Benemérita Universidad Autónoma de Puebla

Facultad de Ciencias Físico Matemáticas
Licenciatura en Matemáticas

Teoría de Módulos Semisimples

Tesis

que para obtener el Título de Licenciado en Matemáticas
presenta

Abel Jesús Morales Méndez

Director de Tesis
Juan Angoa

Puebla, Pue. Junio 2014

INTRODUCCIÓN

En el desarrollo de las matemáticas han surgido muchos matemáticos que han revolucionado los estudios de las mismas. El álgebra es una de las ramas de las matemáticas, al igual que las demás, muy interesante. A lo largo del tiempo han existido diversos y grande matemáticos como Sophus Lie, Evariste Galois, Niels Henrik Abel, Nathan Jacobson, Felix Klein, Jonhs Weddenburn, Isaac Schur y Ludwing Sylow quienes a lo largo del tiempo han aportado grandes avances al Álgebra y la Geometría; sólo por mencionar algo de dos de ellos: Niels Henrik Abel que aportó grandes avances para el Analísis y Álgebra como las funciones abelianas, categorías abelianas y grupos abelianos que hoy llevan su nombre y quien por problemas económicos murió por tuberculosis a la edad de 26 años; Evariste Galois quien en su adolescencia ya era un gran matemático y para nuestra desgracia fue asesinado a sus 21 años; a este matemático se le atribuye la teoría que lleva su nombre la cual surge al tratar de resolver el problema de encontrar las raíces de un polinomio de grado n, únicamente usando sus radicales.

El estudio de los R-módulos es una rama de las matemáticas que como la teoría de grupos, no tan longeva como otras ramas, por mencionar alguna, la geometría la cual ya se conocía desde los pitagóricos.

En este trabajo presentaremos un estudio de R-módulos donde R será un anillo con uno y no necesariamente conmutativo, como por ejemplo los anillos con división infinitos. Los módulos a los que nos enfocaremos con más detalle seran los módulos simples, aquellos que sólo tienen como submódulos los triviales; estos módulos son de gran importancia pues como veremos, facilitan de una u otra manera algunas definiciones y también, que algunos conceptos sean equivalentes, como el ser finitamente generado y finitamente cogenerado. Daremos algunas otras clases de módulos más, como el superfluo y el esencial, y ya con base en estos módulos, definiremos en la clase de los módulos simples, el soclo y el radical que juegan un papel muy importante en la teoría de R-módulos. También estudiaremos módulos Artinianos y Noetherianos, módulos que tienen cadenas descendentes y ascendentes, de submódulos respectivamente, llamados así en honor de los matemáticos Emil Artin y Emmy Noether, respectivamente.

Contenido

Capítulo 1

Teoría de Módulos, preliminares.

En este capítulo daremos las siguientes definiciones: grupo, anillo, ideal de un anillo, homomorfismo de anillos y grupos, R-módulo, submódulo, etc. También señalaremos algunos ejemplos y estructuras que no veremos a fondo pero se daran referencias, si desean saber más del tema. Sin olvidar Teoremas y Proposiciones que serán de importancia a lo largo del desarrollo de los siguientes capítulos.

1.1 Grupos y Anillos

Definición 1.1. *Un semigrupo es una estructura* $(S, \cdot)$*, donde* $S \neq \emptyset$ *es un conjunto y* $\cdot$ *es una operación binaria sobre* S *la cual satisface la ley asociativa* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*, para todo* $a, b, c \in S$*.*

Definición 1.2. *Un monoide es una estructura* $(S, 1, \cdot)$*, donde* $(S, \cdot)$ *es un semigrupo y* 1 *es un elemento de* S *que actúa como identidad o elemento neutro (para toda* $a \in S$ $a \cdot 1 = a = 1 \cdot a$*).*

Definición 1.3. *Un grupo es un monoide con inverso, esto es, que para cada* $a \in S$ *existe* $b \in S$ *tal que* $ab = 1 = ba$*, normalmente se denota* $b = a^{-1}$*;* a^{-1} *es llamado el inverso de* a*.*

Es fácil con la definición de grupo construir muchos ejemplos de grupos, por sólo dar un ejemplo; sea n un entero, contruiremos un grupo de orden n. Sea G el conjunto con los símbolos a^i, i=0,1,2,3,... ,$n-1$ donde se debe cumplir $a^0 = a^n = e$, $a^i a^j = a^{i+j}$ si $i+j \leq n$ y $a^i a^j = a^{i+j-n}$ si $i+j > n$, ya con esto no es difícil ver que G es un grupo y esté grupo es llamado el grupo cíclico de orden n.

Definición 1.4. *Un grupo abeliano satisface la ley conmutativa; $ab = ba$ para todo par de elementos $a, b \in S$. Usualmente los grupos abelianos son denotados aditivamente por $(S, 0, +)$.*

Notemos que los enteros con la suma, es un grupo, con neutro el cero y los racionales sin el cero son un ejemplo de grupo multiplicativo, con 1 siendo su neutro.

Definición 1.5. *Un anillo con 1 es un conjunto R con dos operaciones binarias, la suma y el producto, con la suma es grupo abeliano y con el producto es un monoide donde el 1 es la unidad, y en donde se satisface la ley distributiva a izquierda $a(b+c) = ab + ac$ y ley distributiva a derecha $(a+b)c = ac + bc$ con $a, b, c \in R$.*

Definición 1.6. *Un anillo es conmutativo siempre que: para todo $a, b \in R$, $ab = ba$. Un anillo con división es un anillo donde se cumplé que; $0 \neq 1$ y $\forall a \in R - \{0\}$, $\exists b \in R$ tal que $ab = 1$ y $ba = 1$.*

Algunos ejemplos de anillos son: los números reales, racionales y complejos con el producto y suma usuales. Otro ejemplo es $\mathbb{Z}_n$ el conjunto de las clases residuales módulo $n \in \mathbb{N}$, es un ejemplo de un anillo conmutativo con 1. Note que los cuaterniones son un anillo con división.

Definición 1.7. *Un subconjunto S de un anillo R, es llamado un subanillo si es cerrado bajo el producto y la suma de R, contiene al 0 y 1, y es un anillo con las operaciones de R restringidas a S.*

1.1.1 Homomorfismos e Ideales.

De aquí en adelante cualquier anillo mencionado será anillo con 1, a menos que se diga lo contrario.

Definición 1.8. *Sean R y S dos anillos con 1. Una función $\psi : R \to S$ es llamado un homomorfismo de anillos si preserva las operaciones de anillo, es decir, $\psi(a+b) = \psi(a) + \psi(b)$, $\psi(ab) = \psi(a)\psi(b)$ y $\psi(1_R) = 1_S$.*

Definición 1.9. *Un homomorfismo ψ es un monomorfismo si éste es una función uno a uno, es decir, es inyectiva.*

Definición 1.10. *Un homomorfismo ψ es un epimorfismo si éste es sobreyectivo (sobre).*

Definición 1.11. *Un homomorfismo es un isomorfismo si es monomorfismo y epimorfismo, es decir, si es uno a uno y sobre.*

Definición 1.12. *Un homomorfismo de un anillo R en él mismo, es llamado un endomorfismo de R; si éste es isomorfismo, entonces es un automorfismo de R.*

Si $\phi : R \to S$ y $\psi : S \to T$ son homomorfismos entonces se define la composición $\psi \circ \phi : R \to T$ dada por $(\psi \circ \phi)(s) = \psi(\phi(s))$, con $s \in R$.

Proposición 1.13. *Sean R y S anillos y $\psi : R \to S$ un homomorfismo de anillos. Entonces ψ es isomorfismo si y sólo si existen $\phi, \phi' : S \to R$ tal que*

$$\phi \circ \psi = 1_R \quad y \quad \psi \circ \phi' = 1_S$$

Definición 1.14.

1. *Sea R un anillo. I es un ideal de R si es un subgrupo aditivo de R, y si $sk, ks \in I$, para toda $k \in I$ y para todo $s \in R$.*
2. *I es un ideal izquierdo de R, si es un subgrupo de R, tal que $rk \in I$ para toda $k \in I$ y para toda $r \in R$.*
3. *I es un ideal derecho de R, si es un subgrupo de R, tal que $kr \in I$ para toda $k \in I$ y para toda $r \in R$.*

Notemos que los dos subconjuntos $\{0\}$ y R son ideales de R; se llaman ideales triviales de R. Cualquier otro ideal I que no sea alguno de los triviales es llamado ideal propio de R. Observe que si $a \in R$, entonces $a = a1$; de aquí es inmediato que cualquier ideal I es todo R si y sólo si $1 \in I$.

Definición 1.15. *El anillo R es llamado simple en el caso de que sus únicos ideales sean R y $\{0\}$.*

La colección de todos los ideales de un anillo R es un conjunto parcialmente ordenado por la inclusión de conjuntos.

Notemos que un anillo con división es un anillo simple, un ejemplo son las matrices cuadradas con determinante distinto de cero. Por otro lado, se tiene que un anillo conmutativo simple es un campo, pero en general, un anillo simple no nesesariamente es anillo con división y un anillo con división no necesariamente es conmutativo (piense en el anillo de las matrices cuadradas invertibles con la multiplicación no es conmutativa). No siempre cada anillo con división es un campo por ejemplo, los cuaterniones. Pero sin embargo, sí se cumple que un anillo con división finito es campo, lo cual fue probado por Wedderburn en 1905, matemático escocés.

Definición 1.16. *Dado un homomorfismo de anillo $\phi : R \to S$, la imagen y el núcleo de ϕ, $Im\ \phi$ y $Ker\ \phi$ respectivamente están definidas como:*

$$Im\ \phi = \{y \in S | \ \exists x \in R,\ \phi(x) = y\} \quad y \quad Ker\ \phi = \{x \in R | \ \phi(x) = 0\}.$$

Se sabe que $Im\ \phi$ es un subanillo de S y el $Ker\ \phi$ es un ideal de R.

Proposición 1.17. *Sean R y S anillos y $\phi : R \to S$ un homomorfismo de anillo. Entonces*

1. *ϕ es sobreyectiva si y sólo si $Im\ \phi = S$.*
2. *ϕ es inyectiva si y sólo si $Ker\ \phi = \{0\}$.*

DEMOSTRACIÓN. 1) Se sigue de la definición.

2) $\Rightarrow$) Si ϕ es inyectiva y $x \in Ker\ \phi$. Entonces $\phi(x) = 0 = \phi(0)$ entonces $x = 0$.

$\Leftarrow$) Recíprocamente, ahora sean $Ker\ \phi = \{0\}$ y $\phi(x) = \phi(y)$, entonces $0 = \phi(x) - \phi(y) = \phi(x - y)$ por tanto $x - y \in Ker\ \phi = \{0\}$, por lo tanto $x - y = 0$ entonces $x = y$. □

Si I es un ideal propio del anillo R. Entonces I determina una relación de congruencia sobre R definida por $a \equiv b\,(mod\, I)$ en el caso en que $a - b \in I$. El conjunto cociente R/I, hereda de R una suma y una multiplicación unívocamente definidas: $(a + I) + (b + I) =$

$(a+b)+I$ y $(a+I)(b+I)=(ab)+I$, respectivamente teniendo neutro aditivo y multiplicativo $0+I$ y $1+I$ respectivamente, que lo hace un anillo, denominado el anillo cociente (o anillo de clases residuales) R/I. La aplicación definida $f : R \to R/I$ que aplica cada elemento de $r \in R$ a su clase $r+I = \{r+x|\ x \in I\}$, es un homomorfismo de anillos sobreyectivo (epimorfismo).

Definición 1.18. *Sea $\phi : R \to S$ un homomorfismo de anillos e $I \subseteq S$ un ideal de S, la imagen inversa de I bajo ϕ se denota $\phi^{\leftarrow}(I)$ y se define por: $\phi^{\leftarrow}(I) = \{r \in R|\ \phi(r) \in I\}$.*

Lema 1.19. *Sea $\phi : R \to S$ un homomorfismo de anillos. Si $I \subseteq S$ es un ideal entonces su imagen inversa $\phi^{\leftarrow}(I) \subseteq R$ también es un ideal.*

Demostración. Como $I \subseteq S$ es un subgrupo con respecto a la adición, entonces $\phi^{\leftarrow}(I) \subseteq R$ también es un subgrupo. Ahora, si $a \in R$ y $x \in \phi^{\leftarrow}(I)$, entonces $\phi(x) \in I$ y así $\phi(a)\phi(x) \in I$ ya que I es ideal, y como ϕ es homomorfismo de anillos entonces $\phi(ax) = \phi(a)\phi(x) \in I$, es decir, $ax \in \phi^{\leftarrow}(I)$. □

Proposición 1.20. *Existe una correspondencia biyectiva que conserva el orden de los ideales K de R y los ideales $\mathbf{G}$ de R/I, donde $I \subseteq K$; dada por $K = f^{\leftarrow}(\mathbf{G})$ y $f : R \to R/I$ es el epimorfismo canónico.*

Demostración. El Lema 1.19 asegura que para cada ideal $\mathbf{G}$ de R/I, $K = f^{\leftarrow}(\mathbf{G})$ es un ideal de R. □

Definición 1.21. *Sea R un anillo. Un ideal maximal de R es un ideal propio $M \subseteq R$ tal que para cualquier otro ideal I de R con $M \subseteq I \subseteq R$ se tiene que $M = I$ o $I = R$.*

Sea R es un anillo y $a \in R$, entonces el conjunto de todos los productos xa, con $x \in R$, es un ideal izquierdo, llamado ideal izquierdo principal generado por a, denotado Ra. Note que si R tiene elemento unidad, entonces a es unidad sí y sólo si $R = Ra$.

