda $i \in I$.

\Rightarrow : Supongamos que $(Q', \{\eta'_i\}_I)$ es un coproducto. Entonces existe un único morfismo $\psi' : Q' \rightarrow Q$ tal que $\psi' \eta'_i = \eta_i$ para toda $i \in I$. Como $\text{Id}_{Q'} \eta'_i = \eta'_i$ y también $(\psi') \eta'_i = \eta'_i$, de la unicidad se sigue que $\psi \psi' = \text{Id}_{Q'}$. Análogamente $\psi' \psi = \text{Id}_Q$. Por lo tanto ψ es un isomorfismo.

\Leftarrow : Supongamos que existe $\psi : Q \rightarrow Q'$ isomorfismo tal que $\psi \eta_i = \eta'_i$. Tomemos $\{\gamma_i\}_I$ con $\gamma_i \in \text{Hom}_{\mathcal{C}}(Q_i, B)$ para todo $i \in I$. Como $(Q, \{\eta_i\}_I)$ es un coproducto entonces existe un único $h : Q \rightarrow B$ tal que $h \eta_i = \gamma_i$ para toda $i \in I$. Sea $f = h \psi^{-1}$. Entonces

$$f \eta'_i = h \psi^{-1} \eta'_i = h \psi^{-1} \psi \eta_i = h \eta_i = \gamma_i.$$

Si $f' : Q' \rightarrow B$ es tal que $f' \eta'_i = \gamma_i \forall i \in I$. Entonces $(f' \psi) \eta_i = f' \eta'_i = \gamma_i$, por la unicidad de h se tiene que $f' \psi = h$, por lo tanto $f' = h \psi^{-1} = f$. \square

Ejemplo A.3.4. 1. Sea $\{A_i\}_{i \in I}$ una familia no vacía de conjuntos, el producto cartesiano de la familia se define como

$$\prod_{i \in I} A_i = \left\{ f : I \rightarrow \bigcup_{i \in I} A_i \mid f \text{ es función y } f(i) \in A_i \forall i \in I \right\}$$

Para cada $i \in I$ definimos $\pi_i : \prod A_i \rightarrow A_i$ como $\pi_i(f) = f(i)$ que se les llama las proyecciones canónicas. Entonces $(\prod A_i, \{\pi_i\}_I)$ es el producto de la familia $\{A_i\}_{i \in I}$ en la categoría *Sets*. Dado un elemento $f \in \prod A_i$ se suele escribir $f = (f_i)_I$ donde $f_i = f(i) \in A_i$.

2. Sea L una retícula (Definición 2.3.1) vista como categoría (Ejemplo A.1.2(8)). Sean $x, y \in L$, entonces $x \wedge y \in L$ es el producto de x y y en L . El coproducto de x y y en L es el elemento $x \vee y \in L$.

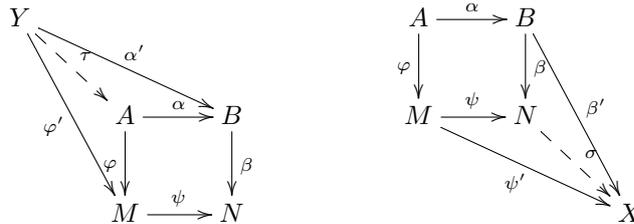
A.4. Producto Fibrado y Coproducto Fibrado

Sea \mathcal{C} una categoría. Considerer el siguiente diagrama:

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ \varphi \downarrow & & \downarrow \beta \\ M & \xrightarrow{\psi} & N \end{array}$$

Definición A.4.1. 1. El par (φ, α) es llamado el *producto fibrado* del par (ψ, β) si para cualquier par (φ', α') con $\varphi' : Y \rightarrow M$, $\alpha' : Y \rightarrow B$ existe un único $\tau : Y \rightarrow A$ tal que $\varphi' = \varphi\tau$ y $\alpha' = \alpha\tau$.

