Una introducción a la teoría de módulos sobre anillos no conmutativos

Mauricio Medina-Bárcenas

2023

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 sugerencia y/o comentario que me lo pueden hacer llegar a mi correo inv.asoc27mmedina@cidesi.edu.mx

Dr. Mauricio Medina-Bárcenas
Santiago de Querétaro, Diciembre 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. Cápsulas Inyectivas y Cubiertas Proyectivas 86

6.3.1. Ejemplo de una cápsula inyectiva 90
6.4. Ejercicios 93

7. Dos teoremas de descomposición de anillos **95**
7.1. Anillos Locales 95
7.2. Teorema de Krull-Remak-Schmidt-Azumaya 98
7.3. Teorema de Wedderburn-Artin 100
7.4. Ejercicios 103

8. Módulos Artinianos y Noetherianos **105**
8.1. Módulos Artinianos y Noetherianos 105
8.2. Teorema de Hopkins-Levitzki 113
8.3. Descomp. Módulos inyectivos sobre Noeth. y Art. 116
8.4. Ejercicios 120

A. Nociones Básicas de Categorias **123**
A.1. Definición de Categoría 123
A.2. Funtores 126
A.3. Producto y Coproducto 127
A.4. Producto Fibrado y Coproducto Fibrado 129

Indice **132**

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.
$\mathbb{Z}_{p^\infty}$	p-Grupo de Prüfer.
Ab	Categoría de grupos abelianos.
R^{op}	Anillo opuesto.
$R[x_1, ..., x_n]$	Anillo de polinomios en identerminadas $x_1, ..., x_n$ con coeficientes en R.
R-Mod	Categoría de R-módulos izquierdos.
R-Simp	Conjunto de representantes de clases de isomorfismo de R-módulos simples.
${}_RM$ (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.
$\mathrm{M}_{n\times k}(R)$	Grupo de matrices de $n \times k$ con coeficientes en R.
$\mathrm{M}_n(R)$	Anillo de matrices de $n \times n$ con coeficientes en R.
$\mathrm{TI}_n(R)$	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.
$\mathrm{Zoc}(M)$	Zoclo del módulo M.
$\mathrm{Rad}(M)$	Radical del módulo M.
$N << M$	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.
$\mathrm{Hom}_R(M, N)$	Conjunto de R-morfismos de M en N.
$\mathrm{End}_R(M)$	Anillo de endomorphimos del R-módulo M.
Id_M	Morfismo identidad del módulo M.
$\rightarrowtail$	Monomorfismo.
$\twoheadrightarrow$	Epimorfismo.
$\hookrightarrow$	Inclusión.
$\mathrm{Ker}\,\varphi$	Núcleo del morfismo φ.
$\mathrm{Im}\,\varphi$	Imagen del morfismo φ.
$M \otimes_R N$	Producto tensorial de los módulos M y N sobre el anillo R.
$\mathrm{Coker}\,\varphi$	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.
$Obj(\mathcal{C})$	Objetos de la categoría $\mathcal{C}$.
$\mathrm{Hom}_{\mathcal{C}}(A, B)$	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 $\mathrm{M}_n(K)$ 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 $\mathrm{TI}_n(K)$ de $\mathrm{M}_n(K)$ es un subanillo.

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

(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 $\mathrm{TI}_2(K)$.

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

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

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 $(S, \mp, *, 0_S, 1_S)$ son anillos con uno, una función $\varphi : R \to S$ es un *morfismo de anillos* si:

1. $\varphi(r+s) = \varphi(r) \overline{+} \varphi(s)$
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 $\iota : S \to R$ 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, $ev_a : R[x] \to R$ es un morfismo de anillos.

(III) Sea R un anillo. La función $\varphi : R \to \mathrm{M}_2(R)$ definida como $\varphi(r) = \left(\begin{smallmatrix} r & 0 \\ 0 & r \end{smallmatrix}\right)$ es un morfismo de anillos.

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

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

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

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

respectivamente.

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

1. $\operatorname{Ker} \varphi$ *es un ideal bilateral de R.*
2. $\operatorname{Im} \varphi$ *es un subanillo de S.*
3. *φ es inyectiva si y solo si* $\operatorname{Ker} \varphi = \{0\}$.
4. *φ induce un isomorfismo de anillos entre $R/\operatorname{Ker} \varphi$ y $\operatorname{Im} \varphi$.*
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 $\varphi : M \to M$. Denotemos $\mathrm{End}_{\mathbb{Z}}(M) = \{\varphi \mid \varphi \text{ endomorfismo de } M\}$.

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

$$\begin{aligned} \varphi \widehat{+} \psi : \quad & M \longrightarrow M \\ & m \longmapsto \varphi(m) + \psi(m) \end{aligned} \qquad \begin{aligned} -\varphi : \quad & M \longrightarrow M \\ & m \longmapsto -\varphi(m) \end{aligned}$$

$$\begin{aligned} \widehat{0} : \quad & M \longrightarrow M \\ & m \longmapsto 0 \end{aligned} \qquad \begin{aligned} \varphi \circ \psi : \quad & M \longrightarrow M \\ & m \longmapsto \varphi(\psi(m)) \end{aligned}$$

$$\begin{aligned} 1_M : \quad & M \longrightarrow M \\ & m \longmapsto m \end{aligned}$$

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

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

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

$$\begin{aligned} \lambda(r) : \quad & M \longrightarrow M \\ & m \longmapsto \lambda(r)(m) := rm. \end{aligned}$$

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

$$
\begin{array}{llll}
\varphi: & R \longrightarrow \mathrm{End}_{\mathbb{Z}}(R_+) & & \\
 & r \longmapsto \varphi(r): & R_+ \longrightarrow R_+ & \\
 & & x \longmapsto \varphi(r)(x) := rx &
\end{array}
$$

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

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

$$
\begin{array}{l}
\mathbb{Z} \longrightarrow S \\
1 \longmapsto 1_S \\
n \longmapsto 1_S + 1_S + ... + 1_S \ (n \ \ veces)
\end{array}
$$

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

Si M es un grupo abeliano

$$
\begin{array}{llll}
\lambda: & \mathbb{Z} \longrightarrow \mathrm{End}_{\mathbb{Z}}(M) & & \\
 & 1 \longmapsto Id_M & & \\
 & n \longmapsto \lambda(n): & M \longrightarrow M & \\
 & & m \longmapsto \lambda(n)(m) := nm &
\end{array}
$$

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

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

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

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

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

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

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 $(M, \overline{+}, 0)$ un grupo. Se dice que M es un R-módulo izquierdo, denotado ${}_RM$, si existe una acción

$$R \times M \longrightarrow M$$

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

que cumple:

1. $r(m\overline{+}n) = rm\overline{+}rn$
2. $(r + s)m = rm\overline{+}sm$
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) Considremos el anillo $R = \begin{pmatrix} \mathbb{Q} & 0 \\ \mathbb{R} & \mathbb{R} \end{pmatrix}$ con las operaciones de matrices. Entonces

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

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 topologico 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 $f : R \to S$ 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 $_KV$ un K-espacio vectorial (de cualquier dimensión). Sea
$$\mathrm{End}_K(V) = \{f : V \to V \mid f \text{ es una transformación lineal}\}.$$
Demuestre que $\mathrm{End}_K(V)$ es un anillo con la suma puntual y la composición.

3. De un K-espacio vectorial V tal que $\mathrm{End}_K(V)$ no sea un anillo conmutativo.

4. Sea K un campo. Demuestre que $\left(\begin{smallmatrix} 0 & 0 \\ 0 & K \end{smallmatrix}\right)$ no es un ideal bilateral de $\mathrm{TI}_2(K)$.

5. Sea K un campo. Demuestre que $\left(\begin{smallmatrix} K & 0 \\ K & 0 \end{smallmatrix}\right)$ es un ideal bilateral de $\mathrm{TI}_2(K)$ pero no de $\mathrm{M}_n(K)$.

6. Sea I el ideal del ejercicio anterior. Demuestre que $\mathrm{TI}_2(K)/I$ es isomorfo a K.

7. Demuestre la Proposición 1.1.7

8. Sea K un campo. Demuestre que el anillo $\mathrm{M}_n(K)$ no tiene ideales bilaterales distintos de 0 y $\mathrm{M}_n(K)$.

9. Sean R un anillo conmutativo, G y H grupos finitos. Suponga que $f : G \to H$ es un morfismo de grupos. Demuestre que $\overline{f} : R[G] \to R[H]$ definida como $\overline{f}\left(\sum_{g\in G} r_g g\right) = \sum_{g\in G} r_g f(g)$ 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 $\mp$ 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 $\mathrm{M}_{n\times k}(R)$ las matrices de tamaño $n \times k$ con coeficientes en R. Demuestre que $\mathrm{M}_{n\times k}(R)$ es un $\mathrm{M}_n(R)$-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 siguietes afirmaciones son equivalentes:

    (a) M es fiel.

    (b) R es (isomorfo a) un subanillo de $\mathrm{End}_{\mathbb{Z}}(M)$.

    (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 $N \leq {}_RM$) si

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

Denotemos $Sub({}_RM) := \{N \mid N \leq {}_RM\}$ 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 ${}_RR$, $I \leq {}_RR$ 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 division (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 $X \subseteq M$, $AX = \{a_1x_1 + a_2x_2 + ... + a_nx_n \mid a_i \in A\ x_i \in X\ n \in \mathbb{N}\}$ 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 $RX \leq {}_RM$.*

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 $x = r_1x_1 + \cdots + r_nx_n$ y $sx = sr_1x_1 + \cdots + sr_nx_n \in RX$. 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 $z = a_1x_1 + a_2x_2 + ... + a_nx_n$ con $a_i \in R$ y $x_i \in N$ como $N \leq {}_R M$ entonces $a_ix_i \in N$ y $a_ix_i + a_{i+1}x_{i+1} \in N$ por lo tanto $a_1x_1 + ... + a_nx_n \in N$ asi $RN \subseteq N$ 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 $an = an + 0 \in N$. Por lo tanto $N \leq {}_R M$. ☐

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 $a_1, ..., a_n \in R$ y $x_1, ..., x_n \in X$ entonces $a_1x_1 + ... + a_nx_n \in \ell(X)$ así que $RX \subseteq \ell(X)$. ☐

Observación 2.1.9. Por el lemma anterior tenemos que

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

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 $(H \cap K) + (H \cap L) \leq H \cap (K + L)$. ☐

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 $(H \cap K) + (H \cap L) = \overline{0} + \overline{0} = \overline{0}$.

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

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

Demostración. $\supseteq\rfloor$ Es la Observación 2.1.10.

$\subseteq\rfloor$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. □

A partir de este momento denotaremos ${}_RM$ 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 $RX = Rx_1 + Rx_2 + ... + Rx_n$. Si $M = \sum_{i \in I} M_i$ entonces para cada $i \in \{1, ..., n\}$, x_i está en una suma finita de submódulos en la familia $\{M_i\}_{i \in I}$. Entonces $X = \{x_1, ..., x_n\}$ 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 $X = \{x_1, ..., x_n\} \subseteq M$ tal que $M = \sum_{i=1}^{n} Rx_i = RX$ por lo tanto M es f.g. □

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

(b)⇒(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 $L = M$. □

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

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

Sea $L = K + Rx_2 + ... + Rx_n$. Entonces $L < M$. Sea $\mathbf{P} = \{N < {}_RM \mid L \leq N\}$ 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 **P** no vacia, 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 $V \in$ **P**. Por el lema de Zorn **P** tiene elementos máximos. Sea N máximo en **P**, si $N < T \leq M$ entonces $x_1 \in T$ ya que de lo contrario T estaría en **P** contradiciendo la maximalidad de N. Por lo tanto $T = M$. □

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 primo[1]. 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 $\{N_\alpha\}_{\alpha\in X} \subseteq Sub(M)$ 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 $m = n_{\alpha_1} + ... + n_{\alpha_k}$ con $n_{\alpha_i} \in N_{\alpha_i}$.*

Demostración. (a)⇒(b) Sea $m \in M$ tal que $m = a_{\alpha_1} + ... + a_{\alpha_k}$ y $m = b_{\alpha_1} + ... + b_{\alpha_s}$ 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 $a_{\alpha_j} = b_{\alpha_1} + ... + b_{\alpha_s} - a_{\alpha_1} - ... - a_{\alpha_k}$ 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)⇒(a) Si $N_\alpha \cap \sum_{\beta\neq\alpha} N_\beta \neq 0$ tomemos un elemento n_α en la intersección. Así, $n_\alpha = n_{\beta_1} + ... + n_{\beta_k}$ 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, $n_\alpha = 0$. □

[1] Para la definición de suma directa vea la Sección 4.1

2.2. Cocientes

Sea ${}_RM$ 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 equivaliencia $\overline{x}$. Entonces

$$\overline{x} = \{y \in M \mid x \equiv y\,(N)\} = \{y \in M \mid y = x + n \; p.a. \; n \in N\} = \{x + n \mid n \in N\}\,.$$

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 $r \in R$

$$(x + N)\overline{+}(y + N) := (x + y) + N$$

$$r(x + N) := rx + N$$

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 $f_N^* \circ f_N(H) = f_N^*(H/N) = \{x \in M \mid x + N \in H/N\} = H$. □

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

Como ${}_RR$ 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 $m_1, ..., m_n \in M$. Sea $x+N \in M/N$. Se tiene que $x = r_1 m_1 + r_2 m_2 + \cdots + r_n m_n$. Entonces, $x + N = (r_1 m_1 + r_2 m_2 + \cdots + r_n m_n) + N = r_1 m_1 + N + r_2 m_2 + N + \cdots + r_n m_n + N$. Lo que implica que $m_1 + N, m_2 + N, ..., m_n + N$ generan a M/N. □

Observación 2.2.5. En general, submodulos 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 ${}_RR$ 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 $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & q \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & aq \\ 0 & 0 \end{smallmatrix}\right)$. 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 ${}_RI$ tampoco.

2.3. Ejercicios

1. Considere el anillo R del Ejemplo 1.2.7.II. Demuestre que $\left(\begin{smallmatrix} 0 & 0 \\ 0 & \mathbb{R} \end{smallmatrix}\right)$ 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 ${}_RM$ entonces $\bigcap\{N_\alpha\}_{\alpha\in X}$ es un submodulo de ${}_RM$.

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 submodulo finitamente generado de ${}_{\mathbb{Z}}\mathbb{Q}$ es cíclico.

7. Sea $X \subseteq {}_{\mathbb{Z}}\mathbb{Q}$ un subconjunto generador, es decir, $\mathbb{Z}X = {}_{\mathbb{Z}}\mathbb{Q}$ y sea $x_0 \in X$. Demuestre que $\mathbb{Z}(X - \{x_0\}) = {}_{\mathbb{Z}}\mathbb{Q}$. Concluya que ${}_{\mathbb{Z}}\mathbb{Q}$ no es finitamente generado.

8. Demuestre que ${}_{\mathbb{Z}}\mathbb{Q}$ no tiene submódulos maximos.

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 contensión de conjuntos y el supremo e ínfimo son la union y la intesección 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 contensión y el supremo e ínfimo quedan descritos por la union y tomar el interior de la intersección de una familia de conjuntos abiertos respectivamente.

14. Demuestre que $Sub({}_RM)$ es una retícula completa donde $\leq$ esta dado por $\subseteq$. Además, dada una familia de submódulos de ${}_RM$, $\{N_\alpha\}_{\alpha\in X}$, 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 $(L, \leq, \bigwedge, \bigvee)$ 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 ${}_RM$ un R-módulo. Demuestre que $Sub({}_RM)$ es una retícula superiormente continua.

16. Sea $N \leq M$. Demuestre que la relación $\equiv\ (N)$ es de equivalencia.

17. Demuestre la Proposicón 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 ${}_RM$ y ${}_RN$ son R-módulos una función $\varphi : M \to N$ 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. $\varphi : {}_RM \to {}_RN$ 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*:

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

(II) Sea ${}_RN \leq {}_RM$ y consideremos la función:

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

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 $N \leq {}_RM$, 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 ésto, sean $x, y \in M$ y $r \in R$

$$\pi(rx+y) = (rx+y) + N = (rx+N) + (y+N)$$

$$= r(x+N) + (y+N) = r\pi(x) + \pi(y)$$

.

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

2. Si $\varphi : M \to N$ 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, $\varphi : M \to N$ y $\psi : N \to L$ 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

$$\varphi^{-1}(rn+l) = \varphi^{-1}(r\varphi(x) + \varphi(y)) = \varphi^{-1}(\varphi(rx+y)) = rx+y$$

$$= r\varphi^{-1}(n) + \varphi^{-1}(l)$$

□

Observación 3.1.5. Sea $\varphi : M \to N$ un R-morfismo. Usaremos el termino *monomorfismo* para referirnos a que φ es inyectivo y usaremos el termimo *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 $\varphi : M \to N$ 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 $\varphi : M \to N$.

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 $\varphi : M \to N$ 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 $u_1, u_2 \in U$ asi $rx + y = r\varphi(u_1) + \varphi(u_2) = \varphi(ru_1 + u_2) \in \varphi(U)$ 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 $rx + y \in \varphi^{-1}(V)$. □

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

1. El *núcleo* de φ se define como:

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

2. La *imagen* de φ se define como:

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

3. El *conúcleo* de φ se define como:

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

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

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

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

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

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

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

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 $u - x \in \operatorname{Ker}\varphi$. Por lo tanto $x = x + (u - x) \in U + \operatorname{Ker}\varphi$. Recíprocamente, si $x \in U + \operatorname{Ker}\varphi$, entonces $x = u + k$ con $u \in U$ y $k \in \operatorname{Ker}\varphi$. 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 $y \in \varphi\left(\varphi^{-1}(V)\right)$ entonces $y = \varphi(x)$ para algún $x \in \varphi^{-1}(V)$, lo que implica que $y = \varphi(x) \in V$. Por lo tanto $y \in \operatorname{Im}\varphi$ y $y \in V$, es decir, $y \in V \cap \operatorname{Im}\varphi$. Recíprocamente, si $y \in V \cap \operatorname{Im}\varphi$ entonces $y \in V$ y $y = \varphi(x)$ para algún $x \in M$. Entonces $x \in \varphi^{-1}(V)$ y por lo tanto $y \in \varphi\left(\varphi^{-1}(V)\right)$.

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

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

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

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "\gamma"] & B \arrow[d, "\beta"] \\ C \arrow[r, "\delta"] & D \end{tikzcd}$$

es conmutativo con γ sobre y β inyectivo, entonces:

1. $\operatorname{Im}\alpha = \beta^{-1}(\operatorname{Im}\delta)$

2. $\operatorname{Ker}\delta = \gamma(\operatorname{Ker}\alpha)$

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

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

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

(a) *φ es inyectiva.*

(b) $\operatorname{Ker}\varphi = 0$

Demostración. (a)⇒(b). Sea $x \in \operatorname{Ker}\varphi$ entonces $\varphi(x) = 0$ pero también $\varphi(0) = 0$ por ser φ R-morfismo y como φ es inyectiva entonces $x = 0$.
(b)⇒(a). Si $\varphi(x) = \varphi(y)$ se tiene que $\varphi(x - y) = 0$ entonces $x - y \in \operatorname{Ker}\varphi$ por lo tanto $x = y$ y φ es inyectiva. □

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

(a) *φ es suprayectiva.*

(b) $\operatorname{Coker}(\varphi) = 0$

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

Proposición 3.1.15. *Si $\varphi : A \to B$ 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 $B_j \subseteq \operatorname{Im}\varphi$ 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 $\operatorname{Ker}\varphi \subseteq A_i$ para todo $i \in I$, entonces se da la igualdad.*

Demostración. *1* y *2* se dejan como ejercicio.

3. $x \in \sum_{j\in J}\varphi^{-1}(B_j) \Leftrightarrow x = x_{j1} + ... + x_{jn}$ con $x_{jk} \in \varphi^{-1}(B_{jk})$ entonces $\varphi(x) = \varphi(x_{j1}) + ... + \varphi(x_{jn})$ con $\varphi(x_{jk}) \in B_{jk}$ así que $\varphi(x) \in \sum_{j\in J} B_j$ lo que implica que $x \in \varphi^{-1}(\sum_{j\in J} B_j)$. Ahora, si suponemos que $B_j \subseteq \operatorname{Im}\varphi$ para toda $j \in J$ tenemos que

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

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

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 $\operatorname{Ker}\varphi \subseteq A_i$ para toda $i \in I$ tenemos que

$$\varphi\left(\bigcap_{i\in I} A_i\right) = \varphi\left(\left(\bigcap_{i\in I} A_i\right) + \operatorname{Ker}\varphi\right) = \varphi\left(\bigcap_{i\in I}\varphi^{-1}(\varphi(A_i))\right)$$

$$= \varphi\left(\varphi^{-1}\left(\bigcap_{i\in I}\varphi(A_i)\right)\right) = \bigcap_{i\in I}\varphi(A_i) \cap \operatorname{Im}\varphi = \bigcap_{i\in I}\varphi(A_i).$$

□

3.2. Teoremas de Isomorfismo

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

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

$$m + \operatorname{Ker}\varphi = m' + \operatorname{Ker}\varphi \Leftrightarrow m - m' \in \operatorname{Ker}\varphi \Leftrightarrow \varphi(m - m') = 0$$

$$\Leftrightarrow \varphi(m) - \varphi(m') = 0 \Leftrightarrow \varphi(m) = \varphi(m').$$

Por lo tanto φ_1 está bien definida y es inyectiva. Además, φ_1 es R-morfismo ya que $\varphi_1(r(m + \operatorname{Ker}\varphi) + (n + \operatorname{Ker}\varphi)) = \varphi_1((rm + n) + \operatorname{Ker}\varphi) = \varphi(rm + n) = r\varphi(m) + \varphi(n) = r\varphi_1(m + \operatorname{Ker}\varphi) + \varphi_1(n + \operatorname{Ker}\varphi)$. Más aún, como $\operatorname{Im}\varphi = \operatorname{Im}\varphi_1$ 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 $\varphi : M \to N$ es un R-morfismo entonces $M/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$.*

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 $f : H \to (H + K)/K$ definida como $f(h) = h + K$. Entonces $\operatorname{Ker} f = \{h \in H \mid h + K = K\} = H \cap K$. 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 $f : M/K \to M/L$ 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 $m + K \in \operatorname{Ker} f \Leftrightarrow f(m + K) = L \Leftrightarrow m + L = L \Leftrightarrow m \in L$ así que $\operatorname{Ker} f = \{m + K \mid m \in L\} = L/K$. 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 $(\_ \cdot x) : R \to Rx$ multiplicar por x por la izquierda. Por el 1er Teorema de isomorfismo (Teorema 3.2.2) $M = Rx \cong R/\operatorname{Ker}(\_ \cdot x)$.
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 $\operatorname{Ker}(\_ \cdot x) = \{r \in R \mid rx = 0\}$ 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 $\varphi : M \to N$ un R-morfismo.*

1. *Sea $\alpha : M \to M'$ un epimorfismo tal que $\operatorname{Ker}\alpha \subseteq \operatorname{Ker}\varphi$. Entonces existe un único R-morfismo $\beta : M' \to N$ tal que $\varphi = \beta\alpha$.*

2. *Sea $\gamma : N' \to N$ un monomorfismo tal que $\operatorname{Im}\varphi \subseteq \operatorname{Im}\gamma$. Entonces existe un único $\delta : M \to N'$ tal que $\varphi = \gamma\delta$*

Demostración. 1. Definimos $\beta : M' \to N$ como $\beta(y) = \varphi(x)$ si $\alpha(x) = y$.Notemos que si $\alpha(x) = \alpha(x')$, entonces $x - x' \in \operatorname{Ker}\alpha \subseteq \operatorname{Ker}\varphi$. 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 $\operatorname{Ker}\alpha = \operatorname{Ker}\varphi$, y β es epi si y solo si φ es epi.

2. Definimos $\delta : M \to N'$ como $\delta(x) = y$ donde $\gamma(y) = \varphi(x)$ Notemos que si $\varphi(x) = \gamma(y')$ entonces $\gamma(y) = \gamma(y') \Leftrightarrow y - y' \in \operatorname{Ker}\gamma = \{0\}$ 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 $\operatorname{Im}\varphi = \operatorname{Im}\gamma$. □

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 $\alpha : M \to N$ se *escinde* si $\operatorname{Im}\alpha$ es un sumando directo de N.

3. Decimos que un epimorfismo $\beta : M \to N$ se *escinde* si $\operatorname{Ker}\beta$ es un sumando directo de M.

Lema 3.2.10. *Si el siguiente diagrama*

$$\begin{tikzcd} L \arrow[r, "\alpha"] \arrow[dr, "\lambda"'] & N \arrow[d, "\beta"] \\ & M \end{tikzcd}$$

es conmutativo, entonces:

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

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

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

Corolario 3.2.11. *Con el diagrama del lema anterior.*

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

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

(a) *α es mono y se escinde.*

(b) *Existe $\beta : N \to M$ tal que $\beta\alpha = Id_M$*

Demostración. (a)⇒(b). Supongamos que α es un monomorfismo y que $\operatorname{Im}\alpha \oplus N' = N$ para $N' \leq N$. Sea $\alpha_0 : M \to \operatorname{Im}\alpha$ la corresticción de α a su imagen. Como α es mono, α_0 es un isomorfismo. Sea $\rho : N \to \operatorname{Im}\alpha$ 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 $\beta\alpha = Id_M$.

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

$$\begin{tikzcd} M \arrow[r, tail, "\alpha"] \arrow[dr, "Id"'] & N \arrow[d, "\beta"'] \\ & M \end{tikzcd}$$

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

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

(a) *γ es epi y se escinde.*

(b) *Existe $\delta : L \to N$ tal que $\gamma\delta = Id_L$.*

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 $\operatorname{Ker} f_{i+1} = \operatorname{Im} f_i$ 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*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\alpha"'] & B \arrow[r, "g"] \arrow[d, "\beta"'] & C \arrow[d, "\gamma"'] \\ A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \end{tikzcd}$$

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. $b \in \operatorname{Ker} g = \operatorname{Im} f$. 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, $x - \beta(b) \in \operatorname{Ker} g' = \operatorname{Im} f'$ 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 $\beta(b) \in \operatorname{Ker} g' = \operatorname{Im} f'$. 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, loque implica que $g(b) = 0$, es decir, $b \in \operatorname{Ker} g = \operatorname{Im} f$. 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. □

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

$$\begin{tikzcd} A \arrow[r, "f_1"] \arrow[d, "\alpha"'] & B \arrow[r, "f_2"] \arrow[d, "\beta"'] & C \arrow[r, "f_3"] \arrow[d, "\gamma"'] & D \arrow[r, "f_4"] \arrow[d, "\delta"'] & E \arrow[d, "\epsilon"'] \\ A' \arrow[r, "g_1"] & B' \arrow[r, "g_2"] & C' \arrow[r, "g_3"] & D \arrow[r, "g_4"] & E' \end{tikzcd}$$

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 $c \in \operatorname{Ker} f_3 = \operatorname{Im} f_2$ 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 $\beta(b) \in \operatorname{Ker} g_2 = \operatorname{Im} g_1$. 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. $d \in \operatorname{Ker} f_4 = \operatorname{Im} f_3$. 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. $c' - \gamma(c) \in \operatorname{Ker} g_3 = \operatorname{Im} g_2$ 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*. □

Corolario 3.3.5. *Si tenemos el siguiente diagrama conmutativo*

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d, "\cong"] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d, "\cong"] & 0 \\ 0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0 \end{tikzcd}$$

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 $\operatorname{Im} f = \operatorname{Ker} g$ 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 $i : N \to M$ es la inclusión canónica dada por $i(n) = n + 0$ y $\pi : M \to L$ 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

$$0 \to \left(\begin{smallmatrix} 0 & 0 \\ K & 0 \end{smallmatrix}\right) \xrightarrow{f} R \xrightarrow{g} \left(\begin{smallmatrix} K & 0 \\ K & 0 \end{smallmatrix}\right) \to 0$$

donde $f\left(\begin{smallmatrix} 0 & 0 \\ a & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & a \end{smallmatrix}\right)$ y $g\left(\begin{smallmatrix} a & 0 \\ b & c \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & 0 \\ b & 0 \end{smallmatrix}\right)$. 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 $\varphi : M \to N$:*

(a) *φ se escinde.*

(b) *La sucesión exacta $0 \to M \xrightarrow{\varphi} N \to \operatorname{Coker} \varphi \to 0$ se escinde.*

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

(a) *φ se escinde.*

(b) *La sucesión exacta $0 \to \operatorname{Ker} \varphi \to M \xrightarrow{\varphi} N \to 0$ se escinde.*

3.4. El grupo de R-morfismos Hom_R

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

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

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

Observación 3.4.3. Dado $f \in \mathrm{Hom}_R(M,N)$ y $r \in R$, si consideramos $rf : M \to N$ 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 $srf(x) = s(rf)(x)$ 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-bimodulo* (${}_RM_S$) si M es un R-modulo izquierdo y M es un S-modulo 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 $\mathrm{M}_{n\times\ell}(K)$ es un $\mathrm{M}_n(K)$-$\mathrm{M}_\ell(K)$-bimódulo con la multiplicación de matrices.

Proposición 3.4.6. *Sea ${}_RM_S$ un R-S-bimodulo y ${}_RN$ un R-módulo. Entonces* $\mathrm{Hom}_R(M,N)$ *es un S-módulo izquierdo.*

Demostración. Sean M un R-S-bimodulo y que N es un R-modulo. Para cada $s \in S$ y $f \in \mathrm{Hom}_R(M,N)$, definimos $sf : M \to N$ 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 $sf \in \mathrm{Hom}_R(M,N)$. Por lo tanto ${}_S\mathrm{Hom}({}_RM_S, {}_RN)$ es un S-modulo izquierdo. $\square$

Teorema 3.4.7. *Para todo R-modulo M, ${}_RM \cong {}_R\mathrm{Hom}(R,M)$.*

Demostración. Como R es un R-R-bimódulo, $\mathrm{Hom}_R(R,M)$ es un R-modulo izquierdo. Definimos $\rho : M \to \mathrm{Hom}_R(R,M)$ de la siguiente manera: dado $m \in M$, $\rho(x) : R \to M$ 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

$$\rho(rm+n)(s) = s(rm+n) = srm + sn = \rho(m)(sr) + \rho(n)(s)$$

$$= (r\rho)(m)(s) + \rho(n)(s) = (r\rho(m) + \rho(n))(s).$$

Además, si $f \in \mathrm{Hom}_R(R,M)$, tomando $f(1) = x$, se tiene que $f(r) = f(r1) = rf(1) = rx$. Por lo tanto ρ es un epimorfismo. Ahora, si $\rho(x) = \overline{0}$, 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 isomorphismo. $\square$

Observación 3.4.8. Para todo R-módulo M, el grupo $\mathrm{Hom}_R(M, M)$ 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 $\mathrm{End}_R(M)$.

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

Demostración. Supongamos que M y N son R-módulos simples, si $\varphi : M \to N$ es un R-morfismo y $\varphi \neq \overline{0}$ entonces $\mathrm{Ker}\,\varphi = 0$ ya que $\mathrm{Ker}\,\varphi < M$. 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 $\mathrm{End}_R(S)$ de un R-módulo simple ${}_RS$ es un anillo con división. $\square$

Observación 3.4.10. Notemos que si M es un R-módulo tal que $\mathrm{End}_R(M)$ 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 $\mathrm{End}_{\mathbb{Z}}(\mathbb{Q}) \cong \mathbb{Q}$ (Ejercicio3.5.4).

Observación 3.4.11. Por el Teorema 3.4.7, ${}_RR \cong \mathrm{End}_R(R)$. Se puede ver que este isomorfismo cumple que si $f, g \in \mathrm{End}_R(R)$ 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 $R^{op} \cong \mathrm{End}_R(R)$.

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

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

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 $\mathrm{Hom}_R(\_, N)$ a la sucesión

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

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

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

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

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 canonica

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

Por la Proposición 3.4.13, hay una secesión exacta

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

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 ${}_KV$ y ${}_KW$ espacios vectorial sobre el campo K. Entonces $f : V \to W$ 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 $\operatorname{End}_{\mathbb{Z}}(\mathbb{Q}) \cong \mathbb{Q}$ (como anillos).