1.1.2 Endomorfismos de Anillos

Sea A un grupo abeliano escrito aditivamente.Veremos que los morfismos de A en A forman un grupo, veremos que los morfismos forman un grupo, llamados los endomorfismos de A.

En efecto el conjunto E, de todos los endomorfismos de A, forman un grupo abeliano con respecto a la adición $(f, g) \mapsto f + g$, definida por $(f + g)(a) = f(a) + g(a)$, para $a \in A$. Y el neutro y los inversos están dados por $0(a) = 0$ y $(-f)(a) = -f(a)$ respectivamente.

También notemos que E con la composición de funciones es una operación asociativa que distribuye la operación aditiva sobre E. Si $A \neq \{0\}$, entonces E es una anillo con identidad $1_A : A \to A$. Pero notemos que si $f, g \in E$, entonces en general el producto $fg \in E$ depende de como consideremos la operación si a la derecha o a la izquierda: $(fg)(a) = f(g(a))$ ó $(a)(fg) = ((a) f) g$, respectivamente.

En otras palabras, se definen naturalmente, para cada grupo abeliano $A \neq \{0\}$, dos anillos de endomorfismos, un anillo de endomorfismos izquierdo y un anillo de endomorfismos derecho denotados $End^l(A)$ y $End^r(A)$, respectivamente. Si no se dice lo contrario $End(A)$, denotará al anillo $End^l(A)$.

1.2 Módulos y Submódulos

Definición 1.22. *Sea R un anillo. Entonces el par (M, λ) es un R-módulo izquierdo en donde M es un grupo abeliano y λ una transformación de R en el conjunto de los endomorfismos izquierdos de M, tal que, si $M \neq \{0\}$, $\lambda : R \to End^l(M)$ es un homomorfismo de anillo. Esto simplemente significa que para cada $a \in R$ existe una transformación $\lambda(a) : M \to M$ tal que para todo $a, b \in R$ y toda $x, y \in M$*

$$\lambda(a)(x + y) = \lambda(a)(x) + \lambda(a)(y), \quad \lambda(a + b)(x) = \lambda(a)(x) + \lambda(b)(x)$$

$$\lambda(ab)(x) = \lambda(a)(\lambda(b)(x)), \quad \lambda(1)(x) = x.$$

De la misma forma se puede definir un R-módulo derecho simplemente usando una transformación $\lambda : R \to End^r(M)$ así también se dan definiciones similares a la derecha.

EL primer ejemplo vendra ilustrado como se trabaja con la transformación λ que se da en la definición de R-módulo izquierdo y de ahí en adelante abusaremos de la notación y sólo se dara una sencilla definición como una multiplicación natural en el grupo abeliano.

Ejemplo 1.23. *1.-Sean M un grupo abeliano y $\mathbb{Z}$ el anillo de los enteros, M tiene una estructura de $\mathbb{Z}$-módulo izquierdo, definiendo a $\lambda : \mathbb{Z} \to End^l(M)$ con regla de correspondencia $k \mapsto \lambda(k)$ y $\lambda(k) : M \to M$, definida recursivamente para $k \in \mathbb{Z}^+$ por:*

a) $\lambda(1)(m) = 1 \cdot m := m$

b) $\lambda(k)(m) = k \cdot m := (k-1) \cdot m + m,\ k \geq 2.$

c) $\lambda(0)(m) = 0 \cdot m := 0$

y

d) $\lambda(-k)(m) = (-k) \cdot m := k \cdot (-m).$

Donde $m \in M$.

2.- Cada grupo abeliano M es módulo a la izquierda sobre su anillo de endomorfismos respecto a la siguiente operación:

$$f \cdot m := f(m), \quad \text{con } m \in M \ \text{ y } \ f \in End(M).$$

3.-Si D es un anillo con división, entonces el D-módulo izquierdo, es simplemente el D-espacio vectorial izquierdo.

4.-Para un anillo R existe un único homomorfismo de anillo de $\mathbb{Z}$ a R. También para cada grupo abeliano M existe un única estructura de $\mathbb{Z}$-módulo. Esta estructura simple sobre el grupo aditivo esta dada por la función multiplicación $(n, x) \mapsto nx$.

5.-Sean R y S anillos y sea $\phi : R \to S$ un homomorfismo de anillos, entonces ϕ induce estructuras de R-módulo izquierdo y derecho sobre el grupo aditivo de S. En efecto, la multiplicación por un escalar, para el R-módulo izquierdo S, esta dada por $(r, s) \mapsto \phi(r)s$ para cada $r \in R$ y $s \in S$, claro notemos que el producto $\phi(r)s$ es calculado en el anillo S.

En los cursos elementales, encontramos que un espacio vectorial, está definido sobre campos y no se definen estructuras laterales. Pero en un anillo no conmutativo con división D, un D-espacio vectorial izquierdo no siempre es lo mismo que un D-espacio vectorial derecho. Daremos un ejemplo que muestre este hecho:

Sea A un anillo, dado un módulo izquierdo M sobre A, no siempre se puede convertir a M en módulo derecho, con sólo cambiar el lado de la acción de los escalares. En efecto, sea V el grupo abeliano definido por

$$V := \{e, a, b, ab\},\ a^2 = b^2 = e,\ ab = ba.$$

y consideremos las funciones: $f : V \to V$ y $g : V \to V$ con las reglas de correspondencia dadas por $f(e) = e$,$f(a) = a$, $f(b) = ab$, $f(ab) = b$ y $g(e) = e$, $g(a) = b$, $g(b) = a$ y $g(ab) = ab$, respectivamente. Resultan ser endomorfismos para los cuales se tiene

$$(f \circ g)(a) = f(g(a)) = f(b) = ab \neq b = g(a) = g(f(a)) = (g \circ f)(a)$$

así con este ejemplo podemos adelantar que $f \circ g \neq g \circ f$; sea $A = End(V)$ el anillo de endomorfismos. Por el ejemplo 2) se induce sobre V una estructura de A-módulo izquierdo.

Definamos $m \times h := h \cdot m = h(m)$, con $h \in A$, $m \in V$.

Nótese que $a \times (fg) = fg(a) = f(b) = ab \neq b = g(a) = a \times g = f(a) \times g = (a \times f) \times g$, con lo cual éste producto no da a V estructura de A-módulo derecho.

Si no es claro la noción de R-módulo izquierdo (derecho), consulte en [6] más ejemplos de R-módulos.

Definición 1.24. *Sean R y S dos anillos. Un grupo abeliano M es un R-S-bimódulo izquierdo y derecho en el caso en que M sea ambos R-módulo izquierdo y S-módulo derecho, y además, se satisface $r(xs) = (rx)s$ para $r \in R$, $s \in S$ y $x \in M$.*

Existe otro tipo de bimódulo respecto a como estén operando los anillos, así la definición puede modificarse. Un R-S-bimódulo con ambos módulos izquierdos, es un bimódulo el cual se denotara por ${}_{R-S}M$ (en la definición anterior ${}_RM_S$), y cumplirá $r(sx) = s(rx)$ para $r \in R$, $s \in S$ y $x \in M$.

Definición 1.25. *Sea M un R-módulo izquierdo. Entonces un subgrupo abeliano N de M es un submódulo de M en el caso de que N sea estable bajo los endomorfismos de M inducidos por R (para toda $r \in R$: $\lambda(N) \subseteq N$), en otras palabras, N es submódulo de M si y sólo si, es un subgrupo de M, cerrado bajo la multiplicación por un escalar por elementos de R.*

En particular, un submódulo N de M, es un R-módulo izquierdo sí M lo es.

Definición 1.26. *Si $X \subseteq M$ y $A \subseteq R$, entonces cualquier elemento de M de la forma*

$$a_1x_1 + a_2x_2 + ... + a_nx_n = \Sigma_{i=1}^{n} a_ix_i$$

con $x_1, ..., x_n \in X$ y $a_1, ..., a_n \in A$ es una combinación lineal de X con coeficientes en A, o similarmente A-combinación lineal de X. Se denotara el conjunto de todas las A-combinaciones lineales de X por AX.

Proposición 1.27. *Sean M un R-módulo izquierdo y X un subconjunto no vacío de M. Entonces RX es un R-submódulo de M.*

Demostración. Las R-combinaciones lineales de X son claramente cerradas bajo la operación de M, y notemos que $a\,(r_1x_1 + ... + r_nx_n) = (ar_1)\,x_1 + ... + (ar_n)\,x_n$. entonces es un submódulo de M. $\square$

Proposición 1.28. *Sean M un R-módulo izquierdo y N un subconjunto distinto del vacío de M. Entonces los siguientes afirmaciones son equivalentes:*

1. *N es submódulo de M.*
2. *$RN = N$*
3. *Para todo $a, b \in R$ y todo $x, y \in N$, $ax + by \in N$.* $\square$

Lema 1.29. *Si M es un R-módulo izquierdo y si $M_1, ..., M_n$ son submódulos de M, entonces*

$$M_1 + ... + M_n = \{m_1 + ... + m_n |\ m_i \in M_i,\ i \in \{1, ..., n\}\}$$

es también un submódulo de M. De hecho, $M_1 + ... + M_n$ es el conjunto de todas las R-combinaciones lineales de $M_1 \cup ... \cup M_n$. $\square$

Proposición 1.30. *Sea M un R-módulo izquierdo, entonces el conjunto $\varphi\,(M)$ de submódulos de M es una red completa de módulos con respecto a $\leq$ (denota la relación de submódulo). Es decir, en esta red, si Γ es un conjunto distinto del vacío, entonces la suma $\Sigma\Gamma$ y la intersección $\cap\Gamma$ son submódulos. En particular, si K y L son submódulos de M, entonces $K + L$ y $K \cap L$ son la suma y la intersección respectivamente, además si H es cualquier submódulo de M entonces $K \leq H$ implica $H \cap (K + L) = K + (H \cap L)$, (ley modular).* $\square$

1.2.1 Módulo Cociente

Sea M un R-módulo izquierdo y sea K un submódulo. Entonces es fácil ver que el conjunto cociente

$$M/K = \{x + K|\ x \in M\}$$

es un R-módulo relativo a la adición y multiplicación por un escalar definida vía

$$(x + K) + (y + K) = (x + y) + K, \quad a\,(x + K) = ax + K.$$

Con la identidad aditiva e inversos dados por $K = 0{+}K$ y $-(x + K) = -x + K$. Entonces el módulo M/K es llamado el R-módulo izquierdo cociente de M en K. Existe una correspondencia biyectiva que conserva el orden entre los submódulos de M que contienen a K y los submódulos de M/K. Luego un módulo cociente M/K es simple si y sólo si K es un submódulo maximal de M.

Nota 1.31. *Sea M un S-módulo izquierdo y R otro anillo y sea $\phi : R \to S$ un homomorfismo de anillos. Si la estructura de ${}_SM$ se obtiene del homomorfismo de anillos $\lambda : S \to End^l\,(M)$, entonces $\lambda\phi : R \to End^l\,(M)$ induce una R-estructura izquierda sobre M, donde la multiplicación por un escalar se obtiene $(r, x) \mapsto \phi\,(r)\,x$.*

Así M es un R-módulo izquierdo con ${}_RM$ inducido por $rx = \phi\,(r)\,x$ con $r \in R$ y $x \in M$.

Definición 1.32. *Sea M un R-módulo vía el homomorfismo de anillos $\lambda : R \to End^l\,(M)$, abreviandolo $ax = \lambda\,(a)\,x$. El núcleo,*

$$K = Ker\ \lambda = \{a \in R|\ ax = 0\ ,\ x \in M\},$$

es un ideal bilateral de R y es llamado el anulador de M en R. Si $K = \{0\}$ (es decir, λ es inyectivo) entonce M es un R-módulo izquierdo fiel.

1.2.2 Homomorfismo de Módulos

Definición 1.33. *Si M y N son dos R-módulos izquierdos, entonces la función $f : M \to N$ es un R-homomorfismo de módulo izquierdo en el caso en que para todo $a, b \in R$ y toda $x, y \in M$*

$$f\,(ax + by) = af\,(x) + bf\,(y)\,,$$

es decir, f es R-lineal.