2. El par (ψ, β) es llamado el *coproducto fibrado* del par (φ, α) si para cualquier par (ψ', β') con $\psi' : M \rightarrow X$, $\beta' : B \rightarrow X$ y $\psi'\varphi = \beta'\alpha$ existe un único $\sigma : N \rightarrow X$ tal que $\psi' = \sigma\psi$ y $\beta' = \sigma\beta$.



Proposición A.4.2. *El coproducto fibrado del par (φ, α) y el producto fibrado del par (ψ, β) , son únicos salvo isomorfismos.*

Demostración. Sean (ψ, β) y (ψ', β') dos pushouts para (φ, α) , entonces por la definición de pullback tenemos que existen $\sigma : N \rightarrow X$ y $\rho : X \rightarrow N$ tales que $\psi' = \sigma\psi$, $\beta' = \sigma\beta$ y $\psi = \rho\psi'$, $\beta = \rho\beta'$. Así para $\rho\sigma : N \rightarrow N$ tenemos que $\psi = \rho\psi' = \rho\sigma\psi$ y $\beta = \rho\beta' = \rho\sigma\beta$ de lo que se sigue que $\rho\sigma = Id_N$. Análogamente $\sigma\rho = Id_X$ por lo tanto ρ y σ son isomorfismos uno inverso del otro.

Ahora sean (φ, α) y (φ', α') dos pullbacks para (ψ, β) , entonces tenemos que existen $\tau : Y \rightarrow A$ y $\tau' : A \rightarrow Y$ tales que $\alpha' = \alpha\tau$, $\varphi' = \varphi\tau$ y $\alpha = \alpha'\tau'$,

$\varphi = \varphi'\tau'$. Para $\tau\tau' : A \rightarrow A$ tenemos que $\alpha = \alpha'\tau' = \alpha\tau\tau'$ y $\varphi = \varphi'\tau' = \varphi\tau\tau'$, así que por lo tanto $\tau\tau' = Id_A$. Análogamente $\tau'\tau = Id_Y$ lo que implica que τ y τ' son isomorfismos uno inverso del otro. \square

Ejemplo A.4.3. 1. Sea C un conjunto. Tomemos $\mathbf{P}(C)$ el conjunto potencia de C , el cual es una retícula. Sean $A, B \in \mathbf{P}(C)$. Denotemos $\psi : A \hookrightarrow C$ y $\beta : B \hookrightarrow C$ las funciones inclusiones. Consideremos $A \cap B$ y sean $\varphi : A \cap B \hookrightarrow A$ y $\alpha : A \cap B \hookrightarrow B$ las inclusiones. Entonces el par (φ, α) es el producto fibrado del par (ψ, β) .

$$\begin{array}{ccc} A \cap B & \xrightarrow{\alpha} & B \\ \varphi \downarrow & & \downarrow \beta \\ A & \xrightarrow{\psi} & C \end{array}$$

2. Ahora, sea X un conjunto y consideremos $A, B, C \in \mathbf{P}(X)$ tales que $A \subseteq B$ y $A \subseteq C$. Sean $\alpha : A \hookrightarrow B$ y $\varphi : A \hookrightarrow C$ las inclusiones. Consideremos $B \cup C$ y sean $\psi : C \hookrightarrow B \cup C$ y $\beta : B \hookrightarrow B \cup C$ las inclusiones. Entonces el par (ψ, β) es el coproducto fibrado del par (φ, α) .

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ \varphi \downarrow & & \downarrow \beta \\ C & \xrightarrow{\psi} & B \cup C \end{array}$$

Proposición A.4.4. *Supongamos que tenemos el diagrama conmutativo*

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ \varphi \downarrow & & \downarrow \beta \\ M & \xrightarrow{\psi} & N \end{array}$$

1. Si (φ, α) es el producto fibrado del par (ψ, β) , entonces
 - (a) Si β es un monomorfismo entonces φ también lo es.
 - (b) Si ψ es monomorfismo entonces α también lo es.
2. Si (ψ, β) es el coproducto fibrado del par (φ, α) , entonces
 - (a) Si α es un epimorfismo entonces ψ también lo es.
 - (b) Si φ es un epimorfismo entonces β también lo es.