5. Sea $n \in \mathbb{Z}$. Demuestre que $\operatorname{End}_R(\mathbb{Z}_n) \cong \mathbb{Z}_n$ (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 $\varphi_1 : K \to N$ y $\varphi_2 : L \to N$. Demuestre que existe un único R-morfismo $\varphi : M \to N$ tal que $\varphi\mid_N = \varphi_1$ y $\varphi\mid_L = \varphi_2$.

9. Sean $N, L \leq M$. Demuestre que si $N \cap L = 0$ entonces M/N tiene un submódulo isomorfo a L.

10. Sea R un anillo e I un ideal izquierdo mínimo. Demuestre que $I^2 = 0$ o I es un sumando directo de R.

11. Demuestre el Corolario 3.2.13.

12. **Propiedad universal del núcleo.** Sea $\varphi : M \to N$ un R-morfismo. Suponga que existe $\psi : M' \to M$ tal que $\varphi\psi = 0$. Demuestre que existe un único R-morfismo $\overline{\psi} : M' \to \operatorname{Ker}\varphi$ tal que $i\overline{\psi} = \psi$ donde $i : \operatorname{Ker}\varphi \to M$ es la inclusión.

$$\begin{tikzcd}
& M' \arrow[dl, dashed, "\overline{\psi}"'] \arrow[d, "\psi"] \arrow[dr, "0"] & \\
\operatorname{Ker}\varphi \arrow[r, hook] & M \arrow[r, "\varphi"'] & N
\end{tikzcd}$$

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

$$\begin{tikzcd}
M \arrow[r, "\varphi"] \arrow[dr, "0"'] & N \arrow[r, two heads] \arrow[d, "\psi"] & \operatorname{Coker}\varphi \arrow[dl, dashed, "\overline{\psi}"] \\
& N' &
\end{tikzcd}$$

14. Demuestre la Observación 3.3.2.

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

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A' \arrow[r] \arrow[d] & B' \arrow[r] \arrow[d] & C' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A'' \arrow[r] \arrow[d] & B'' \arrow[r] \arrow[d] & C'' \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

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.

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

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
 & \operatorname{Ker} f \arrow[d] & \operatorname{Ker} g \arrow[d] & \operatorname{Ker} h \arrow[d] & \\
0 \arrow[r] & A \arrow[r, "\alpha"] \arrow[d, "f"] & B \arrow[r, "\beta"] \arrow[d, "g"] & C \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & A' \arrow[r, "\alpha'"] \arrow[d] & B' \arrow[r, "\beta'"] \arrow[d] & C' \arrow[r] \arrow[d] & 0 \\
 & \operatorname{Coker} f \arrow[d] & \operatorname{Coker} g \arrow[d] & \operatorname{Coker} h \arrow[d] & \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Demuestre que hay una sucesión exacta

$$0 \to \operatorname{Ker} f \to \operatorname{Ker} g \to \operatorname{Ker} h \xrightarrow{\delta} \operatorname{Coker} f \to \operatorname{Coker} g \to \operatorname{Coker} h \to 0.$$

17. Sea $0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to 0$ una sucesión exacta corta. Demuestre que son equivalentes:

    (a) La sucesión se escinde.

    (b) Existe un R-morfismo $\alpha : B \to A$ tal que $\alpha\varphi = Id_A$.

    (c) Existe un R-morfismo $\beta : C \to B$ tal que $\psi\beta = Id_C$.

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

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

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

18. Sea R un anillo. Suponga que hay una sucesión exacta corta de R-modulos

$$0 \to A \to B \to R \to 0.$$

Demuestre que la sucesión se escinde.

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

20. Demuestre la Proposición 3.4.13.

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

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

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 $e^2 = e$.

22. Sea R un anillo y $e^2 = e \in R$ un idempotente. Demuestre que si e tiene inverso entonces $e = 1$.

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

24. 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.

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

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

26. 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.

27. 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.

28. 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 $N = \bigoplus_I (N \cap A_i)$.

29. Sean M y N dos R-módulos. Considere los siguentes submódulos de M y N respectivamente.

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

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

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

30. 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).

31. Sean M y N dos D-módulos con D un dominio entero. Suponga que $t(M) = M$ y $t(N) = 0$. Demuestre que $\mathrm{Hom}_D(M, N) = 0$.

32. Sean R y S dos anillos y M un S-R-bimódulo. Considere $T = \begin{pmatrix} R & 0 \\ M & S \end{pmatrix}$ con las operaciones usuales de matrices. Demuestre lo siguiente:

    a) T es una anillo con unidad.

    b) Un subconjunto $\begin{pmatrix} A & 0 \\ B & C \end{pmatrix}$ de T es un ideal izquierdo si y solo si A es un ideal izquierdo de R, C es un ideal izquierdo de S, B es un S-submódulo de M y se cumple $MA + B \subseteq B$.

    c) Caracterice los ideales derechos de T como en el inciso anterior.

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

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

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

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

y dado $r \in R$ podemos definir la función $rf : I \to \bigcup_I M_i$ 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 $\operatorname{sop}((x_i)_I)$, como el subconjunto de I dado por

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

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

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

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

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

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

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

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

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

Dada una familia de R-módulos izquierdos $\{M_i\}_I$, para cada $j \in I$ tenemos un R-morfismo $\pi_j : \prod_I M_i \to M_j$ 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-morfismo $\{\gamma_i : C \to M_i\}_I$, existe un único R-morfismo $\gamma : C \to \prod_I M_i$ tal que $\pi_i\gamma = \gamma_i$ para todo $i \in I$.*

$$\begin{tikzcd}
\prod_I M_i \arrow[r, "\pi_j"] & M_j \\
C \arrow[u, dashed, "\gamma"] \arrow[ur, "\gamma_j"'] &
\end{tikzcd}$$

Demostración. Supongamos que C es un R-módulo y $\{\gamma_i : C \to M_i\}_I$ es una familia de R-morfismos. Definimos $\gamma : C \to \prod_I M_i$ como $\gamma(c) = (\gamma_i(c))_I$. Así, para $x, y \in C$ y $r \in R$, $\gamma(rx+y) = (\gamma_i(rx+y))_I = (r\gamma_i(x) + \gamma(y))_I = r(\gamma_i(x))_I + (\gamma_i(y))_I = r\gamma(x) + \gamma(y)$. Por lo tanto γ es un R-morfismo. Dada $j \in I$, $\pi_j(\gamma(c)) = \pi((\gamma_i(c))_I) = \gamma_j(c)$ lo que implica que $\pi_j\gamma = \gamma_j$. Por último, si $\gamma' : C \to \prod\{M_i\}_{i\in I}$ 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 $\gamma' = \gamma$ □

Dada una familia de R-módulos izquierdos $\{M_i\}_I$, para cada $j \in I$ tenemos un R-morfismo $\eta_j : M_j \to \coprod_I M_i$ al que llamamos *la inclusión canónica de* M_j definido como $\eta_j(x) = (\widehat{x_j})_I$, donde $(\widehat{x_j})_I$ 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 $\coprod_I M_i$ y las inclusiones canónicas $\{\eta_i\}_I$. Entonces para todo R-módulo B y toda familia de R-morfismos $\{\alpha_i : M_i \to B\}_I$, existe un único R-morfismo $\alpha : \coprod_I M_i \to B$ tal que $\alpha\eta_i = \alpha_i$ para todo $i \in I$.*

$$\begin{tikzcd}
M_j \arrow[r, "\eta_j"] \arrow[dr, "\alpha_j"'] & \coprod_I M_i \arrow[d, dashed, "\alpha"] \\
& M_j
\end{tikzcd}$$

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

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

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

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

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 $\eta_i : M_i \to \coprod_I M_i$. Definimos $\widehat{M_i} := \eta(M_i) = \{(\widehat{x_i})_I | x_i \in M_i\}$. 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 $\sum_{i\in\mathrm{sop}(x_i)}(\widehat{x_i})_I = \sum_{i\in\mathrm{sop}(x_i)} \eta_i(x_i)$ así que $(x_i)_I \in \sum_{i\in\mathrm{sop}(x_i)} \widehat{M_i} \subseteq \sum_I \widehat{M_i}$. Por lo tanto $\coprod M_i \subseteq \sum_I \widehat{M_i}$. 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 tambien $x_j = 0$ 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 $\{\alpha_i : A_i \to B_i\}_I$ una familia de R-morfismos. Entonces:*

1. *Existe un único morfismo* $\prod \alpha_i : \prod_I A_i \to \prod_I B_i$ *dado por* $\prod \alpha_i((a_i)_I) = (\alpha(a_i))_I$.

2. *Existe un único morfismo* $\bigoplus \alpha_i : \bigoplus_I A_i \to \bigoplus_I B_i$ *dado por* $\bigoplus \alpha_i((a_i)_I) = (\alpha_i(a_i))_I$.

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

$$\begin{tikzcd}
\prod_I B_i \arrow[r, "\pi_j^B"] & B_j \\
\prod_I A_i \arrow[r, "\pi_j^A"'] \arrow[u, dashed] & A_j \arrow[u, "\alpha_j"']
\end{tikzcd}$$

Por la Propiedad universal del producto (Teorema 4.1.3), existe un único R-morfismo $\prod \alpha_i : \prod_I A_i \to \prod_I B_i$ 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 $\eta_i^B : B_i \to \bigoplus_I B_i$ las inclusiones canónicas. Entonces para cada $j \in I$ tenemos un R-morfismo $\eta_j^B \alpha_j : A_j \to \bigoplus_I B_i$.

$$\begin{tikzcd}
A_j \arrow[r, "\eta_j^A"] \arrow[d, "\alpha_j"'] & \bigoplus_I A_i \arrow[d, dashed] \\
B_j \arrow[r, "\eta_j^B"'] & \bigoplus_I B_i
\end{tikzcd}$$

Por la Propiedad universal de la suma direct (Teorema 4.1.4), existe un único R-morfismo $\bigoplus_I \alpha_i : \bigoplus_I A_i \to \bigoplus_I B_i$ 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* $\{0 \to A_i \xrightarrow{\alpha_i} B_i \xrightarrow{\beta_i} C_i \to 0\}_I$ *una familia de sucesiones exactas en* R*-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 Proposión 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, $\operatorname{Im} \prod_I \alpha_i \subseteq \operatorname{Ker} \prod_I \beta_i$. Ahora sea $(b_i)_I \in \operatorname{Ker} \prod_I \beta_i$. Entonces $0 = \prod_I \beta_i((b_i)_I) = (\beta_i(b_i))_I$. Esto implica que para cada $j \in I$, $b_j \in \operatorname{Ker} \beta_j$. 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 $\operatorname{Im} \prod_I \alpha_i = \operatorname{Ker} \prod_I \beta_i$. Sea $(c_i)_I \in \prod_I C_i$. Como $\beta_i : B_i \to C_i$ 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). □

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:*

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

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

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

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

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

dado por $\alpha(\varphi) = (\alpha_i(\varphi))_I = (\varphi\eta_i)_I$. Veamos que α es un isomorfismo. Sean $\varphi, \psi \in \operatorname{Hom}_R\left(\bigoplus_I M_i, N\right)$. 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 $(\beta_i)_I \in \prod_I \operatorname{Hom}_R(M_i, N)$. Entonces tenemos para cada $i \in I$, $\beta_i : M_i \to N$. Por la Propiedad universal de la suma directa (Teorema 4.1.4) existe un único morfismo $\beta \in \operatorname{Hom}_R\left(\bigoplus_I M_i, N\right)$ 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. □

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

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

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 $\operatorname{Hom}_{\mathbb{Z}}\left(\prod_{p \in \mathbb{P}} \mathbb{Z}_p, \mathbb{Q}\right) \neq 0$ pero $\prod_{p \in \mathbb{P}} \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}_p, \mathbb{Q}) = 0$, 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:*

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

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

$$\mathrm{Hom}_{\mathbb{Z}}\left(M, \bigoplus_{n>0} \mathbb{Z}_{p^n}\right) \ncong \bigoplus_{n>0} \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z}_{p^n}).$$

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

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

(I) *Existe un subconjunto finito I_0 de I tal que ${}_RR = \bigoplus_{I_0} A_j$.*

(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 $e_ie_j = \begin{cases} e_i & i = j \\ 0 & i \neq j \end{cases}$.*

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

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

(II). Tenemos que $1 = e_1 + ... + e_n$ con $e_i \in A_i$. Multiplicando por e_j, se tiene que $e_j = e_1e_j + ... + e_ne_j$. Así,

$$0 = e_j - e_je_j = e_je_1 + ... + e_je_{j-1} + e_je_{j+1} + ... + e_je_n.$$

Como cada $e_je_i \in A_i$ y la suma es directa, cada sumando tiene que ser cero, es decir, $e_je_i = \begin{cases} e_i & i = j \\ 0 & i \neq j \end{cases}$. Ahora, si $a_j \in A_j$ entonces $a_j = a_je_1 + ... + a_je_n = a_je_j$ así que $A_j \subseteq A_je_j \subseteq Re_j \subseteq A_j$. Por lo tanto $A_j = Re_j$.

(III). Sea $r \in R$, tenemos que $r = \sum re_j = \sum e_jr$. Como A_j es bilateral $re_j, e_jr \in A_j$. Lo que implica que $re_j = e_jr$. Por otro lado, si e_i es central, entonces $Re_i = e_iRe_i$ 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 ${}_RR = \sum Re_i$. Supongamos que $r \in Re_i \cap \sum_{i\neq j} Re_j$ entonces $r = r_ie_i = \sum_{i\neq j} r_je_j$ lo que implica que $re_i = re_ie_i = \sum_{i\neq j} r_je_je_i$. Como los $e_i's$ son idempotentes ortgonales $r = re_i = 0$. Por lo tanto $\bigoplus Re_i = {}_RR$. Si cada e_i es central $(Re_i)r = Rre_i \subseteq Re_i$. Por lo tanto Re_i es ideal derecho. □

4.2. Producto Fibrado y Coproducto Fibrado

Considere el siguiente diagrama conmutativo de R-morfismos

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "\varphi"'] & B \arrow[d, "\beta"] \\ M \arrow[r, "\psi"] & N. \end{tikzcd}$$

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 $\varphi' : Y \to M$, $\alpha' : Y \to B$ existe un único $\tau : Y \to A$ tal que $\varphi' = \varphi\tau$ y $\alpha' = \alpha\tau$.

$$\begin{tikzcd} Y \arrow[dr, dashed, "\tau"] \arrow[drr, "\alpha'"] \arrow[ddr, "\varphi'"'] & & \\ & A \arrow[r, "\alpha"] \arrow[d, "\varphi"'] & B \arrow[d, "\beta"] \\ & M \arrow[r, "\psi"] & N \end{tikzcd}$$

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

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "\varphi"'] & B \arrow[d, "\beta"] \arrow[ddr, "\beta'"] & \\ M \arrow[r, "\psi"] \arrow[drr, "\psi'"'] & N \arrow[dr, dashed, "\sigma"] & \\ & & X \end{tikzcd}$$

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*

$$\begin{tikzcd} & M \arrow[d, "0"] \\ N \arrow[r, "0"'] & 0. \end{tikzcd}$$

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

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

$$\begin{tikzcd}
Y \arrow[dr, dashed, "\tau"] \arrow[drr, "\alpha"] \arrow[ddr, "\varphi"'] & & \\
& M \times N \arrow[r, "\pi_1"] \arrow[d, "\pi_2"] & M \arrow[d, "0"] \\
& N \arrow[r, "0"'] & 0.
\end{tikzcd}$$

$\square$

Teorema 4.2.3. *Tomemos el ángulo* (ψ, β)

$$\begin{tikzcd}
& B \arrow[d, "\beta"] \\
M \arrow[r, "\psi"'] & N.
\end{tikzcd}$$

Sea $A := \{(m, b) \mid m \in M\ b \in B$ *y* $\psi(m) = \beta(b)\}$ *y sean* $\varphi : A \to M$ *y* $\alpha : A \to B$ *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 $\varphi' : Y \to M$ y $\alpha' : Y \to B$ morfismos tales que $\beta\alpha' = \psi\varphi'$. Definimos $\tau : Y \to A$ 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 $\varphi\tau(y) = \varphi(\varphi'(y), \alpha'(y)) = \varphi'(y)$ asi que $\alpha\tau = \alpha'$ y $\varphi\tau = \varphi'$.

Supongamos que tenemos $\tau' : Y \to A$ 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 $(\tau - \tau') = 0$. $\square$

Teorema 4.2.4. *Tomemos el ángulo* (φ, α)

$$\begin{tikzcd}
A \arrow[r, "\alpha"] \arrow[d, "\varphi"'] & B \\
M. &
\end{tikzcd}$$

Sea $N = (M \oplus B)/U$ *con* $U := \{(\varphi(a), -\alpha(a)) \mid a \in A\}$ *y sean* $\psi : M \to N$ *y* $\beta : B \to N$ *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 $\psi' : M \to X$ y $\beta' : B \to X$ morfismos tales que $\beta'\alpha = \psi'\varphi$. Definimos $\sigma : N \to X$ 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 $\sigma' : N \to X$ 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 $\{\overline{(m,0)}, \overline{(0,b)} \mid m \in M\ b \in B\}$ generan N entonces $(\sigma - \sigma') = 0$. □

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 $\operatorname{Im}\psi$ es un sumando directo de N si y sólo si existe $\kappa : B \to M$ tal que $\varphi = \kappa\alpha$.*

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "\varphi"'] & B \arrow[d, "\beta"] \arrow[dl, dashed, "\kappa"'] \\ M \arrow[r, "\psi"] & N \end{tikzcd}$$

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 $N = \operatorname{Im}\psi \oplus N_0$. Entonces ψ tambien es un monomorfismo, así que ψ induce un isomorfismo $\psi_0 : M \to \operatorname{Im}\psi$. Sea $\pi : N \to \operatorname{Im}\psi$ 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 $\kappa : B \to M$ tal que $\kappa\alpha = \varphi$. Tomemos $\xi : N \to M$ 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, $\xi\psi = Id_M$. Entonces por el Corolario 3.2.11.(*3*), $N = \operatorname{Im}\psi \oplus \operatorname{Ker}\xi$. □

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 $\operatorname{Ker}\alpha$ es un sumando directo de A si y sólo si existe $\kappa : B \to M$ tal que $\beta = \psi\kappa$.*

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "\varphi"'] & B \arrow[d, "\beta"] \arrow[dl, dashed, "\kappa"'] \\ M \arrow[r, "\psi"] & N \end{tikzcd}$$

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

$$\begin{tikzcd}
0 \arrow[r] & K \arrow[r, "\tau"] \arrow[d, "1"] & A \arrow[r, "\alpha"] \arrow[d, "\varphi"] & B \arrow[r] \arrow[d, "\beta"] & 0 \\
0 \arrow[r] & K \arrow[r, "\xi"'] & M \arrow[r, "\psi"'] & N \arrow[r] & 0,
\end{tikzcd}$$

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 $\tau : K \to A$ tal que $\tau(k) = (\xi(k), 0)$. Porlo tanto $\varphi\tau = \xi$ y $\alpha\tau = 0$, lo que nos dice también que $\operatorname{Im}\tau \subseteq \operatorname{Ker}\alpha$. 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, $\tau(k) = (\xi(m), 0) = (m, b)$, y así $\operatorname{Ker}\alpha = \operatorname{Im}\tau$. 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 ${}_SU$ un S-módulo izquierdo. Consideremos $A \times U$ (como conjunto) y tomemos el $\mathbb{Z}$-módulo $F = \mathbb{Z}^{(A\times U)}$. Sean $\{\eta_{(a,u)} : \mathbb{Z} \to F \mid (a,u) \in A \times U\}$ 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 $\operatorname{sop}(x) = \{(a_1,u_1),(a_2,u_2),...,(a_n,u_n)\}$. 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:

$$D_1 = \{(a_1 + a_2, u) - (a_1, u) - (a_2, u) \mid a_1, a_2 \in A\ u \in U\}$$

$$D_2 = \{(a, u_1 + u_2) - (a, u_1) - (a, u_2) \mid a \in A\ u_1, u_2 \in U\}$$

$$T = \{(as, u) - (a, su) \mid a \in A\ u \in U\ s \in S\}$$

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 ${}_SU$ 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 $(a_1 + a_2, u) - (a_1, u) - (a_2, u) \in K$. Analogamente se tienen *2* y *3*. Los incisos *4* y *5* los dejamos como ejercicio 4.4.15. Para *6*, si $z > 0$, entonces $z(a \otimes u) = (a \otimes u) + (a \otimes u) + \cdots + (a \otimes u)$ (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, ${}_SU$ un S-módulo izquierdo y M un grupo abeliano. Una función $\varphi : A\times U \to M$ 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 ${}_SU$ un S-módulo izquierdo, podemos considerar la siguiente función

$$A\times U \overset{i}{\hookrightarrow} F \overset{\pi}{\twoheadrightarrow} A\otimes_S U := F/K$$

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

Proposición 4.3.6. *Sean A_S un S-módulo derecho y ${}_SU$ un S-módulo izquierdo. Entonces $\tau : A\times U \to A\otimes_S U$ es S-tensorial. Además, para todo $\mathbb{Z}$-morfismo $\lambda : A\otimes_S U \to M$ 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, ${}_SU$ un S-módulo izquierdo y M un grupo abeliano, denotemos por $\mathrm{Tens}_S(A\times U, M)$ a la colección de funciones S-tensoriales.

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

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

de $\mathbb{Z}$-módulos.

Demostración. Dados $\lambda, \zeta \in \mathrm{Tens}_S(A \times U, M)$, definimos $(\lambda+\zeta)(a,u) = \lambda(a,u)+\zeta(a,u)$. Claramente esta operación hace a $\mathrm{Tens}_S(A \times U, M)$ un grupo abeliano. Definimos $\Phi : \mathrm{Hom}_{\mathbb{Z}}(A \otimes_S U, M) \to \mathrm{Tens}_S(A \times U, M)$ como $\Phi(\lambda) = \lambda\tau$ la cual está bien definida por la Proposición4.3.6. Sean $\lambda, \zeta \in \mathrm{Hom}_{\mathbb{Z}}(A \otimes_S U, M)$. Entonces

$$\Phi(\lambda + \zeta)(a, u) = (\lambda + \zeta)\tau(a, u) = (\lambda + \zeta)(a \otimes u) = \lambda(a \otimes u) + \zeta(a \otimes u)$$

$$= \lambda\tau(a, u) + \zeta\tau(a, u) = \Phi(\lambda)(a, u) + \Phi(\zeta)(a, u).$$

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 $\varphi \in \mathrm{Tens}_S(A \times U, M)$. Como $A \times U$ es base de F entonces existe un único $\mathbb{Z}$-morfismo $\overline{\varphi} : F \to M$, dado como $\overline{\varphi}\left(\sum_{i=1}^{n} z_i(a_i, u_i)\right) = \sum_{i=1}^{n} z_i\varphi(a_i, u_i)$. Ahora, como φ es S-tensorial se tiene que $K \subseteq \mathrm{Ker}\,\varphi$ (Definición 4.3.1), lo que implica que existe $\lambda : A \otimes_S U \to M$ tal que $\lambda\pi = \overline{\varphi}$. Por lo tanto $\lambda\tau = \varphi$ y así Φ es suprayectiva.

$$\begin{tikzcd}
A \times U \arrow[r, hook] \arrow[d, "\varphi"'] & F \arrow[r, two heads, "\pi"] \arrow[dl, dashed, "\exists\overline{\varphi}"'] & A \otimes_S U \arrow[dll, dashed, "\exists\lambda"] \\
M & &
\end{tikzcd}$$

Por lo tanto Φ es un isomorfismo. $\square$

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

$$\begin{tikzcd}
A \times U \arrow[r, "\tau"] \arrow[d, "\varphi"'] & {}_{\mathbb{Z}}T \arrow[dl, dashed, "\exists!\lambda"] \\
{}_{\mathbb{Z}}M &
\end{tikzcd}$$

Demostración. La prueba se sigue de la Proposición 4.3.7. $\square$

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

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

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

1. $Id_A \otimes Id_U = Id_{A \otimes_S U}$.
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 ${}_SU$ S-módulos. Supongamos que además ${}_RA$ 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

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

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 ${}_SU_T$ 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 ${}_RA_S$, ${}_SU$ y ${}_RM$. Si $\varphi : A \times U \to M$ 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 $\lambda : A \otimes_S U \to M$ tal que $\lambda\tau = \varphi$.*

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

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

□

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

Demostración. Definimos $\varphi : S \times U \to U$ 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 $\lambda : S \otimes_S U \to U$ 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 $\lambda\left(\sum s_i \otimes u_i\right) = 0$, 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. □

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, ${}_RM_S$ y ${}_SU$.

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

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

como

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

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

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

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 $\zeta : (A \otimes_R M) \otimes_S U \to A \otimes_R (M \otimes_S U)$ 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.

□

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*

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

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

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

como

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

Entonces existe un único morfismo $\lambda : A \otimes U \to \bigoplus_I (A_i \otimes U)$ 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 $\lambda_i : A_i \otimes_S U \to A \otimes_S U$. Por la propiedad universal de la suma directa (Teorema 4.1.4), existe un único morfismo

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

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

$$\zeta\lambda\left(\sum((a_{i_k})_I)_k \otimes u\right) = \zeta\left(\sum\left((a_{i_k} \otimes u)_k\right)\right)$$

$$= \sum\sum_I \iota_{i_k}(a_{i_k}) \otimes u = \sum((a_{i_k})_I)_k \otimes u.$$

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

$$\lambda\zeta((a_i \otimes u)_I) = \lambda\left(\sum_I (\iota_i(a_i) \otimes u)\right) = \sum_I \lambda(\iota_i(a_i) \otimes u)$$

$$= \sum_I \mu_i(a_i \otimes u) = (a_i \otimes u)_I$$

donde $\mu_i : A_i \otimes_S U \to \bigoplus_I (A_i \otimes_S U)$ es la inclusión canónica. Por lo tanto λ es un isomorfimo. 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

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

$\square$

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

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

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 monomorfimo $\varphi : \mathbb{Z} \to \prod_{p\in\mathbb{P}} \mathbb{Z}_p$. Afirmamos que

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

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, $c_1, ..., c_\ell$ tales que

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

$$= \sum_{i=1}^{\ell} 1 \otimes ([c_i a_i n_i]_p)_{\mathbb{P}} = \sum_{i=1}^{\ell} 1 \otimes \varphi(c_i a_i n_i) = 1 \otimes \varphi \left(\sum_{i=1}^{\ell} c_i a_i n_i \right).$$

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 $\varphi : \mathbb{Z} \to \prod_{p\in\mathbb{P}} \mathbb{Z}_p$.

3. ¿Existe un monomorfismo $\varphi : \mathbb{Z} \to \bigoplus_{p\in\mathbb{P}} \mathbb{Z}_p$?

4. Sea $\varphi : M \to \prod_I N_i$ un R-morfismo. Demuestre que si $\pi_i\varphi = 0$ para todo $i \in I$, entonces $\varphi = 0$, donde $\pi_i : \prod_I N_i \to N$ son las proyecciones canónicas.

5. Sea $\varphi : \bigoplus_I M_i \to N$ un R-morfismo. Demuestre que si $\varphi\eta_i = 0$ para todo $i \in I$, entonces $\varphi = 0$, donde $\eta_i : M_i \to \bigoplus_I M_i$ 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 $\{M_1, M_2, ..., M_n\}$ 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 $i : L \to M$ y $j : N \to M$. 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:
$$\begin{tikzcd} 0 \arrow[r] \arrow[d] & M \\ N & \end{tikzcd}$$

12. Sea $0 \to A \overset{\alpha}{\to} B \overset{\xi}{\to} C \to 0$ una sucesión exacta corta y $\varphi : A \to M$ un R-morfismo. Demuestre que el coproducto fibrado (ψ, β) de (φ, α) determina el siguiente diagrama conmutativo con renglones exactos
$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\alpha"] \arrow[d, "\varphi"'] & B \arrow[r, "\xi"] \arrow[d, "\beta"'] & C \arrow[r] \arrow[d, "1"'] & 0 \\ 0 \arrow[r] & M \arrow[r, "\psi"'] & N \arrow[r] & C \arrow[r] & 0. \end{tikzcd}$$

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, ${}_SU$ y ${}_SV$ S-módulos, $\alpha \in \mathrm{Hom}_S(A,B)$ y $\mu \in \mathrm{Hom}_S(U,V)$. Demuestre que la función $\varphi : A \times U \to B \otimes_S V$ 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
$$N \otimes_S \prod_I M_i \to \prod_I N \otimes_S M_i.$$

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 submodulo $L \leq M$ que es máximo con la propiedad de $N \cap L = 0$.

Proposición 5.1.2. *Sea M un modulo 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. □

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 $n.m \neq 0$ entonces $\mathbb{Z}m \cap \mathbb{Z}n = \mathbb{Z}[m;n] \neq 0$ donde $[m;n]$ denota el mínimo común multiplo. 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)⇒(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)⇒(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 $N \leq_e M$. □

Proposición 5.1.6. *Sea M un modulo 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 $U \oplus N \leq_e M$. □

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 $\varphi : M \to N$ 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 $U \subseteq \operatorname{Ker} \varphi \subseteq \varphi^{-1}(0) \subseteq \varphi^{-1}(B)$. Así $U = \varphi^{-1}(B) \cap U = 0$ y por lo tanto $\varphi^{-1}(B) \leq_e M$. □

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 $m = m_{i_1} + .. + m_{i_k}$ con $m_{ij} \in M_{ij}$. 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 $A_1 + A_2 = A_1 \oplus A_2$. 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 $m_i = m_1 + ... + m_{i-1}$ con $m_j \in M_j$. Entonces existe $0 \neq r \in R$ tal que $0 \neq r(m_1 + \cdots + m_{i-1}) \in A_1 + \cdots + A_{i-1}$. Así $rm_i \in M_i \cap (A_1 \oplus \cdots \oplus A_{i-1})$. Entonces, existe $0 \neq s \in R$ tal que $0 \neq srm_i \in A_i$ lo que implica que $srm_i \in A_i \cap A_1 \oplus \cdots \oplus A_{i-i}$. Así $srm_i = 0$ que es una contradicción. Por lo tanto $m_i = 0$. Esto implica que $\sum_I M_i = \bigoplus_I M_i$. □

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 $\bigoplus_I A_i \leq_e M$. □

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)⇒(b). Se tiene por el Corolario 5.1.10.

(b)⇒(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)⇒(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 $B \cap M_i \leq_e M$. □

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'. □

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 extenciones 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 extenciones esenciales distintas de N dentro de M, entonces N es un p.c. de un p.c. de él. □

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 $x \in U$ asi 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. □

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 ($N << M$) 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 $A \cap B << B$.*

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

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 $(A^\bullet \cap A^{\bullet\bullet}) << A^{\bullet\bullet} < M$. Entonces $(A^\bullet \cap A^{\bullet\bullet}) << M$ 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 $A^{\bullet\bullet}$. □

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 ${}_{\mathbb{Z}}\mathbb{Q}$ si $(\mathbb{Z}q_1+...+\mathbb{Z}q_n)+U = \mathbb{Q}$ entonces $\{q_1, ..., q_n\} \cup U$ 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 ${}_{\mathbb{Z}}\mathbb{Q}$:
$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid p \nmid b \right\}.$$
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 $B << M$ entonces $A << N$.*

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

3. *Si $A << M$ y $\varphi \in \operatorname{Hom}_R(M, N)$ entonces $\varphi(A) << N$.*

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 $B << M$ 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, $A << N$.

2. Por inducción. Si $n = 1$, se tiene el resultado por hipótesis. Supongamos que la afirmación es valida para $n > 1$ y que $A_1 + ... + A_{n-1} << M$. Si $(A_1 + ... + A_{n-1} + A_n) + U = M$ con $U \leq M$ entonces $(A_1 + ...A_{n-1}) + (A_n + U) = M$. Por hipótesis de inducción, $A_n + U = M$ y como $A_n << M$ 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 $A << M$, $\varphi^{-1}(U) = M$ lo que implica que $\varphi(M) = \varphi\varphi^{-1}(U) = U \cap \operatorname{Im}\varphi$, así que $\varphi(A) \subseteq U$. Entonces $N = \varphi(A) + U = U$ y por lo tanto $\varphi(A) << N$. □

Lema 5.1.26. *Sea M un modulo. 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. $\Rightarrow\rfloor$ 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.

