Universidad Nacional Autónoma de México

Facultad de Ciencias

Introducción a la suma directa de módulos.

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

Matemática

PRESENTA:

Orea Romero Carolina Stephanie

TUTORA

Dra. Edith Corina Sáenz Valadez

Ciudad de México 2021

II

Índice general

Introducción.

El concepto de módulo surge por primera vez en un trabajo de Richard Dedekin en 1871, pero no de la forma en que lo estudiamos hoy. Para Dedekind los módulos eran lo que en la terminología de hoy son los $\mathbb{Z}$-submódulos de $\mathbb{C}$. Fue el matemático Leopold Kronecker el primero que dio ejemplos de módulos para anillos distintos de $\mathbb{Z}$. Alrededor de 1920 los algebristas Emmy Noether y Michael Artin estudiaron a profundidad el concepto de módulo y quitaron hipótesis que no eran indispensables. De hecho, el matemático Israel Kleiner afirma que fue Noether quien inició el estudio de los módulos de una manera abstracta. En 1950, con la llegada del álgebra homológica, la teoría de módulos cobró vital relevancia.

La teoría de módulos engloba la teoría de los grupos abelianos ($\mathbb{Z}$-módulos) y la de los espacios vectoriales (módulos sobre un campo). Frecuentemente es útil pensar en las propiedades de estos útlimos para comprender nociones de los módulos, pero hay que tener cuidado pues no todos los conceptos de los espacios vectoriales se pueden generalizar a la teoría de módulos, por ejemplo el concepto de base.

En esta tesis estudiaremos la suma directa de los módulos sobre un anillo con uno. La suma directa de módulos es importante ya que el Teorema de Krull-Schmidt afirma que, bajo ciertas condiciones de finitud, todo módulo se puede descomponer de manera única (salvo isomorfismo) en una suma directa de submódulos inescindibles. El resultado anterior facilita el estudio de los módulos ya que, mediante el uso de la descomposición en suma directa del módulo, se reduce el estudio de éste al estudio de los submódulos inescindibles que aparecen en dicha descomposición.

El trabajo consta de 3 capítulos. En el primer capítulo damos la definición de módulo, de homomorfismo de módulos y estudiamos sus principales propiedades. De esta manera, en las primeras secciones recordamos concepto básicos de la teoría de conjuntos y de anillos que serán necesarios en el desarrollo de la teoría de módulos. En el capítulo 2 estudiamos la noción de sumando directo. Para ello, estudiamos los conceptos de homomorfismo que se escinde, endomorfismo idempotente y módulo inescindible. Finalmente en el capítulo 3 estudiamos de manera profunda el concepto de suma directa. Para esto, iniciamos estudiando la noción de producto directo para luego estudiar la noción de coproducto. Una vez establecida la noción de coproducto finalizamos el trabajo estableciendo el concepto de suma directa externa y el de suma directa interna.

Capítulo 1

Preliminares

En este capítulo abordaremos los conceptos fundamentales para el estudio de la suma directa de módulos, dando por conocida la Teoría básica de grupos. Definiremos a los conjuntos parcialmente ordenados, al producto cartesiano de conjuntos y algunos conceptos básicos de anillos y módulos. Enfatizando en éstos últimos daremos la definición de homomorfismo de módulos, veremos algunas caracterizaciones importantes y enunciaremos los Teoremas de isomorfismo de módulos.

1.1. Conjuntos parcialmente ordenados.

En esta sección definiremos algunos conceptos que utilizaremos más adelante. Para mayor información se puede consultar el siguiente libro [5].

Definición 1.1.1. *Una relación $\leq$ en un conjunto P es un* ***orden parcial*** *en P si es reflexiva, transitiva y antisimétrica. Un par $(P, \leq)$ que consiste de un conjunto y un orden parcial es llamado* ***conjunto parcialmente ordenado****. Por simplicidad escribiremos P en lugar de $(P, \leq)$.*

Definición 1.1.2. *Sea P un conjunto parcialmente ordenado. Un elemento $m \in P$ es* ***maximal (minimal)*** *en P si para todo $x \in P$ con $x \geq m$ $(x \leq m)$ implica que $x = m$.*

Definición 1.1.3. *Sean P un conjunto parcialmente ordenado y $A \subseteq P$.*

1. *Un elemento $e \in A$ es* ***mayor (menor)*** *en A, si para todo $x \in A$ se tiene que $x \leq e$ $(e \leq x)$.*

2. *Decimos que $b \in P$ es una* ***cota superior (inferior)*** *de A si para toda $a \in A$ se tiene que $a \leq b$ $(b \leq a)$.*

3. *Decimos que un elemento $x \in P$ es* ***supremo (ínfimo)*** *de A si es el menor (mayor) del conjunto de todas las cotas superiores (inferiores) de A. Y lo denotaremos por $supA$, $(infA)$.*

Notemos que no todo subconjunto de un conjunto parcialmente ordenado tiene elemento mayor o menor, pero de tenerlo este es único.

Definición 1.1.4. *Sean P un conjunto parcialmente ordenado y $P_1 \subseteq P$. Decimos que P_1 es una* ***cadena*** *de P si para cualesquiera dos elementos $a, b \in P_1$ se tiene que $a \leq b$ ó $b \leq a$.*

Definición 1.1.5. *Dado un conjunto parcialmente ordenado P y P_1 una cadena de P. Decimos que la cadena P_1 está* ***acotada superiormente (inferiormente)****, si tiene cota superior (inferior).*

Definición 1.1.6. *Una* ***retícula (retícula completa)****, es un conjunto parcialmente ordenado P en el cuál cada par de elementos (cada subconjunto) de P tiene supremo e ínfimo.*

1.2. Producto cartesiano de conjuntos.

En esta sección daremos la definición de conjunto de índices y producto cartesiano de conjuntos [5], las cuales serán de utilidad en el Capítulo 3.

Definición 1.2.1. *Sea $\mathcal{A}$ una familia de conjuntos. Una* ***función indizadora*** *para $\mathcal{A}$ es una función suprayectiva $\sigma : I \to \mathcal{A}$, donde I es un conjunto no vacío. I es llamado* ***conjunto de índices****. La colección $\mathcal{A}$, junto con la función indizadora es llamada* ***familia indizada de conjuntos****. Y la denotaramos por $\{A_\alpha\}_{\alpha \in I}$.*

Ejemplo 1.2.2. *Cualquier familia no vacía de conjuntos $\mathcal{A}$ puede considerarse como una familia indizada de conjuntos, donde la función indizadora es $\sigma : \mathcal{A} \to \mathcal{A}$ dada por $\sigma(A) = A$ y el conjunto de índices es el el mismo $\mathcal{A}$. A saber $\mathcal{A} = \{A_\alpha : \alpha \in \mathcal{A}\}$.*

Definición 1.2.3. *Sea $\{A_\alpha\}_{\alpha \in I}$ una familia indizada de conjuntos. El* ***producto cartesiano de la familia*** *$\{A_\alpha\}_{\alpha \in I}$, denotado por $\bigtimes_{\alpha \in I} A_\alpha$ lo definimos como el conjunto de todas las funciones que van de I a $\bigcup_{\alpha \in I} A_\alpha$, representadas por $\sigma = (a_\alpha)_{\alpha \in I}$, tales que $\sigma(\alpha) = a_\alpha \in A_\alpha$ para cada $\alpha \in I$, a las cuales algunas veces llamaremos I-***tuplas****. Esto es*

$$\bigtimes_{\alpha \in I} A_\alpha = \{\sigma : I \to \bigcup_{\alpha \in I} A_\alpha : \ \forall \alpha \in I \ \sigma(\alpha) \in A_\alpha\}.$$

Si $\beta \in I$, al conjunto A_β lo llamaremos el **β-ésimo factor** del producto $\bigtimes_{\alpha \in I} A_\alpha$. La **coordenada β-ésima** de un elemento $(\sigma(\alpha))_{\alpha \in I}$ en el producto $\bigtimes_{\alpha \in I} A_\alpha$ es por definición $a_\beta = \sigma(\beta)$.
Si $I = \{1, 2, ..., n\}$ entonces $\bigtimes_{\alpha \in I} A_\alpha = A_1 \times A_2 \times ... \times A_n$. Notemos además que si $A = A_\alpha$ para cada $\alpha \in I$, entonces el producto cartesiano $\bigtimes_{\alpha \in I} A_\alpha = A^I$.

Ejemplo 1.2.4. *Consideremos al conjunto de índices* $I = \mathbb{N}$ *y* $A_n = \{0, 1\}$ *para cada* $n \in \mathbb{N}$. *El producto cartesiano* $\bigtimes_{n\in N} A_n$ *es precisamente el conjunto de todas las sucesiones de ceros y unos, a veces llamado* ***Conjunto de Cantor***.

Definición 1.2.5. *Para cada* $\alpha \in I$, *definimos la* α***-ésima proyección*** $\pi_\alpha : \bigtimes_{\alpha\in I} A_\alpha \to A_\alpha$ *dada por* $\pi_\alpha((a_\beta)_{\beta\in I}) = a_\alpha$.

Notemos que si $\sigma, \sigma' \in \bigtimes_{\alpha\in I} A_\alpha$, entonces $\sigma = \sigma'$ si y solo si $\pi_\alpha\sigma = \pi_\alpha\sigma'$ para toda $\alpha \in I$. Este hecho establece una afirmación de unicidad que enunciaremos en el siguiente lema.

Lema 1.2.6. *Sean* $\{A_\alpha\}_{\alpha\in I}$ *una familia indizada de conjuntos no vacíos y* Y *un conjunto, para cada* $\alpha \in I$ *sea* $f_\alpha : Y \to A_\alpha$ *una función . Entonces existe una única función* $f : Y \to \bigtimes_{\alpha\in I} A_\alpha$ *tal que* $\pi_\alpha f = f_\alpha$ *para cada* $\alpha \in I$.

□

1.3. Anillos.

En esta sección daremos algunas definiciones básicas tales como, anillo, ideal, homomorfismo de anillos, las cuales nos serán de gran utilidad para entender el concepto de módulo, el cual introduciremos en la siguiente sección.
Para profundizar en la Teoría de Anillos podemos consultar el siguiente libro [7].

Definición 1.3.1. *Un* ***anillo*** $(R, +, \cdot)$ *es una terna donde* R *es un conjunto no vacío y* $+, \cdot$ *denotan dos operaciones binarias, la operación* $+ : R \times R \to R$ *llamada suma y la operación* $\cdot : R \times R \to R$ *llamada producto que satisfacen las siguientes propiedades:*

1. *El par* $(R, +)$ *es un grupo abeliano, es decir, la operación* $+$ *es asociativa, conmutativa, tiene neutro aditivo* $0 \in R$ *y cada* $r \in R$ *tiene inverso aditivo* $-r \in R$.

2. *El producto es asociativo, es decir, para cualesquiera* $a, b, c \in R$ *se tiene que* $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

3. *La suma y el producto se relacionan mediante las propiedades distributivas. Es decir, para cualesquiera* $a, b, c \in R$ *se tiene que:*

   - $a \cdot (b + c) = a \cdot b + a \cdot c$.
   - $(a + b) \cdot c = a \cdot c + b \cdot c$.

Algunas veces nos referiremos a un anillo $(R, +, \cdot)$ simplemente como R.

Definición 1.3.2. *Si el anillo R satisface además que existe un elemento $1 \in R$ tal que $1 \cdot r = r = r \cdot 1$ para todo $r \in R$, diremos que R es un* ***anillo con elemento unitario*** *o* ***anillo con uno****.*

Definición 1.3.3. *Si en un anillo R el producto es conmutativo, es decir para todo $a, b \in R$ se tiene que $a \cdot b = b \cdot a$, decimos que R es un* ***anillo conmutativo****.*

Ejemplo 1.3.4. *El conjunto de los números enteros $\mathbb{Z}$ es un anillo conmutativo con uno, con la suma y el producto usuales.*

Ejemplo 1.3.5. *Consideremos $(M, +)$ un grupo abeliano y el conjunto*

$$End^i(M) = \{f : M \to M : f \text{ es un homomorfismo de grupos}\}.$$

Sean $f, g \in End^i(M)$, definimos $f \hat{+} g : M \to M$ dada por $(f \hat{+} g)(m) = f(m) \hat{+} g(m)$ para toda $m \in M$ y $f \circ g : M \to M$ como $f(g(m))$ para toda $m \in M$.
Es fácil mostrar que $(End^i(M), \hat{+}, \circ)$ es un anillo con uno. Al anillo $End^i(M)$ se le conoce como ***el anillo de endomorfismos izquierdos de M****.*

Definición 1.3.6. *Sea R un anillo. Un* ***ideal izquierdo*** *de R es un subconjunto no vacío $I \subseteq R$ que satisface:*

1. *$(I, +)$ es un subgrupo de $(R, +)$.*
2. *Para todo $r \in R$ y para todo $x \in I$ se tiene que $rx \in I$.*

Ejemplo 1.3.7. *Consideremos el anillo $\mathbb{Z}$ con la suma y el producto usuales y el conjunto $I = \{z \in \mathbb{Z} : z \text{ es par}\}$. Es rutinario ver que I es un ideal izquierdo de $\mathbb{Z}$.*

A continuación introduciremos el concepto de elemento idempotente de un anillo R, el cual usaremos en el Capítulo 2.

Definición 1.3.8. *Sea R un anillo. Un elemento $e \in R$ es un* ***idempotente*** *si $e^2 = e$.*

Ejemplos 1.3.9. *Consideremos un anillo R con uno. Entonces:*

1. *El anillo R tiene al menos dos idempotentes a saber 0 y 1.*
2. *Sea $e \in R$ un idempotente de R. Entonces $(1 - e)$ también es un idempotente de R. En efecto, $(1 - e)^2 = 1 - e - e + e^2 = 1 - e - e + e = 1 - e$.*

A continuación daremos la definición de homomorfismo de anillos, la cual usaremos en la siguiente sección.

Definición 1.3.10. *Sean A y B anillos. Un* ***homomorfismo de anillos*** *$f : A \to B$ es una función tal que:*

1. *$f(a + b) = f(a) + f(b)$ para cualesquiera $a, b \in A$.*
2. *$f(a \cdot b) = f(a) \cdot f(b)$ para cualesquiera $a, b \in A$.*

Por otro lado si, A y B son anillos con uno y $f : A \to B$ es un homomorfismo de anillos tal que $f(1_A) = 1_B$ entonces decimos f es un **homomorfismo de anillos con uno**.
Dado un anillo A y $a, b \in A$ algunas veces escribiremos ab en lugar de $a \cdot b$.

Ejemplo 1.3.11. *Sean A, B y C anillos y $f : A \to B$ y $g : B \to C$ homomorfismos de anillos. La composición de homomorfismos $g \circ f : A \to C$ también es un homomorfismo de anillos.*

Notemos que si $(A, +, \cdot)$ y $(B, +, \cdot)$ son anillos tenemos en particular que $(A, +)$ y $(B, +)$ son grupos abelianos. Por el inciso 1 de la Definición (1.3.10) se tiene que si $f : A \to B$ es un homomorfismo de anillos entonces f es en particular un homomorfismo de grupos. De donde por la Teoría de grupos, ver [6] o [2] se tiene el siguiente lema.

Lema 1.3.12. *Sean A y B anillos y $f : A \to B$ un homomorfismo de anillos. Entonces :*

1. $f(0_A) = 0_B$.

2. $f(-a) = -f(a)$, *para todo* $a \in A$.

$\square$

1.4. Módulos y submódulos.

En esta sección introduciremos el concepto de módulo y submódulo sobre un anillo R, ver [4]. A dicho anillo R lo supondremos siempre con uno. Así mismo daremos algunos ejemplos y veremos ciertos tipos de módulos con los cuales trabajaremos posteriormente.

Definición 1.4.1. *Sea R un anillo. Un par (M, λ) es un R-**módulo izquierdo**, si M es un grupo abeliano y λ es un homomorfismo de anillos con uno, de R al anillo de endomorfismos izquierdos de M. Esto es $\lambda : R \to End^i(M)$ satisface las siguientes propiedades.*
Para todo $a, b \in R$ y para toda $x, y \in M$ se cumple que:

1. $\lambda(a)(x + y) = \lambda(a)(x) + \lambda(a)(y)$, *ya que $\lambda(a)$ es un homomorfismo de grupos.*

2. $\lambda(a + b)(x) = \lambda(a)(x) + \lambda(b)(x)$, *ya que λ es un homomorfismo de anillos.*

3. $\lambda(ab)(x) = \lambda(a)(\lambda(b)(x))$, *ya que λ es un homomorfismo de anillos.*

4. $\lambda(1)(x) = x$, *ya que λ es un homomorfismo de anillos con uno.*

Por comodidad se omitirá λ y los paréntesis y solo escribiremos ax en lugar de $\lambda(a)(x)$.
Podemos pensar al homomorfismo de anillos con uno $\lambda : R \to End^i(M)$ como una operación de multiplicación por la izquierda por R. Es decir como una función

$$\cdot : R \times M \to M$$
$$(a, x) \mapsto ax.$$

Los R-módulos derechos se definen de manera análoga con la multiplicación por escalares por la derecha.
En ésta tesis trabajaremos únicamente con R-módulos izquierdos y cuando sea claro escribiremos que M es un R-módulo ó simplemente un módulo en lugar de escribir (M, λ).

Ejemplos 1.4.2. *Consideremos los siguientes ejemplos:*

1) Los grupos abelianos son exactamente los $\mathbb{Z}$-módulos.

2) Si R es un anillo, entonces los ideales izquierdos de R son los R-módulos izquierdos.

3) Sean K un campo y V un K-espacio vectorial. Se tiene que V es un K-módulo.

4) Sea M un grupo abeliano. El módulo cero es $\{0_M\}$ donde 0_M es el elemento neutro de M y las operaciones de suma y producto están dadas por:

- $0_M + 0_M = 0_M$.
- $r \cdot 0_M = 0_M$ *para toda* $r \in R$.

A continuación definiremos un submódulo de un módulo M. Este concepto será de gran utilidad ya que nos permitirá estudiar y caracterizar a los módulos.

Definición 1.4.3. *Sean (M, λ) un R-módulo y $N \subseteq M$ un subgrupo abeliano de M. Decimos que N es un R-**submódulo** de M si $\lambda : R \to End^i(N)$ es un homomorfismo de anillos con uno. Es decir, para cada $a \in R$ hay una función $\lambda(a) : N \to N$ tal que para todo $a, b \in R$ y para todo $x, y \in N$ se cumple que :*

1. $\lambda(a)(x + y) = \lambda(a)(x) + \lambda(a)(y)$.
2. $\lambda(a + b)(x) = \lambda(a)(x) + \lambda(b)(x)$.
3. $\lambda(ab)(x) = \lambda(a)(\lambda(b)(x))$.
4. $\lambda(1)(x) = x$.

Y lo denotaremos por $N \leq M$.

Nos referiremos a los R-submódulos izquierdos de M cómo submódulos de M cuando el anillo R sea claro.

Observación 1.4.4. *Es fácil ver que si N es un R-submódulo de M, entonces N es un R-módulo.*

Ejemplos 1.4.5.

1) *Sea V un K-espacio vectorial. Entonces los submódulos de V son los K-subespacios vectoriales de V.*

2) *Consideremos $\mathbb{R}^3$ como $\mathbb{R}$-módulo y sea*

$$U = \{(x, y, z) \in \mathbb{R}^3 : 2x - y + 5z = 0\}.$$

Entonces U es un submódulo de $\mathbb{R}^3$.

A continuación dado un subconjunto X de un módulo M, definiremos el submódulo de M generado por el conjunto X. Para esto necesitaremos el siguiente resultado.

Lema 1.4.6. *Sean M un R-módulo y $X \subseteq M$. Entonces la intersección de todos los R-submódulos de M que contienen a X es un R-submódulo de M.*

Demostración. Sean A un conjunto de índices y $\{S_{\alpha_i}\}_{\alpha_i \in A}$ la familia de R-submódulos de M que contienen a X. Dado que $M \in \{S_{\alpha_i}\}_{\alpha_i \in A}$ tenemos que $\{S_{\alpha_i}\}_{\alpha_i \in A} \neq \emptyset$.
De la teoría de grupos sabemos que la intersección de subgrupos de un grupo G es un subgrupo de G y como para cada $\alpha_i \in A$, S_{α_i} es un submódulo de M, en particular S_{α_i} es un subgrupo abeliano de M por lo que $\bigcap\limits_{\alpha_i \in A} S_{\alpha_i}$ es un subgrupo abeliano del grupo M.
Resta verificar que la función $\lambda : R \to End^i(\bigcap\limits_{\alpha_i \in A} S_{\alpha_i})$ es un homomorfismo de anillos. Consideremos $a, b \in R$ y $x, y \in \bigcap\limits_{\alpha_i \in A} S_{\alpha_i}$, como $x = s_i$ y $y = s'_i$ para toda α_i. Como S_{α_i} es un submódulo de M para cada α_i tenemos que:

1. $a(x + y) = a(s_i + s'_i) = as_i + as'_i = ax + ay$.
2. $(a + b)x = (a + b)s_i = as_i + bs_i = ax + bx$.
3. $(ab)x = (ab)s_i = a(bs_i) = a(bx)$.
4. $1x = 1s_i = s_i = x$.

Por lo tanto $\bigcap\limits_{\alpha_i \in A} S_{\alpha_i}$ es un submódulo de M. □

Es claro que la intersección de todos los submódulos de M que contienen al conjunto X también contiene al conjunto X. Esto motiva la siguiente definición.

Definición 1.4.7. *Sean M un R-módulo y $X \subseteq M$. Se tiene que la intersección de todos los submódulos de M que contienen a X se llama el* ***submódulo generado*** *por X y se denota por $\langle X \rangle$. También decimos que X es un* ***conjunto generador*** *de $\langle X \rangle$. Además, si X es finito decimos que X es un* ***conjunto generador finito****.*

Observación 1.4.8. *Sean M un R-módulo y $X \subseteq M$. Tenemos que $\langle X \rangle$ es el menor submódulo de M que contiene a X (con respecto a la relación contención.*

Ejemplo 1.4.9. *Consideremos el $\mathbb{R}$-módulo $\mathbb{R}^3$ y $X = \{(3, -2, 1)\} \subseteq \mathbb{R}^3$. Se puede ver que el $\mathbb{R}$-submódulo generado por X, es $\langle X \rangle = \{\lambda(3, -2, 1) : \lambda \in \mathbb{R}\}$.*

En general no es fácil encontrar el submódulo generado por un subconjunto X de un módulo M, ya que para ello es necesario encontrar todos los submódulos del módulo M que contienen a X.
Por ello daremos una caracterización de $\langle X \rangle$, para la cual requerimos la definición de combinación lineal y algunos resultados.