Definición 1.34. *Sean M y N R-módulos izquierdos y sea $f : M \to N$ un R-homomorfismo izquierdo. Entonces la imagen de f ($Im\ f$), y el núcleo de f ($Ker\ f$), estan definidos por*

$$Im\ f = \{g \in N | \ \exists x \in M,\ f(x) = g\} \text{ y } Ker\ f = \{x \in M | \ f(x) = 0\}.$$

Notemos que la imagen y el núcleo de f son submódulos de N y de M respectivamente. La coimagen y el conúcleo de f están definidos por $Coim\ f = M/Ker\ f$ y $Coker\ f = N/Im\ f$, respectivamente.

Definición 1.35. *Un homomorfismo de módulos $f : M \to N$ es llamado un epimorfismo es caso de ser suprayectiva o sobre.*

Definición 1.36. *Un homomorfismo $f : M \to N$ es llamado un monomorfismo en el caso en que es inyectivo o uno a uno.*

Abreviaremos monomorfismo y epimorfismo por mono y epi respectivamente. Si M es un R-módulo izquierdo, entonces cada submódulo de M es la imagen de algún monomorfismo.

Definición 1.37. *Para cada K submódulo de M, la transformación inclusión $i_k = i_{K \leq M} : K \to M$ es un R-monomorfismo, también es llamado el encajamiento natural de K en M.*

Análogamente, cada submódulo es el núcleo de algún epimorfismo. En particular si K es un submódulo de M, entonces la transformación $\eta_K : M \to M/K$ de M sobre el módulo cociente M/K definido $\eta_K(x) = x + K \in M/K$ con $x \in M$, es un R-epimorfismo con núcleo K. η_K es llamado el epimorfismo natural de M sobre M/K.

Definición 1.38. *Un R-homomorfismo $f : M \to N$ es un R-isomorfismo en el caso de ser biyectivo.*

Dos módulos se dice que son R-isomorfos denotados por $M \cong N$, en el caso en que existe un R-isomorfismo $f : M \to N$. Esta relación es una relación de equivalencia.

Proposición 1.39. *Sean M y N R-módulos izquierdos y sea $f : M \to N$ un R-homomorfismo. Entonces las siguientes afirmaciones son equivalentes:*

a) f *es un epimorfismo sobre* N*.*

b) $Im\ f = N$*.*

c) *Para cada* ${}_RK$ *y cada par de* $g, h : N \to K$ *de R-homomorfismos; si* $gf = hf$ *entonces* $g = h$*.*

d) *Para cada* ${}_RK$ *y cada* $g : N \to K$ *R-homomorfismos; si* $gf = 0$ *entonce* $g = 0$*.*

DEMOSTRACIÓN. a) $\Leftrightarrow$ b) y a) $\Rightarrow$ c) son triviales.

c) $\Rightarrow$ d). Sea $h : N \to K$ el homomorfismo cero. Entonces $gf = 0 = hf$, asumiendo c), se tiene que $g = h = 0$.

d) $\Rightarrow$ b). Sea $\eta_{Im\ f} : N \to Coker\ f = N/Im\, f$, claramente se satisface $\eta_{Im\ f} f = 0$, asumiendo d) implica que $\eta_{Im\ f} = 0$, pero es epimorfismo sobre $N/Im\ f$, se tiene que $N/Im\ f = 0$, es decir, $Im\ f = N$. $\square$

Proposición 1.40. *Sean* M *y* N *R-módulos izquierdos y sea* $f : M \to N$ *un R-homomorfismo. Entonces las siguientes afirmaciones son equivalentes:*

a) f *es monomorfismo.*

b) $Ker\ f = \{0\}$

c) *Para cada* ${}_RK$ *y cada par de* $g, h : K \to M$ *de R-homomorfismos; si* $fg = fh$ *entonces* $g = h$*.*

d) *Para cada* ${}_RK$ *y cada* $g : K \to M$ *de R-homomorfismos; si* $fg = 0$ *entonces* $g = 0$*.*

DEMOSTRACIÓN. a) $\Leftrightarrow$ b) y a) $\Rightarrow$ c) son triviales. d) $\Rightarrow$ b) Sea $i_{Ker\ f} : Ker\ f \to M$ un R-homomorfismo y $f i_{Ker\ f} = 0$, asumiendo d) se tiene que $i_{Ker\ f} = 0$, entonces $Im\ f = Ker\ f = \{0\}$ $\square$

Proposición 1.41. *Sea* M *y* N *R-módulos izquierdos y sea* $f : M \to N$ *un R-homomorfismo. Entonces* f *es un isomorfismo si y sólo si existen funciones* $g, h : N \to M$ *tal que*

$$fg = 1_N \ \ y \ \ hf = 1_M.$$

Cuando estas últimas condiciones se satisfacen, entonces $g = h$ y g es un isomorfismo.

Demostración. ($\Leftarrow$) Si existen $g, h : N \to M$, tales que $hf = 1_M$ y $fg = 1_N$, entonces $g = 1_M g = hfg = h1_N = h$, así que f es biyectiva, así que es isomorfismo.

($\Rightarrow$) Como f es isomorfismo entonces es bijectiva, luego existe una funcion $g : N \to M$ tal que $gf = 1_N$ y $fg = 1_M$. Falta ver que g es lineal, entonces $f(g(ax + by)) = ax + by = af(g(x)) + bf(g(y)) = f(ag(x)) + f(bg(y)) = f(ag(x) + bg(y))$ y como f es inyectiva se tiene que g es R-lineal. $\square$

1.2.3 El Teorema del Factor

Cuando un homomorfismo $f : M \to N$ es la composición de homomorfismos $f = gh$, se dice que f se factoriza a través de g y h.

Teorema 1.42. Teorema del Factor. *Sea M, M', N y N' R-módulos izquierdos y sea $f : M \to N$ un R-homomorfismo.*

1. *Si $g : M \to M'$ es un epimorfismo con $Ker\ g \subseteq Ker\ f$, entonces existe un único homomorfismo $h : M' \to N$ tal que $f = hg$. Por otra parte, $Ker\ h = g(Ker\ f)$ y $Im\ h = Im\ f$, de modo que h es mono si y sólo si $Ker\ g = Ker\ f$ y h es epi si y sólo si f es epi.*

2. *Si $g : N' \to N$ es un monomorfismo con $Im\ f \subseteq Im\ g$, entonces existe un único homomorfismo $h : M \to N'$ tal que $f = gh$. Por otra parte, $Ker\ h = Ker\ f$ y $Im\ h = g^{\leftarrow}(Im\ f)$, de modo que h es mono si y sólo si f es mono y h es epi si y sólo si $Im\ g = Im\ f$.*

Demostración. (1) Como $g : M \to M'$ es epi, para cada $m' \in M'$ existe un $m \in M$ tal que $g(m) = m'$. Si también $l \in M$ tal que $g(l) = m'$, entonces claramente $m - l \in Ker\ g$, pero $Ker\ g \subseteq Ker\ f$, entonces se tiene que $f(l) = f(m)$. Entonces existe una función $h : M' \to N$ definida como $h(m') = f(m)$, tal que $g(m) = m'$; además $f = hg$. Para ver que h es un R-homomorfismo, sean $x', y' \in M'$ y sea $x, y \in M$ con $g(x) = x'$, $g(y) = y'$. Entonces para cada $a, b, \in R$, $g(ax + by) = ax' + by'$, de modo que

$$h(ax' + by') = f(ax + by) = af(x) + bf(y) = ah(x') + bh(y').$$

La unicidad se sigue de saber que g es epi.

$$\begin{tikzcd} M \arrow[rr, "f"] \arrow[dr, "g"'] & & N \\ & M' \arrow[ur, dashed, "h"'] & \end{tikzcd}$$

(2) Para cada $m \in M$, $f(m) \in Im\ f \subseteq Im\ g$. Como g es mono, existe un único $n' \in N'$ tal que $g(n') = f(m)$. Por lo tanto, existe una función $h : M \to N'$ via $m \mapsto n'$ tal que $f = gh$, y para checar que es homomorfismo es similar a la parte (1).

$$\begin{tikzcd} M \arrow[rr, "f"] \arrow[dr, dashed, "h"] & & N \\ & N' \arrow[ur, "g"] & \end{tikzcd}$$

$\square$

Corolario 1.43. El Teorema de Isomorfismos *Sean M y N R-módulos izquierdos:*

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

2. *Si $K \leq L \leq M$, entonces $M/L \cong (M/K)/(K/L)$.*

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

Demostración. (1) Sea $f : M \to N$ el epimorfismo y sea $\eta_K : M \to M/K$ el epimorfismo natural con $K = Ker\ f$, aplicando el Teorema del factor existe $\eta : M/K \to N$ homomorfismo tal que $f = \eta\eta_K$, como

$Ker\ f = Ker\ \eta_K$, η es monomorfismo y f es epimorfismo, entonces también η es epimorfismo, por lo tanto η es isomorfismo.

$$\begin{tikzcd} M \arrow[rr, "f"] \arrow[dr, "\eta_K"'] & & N \\ & N' \arrow[ur, dashed, "\eta"'] & \end{tikzcd}$$

(2) Sólo hay que tomar $f : M/K \to M/L$ definida como $f(x+K) = x + L$, que está bien definida por la hipótesis de que $K \leq L$, además tenemos que $Ker\ f = L/K$. Ahora, como f es epimorfismo aplicamos (1), y tenemos que $M/K \cong (M/L)/(L/K)$.

(3) Se define $f : H \to (H + K)/K$ como $f(x) = x+K$ para $x \in H$, notamos que el $Ker\ f = K \cap H$, entonces así por (1) se obtiene el isomorfismos $(H + K)/K \cong H/(H \cap K)$ □

Definición 1.44. *Sea M un R-módulo izquierdo. Entonces para cada $X \subseteq M$, el anulador izquierdo de X en R es*

$$l_R(X) = \{r \in R |\ rx = 0\ (x \in X)\}$$

y, para cada $A \subseteq R$, el anulador derecho de A en M es

$$r_M(A) = \{x \in M |\ ax = 0\ (a \in A)\}$$

para elementos de la forma $\{x\}$ y $\{a\}$, se abreviaran $l_R(x)$ y $r_M(a)$.

Corolario 1.45. *Un R-módulo M es cíclico si y sólo si es isomorfo a un módulo cociente de ${}_RR$.*

Demostración. Si $M = Rx$, entonces $\rho_x : R \to M$ es un epimorfismo con núcleo $l_R(x)$, por tanto $M \cong R/l_R(x)$. Por otro lado si $f : R/I \to M$ es un isomorfismo de módulos, donde I es un submodulo de ${}_RR$. Sea $x = f(1+I)$, veamos que $M = Rx$. Sea $m \in M$, existe $z + I \in R/I$, tal que $f(z + I) = m$, pero $zf(1 + I) = f(z + I) = m$, asi que $m = zx$. □

Corolario 1.46. *Un R-módulo M cíclico es simple si y sólo si $l_R(x)$ es un ideal maximal izquierdo para algún $x \in M$.*

DEMOSTRACIÓN. Si M es simple para cualquier $x \in M \setminus \{0\}$, $M = Rx$, por el Corolario 1.45, vemos que $M \cong R/l_R(x)$, así que $l_R(x)$ es un ideal maximal izquierdo. Ahora, si $l_R(x)$ es un ideal maximal izquierdo para algún $x \in M$ tal que $M = Rx$, entonces $h : R/l_R(x) \to M$, definida como $h(r + l_R(x)) = rx$, se puede demostrar que es un homomorfismo inyectivo no nulo de $R - modulos$, como $M = Rx$, h es este epimorfismo, asi que es isomorfismo. $\square$

Corolario 1.47. *Sean M y K R-módulos izquierdos y $j : K \to M$ un R-monomorfismo con $Im\ j = I$, entonces existe un único isomorfismo $\nu : I \to K$ tal que $j\nu = i_I$*

DEMOSTRACIÓN. Aplicando el Teorema 1.42,(2) tomando $f = i_I$ y $j = g$ el monomorfismo, entonces se concluye lo requerido. $\square$

1.2.4 Sucesiones Exactas

Definición 1.48. *Un par de homomorfismos $M' \xrightarrow{f} M \xrightarrow{g} M''$ se dice que es una sucesión exacta en el caso en que $Im\ f = Ker\ g$, así una sucesión finita o infinita*

$$\cdots \xrightarrow{f_{n-2}} M_{n-2} \xrightarrow{f_{n-1}} M_{n-1} \xrightarrow{f_n} M_n \xrightarrow{f_{n+1}} M_{n+1} \xrightarrow{f_{n+2}} \cdots$$

de homomorfismos es exacta en cada M_n en el caso $Im\ f_n = Ker\ f_{n+1}$.