$\Leftarrow\rfloor$ 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. □

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 perdida 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 $\phi \in \Gamma$. 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 lo 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 submodulos simples.*

(c) *M es suma directa de submodulos 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 submodulos simples de U. Por hipótesis $M = U_0 \oplus V$, usando la ley modular $U = U \cap M = U \cap U_0 \oplus V = U_0 \oplus (V \cap U)$. 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. Más adelante probaremos, en el Teorema 5.2.12, que no es necesario especificar el lado en la definición anterior.

Ejemplo 5.2.6. Sea K un campo. Entonces $\mathrm{M}_2(K)$ es semisimple. De hecho $\mathrm{M}_2(K) = \left(\begin{smallmatrix} K & 0 \\ K & 0 \end{smallmatrix}\right) \oplus \left(\begin{smallmatrix} 0 & K \\ 0 & K \end{smallmatrix}\right)$ (Ejemplo 2.1.4.II.). Por otro lado $\mathrm{TI}_2(K)$ no es semisimple, el ideal izquierdo $\left(\begin{smallmatrix} 0 & 0 \\ K & 0 \end{smallmatrix}\right)$ no es un sumando directo.

Corolario 5.2.7. *1. Todo submodulo 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 $\varphi : M \to N$ 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. □

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 $I_0 \subseteq I$ I_0 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)⇔(b) Es clara.

(b)⇒(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)⇒(b) Supongamos que $M = Rx_1 + Rx_2 + \cdots + Rx_n$. Como M es semisimple, cada Rx_i también lo es. Si $Rx_i = \bigoplus_J S_j$ con S_j simple, escribimos $x_i = x_{j_1} + \cdots + x_{j_\ell}$ 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)⇒(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 $A_1 \supseteq A_1 \cap A_2 \supseteq \cdots \supseteq \bigcap_{i=1}^n A_i \supseteq \cdots$. 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 $l_1, .., l_n > 0$ tales que

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

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

(d)⇒(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 submodulo de la forma $\bigoplus_{\mathbb{N}} S_i$. Tomemos para cada $i \in \mathbb{N}$ $A_i = \bigoplus_{j>i} S_j$. Si $0 \neq x \in \bigoplus_{\mathbb{N}} S_i$ $x = s_{i_1} + ... + s_{i_k}$ así que $x \in \bigoplus_{i=1}^{l} S_i$

(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 $\{i_1, ..., i_m\}$ tal que $\bigcap_{j=1}^{m} A_{i_j} = 0$, contradicción. Por lo tanto I es finito. □

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

Lema 5.2.11. *Sea M semisimple, $\{\Omega_j\}_J$ las clases de isomorfismo de submodulos 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 esta 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. □

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)⇒(b). Tenemos que ${}_R R = \bigoplus_{i=1}^n S_i$ con S_i simple. Por la Proposición 4.1.12 ${}_R R = \bigoplus_{i=1}^n Re_i$ con los e_i idempotentes ortogonales. Ahora $1 = e_1 + ... + e_n$, entonces $r = e_1 r + ... + e_n r$ para cada $r \in R$. Así que $\sum_{i=1}^n e_i R = R$. Si $e_i r_i = \sum_{i\neq j} e_j r_j$ 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 $a = er_1$ para algún $r_1 \in R$. Definimos $\varphi : Re \to Ra$ 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 $\psi : Ra \oplus U \to R$ como $\psi(ra + u) = \varphi^{-1}(ra)$ que es morfismo y $\psi(a) = e$. Como $\psi \in \mathrm{End}({}_R R)$ 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. □

5.3. Radical y zoclo

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

1.

$$\sum_{A<<M} A = \bigcap \{B < M \mid B \textit{ máximo}\}$$

$$= \bigcap \{\operatorname{Ker}\varphi \mid \varphi \in \operatorname{Hom}_R(M, N) \textit{ con } N \textit{ semisimple}\}.$$

2.

$$\bigcap_{A \leq_e M} A = \sum \{B \leq M \mid B \textit{ simple}\}$$

$$= \sum \{\operatorname{Im}\varphi \mid \varphi \in \operatorname{Hom}_R(N, M) \textit{ con } N \textit{ semisimple}\}.$$

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

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

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

$$\bigcap \{\operatorname{Ker}\varphi \mid \varphi \in \operatorname{Hom}_R(M, N) \text{ con } N \text{ semisimple}\} \subseteq \bigcap \{\operatorname{Ker}\pi_B \mid B \text{ máximo}\}$$

$$= \bigcap \{B < M \mid B \text{ máximo}\}.$$

Si $A << M$ y $\varphi : M \to N$ es un morfismo, entonces $\varphi(A) << N$. 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

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

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

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

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

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

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 $\operatorname{Rad}(M)$.

2. El submódulo dado en el Teorema 5.3.1.*2* es llamado el *zoclo* de M y se denota $\operatorname{Zoc}(M)$.

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

1. *$Rm << M$ si y sólo si $m \in \operatorname{Rad}(M)$.*

2. *$\operatorname{Zoc}(M)$ 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 $\operatorname{Rad}(\mathbb{Q}) = \mathbb{Q}$. Es decir, $\mathbb{Q}$ no tiene submódulos máximos. Por otro lado, $\operatorname{Zoc}(\mathbb{Q}) = 0$.

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

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

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

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

Teorema 5.3.6. *Sean M y N R-módulos.*

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

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

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

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

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

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

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

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

$$\operatorname{Rad}\left(\frac{M}{\operatorname{Rad}(M)}\right) = \bigcap\{B/\operatorname{Rad}(M) \mid B \leq M \text{ máximo}\}$$

$$= \frac{\bigcap\{B \mid B \text{ máximo}\}}{\operatorname{Rad}(M)} = \frac{\operatorname{Rad}(M)}{\operatorname{Rad}(M)} = 0.$$

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

3. Por el Corolario 5.3.3.*2*.

□

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

- *I.* $\operatorname{Rad}(C) \leq \operatorname{Rad}(M)$
- *II.* $\operatorname{Zoc}(C) \leq \operatorname{Zoc}(M)$

2. Si $M = \bigoplus_I M_i$ *entonces*

- *I.* $\operatorname{Rad}(M) = \bigoplus_I \operatorname{Rad}(M_i)$
- *II.* $\operatorname{Zoc}(M) = \bigoplus_I \operatorname{Zoc}(M_i)$
- *III.* $M/\operatorname{Rad}(M) \cong \bigoplus_I (M_i/\operatorname{Rad}(M_i))$

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

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

2.II. Es análoga a la anterior.

2.III. Definimos el siguiente morfismo

$$\varphi : M/\operatorname{Rad}(M) \to \bigoplus_I (M_i/\operatorname{Rad}(M_i))$$

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

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

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

3. $\operatorname{Rad}(R)$ *es un ideal bilateral.*

4. Si M *es f.g. entonces* $\operatorname{Rad}(M) << M$.

5. Si M *es f.g. y* $A \subseteq \operatorname{Rad}(R)$ *entonces* $AM << M$. *(Nakayama)*

6. Si $0 \neq M$ *es f.g. entonces* $\operatorname{Rad}(M) < M$.

7. Si $C \leq M$ *entonces* $\frac{C+\operatorname{Rad}(M)}{C} \subseteq \operatorname{Rad}(M/C)$.

Demostración. 1. Es clara por el Corolario 5.3.7.*2.I.*

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

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

3. Es inmediata del inciso *2.*

4. Por la Proposición 5.3.5.

5. Sea $A \subseteq \operatorname{Rad}(R)$. Entonces

$$AM \subseteq \operatorname{Rad}(R)M \subseteq \operatorname{Rad}(M) << M.$$

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

7. Tomemos $\pi : M \to M/C$ la proyección canónica. Entonces $\pi(\operatorname{Rad}(M)) = \frac{C+\operatorname{Rad}(M)}{C} \subseteq \operatorname{Rad}(M/C)$. □

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

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

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* $\operatorname{Rad}(M) = 0$.

Demostración. $\Rightarrow$. Por la Proposición 5.3.8, $\operatorname{Rad}(M) = 0$. 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, $B \cap C << B$ así que $B \cap C << M$. Tenemos que $\operatorname{Rad}(M) = 0$, entonces $B \cap C = 0$. Por lo tanto $M = C \oplus B$. Es decir, todo submodulo es sumando directo. □

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

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

(a) $\operatorname{Rad}(R)M = \operatorname{Rad}(M)$ *para todo* R*-módulo* M.

(b) *Sea* M *un* R*-módulo. Si* $\operatorname{Rad}(R)M = 0$ *entonces* $\operatorname{Rad}(M) = 0$.

(c) $\operatorname{Rad}(\overline{M}) = 0$ *para todo* $\overline{R}$*-módulo* $\overline{M}$.

Demostración. (a)⇒(b). Es clara.

(b)⇒(c). Sea $\overline{M} \in \overline{R}$-Mod. Consideremos el morfismo canónico de anillos $\rho : R \to \overline{R}$. Entonces $\overline{M}$ es un R-módulo, así $\mathrm{Rad}(R)\overline{M} = 0$ lo que implica que $\mathrm{Rad}({}_R\overline{M}) = 0$ pero $0 = \mathrm{Rad}({}_R\overline{M}) = \mathrm{Rad}({}_{\overline{R}}\overline{M})$.

(c)⇒(a). Sea M un R-módulo y consideremos el R-módulo $\frac{M}{\mathrm{Rad}(R)M}$. Como $\mathrm{Rad}(R)(\frac{M}{\mathrm{Rad}(R)M}) = 0$ entonces $\frac{M}{\mathrm{Rad}(R)M}$ es un $\overline{R}$-módulo y tiene los mismos submódulos que como R-módulo. Por hipótesis, $\mathrm{Rad}({}_{\overline{R}}\frac{M}{\mathrm{Rad}(R)M}) = 0$ así que $\mathrm{Rad}({}_R(\frac{M}{\mathrm{Rad}(R)M})) = 0$. Por el Teorema 5.3.6.*2*, $\mathrm{Rad}(M) \subseteq \mathrm{Rad}(R)M$. □

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

1. $A << R$
2. $A \subseteq \mathrm{Rad}(R)$
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* ⇒ *2*. Es clara.

2 ⇒ *1*. Por la Proposición 5.3.8.*4*, $\mathrm{Rad}(R) << R$ y como $A \subseteq \mathrm{Rad}(R)$ entonces $A << R$.

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

3 ⇒ *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 ⇒ *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 $A << R$. □

Observación 5.3.14. Tambien se tiene la version para ideales derechos del lema anterior.

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

Demostración. Por la Proposicion 5.3.8.*4*, $\mathrm{Rad}({}_RR) << {}_RR$, así que por el Lema 5.3.13, para todo $a \in \mathrm{Rad}({}_RR)$ $1 - a$ tiene inverso. Como $\mathrm{Rad}({}_RR)$ es un ideal bilateral, por la Observacion 5.3.14, $\mathrm{Rad}({}_RR) << R_R$. Por lo tanto $\mathrm{Rad}({}_RR) \subseteq \mathrm{Rad}(R_R)$. Por simetría se tiene la igualdad. □

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

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

Demostración. Sea ${}_SM$ 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 ${}_SN \leq {}_SM$, entonces ${}_RN \leq {}_RM$. Ahora si ${}_RL \leq {}_RM$, dado $s \in S$ y $l \in L$ entonces $sl = rl \in L$ donde $r \in R$ es tal que $\varphi(r) = s$. □

Teorema 5.3.18. *Sea R un anillo tal que $\frac{R}{\operatorname{Rad}(R)}$ es s.s. Entonces:*

1. *Todo simple izq. (resp. der.) es isomorfo a un submodulo izq. (resp. der.) de $\frac{R}{\operatorname{Rad}(R)}$.*
2. *El numero de bloques de $\frac{R}{\operatorname{Rad}(R)}$ es finito e igual al numero de clases de isomorfismo de modulos simples izq. (resp. der.).*

Demostración. 1. Sea ${}_RS$ simple, entonces existe $\mathcal{M} \leq R$ ideal máximo tal que $S \cong R/\mathcal{M}$. Tenemos que $\operatorname{Rad}(R) \subseteq \mathcal{M}$ entonces

$$S \cong \frac{R}{\mathcal{M}} \cong \frac{R/\operatorname{Rad}(R)}{\mathcal{M}/\operatorname{Rad}(R)}$$

Como $R/\operatorname{Rad}(R)$ es s.s. entonces $\mathcal{M}/\operatorname{Rad}(R)$ es sumando directo, es decir, $R/\operatorname{Rad}(R) = (\mathcal{M}/\operatorname{Rad}(R)) \oplus (A/\operatorname{Rad}(R))$. Por lo tanto

$$A/\operatorname{Rad}(R) \cong \frac{R/\operatorname{Rad}(R)}{\mathcal{M}/\operatorname{Rad}(R)} \cong S$$

2. Por el Lemma 5.3.17 los R-submodulos de ${}_R(\frac{R}{\operatorname{Rad}(R)})$ coinciden con los ideales izquierdos de $R/\operatorname{Rad}(R)$. Entonces $R/\operatorname{Rad}(R)$ es semisimple como $\frac{R}{\operatorname{Rad}(R)}$-módulo. Lo que implica que los bloques de $R/\operatorname{Rad}(R)$ son finitos. Además por (*1*), $R/\operatorname{Rad}(R)$ contiene una copia de cada R-módulo simple. $\square$

Teorema 5.3.19. *Sea R un anillo tal que $R/\operatorname{Rad}(R)$ es s.s. Entonces para todo R-módulo M:*

1. $\operatorname{Rad}(M) = \operatorname{Rad}(R)M$
2. $\operatorname{Zoc}(M) = \{m \in M \mid \operatorname{Rad}(R)m = 0\}$

Demostración. 1. Tenemos que $\operatorname{Rad}(R)(\frac{M}{\operatorname{Rad}(R)M}) = 0$, así que $\frac{M}{\operatorname{Rad}(R)M}$ es un $R/\operatorname{Rad}(R)$-módulo. Como $R/\operatorname{Rad}(R)$ es semisimple entonces $\frac{M}{\operatorname{Rad}(R)M}$ es s.s. como $\frac{R}{\operatorname{Rad}(R)}$-módulo. Por el Lema 5.3.17 $\frac{M}{\operatorname{Rad}(R)M}$ es s.s. como R-módulo. Por lo tanto $\operatorname{Rad}(\frac{M}{\operatorname{Rad}(R)M}) = 0$. Así $\operatorname{Rad}(M) \subseteq \operatorname{Rad}(R)M$.

2. Todo s.s. tiene radical cero y $\operatorname{Rad}(R)M \subseteq \operatorname{Rad}(M)$. Entonces, si $A := \{m \in M \mid \operatorname{Rad}(R)m = 0\}$, tenemos que $\operatorname{Zoc}(M) \subseteq A$. Por otra parte, $\operatorname{Rad}(R)A = 0$, así que A es un $\frac{R}{\operatorname{Rad}(R)}$-módulo y tiene los mismos submodulos que ${}_RA$. Pero A como $\frac{R}{\operatorname{Rad}(R)}$-módulo es s.s. lo que implica que ${}_RA$ es s.s.. Por lo tanto $A \subseteq \operatorname{Zoc}(M)$. $\square$

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 $(L, \leq, \bigwedge, \bigvee)$ 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

   $$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "\varphi"'] & B \arrow[d, "\beta"] \\ M \arrow[r, "\psi"'] & N \end{tikzcd}$$

   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

   $$0 \to A \to B \to C \to 0$$

   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 $\left(\begin{smallmatrix} 0 & 0 \\ K & 0 \end{smallmatrix}\right)$ no es un sumando directo de $\mathrm{TI}_2(K)$.

9. Demuestre que si S es un R-módulo simple, entonces $\mathrm{Rad}(S) = 0$.

10. De un ejemplo de un R-módulo M tal que $\mathrm{Zoc}(M/\mathrm{Zoc}(M)) \neq 0$.

11. De un ejemplo de un R-módulo M tal que $\mathrm{Rad}(\mathrm{Rad}(M)) \neq \mathrm{Rad}(M)$.

12. Sea $N \leq M$. Demuestre que $\mathrm{Zoc}(N) = N \cap \mathrm{Zoc}(M)$.

13. ¿Es cierto para $N \leq M$ que $\operatorname{Rad}(N) = N \cap \operatorname{Rad}(M)$.

14. Considere la sucesión exacta $0 \to A \to B \to C \to 0$. Demuestre que si $\operatorname{Rad}(A) = A$ y $\operatorname{Rad}(C) = C$ entonces $\operatorname{Rad}(B) = B$.

15. Sea $\{M_i\}_I$ una familia de R-módulos. Demuestre que:

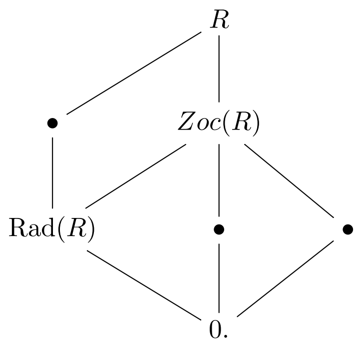
    a) $\operatorname{Rad}\left(\prod_I M_i\right) \leq \prod_I \operatorname{Rad}(M_i)$.

    b) $\operatorname{Zoc}\left(\prod_I M_i\right) \leq \prod_I \operatorname{Zoc}(M_i)$.

16. Sea $\mathbb{F}_2$ el campo con dos elementos. Considere $R = \mathrm{TI}_2(\mathbb{F}_2)$. Demuestre que

    a) los ideales izquierdos de R son

$$\left\{0, R, \left(\begin{smallmatrix} \mathbb{F}_2 & 0 \\ \mathbb{F}_2 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ \mathbb{F}_2 & \mathbb{F}_2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ \mathbb{F}_2 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 0 & \mathbb{F}_2 \end{smallmatrix}\right), \{0, \left(\begin{smallmatrix} 0 & 0 \\ 1 & 1 \end{smallmatrix}\right)\}\right\}.$$



    b) $\operatorname{Rad}(R) = \left(\begin{smallmatrix} 0 & 0 \\ \mathbb{F}_2 & 0 \end{smallmatrix}\right)$ y $\operatorname{Zoc}(R) = \left(\begin{smallmatrix} 0 & 0 \\ \mathbb{F}_2 & \mathbb{F}_2 \end{smallmatrix}\right)$.

    c) $R/\operatorname{Rad}(R)$ es semisimple.

    d) R es un R-submódulo esencial en $\mathrm{M}_2(\mathbb{F}_2)$.

Capítulo 6

Módulos Proyectivos 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 $r_1 = r_2 = \cdot = r_n = 0$.

Definición 6.1.2. Un R-módulo ${}_RF$ es *libre* si tiene una base.

Proposición 6.1.3. *Las siguientes condiciones son equivalentes para un modulo ${}_RF$:*

(a) F *es libre;*

(b) $F = \bigoplus_I A_i$ *con* $A_i \cong {}_RR$ *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 vacio es 0. Supongamos que $F \neq 0$.

1⇒2 Sea X una base de F y $a \in X$. Consideremos el R-morfismo $\varphi : R \to Ra$ 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 congunto 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 $a_1, ..., a_n \in X$ con $a_i \neq a_0$ y $r_0, r_1, ..., r_n \in R$ tales que $c = r_0a_0 = \sum_{i=1}^n r_ia_i$. Así $r_0a_0 + \sum(-r_i)a_i = 0$. Como X es base, $r_0 = r_1 = ... = r_n = 0$. Entonces $Ra_0 \cap \sum Ra = 0$ y por lo tanto $F = \bigoplus_{a \in X} Ra$.

2⇒1 Por hipótesis existe un isomorfismo $\varphi_i : R \to A_i$ 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. □

Lema 6.1.4. *Sea I un conjunto. Entonces $R^{(I)}$ es un modulo 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 modulo libre y tiene al conjunto $\{\eta_i(1) \mid i \in I\}$ como base, donde η_i son las inclusiones canónicas. □

Proposición 6.1.5. *Todo modulo M es imagen epimorfica de un módulo libre. Si M es f.g. entonces M es imagen epimorfica de un modulo libre con base finita.*

Demostración. Sea Y un conjunto generador de M. Consideremos el modulo libre $R^{(Y)}$. Definimos el R-morfismo $\varphi : R^{(Y)} \to M$ como $\varphi(\eta_y(1)) = y$. Claramente φ es suprayectivo. Ahora supongamos que M es f.g. con conjunto generador $\{m_1, m_2, ..., m_n\}$. Definimos el siguiente epimorfismo $\varphi : R^{(n)} \to M$ como $\varphi(e_i) = m_i$ para todo $1 \leq i \leq n$, where $e_i = (\delta_{ij})_{j=1}^{n} \in R^{(n)}$. □

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. □

Teorema 6.1.7. *Sea R un anillo y denotemos $\overline{R} := R/\operatorname{Rad}(R)$. Son equivalentes:*

(a) *R un anillo bueno izquierdo.*

(b) *Si $\varphi : M \to N$ es un R-morfismo entonces $\varphi(\operatorname{Rad}(M)) = \operatorname{Rad}(\varphi(M))$.*

(c) *Sea M un R-módulo y $U \leq M$ entonces $\frac{\operatorname{Rad}(M)+U}{U} = \operatorname{Rad}(M/U)$.*

(d) *Sea M un R-módulo y $U \leq M$. Si $\operatorname{Rad}(M) = 0$ entonces $\operatorname{Rad}(M/U) = 0$.*

Demostración. (a)⇒(b). Sea $\varphi : M \to N$ un R-morfismo. Entonces

$$\varphi(\operatorname{Rad}(M)) = \varphi(\operatorname{Rad}(R)M) = \operatorname{Rad}(R)\varphi(M) = \operatorname{Rad}(\varphi(M)).$$

(b)⇒(c). Sólo hay que considerar la proyección canónica $\pi : M \to M/U$.

(c)⇒(d). Es claro.

(d)⇒(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, $\operatorname{Rad}(F) = \operatorname{Rad}(R)F$. Como $\operatorname{Rad}(F/\operatorname{Rad}(F)) = \operatorname{Rad}(R/\operatorname{Rad}(R)F) = 0$, por hipótesis:

$$\operatorname{Rad}\left(\frac{\left(\frac{F}{\operatorname{Rad}(R)F}\right)}{\left(\frac{\operatorname{Rad}(R)F+U}{\operatorname{Rad}(R)F}\right)}\right) = 0$$

pero

$$\frac{\left(\frac{F}{\operatorname{Rad}(R)F}\right)}{\left(\frac{\operatorname{Rad}(R)F+U}{\operatorname{Rad}(R)F}\right)} \cong \frac{F}{\operatorname{Rad}(R)F + U} \cong \frac{\left(\frac{F}{U}\right)}{\left(\frac{\operatorname{Rad}(R)F+U}{U}\right)}.$$

Por lo tanto

$$\operatorname{Rad}\left(\frac{\left(\frac{F}{U}\right)}{\left(\frac{\operatorname{Rad}(R)F+U}{U}\right)}\right)=0$$

Por el Teorema 5.3.6,

$$\operatorname{Rad}(F/U)\subseteq\frac{\operatorname{Rad}(R)F+U}{U}\subseteq\operatorname{Rad}(R)(F/U).$$

Por lo tanto $\operatorname{Rad}(R)M=\operatorname{Rad}(M)$. □

Teorema 6.1.8. *Si $\varphi : M \to F$ es un epimorfismo y ${}_RF$ 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 $\varphi' : F \to M$ 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., $\varphi\varphi'=Id_F$. Por lo tanto $M=\operatorname{Im}\varphi'\oplus\operatorname{Ker}\varphi$ por el Corolario 3.2.11.*3*. □

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 $\bigoplus_K Rx_k$ con $Rx_k \cong R$. Supongamos que K está bien ordenado. Para cada $k\in K$ definimos $F_k=\bigoplus_{j\leq k} Rx_j$ y $\overline{F_k}=\bigoplus_{j<k} Rx_j$. 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

$$H_k/\overline{H_k}=H_k/(H_k\cap\overline{F_k})\cong(\overline{F_k}+H_k)/\overline{F_k}\leq F_k/\overline{F_k}\cong Rx_k\cong R.$$

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 $h_k\in H_k$. 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 $\pi : H_k\to H_k/\overline{H_k}$ se escinde. Por lo tanto

$$H_k=\overline{H_k}\oplus Rh_k.$$

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 indice 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 $h'=a+rh_j$ 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 $r_1 h_{k_1} + ... + r_n h_{k_n} = 0$ con $k_1 < ... < k_n$, entonces $r_n h_{k_n} \in R h_{k_n} \cap \overline{H_{k_n}} = \{0\}$ 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 $A \times U \to U$ como: fijemos $\beta \in \Lambda$

$$(a, u) \mapsto \begin{cases} s_\beta u & \text{Si } \beta \text{ aparece en la reperesenctación de } a. \\ 0 & \text{En otro caso.} \end{cases}$$

Entonces existe un único morfismo $A \otimes_S U \to U$ 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 unicamente 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 $x_1, ..., x_m$ y ${}_S U$ un módulo libre con base $z_1, ..., z_n$. 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 elemnto 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 unicamente 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 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 ${}_KV$ un espacio vectorial de dimensión infinita (numerable). Sea $R = \mathrm{End}_K(V)$. Fijemos una base $\{v_1, v_2, ..., v_n, ...\}$ de V. Consideremos los siguientes R-morfismos $\Theta_1, \Theta_2 : R \to R$ definidos como: Sea $\varphi, \psi \in R$,

$$\Theta_1(\varphi)(v_i) = \begin{cases} \varphi(v_n) & \text{si } i = 2n-1 \\ 0 & \text{si } i = 2n \end{cases} \qquad \Theta_2(\psi)(v_i) = \begin{cases} \psi(v_n) & \text{si } i = 2n \\ 0 & \text{si } i = 2n-1 \end{cases}$$

Por la propiedad universal de la suma directa, existe un único R-morfismo $\Theta : R \oplus R \to R$ 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 $\varphi : R \to R$ como $\varphi(v_i) = \alpha(v_{2i-1})$ y definimos $\psi : R \to R$ 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 Proyectivos

Definición 6.2.1. Se dice que un módulo ${}_RQ$ es *inyectivo* si para todo monomorfismo $\alpha : A \to B$ y para todo R-morfimo $\varphi : A \to Q$ existe un R-morfismo $\kappa : B \to Q$ tal que $\varphi = \kappa\alpha$.

$$\begin{tikzcd} A \arrow[r, tail, "\alpha"] \arrow[d, "\varphi"'] & B \arrow[dl, dashed, "\kappa"] \\ Q & \end{tikzcd}$$

Teorema 6.2.2. *Las siguientes condiciones son equivalentes para un módulo* ${}_RQ$*:*

(a) *Q es inyectivo*

(b) *Todo monomorfismo $\xi : Q \to B$ se escinde.*

Demostración. 1. (a)$\Rightarrow$(b). Sea $\xi : Q \to B$ un monomorfismo. Considere Id_Q. Como Q es inyectivo, existe $\kappa : B \to Q$ 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 $\kappa : B \to Q$ tal que $\varphi = \kappa\alpha$. □

Corolario 6.2.3. *Sea Q un R-módulo y $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ una sucesión exacta corta. Entonces la sucesión*

$$0 \to \mathrm{Hom}_R(C, Q) \xrightarrow{g^*} \mathrm{Hom}_R(B, Q) \xrightarrow{f^*} \mathrm{Hom}_R(A, Q) \to 0$$

es exacta si y solo si Q es inyectivo.

Demostración. $\Rightarrow$ Por el Proposición 3.4.12, basta probar que f^* es suprayectiva. Sea $\varphi : A \to Q$ cualquier R-morfismo. Como f es inyectivo y Q es un módulo inyectivo, existe $\kappa : B \to Q$ tal que $\varphi = \kappa f = f^*(\kappa)$. Es decir, f^* es suprayectiva.

$\Leftarrow$ Sea $\varphi : A \to Q$ un R-morfismo y $f : A \to B$ un monomorfismo. Tenemos una sucesión exacta corta $0 \to A \to B \to \mathrm{Coker}\, f \to 0$. Por hipótesis, $\mathrm{Hom}_R(B, Q) \xrightarrow{f^*} \mathrm{Hom}_R(A, Q)$ es suprayectiva. Entonces, para $\varphi \in \mathrm{Hom}_R(A, Q)$ existe $\kappa \in \mathrm{Hom}_R(B, Q)$ tal que $\varphi = f^*(\kappa) = \kappa f$. Por lo tanto, Q es inyectivo. □

Definición 6.2.4. Se dice que un módulo ${}_RP$ es *proyectivo* si para todo epimorfismo $\psi : B \to C$ y para todo R-morfismo $\beta : P \to C$ existe un R-morfismo $\lambda : P \to B$ tal que $\beta = \psi\lambda$.

$$\begin{tikzcd} & P \arrow[dl, dashed, "\lambda"'] \arrow[d, "\beta"] \\ B \arrow[r, two heads, "\psi"] & C \end{tikzcd}$$

Teorema 6.2.5. *Las siguientes condiciones son equivalentes para un módulo* ${}_RP$*:*

(a) *P es proyectivo.*

(b) *Todo epimorfismo $\xi : B \to P$ se escinde.*

Demostración. (a)$\Rightarrow$(b). Sea $\xi : B \to P$ un epimorfismo. Considere Id_P. Como P es proyectivo, existe $\lambda : P \to B$ 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 hipotesis α se escinde, lo que implica que existe $\lambda : P \to B$ tal que $\beta = \psi\lambda$ por el Teorema 4.2.6.(*2*). $\square$

Corolario 6.2.6. *Sea P un R-módulo y $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ una sucesión exacta corta. Entonce Q es inyectivo si y solo si la sucesión*

$$0 \to \mathrm{Hom}_R(P, A) \xrightarrow{f_*} \mathrm{Hom}_R(P, B) \xrightarrow{g_*} \mathrm{Hom}_R(P, C) \to 0$$

es exacta si y solo si P es proyectivo.

Demostración. $\Rightarrow$ Por la Proposición 3.4.13, basta ver que g_* es suprayectiva. Sea $\beta \in \mathrm{Hom}_R(P, C)$. Como g es suprayectiva y P es proyectivo, existe $\lambda : P \to B$ tal que $\beta = g\lambda = g_*(\lambda)$.

$\Leftarrow$ Sea $g : B \to C$ un epimorfismo y $\beta : P \to C$ cualquier R-morfismo. Tenemos la sucesión exacta corta $0 \to \mathrm{Ker}\, g \to B \to C \to 0$. Por hipótesis $g_* : \mathrm{Hom}_R(P, B) \to \mathrm{Hom}_R(P, C)$ es suprayectiva, así que existe $\lambda : P \to B$ 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 $R \to R/I$ 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 $\mathrm{Zoc}(R) := \sum S_i$ con $S_i \leq R$, S_i simple. Si $\mathrm{Zoc}(R) < R$, como R es f.g. entonces existe $\mathcal{M} \leq R$ máximo tal que $\mathrm{Zoc}(R) \subseteq \mathcal{M}$.Como $R/\mathcal{M}$ es simple y cada simple es proyectivo entonces la proyección canónica $\pi : R \to R/\mathcal{M}$ se escinde, es decir, $R = A \oplus \mathcal{M}$ con $A \cong R/\mathcal{M}$ simple. Contradicción ya que $\mathrm{Zoc}(R)$ es la suma de todos los simples de R y $\mathrm{Zoc}(R) \subseteq \mathcal{M}$. $\square$

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 $\beta : A \to B$ un epimorfismo y $\psi : P_i \to B$. Como P es proyectivo, existe $\lambda : P \to A$ tal que $\beta\lambda = \psi\pi_i$ donde $\pi_i : P \to P_i$ es la proyección canónica. Sea $\eta_i : P_i \to \bigoplus_I P_i$ la inclusión canónica. Entonces $\beta\lambda\eta_i = \psi\pi_i\sigma\eta_i = \psi Id_{P_i} = \psi$.

$$\begin{tikzcd}
 & P_i \arrow[d, "\eta_i"] \\
 & P \arrow[d, "\pi_i"] \arrow[ddl, "\lambda"'] \\
 & P_i \arrow[d, "\psi"] \\
A \arrow[r, two heads, "\beta"] & B
\end{tikzcd}$$

$\Leftarrow$. Sean $\beta : A \to B$ un epimorfismo y $\psi : P \to B$. Como P_i es proyectivo para cada $i \in I$, existen morfismos $\lambda_i : P_i \to A$ 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 $\lambda : P \to A$ 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 $\beta\lambda = \psi$.

$$\begin{tikzcd}
 & P_i \arrow[d, "\eta_i"] \arrow[ddl, "\lambda_i"'] \\
 & P \arrow[d, "\psi"] \arrow[dl, dashed, "\lambda_i"] \\
A \arrow[r, two heads, "\beta"'] & B
\end{tikzcd}$$

□

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* $\mathrm{Hom}_{\mathbb{Z}}(M/P, \mathbb{Z}) = 0$.