Definición 1.4.10. *Sean M un R-módulo, $\emptyset \neq X \subseteq M$ y $\emptyset \neq A \subseteq R$. Cualquier elemento de la forma $a_1x_1 + a_2x_2 + ... + a_nx_n$ con $x_1, x_2, ..., x_n \in X$ y $a_1, a_2, ..., a_n \in A$ es una* ***combinación lineal de*** *X con coeficientes en A. Denotaremos al conjunto de todas las combinaciones lineales de X con coeficientes en A por AX. Además si $X = \emptyset$ definimos $R\emptyset = \{0_M\}$.*

Ejemplo 1.4.11. *Consideremos $M = C^0(-\infty, +\infty)$ el $\mathbb{R}$-módulo formado por las funciones de variable real, continuas, definidas en el intervalo $(-\infty, +\infty)$, con las operaciones usuales de suma de funciones y multiplicación por escalares. Sean $X = \{cos(x), sen(x)\}$ y $A = \mathbb{Q} \subset \mathbb{R}$. Tenemos que*

$$AX = \{\lambda_1 cos(x) + \lambda_2 sen(x) : \lambda_1, \lambda_2 \in \mathbb{Q}\}.$$

El siguiente resultado afirma que el conjunto formado por todas las combinaciones lineales de X con coeficientes en R es un R-submódulo de M.

Proposición 1.4.12. *Sean M un R-módulo y X un subconjunto no vacío de M. Entonces el conjunto RX es un R-submódulo de M.*

Demostración. Sea $x \in X$, como $0_M = 0x \in RX$. Si $x, y \in RX$, entonces $x = r_1x_1 + r_2x_2 + ... + r_nx_n$ y $y = r'_1x_1 + r'_2x_2 + ... + r'_nx_n$ para algunos $r_i, r'_i \in R$ y $x_i \in X$ con $i = 1, ..., n$. Así $x - y = (r_1x_1 + r_2x_2 + ... + r_nx_n) - (r'_1x_1 + r'_2x_2 + ... + r'_nx_n) = (r_1 - r'_1)x_1 + (r_2 - r'_2)x_2 + ... + (r_n - r'_n)x_n \in RX$. Como $RX \subseteq M$ obtenemos que RX es un subgrupo de M.
Ahora sean $a, b \in R$, entonces:

1. $a(x + y) = a(r_1x_1 + r_2x_2 + ... + r_nx_n + r'_1x_1 + r'_2x_2 + ... + r'_nx_n) = (ar_1x_1 + ar_2x_2 + ... + ar_nx_n) + (ar'_1x_1 + ar'_2x_2 + ... + ar'_nx_n) = a(r_1x_1 + r_2x_2 + ... + r_nx_n) + a(r'_1x_1 + r'_2x_2 + ... + r'_nx_n) = ax + ay.$

2. $(a+b)x = (a+b)(r_1x_1+r_2x_2+...+r_nx_n) = (ar_1x_1+ar_2x_2+...+ar_nx_n)+(br_1+br_2x_2+...+br_nx_n) = a(r_1x_1+r_2x_2+...+r_nx_n)+b(r_1x_1+r_2x_2+...+r_nx_n) = ax+bx$.

3. $(ab)x = (ab)(r_1x_1+r_2x_2+...+r_nx_n) = (abr_1x_1+abr_2x_2+...+abr_nx_n) = a(br_1x_1+br_2x_2+...+br_nx_n) = a(bx)$.

4. $1(x) = 1(r_1x_1+r_2x_2+...+r_nx_n) = (1r_1x_1+1r_2x_2+...+1r_nx_n) = (r_1x_1+r_2x_2+...+r_nx_n) = x$

Ver la Definición (1.4.3). De lo anterior probamos que RX es un submódulo de M. □

Antes de poder dar la caracterización del submódulo generado por un conjunto X necesitamos el siguiente resultado, el cual nos proporciona una caracterización de un submódulo N de un módulo M.

Proposición 1.4.13. *Sean M un R-módulo izquierdo y N un subconjunto no vacío de M. Entonces los siguientes enunciados son equivalentes:*

(a) N es un submódulo de M.

(b) $RN = N$.

(c) Para cada $a, b \in R$ y cada $x, y \in N$ se tiene que $ax + by \in N$.

Demostración. Veamos que (a) implica (b). Supongamos que N es un submódulo de M. Claramente $N \subseteq RN$, entonces resta verificar que $RN \subseteq N$. Sea $x \in RN$, $x = r_1x_1 + r_2x_2 + ... + r_nx_n$ para algunos $r_i \in R$ y $x_i \in N$ donde cada $r_ix_i \in N$. Dado que N es un submódulo de M es cerrado bajo la suma, entonces $x = r_1x_1 + ... + r_nx_n \in N$. Lo que prueba que $RN \subseteq N$.
Veamos que (b) implica (a). Supongamos que $RN = N$, como $\emptyset \neq N \subseteq M$ por la Proposición 1.4.12 tenemos que $N = RN$ es un submódulo de M.
Veamos que(b) implica (c). Supongamos ahora que $RN = N$ y sean $a, b \in R$ y $x, y \in N$ entonces $ax + by \in RN = N$
Finalmente veamos que (c) implica (b). Supongamos que para cada $a, b \in R$ y cada $x, y \in N$ se tiene que $ax + by \in N$. Como $N \subseteq RN$ pues para cada $n \in N$ tenemos que $n = 1n \in RN$, resta verificar que $RN \subseteq N$. En efecto sea $x \in RN$, tenemos que $x = rn$ para algún $r \in R$ y $n \in N$, así $x = rn + 0 \in N$. Por tanto $RN \subseteq N$. Por lo tanto $RN = N$.

□

La siguiente proposición nos da una caracterización del submódulo generado por un conjunto X.

Proposición 1.4.14. *Sea M un R-módulo y X un subconjunto de M. Entonces el submódulo de M generado por X esto es $\langle X \rangle$ es precisamente el conjunto de todas las R-combinaciones lineales de X, esto es RX.*

Demostración. Podemos suponer que X es un conjunto distinto del vacío. Pues si $X = \emptyset$ tenemos que $\langle X \rangle = \{0_M\} = RX$.
Debido a la proposición 1.4.12 tenemos que RX es un submódulo de M. Por otro lado, tenemos que para todo $x \in M$, $1x = x$ por lo que $X \subseteq RX$.
Finalmente, por la proposición 1.4.13 inciso (b) tenemos que cada submódulo que contiene a X debe contener las R-combinaciones lineales de X. Por lo tanto RX está contenido en cada submódulo de M que contiene a X y como RX es uno de estos submódulos tenemos que el submódulo generado por X es RX. $\square$

Definición 1.4.15. *Decimos que un módulo M es finitamente generado si existe un subconjunto finito X de M tal que $M = \langle X \rangle$.*

En particular, si M es un R-módulo y $X = \{m\}$ para algún $m \in M$ tenemos la siguiente definición.

Definición 1.4.16. *Sea M un R-módulo y $m \in M$.*

1. *El submódulo de M generado por el conjunto $\{m\}$ es*

$$\langle \{m\} \rangle := \{rm : r \in R\},$$

   llamado el ***submódulo cíclico generado por*** *$\{m\}$ y se denota por Rm.*

2. *Decimos que M es un* ***módulo cíclico*** *si $M = \langle \{m\} \rangle$.*

Por comodidad para $m \in M$ escribiremos $\langle m \rangle$ en lugar de $\langle \{m\} \rangle$.

Ejemplo 1.4.17. *Consideremos el $\mathbb{Z}$-módulo $\mathbb{Z}$ y $m \in \mathbb{Z}$ con $m > 1$. Tenemos que el $\mathbb{Z}$-módulo cíclico generado por m es $\mathbb{Z}m = \{km : k \in \mathbb{Z}\}$.*

Definición 1.4.18. *Dado un R-módulo M y $\emptyset \neq X \subseteq M$, definimos*

$$\sum_{x \in X} Rx := \{ \sum_{finitas} r_i x_i : \ r_i \in R \text{ y } x_i \in X\}.$$

Observación 1.4.19. *Dado un R-módulo M y X un conjunto generador de M tenemos que $M = \sum_{x \in X} Rx = RX$.*

A continuación dados los módulos $M_1, M_2, ..., M_n$ definiremos la suma de ellos.

Definición 1.4.20. *Si $M_1, M_2, ..., M_n$ son submódulos de M. Definimos la suma de $M_1, M_2, ..., M_n$ como el conjunto*

$$\{m_1 + m_2 + ... + m_n : \ m_i \in M_i \ (i = 1, ..., n)\}$$

y la denotamos por $M_1 + M_2 + ... + M_n$.

Ejemplo 1.4.21. *Consideremos al $\mathbb{R}$-módulo $\mathbb{R}^3$ y a sus submódulos: $M_1 = \{(x, y, 0) : \ x, y \in \mathbb{R}\}$, $M_2 = \{(0, y', 0) : \ y' \in \mathbb{R}\}$, $M_3 = \{(0, 0, z) : \ z \in \mathbb{R}\}$ y $M_4 = \{(0, y'', z') : \ y'', z' \in \mathbb{R}\}$. Entonces*

$$M_1 + M_2 + M_3 + M_4 = \{(x, y, 0) + (0, y', 0) + (0, 0, z) + (0, y'', z')\}.$$

Lema 1.4.22. *Sea M un R-módulo izquierdo. Si $M_1, M_2, ..., M_n$ son submódulos de M, entonces $M_1 + M_2 + ... + M_n$ es un submódulo de M. De hecho $M_1 + M_2 + ... + M_n$ es el conjunto de todas las combinaciones lineales de $M_1 \cup M_2 \cup ... \cup M_n$.*

Demostración. Sean $x = m_1 + m_2 + ... + m_n, y = m_1' + m_2' + ... + m_n' \in M_1 + M_2 + ... + M_n$ y sean $r_1, r_2 \in R$. Se tiene que $r_1x + r_2y = r_1(m_1 + m_2 + ... + m_n) + r_2(m_1' + m_2' + ... + m_n') = r_1m_1 + r_1m_2 + ... + r_1m_n + r_2m_1' + r_2m_2' ... + r_2m_n' = r_1m_1 + r_2m_1' + r_1m_2 + r_2m_2' ... + r_1m_n + r_2m_n'$. Como cada M_i es submódulo de M para cada $i = 1, ..., n$ se tiene que $r_1m_i + r_2m_i' \in M_i$ Por tanto $r_1x + r_2y = r_1m_1 + r_2m_1' + r_1m_2 + r_2m_2' + ... + r_1m_n + r_2m_n' \in M_1 + M_2 + ... + M_n$. Por la proposición (1.4.13) inciso (c) concluimos que $M_1 + M_2 + ... + M_n$ es un submódulo de M.

□

Hasta ahora hemos estudiado la intersección y la suma de módulos. A continuación veremos como se relacionan estas dos operaciones.
En general, para un R-módulo M y cualesquiera H,K,L, submódulos de M se verifica que $H \cap (K + L) \geq (H \cap K) + (H \cap L)$. En particular, cuando $K \leq H$ tenemos la siguiente proposición llamada ley modular.

Proposición 1.4.23. ***(Ley modular).*** *Sean H,K y L submódulos de M. Entonces, si $K \leq H$ se tiene que $H \cap (K + L) = K + (H \cap L)$.*

Demostración. Sea $x \in H \cap (K + L)$ entonces $x \in H$ y $x \in (K + L)$ así $x = h = k + l$ para algunas $h \in H$, $k \in K$ y $l \in L$. Se tiene que $l = h - k$ y como $K \subseteq H$. De donde $l \in H$ esto implica que $l \in L \cap H$. Por tanto $x = k + l \in K + (H \cap L)$. □

Si N es un submódulo de un R-módulo M tenemos que N es un subgrupo del grupo abeliano M y por tanto podemos considerar el grupo cociente
$M/N := \{x + N : x \in M\}$. A este grupo cociente le podemos dar una estructura de R-módulo como sigue:
Para $x + N \in M/N$ y $a \in R$ definimos $a(x + N) := ax + N$. Veamos que está bien definida. Es decir si $x + N = y + N$ entonces $ax + N = ay + N$. Como $x + N = y + N$ tenemos que $x - y \in N$ de donde $a(x - y) \in N$ y por tanto $ax + N = ay + N$. Es decir, la operación multiplicación por escalares está bien definida. De lo anterior podemos dar la siguiente definición.

Definición 1.4.24. *Sea N un submódulo de un R-módulo M, al grupo cociente M/N le damos una estructura de R-módulo como sigue:*
Para $(x + N) \in M/N$ y $a \in R$ definimos $a(x + N) := ax + N$. Al módulo resultante M/N lo llamaremos ***módulo cociente****.*

Ejemplo 1.4.25. *Consideremos al $\mathbb{Z}$-módulo $\mathbb{Z}$. Entonces $\mathbb{Z}_m = \mathbb{Z}/\mathbb{Z}m$ es el módulo cociente del módulo $\mathbb{Z}$ con el submódulo $\mathbb{Z}m$.*

1.5. Homomorfismos de módulos.

En esta sección estudiaremos el concepto de homomorfismo de módulos. En particular enunciaremos el Teorema del factor y como corolario de este enunciaremos los Teoremas de isomorfismo.

Definición 1.5.1. *Sean M y N R-módulos. La función $f : M \to N$ es un **R-homomorfismo** si para toda $a, b \in R$ y para toda $x, y \in M$ se cumple que $f(ax + by) = af(x) + bf(y)$; es decir si f es R-lineal.*

Por comodidad a los R-homomorfismos de módulos les llamaremos simplemente homomorfismos cuando el anillo R sea claro.

Observación 1.5.2. *La aritmética de los homomorfismos de módulos es análoga a la de los homomorfismos de grupos y transformaciones lineales de espacios vectoriales. En particular la composición de dos R-homomorfismos es también un R-homomorfismo.*

Ejemplos 1.5.3.

1. *Consideremos un módulo M y $N \leq M$. La función $i_N : N \to M$ dada por $i(n) = n$ para toda $n \in N$ es un homomorfismo de módulos llamado **inclusión canónica de N en M**.*

2. *Consideremos a un módulo M. La función $1_M : M \to M$ dada por $1_M(m) = m$ para toda $m \in M$ es un homomorfismo de módulos llamado **homomorfismo identidad**.*

3. *Consideremos dos módulos M y N. El homomorfismo $\hat{0} : M \to N$ dado por $\hat{0}(m) = 0$ para toda $m \in M$ es llamado **homomorfismo cero**.*

Los siguientes conceptos nos serán de gran utilidad para el estudio de los homomorfismos de módulos.

Definición 1.5.4. *Sean M y N módulos y $f : M \to N$ un homomorfismo.*

1. *La **Imagen** de f se define por $Imf := \{f(x) \in N : x \in M\}$.*

2. *El **Kernel** de f se define por $Kerf := \{x \in M : f(x) = 0\}$.*

3. *La **Coimagen** de f se define por $Coimf = M/Kerf$.*

4. *El **Cokernel** de f de define por $Cokerf = N/Imf$.*

5. *Sea $L \subseteq N$, la **Imagen inversa** de L se define por $f^{-1}(L) = \{x \in M : \ f(x) \in L\}$.*

Observación 1.5.5. *Notemos que la Imagen de f y el Kernel de f son submódulos de N y M respectivamente.*

Ejemplo 1.5.6. *Sean M un módulo y N submódulo de M. Consideremos el homomorfismo inclusión $i_N : N \to M$ de N en M. Entonces $Imi_N = N$ y $Keri_N = 0$.*

La siguiente proposición nos será de gran ayuda para saber cuando dos homomorfismos son iguales.

Proposición 1.5.7. *Sean M y N R-módulos, y X un conjunto generador de M. Si $f : M \to N$ es un R-homomorfismo, entonces Imf es generada por $f(X) := \{f(x) : \ x \in X\}$. Más aún si $g : M \to N$ es un R-homomorfismo, entonces $f = g$ si y sólo si $f(x) = g(x)$ para cada $x \in X$.*

Demostración. Debido a la Observación (1.4.19) tenemos que $M = RX$ por lo que $Imf = f(M) = f(RX) = Rf(X)$. Si $f = g$ se tiene que $f(m) = g(m)$ para cada $m \in M$ en particular se cumple para cada $x \in X$.
Ahora supongamos que $f(x) = g(x)$ para cada $x \in X$. Afirmamos que $K = \{y \in M : \ f(y) = g(y)\}$ es un submódulo de M. En efecto sean $a, b \in R$ y $x, y \in K$, entonces $ax+by \in M$ y $f(ax+by) = f(ax)+f(ay) = af(x)+bf(y) = ag(x) + bg(y) = g(ax) + g(by) = g(ax + by)$ de donde $ax + by \in K$ y por la Proposición (1.4.13) tenemos que K es un submódulo de M. Y como $X \subseteq K$ nuevamente por la Proposición (1.4.13) $M = RX \subseteq K$. Así $f(y) = g(y)$ para toda $y \in M$. □

Definición 1.5.8. *Sean M, N y L módulos y $f : M \to N$ un homomorfismo. Entonces:*

1. *Si $g, h : N \to L$ son homomorfismos, f es un **epimorfismo** si siempre que $gf = hf$, se tiene $g = h$.*

2. *Si $g, h : L \to M$ son homomorfismos, f es un **monomorfismo** si siempre que $fg = fh$ se tiene que $g = h$.*

3. *El homomorfismo f es un **isomorfismo** si es epimorfismo y monomorfismo.*

Ejemplos 1.5.9.

1. *Para cada submódulo K de M el homomorfismo $\eta_K : M \to M/K$ de M sobre M/K, definida por $\eta_K(x) = x + K$ para cada $x \in M$, es un epimorfismo de módulos llamado **epimorfismo canónico** con $Ker\eta_K = K$.*

2. *Sean M un módulo y N un submódulo de M, la inclusión canónica de N en M es un monomorfismo de módulos.*

3. *La composición de epimorfismos (monomorfismos) es un epimorfismo (monomorfismo).*

4. *Consideremos a los $\mathbb{R}$-módulos*

$$P^3(t) := \{a_0 + a_1t + a_2t^2 + a_3t^3 : \ a_0, a_1, a_2, a_3 \in \mathbb{R}\}$$

   y $\mathbb{R}^4$. El homomorfismo $T : P^3(t) \to \mathbb{R}^4$ dado por

$$T(a_0 + a_1t + a_2t^2 + a_3t^3) = (a_0, a_1, a_2, a_3)$$

es un isomorfismo de $\mathbb{R}$-módulos.

Las siguientes proposiciones caracterizan a los epimorfismos de módulos y a los monomorfismos de módulos.

Proposición 1.5.10. *Sean M y N dos módulos y sea $f : M \to N$ un homomorfismo. Entonces los siguientes enunciados son equivalentes:*

(a) f *es un epimorfismo.*

(b) f *es suprayectivo.*

(c) $CoKerf = 0$.

(d) Para cada módulo K y cada homomorfismo $g : N \to K$, $gf = \hat{0}$ implica que $g = \hat{0}$.

Demostración. Veamos que (a) implica (b). Si f no es suprayectivo, entonces Imf es un submódulo propio de N y $0 \neq N/Imf$. Consideremos los homomorfismos $\alpha : N \to N/Imf$ dado por $\alpha(n) = n + Imf$ y $\beta : N \to N/Imf$ dado por $\beta(n) = 0 + Imf$ y notemos que como $N/Imf \neq 0$, entonces $\alpha \neq \beta$. Por otro lado para cada $x \in M$ se tienen que $\alpha f(x) = \alpha(f(x)) = f(x) + Imf = 0 + Imf$ y también $\beta f(x) = \beta(f(x)) = 0 + Imf$, de donde $\alpha f = \beta f$. Y como f es epimorfismo $\alpha = \beta$ lo cuál es una contradicción pues $\alpha \neq \beta$. Por tanto f es suprayectivo.
Veamos que (b) implica (a). Supongamos que f es suprayectivo y sean L un módulo y $\alpha, \beta : N \to L$ homomorfismos tales que $\alpha f = \beta f$. Ahora si $x \in N$, entonces existe $y \in M$ tal que $x = f(y)$ por lo que $\alpha(x) = \alpha f(y) = \beta(f(y)) = \beta(x)$. Así $\alpha = \beta$ y por lo tanto f es epimorfismo.
Veamos que (b) implica (c). Es clara dado que f es suprayectivo, es decir $Imf = N$ así. $N/Imf = N/N = 0$.
Veamos que (c) implica (b). Supongamos que $N/Imf = 0$ esto implica que para cada $n \in N$ se tiene que $n + Imf = 0 + Imf$ es decir $n \in Imf$ por lo tanto $N = Imf$.
Veamos que (c) implica (d). Supongamos que $Cokerf = 0$ y sean K un R-módulo y $g : N \to K$ un homomorfismo tal que $gf = \hat{0}$. Consideremos al homomorfismo cero, entonces $\hat{0} = \hat{0}f$, de donde $gf = \hat{0}f$. Por (a) concluimos que $g = \hat{0}$.
Finalmente veamos que (d) implica (b). Supongamos que para cada módulo K y cada homomorfismo $g : N \to K$, $gf = \hat{0}$ implica que $g = \hat{0}$. Consideramos el homomorfismo $\rho : N \to N/Imf$ dado por $\rho(n) = n + Imf$. Ahora consideremos la composición ρf entonces $\rho(f(m)) = f(m) + Imf = 0 + Imf$ es decir $\rho f = 0$ así $g = \hat{0}$. Por lo tanto $N = Imf$.

□

Proposición 1.5.11. *Sean M y N dos R-módulos izquierdos y $f : M \to N$ un homomorfismo. Entonces los siguientes enunciados son equivalentes:*

(a) f *es inyectivo.*

(b) f *es monomorfismo.*

(c) $Kerf = 0$.