Proposición 1.49. *Dados los módulos M y N y un homomorfismo $f : M \to N$, las sucesiones*

1. $0 \to M \xrightarrow{f} N$ *es exacta si y sólo si f es mono.*

2. $M \xrightarrow{f} N \to 0$ *es exacta si y sólo si f es epi.*

3. $0 \to M \xrightarrow{f} N \to 0$ *es exacta si y sólo si f es isomorfismo.*

$\square$

Proposición 1.50. *Si M y N son módulos y si $f : M \to N$ es un homomorfismo, entonces*

$$0 \to Ker\ f \xrightarrow{i} M \xrightarrow{f} N \xrightarrow{\eta} Coker\ f \to 0$$

son exactas, donde i es la inclusión y $\eta : N \to N/Im\ f$ es el epimorfismo natural. □

Lema 1.51. *Supongamos que el siguiente diagrama de módulos y homomorfismos conmuta y tiene filas exactas.*

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

1. *Si α, γ y f' son mono, entonces también lo es β.*

2. *Si α, γ y g son epi, entonces también lo es β.*

3. *Si β es mono, y si α y g son epi, entonces γ es mono.*

4. *Si β es epi, y si f' y γ son mono, entonces α es epi.*

Demostración. (1) Mostremos que $Ker\ \beta = \{0\}$, sea $b \in Ker\ \beta$, y como el diagrama conmuta, $\gamma g(b) = g'\beta(b) = 0$, como γ es mono entonces $g(b) = 0$ por lo tanto $b \in Ker\ g$, pero por la exactitud de las flechas $Im\ f = Ker\ g$, entonces existe un $a \in A$ tal que $f(a) = b$ y como el diagrama conmuta $f'\alpha(a) = \beta f(a) = \beta(b) = 0$, y como f' y α son mono entonces $a = 0$, por lo tanto $b = f(a) = 0$.

(2) Si $b' \in B'$, demostraremos que existe un $b_1 \in B$ tal que $\beta(b_1) = b'$. Sea $b' \in B'$, entonces $g'(b') \in C'$, como γ es epi entonces existe un $c \in C$ tal que $\gamma(c) = g'(b')$, pero también g es epi por tanto existe un $b \in B$ tal que $\gamma(g(b)) = g'(b')$, ahora como el diagrama conmuta tenemos

$$g'(\beta(b)) = \gamma(g(b)) = g'(b'),$$

entonces $g'(\beta(b)) - g'(b') = g'(\beta(b) - b') = 0$ implica que $\beta(b) - b' \in Ker\ g' = Im\ f'$ por las lineas exactas, por tanto existe un $a' \in A'$ tal que $f'(a') = \beta(b) - b'$, más aun α también es epi, así existe un $a \in A$ tal que $f'(\alpha(a)) = \beta(b) - b'$, una vez más por el diagrama conmutativo

$$\beta(f(a)) = f'(\alpha(a)) = \beta(b) - b',$$

entonces

$$\beta(f(a)) - \beta(b) = \beta(f(a) - b) = b'.$$

Si $b_1 = f(a) - b$, entonces obtenemos que $\beta(b_1) = b'$. Por lo tanto β es epi.

(3) Veamos que el $Ker\ \gamma = \{0\}$. Sea $c \in Ker\,\gamma$, pero como g es epi, existe un $b \in B$ tal que $g(b) = c$, pero como el diagrama conmuta entonces $\gamma(g(b)) = g'(\beta(b)) = 0$ por tanto $\beta(b) \in Ker\,g' = Im\,f'$, es decir, existe un $a' \in A'$ tal que $f'(a') = \beta(b)$, pero como α es epi entonces existe un $a \in A$ tal que $\alpha(a) = a'$, y como el diagrama conmuta se tiene $\beta(b) = f'(\alpha(a)) = \beta(f(a))$, pero como β es mono entonces, $f(a) = b$, por lo tanto al aplicar g a la igualdad

$$c = g(b) = g(f(a)) = 0$$

por lo tanto $Ker\,\gamma = 0$.

(4) Sea $a' \in A'$. Entonces donde β es epi, existe un $b \in B$ tal que $\beta(b) = f'(a')$. Como el diagrama conmuta y las filas son exactas se tiene $\gamma g(b) = g'\beta(b) = g'f'(a') = 0$, pero γ es mono, así $b \in Ker\ g = Im\ f$, así entonces existe un $a \in A$ con $f(a) = b$, pero se tiene $f'\alpha(a) = \beta f(a) = \beta(b) = f'(a')$, finalmente como f' es mono se tiene $\alpha(a) = a'$. Así α es epi. $\square$

Lema 1.52 (Lema de los 5)**.** *Supongamos que el siguiente diagrama de módulos y homomorfismo es conmutativo y tiene filas exactas.*

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

1. *si α es epi y β y δ son mono, entonces γ es mono.*
2. *si ε es monic y β y δ son epi, entonces γ es epi.*
3. *si α, β, δ y ε son isomorfismos, entonces γ es isomorfismo.*

$\square$

Capítulo 2

Sumandos Directos

2.1 Sucesiones Exactas que se parten

Dados dos módulos M_1 y M_2, puede ser construido el producto cartesiano $M_1 \times M_2$. La estructura de este producto de módulos esta definida coordenada a coordenada de los factores M_1 y M_2. Dado un módulo M nos concentraremos en hallar condiciones que nos aseguran que pueda descomponerse M en factores, como el producto cartesiano de módulos. M_1 y M_2 submódulos de un módulo M, generan a M en el caso de que $M_1 + M_2 = M$, son independientes en el caso de que $M_1 \cap M_2 = \{0\}$. Si M_1 y M_2 son submódulos de M, existe un R-homomorfismo canónico i del producto cartesiano $M_1 \times M_2$ al módulo M definido vía:

$i : (x_1, x_2) \mapsto x_1 + x_2$, donde $((x_1, x_2) \in M_1 \times M_2)$.

con imagen y núcleo:

$Im\ i = M_1 + M_2$ y $Ker\ i = \{(x, -x) : x \in M_1 \cap M_2\}$.

i es un epimorfismo si y sólo si $M_1 + M_2 = M$, y es monomorfismo si y sólo si $M_1 \cap M_2 = \{0\}$.

Definición 2.1. *Si el R-homomorfismo canónico i (definido antes) es un isomorfismo, entonces M será una suma directa de los submódulos M_1 y M_2, y se denotará $M = M_1 \oplus M_2$.*

Así $M = M_1 \oplus M_2$ si y sólo si para cada $x \in M$ existen únicos elementos $x_1 \in M_1$, $x_2 \in M_2$ tal que $x = x_1 + x_2$.

Un submódulo M_1 de M es un sumando directo de M en caso de que exista un submódulo M_2 de M, tal que $M = M_1 \oplus M_2$; tal M_2 es también un sumando directo, y M_1 y M_2 son sumandos directos complementarios o complementos directos.

Lema 2.2. *Sean $f : M \to N$ y $g : N \to M$ homomorfismos, tal que $f \circ g = 1_N$ entonces f es un epimorfismo, g es un monomorfismo y $M = Kerf \oplus Img$.*

Demostración. Veamos que f es epi. Sea $z \in N$ entonces $z = 1_N(z) = f(g(z))$, sea $g(z) = y$ para algún $y \in M$, por tanto existe un $y \in M$ tal que $f(y) = z$, por lo tanto f es epi. Ahora veamos que g es mono, sea $g(y_1) = g(y_2)$, entonces $f(g(y_1)) = f(g(y_2))$, se obtiene $y_1 = 1_N(y_1) = f(g(y_1)) = f(g(y_2)) = 1_N(y_2) = y_2$, por lo tanto g es mono. Ahora mostremos Si $x \in Kerf \cap Img$ entonces $f(x) = 0$ y $x = g(y)$, con $y \in N$, luego $0 = f(x) = f(g(y)) = y$ y como g es homomorfismo entonces $x = g(y) = 0$, así $Kerf \cap Img = \{0\}$. Si $x \in M$ entonces $f(x - g(f(x))) = f(x) - f(g(f(x))) = f(x) - f(x) = 0$, entonces $\forall x \in M$, $x = x - g(f(x)) + g(f(x)) \in Kerf + Img$, por lo tanto $M = Kerf \oplus Img$. $\square$

Definición 2.3. *Si $f : M \to N$ y $g : N \to M$ son homomorfismos con $fg = 1_N$, entonces decimos que f es un epimorfismo que se parte, y también análogamente se dice que g es monomorfismo que se parte.*

Definición 2.4. *Una sucesión exacta corta*

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

se parte en el caso que f sea un monomorfismo que se parte y g sea un epimorfismo que se parte.

Proposición 2.5. *Sea $0 \to M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \to 0$ una sucesión exacta corta en ${}_RM$ los siguientes enunciados son equivalentes:*

a) La sucesión es exacta corta que se parte.

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

c) El epimorfismo $g : M \to M_2$ se parte.

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

e) *Cada homomorfismo* $h : M_1 \to N$, *se factoriza a través de* f.

f) *Cada homomorfismo* $h : N \to M_2$, *se factoriza a través de* g.

$$\begin{tikzcd} & & N \\ 0 \arrow[r] & M_1 \arrow[ur, "h"] \arrow[r, "f"'] & M \arrow[u, dashed, "\overline{h}"'] \end{tikzcd} \qquad \begin{tikzcd} M \arrow[r, "g"] & M_2 \arrow[r] & 0 \\ & N \arrow[u, "h"'] \arrow[ul, dashed, "\overline{h}"] & \end{tikzcd}$$

Demostración. $(a) \Rightarrow (b)$ y $(a) \Rightarrow (c)$ son triviales por definición. $(b) \Rightarrow (d)$ y $(c) \Rightarrow (d)$ son consecuencia del Lema anterior; notemos que (b) y (c) juntos dan (a).

$(d) \Rightarrow (e)$. Supongamos $M = Imf \oplus K$ y $h : M_1 \to N$, donde f es mono, para cada $m \in M$ existen únicos $m_1 \in M_1$ y $k \in K$ tal que $m = f(m_1) + k$, definimos $\overline{h} : M \to N$, por $\overline{h} : m = f(m_1) + k \mapsto h(m_1)$, es fácil ver que $\overline{h}$ es un $R - homomorfismo$. Sea $m_1 \in M_1$, $f(m_1) \in Imf \subseteq M$ luego $\forall k \in K,\ f(m_1) + k = h(m_1)$ por tanto $\overline{h}f = h$, así el diagrama conmuta.

$(d) \Rightarrow (f)$. Supongamos que $M = Kerg \oplus K$ y $h : N \to M_2$, donde $K \cap Kerg = \{0\}$ y $g(M) = g(K)$, notemos $g|_K : K \to M_2$ es isomorfismo, por tanto sea $g_1 : M_2 \to K$ su inverso, entonces $\overline{h} = g_1 h : N \to M$. Sea $n \in N$ entonces $h(n) \in M_2$ luego $g_1(h(n)) \in K$ con $\overline{h}(n) = g_1(h(n))$ pero si $g\overline{h} = gg_1 h = 1_{M_2} h = h$ que así se cumple (f).

$(e) \Rightarrow (b)$. Basta considerar en la hipótesis $h = 1_N$, y $N = M_1$, luego tomando $\overline{h} : m = 1_{M_1}(m_1) + k \mapsto h(m_1)$.

$(f) \Rightarrow (c)$. Se toma $h = 1_{M_2}$. $\square$

Sean M_1 y M_2 módulos. Entonces al producto de módulos $M_1 \times M_2$ se le asocian con la inyección natural y la proyección natural, $\tau_j : M_j \to M_1 \times M_2$ y $\pi_j : M_1 \times M_2 \to M_j$ $(j = 1, 2)$ definidas como $\tau_1(x) = (x, 0)$ $\tau_2(x) = (0, x)$ y $\pi_1(x_1, x_2) = x_1$ $\pi_2(x_1, x_2) = x_2$. Claramente son R-homomorfismos con

$$0 \to M_1 \overset{\tau_1}{\to} M_1 \times M_2 \overset{\pi_2}{\to} M_2 \to 0$$

$0 \to M_2 \xrightarrow{\tau_2} M_1 \times M_2 \xrightarrow{\pi_1} M_1 \to 0$, son exactas, como $\pi_1 \circ \tau_1 = 1_{M_1}$ $\pi_2 \circ \tau_2 = 1_{M_2}$, son exactas cortas. También observemos $\pi_j \circ \tau_i = \delta_{ij} 1_{M_i}$, y $\pi_1 \circ \tau_1 + \pi_2 \circ \tau_2 = 1_{M_1 \times M_2}$.