Demostración. Sea $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$ tal que $\varphi(P) = 0$. Consideremos los siguientes dos subgrupos de M

$$A = \{(2a_1, 2^2a_2, ..., 2^na_n, ...) \mid a_i \in \mathbb{Z}\}$$

$$B = \{(3b_1, 3^2b_2, ..., 3^nb_n, ...) \mid b_i \in \mathbb{Z}\}$$

Entonces $A + B = M$. Notemos que cada elemento de A se puede escribir de la forma

$$(2a_1, 2^2a_2, ..., 2^{n-1}a_{n-1}, 0, 0, ...) + 2^nx$$

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 $\varphi(M) = 0$. □

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 $\pi_i : F \to \mathbb{Z}e_i$ 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 $\varphi : M \to \mathbb{Z}$ tal que $\varphi(P) = 0$, contradiciendo el lema anterior. □

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 $\alpha : A \to B$ un monomorfismo y $\varphi : A \to Q_i$ un R-morfismo. Consideremos $\eta_i : Q_i \to \bigoplus Q_i$ la inclusión canónica, σ la inclusión de la suma directa en el producto y $\pi_i : \prod_I Q_i \to Q_i$ la proyección canónica. Como Q es inyectivo existe $\kappa : B \to Q$ tal que $\kappa\alpha = \sigma\eta_i\varphi$.

Entonces $\pi_i\kappa$ es el morfismo requerido ya que $\pi_i\kappa\alpha = \pi_i\sigma\eta_i\varphi = Id_{Q_i}\varphi = \varphi$.

$$
\begin{tikzcd}
A \arrow[r, tail, "\alpha"] \arrow[d, "\varphi"'] & B \arrow[dddl, "\kappa"] \\
Q_i \arrow[d, "\eta_i"'] & \\
\bigoplus Q_i \arrow[d, "\sigma"'] & \\
\prod Q_i \arrow[d, "\pi_i"'] & \\
Q_i &
\end{tikzcd}
$$

$\Leftarrow$. Sea $\alpha : A \to B$ un monomorfismo y $\varphi : A \to Q$ un R-morfismo. Como Q_i es inyectivo para cada $i \in I$, existen morfismos $\kappa_i : B \to Q_i$ 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 $\kappa : B \to Q$ tal que $\pi_i\kappa = \kappa_i$. Entonces $\pi_i\kappa\alpha = \pi_i\varphi$ y por la unicidad de κ se tiene que $\kappa\alpha = \varphi$.

$$
\begin{tikzcd}
A \arrow[r, tail, "\alpha"] \arrow[d, "\varphi"'] & B \arrow[dl, dashed, "\kappa"'] \arrow[ddl, "\kappa_i"] \\
Q \arrow[d, "\pi_i"'] & \\
Q_i &
\end{tikzcd}
$$

□

Ejemplo 6.2.12. Sea $R = \prod_{\mathbb{N}} K_i$ un producto directo de campos. Se sigue de los ejercicios 6.4.12 y 6.4.16 que todo R-módulo simple es inyectivo. No es dificil 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 $\alpha : F \to P$. Como P es proyectivo, α se escinde, es decir, $F = \operatorname{Ker}\alpha \oplus K$. Pero $K \cong \operatorname{Im}\alpha = P$, 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 $\varphi_i \in \operatorname{Hom}_R(P, R)$ 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* $\mathrm{Hom}_R(P,R)$ *que satisfacen* (1) *y* (2) *del inciso* (b).

Demostración. (a)⇒(b). Tenemos que existe $F = \bigoplus_I Rx_i$ libre y un epimorfismo $\xi : \bigoplus_I Rx_i \to P$ dado por $\xi(\sum r_i x_i) = \sum r_i y_i$. Como P es proyectivo existe $\lambda : P \to \bigoplus_I Rx_i$ tal que $\xi\lambda = Id_P$. Sea $\pi_i : \bigoplus_I Rx_i \to Rx_i \cong R$ la proyección canónica. Ahora si $a \in \bigoplus_I Rx_i$, entonces $a = \sum \pi_i(a)x_i$. Así que para cada $p \in P$,

$$p = \xi\lambda(p) = \xi(\sum \pi_i(\lambda(p))x_i) = \sum \pi_i(\lambda(p))\xi(x_i) = \sum \pi_i(\lambda(p))y_i.$$

Tomando $\varphi_i = \pi_i\lambda$ se tiene que $p = \sum \varphi_i(p)y_i$.

(b)⇒(c). Es claro.

(c)⇒(a). La condicion (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 $\xi : F \to P$ el epimorfismo dado por $\xi(x_i) = y_i$. Usando (1) definimos $\tau : P \to F$ 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 $F = \mathrm{Ker}\,\xi \oplus \mathrm{Im}\,\tau$. Como ξ es suprayectiva, $P \cong \mathrm{Im}\,\tau$ y por lo tanto P es un sumando directo de un libre. Lo que implica que P es proyectivo. □

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* $\varphi : I \to Q$ *existe* $\eta : R \to Q$ *tal que* $\eta i = \varphi$*, donde* $i : I \to R$ *es la inclusión canónica.*

Demostración. Sea $\alpha : A \to B$ un monomorfismo y $\psi : A \to Q$ un morfismo. Consideremos el conjunto $\Gamma = \{(C,\gamma) \mid C \leq B,\ \gamma : C \to Q \text{ tal que } \gamma\alpha = \psi\}$. Se tiene que $\Gamma \neq \emptyset$ ya que $(\mathrm{Im}\,\alpha, \alpha_0) \in \Gamma$ 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 concideremos $(C : b) = \{r \in R \mid rb \in C\} \leq R$ que es distinto de cero. Entonces tenemos un R-morfismo $(\_ \cdot b) : (C : b) \to C$ dado por $(\_ \cdot b)(r) = rb$. Por hipótesis existe $\tau : R \to Q$ tal que $\tau i = \gamma(\_ \cdot b)$. Definimos $\gamma_1 : C + Rb \to Q$ 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. □

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 imagenes homomorficas, bajo sumas directas y bajo productos.*

Demostración. Supongamos que ${}_{\mathbb{Z}}D$ es divisible y $\varphi : D \to G$ es un homomorfismo. Entonces $z\,\mathrm{Im}\,\varphi = z\varphi(D) = \varphi(zD) = \varphi(D) = \mathrm{Im}\,\varphi$ 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 $z\bigoplus_I D_i = \bigoplus_I zD_i = \bigoplus_I D_i$. □

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 $\varphi : F \to A$ (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 $\mathbb{Z}^{(I)}/\operatorname{Ker}\varphi \hookrightarrow \mathbb{Q}^{(I)}/i(\operatorname{Ker}\varphi)$ donde $\mathbb{Q}^{(I)}/i(\operatorname{Ker}\varphi)$ es divisible. Por lo tanto A se sumerje en un divisible. □

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 $i : \mathbb{Z}z_0 \to \mathbb{Z}$ la inclusión canónica. Definimos $\varphi : \mathbb{Z}z_0 \to Q$ como $\varphi(nz_0) = nq_0$ que es un $\mathbb{Z}$-morfismo. Como Q es inyectivo, existe $\kappa : \mathbb{Z} \to Q$ 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 $\varphi : \mathbb{Z}n \to D$ 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 $\kappa : R \to D$ 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. □

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 permancen ciertas (usando el Ejercicio 6.4.6). 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* $\operatorname{Hom}_{\mathbb{Z}}(R_R, D)$ *es inyectivo.*

Demostración. Sean $\alpha : A \to B$ un R-monomorfismo y $\varphi : A \to \operatorname{Hom}_{\mathbb{Z}}(R_R, D)$ cualquier R-morfismo. Definimos $\sigma : \operatorname{Hom}_{\mathbb{Z}}(R_R, D) \to D$ como $\sigma(f) = f(1)$, el cual es un $\mathbb{Z}$-morfismo. Así que tenemos un $\mathbb{Z}$-morfismo $\sigma\varphi : A \to D$. Por lo tanto existe un $\mathbb{Z}$-morfismo $\tau : B \to D$ tal que $\tau\alpha = \sigma\varphi$.

Definimos $\kappa : B \to \operatorname{Hom}_{\mathbb{Z}}(R_R, D)$ 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 $\operatorname{Hom}_{\mathbb{Z}}(R_R, D)$ es inyectivo.

$$\begin{tikzcd}
{}_R A \arrow[r, tail, "\alpha"] \arrow[d, "\varphi"'] & {}_R B \arrow[dl, dashed, "\kappa"] \arrow[ddl, "\tau"] \\
\mathrm{Hom}({}_{\mathbb{Z}}R_R, {}_{\mathbb{Z}}D) \arrow[d, "\sigma"'] & \\
{}_{\mathbb{Z}}D &
\end{tikzcd}$$

□

Teorema 6.2.24. *Para todo R-modulo M existe un monomorfismo $\varphi : M \to Q$ con Q un R-módulo inyectivo.*

Demostración. Sea M un R-módulo. Visto M como grupo abeliano existe un monomorfismo $\mu : {}_{\mathbb{Z}}M \to {}_{\mathbb{Z}}D$ con D divisible por el Teorema 6.2.20. Definimos $\rho : {}_RM \to {}_R\operatorname{Hom}_{\mathbb{Z}}(R, D)$ 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. □

Corolario 6.2.25. *Un módulo ${}_RQ$ es inyectivo si y sólo si Q es isomorfo a un sumando directo de $\operatorname{Hom}_{\mathbb{Z}}(R_R, D)$ para algún ${}_{\mathbb{Z}}D$ divisible.*

Demostración. $\Rightarrow$. Por el Teorema 6.2.24 existe un monomorfismo de Q en $\operatorname{Hom}_{\mathbb{Z}}(R, D)$ 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 $\operatorname{Hom}_{\mathbb{Z}}(R_R, D)$.

$\Leftarrow$. Se sigue por la Proposición 6.2.11. □

Lema 6.2.26. *Si $\rho : M \to N$ es un monomorfismo entonces existen un R-módulo N' tal que $M \leq N'$ y $\tau : N' \to N$ 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 $\beta : L \to N - \rho(M)$ una biyección. Definimos $N' = L \cup M$ y $\tau : N' \to N$ como $\tau(m) = \rho(m)$ si $m \in M$ y $\tau(l) = \beta(l)$ si $l \in L$.

Le damos estructura de R-modulo 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. □

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 ${}_RQ$ un R-módulo inyectivo y $S = \operatorname{End}_R(Q)$. Son equivalentes para $f \in S$:*

(a) $f \in \operatorname{Rad}(S)$

(b) $\operatorname{Ker} f \leq_e Q$

Demostración. (a)$\Rightarrow$(b). Sea $f \in \operatorname{Rad}(S)$. Sea $U \leq Q$ tal que $U \cap \operatorname{Ker} f = 0$. Entonces $f|_U$ es un monomorfismo. Como Q es inyectivo existe $g \in S$ tal que $g \circ f|_U = i$ donde $i : U \to Q$ es la inclusión canónica. Entonces para todo $u \in U$, $u = i(u) = gf(u)$ lo que implica que $U \subseteq \operatorname{Ker}(Id_Q - gf)$. Como $f \in \operatorname{Rad}(S)$, gf también. Así que $Id_Q - gf$ tiene inverso. Por lo tanto $U \subseteq \operatorname{Ker}(Id_Q - gf) = 0$.

(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 $x \in \operatorname{Ker} f \cap \operatorname{Ker} g$ entonces $x = hf(x) + g(x) = 0$. Como $\operatorname{Ker} f \leq_e Q$, $\operatorname{Ker} g = 0$, 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 $Sf << S$ y así $f \in \operatorname{Rad}(S)$. □

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 $_RQ$ inyectivo y $S := \mathrm{End}_R(Q)$. Entonces $S/\mathrm{Rad}(S)$ es un anillo regular de von Neumann, es decir, para cada $f \in S$ existe $g \in S$ tal que $fgf - f \in \mathrm{Rad}(S)$.*

Demostración. Sea $f \in S$. Sea $U \leq Q$ un p.c. de $\mathrm{Ker}\, f$, entonces $\mathrm{Ker}\, f \oplus U \leq_e Q$. Además $f|_U$ es un monomorfismo, así que existe $g \in S$ tal que $gf|_U = i$ donde $i : U \to Q$ es la inclusión canónica. Si $k + u \in \mathrm{Ker}\, f \oplus U$ entonces

$$(fgf - f)(k + u) = fgf(k + u) - f(k + u) = fgf(u) - f(u)$$

$$= fgf(u) - f(gf(u)) = 0$$

Por lo tanto $\mathrm{Ker}\, f \oplus U \subseteq \mathrm{Ker}(fgf - f)$, así que $\mathrm{Ker}(fgf - f) \leq_e Q$. Por el Teorema 6.2.28, $fgf - f \in \mathrm{Rad}(S)$. □

Teorema 6.2.31. *Sea P proyectivo y $S := \mathrm{End}_R(P)$. Son equivalentes para $f \in S$:*

(a) $f \in \mathrm{Rad}(S)$

(b) $\mathrm{Im}\, f << P$

Demostración. (a)⇒(b). Sea $U \leq P$ tal que $\mathrm{Im}\, f + U = P$. Consideremos $\pi : P \to P/U$ la proyección canónica. Entonces para cada $p \in P$ existen $f(x) \in \mathrm{Im}\, f$ y $u \in U$ tales que $p + P = (f(x) + u) + P = f(x) + P$. Por lo tanto πf es suprayectiva. Como P es proyectivo, existe $g \in S$ tal que $\pi f g = \pi$. Entonces $\pi(Id_P - fg) = 0$ lo que implica que $\mathrm{Im}(Id_P - fg) \subseteq \mathrm{Ker}\, \pi = U$. Como $f \in \mathrm{Rad}(S)$, $Id_P - fg$ tiene inverso. Por lo tanto $\mathrm{Im}(Id_P - fg) = P = U$.

(b)⇒(a). Supongamos que $S = fS + G$ para algún ideal derecho G de S. Entonces existen $h \in S$ y $g \in G$ tales que $Id_P = fh + g$. Así, para todo $x \in P$, $x = (fh + g)(x) = f(h(x)) + g(x)$ lo que implica que $P = \mathrm{Im}\, f + \mathrm{Im}\, g$. Pero $\mathrm{Im}\, f << P$ por lo que $\mathrm{Im}\, g = P$, es decir, g es sobre. Como P es proyectivo existe $k \in S$ tal que $gk = Id_P$. Por lo tanto $G = S$. Entonces $fS << S_S$ y $f \in \mathrm{Rad}(S)$. □

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 $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}) \cong \mathbb{Z}$ (Observación 3.4.11). Por otro lado, tenemos que $\mathrm{Rad}(\mathbb{Z}) = 0$. Así que $\mathbb{Z} = \mathrm{End}_{\mathbb{Z}}(\mathbb{Z})/\mathrm{Rad}(\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}))$ que no es un anillo regular de von Neumann (Ejercicio 6.4.10).

Teorema 6.2.33. *Si $0 \neq P$ es proyectivo entonces $\mathrm{Rad}(P) \neq P$.*

Demostración. Sea $S := \mathrm{End}_R(P)$. Para cada $p \in P$ y $\varphi : P \to R$ definimos $\varphi_p : P \to P$ como $\varphi_p(x) = \varphi(x)p$. Sea $p \in \mathrm{Rad}(P)$. Entonces $Rp << P$ así que $\mathrm{Im}\, \varphi_p = \varphi(P)p \subseteq (Rp) << P$. Por lo tanto $\mathrm{Im}\, \varphi_p << P$. Por el Teorema 6.2.31 $\varphi_p \in \mathrm{Rad}(S)$.

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 $(Id_p - \varphi_{i_{p_i}})(x) = 0$. Supongamos que $\mathrm{Rad}(P) = P$. Si $0 \neq x \in P$, $x = \sum \varphi(x)p_i$. Como cada $p_i \in \mathrm{Rad}(P)$ entonces $\varphi_{i_{p_i}} \in \mathrm{Rad}(S)$ para toda i. Lo que implica que $\sum \varphi_{i_{p_i}} \in \mathrm{Rad}(S)$ y por lo tanto $Id_P - \sum \varphi_{i_{p_i}}$ tiene inverso. Contradicción. □

Corolario 6.2.34. *Si P es proyectivo y $P = P_1 \oplus P_2$ con $P_2 \subseteq \mathrm{Rad}(P)$ entonces $P_2 = 0$.*

Demostración. Consideremos $\pi : P \to P_2$ la proyección canónica. Entonces si $P_2 \subseteq \mathrm{Rad}(P)$

$$P_2 = \pi(P_2) \subseteq \pi(\mathrm{Rad}(P)) \subseteq \mathrm{Rad}(P_2) \subseteq P_2$$

Así que $\mathrm{Rad}(P_2) = P_2$. Como P_2 es proyectivo, $P_2 = 0$ por el Teorema 6.2.33. □

6.3. Cápsulas Inyectivas y Cubiertas Proyectivas

Definición 6.3.1. Un R-morfismo $\alpha : A \to B$ se llama:

1. *superfluo* si $\operatorname{Ker}\alpha << A$
2. *esencial* si $\operatorname{Im}\alpha \leq_e B$

Lema 6.3.2. *Sea $\alpha : A \to B$ y $\beta : B \to C$ dos R-morfismos.*

1. *Si $\alpha : A \to B$ y $\beta : B \to C$ son epimorfismos superfluos entonces $\beta\alpha$ también lo es.*
2. *Si $\alpha : A \to B$ y $\beta : B \to C$ son monomorfismos esenciales entonces $\beta\alpha$ tambien lo es.*

Demostración. (1). Supongamos que $\operatorname{Ker}\beta\alpha + U = A$, con $U \leq A$. Entonces

$$\alpha(\operatorname{Ker}\beta\alpha + U) = \alpha(A) = B.$$

Por otro lado $\alpha(\operatorname{Ker}\beta\alpha + U) = \alpha(\operatorname{Ker}\beta\alpha) + \alpha(U) = \alpha(\alpha^{-1}(\operatorname{Ker}\beta)) + \alpha(U) = \operatorname{Ker}\beta + \alpha(U)$ así que $B = \operatorname{Ker}\beta + \alpha(U)$ pero $\operatorname{Ker}\beta << B$ entonces $B = \alpha(U)$. Por lo tanto $\operatorname{Ker}\alpha + U = A$ ya que si $a \in A$ entonces $\alpha(a) \in B = \alpha(U)$ y así $\alpha(a) = \alpha(u)$ p.a. $u \in U$. Esto implica que $a-u \in \operatorname{Ker}\alpha$ y entonces $a = u+(a-u)$. Como $\operatorname{Ker}\alpha << A$, $U = A$. Por lo tanto $\operatorname{Ker}\alpha\beta << A$.

(2). Sea $U \leq C$ tal que $\operatorname{Im}\beta\alpha \cap U = 0$. Como β es mono entonces $0 = \beta^{-1}(0) = \beta^{-1}(\operatorname{Im}\beta\alpha \cap U) = \beta^{-1}(\operatorname{Im}\beta\alpha) \cap \beta^{-1}(U)$, pero $\operatorname{Im}\beta\alpha = \beta(\operatorname{Im}\alpha)$ así que

$$0 = \beta^{-1}(\operatorname{Im}\beta\alpha) \cap \beta^{-1}(U) = \beta^{-1}(\beta(\operatorname{Im}\alpha)) \cap \beta^{-1}(U) = \operatorname{Im}\alpha \cap \beta^{-1}(U).$$

Como $\operatorname{Im}\alpha \leq_e B$, $\beta^{-1}(U) = 0$. Entonces $\operatorname{Im}\beta \cap U = 0$ y como $\operatorname{Im}\beta \leq_e C$, $U = 0$. Por lo tanto $\operatorname{Im}\beta\alpha \leq_e C$. □

Definición 6.3.3. Un monomorfismo $\eta : M \to Q$ es una *cápsula inyectiva* de M si Q es inyectivo y η es un monomorfismo esencial.

Definición 6.3.4. Un epimorfismo $\xi : P \to M$ es una *cubierta proyectiva* de M si P es proyectivo y ξ es un epimorfismo superfluo.

Ejemplo 6.3.5. (I) Si $i : \mathbb{Z} \to \mathbb{Q}$ es la inclusión canónica, entonces i es cápsula inyectiva de $\mathbb{Z}$ ya que $\mathbb{Z} \leq_e \mathbb{Q}$.

(II) Considere el anillo $R = \mathbb{Z}_4$. Entonces R es una cubierta proyectiva de $\mathbb{Z}_2$ como $\mathbb{Z}_4$-módulo.

Lema 6.3.6. *1. Si $\eta_i : M_i \to Q_i$ es capsula inyectiva de M_i con $1 \leq i \leq n$ entonces $\bigoplus \eta_i : \bigoplus_{i=1}^n M_i \to \bigoplus_{i=1}^n Q_i$ es capsula inyectiva de $\bigoplus M_i$.*

2. Si $\xi_i : P_i \to M_i$ es cubierta proyectiva de M_i con $1 \leq i \leq n$ entonces $\bigoplus \xi_i : \bigoplus_{i=1}^n P_i \to \bigoplus_{i=1}^n M_i$ es cubierta proyectiva de $\bigoplus M_i$.

Demostración. Se sigue de que la suma directa preserva monomorfismos y epimorfismos (Proposición 4.1.7), y de los Lemas 5.1.25 y 5.1.8. □

Teorema 6.3.7. *Si $\varphi : M_1 \to M_2$ es un isomorfismo, $\eta_1 : M_1 \to Q_1$ es una cápsula inyectiva de M_1 y $\eta_2 : M_2 \to Q_2$ es un monomorfismo, entonces existe $\psi : Q_1 \to Q_2$ monomorfismo que se escinde y tal que $\eta_2\varphi = \psi\eta_1$. Definiendo $\eta_2' : M_2 \to \operatorname{Im}\psi$ se tiene que η_2' es cápsula inyectiva de M_2. Además ψ es isomorfismo si y sólo si η_2 es cápsula inyectiva.*

$$\begin{tikzcd}
M_1 \arrow[r, tail, "\eta_1"] \arrow[d, tail, "\varphi"'] & Q_1 \arrow[ddl, tail, dashed, "\psi"] \\
M_2 \arrow[d, tail, "\eta_2"'] & \\
Q_2 &
\end{tikzcd}$$

Demostración. Como Q_2 es inyectivo existe $\psi : Q_1 \to Q_2$ tal que $\psi\eta_1 = \eta_2\varphi$. Notemos que $\operatorname{Ker}\psi \cap \operatorname{Im}\eta_1 = 0$ ya que $\eta_2\varphi$ es monomorfismo. Como $\operatorname{Im}\eta_1 \leq_e Q_1$, $\operatorname{Ker}\psi = 0$. Por lo tanto ψ es un monomorfismo. Ahora, como Q_2 es inyectivo, ψ se escinde. Así que $\operatorname{Im}\psi$ es sumando directo de Q_2, lo que implica que $\operatorname{Im}\psi$ es inyectivo. Notemos que $\operatorname{Im}\eta_2 \subseteq \operatorname{Im}\psi$ ya que si $x \in \operatorname{Im}\eta_2$ existe $y \in M_2$ tal que $x = \eta_2(y)$ pero φ es isomorfismo, así que existe $z \in M_1$ tal que $\varphi(z) = y$. Entonces $x = \eta_2\varphi(z) = \psi\eta_1(z)$ y por lo tanto $x \in \operatorname{Im}\psi$. Tomemos η_2 correstringida a su imagen, i.e., $\eta_2' : M_2 \to \operatorname{Im}\psi$ y ψ también correstringida a su imagen, $\psi' : Q_1 \to \operatorname{Im}\psi$, que es un isomorfismo. Además $\psi'\eta_1(M_1) = \eta_2'\varphi(M_1) = \eta_2'(M_2)$, así que $\eta_1(M_1) = \psi'^{-1}(\eta_2'(M_2))$. Como $\eta_1(M_1) \leq_e Q_1$ y ψ' es un isomorfismo, $\psi'(\eta_1(M_1)) \leq_e \operatorname{Im}\psi$. Pero $\psi'\eta_1(M_1) = \eta_2'(M_2)$ y por lo tanto $\operatorname{Im}\eta_2' \leq_e \operatorname{Im}\psi$. Lo que implica que η_2' es cápsula inyectiva de M_2.

Si ψ es isomorfismo entonces $\eta_2' = \eta$, así que η_2 es cápsula inyectiva de M_2. Recíprocamente, si η_2 es cápsula inyectiva de M_2, entonces $\operatorname{Im}\eta_2 \leq_e Q_2$ pero $\operatorname{Im}\eta_2 \leq \operatorname{Im}\psi$ lo que implica que $\operatorname{Im}\psi \leq_e Q_2$. Como $\operatorname{Im}\psi$ es sumando directo de Q_2, $\operatorname{Im}\psi = Q_2$. Por lo tanto ψ es isomorfismo. □

Teorema 6.3.8. *Si $\varphi : M_1 \to M_2$ es un isomorfismo, $\xi_1 : P_1 \to M_1$ es un epimorfismo y $\xi_2 : P_2 \to M_2$ es una cubierta proyectiva, entonces existe $\psi : P_1 \to P_2$ epimorfismo que se escinde y tal que $\xi_2\psi = \varphi\xi_1$. Si $P_1 = \operatorname{Ker}\psi \oplus P_0$ definiendo $\xi_1' = \xi_1|_{P_0}$ se tiene que ξ_1' es cubierta proyectiva de M_1. Además ψ es isomorfismo si y sólo si ξ_1 es cubierta proyectiva.*

$$\begin{tikzcd}
 & P_1 \arrow[d, "\xi_1"] \arrow[ddl, dashed, "\psi"'] \\
 & M_1 \arrow[d, "\varphi"] \\
P_2 \arrow[r, two heads, "\xi_2"] & M_2
\end{tikzcd}$$

Demostración. Como P_1 es proyectivo, existe $\psi : P_1 \to P_2$ tal que $\xi_2\psi = \varphi\xi_1$. Tenemos que $\operatorname{Im}\psi + \operatorname{Ker}\xi_2 = P_2$ ya que si $x \in P_2$ entonces $\xi_2(x) = \varphi\xi_1(y)$ para algún $y \in P_1$ y $\varphi\xi_1(y) = \xi_2\psi(y)$. Así que $x - \psi(y) \in \operatorname{Ker}\xi_2$. Entonces $x = (x - \psi(y)) + \psi(y)$. Pero $\operatorname{Ker}\xi_2 << P_2$. Por lo tanto $\operatorname{Im}\psi = P_2$, es decir, ψ es un epimorfismo. Como P_2 es proyectivo, ψ se escinde i.e. $P_1 = \operatorname{Ker}\psi \oplus P_0$ y podemos tomar $\xi_1' = \xi|_{P_0}$. Ahora si $\psi(x) = 0$, entonces $0 = \xi_2\psi(x) = \varphi\xi_1(x)$. Como φ es monomorfismo, $\xi_1(x) = 0$. Por lo tanto $\operatorname{Ker}\psi \leq \operatorname{Ker}\xi_1$. Si $m_1 \in M_1$, entonces existe $k + p = x \in P_1$ con $k \in \operatorname{Ker}\psi$ y $p \in P_0$, tal que $m_1 = \xi_1(x)$ pero $\xi_1(x) = \xi'(p)$. Por lo tanto ξ_1' es suprayectiva. Sea $\psi' = \psi|_{P_0}$. Entonces ψ' es un isomorfismo y $\varphi\xi_1' = \xi_2\psi'$. Así que $\xi_1' = \varphi^{-1}\xi_2\psi'$. Se sigue que $\operatorname{Ker}\xi_1' = \psi'^{-1}(\operatorname{Ker}\varphi^{-1}\xi_2) = \psi'^{-1}(\xi_2^{-1}(\operatorname{Ker}\varphi^{-1})) = \psi'^{-1}(\xi_2^{-1}(0)) = \psi'^{-1}(\operatorname{Ker}\xi_2)$. Como el $\operatorname{Ker}\xi_2 << P_2$, $\operatorname{Ker}\xi_1' << P_0$ por el Lema 5.1.25. Por lo tanto ξ_1' es cubierta proyectiva de M_1. Si ahora tenemos que ψ es un isomorfismo entonces $\xi_1' = \xi$. Así que ξ_1 es cubierta proyectiva de M_1. Recíprocamente, si ξ_1 es cubierta proyectiva de M_1 entonces $\operatorname{Ker}\xi_1 << P_1$. Como $\operatorname{Ker}\psi \leq \operatorname{Ker}\xi_1$, $\operatorname{Ker}\psi << P_1$ pero $\operatorname{Ker}\psi$ es sumando directo de P_1. Por lo tanto $\operatorname{Ker}\psi = 0$. En consecuencia, ψ es un isomorfismo. □

Observación 6.3.9. Como consecuencia de los Teoremas 6.3.7 y 6.3.8, tenemos que la cápsula inyectiva y la cubierta proyectiva (si existe) de un módulo M, es única salvo isomorfismo.

Teorema 6.3.10. *Todo R-módulo M tiene cápsula inyectiva.*

Demostración. Sea M un R-módulo. Por el Teorema 6.2.24, existe un monomorfismo $\mu : M \to Q$ con Q inyectivo. Sea $A = \mu(M) \leq Q$. Sean A' un pseudocomplemento de A y A'' un pseudocomplemento de A' tal que $A \subseteq A''$. Entonces $A \leq_e A''$ y A' y A'' son pseudocomplementos uno del otro.

Definimos

$$\alpha : Q \to Q/A' \oplus Q/A'' \quad \text{como} \quad \alpha(q) = (q + A', q + A'')$$

$$\beta : A' \oplus A'' \to Q/A' \oplus Q/A'' \quad \text{como} \quad \beta(a' + a'') = (a'' + A', a' + A'').$$

Sea $i : A' \oplus A'' \to Q$ la inclusión canónica. Entonces $\alpha i = \beta$ y $\operatorname{Im}\beta \subseteq \operatorname{Im}\alpha$. Ahora si $\beta(a' + a'') = 0$, es decir, $(a'' + A', a' + A'') = (0 + A', 0 + A'')$, entonces $a' \in A'' \cap A' = 0$ y $a'' \in A' \cap A'' = 0$. Por lo tanto β es monomorfismo. Si $\alpha(q) = 0$, es decir, $(q + A', q + A'') = (0 + A', 0 + A'')$, entonces $q \in A' \cap A'' = 0$. Por lo tanto α es monomorfismo. Como Q es inyectivo, α se escinde. Por la Proposición 5.1.17, tenemos que $(A'' + A')/A' \leq_e Q/A'$ y $(A' + A'')/A'' \leq_e Q/A''$. Entonces $\operatorname{Im}\beta = (A'' + A')/A' \oplus (A' + A'')/A'' \leq_e Q/A' \oplus Q/A''$ pero $\operatorname{Im}\beta \subseteq \operatorname{Im}\alpha$ y α se escinde lo que implica que $\operatorname{Im}\alpha = Q/A' \oplus Q/A''$. Por lo tanto α es un isomorfismo.

Sea $q \in Q$ y $(q + A', 0 + A'') \in Q/A' \oplus Q/A''$. Como α es suprayectiva, existe $q' \in Q$ tal que $\alpha(q') = (q + A', 0 + A'')$. Entonces $(q' + A', q' + A'') = (q + A', 0 + A'')$, lo que implica que $q' \in A''$ y $q - q' \in A'$. Así $q = (q - q') + q' \in A' \oplus A''$. Por lo tanto $Q = A' \oplus A''$, lo que implica que A'' es inyectivo. Tomemos μ' igual a μ correstringida a A'', es decir, $\mu' : M \to A''$. Entonces μ' es cápsula inyectiva de M. □

Como el Teorema 6.3.10 nos asegura que todo R-módulo tiene cápsula inyectiva y sabemos que la cápsula inyectiva es única salvo isomorfismo, dado un R-módulo M, denotaremos $E(M)$ a su cápsula inyectiva.