(d) *Para cada R-módulo izquierdo K y cada R-homomorfismo $g : K \to M$, $fg = \hat{0}$ implica que $g = \hat{0}$.*

Demostración. Veamos que (a) implica (b). Supongamos que f es inyectiva y sean $g, h : M \to N$ dos homomorfismos tales que $fg = fh$. Si $x \in M$, entonces $f(g(x)) = fg(x) = fh(x) = f(h(x))$ y como f es inyectiva se tiene que $g(x) = h(x)$ para cada $x \in M$. Por lo tanto $g = h$.
Veamos que no (a) implica no (b). Supongamos que f no es inyectiva, entonces existen $x, y \in M$ con $x \neq y$ tales que $f(x) = f(y)$, así $f(x-y) = 0$ pero $x-y \neq 0$. Ahora sea $K = R(x-y) \neq \{\hat{0}\} \leq M$. Para cada $r \in R$ definimos $g : K \to M$ como $g(r(x-y)) = 0$ y $h : K \to M$ como $h(r(x-y)) = r(x-y)$, entonces g es el homomorfismo cero y h es la inclusión de K en M por lo que $g \neq h$. Pero para cada $r \in R$ $fg(r(x-y)) = f(0) = 0$ y $fh(r(x-y)) = f(r(x-y)) = rf(x-y) = r0 = 0$. Es decir $fg = fh$. Por lo tanto f no es monomorfismo.
Veamos que (a) implica (c). Supongamos que f es inyectiva y $Kerf \neq 0$, entonces existe $0 \neq x \in Kerf$. De donde $f(x) = 0 = f(0)$ lo que es una contradicción el hecho de que f es inyectiva. Por lo tanto $Kerf = 0$.
Ahora veamos que (c) implica (a). Supongamos que $Kerf = 0$ y sean $x, y \in M$ tales que $f(x) = f(y)$. Entonces $f(x) - f(y) = 0$ por lo que $f(x-y) = 0$. Es decir $x - y \in Kerf = 0$, entonces $x - y = 0$ de donde $x = y$. Por lo tanto f es inyectiva.
Veamos que (a) implica (d). Supongamos que f es inyectiva. Sea K un R-módulo y $g : K \to M$ un homomorfismo tal que $fg = \hat{0}$. Consideremos al homomorfismo cero $\hat{0} : K \to M$, como $\hat{0} = f\hat{0}$ entonces $fg = f\hat{0}$ por lo tanto $g = \hat{0}$.
Finalmente veamos que (d) implica (c). Sea $K = Kerf \leq M$, consideremos al homomorfismo inclusión $i : K \to M$. Entonces $\hat{0} = fi : K \to N$ dado por $fi(k) = f(k) = 0$. Entonces $i = \hat{0}$ por lo tanto $K = Kerf = 0$. $\square$

Proposición 1.5.12. *Sean M y N R-módulos y $f : M \to N$ un homomorfismo. Entonces f es un isomorfismo si y sólo si existen funciones $g, h : N \to M$ tales que $fg = 1_N$ y $hf = 1_M$. Más aún, cuando estás últimas condiciones se satisfacen, $g = h$ es un isomorfismo.*

Demostración. Supongamos que el homomorfismo f es un isomorfismo, entonces f es una biyección por lo que existe una función $g : N \to M$ tal que $fg = 1_N$ y $gf = 1_M$.
Resta verificar que la función g es un homomorfismo. Sean $x, y \in N$ y $a, b \in R$. Entonces $f(g(ax + by)) = ax + by = af(g(x)) + bf(g(y)) = f(ag(x) + bg(y))$. Como f es isomorfismo, en particular monomorfismo y por la Proposición (1.5.11) es inyectivo, de donde $g(ax + by) = ag(x) + bg(y)$.
Ahora supongamos que existen funciones $g, h : N \to M$ tales que $fg = 1_N$ y $hf = 1_M$, entonces f es biyectiva por lo tanto es inyectiva y suprayectiva. De las Proposiciones (1.5.11) y (1.5.10) tenemos que f es monomorfismo y epimorfismo. Por lo tanto f es un isomorfismo. $\square$

Observación 1.5.13. *Cuando $f : M \to N$ es un isomorfismo, entonces el único homomorfismo $g : N \to M$ que satisface las condiciones del Teorema anterior se le llama el* ***inverso*** *de f y lo denotamos por f^{-1}.*

A continuación enunciaremos y demostraremos el Teorema del factor, el cual nos será útil para demostrar los Teoremas de isomorfismo.

Teorema 1.5.14. ***(Teorema del factor.)****Sean M, M',N y N' módulos izquierdos y $f : M \to N$ un homomorfismo.*

1. *Si $g : M \to M'$ es un epimorfismo con $Kerg \subseteq Kerf$. Entonces existe un único homomorfismo $h : M' \to N$ tal que $f = hg$.*
   Además, $Kerh = g(Kerf)$ y $Imh = Imf$, de donde h es monomorfismo si y sólo si $Kerg = Kerf$ y h es epimorfismo si y sólo si f es epimorfismo.
2. *Si $g : N' \to N$ es un monomorfismo con $Imf \subseteq Img$. Entonces existe un único homomorfismo $h : M \to N'$ tal que $f = gh$. Además,*
   $Kerh = Kerf$ y $Imh = g^{-1}(Imf)$, entonces h es monomorfismo si y sólo si f es monomorfismo, y h es epimorfismo si y sólo si $Img = Imf$.

Demostración.

1. Debido a la Proposición (1.5.10) tenemos que el homomorfismo g es suprayectivo. Es decir para cada $m' \in M'$ hay al menos un $m \in M$ tal que $g(m) = m'$, además si hay un $l \in M$ con $g(l) = m'$, se tiene que $(m - l) \in Kerg$. Como $Kerg \subseteq Kerf$, tenemos que $f(m) = f(l)$, por lo que hay una función bien definida $h : M' \to N$ dada por $h(m') = f(m)$. Es claro que $f = hg$.
   Veamos que la función h es homomorfismo. Sean $x', y' \in M'$ y $x, y \in M$ con $g(x) = x'$ y $g(y) = y'$. Entonces $g(ax + by) = ax' + by'$ para cada $a, b \in R$ así que $h(ax' + by') = f(ax + by) = af(x) + bf(y) = ah(x') + bh(y')$, por lo tanto h es homomorfismo.
   Supongamos que existe un homomorfismo $h' : M' \to N$ tal que $f = h'g$ entonces $hg = h'g$ y como g es epimorfismo tenemos que $h = h'$ por lo tanto el homomorfismo h es único.
   Veamos ahora que $Kerh = g(Kerf)$ y $Imh = Imf$. Sea $m' \in M'$ tal que $h(m') = f(m) = 0$ con $m \in M$. Entonces $m \in Kerf$. Como $g(m) = m'$ tenemos que $m' \in g(Kerf)$. Por tanto $Kerh \subseteq g(Kerf)$. La otra contención es análoga. Es claro por la definición de $h : M' \to N$ que $Imh = Imf$.
   Veamos que h es monomorfismo si y sólo si $Kerg = Kerf$ y h es epimorfismo si y sólo si f es epimorfismo.
   Supongamos que h es monomorfismo, debido la Proposición (1.5.11) tenemos que $Kerh = 0$, así $Kerh = 0 = g(Kerf)$ por lo que $Kerf \subseteq Kerg$ y por hipótesis $Kerg \subseteq Kerf$. Por lo tanto $Kerg = Kerf$.
   Si $Kerg = Kerf$, entonces como $Kerh = g(Kerf) = g(Kerg) = 0$ tenemos que $Kerh = 0$ y debido a la Proposición (1.5.11) h es monomorfismo.
   Ahora supongamos que h es epimorfismo y veamos que f es epimorfismo. Como el homomorfismo $f = hg$ y tanto h como g son epimorfismos tenemos que f es epimorfismo pues la composición de epimorfismos es también

un epimorfismo.
Finalmente supongamos que f es epimorfismo, entonces $Imf = N$. Y por hipótesis $Imh = Imf = N$, entonces el homomorfismo h es suprayectivo y por la Proposición (1.5.10) tenemos que h es epimorfismo.

2. Como para cada $m \in M$, $f(m) \in Imf \subseteq Img$ y $g : N' \to N$ es monomorfismo, entonces hay un único $n' \in N'$ tal que $g(n') = f(m)$. Por lo que hay una función bien definida $h : M \to N'$, dada por $h(m) = n'$ tal que $f = gh$.
   Claramente la función h es un homomorfismo, veamos que es único. Sea $h' : M \to N'$ un homomorfismo tal que $f = gh$. Entonces $gh = gh'$ y como g es monomorfismo se tiene que $h = h'$.
   Afirmamos que $Kerh = Kerf$ y $Imh = g^{-1}(Imf)$. En efecto, si $m \in Kerh$, entonces $0 = h(m)$ y como $f = gh$ tenemos que $0 = g(0) = g(h(m)) = f(m)$ por lo que $m \in Kerf$. La otra contención es análoga.
   Es claro por la definición de $h : M \to N'$que $Imh = g^{-1}(Imf)$.
   Veamos ahora que h es monomorfismo si y sólo si f es monomorfismo y h es epimorfismo si y sólo si $Img = Imf$.
   Primero supongamos que h es monomorfismo, como $f = gh$ y la composición de monomorfismos es un monomorfismo, tenemos que f es un monomorfismo.
   Supongamos que f es un monomorfismo, entonces por la Proposición (1.5.11) $Kerf = 0$ y como $0 = Kerf = Kerh$ nuevamente por la Proposición (1.5.11) tenemos que h es un monomorfismo.
   Ahora supongamos que h es epimorfismo, queremos ver que $Img = Imf$. Por hipótesis tenemos que $Imf \subseteq Img$, resta verificar que $Img \subseteq Imf$. Sea $x \in Img$, entonces $x = g(n')$ para algún $n' \in N'$, y como h es epimorfismo, por la Proposición (1.5.10) tenemos que h es suprayectivo, entonces $n' = h(m)$ para algún $m \in M$, así $x = g(n') = g(h(m)) = f(m)$ por lo que $x = f(m)$, es decir $x \in Imf$. Por lo tanto $Img \subseteq Imf$.

   Finalmente supongamos que $Img = Imf$, como el homomorfismo $f = gh$ entonces $Img = Imf = Imgh$. Y notemos que $Imh = g^{-1}Imf$, así $N' = g^{-1}(Img) = g^{-1}(Imf) = g^{-1}(Imgh) = g^{-1}(g(Imh)) = Imh$ por lo que el homomorfismo h es suprayectivo y por la Proposición (1.5.10) h es epimorfismo.

□

A consecuencia del primer inciso del Teorema del factor tenemos un importante corolario llamado "Los Teoremas de isomorfismo", el cuál presentaremos a continuación.

Corolario 1.5.15. ***(Teoremas de isomorfismo)***. *Sean M y N módulos.*

1. *Si $f : M \to N$ es un epimorfismo con $Kerf = K$. Entonces existe un único isomorfismo $h : M/K \to N$ tal que $h(m + K) = f(m)$ para toda $m \in M$.*

2. Si $K \leq L \leq M$. Entonces $M/L \cong (M/K)/(L/K)$.

3. Si $H \leq M$ y $K \leq M$. Entonces $(H+K)/K \cong H/(H \cap K)$.

Demostración.

1. Sea $M' = M/K$ y g el epimorfismo canónico (Ver Ejemplo 1.5.9) $g = \eta_k : M \to M/K$. Como $Kerf = K = Kerg$, por (1.5.14) inciso 1 tenemos que existe un único homomorfismo $h : M' \to N$ tal que $f = hg$ de donde $h(m+K) = f(m)$. Además como $Kerh = g(Kerf) = g(K) = 0$. Tenemos que h es monomorfismo. Como por hipótesis f es epimorfismo tenemos que h también es epimorfismo. Por lo tanto h es isomorfismo.

2. Definamos la función $f' : M/K \to M/L$, vía $f'(m+K) = m+L$.
   Veamos que f' está bien definida. En efecto, sean $m_1+K, m_2+K \in M/K$. Si $m_1+K = m_2+K$, entonces $m_1 - m_2 \in K \subseteq L$, por lo que $m_1 - m_2 \in L$ de donde $m_1 + L = m_2 + L$.

   Ahora veamos que f' es homomorfismo. Sean $m_1, m_2 \in M$ y $r_1, r_2 \in R$, entonces: $f'((r_1m_1 + r_2m_2) + K) = (r_1m_1 + r_2m_2) + L = r_1(m_1 + L) + r_2(m_2 + L) = r_1f'(m_1 + K) + r_2f'(m_2 + K)$. Por lo tanto f' es homomorfismo.
   Por otro lado notemos que

   $$Kerf' = \{m+K \in M/K : m+L = 0+L\} = \{m+K \in M/K : m \in L\} = L/K.$$

   Afirmamos que f' es epimorfismo. En efecto, sea $m + L \in M/L$, entonces $m + K \in M/K$ y $f'(m+K) = m+L$, de donde f' es suprayectivo. Y por la Proposición (1.5.10) f' es epimorfismo.

   Debido al inciso anterior tenemos que, existe un único isomorfismo $h : (M/K)/(L/K) \to M/L$. Por lo tanto $(M/K)/(M/L) \cong M/L$.

3. Definamos la función $f'' : H \to (H+K)/K$, vía $f''(h) = h+K$.
   Claramente f'' está bien definida. Veamos que f'' es homomorfismo.
   Sean $h_1, h_2 \in H$ y $r \in R$, entonces:

   $$f''(h_1 + h_2) = (h_1 + h_2) + K = (h_1 + K) + (h_2 + K) = f''(h_1) + f''(h_2)$$

   y $f''(rh_1) = (rh_1) + K = r(h_1 + K)$. Por lo tanto f'' es homomorfismo.
   Por otro lado notemos que,

   $$Kerf'' = \{h \in H : h + K = 0 + K\} = \{h \in H : h \in K\} = H \cap K.$$

   Veamos ahora que f'' es epimorfismo. En efecto, sea $h+K \in (H+K)/K$. Entonces $h \in H$ y $f''(h) = h + K$ por lo que f'' es suprayectivo. Y por la Proposición (1.5.10) f'' es epimorfismo. Por (1.5.15) inciso 1, existe un único isomorfismo

$$h : H/(H \cap K) \to (H + K)/K.$$

Por lo tanto $(H + K)/K \cong H/(H \cap K)$.

□

A continuación daremos la definición de sucesión exacta la cuál usaremos más adelante.

Definición 1.5.16. *Se dice que una sucesión de homomorfismos (finita o infinita) de R-módulos* $\dots \xrightarrow{f_{n-1}} M_{n-1} \xrightarrow{f_n} M_n \xrightarrow{f_{n+1}} M_{n+1} \longrightarrow \dots$ *es* ***exacta*** *si para cada par sucesivo de homomorfismos* f_n, f_{n+1} *se tiene que* $Imf_n = Kerf_{n+1}$.

Ejemplo 1.5.17. *Consideremos dos módulos* M *y* N *y* $f : M \to N$ *un homomorfismo, entonces* $0 \longrightarrow Kerf \xrightarrow{i} M \xrightarrow{f} N \xrightarrow{\eta} Cokerf \longrightarrow 0$ *es una sucesión exacta, donde* i *es la inclusión de* $Kerf$ *en* M *y* η *es el epimorfismo canónico de* N *en* $Cokerf = N/Imf$.
En efecto, sabemos que el homomorfismo inclusión es un monomorfismo con $i(Kerf) = Im(i) = Kerf$ *y por otro lado el homomorfismo* η *es un epimorfismo con* $Ker\eta = Imf$.

Ahora introduciremos el concepto de diagrama conmutativo y enunciaremos el Lema del quinto, el cual relaciona las sucesiones exactas y los diagramas conmutativos, y lo usaremos en el siguiente capitulo.

Definición 1.5.18. *Sean* A*,* B*,* C*, y* D *módulos y* $f : A \to B$*,* $g : C \to D$*,* $\alpha : A \to C$ *y* $\beta : B \to D$*, homomorfismos de módulos. Decimos que un diagrama de módulos y homomorfismos de la forma*

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

conmuta *si* $\beta f = g\alpha$.

Lema 1.5.19. ***(Lema del quinto.)*** *Supongamos que el siguiente diagrama de módulos y homomorfismos*

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

conmuta y tiene renglones exactos. Entonces:

(a) Si α es epimorfismo y β y δ son monomorfismos, entonces γ es monomorfismo.

(b) Si ϵ es monomorfismo y β y δ son epimorfismos,entonces γ es epimorfismo.

(c) Si α, β, δ y ϵ son isomorfismos, entonces γ es un isomorfismo.

Demostración. Supongamos que α es epimorfismo y β y δ monomorfismos. Sea $c \in Ker\gamma$, entonces $\gamma(c) = 0$ y como el diagrama es conmutativo $\delta(f_3(c)) = g_3(\gamma(c)) = 0$. De donde $f_3(c) = 0$ pues δ es monomorfismo y por la Proposición (1.5.11) $Ker\delta = 0$.
Como $Imf_2 = Kerf_3$ existe $b \in B$ con $f_2(b) = c$ y por la conmutatividad del diagrama $g_2(\beta(b)) = \gamma(f_2(b)) = \gamma(c) = 0$. Por lo que existe $a' \in A'$ tal que $g_1(a') = \beta(b)$, y como α es epimorfismo por la Proposición (1.5.10) se tiene que es suprayectivo, entonces existe $a \in A$ tal que $\alpha(a) = a'$.
Así $g_1(\alpha(a)) = g_1(a') = \beta(f_1(a)) = \beta(b)$, esto implica que $f_1(a) = b$ pues β es monomorfismo y por la Proposición (1.5.11) es inyectivo, entonces $f_2(b) = f_2(f_1(a)) = 0 = c$. Por lo tanto $Ker\gamma = 0$ y por la Proposición (1.5.11) concluimos que γ es monomorfismo.
Ahora supongamos que ϵ es monomorfismo y β y δ epimorfismos. Sea $c' \in C'$, como δ es epimorfismo por la Proposición (1.5.10) es suprayectivo, entonces existe $d \in D$ tal que $\delta(d) = g_3(c')$. Y como el diagrama tiene renglones exactos la $Img_3 = Kerg_4$ por lo que $g_4(g_3(c')) = 0 = \epsilon(f_4(d))$. Además ϵ es monomorfismo y por la Proposición (1.5.11) es inyectivo, entonces $f_4(d) = 0$.
Entonces existe $c \in C$ con $f_3(c) = d$ por lo que $g_3(c'-\gamma(c)) = g_3(c')-g_3(\gamma(c)) = \delta(d) - \delta(f_3(c)) = \delta(d) - \delta(d) = 0$. Así existe $b' \in B$ con $g_2(b') = c' - \gamma(c)$, y como β es epimorfismo por la Proposición (1.5.10) es suprayectivo por lo que existe $b \in B$ tal que $\beta(b) = b'$.
Entonces $\gamma(f_2(b) + c) = \gamma(f_2(b)) + \gamma(c) = g_2(\beta(b)) + \gamma(c) = g_2(b') + \gamma(c) = c' - \gamma(c) + \gamma(c) = c'$. Por lo tanto γ es suprayectivo y debido a la Proposición (1.5.10) concluimos que γ es suprayectivo.
Finalmente supongamos que α, β, δ y ϵ son isomorfismos, es decir son monomorfismos y epimorfismos. De los incisos (a) y (b) se sigue que γ es un isomorfismo.
$\square$

Capítulo 2

Sumandos directos.

2.1. Homomorfismos que se escinden.

En esta sección introduciremos los conceptos de sumando directo y complemento directo de un módulo M. Daremos la definición de epimorfismo y monomorfismo que se escinden, retomaremos las sucesiones exactas, veremos cuando una sucesión exacta corta se escinde y finalmente daremos algunas caracterizaciones de ellas.

Definición 2.1.1. *Sean M_1 y M_2 submódulos de un módulo M.*

1. *Decimos que M es **generado** por M_1 y M_2 si $M_1 + M_2 = M$.*
2. *Decimos que M_1 y M_2 son **independientes** si $M_1 \cap M_2 = 0$.*

Ejemplos 2.1.2.

1. *Consideremos al $\mathbb{R}$-módulo $M = \mathbb{R}^3$ y a sus submódulos $M_1 = \{(x, y, 0) : \ x, y \in \mathbb{R}\}$ y $M_2 = \{(0, y, z) : \ y, z \in \mathbb{R}\}$. Entonces M es generado por M_1 y M_2, es decir $M = M_1 + M_2$ y en este caso M_1 y M_2 no son independientes.*
2. *Nuevamente consideremos al $\mathbb{R}$-módulo $M = \mathbb{R}^3$ y sean $M' = \{(0, y, 0) : \ y \in \mathbb{R}\}$ y $M'' = \{(0, 0, z) : \ z \in \mathbb{R}\}$. Entonces M' Y M'' son independientes y en este caso M' y M'' no generan a M.*

Si M_1 y M_2 son R-submódulos de un R-módulo M tenemos que hay un R-homomorfismo $i : M_1 \times M_2 \to M$ dado por
$i(x_1, x_2) = x_1 + x_2$. Tenemos que $Imi = M_1 + M_2$ y
$Keri = \{(x, -x) : \ x \in M_1 \cap M_2\}$. Así que i es epimorfismo si y sólo si M_1 y M_2 generan a M y es monomorfismo si y sólo si M_1 y M_2 son independientes. Cuando el homomorfismo i es un isomorfismo tenemos la siguiente definición.

Definición 2.1.3. *Sean M_1 y M_2 submódulos de un módulo M. Decimos que M es **suma directa (interna)** de sus submódulos M_1 y M_2 si el homomorfismo $i : M_1 \times M_2 \to M$ es un isomorfismo. Y la denotamos como $M = M_1 \oplus M_2$.*

Es decir cuando M_1 y M_2 son independientes y generan a M.

Se puede ver fácilmente que M es suma directa de M_1 y M_2 si y sólo si para cada $x \in M$, x se tiene que x se escribe de manera única como $x = x_1 + x_2$ con $x_1 \in M_1$ y $x_2 \in M_2$.

Definición 2.1.4. *Un submódulo M_1 de un módulo M es un* ***sumando directo*** *de M si existe un submódulo M_2 de M tal que $M = M_1 \oplus M_2$.*
En este caso decimos que M_2 es también un sumando directo de M y a M_1 y M_2 los llamamos ***complementos directos*** *o* ***sumandos directos complementarios****.*

Ejemplos 2.1.5.