Proposición 2.6. *Para una sucesión de R-homomorfismos*

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

los siguientes enunciados son equivalentes:

1. *Es sucesión exacta que se parte.*

2. *Existe R-homomorfismos $f_2 : M_2 \longrightarrow M$ y $g_1 : M \longrightarrow M_1$ tal que $0 \longrightarrow M_2 \xrightarrow{f_2} M \xrightarrow{g_1} M_1 \longrightarrow 0$ es exacta corta que se parte, para $i, j \in (1, 2)$ cumple con la propiedad $g_i f_i = \delta_{ij} 1_{M_i}$ y $f_1 g_1 + f_2 g_2 = 1_M$.*

3. *Existe un isomorfismo $h : M_1 \times M_2 \longrightarrow M$ tal que el diagrama conmuta.*

$$\begin{tikzcd}
& & M_1 \times M_2 \arrow[dd, dashed, "h"] \arrow[dr, "\pi_2"] & & \\
0 \arrow[r] & M_1 \arrow[ur, "\tau_1"] \arrow[dr, "f_1"'] & & M_2 \arrow[r] & 0 \\
& & M \arrow[ur, "g_2"'] & &
\end{tikzcd} \tag{2.1}$$

Demostración. 1) $\Rightarrow$ 3). Definimos $h : M_1 \times M_2 \longrightarrow M$, con la regla $h(x_1, x_2) = f_1(x_1) + f_2(x_2)$, donde $f_2 : M_2 \longrightarrow M$ cumple con $g_2 f_2 = 1_{M_2}$, luego por el Lema 1.52, h es isomorfismo.

3) $\Rightarrow$ 2). Dado h isomorfismo, como el diagrama 2.1 es conmutativo, definimos $f_i = h\tau_i$ y $g_i = \pi_i h^{-1}$ para $(i = 1, 2)$ por el digrama 2.1, entonces

$$g_i f_j = (\pi_i h)\left(h^{-1}\tau_j\right) = \pi_i \tau_j = \delta_{ij} 1_{M_i}$$

.

y

$$f_1 g_1 + f_2 g_2 = h\tau_1\pi_1 h^{-1} + h\tau_2\pi_2 h^{-1} =$$
$$h(\tau_1\pi_1 + \tau_2\pi_2) h^{-1} = hh^{-1} = 1_M.$$

2) $\Rightarrow$ 1). Sea $0 \to M_2 \xrightarrow{f_2} M \xrightarrow{g_1} M_1 \to 0$, exacta corta, $g_i f_j = \delta_{ij} 1_{M_i}$ y $f_1 g_1 + f_2 g_2 = 1_M$, por tanto $M = Imf_1 + Imf_2$,

pero como $g_2f_1 = 0$ entonces $Imf_1 \subseteq Kerg_2$ y $g_2f_2 = 1_{M_2}$, entonces $M = Kerg_2 \oplus Imf_2$, y se tiene que

$$Kerg_2 = M \cap Kerg_2 = Imf_1 \cap Kerg_2 + Imf_2 \cap Kerg_2 = Imf_1.$$

Entonces la sucesión $0 \to M_2 \xrightarrow{f_2} M \xrightarrow{g_1} M_1 \to 0$ es exacta en M; donde se tiene $g_1f_1 = 1_{M_1}$ y $g_2f_2 = 1_{M_2}$, entonces es una sucesión que se parte. □

2.1.1 Proyecciones

Sea K un sumando directo de un módulo M con complemento directo K', es decir, $M = K \oplus K'$, entonces definimos $P_K; k + k' \mapsto k$ y $P_{K'}; k + k' \mapsto k'$, donde $k \in K$ y $k' \in K'$, definen epimorfismos $P_K : M \to K$ y $P_{K'} : M \to K'$ llamadas proyecciones de M sobre K y K' respectivamente.

Proposición 2.7. *Si $M = K \oplus K'$, entonces la proyección P_K de M sobre K es el único epimorfismo tal que $M \overset{P_K}{\to} K \to 0$ que satisface:*

$$P_K|_K = 1_K \textit{ y } KerP_K = K'.$$

Demostración. Supongamos que P_K no es la única, por tanto existe $g : M \to K$ homomorfismo tal que $g|_K = 1_K$ y $Kerg = K'$, entonces $\forall k \in K$, $k' \in K'$, $g\,(k + k') = g\,(k) + g\,(k') = k = P_K\,(k + k')$, por lo tanto esta es P_K, así es única. □

Si $M = K \oplus K'$ entonces K' es también un sumando directo de M con complemento K. Si P_K es una proyección de M sobre K, a lo largo de K' entonces la proyección $P_{K'}$ de M sobre K' a lo largo de K, se puede caracterizar $P_{K'}\,(m) = m - P_K\,(m)$ con $m \in M$.

Ahora si $i_K : K \to M$ y $i_{K'} : K' \to M$ son las inclusiones naturales, entonces

$$0 \to K' \overset{i_{K'}}{\to} M \overset{P_k}{\to} K \to 0 \textit{ y } 0 \to K' \overset{i_K}{\to} M \overset{P_{K'}}{\to} K \to 0$$

son sucesiones exactas que se parten.

Proposición 2.8. *Sean $M = K \oplus K'$, P_K proyección de M sobre K a lo largo de K' y sea L un submódulo de M entonces $M = L \oplus K'$ si y sólo si $(P_K|_L) : L \to K$ es isomorfismo.*

Demostración. Sea $L \leq M = K \oplus K'$, entonces $Ker\left(P_K|_L\right) = L \cap Ker\ P_K = L \cap K'$, notemos que $P_K|_L$ es monomorfismo si y sólo si $L \cap K' = 0$. Por otro lado, como $P_K|_K = 1_K$, $KerP_K = K'$ y la ley modular.

$P_K\left(L\right) = P_K\left(L + K'\right) = P_K\left(\left(L + K'\right) \cap \left(K + K'\right)\right)$
$= P_K\left(\left(L + K'\right) + K\right) + P_K\left(K'\right) = P_K\left(\left(L + K'\right) + K\right)$
$= \left(L + K'\right) \cap K$.

Por otro lado $P_K\left(L\right) = K$ si y sólo si $K \subseteq L + K'$ si y sólo si $L + K' = M$. $\square$

2.1.2 Endomorfismos e Idempotentes

Supongamos que ${}_RM = K \oplus K'$ y P_K proyección de M de K a lo largo de K'. Definimos $e_K \in End\left({}_RM\right)$ por $e_K : x \mapsto P_K\left(x\right)$ con $x \in M$ y como $\left(p_K|_K\right) = 1_K$, e_K es un idempotente del anillo de endomorfismos de M, es decir, $e_K = e_K^2 \in End\left({}_RM\right)$ y $K = Me_K$ (e_K *como un operador derecho de* M), entonces cada sumando directo, es la imagen de algún endomorfismo idempotente de M.

Lema 2.9. *Sea e un idempotente en $End\left({}_RM\right)$, entonces $1 - e$ es un idempotente en $End\left(M\right)$ tal que $Ker\ e = \{x \in M | x = x\left(1 - e\right)\} = Im\left(1 - e\right)$ $Im\ e = \{x \in M | x = xe\} = Ker\left(1 - e\right)$ y $M = Me \oplus M\left(1 - e\right)$.*

Demostración. Notemos que, $e^2 = e$ entonces

$$\left(1 - e\right)^2 = \left(1 - e\right)\left(1 - e\right) = 1 - e - e + e^2 = 1 - e,$$

así $1 - e$ es idempotente, pero también $e\left(1 - e\right) = \left(1 - e\right)e = 0$.

Si $y = xe$, entonces $ye = xe^2 = xe$ así $y = ye$, luego se dan las inclusiones:

$Im\ e \subseteq \{x \in M | x = xe\} = \{x \in M | x - xe = 0\}$
$= \{x \in M | x\left(1 - e\right) = 0\} \subseteq Ker\left(1 - e\right)$.

Análogamente

$$Im\left(1 - e\right) \subseteq \{x \in M | x = x\left(1 - e\right)\}$$

$$= \{x \in M | x - x + xe = 0\} = \{x \in M | xe = 0\} \subseteq Ker\ e$$

.

Notemos que $x = xe + x(1-e)$ para todo $x \in M$, entonces $M = Me + M(1-e)$; $Me \cap M(1-e) = \{0\}$, ya que $xe = y(1-e)$, $xe = xe^2 = y(1-e)e = 0$, entonces $xe = 0$. Por tanto $M = Me \oplus M(1-e)$ y así se cumple la igualdad. Finalmente si $x \in Ker\ e$, entonces $x = z_1 + z_2$, con $z_1 = m_1 e$ y $z_2 = m_2(1-e)$, como $0 = xe = m_1 e + m_2(1-e)e$, tenemos que $m_1 e = 0$, por tanto $x = z_1 \in M(1-e)$, así se cumple $Ker\ e = Im(1-e)$.

Análogamente se demuestra $Ker(1-e) = Im\ e$. □

Proposición 2.10. *Si ${}_RM = K \oplus K'$ entonces existe un único idempotente $e_K \in End({}_RM)$ tal que $K = Me_K$ $K' = M(1-e_K)$.*

Demostración. De la Proposición 2.7, se obtiene la unicidad, por lo anterior $e_K \in End({}_RM)$ tal que $x \mapsto xe$, es la proyección de M sobre Me a lo largo de $M(1-e)$. □

Corolario 2.11. *Un submódulo $K \leq M$ es un sumando directo de M si y sólo si $K = Ime$ para algún idempotente en el anillo de endomorfismos de M.*

Es claro que cualquier módulo distinto del cero tiene dos sumandos directos, 0 y el mismo M.

Definición 2.12. *Un módulo no cero M es indescomponible si* 0 *y M son los únicos sumandos directos.*

Definición 2.13. *Un par de idempotentes e_1 y e_2 en un anillo R, se dice que son ortogonales si $e_1 e_2 = 0 = e_2 e_1$.*

Definición 2.14. *Un idempotente $e \in R$ es llamado idempotente primitivo en el caso de que $e \neq 0$ y para cada par e_1,e_2 de idempotentes ortogonales $e = e_1 + e_2$ implica que $e_1 = 0$ o $e_2 = 0$.*

Si $e = e^2 \in R$ entonces e y $1-e$ son idempotentes ortogonales tal que $1 = e + (1-e)$.

Proposición 2.15. *Si M es un módulo no cero, entonces los siguientes enunciados son equivalentes:*

1. *M es indescomponible.*

2. *0 y 1 son los únicos idempotentes en* $End\,(M)$.

3. *1 es un idempotente primitivo en* $End\,(M)$.

DEMOSTRACIÓN. 1)⇒ 2) Si M es indescomponible entonces los únicos sumandos directos son 0 y M, luego existe $e \in End\,(M)$ tal que $M = Me$ y $0 = M\,(1-e)$, luego $e = 1$ y $1 - e = 0$ y son los únicos idempotentes en $End\,(M)$.

2)⇒ 3) Si $1, 0 \in End\,(M)$ son los únicos idempotentes notemos que $1 = 1 + 0$, entonces por definición 1 es idempotente primitivo en $End\,(M)$.

3)⇒ 1) Si 1 es idempotente primitivo y e idempotente, como $1 = e + (1 - e)$, entonces $1 - e = 0$, es decir, $e = 1$ o sea los únicos idempotentes son 0 y 1, por tanto M es indescomponible, pues $M = M\,(1) \oplus M\,(0)$. □

2.1.3 Submódulos Esencial y Superfluo

Un submódulo K es un sumando directo de M, si y sólo si existe un submódulo K_1 de M tal que $K \cap K_1 = \{0\}$ y $K + K_1 = M$.

Para cualquier submódulo K de M, también podemos encontrar submódulos que satisfacen con K las condiciones anteriores, por ejemplo: $K \cap \{0\} = \{0\}$ y $K + M = M$.

Definición 2.16. *Un submódulo K de M es esencial en M si para cada submódulo L de M tal que $K \cap L = \{0\}$ se puede implicar que $L = \{0\}$. Si tal es el caso se denota por $K \trianglelefteq M$.*

Definición 2.17. *Un submódulo K de M es superfluo en M si para cada submódulo L de M tal que $K + L = M$ se pueda implicar que $L = M$. Si tal es el caso se denotara por $K \ll M$.*

Definición 2.18. *Un monomorfismo $f : K \to M$ se dice que es esencial en el caso en que $Imf \trianglelefteq M$. Un epimorfismo $f : M \to K$ es superfluo en caso $Kerg \ll M$.*

Proposición 2.19. *Para un submódulo K de M, las siguientes afirmaciones son equivalentes:*

1. $K \trianglelefteq M$.