Demostración. Sólo probaremos 1.(a) y 2.(a). los otros dos resultados son análogos.

1.(a). Supongamos que β es monomorfismo y sean $f, g : X \rightarrow A$ tales que $\varphi f = \varphi g$. Entonces $\psi\varphi f = \psi\varphi g$, como el diagrama conmuta $\beta\alpha f = \beta\alpha g$. Por hipótesis β es monomorfismo así que $\alpha f = \alpha g$. Notemos que $\beta(\alpha g) = \psi(\varphi f)$ entonces por la propiedad universal del producto fibrado existe un único $h : X \rightarrow A$ tal que $\varphi h = \varphi f$ y $\alpha h = \alpha g$ lo que implica que $f = h = g$.

2.(a). Supongamos que tenemos $f, g : N \rightarrow X$ tales que $f\psi = g\psi$. Entonces $f\psi\varphi = g\psi\varphi$, como el diagrama conmuta $f\beta\alpha = g\beta\alpha$. Por hipótesis α es epimorfismo así que $f\beta = g\beta$. Notemos que $(f\beta)\alpha = (g\psi)\varphi$ así que por la propiedad universal del coproducto fibrado existe un único $h : N \rightarrow X$ tal que $h\beta = f\beta$ y $h\psi = g\psi$ lo que implica que $f = h = g$. \square

Índice alfabético

- Algebra de grupo, 1
- Anillo, 1
 - Bueno, 66
 - de endomorfismos, 29
 - Opuesto, 29
 - Sub-, 1
 - V-, 87
 - von Neumann, 83
- Anulador, 6, 23
- Base, 71
- Base Dual, 80
- Bimódulo, 28
- Bimorfismo, 90
- Cíclico, 11
- Categoría, 89
- Combinaciones Lineales, 9
- Componente Homogenea, 62
- Conúcleo, 19
- Conjunto
 - codirigido, 15
 - dirigido, 15
- Coproducto, 35, 94
 - Fibrado, 41, 95
- Criterio de Baer, 81
- Divisible, 81
- Dominio, 73
 - Entero, 73
- Epimorfismo, 18, 90
 - Escinde, 23
- Extensión Esencial, 57
- Finitamente Cogenerado, 61
- Finitamente Generado, 11
- Función
 - tensorial, 46
 - Biaditiva, 46
- Funtor, 92
- Adjunto, 93
- Contravariante, 92
- Covariante, 92
- Exacto Izquierdo, 93
- Ideal, 2
 - Derecho, 2
 - Izquierdo, 2
- Idempotente, 33
 - Ortogonales, 40
- Imagen, 19
- Inclusión Canónica, 17
- Isomorfismo, 18, 90
 - 1er Teorema, 22
 - 2do Teorema, 22
 - 3er Teorema, 22
 - de Anillos, 3
- Lemma del Quinto, 26
- Ley Modular, 10
- Módulo, 4
 - Cociente, 13
 - Fiel, 6
 - Inyectivo, 76
 - Libre, 71
 - Proyectivo, 76
 - Semisimple, 60
 - Simple, 9
- Monomorfismo, 18, 90
 - Escinde, 23
- Morfismo, 89
 - R-, 17
 - de Anillos, 2
- Núcleo, 19
- Objeto, 89
- Producto, 35, 94
 - Fibrado, 41, 95

- Tensorial, 45
- Proyección Canónica, 18
- Pseudocomplemento, 55

- Radical, 64
- Rechazo, 34
- Restricción de escalares, 6
- Retícula, 15
 - Completa, 15
 - Inferiormente continua, 69
 - Superiormente continua, 16

- Soporte, 35
- Submódulo, 9
 - Cerrado, 57
 - de torsión, 16, 34
 - Esencial, 55
 - Generado, 10
 - Máximo, 11
 - Superfluo, 58
 - Totalmente invariante, 33
- Sucesión exacta, 25
 - Corta, 25
 - se escinde, 27
- Suma directa, 12
 - Externa, 37
- Sumando Directo, 23
- Suplemento, 58

- Traza, 34

- Zoclo, 64