1. *Si M es un módulo distinto de cero, M es suma directa de M y 0.*
2. *Consideremos al $\mathbb{R}$-módulo $M = \mathbb{R}^2$ y a sus submódulos $M_1 = \{(x, 0) : x \in \mathbb{R}\}$ y $M_2 = \{(0, y) : y \in \mathbb{R}\}$. Entonces M es la suma directa de M_1 y M_2, esto es $M = M_1 \oplus M_2$ y en este caso M_1 y M_2 son complementos directos.*

El siguiente lema nos será de gran utilidad para encontrar sumandos directos de un módulo.

Lema 2.1.6. *Sea $f : M \to N$ y $f' : N \to M$ dos homomorfismos de módulos tales que $ff' = 1_N$. Entonces f es un epimorfismo, f' un monomorfismo y $M = Kerf \oplus Imf'$.*

Demostración. Veamos que f es epimorfismo. Si $y \in N$, entonces $f'(y) = x$ para alguna $x \in M$ y como $ff' = 1_N$ tenemos que $y = f(f'(y)) = f(x)$ por lo que $y \in Imf$, así $N \subseteq Imf$ y como $Imf \subseteq N$ tenemos que $Imf = N$ por lo que f es suprayectivo y por la Proposición (1.5.10) f es epimorfismo.
Veamos que f' es monomorfismo. Si $x \in Kerf'$, entonces $f'(x) = 0$ y como $ff' = 1_N$ tenemos que $0 = f(0) = f(f'(x)) = x$ así $x = 0$. Por lo tanto $Kerf' = 0$ y debido a la Proposición (1.5.11) f' es monomorfismo.
Ahora veamos que $M = Kerf \oplus Imf'$. Primero veremos que Imf' y $Kerf$ generan a M, es decir que $M = Kerf + Imf'$. Por el Lema (1.4.22) $Kerf + Imf' \leq M$, en particular $Kerf + Imf' \subseteq M$. Por otro lado, si $x \in M$, entonces $f(x - f'f(x)) = f(x) - f(x) = 0$ por lo que $x - f'f(x) \in Kerf$ y notemos que $x = x - f'(f(x)) + f'(f(x)) \in Kerf + Imf'$ de donde $M \subseteq Kerf + Imf'$. Por lo tanto $M = Kerf + Imf'$. Finalmente veamos que $Kerf$ e Imf' son independientes, es decir que $Kerf \cap Imf' = 0$. Sea $x = f'(y) \in Kerf \cap Imf'$. Entonces $0 = f(x) = f(f'(y)) = y$ y $x = f'(y) = 0$ por lo que $Kerf \cap Imf' = 0$. Por lo tanto $M = Kerf \oplus Imf'$.

□

Definición 2.1.7. *Sean $f : M \to N$ y $f' : N \to M$ homomorfismos de módulos tales que $ff' = 1_N$. En tal caso decimos que:*

1. *El homomorfismo f es un* ***epimorfismo que se escinde*** *y escribimos*

$$M \xrightarrow[\oplus]{f} N \longrightarrow 0 .$$

2. *El homomorfismo f' es un* ***monomorfismo que se escinde*** *y escribimos*

$$0 \longrightarrow N \xrightarrow[\oplus]{f'} M .$$

Sean M_1 y M_2 dos módulos, podemos considerar su producto cartesiano $M_1 \times M_2$ al cual le podemos asociar los homomorfismos **inclusión natural** y **proyección natural**, $i_j : M_j \to M_1 \times M_2$ y $\pi_j : M_1 \times M_2 \to M_j$ con $j = 1, 2$, definidos por $i_1(x_1) = (x_1, 0)$, $i_2(x_2) = (0, x_2)$ y $\pi_1(x_1, x_2) = x_1$, $\pi_2(x_1, x_2) = x_2$ para todo $x_1 \in M_1$ y $x_2 \in M_2$.
Claramente i_j y π_j son homomorfismos de módulos y podemos observar que $\pi_i i_j = \delta_{ij} 1_{M_i}$ y $i_1\pi_1 + i_2\pi_2 = 1_{M_1 \times M_2}$.

Ejemplo 2.1.8. *Consideremos a los homomorfismos de módulos proyección natural $\pi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ e inclusión natural $i : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$, entonces $\pi i = 1_{\mathbb{Z}}$. Por lo tanto i es un monomorfismo que se* ***escinde*** *y π es un epimorfismo que se escinde.*

Definición 2.1.9. *Sean M_1, M_2 y M módulos, decimos que una sucesión exacta corta $0 \longrightarrow M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \longrightarrow 0$ se* ***escinde*** *si f es un monomorfismo que se escinde y g es un epimorfismo que se escinde.*

Ejemplo 2.1.10. *Consideremos a los homomorfismos inclusión natural i_j y proyección natural π_j con $j = 1, 2$. Como $\pi_1 i_1 = 1_{M_1}$ y $\pi_2 i_2 = 1_{M_2}$ tenemos que las sucesiones exactas cortas $0 \longrightarrow M_1 \xrightarrow{i_1} M_1 \times M_2 \xrightarrow{\pi_2} M_2 \longrightarrow 0$ y $0 \longrightarrow M_2 \xrightarrow{i_2} M_1 \times M_2 \xrightarrow{\pi_1} M_1 \longrightarrow 0$ se escinden.*

La siguientes proposiciones nos proporcionan caracterizaciones para las sucesiones cortas que se escinden.

Proposición 2.1.11. *Sean N un módulo y*

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

una sucesión exacta corta. Entonces los siguientes enunciados son equivalentes:

(a) La sucesión exacta corta se escinde.

(b) El monomorfismo $f : M_1 \to M$ se escinde.

(c) *El epimorfismo $g : M \to M_2$ se escinde.*

(d) *$Imf = Kerg$ es un sumando directo de M.*

(e) *Cada homomorfismo $h : M_1 \to N$ se factoriza mediante f. Es decir, existe un homomorfismo $\bar{h} : M \to N$ tal que $\bar{h}f = h$.*

(f) *Cada homomorfismo $h : N \to M_2$ se factoriza mediante g. Es decir, existe un homomorfismo $\bar{h} : N \to M$ tal que $g\bar{h} = h$.*

Demostración. Notemos que (a) implica (b) y (a) implica (c) se siguen de la definición anterior, ya que una sucesión exacta corta se escinde si $f : M_1 \to M$ es un monomorfismo que se escinde y $g : M \to M_2$ es un epimorfismo que se escinde.
Veamos que (b) implica (d). Como $f : M_1 \to M$ es un monomorfismo que se escinde tenemos que existe un homomorfismo $f' : M \to M_1$ tal que $f'f = 1_{M_1}$. Además la sucesión es exacta por lo que $Imf = Kerg$ y debido al Lema (2.1.6) $M = Imf \oplus Kerf'$, de donde $Imf = Kerg$ es un sumando directo de M.
Veamos que (c) implica (d). Como $g : M \to M_2$ es un epimorfismo que se escinde tenemos que existe un homomorfismo $f' : M_2 \to M$ tal que $ff' = 1_{M_2}$. Nuevamente debido al Lema 1.5.11 $M = Imf' \oplus Kerg$ de donde $Imf = Kerg$ es un sumando directo de M.
Notemos que si suponemos ciertos (b) y (c) entonces ocurre (a), por lo que basta probar que (d) implica (e), (e) implica (b), (d) implica (f) y (f) implica (c). Primero veamos que (d) implica (e). Supongamos que $M = Imf \oplus K$ y $h : M_1 \to N$. Como f es un monomorfismo se tiene que para cada $m \in M$ hay un único $m_1 \in M_1$ y $k \in K$ tal que $m = f(m_1) + k$. Definimos el homomorfismo $\bar{h} : M \to N$ dado por $\bar{h}(m) = \bar{h}(f(m_1) + k) = h(m_1)$. Claramente el homomorfismo $\bar{h}$ está bien definido y $\bar{h}f = h$.
Veamos que (d) implica (f). Supongamos que $M = Kerg \oplus K$ y $h : N \to M_2$. Como $K \cap Kerg = 0$ y $g(M) = g(K)$ ya que $g(Kerg) = 0$, entonces g restringido a K, esto es $g|_K : K \to M_2$ es un isomorfismo, por lo que existe el inverso de g, $g^{-1} : M_2 \to K$. Entonces $\bar{h} := g^{-1}h : N \to K$ es un homomorfismo tal que $g\bar{h} = h$.
Veamos que (e) implica (b). Sea $h = 1_N$ y $N = M_1$, entonces existe un homomorfismo $\bar{h} : M_1 \to M$ tal que $\bar{h}f = h = 1_{M_1}$. Por lo tanto el homomorfismo f es un monomorfismo que se escinde. Finalmente veamos que (f) implica (c). Sea 1_N y $N = M_2$, entonces existe un homomorfismo $\bar{h} : M_2 \to M$ tal que $g\bar{h} = h$. Por lo tanto el homomorfismo g es un epimorfismo que se escinde.

□

Como consecuencia del resultado anterior tenemos el siguiente resultado.

Proposición 2.1.12. *Para una sucesión exacta corta de homomorfismos*

$$0 \longrightarrow M_1 \xrightarrow{f_1} M \xrightarrow{g_2} M_2 \longrightarrow 0$$

los siguientes enunciados son equivalentes.

(a) La sucesión exacta corta se escinde.

(b) Existe una sucesión exacta corta de homomorfismos

$$0 \longrightarrow M_2 \xrightarrow{f_2} M \xrightarrow{g_1} M_1 \longrightarrow 0$$

que se escinde.

(c) Existe un isomorfismo $h : M_1 \times M_2 \to M$ tal que el siguiente diagrama conmuta.

$$\begin{tikzcd}
 & M_1 \times M_2 \arrow[dd, "h"] \arrow[dr, "\pi_2"] & & \\
0 \arrow[r] & M_1 \arrow[u, "i_1"] \arrow[dr, "f_1"'] & & M_2 \arrow[r] & 0 \\
 & & M \arrow[ur, "g_2"'] & &
\end{tikzcd}$$

Demostración. Veamos que (a) implica (c). Definimos $h : M_1 \times M_2 \to M$ dado por $h(x_1, x_2) = f_1(x_1) + f_2(x_2)$ para algunos $x_1 \in M_1$ y $x_2 \in M_2$. Donde $f_2 : M_2 \to M$ satisface que $g_2 f_2 = 1_{M_2}$, entonces el diagrama conmuta. Para ver que el homomorfismo h es isomorfismo consideremos el siguiente diagrama conmutativo con renglones exactos.

$$\begin{tikzcd}
0 \arrow[r] \arrow[d, "1_0"'] & M_1 \arrow[r, "i_1"] \arrow[d, "1_{M_1}"'] & M_1 \times M_2 \arrow[r, "\pi_2"] \arrow[d, "h"'] & M_2 \arrow[r] \arrow[d, "1_{M_2}"'] & 0 \arrow[d, "1_0"'] \\
0 \arrow[r] & M_1 \arrow[r, "f_1"] & M \arrow[r, "g_2"] & M_2 \arrow[r] & 0
\end{tikzcd}$$

Entonces como 1_0, 1_{M_1} y 1_{M_2} son isomorfismos por el Lema del quinto inciso (c) obtenemos que el homomorfismo h es un isomorfismo.
Veamos que (c) implica (b). Dado un isomorfismo h que hace conmutar el diagrama definimos $f_2 := hi_2$ y $g_1 = \pi_1 h^{-1}$. Entonces $g_i f_j = \pi_i h^{-1} h i_j = \pi_i i_j = \delta_{ij} 1_{M_i}$ y $f_1 g_1 + f_2 g_2 = h i_1 \pi_1 h^{-1} + h i_2 \pi_2 h^{-1} = h(i_1\pi_1 + i_2\pi_2)h^{-1} = hh^{-1} = 1_M$.
Finalmente veamos que (b) implica (a). Supongamos entonces que $f_1 g_1 + f_2 g_2 = 1_M$ por lo que $M = Imf_1 + Imf_2$. Pero $g_2 f_1 = 0$ lo que implica que $Imf_1 \subseteq Kerg_2$ y además $g_2 f_2 = 1_{M_2}$, entonces por la Proposición (2.1.6) tenemos que $M = Kerg_2 \oplus Imf_2$. De la ley modular obtenemos que $Kerg_2 = Kerg_2 \cap M = Kerg_2 \cap (Imf_1 + Imf_2) = Imf_1 + (Kerg_2 \cap Imf_2) = Imf_1$. Por lo tanto la sucesión $0 \longrightarrow M_1 \xrightarrow{f_1} M \xrightarrow{g_2} M_2 \longrightarrow 0$ es exacta y como $g_1 f_1 = 1_{M_1}$ y $g_2 f_2 = 1_{M_2}$ la sucesión exacta se escinde.

□

El siguiente ejemplo ilustra el inciso c) de la Proposición anterior.

Ejemplo 2.1.13. *Sean $M = \mathbb{R}^2$ un $\mathbb{R}$-módulo y $M_1 = \mathbb{R}$ y $M_2 = \mathbb{R}$ submódulos de M y supongamos que $0 \longrightarrow M_1 \xrightarrow{f_1} M \xrightarrow{g_2} M_2 \longrightarrow 0$ se escinde. Entonces existe $h : M_1 \times M_2 \to M$ dado por $h(x,y) = f_1(x) + g_2^{-1}(y)$ donde $g_2 g_2^{-1} = 1_{M_2}$; $g_2^{-1} : M_2 \to M$ tal que el siguiente diagrama conmuta.*

$$\begin{tikzcd}
 & & M_1 \times M_2 \arrow[dd, "h"] \arrow[dr, "\pi_2"] & & \\
0 \arrow[r] & M_1 \arrow[ur, "i_1"] \arrow[dr, "f_1"'] & & M_2 \arrow[r] & 0 \\
 & & M \arrow[ur, "g_2"'] & &
\end{tikzcd}$$

Ya que $i_1(x) = (x,0)$ y $h(x,0) = f_1(x) + g_2^{-1}(0) = f_1(x)$.
Por otro lado tenemos que $h(x,y) = f_1(x) + g_2^{-1}(y)$ y
$g_2(f_1(x) + g_2^{-1}(y)) = g_2(f_1(x)) + g_2(g_2^{-1}(y)) = 0 + 1_{M_2}(y) = y = \pi_2(x,y)$.

2.2. Proyecciones.

En esta sección veremos un caso particular de epimorfismos llamados proyecciones, los cuales nos serán de gran utilidad para caracterizar a los sumandos directos de un módulo M.

Definición 2.2.1. *Sea K un sumando directo de un módulo M con complemento directo K', es decir $M = K \oplus K'$. Entonces la función $p_K(k + k') = k$ con $k \in K$ y $k' \in K'$ define un epimorfismo $p_K : M \to K$ llamado la* ***proyección de M en K a lo largo de K'****.*

Proposición 2.2.2. *Sean M un módulo y K, K' submódulos de M.*
Si $M = K \oplus K'$, entonces la proyección de M en K a lo largo de K' es el único epimorfismo $M \xrightarrow{p_K} K \longrightarrow 0$ que satisface $(p|_K) = 1_K$ y $Kerp_K = K'$.

Demostración. Notemos que por consecuencia directa de su definición el epimorfismo p_K satisface que $(p_K|_K) = 1_K$ y $Kerp_K = K'$. Ahora supongamos que $g : M \to K$ es un epimorfismo tal que $(g|_K) = 1_K$ y $Kerg = K'$, entonces para todo $k \in K$ y $k' \in K'$, $g(k + k') = g(k) + g(k') = k = p_K(k + k')$. Por lo tanto p_K es el único epimorfismo que cumple dichas condiciones.

□

Nuevamente consideremos un sumando directo K de un módulo M con complemento directo K', $M = K \oplus K'$. Entonces K' es un sumando directo de M con complemento directo K. Además si p_K es la proyección de M en K a lo largo de K', entonces la proyección $p_{K'}$ de M en K' a lo largo de K puede ser caracterizada por $p_{K'}(m) = m - p_K(m)$ para toda $m \in M$.
Ahora si $i_K : K \to M$ y $i'_K : K' \to M$ son los homomorfismos inclusión de K

en M e inclusión de K' en M, entonces por las proposiciones (2.1.11) y (2.1.12) las sucesiones exactas cortas:

$$0 \longrightarrow K' \xrightarrow{i'_K} M \xrightarrow{p_K} K \longrightarrow 0$$

$$0 \longrightarrow K \xrightarrow{i_K} M \xrightarrow{p'_K} K' \longrightarrow 0$$

se escinden.
En general un sumando directo de un módulo tiene muchos complementos directos, las proyecciones nos proporcionan una útil caracterización para estos.

Proposición 2.2.3. *Sean M un módulo y K, K' sumandos directos de M tales que $M = K \oplus K'$, y sean p_K la proyección de M en K a lo largo de K' y L un submódulo de M. Entonces $M = L \oplus K'$ si y sólo si $p_K|_L : L \to K$ es un isomorfismo.*

Demostración. Sea $L \leq M = K \oplus K'$. Entonces $Ker(p_K|_L) = L \cap Kerp_K = L \cap K'$ por lo que (p_K) es monomorfismo si y sólo si $L \cap K' = 0$.
Por otro lado, como $(p_K|_K) = 1_K$ y $Kerp_K = K'$ tenemos que
$p_K(L) = p_K(L + K') = p_K((L + K') \cap (K + K')) = p_k(((L + K') \cap K) + K')$ y por la ley modular $p_K(((L+K')\cap K)+K') = p_K((L+K')\cap K) = (L+K')\cap K$ entonces $p_K(L) = K$ si y sólo si $M = L + K'$. □

A continuación retomaremos el Ejemplo (2.1.5) inciso 2 para ilustrar la Proposición anterior.

Ejemplo 2.2.4. *Consideremos al $\mathbb{R}$-módulo $M = \mathbb{R}^2$ y a sus submódulos $K = \{(x, 0) : x \in \mathbb{R}\}$, $K' = \{(0, y) : y \in \mathbb{R}\}$ y $L = \{(z, z) : z \in \mathbb{R}\}$. Entonces $M = K \oplus K' = L \oplus K'$ y la proyección $p_K|_L : L \to K$ dada por $p_K|_L((z, z)) = (z, 0)$ es un isomorfismo.*

2.3. Endomorfismos idempotentes.

Sean K un sumando directo de un R-Módulo M con complemento directo K', esto es $M = K \oplus K'$, y p_K la proyección de M en K a lo largo de K'. Definimos $e_K \in End(M)$ como $e_K(x) = p_K(x)$ para todo $x \in M$. Como $(p_K|_K) = 1_K$, tenemos que e_K es un endomorfismo idempotente de M, es decir $e_K = e_K^2 \in End(M)$ y notamos que $K = Ime_K$. Así cada sumando directo de M es la imagen de un endomorfismo idempotente de M.
Recordemos que dado un homomorfismo $f : M \to N$, algunas veces denotamos por $f(M)$ a la Imf. En el siguiente lema veremos que también se cumple el reciproco.

Lema 2.3.1. *Sea $e \in End(M)$ un endomorfismo idempotente. Entonces $1_M - e \in End(M)$ es un endomorfismo idempotente tal que:*

$$Kere = \{x \in M : \ x = (1_M - e)(x)\} = Im(1 - e),$$

$$Ime = \{x \in M : \ x = e(x)\} = Ker(1 - e)$$

y $M = e(M) \oplus (1 - e)(M)$.

Demostración. Recordemos que si e es un idempotente, entonces $1_M - e$ también lo es. Como $e^2 = e$, tenemos que $Ime \subseteq \{x \in M : \ x = e(x)\} \subseteq Ker(1_M - e)$, ya que si $x \in M$, entonces $(1_M - e)(e(x)) = 1_M(e(x)) - e(e(x)) = e(x) - e(x) = 0$ y $Im(1_M - e) = \{x \in M : \ x = (1_M - e)(x)\} \subseteq Kere$, ya que $e(1_M - e)(x)) = e(1_M(x)) - e(e(x)) = e(x) - e(x) = 0$. Y es claro que $Ker(1_M - e) \subseteq Ime$ pues si $x \in Ker(1_M - e)$ entonces $(1_M - e)(x) = x - e(x) = 0$ por lo que $x = e(x) \in Ime$. Análogamente se puede ver que $Kere \subseteq Im(1_M - e)$.
Ahora notemos que para todo $x \in M$ se tiene que $x = e(x) + (1_M - e)(x)$ de donde $M = e(M) + (1_M - e)(M)$. Por otro lado si $x = e(x) = (1_M - e)(y)$ para algún $y \in M$ se tiene que $e(x) = e^2(x) = e((1_M - e)(y)) = e(y - e(y)) = e(y) - e^2(y) = e(y) - e(y) = 0$. Por lo tanto $e(M) \cap (1 - e)(M) = 0$, de donde $M = e(M) \oplus (1 - e)(M)$.

□

Proposición 2.3.2. *Sea M un módulo y K, K' submódulos de M. Si $M = K \oplus K'$, entonces hay un único endomorfismo idempotente $e_K \in End(M)$ tal que $K = e_K(M)$ y $K' = (1_M - e_K)(M)$.*

Demostración. Como $e_K \in End(M)$ es un endomorfismo idempotente por el Lema (2.3.1) $M = e_K(M) \oplus (1_M - e_K)(M)$, entonces $p_{e_K(M)}(x) = e(x)$ es la proyección de M en $e_K(M)$ a lo largo de $(1_M - e_K)(M)$, con $K = e_K(M)$ y $K' = (1_M - e_K)(M)$. De la Proposición (2.2.2) el endomorfismo $e_K(x) = p_{Me_K}$ es único.

□

Corolario 2.3.3. *Un submódulo K de un módulo M es un sumando directo de M si y sólo si $K = Ime$ para algún endomorfismo idempotente e de M.*

Demostración. Supongamos que K es un sumando directo de M, es decir $M = K \oplus K'$ para algún $K' \leq M$, entonces $p_K : M \to K$ es un endomorfismo idempotente tal que $p_K(M) = K$.
Ahora supongamos que $K = Ime$ para algún endomorfismo idempotente e de M, entonces $K = e(M)$. Como e es un endomorfismo idempotente tenemos que $1_M - e$ también es un endomorfismo idempotente y por el Lema (2.3.1) $M = e(M) \oplus (1_M - e)(M)$. Por lo tanto $K = e(M)$ es un sumando directo de M.