Proposición 6.3.11. *Sea M un R-módulo tal que continene una suma directa finita $\bigoplus_{i=1}^n N_i$ esencial. Entonces $E(M) = \bigoplus_{i=1}^n E(N_i)$.*

Demostración. Tenemos que $\bigoplus_{i=1}^n N_i \leq_e M \leq_e E(M)$. Esto implica que $E(M)$ es una cápsula inyectiva de $\bigoplus_{i=1}^n N_i$. Por otro lado, $E\left(\bigoplus_{i=1}^n N_i\right) = \bigoplus_{i=1}^n E(N_i)$ por Lema 6.3.6. Por lo tanto, $E(M) = \bigoplus_{i=1}^n E(N_i)$. □

Proposición 6.3.12. *Sea M un R-módulo y supongamos que $\xi : P \to M$ es una cubierta proyectiva. Sea $\rho : \bigoplus_{i=1}^n N_i \to M$ un epimorfismo superfluo. Si cada N_i tiene cubierta proyectiva $P_i \to N_i$, entonces $P = \bigoplus_{i=1}^n P_i$.*

Demostración. Por el Ejercicio 6.4.18 existe un epimorfismo $\kappa : P \to \bigoplus_{i=1}^n N_i$ tal que $\rho\kappa = \xi$. Esto implica que $\operatorname{Ker}\kappa \leq \operatorname{Ker}\xi$, así que $\operatorname{Ker}\kappa << P$. Por lo tanto κ es una cubierta proyectiva de $\bigoplus_{i=1}^n N_i$. Por el Lema 6.3.6, $\bigoplus_{i=1}^n P_i$ es cubierta proyectiva de $\bigoplus_{i=1}^n N_i$. Por lo tanto $P = \bigoplus_{i=1}^n P_i$. □

Definición 6.3.13. A un monomorfismo esencial $\alpha : A \to B$ le llamamos una *extensión esencial* de A. Decimos que α es *extensión esencial máxima* de A si toda extensión esencial de B es un isomorfismo.

Teorema 6.3.14. *Sea $\gamma : M \to W$ un monomorfismo. Entonces, γ es capsula inyectiva de M si y sólo si γ es extención esencial máxima de M.*

Demostración. Supongamos que W es inyectivo, γ es esencial y que $\beta : W \to B$ es un monomorfismo esencial. Como W es inyectivo β se escinde, es decir, $W \cong \beta(W)$ es sumando directo de B. Pero, $\beta(B) \leq_e B$. Entonces $\beta(W) = B$. Por lo tanto β es un isomorfismo.

Ahora supongamos que γ es extensión esencial máxima. Si $\alpha : M \to Q$ es cápsula inyectiva de M, entonces existe $\beta : W \to Q$ tal que $\beta\gamma = \alpha$. Sea $x \in \operatorname{Im}\gamma \cap \operatorname{Ker}\beta$. Entonces existe $m \in M$ tal que $\gamma(m) = x$ y por otro lado $\beta(x) = 0$. Así, $0 = \beta\gamma(m) = \alpha(m)$, pero α es monomorfismo. Por lo tanto $m = 0$ y $\gamma(m) = x = 0$. Como $\operatorname{Im}\gamma \leq_e W$, $\operatorname{Ker}\beta = 0$. Además $\operatorname{Im}\alpha \subseteq \operatorname{Im}\beta$ y $\operatorname{Im}\alpha \leq_e Q$, por lo tanto $\operatorname{Im}\beta \leq_e Q$. Esto implica que β es extensión esencial de W, pero γ es extensión esencial máxima así que β es isomorfismo. Por lo tanto W es inyectivo y γ es cápsula inyectiva. □

Como hemos visto todo R-módulo tiene cápsula inyectiva. Desgracidamente no es cierto que todo R-módulo tenga cubierta proyectiva como muestra el siguiente ejemplo.

Ejemplo 6.3.15. Consideremos la categoría $\mathbb{Z}$-Mod. Sea $0 \neq n \in \mathbb{Z}$. Consideremos el $\mathbb{Z}$-módulo $\mathbb{Z}/n\mathbb{Z}$. Supongamos que $\xi : P \to \mathbb{Z}/n\mathbb{Z}$ es cubierta proyectiva. Como estamos en $\mathbb{Z}$-Mod, $P = \mathbb{Z}^{(X)}$ para algún conjunto X. Al ser $\mathbb{Z}$ proyectivo, existe $\alpha : \mathbb{Z} \to \mathbb{Z}^{(X)}$ tal que $\pi = \xi\alpha$.

$$\begin{tikzcd}
& \mathbb{Z} \arrow[dl, dashed, "\alpha"'] \arrow[d, "\pi"] \\
\mathbb{Z}^{(X)} \arrow[r, "\xi"'] & \mathbb{Z}/n\mathbb{Z}
\end{tikzcd}$$

Como ξ es un epimorfismo superfluo y π es epimorfismo, α es epimorfismo (Ejercicio 6.4.18). Esto implica que el núcleo de α es sumando directo de $\mathbb{Z}$, pero $\mathbb{Z}$ no tiene sumandos directos no triviales, por lo tanto $\operatorname{Ker}\alpha = 0$. Así α es un isomorfismo. Por lo tanto $\mathbb{Z}^{(X)} \cong \mathbb{Z}$. Esto no puede ser si $|X| > 1$, ya que en $\mathbb{Z}$ todo submódulo es esencial. Por lo tanto $|X| = 1$. Entonces $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ es un epimorfismo superfluo, pero el único submódulo superfluo de $\mathbb{Z}$ es 0. Por lo tanto π es un isomorfismo, que es una contradicción. Por lo tanto $\mathbb{Z}/n\mathbb{Z}$ no tiene cubierta proyectiva.

Existen anillos en los cuales todo módulo tiene cubierta proyectiva. A estos anillos se les llama *perfectos*

6.3.1. Ejemplo de una cápsula inyectiva

En esta sección calcularemos una cápsula inyectiva de un anillo finito usando el Teorema 6.2.24. Considere el siguiente anillo

$$R = \left\{ \begin{pmatrix} a & (x,y) \\ 0 & a \end{pmatrix} \mid a, x, y \in \mathbb{Z}_2 \right\}$$

con las operaciones usuales de matrices y del $\mathbb{Z}_2$-módulo $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. A este anillo se le llama la *extensión trivial* del $\mathbb{Z}_2$ por $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ y se denota como $\mathbb{Z}_2 \ltimes \mathbb{Z}_2 \oplus \mathbb{Z}_2$. El anillo R es un anillo conmutativo finito con 4 ideales no triviales:

$$S_1 = \left\{ \left(\begin{smallmatrix} 0 & (0,0) \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & (1,0) \\ 0 & 0 \end{smallmatrix}\right) \right\}$$

$$S_2 = \left\{ \left(\begin{smallmatrix} 0 & (0,0) \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & (1,1) \\ 0 & 0 \end{smallmatrix}\right) \right\}$$

$$S_3 = \left\{ \left(\begin{smallmatrix} 0 & (0,0) \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & (0,1) \\ 0 & 0 \end{smallmatrix}\right) \right\}$$

$$I = \left\{ \left(\begin{smallmatrix} 0 & (0,0) \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & (1,1) \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & (0,1) \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & (1,0) \\ 0 & 0 \end{smallmatrix}\right) \right\}$$

La retícula de ideales de R se ve de la siguiente manera

$$\begin{tikzcd}[arrows=dash]
 & R \arrow[d] & \\
 & I \arrow[dl] \arrow[d] \arrow[dr] & \\
S_1 \arrow[dr] & S_2 \arrow[d] & S_3 \arrow[dl] \\
 & 0 &
\end{tikzcd}$$

Notemos que I es esencial en R, entonces una cápsula inyectiva para R es una cápsula inyectiva para I. Por el Teorema 6.3.7, la cápsula inyectiva $E(I)$ de I tiene que ser isomorfa a la cápsula inyectiva $E(R)$ de R. Entonces lo que nos interesa calcular es la cápsula inyectiva de uno de los ideales simples S_1, S_2 o S_3 ya que $I = S_i \oplus S_j$ con $i \neq j$. Como grupo abeliano S_1 es isomorfo a $\mathbb{Z}_2$. Notemos que hay un monomorfismo esencial de grupos abelianos $\mathbb{Z}_2 \hookrightarrow \mathbb{Z}_{2^\infty}$ y que $\mathbb{Z}_{2^\infty}$ es divisible. Por el Lema 6.2.23, $\operatorname{Hom}_{\mathbb{Z}}(R, \mathbb{Z}_{2^\infty})$ es un R-módulo inyectivo y por el Teorema 6.2.24, existe un R-monomorfismo $S_1 \hookrightarrow \operatorname{Hom}_{\mathbb{Z}}(R, \mathbb{Z}_{2^\infty})$. Como cada elemento de R tiene orden 2 y en $\mathbb{Z}_{2^\infty}$ solo hay un elemento de orden 2, digamos c, todo morfismo $f \in \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Z}_{2^\infty})$ se factoriza a través del submodulo $\mathbb{Z}c \leq \mathbb{Z}_{2^\infty}$.

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[dr, "\bar{f}"'] & \mathbb{Z}_{2^\infty} \\ & \mathbb{Z}c \arrow[u, hook] \end{tikzcd}$$

Se tiene que $\mathbb{Z}c \cong \mathbb{Z}_2$ como grupos abelianos, así que solo tenemos que describir $\mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Z}_2)$. Para esto notemos que $R \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ como grupos abelianos. Por lo tanto

$$\begin{aligned} &\mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Z}_2) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \mathbb{Z}_2) \\ &\cong \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}_2) \oplus \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}_2) \oplus \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}_2) \cong \mathrm{M}_{1\times 3}(\mathbb{Z}_2), \end{aligned}$$

donde $\mathrm{M}_{1\times 3}(\mathbb{Z}_2)$ es el grupo abeliano de matrices de 1×3 con coeficientes en $\mathbb{Z}_2$. Veamos como es esta acción. Consideremos $(u, v, w) \in \mathrm{M}_{1\times 3}(\mathbb{Z}_2)$ y $\left(\begin{smallmatrix} a & (x,y) \\ 0 & b \end{smallmatrix}\right) \in R$. Entonces

$$(u, v, w) \left(\begin{smallmatrix} a & (x,y) \\ 0 & b \end{smallmatrix}\right) = ua + vx + wy \in \mathbb{Z}_2.$$

El monomorfismo de grupos abelianos $\mu : S_1 \hookrightarrow \mathbb{Z}_{2^\infty}$ está dado por

$$\mu\left(\left(\begin{smallmatrix} 0 & (1,0) \\ 0 & 0 \end{smallmatrix}\right)\right) = c$$

Siguiendo la prueba del Teorema 6.2.24, el monomorfismo $\xi : S_1 \to \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Z}_{2^\infty})$ se calcula como

$$\xi\left(\begin{smallmatrix} 0 & (1,0) \\ 0 & 0 \end{smallmatrix}\right)\left(\left(\begin{smallmatrix} a & (x,y) \\ 0 & a \end{smallmatrix}\right)\right) = \mu\left(\left(\begin{smallmatrix} 0 & (1,0) \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & (x,y) \\ 0 & a \end{smallmatrix}\right)\right) = \mu\left(\left(\begin{smallmatrix} 0 & (a,0) \\ 0 & 0 \end{smallmatrix}\right)\right) = \begin{cases} 0 & \text{si } a = 0 \\ c & \text{si } a = 1 \end{cases}$$

Como $\mathbb{Z}c \cong \mathbb{Z}_2$ mandando c a 1, tenemos que $\xi\left(\begin{smallmatrix} 0 & (1,0) \\ 0 & 0 \end{smallmatrix}\right)$ como morfismo de R a $\mathbb{Z}_2$ se calcula como

$$\xi\left(\begin{smallmatrix} 0 & (1,0) \\ 0 & 0 \end{smallmatrix}\right)\left(\left(\begin{smallmatrix} a & (x,y) \\ 0 & a \end{smallmatrix}\right)\right) = \begin{cases} 0 & \text{si } a = 0 \\ 1 & \text{si } a = 1 \end{cases}$$

Por otro lado

$$(1, 0, 0)\left(\begin{smallmatrix} a & (x,y) \\ 0 & a \end{smallmatrix}\right) = 1a + 0 + 0 = a.$$

Esto implica que bajo el isomorfismo $\mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Z}_{2^\infty}) \cong \mathrm{M}_{1\times 3}(\mathbb{Z}_2)$, $\xi\left(\begin{smallmatrix} 0 & (1,0) \\ 0 & 0 \end{smallmatrix}\right)$ corresponde a $(1, 0, 0)$. Ahora describiremos la estructura de R-módulo izquierdo de $\mathrm{M}_{1\times 3}(\mathbb{Z}_2)$. Sea $\left(\begin{smallmatrix} a & (x,y) \\ 0 & a \end{smallmatrix}\right) \in R$ y $(m, n, w) \in \mathrm{M}_{1\times 3}(\mathbb{Z}_2)$. Así

$$\left[\begin{pmatrix} a & (x,y) \\ 0 & a \end{pmatrix} \cdot (m, n, w)\right]\begin{pmatrix} b & (v,u) \\ 0 & b \end{pmatrix} = (m, n, w)\left[\begin{pmatrix} b & (v,u) \\ 0 & b \end{pmatrix}\begin{pmatrix} a & (x,y) \\ 0 & a \end{pmatrix}\right]$$

$$= (m, n, w)\begin{pmatrix} ab & (av + bx, au + by) \\ 0 & ab \end{pmatrix} = (m, n, w)\begin{pmatrix} ab \\ av + bx \\ au + by \end{pmatrix}$$

$$= mab + n(av + bx) + w(au + by) = b(ma + nx + wy) + v(na) + u(wa).$$

Por lo tanto

$$\begin{pmatrix} a & (x,y) \\ 0 & a \end{pmatrix} \cdot (m, n, w) = (am + xn + yw, an, aw).$$

Con esta acción podemos ver que

$$\begin{pmatrix} 0 & (1,0) \\ 0 & 0 \end{pmatrix} \cdot (0,1,0) = (1,0,0)$$

$$\begin{pmatrix} 0 & (1,0) \\ 0 & 0 \end{pmatrix} \cdot (0,1,0) = (1,0,0)$$

$$\begin{pmatrix} 0 & (0,1) \\ 0 & 0 \end{pmatrix} \cdot (0,0,1) = (1,0,0)$$

$$\begin{pmatrix} 0 & (1,0) \\ 0 & 0 \end{pmatrix} \cdot (0,1,1) = (1,0,0)$$

$$\begin{pmatrix} 0 & (1,0) \\ 0 & 0 \end{pmatrix} \cdot (1,0,1) = (1,0,0)$$

$$\begin{pmatrix} 0 & (1,0) \\ 0 & 0 \end{pmatrix} \cdot (1,1,1) = (1,0,0)$$

Usando la Proposición 5.1.5 tenemos que $\xi : S_1 \to \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Z}_{2^\infty}) \cong \mathrm{M}_{1\times 3}(\mathbb{Z}_2)$ es un monomorfismo esencial, por lo tanto $\mathrm{M}_{1\times 3}(\mathbb{Z}_2)$ es la cápsula inyectiva de S_1. Al principio del ejemplo notamos que $E(R) = E(I)$ y que $I \cong S_1 \oplus S_1$. Por lo tanto una cápsula inyectiva del anillo R es $E(S_1) \oplus E(S_1) = \mathrm{M}_{1\times 3}(\mathbb{Z}_2) \oplus \mathrm{M}_{1\times 3}(\mathbb{Z}_2)$.

$$\begin{tikzcd} S_1 \oplus S_3 \arrow[r, "i"] \arrow[d, "\zeta"'] & R \arrow[dl, dashed, "\overline{\zeta}"] \\ \mathrm{M}_{1\times 3}(\mathbb{Z}_2) \oplus \mathrm{M}_{1\times 3}(\mathbb{Z}_2) & \end{tikzcd}$$

$I = S_1 \oplus S_3$ y $S_3 \cong S_1$. Tenemos que la inclusión canónica i es un monomorfismo esencial y ζ también es un monomorfismo dado por $\zeta\left(\left(\begin{smallmatrix} 0 & (1,0) \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & (0,1) \\ 0 & 0 \end{smallmatrix}\right)\right) = ((1,0,0),(1,0,0))$. Por lo tanto, $\overline{\zeta}$ es un momorfismo esencial. Podemos ver que $\overline{\zeta}$ está definido como

$$\overline{\zeta}\left(\left(\begin{smallmatrix} a & (x,y) \\ 0 & a \end{smallmatrix}\right)\right) = ((x,a,0),(y,a,0)).$$

Veamos que $\overline{\zeta}$ es un R-morfismo.

$$\begin{aligned} \overline{\zeta}\left[\begin{pmatrix} a & (x,y) \\ 0 & a \end{pmatrix}\begin{pmatrix} b & (v,u) \\ 0 & b \end{pmatrix}\right] &= \overline{\zeta}\begin{pmatrix} ab & (av+bx, au+by) \\ 0 & ab \end{pmatrix} \\ &= ((av+bx, ab, 0), (au+by, ab, 0)) \\ &= \begin{pmatrix} a & (x,y) \\ 0 & a \end{pmatrix}((v,b,0),(u,b,0)) \\ &= \begin{pmatrix} a & (x,y) \\ 0 & a \end{pmatrix}\overline{\zeta}\left(\begin{pmatrix} b & (v,u) \\ 0 & b \end{pmatrix}\right) \end{aligned}$$

Así $\overline{\zeta} : R \to \mathrm{M}_{1\times 3}(\mathbb{Z}_2) \oplus \mathrm{M}_{1\times 3}(\mathbb{Z}_2)$ es una cápsula inyectiva del anillo R.

6.4. 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 $\mathbb{Z}_{p^\infty}$ es un subgrupo de $\mathbb{Q}/\mathbb{Z}$.

   b) Demuestre que el conjunto $X = \left\{ \left[\frac{1}{p}\right], \left[\frac{1}{p^2}\right], \ldots \right\}$ generan a $\mathbb{Z}_{p^\infty}$.

   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 $\mathbb{Z}_{p^\infty}$ es esencial.

   f) Demuestre que $\mathbb{Z}_{p^\infty}$ es divisible.

   g) Demuestre que todo $\mathbb{Z}$-morfismo $\varphi : \mathbb{Z}_{p^\infty} \to \mathbb{Z}_{p^\infty}$ 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 $R = \mathrm{TI}_2(K)$.

   a) Demuestre que $\mathrm{Rad}(R)$ es un R-módulo proyectivo.

   b) Demuestre que el R-módulo R/I donde $I = \mathrm{Zoc}(R)$, es inyectivo.

   Vea 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 $R = \{(a_i) \in \prod_I K_i \mid (a_i)$ 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 $\mathrm{End}_R(M)$ es un anillo regular de von Neumann.

    Definición 6.4.1. 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.

17. Sea Q un R-módulo inyectivo. Supongamos que $\varphi : N \to Q$ y $\alpha : N \to M$ son monomorfimos con α monomorfismo esencial. Entonces existe un monomorfismo $\kappa : M \to Q$ tal que $\kappa\alpha = \varphi$.

18. Sea P un R-módulo proyectivo. Supongamos que $\varphi : P \to N$ y $\alpha : M \to N$ son epimorfismos con α epimorfismo superfluo. Entonces existe un epimorfismo $\kappa : P \to M$ tal que $\alpha\kappa = \varphi$.

19. Sea R un anillo. Demuestre que las siguientes afirmaciones son equivalentes:

    (a) Todo cociente de un R-módulo inyectivo es inyectivo.

    (b) Todo ideal izquierdo de R es proyectivo.

20. Sea M un R-módulo y $S = \mathrm{End}_R(M)$. Demuestre que si M es proyectivo e I es un ideal derecho finitamente generado de S, entonces $I = \mathrm{Hom}_R(M, IM)$.

21. Sea M un R-módulo y $S = \mathrm{End}_R(M)$. Demuestre que si M es proyectivo e I, J son ideales derechos de S, entonces $\mathrm{Hom}_R(M, I+J) = \mathrm{Hom}_R(M, I) + \mathrm{Hom}_R(M, J)$.

22. FALTAN EJERCICIOS DE CAPSULAS Y CUBIERTAS PROYECTIVAS

23. Sea P un R-módulo proyectivo. Demuestre que si P es finitamente generado entonces P es cubierta proyectiva de $P/Rad(P)$.

24. Sea $\{K_i\}_I$ una familia de campos. Demuestre que $R = \prod_I K_i$ es cápsula inyectiva de $\bigoplus_I K_i$.

25. Sea K un campo. Demuestre que $\mathrm{M}_2(K)$ como $\mathrm{TI}_2(K)$-módulo es cápsula inyectiva de $\mathrm{TI}_2(K)$.

Capítulo 7

Dos teoremas de descomposición de anillos

7.1. Anillos Locales

Teorema 7.1.1. *Sea R un anillo y $A \subseteq R$ el subconjunto de elementos de R que no tienen inverso multiplicativo. Son equivalentes:*

(a) *A es cerrado bajo suma.*

(b) *A es un ideal bilateral de R.*

(c) *A es el mayor ideal izquierdo (resp. der.) propio de R.*

(d) *En R existe un mayor ideal izquierdo (resp. der.) propio.*

(e) *r o $1-r$ tiene inverso izquierdo (resp. der.) para todo $r \in R$.*

(f) *r o $1-r$ tiene inverso para todo $r \in R$.*

Demostración. (a)$\Rightarrow$(b). Veamos que si un elemento de R tiene inverso por un lado entonces tiene inverso. Sean $b, b' \in R$ tales que $bb' = 1$. Supongamos que $b'b \in A$. Si $1 - b'b \in A$ entonces $b'b + 1 - b'b \in A$ lo que implica que $1 \in A$. Contradicción. Por lo tanto $1 - b'b \notin A$. Entonces existe $s \in R$ tal que $1 = s(1-b'b) = s - sb'b$. Así $b' = sb' - sb'(bb') = sb' - sb'$ y por lo tanto $b' = 0$ lo que implica que $1 = 0$. Contradicción. Así que $b'b$ tiene inverso, es decir, existe $t \in R$ tal que $b'bt = 1$. Se sigue que $b = bb'bt = bt$. Por lo tanto $b'b = b'bt = 1$.

Ahora sea $a \in A$ y $r \in R$, si $ar \notin A$ entonces existe $s \in A$ tal que $ars = 1$ por lo tanto a tiene inverso por la derecha. Por lo anterior a tiene inverso, así que $a \notin A$. Contradicción. Por lo tanto $ar \in A$. Análogamente $ra \in A$. Por lo tanto A es un ideal bilateral de R.

(b)$\Rightarrow$(c). Sea $B < R$ un ideal izquierdo de R. Entonces $Rb \leq B < R$ para todo $b \in B$, así que b no tiene inverso por la izquierda , en particular no tiene inverso lo que implica que $b \in A$. Por lo tanto $B \subseteq A$. Análogamente por la derecha.

(c)$\Rightarrow$(d). Es claro.

(d)$\Rightarrow$(e). Como R tiene un único ideal izquierdo máximo, ese ideal es $Rad(R)$. Además $Rad(R) << R$ así que la implicación se siguen del Lemma 5.3.13.

(e)⇒(f). Sea $b \in R$ tal que $b'b = 1$ para algún $b' \in R$. Si $1 - bb'$ tiene inverso izq. entonces existe $s \in R$ tal que $1 = s(1 - bb') = s - sbb'$ y así $b = sb - sbb'b = b = 0$. Contradicción. Si bb' tiene inverso izquierdo, existe $s \in R$ tal que $sbb' = 1$ lo que implica $b = sbb'b = sb$ y así $1 = sbb' = bb'$. Por lo tanto b tiene inverso.

(f)⇒(a). Sean $a, b \in A$ y supongamos que $a + b \notin A$ entonces existe $s \in R$ tal que $(a + b)s = 1 = as + bs$. Note que con la hipótesis que tenemos podemos ver que si $a \in A$ y $r \in R$ entonces $ar \in R$ como en (a)⇒(b). Entonces $as, bs \in A$ y por lo tanto $as = 1 - bs \in A$ pero $1 - bs$ tiene inverso. Contradicción. □

Definición 7.1.2. Un anillo R se llama *local* si satisface cualquiera de las condiciones del Teorema 7.1.1.

Observación 7.1.3. Si R es local y A es su mayor ideal entonces:

1. R/A es un anillo con división.
2. Todo elemento de R que tenga inverso por un lado tiene inverso.
3. Si $\varphi : R \to S$ es un morfismo de anillos suprayectivo con R local entonces S es local.

Demostración. Solo probaremos *3*. Sea $\varphi : R \to S$ un morfismo de anillos suprayectivo con R local y sea $s \in S$. Entonces existe $r \in R$ tal que $\varphi(r) = s$ y $\varphi(1 - r) = \varphi(1) - \varphi(r) = 1 - s$. Por hipótesis r o $1 - r$ tiene inverso. Si $1 - r$ tiene inverso, digamos t, entonces $1 = \varphi((1 - r)t) = \varphi(1 - r)\varphi(t) = (1 - s)\varphi(t)$ por lo tanto $1 - s$ tiene inverso. Análogamente si r tiene inverso. □

Definición 7.1.4. Un módulo M es *inescindible* si $M \neq 0$ y siempre que $M = U \oplus V$ se tiene que $U = 0$ o $V = 0$.

Lema 7.1.5. *Son equivalentes para un anillo R:*

(a) *${}_RR$ es inescindible.*

(b) *R_R es inescindible.*

(c) *0 y 1 son los únicos idempotentes de R.*

Demostración. (a)⇒(c). Si $e \in R$ es idempotente entonces $R = Re \oplus R(1 - e)$ lo que implica que $Re = 0$ o $Re = R$. Por lo tanto $e = 0$ o $e = 1$.

(c)⇒(a). Si ${}_RR = A \oplus B$ entonces $A = Re$ para algún e idempotente, así que $A = 0$ o $A = R$.

La equivalencia $(b) \Leftrightarrow (c)$ análoga. □

Teorema 7.1.6. *Sea M un módulo y $S = \mathrm{End}_R(M)$. Son equivalentes:*

(a) *M es inescindible.*

(b) *${}_SS$ es inescindible.*

(c) *S_S es inescindible.*

(d) *0 y 1 son los únicos idempotentes de S*

Demostración. (a)$\Rightarrow$(d). Sea $e \in S$ un idempotente entonces $M = e(M) \oplus (1-e)(M)$ pero M es inescindible así que $e(M) = 0$ o $(1-e)(M) = 0$. Si $e(M) = 0$, entonces $e = 0$. Si $(1-e)(M) = 0$ entonces para todo $m \in M$ $0 = m - e(m)$ lo que implica que $e(m) = m$ para todo $m \in M$, es decir, $e = 1$.

(d)$\Rightarrow$(a). Supongamos que $M = A \oplus B$ y tomamos $\eta \in S$ definida como $\eta(a+b) = a$. Entonces η es idempotente. Por hipótesis $\eta = 0$ o $\eta = 1$, lo que implica que $A = 0$ o $B = 0$.

Las demás equivalencias son el Corolario 7.1.5. □

Observación 7.1.7. Notemos que por la Observacion 3.4.11, éste Teorema implica el Lema 7.1.5.

Proposición 7.1.8. *Sea M un módulo y $S = \mathrm{End}_R(M)$. Si S es local entonces M es inescindible.*

Demostración. Sea $e \in S$. Como S es local entonces e o $1-e$ tiene inverso. Por el Ejercicio 3.5.22 $e = 1$ o $1 - e = 1$. □

Corolario 7.1.9. *Si R es local entonces es inescindible.*

Demostración. Tenemos que $R \cong \mathrm{End}_R(R)^{op}$. Por la Proposición 7.1.8 R es inescindible. □

Observación 7.1.10. Notemos que el reciproco del Corolario anterior no es valido. Para esto, considere $\mathbb{Z}$ que es uniforme y por lo tanto inescindible pero $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}) \cong \mathbb{Z}^{op}$ que no es local. Entonces ¿Bajo que condiciones un módulo inescindible tiene anillo de endomorfismos local? Rápidamente por la Proposición 3.4.9, podemos ver que todo módulo simple tiene anillo de endomorfismos local. El siguiente Teorema nos provee de más ejemplos así como el Teorema 8.1.20 que veremos más adelante.

Teorema 7.1.11. *Sea $Q \neq 0$ inyectivo e inescindible entonces* $\mathrm{End}_R(Q)$ *es local.*

Demostración. Si $\varphi \in \mathrm{End}(Q)$ es monomorfismo entonces $\varphi(Q) \neq 0$ es sumando directo de Q pero Q es inescindible, entonces $\varphi(Q) = Q$. Por lo tanto φ es isomorfismo.

Sean $\varphi, \psi \in \mathrm{End}(Q)$ no invertibles, entonces no son monomorfismos, por lo tanto $\mathrm{Ker}\,\varphi \neq 0 \neq \mathrm{Ker}\,\psi$. Si $\mathrm{Ker}\,\varphi$ no es esencial en Q, existe un submódulo $0 \neq N \leq Q$ tal que $\mathrm{Ker}\,\varphi \oplus N \leq_e Q$. Por la Proposición 6.3.11, $Q = E(\mathrm{Ker}\,\varphi) \oplus E(N)$ lo que no puede pasar porque Q es inescindible. Esto implica que $\mathrm{Ker}\,\varphi \cap \mathrm{Ker}\,\psi \neq 0$ y así $\mathrm{Ker}(\varphi + \psi) \neq 0$. Por lo tanto $\varphi + \psi$ no es invertible. Por el Teorema 7.1.1, $\mathrm{End}_R(Q)$ es local. □

7.2. Teorema de Krull-Remak-Schmidt-Azumaya

Lema 7.2.1. *Supongamos que* $M = \bigoplus_I M_i$ *donde cada* $\mathrm{End}_R(M_i)$ *es local. Sean* $\sigma, \tau \in \mathrm{End}(M)$ *tales que* $\sigma+\tau = 1$*. Entonces para cada* $j \in I$ *existe* $U_j \leq M$ *y un isomorfismo* $\varphi_j : M_j \to U_j$ *inducido por* σ *o* τ *tal que* $M = U_j \oplus (\bigoplus_{i\neq j} M_i)$*.*

Demostración. Sea $j \in I$ y tomemos $\pi_j : M \to M_j$ y $\iota_j : M_j \to M$ la proyección y la inclusión canonicas, respectivamente. Escribamos $1 = \pi_j 1 \iota_j = \pi_j(\sigma+\tau)\iota_j = (\pi_j\sigma\iota_j) + (\pi_j\tau\iota)$. Como $\mathrm{End}_R(M)$ es un anillo local, $\pi_j\sigma\iota_j$ es invertible o $\pi_j\tau\iota_j$ es invertible.

Supongamos que $\pi_j\tau\iota_j$ es invertible. Sea $\varphi_j = \tau\iota_j$ y $U_j = \varphi_j(M_j)$. Entonces $\pi_j\varphi_j$ es invertible lo que implica que φ_j es un monomorfismo y por lo tanto un isomorfismo entre M_j y U_j. Además, por el Corolario 3.2.11.(*3*), $M = \mathrm{Im}\,\varphi_j \oplus \mathrm{Ker}\,\pi_j$. Por lo tanto $M = U_j \oplus (\bigoplus_{i\neq j} M_i)$. □

Lema 7.2.2. *Supongamos que* $M = \bigoplus_I M_i$ *con* $\mathrm{End}_R(M_i)$ *local para toda* $i \in I$*, sean* $\sigma, \tau \in \mathrm{End}(M)$ *tales que* $\sigma + \tau = 1$ *y* $E = \{i_1, ..., i_t\} \subseteq I$*. Entonces existen* $C_{i_j} \leq M$ *e isomorfismos* $\varphi_{i_j} : M_{i_j} \to C_{i_j}$ *iducidos por* σ *o* τ *tal que* $M = (C_{i_1} \oplus ... \oplus C_{i_t}) \oplus (\bigoplus_{i\notin E} M_i)$*.*

Demostración. La demostración se sigue por inducción usando el lema anterior. □

Lema 7.2.3. *Supongamos que* $M = \bigoplus_I M_i$ *con cada* $\mathrm{End}_R(M_i)$ *local. Si* $M = A \oplus B$*,* $A \neq 0$ *inescindible y* $\pi : M \to A$ *la proyección canónica entonces existe* $k \in I$ *tal que* π *induce un isomorfismo de* M_k *en* A *y* $M = M_k \oplus B$*.*

Demostración. Sea $\iota : A \to M$ la inclusión canónica y pongamos $\rho = \iota\pi$ así que $\rho \in \mathrm{End}(M)$ además $1 = \rho + (1 - \rho)$. Dado $0 \neq a \in A$, $a = \sum_{j=1}^t m_{i_j}$ con $m_{i_j} \in M_{i_j}$ y $\rho(a) = a$ y $(1 - \rho)(a) = 0$. Aplicando el Lema 7.2.2, existen $\{C_{i_j}\}_{j=1}^t$ submódulos de M tales que $M = (C_{i_1} \oplus ... \oplus C_{i_t}) \oplus (\bigoplus_{i\notin\{i_1,...,i_t\}} M_i)$ con $C_{i_j} \cong M_{i_j}$ e isomorfismos γ_{i_j} inducidos por ρ o $(1 - \rho)$.