2. *La transformación inclusión $i_K : K \to M$ es un monomorfismo esencial.*

3. *Para cada módulo N y para cada $h \in Hom\,(M, N)$, $(Ker h) \cap K = \{0\}$ implica $Ker h = \{0\}$.*

Demostración. a) $\Leftrightarrow$ b) Es clara de la definición. a) $\Rightarrow$ c) es trivial.

c) $\Rightarrow$ a) Supongamos que $L \leq M$ un submódulo, tal que $K \cap L = \{0\}$. Sea $\eta_L : M \to M/L$ el epimorfismo natural. Entonces $Ker\ \eta_L \cap K = \{0\}$, por tanto aplicando c), $Ker\ \eta_L = L = \{0\}$, así K es esencial. $\square$

Sabemos que si f y h son homomorfismos tal que $f \circ h$ es monomorfismo, entonces claramente h es también monomorfismo. En el siguiente Corolario se muestra una propiedad análoga que caracteriza a los monomorfismos esenciales.

Corolario 2.20. *Un monomorfismo $f : L \to M$, es esencial si y sólo si, para todo homomorfismo h, si hf es mono, entonces h es mono.*

Demostración. $\Rightarrow$) Sea $f : L \to M$ tal que $Im\ f \trianglelefteq M$ y sea h homomorfismo tal que hf es mono, entonces $Ker\ h \leq M$, si $Im\ f \cap Ker\ h = \{0\}$ entonces $Ker\ h = \{0\}$, pero si suponemos que $Im\ f \cap Ker\ h \neq \{0\}$ entonces existe $x \in Im\ f \cap Ker\ h$ no cero, implica que existe $l \in L$ tal que $f\,(l) = x$ y $h\,(x) = 0$, por tanto $h\,(f\,(l)) = h\,(x) = 0$, entonces $l \in Ker\ hf = \{0\}$, por lo tanto $x = f\,(0) = 0$, se llega a una contradicción, luego h es mono.

$\Leftarrow$) Sea $S \leq M$ tal que $S \cap Im\ f = \{0\}$, sólo falta ver que $S = \{0\}$. Sea $h : M \to M/S$ el epimorfismo natural, ahora $(h \circ f)\,(x) = h\,(f\,(x)) = 0$, entonces $f\,(x) \in S$, entonces $f\,(x) = 0$, es decir $x = 0$, así que $h \circ f$ es mono, por tanto h es mono y $S = \{0\}$. $\square$

Tenemos los duales de la Proposición anterior y el Corolario.

Proposición 2.21. *Para un submódulo K de M, las siguientes afirmaciones son equivalentes:*

1. *$K \ll M$.*

2. *La transformación natural $p_K : M \to M/K$ es un epimorfismo superfluo.*

3. *Para cada módulo N y para cada $h \in Hom(N, M)$, sí $(Im\ h) + K = M$, entonces $Im\ h = M$.*

Corolario 2.22. *Un epimorfismo $g : M \to N$ es superfluo si y sólo si para todo homomorfismo h,si gh es epi, entonces h es epi.*

Proposición 2.23. *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. 1) Sea $K \trianglelefteq M$ y supongamos que $\{0\} \neq L \leq N$ y $L \cap K \neq \{0\}$, en particular, como $L \leq M$, lo anterior no puede suceder, por tanto $K \trianglelefteq N$. Análogamente cuando tomamos $L \leq M$ y $N \cap L = \{0\}$, entonces $K \cap L = \{0\}$, por tanto $L = \{0\}$ así $N \trianglelefteq M$. Ahora, sea $K \cap L = \{0\}$ con $L \leq M$. Como $K \trianglelefteq N$ y $K \cap L \cap N = \{0\}$ entonces $L \cap N = \{0\}$, pero $N \trianglelefteq M$, entonces $L = \{0\}$.

2) La suficiencia se sigue de 1). Para la necesidad, supongamos que $H \trianglelefteq M$ y $K \trianglelefteq M$. Si $L \leq M$ con $L \cap (H \cap K) = \{0\}$, entonces $L \cap H = \{0\}$ por que $HK \trianglelefteq M$, de donde $L = \{0\}$, por que $H \trianglelefteq M$. $\square$

Ahora veamos la Proposición dual.

Proposición 2.24. *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. *$H + M \ll M$ si y sólo si $H \ll M$ y $K \ll M$*

Demostración. La demostración es dual a la Proposición 2.23. $\square$

Lema 2.25. *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 $L \leq N$ y supongamos que $L + f(K) = N$, sea $z \in M$, tal que $f(z) = l + f(k)$, entonces $f(z - k) = l$, por tanto $z - k \in f^{\leftarrow}(L)$ como $z = z - k + k$, $z \in f^{\leftarrow}(L) + K$, entonces $f^{\leftarrow}(L) + K = M$, con $K \ll M$ luego $K \leq M = f^{\leftarrow}(L)$ entonces $f(K) \leq L$, así $L = N$. $\square$

Lema 2.26. *Un submódulo $K \leq M$ es esencial en M si y sólo si para cada $0 \neq x \in M$ existe $r \in R$ tal que $0 \neq rx \in K$.*

Demostración. $\Rightarrow$) Si $K \trianglelefteq M$ y sea $x \in M$ distinto de cero, entonces $Rx \neq \{0\}$, así que $Rx \cap K \neq \{0\}$, existe $r \in R$ tal que $rx \neq 0$.

$\Leftarrow$) Sea $x \in L \leq M$ distinto del cero, entonces por la hipótesis existe un $r \in R$ tal que $rx \neq 0$, que esta en $K \cap L$, $K \cap L \neq \{0\}$, por tanto K es esencial. □

Proposición 2.27. *Sea $K_1 \leq M_1 \leq M$ y $K_2 \leq M_2 \leq M$ y $M = M_1 \oplus M_2$ entonces*

1. $K_1 \oplus K_2 \ll M_1 \oplus M_2 \Longleftrightarrow K_1 \ll M_1$ *y* $K_2 \ll M_2$*,*
2. $K_1 \oplus K_2 \trianglelefteq M_1 \oplus M_2 \Longleftrightarrow K_1 \trianglelefteq M_1$ *y* $K_2 \trianglelefteq M_2$*.*

Demostración. 1) Sea $p_i : M \to M_i$ la proyección de M sobre M_i a lo largo de M_j con $i \neq j$. Entonces $K_i = p_i(K_i)$. Que $K_1 \ll M_1$ y $K_2 \ll M_2$ se sigue aplicando el Lema 2.25. Para el reciproco si $K_i \ll M_i \leq M$, entonces por el Lema 2.25 y por la Proposición 2.24.2, $K_1 \oplus K_2 = K_1 + K_2 \ll M$, ya que $K_i \ll M$.

2) Sea $K_1 \cap L_1 = \{0\}$ para algún $L_1 \leq M_1$ y $L_1 \neq \{0\}$. Observemos que
$$(K_1 + K_2) \cap L_1 = \{0\}.$$
Si $k_1 \in K_1$ y $k_2 \in K_2$ y $l_1 \in L_1$ con $k_1 + k_2 = l_1$ entonces $k_2 = l_1 - k_1 \in M_1 \cap M_2 = \{0\}$. Así que $L_1 = \{0\}$

Para la suficiencia, tenemos que $K_i \trianglelefteq M_i$ y $0 \neq x_i \in M_i$ entonces por el Lema 2.26 existe un $r_1 \in R$ tal que $0 \neq r_1x_1 \in K_1$. Si $r_1x_2 \in K_2$ entonces, por la independencia $0 \neq r_1x_1 + r_1x_2 \in K_1 \oplus K_2$. Si r_1x_2 no esta en K_2 entonces por el Lema 2.26, existe $r_2 \in R$ tal que $0 \neq r_2r_1x_2$, como $r_2r_1(x_1 + x_2) \in K_1 + K_2$, así
$$0 \neq r_2r_1x_1 + r_2r_1x_2 \in K_1 \oplus K_2.$$
Por lo tanto
$$K_1 \oplus K_2 \trianglelefteq M_1 \oplus M_2.$$
□

Definición 2.28. *Sea N un submódulo de M. Si $N_1 \leq M$ es maximal con respecto a la propiedad $N \cap N_1 = \{0\}$, entonces se dice que N_1 es un M-complemento de N.*

Recordemos unos conceptos necesarios de la teoría de conjuntos: Un conjunto $\mathcal{A}$ se llama parcialmente ordenado, o se dice que tiene un orden parcial, si se tiene una relación $\leq$ en $\mathcal{A}$ tal que

1. $\leq$ es reflexiva, es decir, $x \leq x$ para todo $x \in \mathcal{A}$.

2. $\leq$ es transitiva, es decir, $x \leq y$ y $y \leq z \Rightarrow x \leq z$.

3. Si $x \leq y$ y $y \leq x$, $\Rightarrow x = y$.

   El orden parcial $\leq$ se llama orden total, y el conjunto $\mathcal{A}$ se llamará entonces un conjunto totalmente ordenado o una cadena, si además $\leq$ satisface que:

4. Para todo $x, y \in \mathcal{A}$, $x \leq y$ ó $y \leq x$.

Dado un conjunto parcialmente ordenado $(\mathcal{A}, \leq)$, un elemento $\alpha \in \mathcal{A}$ se llama un elemento maximal si no existe $x \in \mathcal{A}$, $x \neq \alpha$ tal que $\alpha \leq x$.

El Lema de Zorn es un resultado de la teoría de conjuntos y es equivalente al axioma de elección.

Lema 2.29 (Lema de Zorn)**.** *Sea $(\mathcal{A}, \leq)$ un conjunto parcialmente ordenado y supongamos que toda cadena $\mathcal{C} \subseteq \mathcal{A}$ tiene una cota superior en $\mathcal{A}$, entonces $\mathcal{A}$ tiene al menos un elemento maximal.*

Proposición 2.30. *Cada submódulo $N \leq M$ tiene un M-complemento. Si N' es M-complemento de N, entonces*

1. $N \oplus N' \trianglelefteq M$.

2. $(N \oplus N')/N' \trianglelefteq M/N'$.

DEMOSTRACIÓN. Notemos que el Lema de Zorn, asegura la existencia un maximal N', en la familia de los submódulos K de M, tales que $K \cap N = \{0\}$.

1) Si $L \leq M$ distinto de cero y $(N \oplus N') \cap L = \{0\}$, entonces se tiene que $N \cap (N' + L) = \{0\}$, una contradicción, luego $L = \{0\}$.

2) Supongamos que $N' \leq L$ y $L/N' \cap (N \oplus N')/N' = \{0\}$, entonces $L \cap (N + N') \leq N'$, entonces por la ley modular $(L \cap N) \oplus N' = L \cap (N + N') \leq N'$, entonces $(L \cap N) \oplus N' = N'$, es decir, $L \cap N = \{0\}$ y por la maximalidad de N', entonces $L = N'$. $\square$

2.2 Producto Directo

El producto cartesiano $\Pi_A M_\alpha = \{x \mid x : A \to \cup M_\alpha \textit{ tal que } x(\alpha) \in M_\alpha\}$ de una familia de módulos $(M_\alpha)_{\alpha \in A}$ es también un R-módulo con las operaciones definidas coordenada a coordenada. Si π_α denota la proyección α-esima, $\pi_\alpha : \Pi M_\alpha \to M_\alpha$, con $\pi_\alpha(x) = x(\alpha)$, entonces para cada par x, y en el producto y cada $r \in R$: $\pi_\alpha(x + y) = \pi_\alpha(x) + \pi_\alpha(y)$, $\pi_\alpha(rx) = r\pi_\alpha(x)$.

Notemos que para toda $x, y \in \Pi_{\alpha \in A} M_\alpha$, $x = y \Leftrightarrow \pi_\alpha(x) = \pi_\alpha(y)$ para toda $\alpha \in A$.

Esta transformación está bien definida y estas operaciones claramente inducen una estructura de módulo. Una notación para las A-tuplas sobre las operaciones del producto esta dadas por

$$(x_\alpha) + (y_\alpha) = (x_\alpha + y_\alpha), \quad r(x_\alpha) = (rx_\alpha)$$

.

El módulo que resulta es llamado el producto directo de $(M_\alpha)_{\alpha \in A}$, será denotado por $\Pi_A M_\alpha$, o $\Pi_{i=1}^n M_i$ o $M_1 \times M_2 \times \ldots \times M_n$, en el caso finito. Si $M_\alpha = M$ para todo $\alpha \in A$ se escribira $M^A = \Pi_A M$. Esto es simplemente el conjunto de todas las funciones de A a M con la operación coordenada a coordenada. Si $A = \emptyset$, el producto tiene exactamente un elemento y también $\Pi_\emptyset M_\alpha = \{0\} = M^\emptyset$.