□

Definición 2.3.4. *Decimos que un módulo $M \neq 0$ es* ***inescindible*** *si 0 y M son sus únicos sumandos directos.*

Ejemplo 2.3.5. *Consideremos al $\mathbb{Z}$-módulo $\mathbb{Z}$, entonces $\mathbb{Z}$ es inescindible. En efecto, sean $n\mathbb{Z}$ y $m\mathbb{Z}$ submódulos de $\mathbb{Z}$ con $n, m \in \mathbb{N}$, tales que $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$ y $n\mathbb{Z} \cap m\mathbb{Z} = 0$. Si $n \neq 0$, entonces $n\mathbb{Z} \neq 0$ y como $n\mathbb{Z} + m\mathbb{Z} = (n, m)\mathbb{Z}$ y $n\mathbb{Z} \cap m\mathbb{Z} = [n, m]\mathbb{Z} = 0$ tenemos que $(n, m) = 1$ y $[n, m] = 0$ por lo que*

$nm = (n,m)[n,m] = 1 \cdot 0 = 0$ *esto implica que* $m = 0$*, es decir* $m\mathbb{Z} = 0$*. Por lo tanto* $\mathbb{Z} = n\mathbb{Z}$*.*

Definición 2.3.6. *Decimos que un par de idempotentes* e_1*,* e_2 *de un anillo* R *son* ***ortogonales*** *si* $e_1e_2 = \hat{0} = e_2e_1$*.*

Ejemplos 2.3.7.

1. *Dado un anillo* R*, el par de idempotentes* 0*,*1 *son ortogonales.*

2. *Si* e *es un idempotente de un anillo* R*, el par de idempotentes* e*,* $1 - e$ *son ortogonales tales que* $1 = e + (1 - e)$*.*

Definición 2.3.8. *Un idempotente* e *de un anillo* R *es un* ***idempotente primitivo*** *si* $e \neq 0$ *y para cada par* e_1*,* e_2 *de idempotentes ortogonales tales que* $e = e_1 + e_2$ *implica que* $e_1 = 0$ *o* $e_2 = 0$*.*

Ejemplo 2.3.9. *Consideremos el anillo* $\mathbb{Z}$ *tenemos que* 1 *es un idempotente primitivo.*

Proposición 2.3.10. *Sea* M *un módulo no cero. Entonces los siguientes enunciados son equivalentes:*

(a) M *es inescindible.*

(b) $\hat{0}$ *y* 1_M *son los únicos idempotentes en* $End(M)$*.*

(c) 1_M *es un idempotente primitivo en* $End(M)$*.*

Demostración. Veamos que (a) implica (b). Sea $e \in End(M)$ un idempotente tal que $\hat{0} \neq e \neq 1_M$, por Lema (2.3.1) $M = e(M) \oplus (1_M - e)(M)$ lo cual es un contradicción al hecho de que M sea inescindible. Por lo tanto $\hat{0}$ y 1_M son los únicos idempotentes en $End(M)$.
Veamos que (b) implica (c). Supongamos que $\hat{0}$ y 1_M son los únicos idempotentes en $End(M)$. Claramente $1_M = 1_M + \hat{0}$ y $\hat{0}$ y 1_M son los únicos idempotentes ortogonales por lo que 1_M es un idempotente primitivo en $End(M)$.
Finalmente veamos que (c) implica (a). Si e es un idempotente en $End(M)$, entonces e y $1_M - e$ son ortogonales y por Lema (2.3.1) $M = e(M) \oplus (1-e)(M)$. Como 1_M es primitivo y $1_M = e + (1_M - e)$ se tiene que $e = \hat{0}$ o $(1_M - e) = \hat{0}$. Si $e = \hat{0}$, entonces $(1_M - e) = 1_M$ y $M = 0 \oplus M$ por lo que M sería inescindible. Si $(1_M - e) = \hat{0}$, entonces $1_M = e$ y $M = M \oplus 0$ por lo que M sería inescindible. Por lo tanto concluimos que M es inescindible.

□

Corolario 2.3.11. *Sea* e *un endomorfismo idempotente no cero de un módulo* M*. Entonces el sumando directo* $e(M)$ *de* M *es inescindible si y sólo si* e *es un idempotente primitivo en* $End(M)$*.*

Demostración. Supongamos que el sumando directo $e(M)$ de M es inescindible y sean e_1, e_2 idempotentes ortogonales en $End(M)$ tales que $e = e_1 + e_2$. Entonces

$e(M) = e_1(M) \oplus e_2(M)$ y como $e(M)$ es inescindible, entonces $e_1(M) = \hat{0}$ y $e_2(M) = e(M)$ o $e_1(M) = e(M)$ y $e_2(M) = \hat{0}$. Por lo tanto $e_1 = \hat{0}$ o $e_2 = \hat{0}$, es decir e es un idempotente primitivo en $End(M)$.
Ahora supongamos que e es un idempotente primitivo en $End(M)$, entonces para cualquier par de idempotentes ortogonales e_1, e_2 tales que $e = e_1 + e_2$ se tiene que $e_1 = \hat{0}$ o $e_2 = \hat{0}$. Como $e = e_1 + e_2$ tenemos que $e(M) = e_1(M) \oplus e_2(M)$, si $e_1 = \hat{0}$ tenemos que $e(M) = 0 + e_2(M)$, de donde $e(M) = e_2(M)$, es decir $e(M)$ es inescindible. Si $e_2 = \hat{0}$ entonces $e(M) = e_1(M) + 0$ de donde $e(M) = e_1(M)$, es decir M es inescindible.

$\square$

2.4. Submódulos superfluos y esenciales.

Recordemos que un submódulo K de un módulo M es un sumando directo de M si existe un submódulo K' de M tal que $K \cap K' = 0$ y $K + K' = M$. Para cada submódulo K de M siempre podemos encontrar un submódulo que satisfaga alguna de las condiciones anteriores. En efecto $K \cap 0 = 0$ y $K + M = M$. A continuación introduciremos los conceptos de submódulo superfluo y submódulo esencial de un módulo M, los cuales están estrechamente relacionados con las condiciones anteriores.

Definición 2.4.1. *Sea K un submódulo de un módulo M.*

1. *El submódulo K es* ***esencial*** *en M si para cada submódulo $L \leq M$ tal que $K \cap L = 0$ implica que $L = 0$. Y lo denotamos por $K \trianglelefteq M$.*

2. *El submódulo K es* ***superfluo*** *en M si para cada submódulo $L \leq M$ tal que $K + L = M$ implica que $L = M$. Y lo denotamos por $K \ll M$.*

Ejemplos 2.4.2.

1. *Consideremos al $\mathbb{R}$-módulo $\mathbb{R}^2$, entonces $\mathbb{R}^2$ es esencial en $\mathbb{R}^2$. Ya que si $L \leq \mathbb{R}^2$ y $\mathbb{R}^2 \cap L = 0$, entonces $L = 0$. Pues si $L \neq 0$, entonces existe $0 \neq x \in L \subseteq \mathbb{R}^2$ por lo que $0 \neq x \in \mathbb{R}^2$ de donde $\mathbb{R}^2 \cap L \neq 0$ lo cual sería una contradicción pues $\mathbb{R}^2 \cap L = 0$, por lo tanto $L = 0$.*
   De hecho, en general dado un módulo M, tenemos que M es esencial en M.

2. *Dado un módulo M, el submódulo 0 es superfluo en M. Ya que si $L \leq M$ tal que $0 + L = M$, entonces $L = M$. Pues si L es un submódulo propio en M tenemos que $L = L + 0$ está contenido propiamente en M.*

Definición 2.4.3. *Sean K, M y N módulos.*

1. *Un monomorfismo $f : K \to M$ es esencial si $Imf \trianglelefteq M$.*

2. *Un epimorfismo $g : M \to N$ es superfluo si $Kerg \ll M$.*

La siguiente proposición nos proporciona una caracterización de los submódulos esenciales de un módulo.

Proposición 2.4.4. *Para un submódulo K de un módulo M los siguientes enunciados son equivalentes.*

(a) $K \trianglelefteq M$.

(b) El homomorfismo inclusión $i_K : K \to M$ *es un monomorfismo esencial.*

(c) Para cada módulo N y para cada homomorfismo $h : M \to N$, si $(Kerh) \cap K = 0$ implica que $Kerh = 0$.

Demostración. Notemos que (a) implica (b) es claro ya que $Imi_K = K \trianglelefteq M$.
Veamos que (a) implica (c). Sea $h : M \to N$ un homomorfismo tal que $(Kerh) \cap K = 0$. Como K es esencial en M tenemos que $Kerh = 0$.
Finalmente veamos que (c) implica (a). Sean L un submódulo de M tal que $K \cap L = 0$ y $\eta_L : M \to M/L$ el epimorfismo canónico, entonces $(Ker\eta_L) \cap K = L \cap K = 0$ de donde $ker\eta_L = L = 0$. Por lo tanto K es esencial en M.
□

El siguiente corolario caracteriza a los monomorfismos esenciales.

Corolario 2.4.5. *Un monomorfismo $f : L \to M$ es esencial si y sólo si para todo homomorfismo h, si hf es monomorfismo, entonces h es monomorfismo.*

Demostración. Supongamos que el monomorfismo $f : L \to M$ es esencial. Sea h un monomorfismo tal que hf es un monomorfismo. Afirmamos que $Imf \cap Kerh = 0$, pues de lo contrario existe $0 \neq x \in Imf \cap Kerh$ esto implica que $0 \neq x = f(l)$ para algún $l \in L$ con $l \neq 0$ pues $0 \neq f(l)$ y f es monomorfismo, y $h(x) = 0$. Así $h(f((l)) = h(x) = 0$ de donde $l \in Kerhf = 0$, es decir $l = 0$ lo cual es una contradicción al hecho de que $l \neq 0$. Por lo tanto $Imf \cap Kerh = 0$ y como f es esencial en M tenemos que $Kerh = 0$ lo que implica que h es monomorfismo.
Ahora supongamos que para todo homomorfismo h, si hf es monomorfismo, entonces h es monomorfismo. Sea K un submódulo de M tal que $K \cap Imf = 0$ y sea $h : M \to M/K$ el epimorfismo canónico. Veamos que el homomorfismo hf es un monomorfismo. En efecto, sea $x \in Kerhf$, entonces $h(f(x)) = 0$ por lo que $f(x) \in Kerh = K$ de donde $f(x) \in K \cap Imf = 0$, así $f(x) = 0$ y como f es monomorfismo $Kerf = 0$, entonces $x = 0$ por lo tanto $Kerhf = 0$. Entonces hf es monomorfismo por lo tanto h es monomorfismo de donde $Kerh = K = 0$. Por lo tanto f es esencial en M. □

Notemos que la siguiente proposición y el siguiente corolario son los resultados duales de la proposición y el corolario de submódulos esenciales.

Proposición 2.4.6. *Para un submódulo K de un módulo M los siguientes enunciados son equivalentes.*

(a) $K \ll M$.

(b) El epimorfismo canónico $\eta_K : M \to M/K$ *es superfluo.*

(c) Para cada módulo N y para cada homomorfismo $h : N \to M$, si $(Imh) + K = M$ entonces $Imh = M$.

Demostración. Veamos que (a) implica (b). Supongamos que $K \ll M$, como $Ker\eta_K = K$ y $K \ll M$ tenemos que el epimorfismo canónico η_K es superfluo.
Veamos que (b) implica (c). Supongamos que el epimorfismo canónico $\eta_K : M \to M/K$ es superfluo, entonces $Ker\eta_K = K \ll M$. Sea $h : N \to M$ un homomorfismo tal que $(Imh) + K = M$. Como $Imh \leq M$ y K es superfluo en M tenemos que $Imh = M$.
Finalmente veamos que (c) implica (a). Supongamos que para cada módulo N y para cada homomorfismo $h : N \to M$ si $(Imh)+K = M$ implica que $Imh = M$. Sea $L \leq M$ tal que $L + K = M$. Consideremos el monomorfismo inclusión $i : L \to M$, haciendo $N = L$ Y $h = i$, tenemos que $L + K = (Imh) + K = M$ de donde $L = Imh = M$. Por lo tanto $K \ll M$. □

Corolario 2.4.7. *Un epimorfismo $g : M \to N$ es superfluo si y sólo si para todo homomorfismo h, si gh es epimorfismo, entonces h es epimorfismo.*

Demostración. Supongamos que el epimorfismo $g : M \to N$ es superfluo. Sea L un módulo y $h : L \to M$ un homomorfismo tal que gh es epimorfismo. Afirmamos que $M = Kerg + (Imh)$. En efecto como $Kerg$ e Imh son submódulos de M y sabemos que la suma de submódulos de un módulo M es un submódulo de M por lo que en particular $Kerg + (Imh) \subseteq M$, así resta verificar que $M \subseteq Kerg + (Imh)$. Sea $x \in M$, entonces $g(x) = n$ para alguna $n \in N$ y como gh es epimorfismo se tiene que $n = g(h(l))$ para alguna $l \in L$, entonces $n = g(x) = g(h(l))$ lo que implica que $g(x-h(l)) = 0$ es decir $x-h(l) \in Kerg$ y notemos que $x = (x-h(l))+h(l) \in Kerg+Imh$ por lo que $M = Kerg+Imh$. Y como $Kerg \ll M$ se tiene que $Imh = M$ de donde el homomorfismo h es suprayectivo y por la Proposición (1.5.10) epimorfismo.
Ahora supongamos que K es un submódulo de M tal que $M = Kerg + K$. Consideremos al monomorfismo $i_K : K \to M$ y vramos que $gi_K : K \to N$ es un epimorfismo. Por la Proposición (1.5.10) es equivalente a demostrar que gi_K es suprayectivo. Sea $n \in N$. Como $g : M \to$ es epimorfismo, nuevamente por la Proposición (1.5.10) tenemos que g es suprayectivo, así que existe $m \in M$ tal que $n = g(m)$. Pero como $M = Kerg + K$ tenemos que $m = m_1 + k$, donde $m_1 \in Kerg$ y $k \in K$. Así $n = g(m) = g(m_1 + k) = g(m_1) + g(k) = g(k)$. De donde $n = g(k) = gi_K(k)$. Lo cual prueba que gi_K es un epimorfismo, entonces i_k es epimorfismo. Por lo tanto $K = i(K) = M$ por lo que $Kerg$ es superfluo en M.

□

Proposición 2.4.8. *Sea M un módulo con submódulos $K \leq N \leq M$ y $H \leq M$. Entonces.*

(1) $K \trianglelefteq M$ si y sólo si $K \trianglelefteq N$ y $N \trianglelefteq M$.

(2) $H \cap K \trianglelefteq M$ si y sólo si $H \trianglelefteq M$ y $K \trianglelefteq M$.

Demostración. Para el inciso (1) supongamos que $K \trianglelefteq M$ y sea $0 \neq L \leq M$, entonces $L \cap K \neq 0$. En particular en cierto si $L \leq N$, entonces $K \trianglelefteq N$. Además si $K \leq N \leq M$, entonces $L \cap N \neq 0$ de donde $N \trianglelefteq M$.
Ahora supongamos que $K \trianglelefteq N$ y $N \trianglelefteq M$ y sea $L \leq M$ tal que $L \cap K = 0$ como K es esencial en N tenemos que $K \cap L \cap N = 0$ por lo que $L \cap N = 0$ y como $N \trianglelefteq M$, entonces $L = 0$. Por lo tanto $K \trianglelefteq M$.
Para el inciso (2) supongamos que $H \cap K \trianglelefteq M$. Sea $L \leq M$ tal que $K \cap L = 0$. Entonces $H \cap K \cap L = 0$ y como $H \cap K \trianglelefteq M$ tenemos que $L = 0$ por lo que K es esencial en M. Análogamente sea $L' \leq M$ tal que $H \cap L' = 0$, entonces $K \cap H \cap L' = H \cap K \cap L' = 0$ y como $H \cap K \trianglelefteq M$ tenemos que $L' = 0$ por lo que H es esencial en M.
Ahora supongamos que $H \trianglelefteq M$ y $K \trianglelefteq M$. Sea $L \leq M$ tal que $L \cap H \cap K = 0$, como $L \cap H \leq M$ y $K \trianglelefteq M$ tenemos que $L \cap H = 0$ y como $H \trianglelefteq M$ tenemos que $L = 0$. Por lo tanto $H \cap K \trianglelefteq M$.

□

Proposición 2.4.9. *Sea M un módulo con submódulos $K \leq N \leq M$ y $H \leq M$. Entonces.*

(1) $N \ll M$ si y sólo si $K \ll M$ y $N/K \ll M/K$.

(2) $H + K \ll M$ si y sólo si $H \ll M$ y $K \ll M$.

Demostración. Para el inciso (1) supongamos que $N \ll M$. Sea $L \leq M$ tal que $K + L = M$. Entonces $N + L = M$ y como $N \ll M$ se tiene que $L = M$. Por lo tanto $K \ll M$.
Por otro lado, sea $L' \leq M$ tal que $N/K + L'/K = M/K$. Se tiene que $N + L' = M$ de donde $L' = M$, entonces $L'/K = M/K$. Por lo tanto $N/K \ll M/K$.
Ahora supongamos que $K \ll M$ y $N/K \ll M/K$. Sea $L \ll M$ tal que $N + L = M$. Entonces $N/K + L/K = (N + L)/K = M/K$ y como $N/K \ll M/K$ se tiene que $L/K = M/K$ por lo que $L = M$. Por lo tanto $N \ll M$.
Para el inciso (2) supongamos que $H + K \ll M$ y veamos que $H \ll M$ y $K \ll M$. Sea $L \leq M$ tal que $H + L = M$. Entonces $H + K + L = M$ y como $H + K \ll M$ se tiene que $L = M$. Por lo tanto $H \ll M$. Análogamente para K.
Ahora supongamos que $H \ll M$ y $K \ll M$. Sea $L' \leq M$ tal que $(H + K) + L = M$. Como $(H + K) + L = H + (K + L) = M$ y $H \ll M$ tenemos que $K + L = M$ y $K \ll M$, entonces $L = M$. Por lo tanto $(H + K) \ll M$.

□

Lema 2.4.10. *Sean M un módulo y K un submódulo de M. Si $K \ll M$ y $f : M \to N$ es un homomorfismo, entonces $f(K) \ll N$. En particular, si $K \ll M \leq N$ entonces $K \ll N$.*

Demostración. Sea L un submódulo de M tal que $L + f(K) = N$. Afirmamos que $f^{\leftarrow}(L) + K = M$. Como $f^{\leftarrow}(L) + K \subseteq M$ resta verificar que $M \subseteq f^{\leftarrow}(L) + K$. En efecto sea $x \in M$, como $N = L + f(K)$ y $f(x) = n$ para alguna $n \in N$, entonces $f(x) = n = l + f(k)$ para alguna $l \in L$ y $k \in K$ esto implica que $f(x) - f(k) = f(x - k) = l$, de donde $x - k \in f^{\leftarrow}(L)$ y notemos que $x = x - k + k$

por lo que $x \in f^{\leftarrow}(L) + K$. Por lo tanto $M = f^{\leftarrow}(L) + K$ y como $K \ll M$ tenemos que $f^{\leftarrow}(L) = M$, entonces $f(K) \leq L$ de donde $L = N$. Por lo tanto $f(K) \ll N$.

□

El siguiente lema nos proporciona una prueba muy útil para las inclusiones esenciales.

Lema 2.4.11. *Un submódulo K de un R-módulo M es esencial en M si y sólo si para cada $0 \neq x \in M$ existe un $r \in R$ tal que $0 \neq rx \in K$.*

Demostración. Supongamos que $K \trianglelefteq M$ y sea $0 \neq x \in M$, entonces $0 \neq Rx$. Luego $Rx \cap K \neq 0$ de donde $rx \in K$ para alguna $r \in R$.
Ahora supongamos que para cada $0 \neq x \in M$ existe un $r \in R$ tal que $0 \neq rx \in K$. Sea $0 \neq x \in L \leq M$, entonces existe un $r \in R$ tal que $0 \neq rx \in K \cap L$, es decir $0 \neq K \cap L$. Por lo tanto K es esencial en M. □

Proposición 2.4.12. *Supongamos que $K_1 \leq M_1 \leq M$, $K_2 \leq M_2 \leq M$, y $M = M_1 \oplus M_2$, entonces:*

(1) $K_1 + K_2 \ll M_1 \oplus M_2$ si y sólo si $K_1 \ll M_1$ y $K_2 \ll M_2$.

(2) $K_1 + K_2 \trianglelefteq M_1 + M_2$ si y sólo si $K_1 \trianglelefteq M_1$ y $K_2 \trianglelefteq M_2$.

Demostración. Para el inciso (1), supongamos que $K_1 + K_2 \ll M$. Sea $p_i : M \to M_i$ la proyección de M en M_i a lo largo de M_j con $i \neq j$, $i = 1, 2$. Entonces $K_i = p_i(K_i)$ y por el Lema (2.4.10) tenemos que $K_i = p_i(K_i) \ll M_i$. Por lo tanto $K_1 \ll M_1$ y $K_2 \ll M_2$.
Supongamos ahora que $K_i \ll M_i$ para $i = 1, 2$. Sea $i_{K_i} : K_i \to M$ la inclusión de K_i en M. Entonces $i_{K_i}(K_i) = K_i$ y nuevamente por el Lema (2.4.10) tenemos que $K_i \ll M = M_1 \oplus M_2$ y de la Proposición (2.4.9) inciso (2) obtenemos que $K_1 \oplus K_2 = K_1 + K_2 \ll M$.
Para el inciso (2), supongamos primero que $K_1 + K_2 \trianglelefteq M_1 + M_2$. Sea $0 \neq L_1 \leq M_1$ tal que $K_1 \cap L_1 = 0$. Afirmamos que $(K_1 + K_2) \cap L_1 = 0$. En efecto sea $x \in (K_1 + K_2) \cap L_1$, entonces $x = k_1 + k_2 = l_1$ para algún $k_1 \in K_1$, $k_2 \in K_2$ y $l_1 \in L_1$, entonces $k_2 = l_1 - k_1 \in M_1 \cap M_2 = 0$. Por lo tanto $(K_1 + K_2) \cap L_1 = 0$ y como $K_1 + K_2 \trianglelefteq M$ tenemos que $L_1 = 0$. Por lo tanto K_1 es esencial en M_1. Análogamente para K_2.
Supongamos ahora que $K_i \trianglelefteq M_i$ para $i = 1, 2$. Sea $0 \neq x_i \in M_i$, por el Lema (2.4.11) existe un $r_1 \in R$ tal que $0 \neq r_1 x_1 \in K_1$. Si $r_1 x_2 \in K_2$, entonces $0 \neq r_1 x_1 + r_1 x_2 \in K_1 \oplus K_2$. Si $r_1 x_2 \notin K_2$, por Lema (2.4.11) existe $r_2 \in R$ tal que $0 \neq r_2 r_1 x_2 \in K_2$ y tenemos que $0 \neq r_2 r_1 x_1 + r_2 r_1 x_2 \in K_1 \oplus K_2$. Por lo tanto $K_1 \oplus K_2 \trianglelefteq M$. □

Capítulo 3

Suma directa de módulos.