Si cada γ_{i_j} estuviera inducido por $1 - \rho$ entonces, tomando a como antes, $0 = (1 - \rho)(a) = (1 - \rho)(\sum_{j=1}^t m_{i_j})$ con $(1 - \rho)(m_{i_j}) = \gamma_{i_j}(m_{i_j})$. Como la suma de los C_{i_j} es directa, cada $\gamma_{i_j}(m_{i_j}) = 0$ y así $m_{i_j} = 0$. Por lo tanto $a = 0$. Contradicción.

Esto implica que al menos un γ_{i_j} esta inducido por ρ. Sea k ese indice que existe y pongamos $M = C_k \oplus L$. Tenemos que $C_k = \rho(M_k) \subseteq \rho(M) \subseteq A$ y $A = (M \cap A) = (C_k \oplus L) \cap A$. Aplicando la ley modular' obtenemos $A = C_k \oplus (L \cap A)$ pero A es inescindible y $C_k \neq 0$ por lo que $L \cap A = 0$. Por lo tanto $A = C_k$, y como γ_k esta inducido por $\rho = \iota\pi$ tenemos que $M = \mathrm{Im}\,\iota \oplus \mathrm{Ker}\,\pi \cong M_k \oplus B$. □

Teorema 7.2.4 (Krull-Remak-Schmidt-Azumaya)**.** *Sea* $M = \bigoplus_I M_i$ *con cada* $\mathrm{End}_R(M_i)$ *local y* $M = \bigoplus_J N_j$ *con cada* N_j *inescindible. Entonces existe una biyección* $\beta : I \to J$ *tal que* $M_i \cong N_{\beta(i)}$ *para toda* $i \in I$*.*

Demostración. Para cada $l \in J$, $M = N_l \oplus (\bigoplus_{j\neq l} N_j)$, por el Lema 7.2.3 $M = M_l \oplus (\bigoplus_{j\neq l} N_j)$ con $M_l \cong N_l$. En particular $\mathrm{End}_R(N_j)$ es local para toda $j \in J$ y como $\mathrm{End}_R(M_i)$ es local, M_i es inescindible para cada $i \in I$. Entonces la condiciones de ambas descomposiciones son simétricas.

Damos a I y J una partición dada por clases de isomorfismo. Sea $\overline{I}$ y $\overline{J}$ los conjunto de clases respectivos. Definimos $\Phi : \overline{I} \to \overline{J}$ como $\Phi(\overline{i}) = \overline{j}$ si $M_i \cong N_j$, la cual esta bien definida por las condiciones simétricas de las descomposiciones. Por el Lema 7.2.3 Φ es suprayectiva.

Para la inyectividad basta demostrar que $|\bar{i}| = |\Phi(\bar{i})|$, para esto usaremos el teorema de Cantor-Schröeder-Bernstein, dando una función inyectiva de $\Phi(\bar{i})$ en $\bar{i}$ que por las condiciones simétricas basta dar sólo esta.

Si $|\bar{i}| \in \mathbb{N}$ supongamos de cardinalidad t y tomemos $k \in \Phi(\bar{i})$, entonces por el Lema 7.2.3 existe M_{i_1} tal que $M = M_{i_1} \oplus (\bigoplus_{j\neq k} N_j)$ con $i_1 \in \bar{i}$ y $N_k \cong M_{i_1}$. Como $|\bar{i}| = t$, esto solo lo podemos repetir a lo más t veces. Por lo tanto $|\Phi(\bar{i})| \leq |\bar{i}|$.

Supongamos ahora que $|\bar{i}|$ es infinito. Sea $\pi_j : M \to N_j$ la proyección canónica para cada $j \in J$ y para cada $k \in I$ sea

$$E(k) = \{j \in J \mid \pi_j \text{ induce isomorfismo } M_k \text{ en } N_j\}$$

Observaciones:

1. Para todo $k \in I$ se tiene que $E(k)$ es finito. Sea $j \in E(k)$ y $0 \neq m \in M_k$ entonces $m = \sum_{l=1}^{t} n_{j_l}$ con $n_{j_l} \in N_{j_l}$, como π_j induce isomorfismo entre M_k y N_j tenemos que $\pi_j(m) \neq 0$ así que $j \in \{j_1, ..., j_t\}$.

2. Tomemos $j \in \Phi(\bar{i})$ i. e. $N_j \cong M_i$. Por el Lema 7.2.3 existe $k \in I$ tal que π_j induce isomorfismo entre N_j y M_k lo que implica que $k \in \bar{i}$. Por lo tanto $j \in \bigcup_{k\in\bar{i}} E(k)$. Por otro lado, sea $k \in \bar{i}$ y $j \in E(k)$, entonces $M_k \cong M_i$ y $M_k \cong N_j$ por lo tanto $N_j \cong M_i$ lo que implica que $j \in \Phi(\bar{i})$. Por lo tanto $\Phi(\bar{i}) = \bigcup_{k\in\bar{i}} E(k)$.

Existe un función inyectiva de $\Phi(\bar{i}) = \bigcup_{k\in\bar{i}} E(k)$ en $\coprod_{k\in\bar{i}} E(k)$ (unión ajena). Como $|\bar{i}|$ es infinito también existe una finción biyectiva entre $\bar{i}$ e $\bar{i}\times\mathbb{N}$. Definimos la siguiente función inyectiva $\alpha : \coprod_{k\in\bar{i}} E(k) \to (\bar{i}\times\mathbb{N})$ como $\alpha(j_t) = (k, t)$ donde $j_t \in E(k)$ y t es según la numeración que se le da a $E(k)$. Por lo tanto tenemos una función inyectiva de $\Phi(\bar{i})$ en $\bar{i}$. □

La condición de que el anillo de endomorfismos $\mathrm{End}_R(M_i)$ sea local es necesaria. Considere el anillo $R = \mathbb{Z}[\sqrt{-5}]$ que es un dominio (de Dedekind). Es claro que todo dominio entero es inescindible. Denotemos $\theta = \sqrt{-5}$. Se puede ver que el ideal $I = \langle 3, 1+\theta\rangle$ no es principal e $I^2 = \langle \theta - 2\rangle \cong R$. Hay un isomorfismo $I \oplus I \cong R \oplus I^2 \cong R \oplus R$, que no satisface la conclución del Teorema de Krull-Remak-Schmidt-Azumaya. [First Course in Noncommutative rings, pp. 287].

Corolario 7.2.5. *Sea $M = \bigoplus_I M_i$ con $\mathrm{End}_R(M_i)$ local para cada $i \in I$ y $N = \bigoplus_J N_j$ con N_j inescindible para cada $j \in J$. Si $M \cong N$ entonces existe una biyección $\beta : I \to J$ tal que $M_i \cong N_{\beta(i)}$.*

Demostración. Sea $\gamma : N \to M$ un isomorfismo, entonces $M = \bigoplus_J \gamma(N_j)$ con cada $\gamma(N_j)$ inescindible. Aplicando el Teorema 7.2.4 tenemos el resultado. □

Corolario 7.2.6. *La descomposición de un módulo semisimple $\bigoplus_I S_i$ queda totalmente determinada en el sentido del Teorema de Krull-Remak-Schmidt-Azumaya.*

7.3. Teorema de Wedderburn-Artin

Proposición 7.3.1. *1. R es semisimple si y sólo si todo R-módulo izquierdo y derecho es semisimple.*

2. Si R es semisimple y $\rho : R \to T$ es un morfismo de anillos suprayectivo entonces T es semisimple.

Demostración. *1*$\Rightarrow$. Tomemos un R-módulo izquierdo M y $x \in M$. Como $Rx \cong R/(0:x)$ y R es semisimple entonces Rx también, además $M = \sum_{x \in M} Rx$. Por lo tanto M es semisimple.

1$\Leftarrow$. Es obvia.

2. Por restriccíon de escalares (Ejemplo 1.2.7.4) T es un R-módulo. Ahora si I es un T-submódulo de T entonces I es un R-submódulo de ${}_RT$ y, recíprocamente si K es un R-submódulo de ${}_RR$ entonces K es un T-submódulo de T porque ρ es sobre. Por lo tanto T es semisimple. □

Lema 7.3.2. *Sea $A \leq {}_RR$ tal que A es un sumando directo. Entonces el ideal bilateral generado por A contiene a todos los ideales izquierdos de R que son cocientes de A.*

Demostración. Supongamos ${}_RR = A \oplus B$. Sea $\pi : R \to A$ la proyección canónica y sea $\varphi : A \to A'$ un epimorfismo con $A' \leq {}_RR$. Tenemos la siguiente composición:

$$R \xrightarrow{\pi} A \xrightarrow{\varphi} A' \xhookrightarrow{i} R$$

que es un endomorfismo de R así que $i\varphi\pi = (\_ \cdot b)$ para algún $b \in R$. Por lo tanto

$$A' = i\varphi\pi(R) = i\varphi\pi(A) = (\_ \cdot b)(A) = Ab \subseteq AR$$

□

Definición 7.3.3. Sea R un anillo. Decimos que R es un *anillo simple* si no contiene ideales bilaterales distintos de los triviales.

Ejemplo 7.3.4. Sea $n > 0$ y K un anillo con división. Entonces el anillo $M_n(K)$ de matrices cuadradas de $n \times n$ con coeficientes en K es un anillo simple por el Ejercicio 1.3.8.

Teorema 7.3.5. *Sea R semisimple y supongamos que ${}_RR = B_1 \oplus ... \oplus B_n$ (resp. $R_R = C_1 \oplus ... \oplus C_m$) donde los B_i son las componentes homogéneas (resp. C_i). Entonces*

1. Cada $B_j = \sum_{i \in \Omega_j} S_i$ es un ideal bilateral y no contiene ideales bilaterales no triviales de R.

2. $n = m$ y $B_i = C_i$

3.
$$B_iB_j = \begin{cases} 0 & i \neq j \\ B_i & i = j \end{cases}$$

4. B_i considerado como anillo es un anillo simple con elemento unitario.

5. *La descomposición de R como suma directa de ideales bilaterales simples es única (salvo el orden).*

Demostración. 1. Veamos que si $S \subseteq B_i$ con S simple entonces $SR = B_i$.

Sea $r \in R$. Tomemos el epimorfismo $(\_ \cdot r) : S \to Sr$. Como S es simple entonces $Sr = 0$ o $S \cong Sr$. Por lo tanto $SR \subseteq B_i$.

Ahora, sea $S' \cong S$, como S es sumando directo de R, por el Lema 7.3.2 $S' \subseteq SR$ por lo tanto $B_i \subseteq SR$.

Ahora como $B_j = \sum S_i$ entonces $B_j R = \sum(S_i R) = \sum B_j = B_j$. Por lo tanto B_j es bilateral.

2. Por el inciso anterior cada C_i es bilateral, entonces $C_j B_i \subseteq C_j$ y $C_j B_i \subseteq B_i$. Como $C_j B_i$ es un ideal bilateral de R, por el inciso (*1*), $C_j B_i = 0$ o $C_j B_i = C_j = B_i$.

Sea $i_0 \in \{1, .., n\}$ fijo. Si para todo $j \in \{1, ..., m\}$ $C_j B_{i_0} = 0$ entonces

$$B_{i_0} = RB_{i_0} = (\bigoplus C_j)B_{i_0} = \bigoplus (C_j B_{i_0}) = 0$$

Contradicción. Por lo tanto existe $j_0 \in \{1, ..., m\}$ tal que $C_{j_0} = B_{i_0}$.

Si C_{j_1} con $j_1 \neq j_0$ es tal que $C_{j_1} = B_{i_0}$ entonces $C_{j_1} = C_{j_0}$, lo que no puede ser.

3. Como $R = \bigoplus B_i$ se tiene que $B_j = B_j R = \bigoplus B_j B_i$. Ya que esta suma es directa $B_j B_i = 0$ si $i \neq j$.

4. Sea A un ideal bilateral de B_i. Entonces usando el inciso anterior

$$RAR = \bigoplus B_j A \bigoplus B_k = \bigoplus B_j A B_k = B_i A B_i$$

ya que los B_i son bilaterales. Por el inciso (*1*) tenemos que $A = 0$ o $A = B_i$.

5. Se sigue de (*2*). □

Definición 7.3.6. Los ideales bilaterales B_i $i = 1, ..., n$ del Teorema 7.3.5 son llamados los *bloques* del anillo semisimple R.

Observación 7.3.7. Si $R = B_1 \oplus ... \oplus B_n$ es semisimple, entonces el número de bloques de R es igual al número de clases de isomorfismos de R-módulos simples $|R - Simp|$.

Teorema 7.3.8. *Sea $_KV$ un espacio vectorial sobre un anillo con división K. Entonces*

1. *Si $1 \leq \dim_K(V) \leq n$ entonces $\mathrm{End}_K(V)$ es un anillo simple y semisimple.*

2. *Si $\dim_K(V) = \infty$, entonces $\mathrm{End}_K(V)$ no es semisimple ni un anillo simple.*

Demostración. 1. Supongamos que $dim_K(V) = n$ entonces $\mathrm{End}_K(V) \cong M_n(K)$. Por el Ejemplo 2.1.4.*2*, 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. Además $M_n(K) = \bigoplus_{i=1}^n S_l$.

2. Supongamos que $dim_K(V) = \infty$. Decimos que $\varphi \in \mathrm{End}_K(V)$ es de rango finito si $dim_K(\mathrm{Im}\,\varphi)$ es finita. Notemos que si φ es de rango finito y $\psi \in \mathrm{End}_K(V)$ entonces $\varphi\psi$ y $\psi\varphi$ son de rango finito. Por lo tanto $A := \{\varphi \in$

$\mathrm{End}(V) \mid \varphi$ es de rango finito$\}$ es un ideal bilateral de $\mathrm{End}_K(V)$. Este ideal no es trivial ya que si $0 \neq v \in V$ entonces $V = Kv \oplus W$ para algún $W \leq V$. Por lo tanto, si π denota la proyección canónica en Kv se tiene que $0 \neq \pi \in A$. Por otro lado $Id_V \notin A$. Por lo tanto $\mathrm{End}_K(V)$ no es un anillo simple.

Si $\mathrm{End}_K(V)$ fuera semisimple entonces $\mathrm{End}_K(V) = A \oplus B$ para algún $B \neq 0$. Como A es bilateral, $AB \subseteq B$ y $AB \subseteq A$ pero $A \cap B = 0$. Por lo tanto $AB = 0$. Sean $0 \neq \beta \in B$ y $v \in V$ tal que $0 \neq \beta(v)$. Tomemos $K\beta(v) \leq V$. Entonces $V = K\beta(v) \oplus U$ y si definimos $\alpha : V \to V$ como $\alpha(k\beta(v) + u) = k\beta(v)$ se tiene que $\alpha \in A$ pero $\alpha\beta(v) = \beta(v) \neq 0$ i.e. $AB \neq 0$. Contradicción. $\square$

Teorema 7.3.9. *Un anillo simple R que posee un ideal izquierdo simple S es isomorfo al anillo de endomorfismos de un espacio vectorial sobre un anillo con división de dimensión finita.*

Demostración. Sea S el ideal izquierdo simple de R. Como S es simple $K := \mathrm{End}_R(S)$ es un anillo con división y S es un espacio vectorial sobre K.

Afirmamos que $R \cong \mathrm{End}_K(S)$. Sea $\Phi : R \to \mathrm{End}_K(S)$ definido como $\Phi(r)(x) = rx$. Es rutina ver que Φ es un morfismo de anillos. Como $\mathrm{Ker}\,\Phi$ es un ideal bilateral de R y R es simple se tiene que $\mathrm{Ker}\,\Phi = 0$. Sea $\xi \in \mathrm{End}_K(S)$ y $\Phi(x)$ con $x \in S$. Si $y \in S$

$$\xi \circ \Phi(x)(y) = \xi(xy) = \xi((\_ \cdot y)(x)) = (\_ \cdot y)\xi(x) = \xi(x)y = \Phi(\xi(x))(y).$$

Por lo tanto $\xi \circ \Phi(x) = \Phi(\xi(x))$ así que $\Phi(S)$ es un ideal izquierdo de $\mathrm{End}_K(S)$. Además como $Id \in \Phi(R)$, $\mathrm{End}_K(S)\Phi(R) = \mathrm{End}_K(S)$. Como R es simple, $SR = R$ así que $\Phi(R) = \Phi(SR) = \Phi(S)\Phi(R)$. Por lo tanto

$$\begin{aligned}\mathrm{End}_K(S) &= \mathrm{End}_K(S)\Phi(R) = \mathrm{End}_K(S)\Phi(S)\Phi(R)\\ &\leq \Phi(S)\Phi(R) = \Phi(R).\end{aligned}$$

Por lo tanto Φ es un isomorfismo. Además como $\mathrm{End}_K(S)$ es simple, por el Teorema 7.3.8 ${}_KS$ es de dimensión finita. $\square$

Corolario 7.3.10 (Teorema de Wedderburn-Artin)**.** *Si R es semisimple entonces $R = R_1 \times \ldots \times R_n$ con $R_iR_j = 0$ si $i \neq j$ y para cada $1 \leq i \leq n$, $R_i \cong \mathrm{M}_{n_i}(D_i)$ con D_i un anillo con división.*

Demostración. Sólo hay que aplicar el Teorema 7.3.9 a cada bloque de R. $\square$

7.4. Ejercicios

1. Demuestre los incisos *1* y *2* de la Observación 7.1.3.

   Definición: Sea R un anillo y $r \in R$. Decimos que r es *nilpotente* si existe $n \in \mathbb{N}$ tal que $r^n = 0$.

2. Demuestre que si r es nilpotente entonces r no tiene inverso pero $1 - r$ sí.

3. Sea D un dominio entero y P un ideal primo de P. La *localización de D en P* es el subanillo de $K(D)$ (campo de fracciones):

$$D_{(P)} = \left\{ \frac{a}{b} \mid b \in D - P \right\}.$$

   Demuestre que

   a) $D_{(P)}$ es un anillo local.

   b) $D_{(P)} \cong \mathrm{End}_D(D_{(P)})$.

4. Sea M un R-módulo y $S = \mathrm{End}_R(M)$. Demuestre que si S es un anillo simple, entonces M no tiene submódulos totalmente invariantes distintos del 0 y M. Demuestre el recíproco o de un contraejemplo.

5. Sea R un anillo local. Demuestre que todo R-módulo finitamente generado tiene cubierta proyectiva.

6. Sean R, S anillos y M un S-R-bimódulo. Considere el anillo $T = \begin{pmatrix} R & 0 \\ M & S \end{pmatrix}$. Suponga que R es un anillo local. Demuestre que el T-módulo $M = \begin{pmatrix} R & 0 \\ M & 0 \end{pmatrix}$ tiene anillo de endomorfismos local. **Hint:** Vea el Ejercicio 3.5.25.

Capítulo 8

Módulos Artinianos y Noetherianos

8.1. Módulos Artinianos y Noetherianos

Definición 8.1.1. Decimos que un módulo M es *Noetheriano* (resp. *Artiniano*) si todo subconjunto no vacío de submódulos de M tiene elementos máximos (resp. mínimos) con respecto a la inclusión. Decimos que un anillo R es *Noetheriano izquierdo* (resp. *Artiniano izquierdo*) si lo es como R-módulo.

Definición 8.1.2. Se dice que un módulo M satisface *la condicion de cadena ascendente (CCA)* (resp. *la condición de cadena descendente (CCD)*), si para toda cadena ascendente (resp. descendente) de submódulos $A_1 \subseteq A_2 \subseteq A_3 \subseteq ...$ (resp. $A_1 \supseteq A_2 \supseteq A_3 \supseteq ...$) tiene sólo un número finito de distintos A_i's, es decir, existe $n > 0$ tal que $A_n = A_{n+i}$ para todo $i > 0$.

Teorema 8.1.3. *Son equivalentes para un módulo M y $A \leq M$:*

(a) *M es Artiniano.*

(b) *A y M/A son Artinianos.*

(c) *M satisface CCD.*

(d) *Todo cociente de M es finitamente cogenerado.*

(e) *Para cada familia no vacía $\{A_i\}_I$ de submódulos de M, existe $J \subseteq I$ finito tal que $\bigcap_I A_i = \bigcap_J A_i$.*

Demostración. (a)⇒(b). Sea $\{A_i\}_I$ un familia de submódulos de $A \leq M$. En particular $\{A_i\}_I$ es una familia de submódulos de M, así que esta familia tiene mínimos. Por lo tanto A es Artiniano. Ahora si $\{A_i/A\}_I$ es una familia de submódulos de M/A, entonces $\{A_i\}_I$ es un familia de submódulos de M. Sea A_0 un mínimo de la familia $\{A_i\}_I$. Entonces, A_0/A es mínimo de la familia A_i/A. Por lo tanto M/A es Artiniano.

(b)⇒(c). Sea $A_1 \supseteq A_2 \supseteq ...$ una cadena descendente de submódulos de M. Tomemos las familias de submódulos $\{A_i \cap A\}_{\mathbb{N}}$ y $\{A_i + A\}_{\mathbb{N}}$. Por hipótesis, estas familias tienen un elemento mínimo, digamos $A_k \cap A$ y $A_l + A$. Sea $n = \text{máx}\{k, l\}$. Tenemos que

$$(A_1 \cap A) \supseteq ... \supseteq (A_k \cap A) = (A_{k+1} \cap A) = ...$$

y

$$(A_1 + A) \supseteq ... \supseteq (A_l + A) = (A_{l+1} + A) = ...$$

entonces $A_n = (A_n + A) \cap A_n = (A_{n+j} + A) \cap A_n = A_{n+j} + (A \cap A_n) = A_{n+j} + (A \cap A_{n+j}) = A_{n+j}$ para toda $j \in \mathbb{N}$.

(c)$\Rightarrow$(a). Si $\{A_i\}_I$ es una familia de submódulos de M sin elementos mínimos, entonces para toda $i \in I$ existe $j \in I$ tal que $A_i \supset A_j$. Si fijamos $i_0 \in I$, entonces existe una cadena $A_{i_0} \supset A_i \supset ...$ estrictamente descendente.

(d)$\Rightarrow$(e). Sea $\{A_i\}_I$ una familia de submódulos de M y $U = \bigcap_I A_i$. Por hipótesis M/U es f.c., así que existe un subconjunto finito $J \subseteq I$ tal que $\bigcap_I A_i = U = \bigcap_J A_i$.

(e)$\Rightarrow$(d). Consideremos la familia de submódulos $\{A_i \leq M \mid U \subseteq A_i\}_I$. Entonces $\bigcap_I A_i = U$. Así que existe un subconjunto finito $J \subseteq I$ tal que $\bigcap_J A_i = U$. Por lo tanto M/U es finitamente cogenerado.

(a)$\Rightarrow$(e). Sea $\{A_i\}_I$ una familia no vacía de submódulos de M. Tomemos $\{\bigcap_F A_i \mid F \subseteq I \text{ finito}\}$. Por hipótesis esta familia tiene mínimo, digamos $\bigcap_{F_0} A_i$. Para cada $j \in I$, $\bigcap_{F_0} A_i \cap A_j \subseteq \bigcap_{F_0} A_i$ lo que implica que $\bigcap_{F_0} A_i \cap A_j = \bigcap_{F_0} A_i$. Por lo tanto $A_j \supseteq \bigcap_{F_0} A_i$. Así $\bigcap_{F_0} A_i \subseteq \bigcap_I A_i$ y por lo tanto $\bigcap_{F_0} A_i = \bigcap_I A_i$.

(e)$\Rightarrow$(c). Sea $A_1 \supseteq A_2 \supseteq ...$ una cadena descendente de submódulos de M. Por hipótesis existe $F \subseteq \mathbb{N}$, finito tal que $\bigcap_{\mathbb{N}} A_i = \bigcap_F A_i$, es decir, existe $n \in \mathbb{N}$ tal que $\bigcap_{i=1}^{n} A_i = \bigcap_I A_i$. Por lo tanto $A_n = A_{n+j}$ para toda $j \in \mathbb{N}$. □

Observación 8.1.4. Dado un módulo M, en la Proposición 5.1.2 se probó que todo submódulo de M tiene un pseudocomplemento y después en el Ejemplo 5.1.19 se vio que en general no cualquier submódulo tiene un suplemento. Sin embargo, si M es Artiniano, entonces todo submódulo tiene suplemento y esto se puede deducir rápidamente de la definición de módulo Artiniano.

La prueba del siguiente teorema es análoga a la del Teorema 8.1.3.

Teorema 8.1.5. *Son equivalentes para un módulo M y $A \leq M$:*

(a) *M es Noetheriano.*

(b) *A y M/A son Noetherianos.*

(c) *M satisface CCA.*

(d) *Todo submodulo de M es finitamente generado.*

(e) *Para toda familia $\{A_i\}_I$ de submódulos de M existe $J \subseteq I$ finito tal que $\sum_I A_i = \sum_J A_i$.*

Corolario 8.1.6. 1. *Si M es una suma finita de módulos Noetherianos (resp. Artinianos) entonces M es Noetheriano (resp. Artiniano).*

2. *Si R es Noetheriano izq. (resp. Artiniano izq.) y ${}_RM$ es f.g. entonces ${}_RM$ es Noetheriano (resp. Artiniano).*

Demostración. Solo probaremos el caso Noetheriano. El caso Artiniano es análogo.

1. Supongamos que $M = \sum_{i=1}^{n} M_i$ con M_i Noetheriano. Haremos la prueba por inducción sobre n. El caso $n = 1$ es trivial. Supongamos que $n > 1$ y que el resultado es cierto para $k < n$. Por hipótesis de inducción $N = \sum_{i=1}^{n-1} M_i$ es Noetheriano. Tenemos que $M/M_n = (N + M_n)/M_n \cong N/(N \cap M_n)$. Como N es Noetheriano, $N/(N \cap M_n) \cong M/M_n$ también y como M_n es Noetheriano se tiene que M es Noetheriano.

2. Dado $0 \neq x \in M$ tenemos el morfismo $\_ \cdot x : R \to M$ y su imagen es $Rx \cong R/\operatorname{Ker} \_ \cdot x$. Como R es Noetheriano, Rx también lo es. Por lo tanto M es Noetheriano ya que $M = \sum_{i=1}^{n} Rx_i$. □

Ejemplo 8.1.7. Los anillos finitos son ejemplos de anillos que son Noetherianos y Artinianos . Por otro lado, el $\mathbb{Z}$-módulo $\mathbb{Z}_{p^\infty}$ con p un número primo es un módulo Artiniano que no es Noetheriano (Ejercicio 6.4.8). Un ejemplo canónico de un anillo Noetheriano que no es Artiniano es $\mathbb{Z}$, ya que todo ideal izquierdo es finitamente generado (de hecho cíclico) y por otro lado la cadena descendente $p\mathbb{Z} \supseteq p^2\mathbb{Z} \supseteq \cdots$ no se estaciona. El siguiente Teorema nos da más ejemplos de anillos Noetherianos.

Teorema 8.1.8 (de la base de Hilbert)**.** *Si R es un anillo Noetheriano izquierdo entonces $R[x]$ es Noetheriano izquierdo.*

Demostración. Sea $0 \neq A$ un ideal izquierdo de $R[x]$ y

$$A_0 = \{a \in R \mid \exists f \in A \text{ tal que } a \text{ es el coeficiente principal de } f\}$$

(supongamos que 0 es el coef. prin. del polinomio cero). Entonces A_0 es un ideal izquierdo de R. Como R es Noetheriano A_0 es f.g. así que existen $c_1, ...c_k \in A_0$ tal que $A_0 = Rc_1 + ... + Rc_k$. Para cada $i \in \{1, ..., k\}$ sea $P_i(x) \in A$ tal que c_i es el coef. prin. de P_i y sea $B = \sum_{i=1}^{k} R[x]P_i \subseteq A$. Multiplicando por potencias de x podemos suponer que los P_i tienen grado n. Afirmamos que para cada $f \in A$, $f = g + h$ donde $g \in B$ y $h = 0$ o $gr(h) \leq n$. Si $f = 0$ o $gr(f) \leq n$. Entonces $f = 0 + f$. Supongamos que $n < gr(f) = t$. Si b es el coef. prin. de f, entonces $b \in A_0$ por lo que existen $r_1, ..., r_k \in R$ tal que $b = r_1c_1 + ... + r_kc_k$. Sea $h_1 = f - x^{t-n} \sum_{i=1}^{k} r_iP_i$ y $g_1 = x^{t-n} \sum_{i=1}^{k} r_iP_i$ entonces $h_1 = 0$ o $gr(h_1) < t$ y $f = g_1 + h_1$. Si $gr(h_1) > n$ podemos aplicar el mismo procedimiento a h_1 obteniendo $h_1 = g_2 + h_2$ con $g_2 \in B$, y $f = (g_1 + g_2) + h_2$. En a lo más $t - n$ pasos tenemos que $f = g + h$ con $g \in B$ y $gr(h) \leq n$ o $h = 0$.

Tenemos que $h = f - g \in A \cap (R + Rx^1 + ... + Rx^n)$. Por otro lado, $R + Rx^1 + ... + Rx^n$ es f.g. como R-módulo, por lo tanto es Noetheriano. Así que $A \cap (R + Rx^1 + ... + Rx^n)$ es f.g. como R-módulo. Entonces $A \cap (R + Rx^1 + ... + Rx^n) = \sum_{j=1}^{l} RQ_j$ con $Q_j \in A$. Se sigue que $A \subseteq B + \sum_{j=1}^{l} RQ_j \subseteq B + \sum_{j=1}^{l} R[x]Q_j \subseteq A$. Por lo tanto A es f.g. y así $R[x]$ es Noetheriano izquierdo. □

Definición 8.1.9.

1. Si $0 = A_0 \subseteq A_1 \subseteq ... \subseteq A_k = M$ es una cadena finita en M, decimos que la *longitud* de la cadena es k.

2. Sea $0 = A_0 \subseteq A_1 \subseteq ... \subseteq A_k = M$ una cadena en M. Un *refinamiento* de esta cadena es una cadena $0 = B_0 \subseteq B_1 \subseteq ... \subseteq B_l = M$ con $k \leq l$ tal que cada $A_i = B_j$ para algún $1 \leq j \leq l$.

3. Si $\mathcal{A} : 0 = A_0 \subseteq A_1 \subseteq ... \subseteq A_k = M$ es una cadena, los *cocientes de* $\mathcal{A}$ son los cocientes A_i/A_{i-1}.

4. Decimos que dos cadenas en M, $\mathcal{A}$ con conjunto de indices I y $\mathcal{B}$ con conjunto de indices J, son *isomorfas* si existe una biyección δ entre los conjuntos de indices tal que $A_i/A_{i-1} \cong B_{\delta(i)}/B_{\delta(i)-1}$.