Proposición 2.31. *Sea $(M_\alpha)_{\alpha \in A}$ un conjunto indexado de módulos. Si N es un módulo y $(f_\alpha)_{\alpha \in A}$ es un conjunto de homomorfismos $f_\alpha : N \to M_\alpha$, entonces existe un único homomorfismo $f : N \to \Pi_A M_\alpha$ tal que para cada $\alpha \in A$ el siguiente diagrama conmuta.*

$$\begin{tikzcd}
N \arrow[rr, "f"] \arrow[dr, "f_\alpha"'] & & \Pi_A M_\alpha \arrow[dl, "\pi_\alpha"] \\
& M_\alpha &
\end{tikzcd}$$

Demostración. Para cada $x \in N$ definimos $f(x) \in \Pi_A M_\alpha$ coordenada a coordenada por $\pi_\alpha f(x) = f_\alpha(x)$. π_α y f_α son homomorfismos, se sigue que también $f : x \mapsto f(x)$ define un homomorfismo de $N \to \Pi_A M_\alpha$. Por otra parte, $\pi_\alpha f = f_\alpha$ para toda $\alpha \in A$. Ahora supongamos que $g : N \to \Pi_A M_\alpha$ es un homomorfismo tal que $\pi_\alpha g(x) = f_\alpha(x)$ para toda $\alpha \in A$, entonces para cada $\alpha \in A$ tenemos $\pi_\alpha g(x) = \pi_\alpha f(x)$ luego $g(x) = f(x)$, así $f = g$. □

El único homomorfismo $f : N \to \Pi_A M_\alpha$ en la Proposición anterior se llama el *producto directo* de $(f_\alpha)_{\alpha \in A}$ y también suele denotarse por $f = \Pi_A f_\alpha$. Está caracterizado por ser el único homomorfismo tal que $\pi_\alpha(\Pi_A f_\alpha) = f_\alpha$, para cada $\alpha \in A$.

Corolario 2.32. *Sea $f_\alpha : N \to M_\alpha$ con $\alpha \in A$ un conjunto indexado de homomorfismos entonces*

$$Ker(\Pi_A f_\alpha) = \cap_A Ker f_\alpha$$

Demostración. Sean $f = \Pi_A f_\alpha$ y $x \in N$ entonces $f(x) = 0 = (\Pi_A f_\alpha)(x)$ si y sólo si $\pi_\alpha f(x) = 0$ para todo $\alpha \in A$ si y sólo si $f_\alpha(x) = 0$ para todo $\alpha \in A$. □

Si $B \subseteq A$ entonces tenemos los dos productos $\Pi_B M_\beta$ y $\Pi_A M_\alpha$, si $x \in \Pi_B M_\beta$, entonces x es una función con dominio B y tiene una única extensión para un elemento $\overline{x} \in \Pi_A M_\alpha$ tal que $\overline{x}(\alpha) = 0$ para todo $\alpha \notin B$. Entonces existe una transformación $\tau_B : \Pi_B M_\beta \to \Pi_A M_\alpha$, definida por $\tau_B : x \mapsto \overline{x}$. Claramente τ_B es un R-monomorfismo cuya imagen es un submódulo $\Pi_A M_\alpha$, compuesto por las $A - tuplas$ que se anulan fuera de B. Por otro lado para cada $x \in \Pi_A M_\alpha$, o función con dominio A, la restricción $(x \mid B)$ es un elemento de $\Pi_B M_\beta$; claramente $\pi_B : \Pi_A M_\alpha \to \Pi_B M_\beta$, definida por $\pi_B : x \mapsto (x \mid B)$ es un R-homomorfismo de $\Pi_A M_\alpha$ sobre $\Pi_B M_\beta$.

Proposición 2.33. *Sea $(M_\alpha)_{\alpha \in A}$ un conjunto de módulos indexados y sea A la unión ajena de B y C. entonces*

1. $\pi_B \tau_B = 1_{\Pi_B M_\beta}$
2. $\Pi_A M_\alpha = \tau(\Pi_B M_\beta) \oplus \tau(\Pi_C M_\delta)$
3. $0 \to \Pi_B M_\beta \overset{\tau_B}{\to} \Pi_A M_\alpha \overset{\Pi_C}{\to} \Pi_C M_\delta \to 0$ *es exacta que se parte.*

Mediante la Propiedad universal de morfismos de $\Pi_A M_\alpha$ descrita en la Proposición 2.31, caracterizararemos el producto directo de una familia de módulos.

Informalmente, un producto $(M,(p_\alpha))_{\alpha\in A}$ de la familia $(M_\alpha)_{\alpha\in A}$, es una estructura que, dada cualquier colección de homomorfismos $(f_\alpha : N \to M_\alpha)$, produce un único homomorfismo, del módulo M a los de M_α, que se factoriza con p_α, para generar los f_α.

Definición 2.34. *Dada $(M_\alpha)_{\alpha\in A}$ una familia de módulos, al par, consistente en $\big(M,(p_\alpha)_{\alpha\in A}\big)$ con M módulo y $p_\alpha : M \to M_\alpha$ con $\alpha \in A$ homomorfismo, es llamado el producto directo de $(M_\alpha)_{\alpha\in A}$, en caso, que para cada módulo N y cada conjunto de homomorfismos $f_\alpha : N \to M_\alpha$ existe un único homomorfismo $f : N \to M$ tal que $f_\alpha = p_\alpha f$ con $\alpha \in A$.*

Así que la pareja $(\Pi_A M_\alpha,(\pi_\alpha)_{\alpha\in A})$ es un producto de la familia $(M_\alpha)_{\alpha\in A}$.

En general tenemos que si $\big(M,(p_\alpha)_{\alpha\in A}\big)$, es un producto de la familia $(M_\alpha)_{\alpha\in A}$, y tenemos $\big(M',(p'_\alpha)_{\alpha\in A}\big)$, donde cada $p'_\alpha : M' \to M_\alpha$ es un R-homomorfismo con $\alpha \in A$, entonces existe un único homomorfismo $p : M' \to M$ tal que $p_\alpha p = p'_\alpha$ para cada $\alpha \in A$. Esta propiedad nos asegura un cierto tipo de unicidad en los productos. En el Teorema siguiente, se explica lo anterior.

Teorema 2.35. *Sea $\big(M,(p_\alpha)_{\alpha\in A}\big)$ un producto de $(M_\alpha)_{\alpha\in A}$. Entonces un par $\big(M',(p'_\alpha)_{\alpha\in A}\big)$, donde cada $p'_\alpha : M' \to M_\alpha$ es un R-homomorfismo con $\alpha \in A$, es también un producto de $(M_\alpha)_{\alpha\in A}$ si y sólo si existe un único isomorfismo $p : M' \to M$ tal que $p_\alpha p = p'_\alpha$ para cada $\alpha \in A$. Es decir el siguiente diagrama conmuta:*

$$\begin{tikzcd} M' \arrow[rr, "p"] \arrow[dr, "p'_\alpha"'] & & M \arrow[dl, "p_\alpha"] \\ & M_\alpha & \end{tikzcd}$$

Demostración.

($\Rightarrow$) Si $\big(M',(p'_\alpha)_{\alpha\in A}\big)$ también es un producto entonces existen un únicos homomorfismos $p' : M \to M'$, $p : M' \to M$ con $p'_\alpha p' = p_\alpha$ y $p_\alpha p = p'_\alpha$, para cada $\alpha \in A$. Entonces $p'_\alpha = p_\alpha p = p'_\alpha p' p$. pero

$p'_\alpha = 1_{M'}p'_\alpha$ también por unicidad, $p'p = 1_{M'}$, y esto pasa similarmente $pp' = 1_M$.

$$\begin{tikzcd}
M' \arrow[r, "p'p"] \arrow[d, "p'_\alpha"] & M' \arrow[dl, "p'_\alpha"] \\
M_\alpha &
\end{tikzcd}$$

($\Leftarrow$) Supongamos que $f_\alpha : N \to M_\alpha$ con $\alpha \in A$ es un homomorfismo donde $\left(M, (p_\alpha)_{\alpha\in A}\right)$ es un producto. Entonces existe un único homomorfismo h tal que el diagrama conmuta (abajo), para cada $\alpha \in A$. Si suponemos que p es un isomorfismo tal que conmutan los diagramas y tomando $f = p^{-1}h$ tenemos que $\left(M', (p'_\alpha)_{\alpha\in A}\right)$ es un producto, ya que $p'_\alpha f = p'_\alpha p^{-1}h = p_\alpha h = f_\alpha$.

$$\begin{tikzcd}
N \arrow[rr, dashed, "h"] \arrow[dr, dashed, "f"] \arrow[ddr, "f_\alpha"'] & & M \arrow[ddl, "p_\alpha"] \\
& M' \arrow[ur, "p"'] \arrow[d, "p'_\alpha"] & \\
& M_\alpha &
\end{tikzcd}$$

$\square$

Ejemplo 2.36. *Sea V un espacio vectorial de dimensión 2 sobre un campo $\mathbb{K}$, y sea $\{x_1, x_2\}$ una base de V, si (p_1, p_2) es un funcional lineal con núcleo $(\mathbb{K}x_1, \mathbb{K}x_2)$ entonces $(V, (p_1, p_2))$, es un producto de $(\mathbb{K}, \mathbb{K})$.*

Ejemplo 2.37. *Consideremos el grupo abeliano $\mathbb{Z}_{30}$, los residuos módulo 2,3 y 5 respectivamente, nos proporcionan los epimorfismos*

$$p_\alpha : \mathbb{Z}_{30} \to \mathbb{Z}_\alpha,\ (\alpha = 2, 3 \text{ y } 5)\,(p_\alpha\,(x + 30\mathbb{Z}) = x + \alpha\mathbb{Z})\,.$$

La Proposición 2.31 asegura la existencia de un homomorfismo p de $\mathbb{Z}_{30}$ para el producto $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ tal que $p_\alpha = \pi_\alpha p$ con $\alpha = 2, 3, 5$, donde π_α es la $\alpha-$esima proyección del producto de la Proposición 2.31.

$$Kerp = Kerp_2 \cap Kerp_3 \cap Kerp_5 = 2\mathbb{Z}_{30} \cap 3\mathbb{Z}_{30} \cap 5\mathbb{Z}_{30} = \{0\}$$

Entonces p es un monomorfismo. Como $\mathbb{Z}_{30}$ y $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ tienen la misma cardinalidad, p es un isomorfismo, esto implica por el Teorema 2.35 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 muy diferentes.

2.2.1 Coproducto

Ahora daremos la versión dual del producto directo de $(M_\alpha)_{\alpha\in A}$, es decir, el resultado de invertir las flechas.

Formalmente, un par $\left(M, (j_\alpha)_{\alpha\in A}\right)$, consistiendo de un módulo M y homomorfismos $j_\alpha : M_\alpha \to M$, es un coproducto (la suma directa) de los $(M_\alpha)_{\alpha\in A}$ en el caso, en que, dado un N módulo y un conjunto de homomorfismos $f_\alpha : M_\alpha \to N$, existe un único homomorfismo $f : M \to N$ tal que $f_\alpha = f j_\alpha$, con $\alpha \in A$. El siguiente resultado que se obtiene de voltear las flechas en el Teorema 2.35 establece que si existe el suma directa, ésta es única, salvo isomorfismos.

Teorema 2.38. *Sea $\left(M, (j_\alpha)_{\alpha\in A}\right)$ una suma directa de los módulos $(M_\alpha)_{\alpha\in A}$. Entonces un par $\left(M', (j'_\alpha)_{\alpha\in A}\right)$ donde cada $j'_\alpha : M_\alpha \to M'$ es un R-homomorfismo, es también una suma directa de $(M_\alpha)_{\alpha\in A}$ si y sólo si existe un único isomorfismo $j : M \to M'$ tal que $j j_\alpha = j'_\alpha$ para cada $\alpha \in A$.*

$$\begin{tikzcd} M' & & M \arrow[ll, "j"'] \\ & M_\alpha \arrow[ul, "j'_\alpha"] \arrow[ur, "j_\alpha"'] & \end{tikzcd}$$

2.2.2 Sumando Directo Externo

Un elemento $x \in \Pi_A M_\alpha$ es cero para casi todos $\alpha \in A$, si el soporte es finito, es decir el conjunto

$$S(x) = \{\alpha \in A | x(\alpha) = \pi_\alpha(x) \neq 0\}$$

es finito. Estos conjuntos cumplen: $S(x + y) \subseteq S(x) \cup S(y)$ y $S(rx) \subseteq S(x)$. Se sigue, que

$$\oplus_A M_\alpha = \{x \in \Pi_A M_\alpha | x \, \textit{es casi siempre cero}\}$$

es un submódulo de $\Pi_A M_\alpha$.

Este submódulo es la suma directa de $(M_\alpha)_{\alpha\in A}$; después veremos que el término "suma directa" es justificado. Usaremos $\oplus_{i=1}^{n} M_i$ en el caso finito. Si A es finito entonces en la suma directa es el producto cartesiano.

Por otra parte, si $M_\alpha = M$ para todo $\alpha \in A$, entonces $M^A = \oplus_A M$ designa la suma directa externa de A copias de M.