3.1. Producto directo.

En esta sección daremos la generalización de producto directo de módulos y supondremos que $\{M_\alpha\}_{\alpha\in I}$ es una familia indizada de R-módulos (ver la Definición 1.2.1).

Dada una familia $\{M_\alpha\}_{\alpha\in I}$ de R-módulos, al producto cartesiano de $\{M_\alpha\}_{\alpha\in I}$ se le puede dar estructura de R-módulo de la siguiente manera.
Dados $x = (a_\alpha)_{\alpha\in I}, y = (b_\alpha)_{\alpha\in I} \in \bigtimes\limits_I M_\alpha$, definimos

$$x + y = (a_\alpha + b_\alpha)_{\alpha\in I} = (\pi_\alpha(x) + \pi_\alpha(y))_{\alpha\in I}$$

con $\pi_\alpha : \bigtimes\limits_I M_\alpha \to M_\alpha$ dada por $\pi_\alpha(x) = \pi_\alpha((a_\beta)_{\beta\in I}) = a_\alpha$. A la función π_α se le conoce como **la α-ésima proyección**. Para cada $r \in R$,

$$rx = r(a_\alpha)_{\alpha\in I} = (ra_\alpha)_{\alpha\in I}.$$

Al R-módulo resultante lo llamaremos **producto directo** o **cartesiano** de la familia $\{M_\alpha\}_{\alpha\in I}$ y lo denotaremos por $\prod\limits_I M_\alpha$. Cuando I es un conjunto finito lo denotaremos por $\prod_{i=1}^n M_i$ o $M_1 \times M_2 \times ... \times M_n$. Además si $M = M_\alpha$ para toda $\alpha \in I$ denotaremos por M^I a $\prod\limits_I M_\alpha$.
Si $I = \emptyset$ se tiene que el producto directo $\prod\limits_\emptyset M_\alpha = 0 = \{(0_\alpha)_{\alpha\in I}\}$

Por el Lema (1.2.6) estas operaciones están bien definidas en el producto directo y es fácil verificar que inducen una estructura de R-módulo.

Observación 3.1.1. *Dada una familia de R-módulos $\{M_\alpha\}_{\alpha\in I}$ tenemos que $0 = (0_\alpha)_{\alpha\in I}$ es el neutro aditivo del R-módulo producto directo $\prod\limits_I M_\alpha$.*

Más aún, dado que $x = (a_\alpha)_{\alpha\in I} \in \prod_I M_\alpha$ *se tiene que* $-x = (-a_\alpha)\alpha \in I$ *es el inverso aditivo de* $x = (a_\alpha)_{\alpha\in I}$.

La siguiente proposición nos da una propiedad fundamental que caracteriza al producto directo de una familia indizada de módulos. A la cual llamaremos **Propiedad universal del producto directo.**

Proposición 3.1.2. *Sea* $\{M_\alpha\}_{\alpha\in I}$ *una familia indizada de módulos. Sea* N *un módulo y* $\{f_\alpha\}_{\alpha\in I}$ *una familia de homomorfismos con* $f_\alpha : N \to M_\alpha$. *Entonces existe un único homomorfismo* $f : N \to \prod_I M_\alpha$ *tal que para cada* $\alpha \in I$ *el siguiente diagrama conmuta.*

$$\begin{tikzcd} N \arrow[r, "f"] \arrow[d, "f_\alpha"'] & \prod_I M_\alpha \arrow[dl, "\pi_\alpha"] \\ M_\alpha & \end{tikzcd}$$

Demostración. Para cada $x \in N$ definimos $f(x) \in \prod_I M_\alpha$ coordenada a coordenada por $\pi_\alpha f(x) = f_\alpha(x)$. Como π_α y f_α son homomorfismos se sigue que f es un homomorfismo. Más aún $\pi_\alpha f = f_\alpha$ para toda $\alpha \in I$.
Ahora supongamos que $g : N \to \prod_I M_\alpha$ es un homomorfismo tal que $\pi_\alpha g = f_\alpha$ para toda $\alpha \in I$. Entonces para cada $x \in N$ y cada $\alpha \in I$ tenemos que $\pi_\alpha g(x) = \pi_\alpha f(x)$ por lo que $f(x) = g(x)$. Por lo tanto $f = g$.

□

Al homomorfismo $f : N \to \prod_I M_\alpha$ de la proposición anterior algunas veces lo llamaremos el **producto directo de** $\{f_\alpha\}_{\alpha\in I}$ y lo denotaremos por $f = \prod_I f_\alpha$. Está caracterizado por ser el único homomorfismo tal que para cada $\alpha \in I$

$$\pi_\alpha(\prod_I f_\alpha) = \pi_\alpha f = f_\alpha.$$

Ejemplo 3.1.3. *Sea* $N = R$ *el* R*-módulo regular y* $\{M_\alpha\}_{\alpha\in I} = \{Rx_\alpha\}_{\alpha\in I}$ *con* $x_\alpha \in R$ *para cada* $\alpha \in I$ *una familia indizada de módulos. Sea* $\{f_\alpha\}_{\alpha\in I}$ *una familia de homomorfismos con* $f_\alpha : R \to Rx_\alpha$ *dado por* $f_\alpha(r) = rx_\alpha$ *para cada* $\alpha \in I$.
Definiendo $f : R \to \prod_I Rx_\alpha$ *como* $f(r) = r((x_{\alpha_i})_{\alpha_i\in I})$ *tenemos que el siguiente diagrama conmuta.*

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "f_\alpha"'] & \prod_I Rx_\alpha \arrow[dl, "\pi_\alpha"] \\ Rx_\alpha & \end{tikzcd}$$

Corolario 3.1.4. *Sea $\{f_\alpha\}_{\alpha\in I}$ una familia indizada de homomorfismos con $f_\alpha : N \to M_\alpha$ para cada $\alpha \in I$. Entonces $Ker(\prod_I f_\alpha) = \bigcap_I Ker f_\alpha$.*

Demostración. Sean $f = \prod_I f_\alpha$, y $x \in N$. Entonces $f(x) = 0$ si y sólo si para toda $\alpha \in I$ $\pi_\alpha f(x) = 0$ si y sólo si para toda $\alpha \in I$ $f_\alpha(x) = 0$. □

Si I es un conjunto de índices y $J \subseteq I$, entonces tenemos dos productos directos $\prod_J M_\beta$ y $\prod_I M_\alpha$. Si $x \in \prod_J M_\beta$, entonces x es una función con dominio J y tiene una única extensión a un elemento $y \in \prod_I M_\alpha$ donde $y(\alpha) = 0$ para toda $\alpha \notin J$. Entonces hay una función $i_J : \prod_J M_\beta \to \prod_I M_\alpha$ dada por $i_J(x) = y$. Claramente i_J es un monomorfismo cuya imagen es el submódulo de $\prod_I M_\alpha$ que consiste de todas aquellas I-tuplas que se anulan en $I - J$.
Por otra parte, para cada $x \in \prod_I M_\alpha$, la restricción $x|_J$ es un elemento de $\prod_J M_\beta$. Notemos además que la función $\pi_J : \prod_I M_\alpha \to \prod_J M_\beta$ dada por $\pi_J(x) = x|_J$ es un homomorfismo de $\prod_I M_\alpha$ a $\prod_J M_\beta$. La siguiente proposición muestra algunas propiedades interesantes del monomorfismo i_J. Omitimos su demostración.

Proposición 3.1.5. *Sea $\{M_\alpha\}_{\alpha\in I}$ una familia indizada de módulos y sea I la unión disjunta de J y K. Entonces.*

(1) $\pi_J i_J = 1_{\prod_J M_\beta}$.

(2) $\prod_I M_\alpha = i_J(\prod_J M_\beta) \oplus i_K(\prod_K M_\gamma)$.

(3) La sucesión exacta corta $0 \longrightarrow \prod_J M_\beta \xrightarrow{i_J} \prod_I M_\alpha \xrightarrow{\pi_K} \prod_K M_\gamma \longrightarrow 0$ *se escinde.*

□

Si $\beta \in I$, solemos identificar $\prod_{\{\beta\}} M_\beta$ con M_β y $\pi_{\{\beta\}}$ con π_β. El monomorfismo $i_\beta : M_\beta \to \prod_I M_\alpha$ esta caracterizado por $\pi_\alpha i_\beta = \delta_{\alpha\beta} 1_{M_\beta}$ para toda $\alpha \in I$.

La proposición 3.1.2 motiva la siguiente definición.

Definición 3.1.6. *A un par $(M, \{p_\alpha\}_{\alpha\in I})$ que consta de un módulo M y una familia de homomorfismos $p_\alpha : M \to M_\alpha$ para toda $\alpha \in I$ lo llamaremos **producto directo** de la familia de R-módulos $\{M_\alpha\}_{\alpha\in I}$, en caso de que para cada módulo N y cada familia de homomorfismos $\{f_\alpha\}_{\alpha\in I}$ con $f_\alpha : N \to M_\alpha$ exista un único homomorfismo $f : N \to M$ tal que $f_\alpha = p_\alpha f$ para toda $\alpha \in I$.*

El siguiente teorema nos dice que el producto directo es único salvo isomorfismos.

Teorema 3.1.7. *Sea* $(M, \{p_\alpha\}_{\alpha\in I})$ *un producto directo de la familia de R-módulos* $(M_\alpha)_{\alpha\in I}$*. Entonces un par* $(M', \{p'_\alpha\}_{\alpha\in I})$*, donde* M' *es un R-módulo y cada* $p'_\alpha : M' \to M_\alpha$ *es un R-homomorfismo para cada* $\alpha \in I$*, es también un producto de* $(M, \{p_\alpha\}_{\alpha\in I})$ *si y solo si existe un único isomorfismo* $p : M' \to M$ *tal que* $p_\alpha p = p'_\alpha$ *para cada* $\alpha \in I$

Demostración. Como $(M, \{p_\alpha\}_{\alpha\in I})$ es un producto directo de la familia $\{M_\alpha\}_{\alpha\in I}$, existe un único homomorfismo $p : M' \to M$ tal que $p_\alpha p = p'_\alpha$ para cada $\alpha \in I$. Si el par $(M', \{p'_\alpha\}_{\alpha\in I})$ también es un producto para la familia $\{M_\alpha\}_{\alpha\in I}$, entonces existe un único homomorfismo $p' : M \to M'$ tal que $p'_\alpha p = p_\alpha$ para cada $\alpha \in I$. Entonces $p'_\alpha = p_\alpha p = p'_\alpha p' p$. Pero $p'_\alpha = p'_\alpha 1_{M'}$ y por la unicidad de p y p' tenemos que $p'p = 1_{M'}$. Análogamente $pp' = 1_M$ y por la Proposición (1.5.12) p es un isomorfismo.
Ahora sea N un R-módulo y supongamos que $f_\alpha : N \to M_\alpha$ es un R-homomorfismo para cada $\alpha \in I$. Como $(M, \{p_\alpha\}_{\alpha\in I})$ es un producto directo de la familia $\{M_\alpha\}_{\alpha\in I}$, existe un único homomorfismo $h : N \to M$ tal que $f_\alpha = p_\alpha h$ para cada $\alpha \in I$. Si $p : M' \to M$ es un isomorfismo tal que $p_\alpha p = p'_\alpha$, entonces en particular p es un isomorfismo por lo que existe su inverso $p^{-1} : M \to M'$. Haciendo $f = p^{-1}h$ tenemos que $(M', \{p'_\alpha\}_{\alpha\in I})$ es un producto de la familia $\{M_\alpha\}_{\alpha\in I}$ ya que $p'_\alpha f = p'_\alpha p^{-1} h = p_\alpha h = f_\alpha$. □

Ejemplos 3.1.8. *Consideremos los siguientes ejemplos de producto directo.*

1. *Dada una familia de R-módulos* $\{M_\alpha\}_{\alpha\in I}$*,* $(\prod_I M_\alpha, \{\pi_\alpha\}_{\alpha\in I})$ *es un producto directo de la familia* $\{M_\alpha\}_{\alpha\in I}$*.*

2. *Consideremos al grupo abeliano* $\mathbb{Z}_{30}$*. Las clases residuales módulo 2, 3 y 5 respectivamente dan homomorfismos* $p_2 : \mathbb{Z}_{30} \to \mathbb{Z}_2$*,* $p_3 : \mathbb{Z}_{30} \to \mathbb{Z}_3$*,* $p_5 : \mathbb{Z}_{30} \to \mathbb{Z}_5$*. Entonces por la Proposición (3.1.2) existe un único homomorfismo* $p : \mathbb{Z}_{30} \to \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ *tal que* $p_\alpha = \pi_\alpha p$ *con* $\alpha = 2, 3, 5$*, donde* $\pi_\alpha : \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \to \mathbb{Z}_\alpha$ *es la* α*-ésima proyección del producto. Por el Corolario (3.1.4)* $Kerp = Kerp_2 \cap Kerp_3 \cap Kerp_5 = 0$*. Entonces* p *es un monomorfismo y como* $\mathbb{Z}_{30}$ *y* $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ *tienen la misma cardinalidad finita,* p *es un homomorfismo suprayectivo y por la Proposición (1.5.11)* p *es epimorfismo y por lo tanto* p *es un isomorfismo. Del Teorema (3.1.7) tenemos que* $(\mathbb{Z}_{30}, (p_2, p_3, p_5))$ *es un producto de* $\{\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5\}$*, aunque claramente* $\mathbb{Z}_{30}$ *y el producto cartesiano* $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ *son conjuntos diferentes.*

3.2. Coproducto.

En esta sección daremos el concepto dual del producto directo, para el cual simplemente invertiremos las flechas en la definición de producto.

Definición 3.2.1. *A un par $(M, \{j_\alpha\}_{\alpha\in I})$ que consiste de un módulo M y una familia de homomorfismos $\{j_\alpha\}_{\alpha\in I}$ con $j_\alpha : M_\alpha \to M$ para cada $\alpha \in I$ lo llamaremos* ***suma directa*** *o* ***coproducto*** *de la familia de R-módulos $\{M_\alpha\}_{\alpha\in I}$ en caso de que para cada módulo N y cada familia de homomorfismos $\{f_\alpha\}_{\alpha\in I}$ con $f_\alpha : M_\alpha \to N$ exista un único homomorfismo $f : M \to N$ tal que $f_\alpha = fj_\alpha$ para toda $\alpha \in I$.*

Ejemplo 3.2.2. *Sean $M = \mathbb{Z} \times \mathbb{Z}$, $M_\alpha = \mathbb{Z}$ para $\alpha = 1, 2$ y $N = \mathbb{Z}2$. Sean $j_\alpha = i_\alpha : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ con $\alpha = 1, 2$ los homomorfismos inclusión dados por $i_1(z) = (z, 0)$, $i_2(z) = (0, z)$ y $f_\alpha : \mathbb{Z} \to \mathbb{Z}2$ la familia de homomorfismos dados por $f_\alpha(z) = z2$. Definiendo a $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}2$ como $f(z_1, z_2) = (z_1 + z_2)2$ tenemos que $f_\alpha = fj_\alpha$.*

El siguiente teorema establece que si existe la suma directa entonces ésta es única, salvo isomorfismo.

Teorema 3.2.3. *Sea $(M, \{j_\alpha\}_{\alpha\in I})$ un coproducto de la familia de R-módulos $\{M_\alpha\}_{\alpha\in I}$. Entonces un par $(M', \{j'_\alpha\}_{\alpha\in I})$, donde M' es un R-módulo y $j'_\alpha : M_\alpha \to M'$ es un R-homomorfismo para cada $\alpha \in I$, es también un coproducto de la familia $\{M_\alpha\}_{\alpha\in I}$ si, y sólo, si existe un único isomorfismo $j : M \to M'$ tal que $jj_\alpha = j'_\alpha$ para cada $\alpha \in I$.*

Demostración. Como $(M, \{j_\alpha\}_{\alpha\in I})$ es un coproducto de la familia $\{M_\alpha\}_{\alpha\in I}$, existe un único homomorfismo $j : M \to M'$ tal que $j'_\alpha = jj_\alpha$ para cada $\alpha \in I$. Si el par $(M', \{j'_\alpha\}_{\alpha\in I})$ es también un coproducto para la familia $\{M_\alpha\}_{\alpha\in I}$ entonces existe un único homomorfismo $j' : M' \to M$ tal que $j'j'_\alpha = j_\alpha$ para cada $\alpha \in I$. Entonces $j'_\alpha = jj_\alpha = jj'j'_\alpha$. Pero $j'_\alpha = 1_M j'_\alpha$ de donde $jj'j'_\alpha = 1_M j'_\alpha$ y por la unicidad de j y j' tenemos que $jj' = 1_{M'}$. Análogamente $j'j = 1_M$ y de la Proposición (1.5.12) j es un isomorfismo.
Ahora sea N un R-módulo y supongamos que $f_\alpha : M_\alpha \to N$ es un R-homomorfismo para cada $\alpha \in I$. Como $(M, \{j_\alpha\}_{\alpha\in I})$ es un coproducto de la familia $\{M_\alpha\}_{\alpha\in I}$, existe un único R-homomorfismo $h : M \to N$ tal que si $f_\alpha = hj_\alpha$ para cada $\alpha \in I$. Si $j : M \to M'$ es un isomorfismo tal que $jj_\alpha = j'_\alpha$, entonces en particular j es isomorfismo por lo existe su inverso $j^{-1} : M' \to M$. Haciendo $f = hj^{-1}$tenemos que $(M', \{j'_\alpha\}_{\alpha\in I})$ es un coproducto de la familia $\{M_\alpha\}_{\alpha\in I}$ ya que $fj'_\alpha = hj^{-1}j'_\alpha = hj_\alpha = f_\alpha$. □

3.3. Suma directa externa.

En la sección anterior estudiamos la suma directa o coproducto $(M, \{j_\alpha\}_{\alpha\in I})$ de la familia de R-módulos $\{M_\alpha\}_{\alpha\in I}$ y vimos que si ésta existe, entonces es única salvo isomorfismo. En esta sección describiremos explícitamente al módulo M. Para ello, empezaremos dando la siguiente definición.

Decimos que un elemento $x \in \prod_I M_\alpha$ **es cero para casi toda** $\alpha \in I$ si tiene soporte finito. Es decir, si el conjunto $S(x) = \{\alpha \in I : \ x_\alpha = \pi_\alpha(x) \neq 0\}$

es finito. Si además $y \in \prod\limits_I M_\alpha$ y $r \in R$ tenemos que $S(x+y) \subseteq S(x) \cup S(y)$ y $S(rx) \subseteq S(x)$. De donde $\bigoplus\limits_I M_\alpha = \{x \in \prod\limits_I M_\alpha : \ x \ tiene \ soporte \ finito\}$ es un submódulo de $\prod\limits_I M_\alpha$. Abusando del lenguaje (ver la Proposición (3.3.1)) decimos que el submódulo $\bigoplus\limits_I M_\alpha$ es la **suma directa externa** de la familia de R-módulos $\{M_\alpha\}_{\alpha \in I}$.
Cuando I es finito denotaremos a la suma directa externa por $\bigoplus_{i=1}^n M_i$. Notemos que si I es finito, entonces la suma directa externa es de hecho el producto directo. Más aún si $M_\alpha = M$ para cada $\alpha \in I$, entonces $M^{(I)} = \bigoplus\limits_I M$ es la suma directa externa de I copias de M.

Más aún, para una familia indizada de R-módulos $\{M_\alpha\}_{\alpha \in I}$ y para cada $\alpha \in I$, la imagen $i_\alpha(M_\alpha)$ de la **α-ésima inclusión** $i_\alpha : M_\alpha \to \oplus_I M_\alpha$ dada por $i_\alpha(x_\alpha) = (\delta_{\beta,\alpha} x_\alpha)_{\beta \in I}$ es el conjunto de $x \in \prod\limits_I M_\alpha$ tal que $S(x) \subseteq \{\alpha\}$. Más aún, para todo $x \in \prod\limits_I M_\alpha$ se tiene que x tiene soporte finito si, y sólo si es una suma finita de elementos, cuyo soporte es a lo más un conjunto con un sólo elemento (un singular). Así $\bigoplus\limits_I M_\alpha$ es el submódulo de $\prod\limits_I M_\alpha$ generado por los submódulos $\{i_\alpha(M_\alpha)\}_{\alpha \in I}$. Además cada α-ésima inclusión $i_\alpha : M_\alpha \to \oplus_I M_\alpha$ es un monomorfismo y cada α-ésima proyección $\pi_\alpha : \oplus_I M_\alpha \to M_\alpha$ es un epimorfismo.

Proposición 3.3.1. *Sean $\{M_\alpha\}_{\alpha \in I}$ una familia de módulos, N un módulo y $\{f_\alpha\}_{\alpha \in I}$ una familia indexada de homomorfismos $f_\alpha : M_\alpha \to N$ para cada $\alpha \in I$. Entonces existe un único homomorfismo $f : \oplus_I M_\alpha \to N$ tal que $f i_\alpha = f_\alpha$ para cada $\alpha \in I$. Así $(\oplus_I M_\alpha, \{i_\alpha\}_{\alpha \in I})$ es la suma directa de $\{M_\alpha\}_{\alpha \in I}$.*

Demostración. Para cada $x \in \bigoplus\limits_I M_\alpha$ tenemos que el soporte de x es $S(x) = \{\alpha \in I : \ \pi_\alpha(x) = 0\}$ es finito, entonces hay una función $f : \bigoplus\limits_I M_\alpha \to N$ definida por $f(x) = \sum\limits_{\alpha \in S(x)} f_\alpha \pi_\alpha(x)$ donde $f(x) = 0$ si $S(x) = \emptyset$. Es fácil verificar que f es un homomorfismo ya que i_α y π_α son homomorfismos. Además es claro que para cada $\alpha \in I$, $f i_\alpha = f_\alpha$. Ahora supongamos que $g : \oplus_I M_\alpha \to N$ es un homomorfismo tal que $g i_\alpha = f_\alpha$, entonces $g i_\alpha(x) = f i_\alpha(x)$ para cada $x \in M_\alpha$ y para cada $\alpha \in I$, por la Proposición (1.5.7) tenemos que $f = g$. Por lo tanto el homomorfismo f es único. $\square$

Al homomorfismo f lo llamaremos **la suma directa** de $\{f_\alpha\}_{\alpha \in I}$ y escribiremos $f = \bigoplus\limits_I f_\alpha$.