5. Una cadena finita $\mathcal{C}$ en M se llama *serie de composición* si cada cociente de $\mathcal{C}$ es simple.

6. Decimos que M tiene *longitud finita*, si tiene una serie de composición.

Teorema 8.1.10 (Jordan-Hölder-Schreier)**.** *Cualesquiera dos cadenas en M tienen refinamientos isomorfos.*

Demostración. Tomemos dos cadenas $0 = B_0 \subseteq B_1 \subseteq ... \subseteq B_k = M$ y $0 = C_0 \subseteq C_1 \subseteq ... \subseteq C_l = M$. Para cada $1 \leq j \leq l$ definimos, $B_{ij} = B_i + (B_{i+1} \cap C_j)$. Así $B_i \subseteq B_{ij} \subseteq B_{i+1}$. Entonces $B_i = B_{i0}$ y $B_{i+1} = B_{il}$. Análogamente $C_{ij} = C_j + (C_{j+1} \cap B_i)$. Usando el lema de Zassenhause 3.2.7, tenemos que

$$\frac{B_{ij+1}}{B_{ij}} = \frac{B_i + (B_{i+1} \cap C_{j+1})}{B_i + (B_{i+1} \cap C_j)} \cong \frac{C_j + (C_{j+1} \cap B_{i+1})}{C_j + (C_{j+1} \cap B_i)} = \frac{C_{i+1j}}{C_{ij}}.$$

Como en estos kl isomorfismos aparecen precisamente los kl terminos de los refinamientos, tenemos que los refinamientos son isomorfos. □

Corolario 8.1.11. *Sea M un módulo de longitud finita. Entonces*

1. Toda cadena $\mathcal{B} : 0 = B_0 \subset B_1 \subset ... \subset B_k = M$ puede ser refinada a una serie de composición.

2. Cualesquiera dos series de composición de M son isomorfas.

Demostración. *1.* Por hipótesis existe una serie de composición $\mathcal{C}$ de M. Por el Teorema de Jordan-Hölder-Schreier (Teorema 8.1.10) $\mathcal{B}$ y $\mathcal{C}$ tienen refinamientos isomorfos, digamos $\mathcal{B}^*$ y $\mathcal{C}^*$. Como $\mathcal{C}$ es serie de composición, sólo se refina trivialmente. Quitando los factores repetidos de $\mathcal{C}^*$ y los respectivos de $\mathcal{B}^*$ se tiene un refinamiento $\mathcal{B}^*$ isomorfo a $\mathcal{C}$. Como $\mathcal{C}$ es serie de composición, $\mathcal{B}^*$ también.

2. Tomando la notación anterior tenemos que $\mathcal{B}^* \cong \mathcal{C}$ pero ahora estamos suponiendo que $\mathcal{B}$ es serie de descomposición así que $\mathcal{B} = \mathcal{B}^*$. Por lo tanto $\mathcal{B} \cong \mathcal{C}$. □

Corolario 8.1.12. *Si $M = \bigoplus_{i=1}^n S_i$ es un módulo semisimple, entonces M tiene una serie de composición de tamaño n.*

Demostración. Tomemos la cadena $0 = A_0 \subseteq A_1 \subseteq ... \subseteq A_n = M$ donde $A_j = \bigoplus_{i=1}^j S_i$ con $1 \leq j \leq n$. Esta cadena es una serie de composición ya que $A_{j+1}/A_j \cong S_{j+1}$. □

Corolario 8.1.13. *Sea R un anillo. Si R es semisimple entonces ${}_RR$ y R_R tienen la misma longitud finita.*

Demostración. Es claro que si R es semisimple, entonces ${}_RR$ y R_R son de longitud finita. Se sigue del Teorema 5.2.12 que si tenemos la descomposición ${}_RR = \bigoplus_{i=1}^n Re_i$ en simples izquierdos de R, entonces $R_R = \bigoplus_{i=1}^n e_iR$ es una descomposición en simples derechos de R. Por lo tanto al tomar las series de composición como en el Corolario 8.1.12, éstas quedan del mismo tamaño. □

Teorema 8.1.14. *Sea M un módulo. Entonces, M es de longitud finita si y sólo si M es Artiniano y Noetheriano.*

Demostración. $\Rightarrow$. Sea $\mathcal{C}$ un serie de composición de M de longitud l. Sea $A_1 \subseteq A_2 \subseteq ...$ una cadena ascendente de submódulos de M. Si esta cadena tubiera mas de $l+1$ factores distintos tendriamos una cadena $A_{i_1} \subset A_{i_2} \subset ... \subset A_{i_{l+1}}$ que no es posible por el Corolario 8.1.11. Así que la cadena se estaciona. Por lo tanto M es Noetheriano. Analogamente M es Artiniano.

$\Leftarrow$. Por el Teorema 8.1.5, M es Noetheriano si y sólo si todo submodulo es finitamente generado. Entonces todo submódulo de M tiene máximos. Por lo tanto existe una cadena $M = M \supset M_1 \supset M_2 \supset ...$ tal que M_i es máximo en M_{i-1}. Como M es Artiniano, la cadena se estaciona lo que nos da una serie de composición de M. □

Con las definiciones y resultados anteriores podemos extender el Teorema 5.2.9 de la siguiente manera:

Teorema 8.1.15. *Son equivalentes para un módulo semisimple M:*

(a) *M es de longitud finita.*

(b) *M es Artiniano.*

(c) *M es finitamente generado.*

(d) *M es Noetheriano.*

Demostración. (a)$\Rightarrow$(b) Por el Teorema 8.1.14.

(b)$\Rightarrow$(c) Como M es Artiniano, M es finitamente cogenerado por el Teorema 8.1.3. Se sigue del Teorema 5.2.9 que M es finitamente generado.

(c)$\Rightarrow$(d) Sea $N \leq M$. Por el Teorema 5.2.9, M es finitamente cogenerado y por lo tanto N también. Aplicando el Teorema 5.2.9 ahora a N, obtenemos que N es finitamente generado. Se sigue del Teorema 8.1.5 que M es Noetheriano.

(d)$\Rightarrow$(a) Sea $M \to N$ un epimorfismo. Como M es f.g. (por ser Noetheriano) y semisimple entonces N es f.g. y semisimple. Por el Teorema 5.2.9, N es finitamente cogenerado. Por el Teorema 8.1.3, M es Artiniano. Por lo tanto M es de longitud finita por el Teorema 8.1.14. □

Corolario 8.1.16. *M es semisimple y finitamente generado si y solo si M es Artiniano y* $\mathrm{Rad}(M) = 0$.

Demostración. $\Rightarrow$. Si M es s.s. y f.g. entonces es Artiniano, y como M es s.s. $\mathrm{Rad}(M) = 0$.

$\Leftarrow$. Si M es Artiniano todo submódulo tiene suplemento, así que por el Teorema 5.3.10, M es s.s. Además si M es s.s. y Artiniano entonces es f.g. □

Corolario 8.1.17. *Si M es Artiniano entonces $\frac{M}{\mathrm{Rad}(M)}$ es semisimple.*

Demostración. Sabemos que cocientes de módulos Artinianos son Artinianos, además $\mathrm{Rad}(\frac{M}{\mathrm{Rad}(M)}) = 0$. Así, por el Corolario 8.1.16, $\frac{M}{\mathrm{Rad}(M)}$ es s.s. $\square$

Teorema 8.1.18. *Sean M un módulo y $\varphi \in \mathrm{End}_R(M)$.*

1. *Si M es Artiniano, entonces existe $n_0 \in \mathbb{N}$ tal que, para todo $n \geq n_0$*
$$M = \mathrm{Im}\,\varphi^n + \mathrm{Ker}\,\varphi^n.$$
2. *Si M es Artiniano y φ monomorfismo, entonces φ es isomorfismo.*
3. *Si M es Noetheriano, entonces existe $n_0 \in \mathbb{N}$ tal que, para todo $n \geq n_0$*
$$0 = \mathrm{Ker}\,\varphi^n \cap \mathrm{Im}\,\varphi^n.$$
4. *Si M es Noetheriano y φ epimorfismo entonces φ es isomorfismo.*
5. *Si M es de longitud finita, entonces existe un $n_0 \in \mathbb{N}$ tal que, para todo $n \geq n_0$*
$$M = \mathrm{Ker}\,\varphi^n \oplus \mathrm{Im}\,\varphi^n.$$

Demostración. *1.* Tenemos la cadena descendente $\mathrm{Im}\,\varphi \supseteq \mathrm{Im}\,\varphi^2 \supseteq \ldots$ Como M es Artiniano, existe $n_0 \in \mathbb{N}$ tal que $\mathrm{Im}\,\varphi^{n_0} = \mathrm{Im}\,\varphi^n$ para todo $n \geq n_0$. Sean $x \in M$ y $\varphi^n(x) \in \mathrm{Im}\,\varphi^n = \mathrm{Im}\,\varphi^{2n}$. Entonces existe $y \in M$ tal que $\varphi^n(x - \varphi^n(y)) = 0$. Sea $k = x - \varphi^n(y)$. Entonces $k \in \mathrm{Ker}\,\varphi^n$. Por lo tanto $x = \varphi^n(y) + k$.

2. Por el inciso anterior, existe $n > 0$ tal que $M = \mathrm{Im}\,\varphi^n + \mathrm{Ker}\,\varphi^n$. Como φ es monomorfismo, φ^n también. Lo que implica que $\mathrm{Ker}\,\varphi^n = 0$. Entonces φ^n es suprayectiva. Como $\mathrm{Im}\,\varphi^n \subseteq \mathrm{Im}\,\varphi$ tenemos que φ es un epimorfismo. Por lo tanto φ es un isomorfismo.

3. Tenemos la cadena ascendente $\mathrm{Ker}\,\varphi \subseteq \mathrm{Ker}\,\varphi^2 \subseteq \ldots$ Como M es Noetheriano, existe $n_0 \in \mathbb{N}$ tal que $\mathrm{Ker}\,\varphi^{n_0} = \mathrm{Ker}\,\varphi^n$ para todo $n \geq n_0$. Sea $x \in \mathrm{Ker}\,\varphi^n \cap \mathrm{Im}\,\varphi^n$. Entonces $x = \varphi^n(y)$ para algún $y \in M$ y $0 = \varphi^n(x) = \varphi^{2n}(y)$. Esto implica que $y \in \mathrm{Ker}\,\varphi^{2n} = \mathrm{Ker}\,\varphi^n$. Por lo tanto $\varphi^n(y) = x = 0$.

4. Por el inciso anterior, existe $n > 0$ tal que $0 = \mathrm{Ker}\,\varphi^n \cap \mathrm{Im}\,\varphi^n$. Como φ es epimorfismo, φ^n también. Así, $\mathrm{Im}\,\varphi^n = M$ y por lo tanto $\mathrm{Ker}\,\varphi^n = 0$. Entonces $\mathrm{Ker}\,\varphi = 0$. Por lo tanto φ es un isomorfismo.

5. Se sigue de (*1*) y (*3*). $\square$

Corolario 8.1.19. *Sea M un módulo de longitud finita. Las siguientes condiciones son equivalentes para $\varphi \in \mathrm{End}_R(M)$:*

(a) *φ es isomorfismo.*

(b) *φ es monomorfismo.*

(c) *φ es epimorfismo*

Demostración. (a)$\Leftrightarrow$(b) Se sigue del Teorema 8.1.18.*2*, y (a)$\Leftrightarrow$(c) se sigue del Teorema 8.1.18.*4*. $\square$

Teorema 8.1.20. *Sea M un módulo inescindible y de longitud finita. Entonces $\mathrm{End}_R(M)$ es local y los elementos no invertibles $\mathrm{End}(M)$ son exactamente los elementos nilpotentes.*

Demostración. Sea $\varphi \in \mathrm{End}_R(M)$. Por el Teorema 8.1.18, como M es de longitud de finita, $M = \mathrm{Im}\,\varphi^n \oplus \mathrm{Ker}\,\varphi^n$ par algún $n \in \mathbb{N}$. Al ser M es inescindible, $\mathrm{Im}\,\varphi^n = 0$ o $\mathrm{Ker}\,\varphi^n = 0$.

Si $\mathrm{Ker}\,\varphi^n = 0$ entonces $\mathrm{Ker}\,\varphi = 0$ lo que implica que φ es monomorfismo y como M es de longitud finita φ es un isomorfismo. Si $\mathrm{Im}\,\varphi^n = 0$ entonces $\varphi^n = 0$ así que φ es nilpotente lo que implica que $1 - \varphi$ es isomorfismo. □

Teorema 8.1.21. *Sea $M \neq 0$. Si M es Artiniano o Noetheriano entonces existen submodulos $M_1, ..., M_n$ de M inescindibles tales que $M = \bigoplus_{i=1}^n M_i$. Además si M es de longitud finita cada $\mathrm{End}_R(M_i)$ es local.*

Demostración. Tomemos $\Gamma = \{0 \neq B \leq M \mid B$ es sumando directo$\}$, $\Gamma \neq \phi$ ya que $M \in \Gamma$. Si M es Artiniano Γ tiene mínimos. Sea B_0 un mínimo de Γ. Entonces B_0 es inescindible.

Ahora sea $\Delta = \{C \leq M \mid \exists 0 \neq B_0, ..., B_1 \leq M \; B_i$ ines. tal que $M = B_0 \oplus ... \oplus B_n \oplus C\}$ que por lo anterior $\Delta \neq \phi$. Sea C_0 un mínimo de Δ y supongamos que $M = B_0 \oplus ... \oplus B_n \oplus C_0$. Si $C_0 \neq 0$, como es Artiniano tendría un sumando directo $0 \neq B_{n+1}$ inescindible lo que implicaría que $M = B_0 \oplus ... \oplus B_{n+1} \oplus C_1$, que contradice la minimalidad de C_0. Por lo tanto $C_0 = 0$ y $M = \bigoplus_{i=1}^n B_i$.

Si M es Noetheriano, sea B_0 un máximo en Γ entonces $M = B_0 \oplus C$ y C es inescindible. Sea $\Delta = \{D \leq M \mid D$ es sumando directo de M y $D = B_1 \oplus ... \oplus B_n$ con B_i inescindible$\}$ que es no vacío. Sea $B_1 \oplus ... \oplus B_k$ un máximo. Entonces $M = B_1 \oplus ... \oplus B_k \oplus C$, si $C \neq 0$ como es Noetheriano $C = C_1 \oplus B_{k+1}$ con B_{k+1} inescindible, contradiciendo la maximalidad de $B_1 \oplus ... \oplus B_k$. Por lo tanto $M = \bigoplus_{i=1}^k B_i$ con B_i inescindible. □

Teorema 8.1.22. *Las siguientes condiciones son equivalentes para un anillo R:*

(a) *R es Noetheriano izquierdo.*

(b) *Para cada familia $\{Q_i\}_I$ de R-módulos inyectivos, se tiene que $\bigoplus_I Q_i$ es inyectivo.*

(c) *Para cada familia numerable $\{E(S_i)\}_{\mathbb{N}}$ de cápsulas inyectivas de simples, se tiene que $\bigoplus_{\mathbb{N}} E(S_i)$ es inyectivo.*

Demostración. (a)⇒(b). Denotemos $Q = \bigoplus_I Q_i$. Sean $A \leq R$ y $f : A \to Q$ un morfismo. Como R es Noetheriano, A es f.g. Así que existen $\{u_1, ..., u_n\} \subseteq A$ tales que $A = \sum_{j=1}^n Ru_j$. Para cada $j \in \{1, ..., n\}$, $f(u_j) \in \bigoplus_{I_j} Q_i$ donde I_j es un subconjunto finito de I. Si $I_0 = \bigcup_{j=1}^n I_j$ entonces $f(a) \in \bigoplus_{I_0} Q_i$ para toda $a \in A$. Como $\bigoplus_{I_0} Q_i$ es inyectivo y es un sumando directo de Q, f se extiende a R. Por el Criterio de Baer (Teorema 6.2.16), Q es inyectivo.

(b)⇒(c). Es inmediato.

(c)⇒(a). Supongamos que R no es Noetheriano izquierdo, entonces existe una cadena propia ascendente $A_1 \subset A_2 \subset ...$ de ideales izquierdos de R. Sea $A = \bigcup_{\mathbb{N}} A_i$ que es un ideal de R. Notemos que para cada $a \in A$, existe $n_a \in \mathbb{N}$ mínimo tal que $a \in A_{n_a}$. Sean $i \in \mathbb{N}$ y $c_i \in A - A_i$. Tomemos $(Rc_i + A_i)/A_i \cong Rc_i/(Rc_i \cap A_i)$ que es un cociente de Rc_i. Entonces $(Rc_i + A_i)/A_i$ es cíclico, lo que implica que tiene máximos. Sea N_i/A_i un máximo. Entonces $S_i = \frac{(Rc_i+A_i)/A_i}{N_i/A_i}$ es simple. Notemos que $c_i \notin N_i$ así que $c_i + A_i$ no es cero en S_i. Consideremos $E(S_i)$ y sean ι_i la inclusión de S_i en $E(S_i)$, j_i la inclusión de $(Rc_i + A_i)/A_i$ en A/A_i y π_i la proyección de $(Rc_i + A_i)/A_i$ en S_i. Entonces existe $\eta_i : A/A_i \to E(S_i)$ tal que $\eta_i j_i = \iota_i \pi_i$ con $\eta_i(c_i + A_i) \neq 0$. Definimos $\alpha : A \to \bigoplus_{\mathbb{N}} E(S_i)$ como $\alpha(a) = \sum_{i=1}^{n_a} \eta_i(a + A_i)$. Por hipótesis, existe $\beta : R \to \bigoplus_{\mathbb{N}} E(S_i)$ tal que $\beta|_A = \alpha$. Sea b_i la i-esima componente de $\beta(1)$. Existe $n \in \mathbb{N}$ tal que $b_i = 0$ para $i \geq n$. Sea $a \in A$. Como $\sum^{n_a} \eta_i(a + A_i) = \alpha(a) = \beta(a) = a\beta(1)$, $\eta_i(a + A_i) = 0$ para $i \geq n$ y para toda $a \in A$ pero $\eta_n(c_n + A_n) \neq 0$. Contradicción. Por lo tanto R es Noetheriano izquierdo. $\square$

8.2. Teorema de Hopkins-Levitzki

Definición 8.2.1. Un ideal izq. (resp. der. o bilateral) A de R se llama *nil-ideal* si todo elemento de A es nilpotente. Decimos que A es *nilpotente* si existe $m \in \mathbb{N}$ tal que $A^m = 0$.

Proposición 8.2.2.

1. *Todo ideal izq. (resp. der. o bilateral) nilpotente es un nil-ideal.*
2. *La suma de dos ideales nilpotentes es nilpotente.*
3. *Todo nil-ideal esta contenido en* $\mathrm{Rad}(R)$.
4. *Si* $_RR$ *es Noetheriano, todo ideal bilateral que sea nil-ideal es nilpotente.*

Demostración. 4. Sea $B \leq R$ un ideal bilateral que es nil-ideal. Consideremos la siguiente familia

$$\{_RC \leq R \mid C \text{ es nilpotente y } C \subseteq B\}$$

La familia anterior es no vacía y como $_RR$ es Noetheriano tiene máximos. Sea A un máximo y supongamos que $A < B$. Por (*2*), A es el mayor ideal izq. nilpotente incluido en B. Sea $n \in \mathbb{N}$ tal que $A^n = 0$, entonces $(Ar)^n = (Ar)(Ar)\dots(Ar) = A^n r = 0$ lo que implica que $Ar \leq A$ para todo $r \in R$, así que A es bilateral. Consideremos el conjunto $\{(b : A) \mid b \in B - A\}$, el cual tiene máximos. Sea $(b_0 : A)$ un máximo. Supongamos que existe $x \in R$ tal que $b_0x \notin A$. Entonces $(b_0 : A) \subseteq (b_0x : A)$, por la maximidad de $(b_0 : A)$, tenemos que $(b_0x : A) = (b_0 : A)$. Como $b_0x \in B$ entonces existe $l \in \mathbb{N}$ tal que $(b_0x)^l = 0 \in A$. Por lo tanto existe $k \in \mathbb{N}$ mínimo tal que $(b_0x)^{k-1} \notin A$ y $(b_0x)^k \in A$. Así que $((b_0x)^{k-1} : A) = (b_0 : A)$ lo que implica que $b_0xb_0 \in A$. Entonces, tenemos que para todo $x \in R$ tal que $b_0x \notin A$, $b_0xb_0 \in A$.

Sea $rb_0sb_0 \in Rb_0Rb_0$. Si $b_0s \notin A$ entonces $b_0sb_0 \in A$ y por lo tanto $rb_0sb_0 \in A$. Si $b_0s \in A$ entonces $rb_0sb_0 \in A$. Entonces $(Rb_0)^2 \subseteq A$, por lo que $((Rb_0)^2)^n = 0$. Por la maximidad de A, $Rb_0 \leq A$. Contradiccion. Por lo tanto $A = B$. ☐

Observación 8.2.3. Notemos que existen nil-ideales que no son nilpotentes. Para esto consideremos el anillo

$$R = \frac{\mathbb{Z}[x_1, x_2, ...]}{\ell(\{x_1^2, x_2^3, x_3^4, ...\})}$$

Sea $A = \ell(\{\overline{x_1}, \overline{x_2}, ...\})$. Entonces A es un nil-ideal ya que sus generadores son nilpotentes pero es fácil ver que A no es nilpotente.

Teorema 8.2.4. *Si* $_RR$ *es Artiniano entonces* $\mathrm{Rad}(R)$ *es nilpotente.*

Demostración. Tenemos la siguiente cadena descendente

$$R \supseteq \mathrm{Rad}(R) \supseteq \mathrm{Rad}(R)^2 \supseteq ...$$

Como R es Artiniano existe una $n \in \mathbb{N}$ tal que $\mathrm{Rad}(R)^n = \mathrm{Rad}(R)^{n+l}$ para toda $l \geq 0$. Supongamos que $\mathrm{Rad}(R)^n \neq 0$. Consideremos la familia $\{_RA \leq R \mid \mathrm{Rad}(R)^n A \neq 0\}$. Esta familia no es vacía pues $\mathrm{Rad}(R)$ está en ella. Como $_RR$ es Artiniano podemos tomar un mínimo en la familia, digamos A. Como

$\mathrm{Rad}(R)^n A \neq 0$ existe $a \in A$ tal que $\mathrm{Rad}(R)^n a \neq 0$ y por lo tanto $\mathrm{Rad}(R)^n Ra \neq 0$ pero $Ra \leq A$ lo que implica que $Ra = A$. Así

$$\mathrm{Rad}(R)^n A = \mathrm{Rad}(R)^n Ra = \mathrm{Rad}(R)^{n+1} Ra = \mathrm{Rad}(R)^n Rad(R) Ra$$

$$= \mathrm{Rad}(R)^n Rad(R) a.$$

Por la minimidad de A, $\mathrm{Rad}(R)a = A = Ra$. Ahora, por la Proposición 5.3.8 tenemos que

$$\mathrm{Rad}(R)a = \mathrm{Rad}(R)Ra \subseteq \mathrm{Rad}(Ra) << Ra.$$

Por lo tanto $\mathrm{Rad}(R)a < Ra$. Contradicción. $\square$

Corolario 8.2.5. *1. Si ${}_RR$ es Artiniano entonces* $\mathrm{Rad}(R)$ *es el mayor ideal izq. (resp. der. o bilateral) nilpotente.*

2. Si R es conmutativo y Artiniano entonces $\mathrm{Rad}(R) = \{r \mid r \text{ es nilpotente}\}$.

3. Si ${}_RR$ es Artiniano entonces $\mathrm{Rad}(M) = \mathrm{Rad}(R)M << M$ *para todo R-módulo M (También vale por la derecha).*

Demostración. 1. Por el Teorema 8.2.4, $\mathrm{Rad}(R)$ es nilpotente. Si $A \leq R$ es un ideal nilpotente entonces por la Proposicion 8.2.2.*3* $A \subseteq \mathrm{Rad}(R)$.

2. Como $\mathrm{Rad}(R)$ es nilpotente entonces todos sus elementos son nilpotentes. Ahora, si $a \in R$ es nilpotente con $a^n = 0$ entonces $(Ra)^n = Ra^n = 0$ así que $Ra \subseteq \mathrm{Rad}(R)$. Por lo tanto $a \in \mathrm{Rad}(R)$.

3. Por el Corolario 8.1.17 $R/\mathrm{Rad}(R)$ es s.s., entonces para todo R-modulo M, $\mathrm{Rad}(M) = \mathrm{Rad}(R)M$ por el Teorema 5.3.19. Supongamos que $M = \mathrm{Rad}(R)M + U$, entonces $\mathrm{Rad}(R)(\mathrm{Rad}(R)M + U) + U = M$ lo que implica que $\mathrm{Rad}(R)^2M + U = M$. Inductivamente $\mathrm{Rad}(R)^nM + U = M$ para toda n. Como $\mathrm{Rad}(R)$ es nilpotente entonces $U = M$. $\square$

Observación 8.2.6. Notemos que en inciso (*2*) del corolario anterior, si R no es conmutativo entonces no es cierto. Cosidere el anillo $R = M_2(K)$ de las matrices cuadradas de 2×2 con coeficientes en un campo K. Como se vió en el Ejemplo 5.2.6, R es un anillo semisimple. Además R es Artiniano (es la suma de dos simples), así que $\mathrm{Rad}(R) = 0$. Por otro lado, el elemento $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ es nilpotente.

Definición 8.2.7. Un anillo R se llama *semiprimario* si $\mathrm{Rad}(R)$ es nilpotente y $R/\mathrm{Rad}(R)$ es semisimple.

Teorema 8.2.8. *Sea R un anillo semiprimario. Un R-módulo M es Noetheriano si y sólo si M es Artiniano.*

Demostración. Sea R semiprimario, entonces existe $n \geq 1$ tal que $\mathrm{Rad}(R)^n = 0$. Supongamos que M es un R-módulo Artiniano. Por el Teorema 5.3.19 $\mathrm{Rad}(M) = \mathrm{Rad}(R)M$. Consideremos los R-módulos Artinianos

$$M/\mathrm{Rad}(M), \mathrm{Rad}(M)/\mathrm{Rad}(M)^2, ..., \mathrm{Rad}(M)^{n-1}/\mathrm{Rad}(M)^n = \mathrm{Rad}(M)^{n-1}.$$

Cada uno de estos módulos lo podemos ver como $\frac{R}{\mathrm{Rad}(R)}$-módulo y por lo tanto son semisimples, más aún por el Lemma 5.3.17 y el Teorema 8.1.15 son de longitud finita, en particular Noetherianos. En vista del Lemma 5.3.17 estos cocientes son Noetherianos como R-módulos.

Tenemos la siguiente sucesión exacta corta

$$0 \to \operatorname{Rad}(M)^{n-1} \to \operatorname{Rad}(M)^{n-2} \to \frac{\operatorname{Rad}(M)^{n-2}}{\operatorname{Rad}(M)^{n-1}} \to 0.$$

Por el Teorema 8.1.5, $\operatorname{Rad}(M)^{n-2}$ es Noetheriano. Repitiendo este proceso tenemos que M es Noetheriano. Por simetría se tiene la otra implicación. $\square$

Corolario 8.2.9. *Un anillo R es Artiniano si y sólo si R es semiprimario y Noetheriano.*

Demostración. $\Rightarrow$. Por el Corolario 8.1.17 $R/\operatorname{Rad}(R)$ es semisimple y por el Teorema 8.2.4 $\operatorname{Rad}(R)$ es nilpotente. Por lo tanto R es simprimario. Por el Teorema 8.2.8 R es Noetheriano.

$\Leftarrow$ Se sigue del Teorema 8.2.8. $\square$

Observación 8.2.10. Notemos que el Corolario anterior nos dice que todo anillo Artiniano es Noetheriano. A este resultado se le conoce como *Teorema de Hopkins-Levitzki*.

8.3. Descomposición de Módulos Inyectivos sobre Anillos Noetherianos y Artinianos

Definición 8.3.1. Decimos que un módulo M es *uniforme* si $M \neq 0$ y todo submódulo no cero de M es esencial.

Note que todo módulo uniforme es inescindible pero no al revés. Para esto considere el siguiente ejemplo:

Ejemplo 8.3.2. Tomemos el anillo $\mathbb{Z}_2$ y sea R el anillo $R = \begin{pmatrix} \mathbb{Z}_2 & \mathbb{Z}_2 & 0 \\ 0 & \mathbb{Z}_2 & 0 \\ 0 & \mathbb{Z}_2 & \mathbb{Z}_2 \end{pmatrix}$ el cual tiene 32 elementos. Consideremos el idempotente $e = \left(\begin{smallmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right) \in R$ y sea $M = Re$. Entonces M tiene la forma

$$M = \begin{pmatrix} 0 & \mathbb{Z}_2 & 0 \\ 0 & \mathbb{Z}_2 & 0 \\ 0 & \mathbb{Z}_2 & 0 \end{pmatrix}.$$

Este módulo tiene 8 elementos y tiene 3 submódulos propios distintos de cero:

$$A = \begin{pmatrix} 0 & \mathbb{Z}_2 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},\ B = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & \mathbb{Z}_2 & 0 \end{pmatrix} \text{ and } C = \begin{pmatrix} 0 & \mathbb{Z}_2 & 0 \\ 0 & 0 & 0 \\ 0 & \mathbb{Z}_2 & 0 \end{pmatrix}$$

Como M tiene un único submódulo máximo, M es inescindible, pero $A \cap B = 0$ lo que implica que M no es uniforme.

Proposición 8.3.3. *Sea Q inyectivo. Son equivalentes:*

(a) *Q es uniforme.*

(b) *Q es inescindible.*

(c) *Q es la cápsula inyectiva de cada uno de sus submódulos distintos de cero.*

(d) *Todo submódulo distinto de cero de Q es uniforme.*

(e) *Q es la cápsula inyectiva de un submódulo uniforme.*

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

(b)$\Rightarrow$(c). Sea $0 \neq M \leq Q$ entonces $E(M)$ es un sumando directo de Q pero Q es inescindible. Por lo tanto $E(M) = Q$.

(c)$\Rightarrow$(d). Sea $0 \neq M \leq Q$ y $0 \neq A, B \leq M$. Por hipótesis $A \leq_e Q$, lo que implica que $A \cap B \neq 0$. Por lo tanto M es uniforme.

(d)$\Rightarrow$(e). $E(Q) = Q$.

(e)$\Rightarrow$(a). Sea $M \leq Q$ uniforme tal que $E(M) = Q$. Sean $0 \neq A, B \leq Q$, como $M \leq_e Q$ tenemos que $0 \neq M \cap A$ y $0 \neq M \cap B$, además M es uniforme entonces $(M \cap A) \cap (M \cap B) \neq 0$ así que $A \cap B \neq 0$. Por lo tanto Q es uniforme. □

Corolario 8.3.4. *1. La cápsula inyectiva de un simple es inescindible.*

2. Un módulo inyectivo inescindible Q contiene a lo más un módulo simple.

3. *Si R es Artiniano entonces todo módulo inyectivo Q que sea inescindible es la cápsula inyectiva de un simple.*

Demostración. *1.* Si S es simple entonces S es uniforme lo que implica que $E(S)$ es inescindible.

2. Si $S_1, S_2 \leq Q$ son simples, por la Proposición 8.3.3, $E(S_1) = E(S_2) = Q$ lo que implica que $S_1 \leq_e Q$ y $S_2 \leq_e Q$ y así $S_1 \cap S_2 = S_1 = S_2$.

3. Dado $0 \neq q \in Q$, Rq es f.g. Como R es Artiniano, Rq es Artiniano. Así que existe $S \leq Rq$ simple, al ser Q inescindible se tiene que $E(S) = Q$. □

Proposición 8.3.5. *En $\mathbb{Z}$-Mod, los inyectivos inescindibles, hasta isomorfismo, son $\mathbb{Q}$ y $\mathbb{Z}_{p^\infty}$ con p un número primo.*

Demostración. Sea Q un $\mathbb{Z}$-módulo inyectivo e inescindible. Por el Corolario 8.3.4, Q contiene a lo más un simple. Si S es un simple contenido en Q, entonce $E(S) = Q$. Como S es simple, $S \cong \mathbb{Z}_p$ para algún primo p. Por lo tanto $Q \cong \mathbb{Z}_{p^\infty}$. Si Q no contiene submódulos simples, entonces existe $q \in Q$ de orden infinito. Por lo tanto $\mathbb{Z} \cong \mathbb{Z}q \leq Q$. Por la Proposición 8.3.3, $Q = E(\mathbb{Z}q)$. Por lo tanto, $Q \cong \mathbb{Q}$. □

Lema 8.3.6. *Si R es un anillo Noetheriano izq. entonces cada R-módulo $M \neq 0$ contiene un submódulo uniforme distinto de cero.*

Demostración. Sea $0 \neq M$. Podemos tomar $0 \neq B \leq M$ f.g.. Entonces B es Noetheriano. Sea $\Gamma = \{0 \neq X < B \mid X \text{ es un p.c. en } B\}$. Si Γ es vacío entonces B es uniforme. Supongamos que B no es uniforme, entonces Γ es no vacío. Con la inclusión, Γ es un COPO. Como B es Noetheriano, Γ tiene máximos. Sea X_0 un máximo en Γ y supongamos que es p.c. de U_0 en B.
Afirmamos que U_0 es uniforme. Sea $0 \neq U \leq U_0$ y $L \leq U_0$ tal que $L \cap U = 0$ entonces $U \cap (X_0 + L) = 0$. Si tomamos U' un p.c. de U en B tal que $X_0 + L \subseteq U'$ tenemos que $X_0 \subseteq U' \in \Gamma$ pero X_0 es máximo, así que $U' = X_0$. Esto implica que $L = 0$. Por lo tanto $U \leq_e U_0$ y entonces U_0 es uniforme. □

Proposición 8.3.7. *Son equivalentes para un R-módulo $M \neq 0$:*

(a) *M es finitamente cogenerado.*

(b) $\mathrm{Zoc}(M) \leq_e M$ *y* $\mathrm{Zoc}(M)$ *es f.cog.*

(c) *$E(M) = Q_1 \oplus ... \oplus Q_n$ donde $Q_i = E(S_i)$ para algun simple S_i.*

Demostración. (a)⇒(b). Tenemos que $\mathrm{Zoc}(M) = \bigcap_{A \leq_e M} A$. Sea $L \leq M$ tal que $L \cap \mathrm{Zoc}(M) = 0$. Como M es f.c. existe un subconjunto finito de submódulos esenciales $A_1, ..., A_n$ de M tales que $\bigcap_{i=1}^n A_i \cap L = 0$. Como la intersección finita de esenciales es esencial se tienen que $L = 0$. Por lo tanto $\mathrm{Zoc}(M) \leq_e M$. Claramente, submódulos de f.c. son f.c.

(b)⇒(a). Sea $\{A_i\}_I$ una familia de submódulos de M tales que $\bigcap_I A_i = 0$. Entonces $\bigcap_I \mathrm{Zoc}(A_i) = 0$ y como $\mathrm{Zoc}(A_i) \subseteq \mathrm{Zoc}(M)$ existe un subconjunto finito $J \subseteq I$ tal que $\bigcap_J \mathrm{Zoc}(A_i) = 0$. Usando el Ejercicio 5.4.12 tenemos que

$$0 = \bigcap_J \mathrm{Zoc}(A_i) = \bigcap_J (\mathrm{Zoc}(M) \cap A_i) = \mathrm{Zoc}(M) \cap \left(\bigcap_J A_i \right).$$

Se sigue que $\bigcap_J A_i = 0$ ya que $\mathrm{Zoc}(M) \leq_e M$.

(b)⇒(c). Sea $E(M)$ la cápsula inyectiva de M. Por la hipótesis, $\mathrm{Zoc}(M) \leq_e E(M)$. Como $\mathrm{Zoc}(M)$ es f.c., por el Teorema 5.2.9 $\mathrm{Zoc}(M) = S_1 \oplus ... \oplus S_n$ con S_i simple. Como la cápsula inyectiva conmuta con sumas directas finitas se tiene que

$$E(M) = E(\mathrm{Zoc}(M)) = E(S_1 \oplus ... \oplus S_n) = E(S_1) \oplus ... \oplus E(S_n).$$

(c)⇒(b). Supongamos que $E(M) = E(S_1) \oplus ... \oplus E(S_n)$ con S_i simple. Entonces

$$\mathrm{Zoc}(E(M)) = \mathrm{Zoc}\left(\bigoplus_1^n E(S_i)\right) = \bigoplus_1^n \mathrm{Zoc}(E(S_i)) = \bigoplus_1^n S_i$$

ya que $S_i \leq_e E(S_i)$. Ahora, por el Ejercicio 5.4.12, $\mathrm{Zoc}(M) = M \cap \mathrm{Zoc}(E(M)) = \bigoplus_1^n S_i \cap M = \bigoplus_1^n S_i$ pues como $M \leq_e E(M)$, cada S_i está contenido en M. Por lo tanto $\mathrm{Zoc}(M)$ es f.c. por el Teorema 5.2.9. Como $S_i \leq_e E(S_i)$, $\bigoplus_1^n S_i \leq_e E(M)$ y por lo tanto $\mathrm{Zoc}(M) \leq_e M$. □

Corolario 8.3.8. *Sea M un R-módulo. Entonces M es Artiniano si y sólo si para todo cociente M/U se tiene que:*

1. $\mathrm{Zoc}(M/U) \leq_e (M/U)$
2. $\mathrm{Zoc}(M/U)$ *es f.c.*

Demostración. Es clara tomando en cuenta el Teorema 8.1.3. □

Teorema 8.3.9. *1. ${}_RR$ es Noetheriano si y sólo si todo módulo inyectivo ${}_RQ$ es suma directa de inyectivos inescindibles.*

2. ${}_RR$ es Artiniano si y sólo si todo módulo inyectivo ${}_RQ$ es suma directa de cápsulas inyectivas de módulos simples.

Demostración. 1 ⇒. Sea R Noetheriano izquierdo y Q un R-módulo inyectivo. Por el Lema 8.3.6, podemos tomar una familia máxima de submódulos inyectivos e inescindibles de Q tal que su suma sea directa. Denotemos Q_0 a tal suma. Como R es Noetheriano izquierdo, Q_0 es inyectivo. Por lo tanto $Q = Q_0 \oplus Q_1$. Si $Q_1 \neq 0$, entonces existe $0 \neq N \leq Q_1$ uniforme. Así $Q_1 = E(N) \oplus Q_2$ y $E(N)$ es inyectivo e inescindible, así que $Q = (Q_0 \oplus E(N)) \oplus Q_2$ pero $Q_0 \oplus E(N)$ contradice la maximalidad de Q_0. Por lo tanto $Q_1 = 0$ y $Q = Q_0$.

1 ⇐. Sea $\{S_i\}_{\mathbb{N}}$ una familia numerable de módulos simples. Afirmamos que $M := \bigoplus_{\mathbb{N}} E(S_i)$ es inyectivo. Tenemos que $\mathrm{Zoc}(M) = \bigoplus_{\mathbb{N}} S_i = \mathrm{Zoc}(E(M))$. Por hipótesis $E(M) = \bigoplus_J D_j$ con D_j inyectivo inescindible. Sea $J_1 = \{j \in J \mid \mathrm{Zoc}(D_j) \neq 0\}$, entonces $\mathrm{Zoc}(E(M)) = \bigoplus_{J_1} \mathrm{Zoc}(D_j)$. Por el Corolario 8.3.4, $\mathrm{Zoc}(D_j) = T_j$ con T_j simple. Así que

$$\bigoplus_{\mathbb{N}} S_i = \mathrm{Zoc}(M) = \mathrm{Zoc}(E(M)) = \bigoplus_{J_1} T_j$$

Por el Teorema 7.2.4 cada $S_i \cong T_j$ para algún $j \in J_1$ lo que implica que $E(S_i) \cong D_j$. Por lo tanto $M = \bigoplus_{\mathbb{N}} E(S_i) \cong \bigoplus_{J_1} D_j$ pero $M \leq_e E(M)$ y $\bigoplus_{J_1} D_j$ es un sumando directo de $E(M)$ por lo tanto $E(M) = \bigoplus_{J_1} D_j \cong M$. Por lo tanto M es inyectivo y así ${}_RR$ es Noetheriano por el Teorema 8.1.22.

2 $\Rightarrow$. Por el Corolario 8.2.9 R es Noetheriano, así que por *1* se tiene el resultado.

2 $\Leftarrow$. Sea A un ideal izquierdo de R y consideremos $E(R/A)$. Por hipótesis $E(R/A) = \bigoplus_I E(S_i)$ con S_i simple. Como R/A es cíclico existe un subconjunto finito $J \subseteq I$ tal que $R/A \subseteq \bigoplus_J E(S_i)$, i.e., $E(R/A) = \bigoplus_J E(S_i)$. Por la Proposición 8.3.7 y el Corolario 8.3.8 ${}_RR$ es Artiniano. $\square$

Corolario 8.3.10. *La descomposición de un módulo inyectivo sobre un anillo Noetheriano (resp. de un módulo de longitud finita) dada por el Teorema 8.3.9 está unívocamente determinada en el sentido del Teorema de Krull-Remak-Schmidt-Azumaya.*

Corolario 8.3.11. *Todo módulo inyectivo en $\mathbb{Z}$-Mod es de la forma*

$$\mathbb{Q}^{(X)} \oplus \bigoplus_{p>0} \mathbb{Z}_{p^\infty}^{(Y_p)}$$

donde X y Y_p son conjuntos (posiblemente vacios).

8.4. Ejercicios

1. Demuestre el Teorema 8.1.5.
2. Demuestre el caso Artiniano del Corolario 8.1.6.
3. Demuestre los incisos (*1*), (*2*) y (*3*) de la Proposición 8.2.2.
4. Demuestre que un módulo M es Noetheriano si y solo si toda cadena ascendente de submódulos finitamente generados se estaciona.
5. De un ejemplo de un módulo que no sea Noetheriano y que todo submódulo propio sea finitamente generado.
6. Sea $0 \to A \to B \to C \to 0$ una sucesión exacta corta. Demuestre que si A y C son Noetherianos (resp. Artinianos) entonces B es Noetheriano (resp. Artiniano).
7. Sean $M_1, ..., M_n$ R-módulos Noetherianos (resp. Artinianos). Demuestre que $\bigoplus_{i=1}^n M_i$ es Noetheriano (resp. Artinianos).
8. Sea M un R-módulo y $S = \mathrm{End}_R(M)$. Demuestre que si M es proyectivo y Noetheriano entonces S es un anillo Noetheriano derecho. **Hint:** Vea el Ejercicio 6.4.20.
9. Demuestre que todo dominio de ideales principales es Noetheriano.
10. Sea R un anillo Noetheriano izquierdo. Demuestre que $\mathrm{M}_n(R)$ es un anillo Noetheriano derecho para todo $n > 0$.
11. Demuestre que el anillo $R = \begin{pmatrix} \mathbb{Q} & 0 \\ \mathbb{Q} & \mathbb{Z} \end{pmatrix}$ es un anillo Noetheriano izquierdo pero no derecho. Vea el Ejercicio 3.5.32.
12. Sea R un anillo regular de von Neumann. Demuestre que si R es Noetheriano izquierdo entonces R es semisimple.

    Definición: Un idempotente $e^2 = e$ en un anillo R se llama *primitivo* si no se puede expresar como $e = f + g$ con f y g idempotentes distintos de cero.

13. Sea $e^2 = e \in R$. Si e es primitivo, entonces Re es un R-módulo inescindible.
14. Sea R un anillo Artiniano izquierdo. Demueste que existe un conjunto máximo $\{e_1, .., e_n\}$ de idempotentes ortogonales primitivos tales que $1 = \sum_{i=1}^n e_i$.
15. Sea R un anillo Artiniano e $e \in R$ un idempotente primitivo. Supongamos que $Re/\operatorname{Rad}(Re) = S_1 \oplus S_2$ con S_i simple.
16. Demuestre que todo módulo Noetheriano M contiene una familia $\{U_1, .., U_n\}$ de submódulos uniformes tales que $\bigoplus_{i=1}^n$ es esencial en M.

    Definición: Un elemento $0 \neq c$ en un anillo R se llama *regular* si siempre que $rc = 0$ o $cr = 0$ implica que $r = 0$.

17. Sea $c \in R$. Demuestre que c es regular si y solo si $(\_ \cdot c) : R \to Rc$ es un isomorfismo de R-módulos izquierdos.

18. Demuestre que si R es un anillo Noetheriano izquierdo todo ideal esencial contiene un elemento regular.

Apéndice A

Nociones Básicas de Categorias

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 $\mathrm{Hom}_{\mathcal{C}}(A, B)$, cuyos elementos llamamos *morfismos* y que satisface:

1. Si $(A, B) \neq (C, D)$ entonces $\mathrm{Hom}_{\mathcal{C}}(A, B) \cap \mathrm{Hom}_{\mathcal{C}}(C, D) = \phi$

2. Para cada terna de objetos (A, B, C) en $\mathcal{C}$ existe una función

$$\mathrm{Hom}_{\mathcal{C}}(B, C) \times \mathrm{Hom}_{\mathcal{C}}(A, B) \longrightarrow \mathrm{Hom}_{\mathcal{C}}(A, C)$$

$$(\alpha, \beta) \longmapsto \alpha\beta$$

   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 $1_A \in \mathrm{Hom}_{\mathcal{C}}(A, A)$ tal que $1_B\alpha = \alpha = \alpha 1_A$ para todo $\alpha \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ (Morfismo identidad).

Dada una categoria $\mathcal{C}$ y $\varphi \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ se suele escribir al morfismo φ como una flecha con domino A y codominio B

$$\varphi : A \to B$$

Ejemplo A.1.2. (I) La categoría de Conjuntos, Sets. $Obj(Sets)$ = Clase de los conjuntos
$\mathrm{Hom}_{Sets}(A, B) = \{f : A \to B \mid f \text{ es función}\}$

(II) La categoría de grupos, *Gps*, donde los objetos son grupos y los morfismo 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 $\mathrm{Hom}_{\widehat{G}}(*,*) = G$.

(VII) Espacios Topológicos, Top. $Obj(Top)$=Espacios topológicos. Si X y Y son espacios topológicos $\mathrm{Hom}_{Top}(X,Y)$ 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 $\mathrm{Hom}_A(x,y) = \{*\}$ si $x \leq y$ y $\mathrm{Hom}_A(x,y) = \emptyset$ en otro caso.

Definición A.1.3. Sea $\mathcal{C}$ una categoría y $\varphi \in \mathrm{Hom}_{\mathcal{C}}(M,N)$. Decimos que:

1. φ es *monomorfismo* si siempre que $\varphi f = \varphi g$ para $f, g \in \mathrm{Hom}_{\mathcal{C}}(L,M)$, se tiene que $f = g$.

2. φ es *epimorfismo* si siempre que $f\varphi = g\varphi$ para $f, g \in \mathrm{Hom}_{\mathcal{C}}(N,L)$, se tiene que $f = g$.

3. φ es *bimorfismo* si es monomorfismo y epimorfismo.

4. φ es *isomorfismo* si existe $f \in \mathrm{Hom}_{\mathcal{C}}(N,M)$ 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 objeo $*$ y $\mathrm{Hom}_{\widehat{\mathbb{N}}}(*,*) = \mathbb{N}$. Como $\mathbb{N}$ tiene cancelación y la operación es conmutativa, entonces todo $n \in \mathrm{Hom}_{\widehat{\mathbb{N}}}(*,*)$ es monomorfismo y epimorfismo. De este ejemplo vemos que bimorfismo no implica isomorfismo.

Teorema A.1.5. *Sea $\varphi \in \mathrm{Hom}_R(M,N)$ un morfismo en la categoría R-Mod. Entonces:*

1. φ es monomorfismo $\Leftrightarrow$ φ es inyectiva.

2. φ es epimorfismo $\Leftrightarrow$ φ es suprayectiva o sobre.

3. φ es biyectiva $\Leftrightarrow$ φ es bimorfismo $\Leftrightarrow$ φ 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 $\overline{0} : R(x-y) \to M$. Se tiene que $\varphi i(r(x-y)) = r\varphi(x-y) = 0$ y $\varphi\overline{0}(r(x-y)) = \varphi(0) = 0$, es decir, $\varphi i = \varphi\overline{0}$. Por hipótesis, $i = \overline{0}$ lo que implica que $R(x-y) = 0$ y por lo tanto $x = y$.

$\Leftarrow$. Sean $f, g : L \to M$ 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 $I = \operatorname{Im}\varphi$ y tomemos la proyección canonica $\pi : N \to N/I$ y el morfismo $\overline{0} : N \to N/I$. Sea $m \in M$. Entonces $\pi\varphi(m) = \pi(\varphi(m)) = 0$ y $\overline{0}\varphi(m) = 0$. Como φ es un epimorfismo, $\pi = \overline{0}$. 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 $\Leftrightarrow$ φ 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 $f : N \to M$ tal que $\varphi f = Id_N$ y $f\varphi = Id_M$. Lo que implica que φ es inyectiva y es suprayectiva por lo tanto φ es biyectiva. □

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. □

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 $\varphi : M \to N$:*

(a) *φ es monomorfismo.*

(b) *φ es inyectiva.*

(c) $\operatorname{Ker}\varphi = 0$

(d) *Para todo L en R-Mod, si $\psi : L \to M$ 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 $K = \operatorname{Ker}\varphi$ 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 $K = 0$. □

Corolario A.1.8. *Son equivalentes para un R-morfismo $\varphi : M \to N$:*

(a) *φ es epimorfismo.*

(b) *φ es suprayectiva.*

(c) $Coker(\varphi) = 0$

(d) *Para todo L en R-Mod, si $\psi : N \to L$ es tal que $\psi\varphi = 0$ entonces $\psi = 0$.*

Demostración. Ejercicio. □

Regresemos al contexto general

Proposición A.1.9. *Sea $\mathcal{C}$ una categoría. Sean $\varphi \in \mathrm{Hom}_{\mathcal{C}}(M,N)$ y $\psi \in \mathrm{Hom}_{\mathcal{C}}(N,L)$ entonces:*

1. *φ, ψ monomorfismos $\Rightarrow$ $\psi\varphi$ es monomorfismo.*

2. *φ, ψ epimorfismos $\Rightarrow$ $\psi\varphi$ es epimorfismo.*

3. *$\psi\varphi$ es monomorfismo $\Rightarrow$ φ es monomorfismo.*

4. *$\psi\varphi$ es epimorfismo $\Rightarrow$ ψ 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. □

A.2. Funtores

Definición A.2.1. Sean $\mathcal{C}$ y $\mathcal{D}$ categorías. Un *funtor* $F : \mathcal{C} \to \mathcal{D}$ es una asignación de los $Obj(\mathcal{C})$ en $Obj(\mathcal{D})$ y una asignación de $\mathrm{Hom}_{\mathcal{C}}(A,B)$ en $\mathrm{Hom}_{\mathcal{D}}(F(A),F(B))$ para cada dos objetos A,B de $\mathcal{C}$ de tal manera que se respeta la composición, es decir, si $f \in \mathrm{Hom}_{\mathcal{C}}(B,E)$ y $g \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ entonces $F(fg) = F(f)F(g)$ y $F(1_A) = 1_{F(A)}$.

Observación A.2.2. En la definición anterior al funtor F se le llama *funtor covariante* o simplemente funtor. Si dada $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ se tiene que $F(f) \in \mathrm{Hom}_{\mathcal{D}}(F(B),F(A))$ entonces decimos que el funtor es *contravariante*.

Ejemplo A.2.3. (I) Consideremos la categoría de grupos abelianos Ab y la categoría de conjuntos $Sets$. Hay un funtor $U : Ab \to Sets$ 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 funtor que olvida.*

(II) Sean G,H grupos abelianos y consideremos las categorías $\widehat{G}$ y $\widehat{H}$. Si $f : G \to H$ es un morfismo de grupos abelianos entonces f nos define un funtor $\widehat{f} : \widehat{G} \to \widehat{H}$ definido como: $\widehat{f}(*) = *$ y para cada $g \in \mathrm{Hom}_{\widehat{G}}(*,*) = G$, $\widehat{f}(g) = f(g) \in H = \mathrm{Hom}_{\widehat{H}}(*,*)$. 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 funtor $P : \mathcal{O}(X) \to Sets$ 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. $\mathrm{Hom}_{\mathcal{O}(X)}(U,V) = \{*\}$ damos la siguiente función $r : P(V) \to P(U)$ (el funtor 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 funtor $\pi_1 : Top \to Gps$.

(V) Consideremos la categoria DE cuyos objetos son dominios enteros y los morfismo 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 $\_[x] : Rings \to Rings$ dada por $\_[x](R) = R[x]$, el anillo de polinomios con coeficientes en R, y $\_[x](f) : R[x] \to S[x]$ como $\_[x](f)(\sum r_i x^i) = \sum f(r_i)x^i$ si $f : R \to S$ es un morfismo de anillos, nos define un funtor.

Ejemplo A.2.4. Dado un R-módulo M tenemos el siguiente funtor

$$\mathrm{Hom}_R(M, \_) : R - Mod \to Ab$$

Definido de la siguiente manera: Si N es un R-módulo entonces $\mathrm{Hom}_R(M, N)$ es un grupo abeliano. Ahora, si $f : N \to L$ es un R-morfismo,

$$\mathrm{Hom}_R(M, f) : \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, L)$$

es un morfismo de grupos abelianos que se calcula como $\mathrm{Hom}_R(M, f)(g) = fg$.

De forma análoga tenemos el funtor

$$\mathrm{Hom}_R(\_, M) : R - Mod \to Ab$$

solo que este funtor es contravariante, es decir, si $f : N \to L$ es un R-morfismo entonces

$$\mathrm{Hom}_R(f, M) : \mathrm{Hom}_R(L, M) \to \mathrm{Hom}_R(N, M)$$

calculado como $\mathrm{Hom}_R(f, M)(h) = hf$.

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) $P \in Obj(\mathcal{C})$
   b) $\{\pi_i\}_I$ es una familia de morfismos de $\mathcal{C}$ tale que $\pi_i \in \mathrm{Hom}_{\mathcal{C}}(P, A_i)$.
   c) Para toda familia de morfismos $\gamma_i \in \mathrm{Hom}_{\mathcal{C}}(C, A_i)$ $i \in I$ y $C \in Obj(\mathcal{C})$ existe una única $\gamma \in \mathrm{Hom}_{\mathcal{C}}(C, P)$ 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) $Q \in Obj(\mathbf{C})$
   b) $\{\eta_i\}_I$ es una familia de morfismos de $\mathcal{C}$ tale que $\eta_i \in \mathrm{Hom}_{\mathcal{C}}(A_i, Q)$.
   c) Para toda familia de morfismos $\alpha_i \in \mathrm{Hom}_{\mathcal{C}}(A_i, B)$ $i \in I$ y $B \in Obj(\mathcal{C})$ existe una única $\alpha \in \mathrm{Hom}_{\mathcal{C}}(Q, B)$ 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 $\pi'_i \in \mathrm{Hom}_{\mathcal{C}}(P', A_i)$ es también un* *producto de la familia si y solo si existe un isomorfismo* $\varphi \in \mathrm{Hom}_{\mathcal{C}}(P', P)$ *tal que:*

$$\begin{tikzcd} P' \arrow[r, "\varphi", "\cong"'] \arrow[d, "\pi_i'"'] & P \arrow[dl, "\pi_i"] \\ P_i & \end{tikzcd}$$

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 $\varphi \in \mathrm{Hom}_{\mathcal{C}}(M', M)$ tal que $\pi_i \varphi = \pi_i'$ para todo $i \in I$.

$\Rightarrow$. Sumpongamos que $(P', \{\pi_i'\}_I)$ es un producto entonces existe un único $\varphi' \in \mathrm{Hom}_{\mathcal{C}}(M, M')$ tal que $\pi_i'\varphi' = \pi_i$, entonces $\pi_i(\varphi\varphi') = \pi_i$ pero $\pi_i Id_M = \pi_i$ para toda $i \in I$. Entonces por la unicidad del morfismo tenemos que $\varphi\varphi' = Id_M$. Analogamente se tiene que $\varphi'\varphi = Id_{M'}$. Por lo tanto φ es un isomorfismo.

$\Leftarrow$. Sea $\varphi : \pi' \to P$ un isomorfismo y $\{f_i\}_I$ una familia de morfismos $f_i \in \mathrm{Hom}_{\mathcal{C}}(C, A_i)$ para toda $i \in I$. Entonces existe un único $h : C \to P$ 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 $\gamma' : C \to P'$ 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, $\varphi\gamma' = h$ asi que $\gamma' = \varphi^{-1}h = \gamma$ Por lo tanto $(P', \{\pi_i'\}_I)$ es un producto. □

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* $\eta_i \in \mathrm{Hom}_{\mathcal{C}}(Q_i, Q')$ *es también un coproducto de la familia si y solo si existe un único isomorfismo* $\psi \in \mathrm{Hom}_{\mathcal{C}}(Q, Q')$ *tal que:*

$$\begin{tikzcd} Q \arrow[r, "\psi", "\cong"'] & Q' \\ Q_i \arrow[u, "\eta_i"] \arrow[ur, "\eta_i'"'] & \end{tikzcd}$$

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 $\psi : Q \to Q'$ tal que $\psi\eta_i = \eta_i'$ para toda $i \in I$.

$\Rightarrow$: Supongamos que $(Q', \{\eta_i'\})$ es un coproducto. Entonces exite un único morfismo $\psi' : Q' \to Q$ tal que $\psi'\eta_i' = \eta_i$ para toda $i \in I$. Como $Id_{Q'}\eta_i' = \eta_i'$ y tambien $(\psi')\eta_i' = \eta_i'$, de la unicidad se sigue que $\psi\psi' = Id_{Q'}$. Analogamente $\psi'\psi = Id_Q$. Por lo tanto ψ es un isomorfismo.

$\Leftarrow$: Supongamos que existe $\psi : Q \to Q'$ isomorfismo tal que $\psi\eta_i = \eta_i'$. Tomemos $\{\gamma_i\}_I$ con $\gamma_i \in \mathrm{Hom}_{\mathcal{C}}(Q_i, B)$ para todo $i \in I$. Como $(Q, \{\eta_i\}_I)$ es un coproducto entonces existe un unico $h : Q \to B$ 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 $f' : Q' \to B$ 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 $f' = h\psi^{-1} = f$. □

Ejemplo A.3.4. 1. Sea $\{A_i\}_{i\in I}$ una familia no vacia de conjuntos, el producto cartesiano de la familia se define como

$$\prod_{i\in I} A_i = \left\{ f : I \to \bigcup_{i\in I} A_i \mid f \text{ es función y } f(i) \in A_i \ \forall i \in I \right\}$$

Para cada $i \in I$ definimos $\pi_i : \prod A_i \to A_i$ 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:

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "\varphi"'] & B \arrow[d, "\beta"] \\ M \arrow[r, "\psi"] & N \end{tikzcd}$$

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 $\varphi' : Y \to M$, $\alpha' : Y \to B$ existe un único $\tau : Y \to A$ 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 $\psi' : M \to X$, $\beta' : B \to X$ y $\psi'\varphi = \beta'\alpha$ existe un único $\sigma : N \to X$ tal que $\psi' = \sigma\psi$ y $\beta' = \sigma\beta$.

$$\begin{tikzcd} Y \arrow[dr, dashed, "\tau"] \arrow[drr, "\alpha'"] \arrow[ddr, "\varphi'"'] & & \\ & A \arrow[r, "\alpha"] \arrow[d, "\varphi"'] & B \arrow[d, "\beta"] \\ & M \arrow[r, "\psi"] & N \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "\varphi"'] & B \arrow[d, "\beta"] \arrow[ddr, "\beta'"] & \\ M \arrow[r, "\psi"] \arrow[drr, "\psi'"'] & N \arrow[dr, dashed, "\sigma"] & \\ & & X \end{tikzcd}$$

Proposición A.4.2. *El coproducto fibrado del par (φ, α) y el producto fibrado del par (ψ, β), son unicos salvo isomorfismos.*

Demostración. Sean (ψ, β) y (ψ', β') dos pushouts para (φ, α), entonces por la definición de pullback tenemos que existen $\sigma : N \to X$ y $\rho : X \to N$ tales que $\psi' = \sigma\psi$, $\beta' = \sigma\psi$ y $\psi = \rho\psi'$, $\beta = \rho\beta'$. Asi para $\rho\sigma : N \to N$ tenemos que $\psi = \rho\psi' = \rho\sigma\psi$ y $\beta = \rho\beta' = \rho\sigma\beta$ de lo que se sigue que $\rho\sigma = Id_N$. Analogamente $\sigma\rho = Id_X$ 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 $\tau : Y \to A$ y $\tau' : A \to Y$ tales que $\alpha' = \alpha\tau$, $\varphi' = \varphi\tau$ y $\alpha = \alpha'\tau'$,

$\varphi = \varphi'\tau'$. Para $\tau\tau' : A \to A$ tenemos que $\alpha = \alpha'\tau' = \alpha\tau\tau'$ y $\varphi = \varphi'\tau' = \varphi\tau\tau'$, asi que por lo tanto $\tau\tau' = Id_A$. Analogamente $\tau'\tau = Id_Y$ 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).

$$\begin{tikzcd}
A \cap B \arrow[r, hook, "\alpha"] \arrow[d, hook, "\varphi"'] & B \arrow[d, hook, "\beta"] \\
A \arrow[r, hook, "\psi"'] & C
\end{tikzcd}$$

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).

$$\begin{tikzcd}
A \arrow[r, hook, "\alpha"] \arrow[d, hook, "\varphi"'] & B \arrow[d, hook, "\beta"] \\
C \arrow[r, hook, "\psi"'] & B \cup C
\end{tikzcd}$$

Proposición A.4.4. *Supongamos que tenemos el diagrama conmutativo*

$$\begin{tikzcd}
A \arrow[r, "\alpha"] \arrow[d, "\varphi"'] & B \arrow[d, "\beta"] \\
M \arrow[r, "\psi"] & N
\end{tikzcd}$$

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 $f, g : X \to A$ 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 $h : X \to A$ tal que $\varphi h = \varphi f$ y $\alpha h = \alpha g$ lo que implica que $f = h = g$.

2.(a). Supongmos que tenemos $f, g : N \to X$ 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 $h : N \to X$ 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
  Local, 96
  Opuesto, 29
  Semiprimario, 114
  Simple, 100
  Sub-, 1
  V-, 94
  von Neumann, 83
Anulador, 6, 23

Base, 71
Base Dual, 80
Bimódulo, 28
Bimorfismo, 124
Bloques, 101

Cápsula Inyectiva, 86
Cíclico, 11
Categoría, 123
CCA, 105
CCD, 105
Combinaciones Lineales, 9
Componente Homogenea, 62
Conúcleo, 19
Conjunto
  codirigido, 15
  dirigido, 15
Coproducto, 35, 127
  Fibrado, 41, 129
Criterio de Baer, 81
Cubierta proyectiva, 86

Divisible, 81
Dominio, 73
  Entero, 73

Epimorfismo, 18, 124
  Escinde, 23
  Superfluo, 86
Extensión Esencial, 57, 89

Finitamente Cogenerado, 61
Finitamente Generado, 11
Función
  -tensorial, 46
  Biaditiva, 46
Funtor, 126
  Contravariante, 126
  Covariante, 126

Ideal, 2
  Derecho, 2
  Izquierdo, 2
  Nil-, 113
  Nilpotente, 113
Idempotente, 33
  Ortogonales, 40
  Primitivo, 120
Imagen, 19
Inclusión Canónica, 17
Isomorfismo, 18, 124
  1er Teorema, 22
  2do Teorema, 22
  3er Teorema, 22
  de Anillos, 3

Lemma del Quinto, 26
Ley Modular, 10

Módulo, 4
  Artiniano, 105
  Cociente, 13
  Fiel, 6
  Inescindible, 96
  Inyectivo, 76
  Libre, 71
  Longitud Finita, 108
  Noetheriano, 105
  Proyectivo, 76

Semisimple, 60
Simple, 9
Uniforme, 116
Monomorfismo, 18, 124
Escinde, 23
Esencial, 86
Morfismo, 123
R-, 17
de Anillos, 2
Esencial, 86
Superfluo, 86
Módulo
Bi-, 28

Núcleo, 19
Nilpotente, 103

Objeto, 123

Producto, 35, 127
Fibrado, 41, 129
Tensorial, 45
Proyección Canónica, 18
Pseudocomplemento, 55

Radical, 64
Rechazo, 34
Refinamiento, 107
Regular, 120
Restricción de escalares, 6
Retícula, 15
Completa, 15
Inferiormente continua, 69
Superiormente continua, 16

Serie de Composición, 108
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

Teorema
de la base de Hilbert, 107
Hopkins-Levitzki, 115
Jordan-Hölder-Schreier, 108
Krull-Remak-Schmidt-Azumaya, 98
Traza, 34

Zoclo, 64