Además observemos que para cada $x = (x_\alpha)_{\alpha \in I} \in \bigoplus\limits_I M_\alpha$ tenemos que $f(x) = \sum\limits_I f_\alpha(x_\alpha)$. Como $fi_\alpha = f_\alpha$ es claro que $Imf_\alpha \leq Imf$. Por lo tanto la demostración de la siguiente proposición es inmediata a partir de la definición de f.

Proposición 3.3.2. *Sean N un módulo y $\{M_\alpha\}_{\alpha \in I}$ una familia indizada de módulos. Si $f = \bigoplus\limits_I f_\alpha$ es la suma directa de los homomorfismos $f_\alpha : M_\alpha \to N$, entonces $Imf = \sum\limits_I Imf_\alpha$.*

□

Retomemos el ejemplo de la sección anterior.

Ejemplo 3.3.3. *Sean $M = \mathbb{Z} \times \mathbb{Z}$, $M_1 = \mathbb{Z}$, $M_2 = \mathbb{Z}$, $N = \mathbb{Z}2$*

Sea I un conjunto de índices y $J \subseteq I$. Es fácil verificar que la restricción del monomorfismo $i_J : \oplus_J M_\beta \to \oplus_I M_\alpha$ es un homomorfismo en la suma directa $\bigoplus\limits_I M_\alpha$. Similarmente, la restricción $\pi_J : \oplus_I M_\alpha \to \oplus_J M_\beta$ es un epimorfismo.

Concluímos esta sección con la siguiente proposición, la cual establece algunas propiedades de los homomorfismos inclusión y proyección. Omitimos su demostración.

Proposición 3.3.4. *Sea $\{M_\alpha\}_{\alpha \in I}$ una familia indizada de módulos e I la unión disjunta de J y K. Entonces:*

(1) $\pi_J i_J = 1_{\prod\limits_J M_\beta}$.

(2) $\oplus_I M_\alpha = i_J(\oplus_J M_\beta) \oplus i_K(\oplus_K M_\gamma)$.

(3) La sucesión $0 \longrightarrow \oplus_J M_\beta \xrightarrow{i_J} \oplus_I M_\alpha \xrightarrow{\pi_K} \oplus_K M_\gamma \longrightarrow 0$ *es exacta corta.*

□

3.4. Suma directa interna.

En el capítulo anterior vimos que dados dos submódulos M_1, M_2 de un módulo M, si éstos generaban a M y eran independientes entonces M era la suma directa interna de M_1 y M_2. Usando los resultados establecidos en la sección anterior, tenemos que si M_1 y M_2 son submódulos de un módulo M e $i_1 : M_1 \to M$, $i_2 : M_2 \to M$ son las inclusiones de M_1, M_2 en M respectivamente, entonces M es la suma directa interna de M_1 y M_2 si y sólo si $i_1 \oplus i_2$ es un isomorfismo.

En esta sección abordaremos la noción de suma directa interna para una familia indizada $\{M_\alpha\}_{\alpha\in I}$ de submódulos de un módulo M y relacionaremos dicho concepto con el de suma directa externa.

Supongamos que $\{M_\alpha\}_{\alpha\in I}$ es una familia indexada de subódulos de un módulo M. Sea $i_\alpha : M_\alpha \to M$ la inclusión de M_α en M para cada $\alpha \in I$. Decimos que M es la **suma directa interna** de sus submódulos $\{M_\alpha\}_{\alpha\in I}$ si el homomorfismo $i = \underset{I}{\oplus} i_\alpha : \bigoplus\limits_I M_\alpha \to M$ es un isomorfismo. Además se puede ver fácilmente que i es un isomorfismo si y sólo si cada $x \in M$ tiene una única representación como suma de elementos x_α con $x_\alpha \in M_\alpha$, para cada $\alpha \in I$, donde $x_\alpha = 0$ para casi toda $\alpha \in I$, esto es $x = \sum_I x_\alpha$.
Con esta notación de suma y dado que i es un R-homomorfismo tenemos que $\sum_I x_\alpha + \sum_I y_\alpha = \sum_I (x_\alpha + y_\alpha)$ y $r(\sum_I x_\alpha) = \sum_I rx_\alpha$ para cada $r \in R$.
Además si $f : M \to N$ es un R-homomorfismo, entonces como cada elemento $x \in M$ es una suma finita en M ($x = \sum_I x_\alpha$), tenemos que $f(\sum_I x_\alpha) = \sum_I f(x_\alpha)$.
En otras palabras, si M es la suma directa interna de una familia indizada de sus submódulos $\{M_\alpha\}_{\alpha\in I}$, entonces podemos estudiar a M coordenada a coordenada.
Sea $\{M_\alpha\}_{\alpha\in I}$ una familia indizada de submódulos de M con la familia de homomorfismos inclusión $\{i_\alpha\}_{\alpha\in I}$. Entonces debido a la Proposición (3.3.2) tenemos que

$$Im(\underset{I}{\oplus} i_\alpha) = \sum_I Im i_\alpha = \sum_I M_\alpha.$$

Si la suma directa de las inclusiones $i = \underset{I}{\oplus} i_\alpha$ es un monomorfismo, entonces el submódulo $\sum\limits_I M_\alpha$ es una suma directa interna de sus submódulos $\{M_\alpha\}_{\alpha\in I}$.

La siguiente definición generaliza el concepto de independencia de dos submódulos de un módulo M para una familia arbitraria de submódulos.

Definición 3.4.1. *Sea $\{M_\alpha\}_{\alpha\in I}$ una familia indizada de submódulos de un módulo M. Decimos que la familia $\{M_\alpha\}_{\alpha\in I}$ es **independiente** si para cada $\alpha \in I$*

$$M_\alpha \cap (\sum_{\beta\neq\alpha} M_\beta) = 0$$

Notemos que la familia $\{M_\alpha\}_{\alpha\in I}$ puede ser independiente a pares sin ser independiente.

Proposición 3.4.2. *Sea $\{M_\alpha\}_{\alpha\in I}$ una familia indizada de submódulos de un módulo M con la familia de homomorfismos inclusión $\{i_\alpha\}_{\alpha\in I}$. Entonces los siguientes enunciados son equivalentes:*

(a) $\sum\limits_I M_\alpha$ *es la suma directa interna de* $\{M_\alpha\}_{\alpha\in I}$.

(b) $i = \underset{I}{\oplus} i_\alpha : \bigoplus\limits_I M_\alpha \to M$ *es monomorfismo.*

(c) *$\{M_\alpha\}_{\alpha\in I}$ es independiente.*

(d) *$\{M_\alpha\}_{\alpha\in F}$ es independiente para cada subconjunto finito $F \subseteq I$.*

(e) *Para cada par J, K subconjuntos de I, si $J \cap K = \emptyset$, entonces $(\sum\limits_J M_\beta) \cap (\sum\limits_K M_\gamma) = 0$.*

Demostración. Veamos que (a) implica (b). Como $\sum\limits_I M_\alpha$ es la suma directa interna de $\{M_\alpha\}_{\alpha\in I}$ el homomorfismo $i = \bigoplus\limits_I i_\alpha$ es un isomorfismo, en particular es un monomorfismo.
Veamos que (b) implica (c). Definimos $J = \{\alpha\}$ y $K = \{\beta \in I : \beta \neq \alpha\}$. Claramente I es la unión disjunta de J y K y debido a la Proposición (3.3.4) tenemos que $\bigoplus\limits_I M_\alpha = i_J(M_\alpha) \oplus i_K(\bigoplus\limits_K M_\beta)$.
De donde $0 = i_J(M_\alpha) \cap i_K(\bigoplus\limits_K M_\beta) = i_J(M_\alpha) \cap i_K(\sum\limits_K M_\beta) = M_\alpha \cap (\sum\limits_{\beta\neq\alpha} M_\beta)$.
Por lo tanto la familia de submódulos $\{M_\alpha\}_{\alpha\in I}$ es independiente.
Veamos que (c) implica (d). Esta implicación es clara ya que si $\{M_\alpha\}_{\alpha\in I}$ es independiente es particular lo es para cada subconjunto finito $F \subseteq I$.
Veamos que (d) implica (e). Sean J y K subconjuntos de I tales que $J \cap K = \emptyset$. Si $x \in (\sum\limits_J M_\beta) \cap (\sum\limits_K M_\gamma)$, entonces $x = \sum\limits_J x_\beta = \sum\limits_K x_\gamma$, esto implica que $\sum\limits_J x_\beta - \sum\limits_K x_\gamma = 0$ por lo que para cada $\beta \in J$ $x_\beta = x_\gamma$ para algún $\gamma \in K$. Y como $J \cap K = \emptyset$ se tiene que $x_\beta = 0$ para cada $\beta \in J$ de donde $x = 0$. Por lo tanto $(\sum\limits_J M_\beta) \cap (\sum\limits_K M_\gamma) = 0$
Finalmente veamos que (e) implica (a). Supongamos que el homomorfismo $i = \bigoplus\limits_I i_\alpha$ no es monomorfismo, entonces $i((x_\alpha)_{\alpha\in I}) = i((y_\alpha)_{\alpha\in I})$ con $(x_\alpha)_{\alpha\in I} \neq (y_\alpha)_{\alpha\in I}$ por lo que existe $\alpha \in I$ tal que $0 \neq i_\alpha(x_\alpha) = i_\beta(y_\beta)$ para algún $\beta \neq \alpha$. Sea $J = \{\alpha\}$ y $K = \{\beta\}$. Entonces J y K son subconjuntos de I tales que $J \cap K = \emptyset$ y por hipótesis tenemos que $\sum\limits_J M_\alpha \cap \sum\limits_K M_\beta = M_\alpha \cap M_\beta = 0$. Pero $0 \neq i_\alpha(x_\alpha) = i_\beta(y_\beta) \in Imi_\alpha \cap Imi_\beta = M_\alpha \cap M_\beta$ lo cual es contradicción pues $M_\alpha \cap M_\beta = 0$. Por lo tanto el homomorfismo i es un monomorfismo de donde $\sum\limits_I M_\alpha$ es la suma directa interna de $\{M_\alpha\}_{\alpha\in I}$. $\square$

Corolario 3.4.3. *Un módulo M es la suma directa interna de sus submódulos $\{M_\alpha\}_{\alpha\in I}$ si y sólo si la familia de submódulos $\{M_\alpha\}_{\alpha\in I}$ de M es independiente y genera a M.*

Demostración. Si M es la suma directa de sus submódulos $\{M_\alpha\}_{\alpha\in I}$, entonces el homomorfismo $i = \bigoplus\limits_I i_\alpha : \bigoplus\limits_I M_\alpha \to M$ es un isomorfismo, en particular es un monomorfismo y por la Proposición anterior tenemos que $\{M_\alpha\}_{\alpha\in I}$ es independiente. Y también por ser $i = \bigoplus\limits_I i_\alpha$ un isomorfismo tenemos que cada $x \in M$ tiene una única representación como suma $x = \sum\limits_I x_\alpha = \bigoplus\limits_I i_\alpha((x_\alpha)_{\alpha\in I})$

con $x_\alpha \in M_\alpha$. De donde $M = \sum\limits_I Imi_\alpha(M_\alpha) = \sum\limits_I M_\alpha$. Por lo tanto $\{M_\alpha\}_{\alpha\in I}$ genera a M.
Ahora supongamos que $\{M_\alpha\}_{\alpha\in I}$ es independiente y genera a M. Entonces de la Proposición anterior tenemos que $i = \bigoplus\limits_I i_\alpha$ es un monomorfismo. Y como $(M_\alpha)_{\alpha\in I}$ genera, tenemos que $M = \sum\limits_I M_\alpha$. De donde para cada $m \in M$ $m = \sum\limits_I x_\alpha = \bigoplus\limits_I i_\alpha((x_\alpha)_{\alpha\in I}$ para algunas $x_\alpha \in M_\alpha$. Por lo tanto el homomorfismo $i = \bigoplus\limits_I i_\alpha$ es epimorfismo. Así el homomorfismo $i = \bigoplus\limits_I i_\alpha$ es isomorfismo y por lo tanto M es la suma directa interna de sus submódulos $\{M_\alpha\}_{\alpha\in I}$. □

Si los submódulos $\{M_\alpha\}_{\alpha\in I}$ de un módulo M son independientes, decimos que **la suma** $\sum\limits_I M_\alpha$ **es directa** y escribimos $\sum\limits_I M_\alpha = \bigoplus\limits_I M_\alpha$, algunas veces también nos referiremos a esto como una descomposición directa de $\sum\limits_I M_\alpha$.
Notemos que la suma directa externa de $\{M_\alpha\}_{\alpha\in I}$ es la suma directa interna de las imagenes $(i_\alpha(M_\alpha))_{\alpha\in I}$ pero no es la suma directa interna de $\{M_\alpha\}_{\alpha\in I}$. Así la notación $\oplus$ tiene dos usos relacionados.

Proposición 3.4.4. *Sea $\{M_1, M_2, ..., M_n\}$ una sucesión finita de módulos. Entonces $M_1 \times M_2 \times \cdots \times M_n = M_1 \dot{\oplus} M_2 \dot{\oplus} \cdots \dot{\oplus} M_n = i_1(M_1) \oplus i_2(M_2) \oplus \cdots \oplus i_n(M_n)$.*

□

Ejemplos 3.4.5.

1. *Consideremos un espacio vectorial V sobre un campo K, y sea $\{x_\alpha\}_{\alpha\in I}$ un conjunto indexado en V. Entonces $\{x_\alpha\}_{\alpha\in I}$ genera a V si y sólo si $V = \sum\limits_I Kx_\alpha$. Por otro lado, $\{x_\alpha\}_{\alpha\in I}$ es un conjunto linealmente independiente de vectores si, y sólo si, el conjunto indexado $\{Kx_\alpha\}_{\alpha\in I}$ de submódulos cíclicos de V es independiente. Así pues, V es la suma directa interna de $\{Kx_\alpha\}_{\alpha\in I}$, esto es, $V = \sum\limits_I Kx_\alpha = \bigoplus\limits_I Kx_\alpha$ si, y sólo si, $\{x_\alpha\}_{\alpha\in I}$ es una base de V.*

2. *Consideremos al grupo abeliano $\mathbb{Z}_{30}$ y a sus subgrupos $15\mathbb{Z}_{30}$, $10\mathbb{Z}_{30}$, $6\mathbb{Z}_{30}$ y sean i_1, i_2, i_3 los correspondientes homomorfismos inclusión. Entonces por la Proposición (3.3.1) la suma directa $i = i_1 \oplus i_2 \oplus i_3$ es un homomorfismo $i : (15\mathbb{Z}_{30}) \oplus (10\mathbb{Z}_{30}) \oplus (6\mathbb{Z}_{30}) \to \mathbb{Z}_{30}$.*
Además $Imi = 15\mathbb{Z}_{30} + 10\mathbb{Z}_{30} + 6\mathbb{Z}_{30} = \mathbb{Z}_{30}$ por lo que el homomorfismo i es epimorfismo. Y como además la cardinalidad de $15\mathbb{Z}_{30} \times 6\mathbb{Z}_{30} \times 10\mathbb{Z}_{30}$ es igual a la cardinalidad de $\mathbb{Z}_{30}$ se sigue que el homomorfismo i es un isomorfismo. Por lo tanto $\mathbb{Z}_{30}$ es la suma directa interna de sus submódulos $\{15\mathbb{Z}_{30}, 10\mathbb{Z}_{30}, 6\mathbb{Z}_{30}\}$.
Notemos que estos submódulos son isomorfos a $\mathbb{Z}_2$, $\mathbb{Z}_3$ y $\mathbb{Z}_5$ respectivamente. De donde

$$\mathbb{Z}_{30} = (15\mathbb{Z}_{30}) \oplus (10\mathbb{Z}_{30}) \oplus (6\mathbb{Z}_{30}) \cong \mathbb{Z}_2 \dot{\oplus} \mathbb{Z}_3 \dot{\oplus} \mathbb{Z}_5 = \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5.$$

3. *Consideremos al siguiente carcaj* [1]

$$Q = \begin{tikzcd} \underset{1}{\circ} \arrow[r, "\alpha"] & \underset{2}{\circ} \arrow[r, "\beta"] & \underset{3}{\circ} \arrow[loop right, "\gamma"] \end{tikzcd}$$

   Consideremos el ideal $I = \langle \gamma^3 \rangle$ del álgebra de caminos [2] *KQ y consideremos el álgebra cociente $A = KQ/I$. Tenemos que ${}_AA = Ae_1 \oplus Ae_2 \oplus Ae_3$.*

4. *Consideremos a $\mathcal{P}(x) = \{a_0 + a_1x + \cdots + a_nx_n : \ n \in \mathbb{N}, a_i \in \mathbb{C}\}$, el conjunto de los polinomios en la indeterminada x con coeficientes en $\mathbb{C}$, como $\mathbb{C}$-módulo. Sabemos que $\mathcal{B} = \{1, x, x^2, ...\}$ es una base de $\mathcal{P}(x)$. Entonces*

$$\mathcal{P}(x) = \bigoplus_{\mathbb{N}} \mathbb{C}x^i.$$

3.5. Propiedades de independencia.

Además de las propiedades de independencia tratadas en la Proposición (3.4.2) hay otras tres propiedades de independencia que tienen una gran importancia. La primera es una generalización que conocimos en álgebra lineal la cual nos dice que en espacio vectorial un conjunto ordenado de vectores es independiente si y sólo si ninguno de los vectores depende de su predecesor.

Proposición 3.5.1. *Una sucesión $M_1, M_2, ...$ de submódulos de un módulo M es independiente si y sólo si para cada $n \geq 1$*

$$(M_1 + M_2 + \cdots + M_n) \cap M_{n+1} = 0.$$

Demostración. Si la sucesión de submódulos $M_1, M_2, ...$ es independiente tenemos que $M_i \cap (\sum\limits_{j \neq i} M_j) = 0$ para toda $i, j \neq i \in \mathbb{N}$. En particular tenemos que $(M_1 + M_2 + \cdots + M_n) \cap M_{n+1} = 0$ para toda $n \geq 1$.
Ahora supongamos que $(M_1 + M_2 + \cdots + M_n) \cap M_{n+1} = 0$ para toda $n \geq 1$.
Sea $x \in M_i \cap (\sum\limits_{j \neq i} M_j)$ con $i, j \in \mathbb{N}$. Entonces $x \in M_i$ y $x \in \sum\limits_{j \neq i} M_j$ por lo que $x \in M_i$ y $x = m_1 + m_2 + \cdots + m_n$ donde $m_l \in M_l$ con $l \neq i$.
Si $i > n$, entonces $(M_1 + M_2 + \cdots + M_{i-1}) \cap M_i = 0$ y como $x \in (M_1 + M_2 + \cdots + M_{i-1}) = 0$ se tiene que $x = 0$.
Si $i \leq n$. Como $x \in M_i \cap \sum\limits_{j \neq i} M_j)$ tenemos que $x \in M_i$ y $x \in M_1 + M_2 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_n$, entonces $x = m_1 + m_2 + \cdots + m_{i-1} + 0 + m_{i+1} + \cdots + m_n$ por lo que $0 = x - x = m_1 + m_2 + \cdots + m_{i-1} - x + m_{i+1} + \cdots + m_n$. De donde $m_n \in (M_1 + M_2 + \cdots + M_{n-1}) \cap M_n = 0$ por lo que $m_n = 0$.
Recursivamente se prueba que $x = 0$. Por lo tanto la sucesión de submódulos $M_1, M_2, ...$ es independiente. $\square$

[1] Para ver la definición de carcaj consultar la página 41 del libro [1]. Se puede encontrar mayor información acerca de álgebras y carcajes en los siguientes libros [1], [3].

[2] Ver definición en la páginas 43 del libro [1]

Proposición 3.5.2. *Sea $\{M_\beta\}_{\beta\in B}$ una familia de submódulos independientes de un módulo M. Para cada $\beta \in B$, sea $\{L_{\alpha_\beta}\}_{\alpha_\beta\in A_\beta}$ una familia de submódulos de M_β. Sea $A = \bigcup_B A_\beta$ la unión ajena de las A_β. Si $\{L_{\alpha_\beta}\}_{\alpha_\beta\in A_\beta}$ es independiente para cada $\beta \in B$, entonces $\{L_\alpha\}_{\alpha\in A}$ es independiente.*

Demostración. Sea $x \in L_\alpha \cap (\sum_{\gamma\neq\alpha} L_\gamma)$ con $\alpha, \gamma \in A$. Entonces $x \in L_\alpha$ y $x \in \sum_{i=1}^{n} L_i$ con $i \neq \alpha$ por lo que $0 = x - x = x_1 + x_2 + \cdots + x_m - x$. Sin perdida de generalidad podemos suponer que existe un $k \in \mathbb{N}$ y un $\beta \in B$ con $\alpha_1, \alpha_2, ..., \alpha_k \in A_\beta$ y $\alpha_{k+1}, ..., \alpha_n \notin A_\beta$. Como la familia $\{M_\beta\}_{\beta\in B}$ es independiente se tiene que $x_1 + x_2 + \cdots + x_k = 0 = x_{k+1} + \cdots + x_n$. Como también la familia $\{L_{\alpha_\beta}\}_{\alpha_\beta\in A_\beta}$ es independiente tenemos que $x_1 = x_2 = \cdots = x_k = 0$. Análogamente se puede ver que $x_{k+1} = \cdots = x_n = 0$. De donde $x = 0$ y por lo tanto la familia $\{L_\alpha\}_{\alpha\in A}$ es independiente. □

Corolario 3.5.3. *Sean $\{M_\beta\}_{\beta\in B}$ una familia de submódulos de un módulo M y para cada $\beta \in B$ $\{L_{\alpha_\beta}\}$ una familia de submódulos de M_β tales que $M = \sum_B M_\beta$ y $M_\beta = \sum_{A_\beta} L_{\alpha_\beta}$. Sea $A = \cup_B A_\beta$ la unión ajena de las A_β. Entonces $M = \oplus_A L_\alpha$ si y sólo si $M = \oplus_B M_\beta$ y $M_\beta = \oplus_{A_\beta} L_{\alpha_\beta}$ para toda $\beta \in B$.*

Demostración. Supongamos que $M = \oplus_A L_\alpha$. Como $M = \sum_B M_\beta$, para ver que $M = \oplus_B M_\beta$ basta probar que la familia de submódulos $\{M_\beta\}_{\beta\in B}$ es independiente. Para ello hay que probar que $M_\beta \cap (\sum_{\gamma\neq\beta} M_\gamma) = 0$. Notemos que como $M = \oplus_A L_\alpha$, entonces $M_\beta = \oplus_C L_\alpha = \sum_C L_\alpha$ para algún $C \subseteq A$, así mismo $\sum_{\gamma\neq\beta} M_\gamma = \oplus_{A-C} L_\alpha = \sum_{A-C} L_\alpha$. Entonces $M_\beta \cap (\sum_{\gamma\neq\beta} M_\gamma) = \sum_C L_\alpha \cap (\sum_{A-C} L_\alpha)$. Como además $C \cap (A - C) = \emptyset$ y la familia $\{L_\alpha\}_{\alpha\in A}$ es independiente, por la Proposición 3.4.2 tenemos que $M_\beta \cap (\sum_{\gamma\neq\beta} M_\gamma) = \sum_C L_\alpha \cap (\sum_{A-C} L_\alpha) = 0$.

Análogamente se prueba que la familia $\{L_{\alpha_\beta}\}_{\alpha_\beta\in A_\beta}$ es independiente para cada $\beta \in B$.

Ahora supongamos que $M = \oplus_B M_\beta$ y $M_\beta = \oplus_{A_\beta} L_{\alpha_\beta}$ para toda $\beta \in B$. Entonces por la Proposición (3.5.2) tenemos que la familia $\{L_\alpha\}_{\alpha\in A}$ es independiente. □

Proposición 3.5.4. *Supongamos que $\{L_\alpha\}_{\alpha\in A}$ es un conjunto de submódulos independientes de un módulo M. Si $\{M_\alpha\}_{\alpha\in A}$ es un conjunto de submódulos de M tales que $L_\alpha \trianglelefteq M\alpha$ para cada $\alpha \in A$, entonces:*

(1) $\{M_\alpha\}_{\alpha\in A}$ *es independiente.*

(2) $\oplus_A L_\alpha \trianglelefteq \oplus_A M_\alpha$.

Demostración. Supongamos que L_1 y L_2 son submódulos independientes de M con $L_1 \trianglelefteq M_1$ y $L_2 \trianglelefteq M_2$, entonces $(L_1 \cap M_2) \cap L_2 = L_1 \cap L_2 = 0$. Como $L_2 \trianglelefteq M_2$ tenemos que $L_1 \cap M_2 = 0$. Pero $(M_1 \cap M_2) \cap L_1 \leq L_1 \cap M_2 = 0$, y como $L_1 \trianglelefteq M_1$ tenemos que $M_1 \cap M_2 = 0$. Es decir, (M_1, M_2) es un conjunto independiente. Más aún por la Proposición (2.4.12) inciso (2) $K_1 \oplus K_2 \trianglelefteq M_1 \oplus M_2$.
Supongamos ahora que para algún $F = \{\alpha_1, \alpha_2, ..., \alpha_n\} \subseteq A$ $\{M_\alpha\}_{\alpha \in F}$ es independiente y $\bigoplus_F L_\alpha \trianglelefteq \bigoplus_F M_\alpha$. Entonces para cualquier $\alpha_{n+1} \in A - F$

$$(L_{n+1} \cap \sum_{i=1}^{n} M_{\alpha_i}) \cap \sum_{i=1}^{n} L_{\alpha_i} = L_{n+1} \cap \sum_{i=1}^{n} L_{\alpha_i} = 0$$

y como $\bigoplus_{i=1}^{n} L_{\alpha_i} \trianglelefteq \bigoplus_{i=1}^{n} M_{\alpha_i}$ tenemos que $L_{n+1} \cap \sum_{i=1}^{n} M_{\alpha_i} = 0$. De donde

$$(M_{\alpha_{n+1}} \cap \sum_{i=1}^{n} M_{\alpha_i}) \cap L_{n+1} \leq \sum_{i=1}^{n} M_{\alpha_i} \cap L_{n+1} = 0.$$

Finalmente como $L_{n+1} \trianglelefteq M_{\alpha_{n+1}}$ tenemos que $M_{\alpha_{n+1}} \cap \sum_{i=1}^{n} M_{\alpha_i} = 0$. Por lo tanto $\sum_{i=1}^{n+1} M_{\alpha_i} = \bigoplus_{i=1}^{n+1} M_{\alpha_i}$ y nuevamente por la Proposición (2.4.12) inciso (2) $\bigoplus_{i=1}^{n} L_{\alpha_i} \oplus L_{n+1} \trianglelefteq \bigoplus_{i=1}^{n} M_{\alpha_i} \oplus M_{\alpha_{n+1}}$.
Análogamente para cualquier subconjunto finito $F \subseteq A$. Y por la Proposición (3.4.2) inciso (d) el conjunto $\{M_\alpha\}_{\alpha \in A}$ es independiente. $\square$

3.6. Los idempotentes para una descomposición.

En esta sección estableceremos la relación que existe entre la suma directa interna $M = \bigoplus_I M_\alpha$ de una familia de submódulos $\{M_\alpha\}_{\alpha \in I}$ de un módulo M y un conjunto $\{e_\alpha\}_{\alpha \in I}$ de enfomorfsimos idempotentes de M. Es decir, mostraremos la siguiente proposición.

Proposición 3.6.1. *Sea $\{M_\alpha\}_{\alpha \in I}$ una familia de submódulos de un módulo M. Entonces $M = \bigoplus_I M_\alpha$ si, y sólo si existe un único conjunto indexado $\{e_\alpha\}_{\alpha \in I}$ de endomorfismos idempotentes de M tales que para toda $\alpha \in I$, $M_\alpha = Ime_\alpha$ y $\sum_{\beta \neq \alpha} M_\beta = Kere_\alpha$.*
Además, si tal endomorfismo idempotente de M existe, entonces e_α es el idempotente para M_α en la descomposición $M = \bigoplus_I M_\alpha$.

Demostración. Supongamos que M es la suma directa interna $M = \bigoplus_I M_\alpha$. Entonces para cada $\alpha \in I$, $M = M_\alpha \oplus (\sum_{\beta \neq \alpha} M_\beta)$, de donde por el Lema (2.3.1) y la Proposición (2.3.2) existe un único idempotente $e_\alpha \in End(M)$ con $M_\alpha = Ime_\alpha$

y $\sum\limits_{\beta\neq\alpha} M_\beta = Kere_\alpha$. De donde el conjunto indexado $\{e_\alpha\}_{\alpha\in I}$ de endomorfismos idempotentes de M es tal que para toda $\alpha \in I$, $M_\alpha = Ime_\alpha$ y $\sum\limits_{\beta\neq\alpha} M_\beta = Kere_\alpha$. Ahora supongamos que existe un conjunto indexado $\{e_\alpha\}_{\alpha\in I}$ de endomorfismos idempotentes de M tal que para toda $\alpha \in I$, $M_\alpha = Ime_\alpha$ y $\sum\limits_{\beta\neq\alpha} M_\beta = Kere_\alpha$. Entonces por el Lema (2.3.1) tenemos que $M = e_\alpha(M) \oplus (1 - e_\alpha)(M) = Ime_\alpha \oplus Kere_\alpha$ de donde $Ime_\alpha \cap Kere_\alpha = M_\alpha \cap \sum\limits_{\beta\neq\alpha} M_\beta = 0$ para cada $\alpha \in I$. Por lo tanto $\{M_\alpha\}_{\alpha\in I}$ es independiente. Así mismo, por el Lema (2.3.1) tenemos que $Ime_\alpha + Kere_\alpha = M$. Por lo tanto $\{M_\alpha\}_{\alpha\in I}$ genera a M. Finalmente la unicidad se sigue de la Proposición (2.3.2).

□

Llamamos a los idempotentes $\{e_\alpha\}_{\alpha\in I}$ **los idempotentes para la descomposición** de $M = \bigoplus\limits_I M_\alpha$, y para cada $\alpha \in I$, llamamos a e_α el idempotente para M_α es esta descomposición.

Para poder enunciar el Corolario (3.6.5) necesitamos la siguiente definición.

Definición 3.6.2. *Un conjunto de idempotentes $\{e_\alpha\}_{\alpha\in I}$ en un anillo R se dice **ortogonal** si es ortogonal por pares, es decir si para toda $\alpha, \beta \in I$ se tiene que $e_\alpha e_\beta = \delta_{\alpha,\beta} e_\alpha$.*

Ejemplo 3.6.3. *Consideremos el anillo $M_2(\mathbb{R})$ de las matrices de 2×2 con coeficientes en los reales . Entonces el conjunto de idempotentes*

$$B = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

de $M_2(\mathbb{R})$ no es ortogonal.

Más en general, se puede ver que la base canónica correspondiente al $\mathbb{R}$-espacio vectorial de las matrices cuadradas de $n\times n$ con entradas en $\mathbb{R}$ no es un conjunto de idempotentes ortogonales en el anillo $M_n(\mathbb{R})$ de las matrices de $n \times n$ con entradas en $\mathbb{R}$.

Ejemplo 3.6.4. *Consideremos el anillo $M_2(\mathbb{R})$ de las matrices de 2×2 con coeficientes en los reales. Entonces el conjunto*

$$B' = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

es un conjunto de idempotentes ortogonales.

Corolario 3.6.5. *Los idempotentes $\{e_\alpha\}_{\alpha\in I}$ para una descomposición $M = \bigoplus\limits_I M_\alpha$, son ortogonales. Además, si $x \in M$, entonces $e_\alpha(x) = 0$ para casi toda $\alpha \in I$ y $x = \sum\limits_I e_\alpha(x)$.*

Demostración. Si $\alpha \neq \beta \in I$, entonces $M_\beta \subseteq \sum_{\gamma \neq \alpha} M_\gamma = Ker e_\alpha$, por lo que $e_\alpha e_\beta(M) = e_\alpha(e_\beta(M)) = e_\alpha(M_\beta) = 0$.
Por otro lado, si $x \in M$, escribiendo $x = \sum_I x_\alpha$ con $x_\alpha \in M_\alpha = Im e_\alpha$ cero para casi toda $\alpha \in I$, tenemos que $e_\beta(x) = e_\beta(\sum_I x_\alpha) = x_\beta$ para toda $\beta \in I$. $\square$

Definición 3.6.6. *Un conjunto finito ortogonal de idempotentes $e_1, e_2, ..., e_n$ en un anillo R es* ***completo*** *si $e_1 + e_2 + \cdots + e_n = 1 \in R$.*

Ejemplo 3.6.7. *Nuevamente consideremos el anillo $M_2(\mathbb{R})$ de las matrices de 2×2 con coeficientes en los reales. Entonces el conjunto de idempotentes ortogonales*

$$B' = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

del anillo $M_2(\mathbb{R})$ es completo.

Ejemplo 3.6.8. *Consideremos un campo K y*

$$A = \begin{pmatrix} K & 0 & 0 \\ K & K & 0 \\ K & 0 & K \end{pmatrix}$$

el álgebra[3] *de matrices triangulares inferiores con coeficientes en K, $(\lambda_{ij}) \in \mathbb{M}_3(K)$, con $\lambda_{32} = 0$ y $\lambda_{pq} = 0$ si $p > q$. Si*

$$e_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, e_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

entonces $\{e_1, e_2, e_3\}$ es un conjunto completo de idempotentes ortogonales de A. Más aun, el A-módulo A es la suma directa interna de la familia de submódulos $\{Ae_1, Ae_2, Ae_3\}$. Esto es, $A = Ae_1 \oplus Ae_2 \oplus Ae_3$.

Para el siguiente corolario veremos que hay una correspondencia uno a uno entre la descomposición directa (finita) de un módulo M y el conjunto completo de idempotentes ortogonales en su anillo de endomorfismos.

Corolario 3.6.9. *Sean $M_1, M_2, ..., M_n$ submódulos de un módulo M. Entonces $M = M_1 \oplus M_2 \oplus \cdots \oplus M_n$ si y sólo si existe un único conjunto completo $e_1, e_2, ..., e_n$ de idempotentes ortogonales en el anillo $End(M)$, con $M_i = e_i(M)$ para $i = 1, 2, ..., n$.*

Demostración. Sean $e_1, e_2, ..., e_n$ idempotentes de una descomposición $M = M_1 \oplus M_2 \oplus \cdots \oplus M_n$. Entonces por el Corolario anterior son ortogonales y para toda $x \in M$ $x = \sum_{i=1}^{n} e_\alpha(x) = (e_1 + e_2 + \cdots + e_n)(x)$, de donde $e_1 + e_2 + \cdots + e_n = 1_M$.

[3] La definición de K-álgebra se puede consultar en la página 2 del libro [1]

Si $e_1, e_2, ..., e_n \in End(M)$ son idempotentes ortogonales tales que $M_i = e_i(M)$ para toda $i = 1, 2, ..., n$, entonces para cada $x \in M$ $x = (e_1 + e_2 + \cdots + e_n)(x) = e_1(x) + e_2(x) + \cdots + e_n(x)$. Notemos además que si $M_i = e_i(M)$, entonces $\sum\limits_{j \neq i} M_j = Kere_i$. Ya que como para cada $x \in M$ $x = (e_1 + e_2 + \cdots + e_n)(x)$, entonces $x - \sum\limits_{j \neq i} e_j(x) = e_i(x)$ de donde $x = \sum\limits_{j \neq i} e_j(x)$ si y sólo si $e_i(x) = 0$. Y de la Proposición (3.6.1) obtenemos que $M = M_1 \oplus M_2 \oplus \cdots \oplus M_n$. □

Ejemplo 3.6.10. *Consideremos el $\mathbb{Z}$-módulo $\mathbb{Z}_6$. Sabemos que $\mathbb{Z}_6$ es la suma directa interna de la familia de submódulos $\{2\mathbb{Z}_6, 3\mathbb{Z}_6\}$, esto es, $\mathbb{Z}_6 = 2\mathbb{Z}_6 \oplus 3\mathbb{Z}_6$. Denotando por M_1 a $2\mathbb{Z}_6$ y por M_2 a $3\mathbb{Z}_6$, tenemos que el idempotente $e_1 : \mathbb{Z}_6 \to \mathbb{Z}_6$ correspondiente al submódulo M_1 está dado por: $e_1(\bar{0}) = \bar{0}$, $e_1(\bar{1}) = \bar{4}$, $e_1(\bar{2}) = \bar{2}$, $e_1(\bar{3}) = \bar{0}$, $e_1(\bar{4}) = \bar{4}$, $e_1(\bar{5}) = \bar{2}$. De donde concluímos que $Ime_1 = 2\mathbb{Z}_6$ y $Kere_1 = 3\mathbb{Z}_6$. Análogamente tenemos que el idempotente $e_2 : \mathbb{Z}_6 \to \mathbb{Z}_6$ correspondiente al submódulo M_2 está dado por: $e_2(\bar{0}) = \bar{0}$, $e_2(\bar{1}) = \bar{3}$, $e_2(\bar{2}) = \bar{0}$, $e_2(\bar{3}) = \bar{3}$, $e_2(\bar{4}) = \bar{0}$, $e_2(\bar{5}) = \bar{3}$. De donde vemos que se verifica que $Ime_2 = 3\mathbb{Z}_6$ y $Kere_2 = 2\mathbb{Z}_6$. Más aun, $\{e_1, e_2\}$ es un conjunto completo de idempotentes ortogonales del anillo $End(\mathbb{Z}_6)$.*

3.7. Una caracterización de la sumas directas.

Terminamos este trabajo enunciando una caracterización de la suma directa interna de una familia indexada de submódulos de un módulo M.

Proposición 3.7.1. *Sean $\{M_\alpha\}_{\alpha \in I}$ una familia indexada de módulos y M un módulo. Para cada $\alpha \in I$ sea $j_\alpha : M_\alpha \to M$ un homomorfismo. Entonces $(M, \{j_\alpha\}_{\alpha \in I})$ es una suma directa de $\{M_\alpha\}_{\alpha \in I}$ si y sólo si para cada $\alpha \in I$ existe un único homomorfismo $q_\alpha : M \to M_\alpha$ que satisface que para cada $\alpha, \beta \in I$ y toda $x \in M$,*

(1) $q_\alpha j_\alpha = \delta_{\alpha\beta} 1_{M_\alpha}$,

(2) $q_\alpha(x) = 0$ *para casi toda* $\alpha \in I$,

(3) $\sum\limits_I j_\alpha q_\alpha(x) = x$.

Más aún, si $(M, \{j_\alpha\}_{\alpha \in I})$ es una suma directa de $\{M_\alpha\}_{\alpha \in I}$ y para un módulo N, $f_\alpha : M_\alpha \to N$ es un homomorfismo para cada $\alpha \in I$, entonces $f(x) = \sum\limits_I f_\alpha q_\alpha(x)$ para cada $x \in M$ es el único homomorfismo $f : M \to N$ tal que $f_\alpha = f j_\alpha$.

Demostración. Supongamos que $(M, \{j_\alpha\}_{\alpha \in I}$ es una suma directa de $\{M_\alpha\}_{\alpha \in I}$. Entonces por la Proposición (3.3.1) existe un único homomorfismo $j = \bigoplus\limits_I j_\alpha : \bigoplus\limits_I M_\alpha \to M$ tal que $j i_\alpha = j_\alpha$, con $i_\alpha : M_\alpha \to \bigoplus\limits_I M_\alpha$ el monomorfismo coordenado usual de la suma directa. De donde $(\bigoplus\limits_I M_\alpha, \{i_\alpha\}_{\alpha \in I})$ es también una suma directa de $\{M_\alpha\}_{\alpha \in I}$. Así por la Proposición (3.2.3) $j : \bigoplus\limits_I M_\alpha \to M$

es un isomorfismo. Consideremos ahora π_α la proyección usual de la suma directa externa $\bigoplus\limits_I M_\alpha$ y para cada $\alpha \in I$ sea $q_\alpha = \pi_\alpha j^{-1} : M \to M_\alpha$. Entonces $q_\alpha j_\alpha = \pi_\alpha j^{-1} j_\alpha = \pi_\alpha i_\alpha = 1_{M_\alpha}$. Es claro que $q_\alpha(x) = 0$ para casi toda $\alpha \in I$. Ahora veamos que $\sum\limits_I j_\alpha q_\alpha(x) = x$. En efecto, para cada $x \in M$
$x = jj^{-1}(x) = j(\sum\limits_I i_\alpha \pi_\alpha j^{-1}(x)) = \sum\limits_I j i_\alpha \pi_\alpha j^{-1}(x) = \sum\limits_I j_\alpha q_\alpha(x)$.
Por otro lado por la Proposición (3.3.2) $M = \sum\limits_I Im j_\alpha$ y como $q_\beta j_\alpha = \delta_{\alpha\beta} 1_{M_\alpha}$ concluimos que el homomorfismo q_α es único para cada $\alpha \in I$.
Supongamos ahora que existe un único homomorfismo $q_\alpha : M \to M_\alpha$ para cada $\alpha \in I$ que satisface las condiciones (1), (2), (3). Sean N un módulo y $f_\alpha : M_\alpha \to N$ un homomorfismo para cada $\alpha \in I$. Entonces definiendo $f(x) = \sum\limits_I f_\alpha q_\alpha(x)$ con $x \in M$ tenemos que para toda $\alpha \in I$ y $x_\alpha \in M_\alpha$, $f j_\alpha(x_\alpha) = \sum\limits_{\beta \in I} f_\beta q_{beta}(j_\alpha(x_\alpha)) = f_\alpha(x_\alpha)$. Si además $g : M \to N$ es un homomorfismo tal que $g j_\alpha = f_\alpha$ para cada $\alpha \in I$, entonces para $x \in M$ $g(x) = g(\sum\limits_I j_\alpha q_\alpha(x)) = \sum\limits_I f_\alpha q_\alpha(x) = f(x)$. Por lo tanto $(M, \{j_\alpha\}_{\alpha \in I}$ es una suma directa de $\{M_\alpha\}_{\alpha \in I}$. $\square$

El siguiente corolario es una caracterización para el caso finito de la suma directa interna.

Corolario 3.7.2. *Sean $M_1, M_2, ..., M_n$ una sucesión finita de módulos y $j_i : M_i \to M$ con $i = 1, 2, ..., n$ homomorfismos. Entonces $(M, \{j_1, j_2, ..., j_n\})$ es una suma directa interna de $\{M_1, M_2, ..., M_n\}$ si y sólo si existen homomorfismos $q_i : M \to M_i$ con $i = 1, 2, ..., n$ tales que para toda $1 \leq i,\ k \leq n$ $q_k j_i = \delta_{ik} 1_{M_i}$ y $\sum_{i=1}^n j_i q_i = 1_M$.*

$\square$

Bibliografía

[1] Ibrahim Assem, Andrzej Skowronski y Daniel Simson. *Elements of the Representation Theory of Associative Algebras: Volume 1: Techniques of Representation Theory*. Vol. 65. Cambridge University Press, 2006.

[2] Diana Avella y col. *Grupos I*. papirhos, 2014.

[3] Claude Cibils y Francisco Larrion. *Métodos diagramáticos en teoría de representaciones*. Inf. téc. 1982.

[4] Kent R Fuller y Frank Wylie Anderson. *Rings and categories of modules*. Springer-Verlag, 1992.

[5] Fernando Hernández Hernández. *Teoría de conjuntos: una introducción*. Sociedad Matemática Mexicana, 2003.

[6] Joseph J Rotman. *An introduction to the theory of groups*. Vol. 148. Springer Science & Business Media, 2012.

[7] Felipe Zaldívar. *Teoría de Galois*. 3. Anthropos Editorial, 1996.