En general, para conjunto indexado los $(M_\alpha)_{\alpha\in A}$ y para cada $\alpha \in A$, la imagen de $\tau_\alpha (M_\alpha)$ es el conjunto de $x \in \Pi_A M_\alpha$ con $S(x) \subseteq \{\alpha\}$. Por otro lado, $x \in \Pi_A M_\alpha$ tiene soporte finito, si y sólo si es una suma finita de elementos cuyo soporte es a lo más un singular. Así, $\oplus_A M_\alpha$ es el submódulo de $\Pi_A M_\alpha$, generado por submódulos, de la forma $\tau_\alpha (M_\alpha)$. Además, cada $\tau_\alpha : M_\alpha \to \oplus_A M_\alpha$ es un monomorfismo y $\pi_\alpha : \oplus M_\alpha \to M_\alpha$ es un epimorfismo. Supongamos que N, es un módulo y que $(f_\alpha)_{\alpha\in A}$ es un conjunto indexado de homomorfismos $f_\alpha : M_\alpha \to N \quad (\alpha \in A)$. Ya que para cada $x \in \oplus_A M_\alpha$, su soporte, $S(x) = \{\alpha \in A |\ \pi_\alpha (x) \neq 0\}$ es finito, existe una función $f : \oplus_A M_\alpha \to N$ de finida por

$$f(x) = \sum_{\alpha\in S(x)} f_\alpha \pi_\alpha (x)$$

donde la f_α y π_α son homomorfismos y $f(x) = 0$ si $S(x) = \emptyset$, luego f es homomorfismo. Llamaremos a f la suma directa de $(f_\alpha)_{\alpha\in A}$ y escribiremos $f = \oplus_\alpha f_\alpha$, y para cada $x = (x_\alpha)_{\alpha\in A} \in \oplus_A M_\alpha$, $f(x) = \sum_A f_\alpha (x_\alpha)$.

Proposición 2.39. *Sea $(M_\alpha)_{\alpha\in A}$ un conjunto indexado de módulos. Sea N un módulo y $(f_\alpha)_{\alpha\in A}$ una clase de homomorfismos indexados $f_\alpha : M_\alpha \to N$ para cada $\alpha \in A$. Entonces existe un único homomorfismo $f : \oplus_A M_\alpha \to N$ (necesariamente $f = \oplus_A f_\alpha$) tal que el siguiente diagrama conmuta para cada $\alpha \in A$. Así $\left(\oplus_A M_\alpha, (\tau_\alpha)_{\alpha\in A}\right)$ es suma directa de los $(M_\alpha)_{\alpha\in A}$.*

$$\begin{tikzcd}
\oplus_A M_\alpha \arrow[rr, "f"] & & N \\
& M_\alpha \arrow[ul, "\tau_\alpha"] \arrow[ur, "f_\alpha"'] &
\end{tikzcd}$$

Demostración. En vista de nuestras observaciones anteriores sólo bastara ver la unicidad. Pero está suma $f = \oplus_A f_\alpha$ es la única que cumple con las propiedades deseadas. □

Supongamos que $f = \oplus_A f_\alpha$, entonces se tiene $f\tau_\alpha = f_\alpha$ y así es claro que $Imf_\alpha \leq Imf$. La conclusión sera inmediata de la definición de sumando directo.

Proposición 2.40. *Si $f = \oplus_A f_\alpha$ es la suma directa de los homomorfismos $f_\alpha : M_\alpha \to N$, entonces*

$$Imf = \Sigma_A Imf_\alpha$$

.

Supongamos $B \subseteq A$. Entonces es fácil checar que la restricción de τ_α en $\oplus_B M_\beta$ es un homomorfismo en la suma directa $\oplus_A M_\alpha$. Similarmente la restricción de π_β sobre $\oplus_A M_\alpha$ es un epimorfismo sobre el sumando directo $\oplus_B M_\beta$.

Proposición 2.41. *Sea $(M_\alpha)_{\alpha\in A}$ un conjunto indexado de módulos y sea A la unión ajena de B y C entonces*

1. $\pi_\beta \tau_\beta = 1_{\Pi_B M_\beta}$

2. $\oplus_A M_\alpha = \tau_\beta(\oplus_B M_\beta) \oplus \tau_C(\oplus_C M_\lambda)$.

3. $0 \to \oplus_B M_\beta \overset{\tau_\beta}{\to} \oplus_A M_\alpha \overset{\pi_\alpha}{\to} \oplus_C M_\lambda \to 0$ *es exacta corta que se parte.*

2.2.3 Sumando Directo Interno

Sea M_1 y M_2 submódulos de un módulo M, y sea $i_1 : M_1 \to M$ y $i_2 : M_2 \to M$ sus inclusiones. Entonces M es un sumando directo interno de M_1 y M_2 si y sólo si en nuestra terminología actual $i_1 \oplus i_2$ es un isomorfismo. Y en virtud de las Proposiciones anteriores, son equivalentes a que $(M, (i_1, i_2))$ es una suma directa de $\{M_1, M_2\}$.

Más general, supongamos que los $(M_\alpha)_{\alpha\in A}$ es un conjunto indexado de submódulos de un módulo M. Sea

$$i_\alpha : M_\alpha \to M \quad (\alpha \in A)$$

las correspondientes transformaciones inclusión. Generalizando la definición decimos que M es una suma directa interna de los submódulos $(M_\alpha)_{\alpha\in A}$ en el caso en que la transformación suma directa de

$$i = \oplus_A i_\alpha : \oplus_A M_\alpha \to M$$

es un isomorfismo. Esta condición se cumple, si y sólo si cada $x \in M$ tiene una única representación como una suma $x = \Sigma_A x_\alpha$, donde $x_\alpha \in M_\alpha$ es cero para casi todas los $\alpha \in A$. Con esta nueva notación de sumando nosotros tenemos que, como i es un R-homomorfismo:

$$\Sigma_A x_\alpha + \Sigma_A y_\alpha = \Sigma_A (x_\alpha + y_\alpha) \quad y \quad r(\Sigma_A x_\alpha) = \Sigma_A r x_\alpha$$

También si $f : M \to N$ es un homomorfismo, entonces ya que cada uno de estos $\Sigma_A x_\alpha$ es una suma finita en M.

$$f(\Sigma_A x_\alpha) = \Sigma_A f(x_\alpha)$$

. En otras palabras si M es una suma directa interna de $(M_\alpha)_{\alpha\in A}$, entonces nosotros podremos estudiar a M coordenada a coordenada.

Sea $(M_\alpha)_{\alpha\in A}$ un conjunto indexado de submódulos de M con sus transformaciones inclusión $(i_\alpha)_{\alpha\in A}$. Entonces por la Proposición 2.40 tenemos

$$Im(\oplus_A i_\alpha) = \Sigma_A Im i_\alpha = \Sigma_A M_\alpha$$

El cual puede ser o no un epimorfismo, si la suma directa de transformaciones $i = \oplus_A i_\alpha$ es monomorfismo, entonces el submódulo $\Sigma_A M_\alpha$ es una suma directa interna de los submódulos $(M_\alpha)_{\alpha\in A}$. Como para el caso de dos submódulos, podemos caracterizar estos en la red de los submódulos.

Definición 2.42. *Sea $(M_\alpha)_{\alpha\in A}$ familia de submódulos de M. Decimos que $(M_\alpha)_{\alpha\in A}$ es independiente en el caso de que para cada $\alpha \in A$, $M_\alpha \cap (\Sigma_{\beta\neq\alpha} M_\beta) = \{0\}$*

Claramente ésta es una generalización para dos submódulos. Para la familia $(M_\alpha)_{\alpha\in A}$, puede ser independiente en parejas sin ser independiente.

Proposición 2.43. *Sea $(M_\alpha)_{\alpha\in A}$ un conjunto indexado de submódulos de un módulo M con sus transformaciones inclusión $(i_\alpha)_{\alpha\in A}$. Entonces las siguientes afirmaciones son equivalentes:*

1. *$\Sigma_A M_\alpha$ es una suma directa interna de $(M_\alpha)_{\alpha\in A}$.*

2. *$i = \oplus_A i_\alpha : \oplus_A M_\alpha \to M$ es monomorfismo.*

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

4. *$(M_\alpha)_{\alpha\in F}$ es independiente para todos los subconjuntos finitos $F \subseteq A$.*

5. *Para cada par $B, C \subseteq A$, si $B \cap C = \emptyset$, entonces*

$$(\Sigma_B M_\beta) \cap (\Sigma_C M_\gamma) = \{0\}$$

Demostración. En cada una de estas condiciones es equivalentemente que el cero tiene una única representacion $0 = \Sigma_A x_\alpha$ con $x_\alpha \in M_\alpha$ cero para casi todos los términos de $\alpha \in A$. □

Corolario 2.44. *El módulo M es la suma directa interna de sus submódulos $(M_\alpha)_{\alpha\in A}$ si y sólo si los $(M_\alpha)_{\alpha\in A}$ son independientes y generan a M.*

Si los submódulos son independientes, diremos que la suma $\Sigma_A M_\alpha$ es directa y se escribirá

$$\Sigma_A M_\alpha = \oplus_A M_\alpha$$

o también como una descomposición directa de $\Sigma_A M_\alpha$.

Notemos que el sumando directo externo de los $(M_\alpha)_{\alpha\in A}$ es el sumando directo interno de las imágenes de $(\tau_\alpha (M_\alpha))_{\alpha\in A}$, pero no el sumando directo interno de los $(M_\alpha)_{\alpha\in A}$. Para no tener confusiones, denotaremos la suma directa externa por

$$\dot{\oplus}_A M_\alpha$$

o en el caso finito como $M_1 \dot{\oplus} M_2 \dot{\oplus} ... \dot{\oplus} M_n$.

Proposición 2.45. *Sea $(M_1, ..., M_n)$ una sucesión finita de módulos, entonces*

$$M_1 \times ... \times M_n = M_1 \dot{\oplus} ... \dot{\oplus} M_n = \tau_1 (M_1) \oplus ... \oplus \tau_n (M_n)$$

Ejemplo 2.46. *1. Sea* $\mathbf{V}$ *un espacio vectorial sobre un campo* $\mathbb{K}$ *y sea* $(x_\alpha)_{\alpha\in A}$ *un conjunto indexado en* $\mathbf{V}$*. Entonces* $(x_\alpha)_{\alpha\in A}$ *genera a* $\mathbf{V}$ *si y sólo si* $\mathbf{V} = \Sigma_A \mathbb{K}x_\alpha$*. También* $(x_\alpha)_{\alpha\in A}$ *es un conjunto independiente de vectores si y sólo si el conjunto indexado* $(\mathbb{K}x_\alpha)_{\alpha\in A}$ *de submódulos cíclicos de* $\mathbf{V}$ *es independiente. Así,* $\mathbf{V}$ *es suma directa de*

$$\mathbf{V} = \Sigma_A \mathbb{K}x_\alpha = \oplus_A \mathbb{K}x_\alpha$$

si y sólo si $(x_\alpha)_{\alpha\in A}$ *son una base de* $\mathbf{V}$*.*

2. Consideramos el grupo abeliano $\mathbb{Z}_{30}$*. Y sus subgrupos* $15\mathbb{Z}_{30}$*,* $10\mathbb{Z}_{30}$*,* $6\mathbb{Z}_{30}$*; sean* i_2, i_3, i_5 *sus correspondientes transformaciones inclusión. Entonces, por la Proposición 2.39, el sumando directo* $i = i_2 \oplus i_3 \oplus i_5$ *es un homomorfismo*

$$i : (15\mathbb{Z}_{30}) \oplus (10\mathbb{Z}_{30}) \oplus (6\mathbb{Z}_{30}) \to \mathbb{Z}_{30}.$$

Además

$$Imi = 15\mathbb{Z}_{30} + 10\mathbb{Z}_{30} + 6\mathbb{Z}_{30} = \mathbb{Z}_{30}$$

así que i es un epimorfismo. Por argumentos de cardinalidad se sigue que i es un isomorfismo. Así $\mathbb{Z}_{30}$ *es el sumando directo interno de los submódulos* $(15\mathbb{Z}_{30}, 10\mathbb{Z}_{30}, 6\mathbb{Z}_{30})$*. Notemos también que este módulo es isomorfo, respectivamente, a* $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5$*. también* $\mathbb{Z}_{30} = (15\mathbb{Z}_{30}) \oplus (10\mathbb{Z}_{30}) \oplus (6\mathbb{Z}_{30}) \cong \mathbb{Z}_2 \dot{\oplus} \mathbb{Z}_3 \dot{\oplus} \mathbb{Z}_5 = \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

2.2.4 Propiedades de Independencia

Además de la caracterización de independencia dada en la Proposición 2.43 existen otras tres propiedades de independencia de especial importancia. La primera es una generalización, del conocido hecho de que en un espacio vectorial un conjunto de vectores es independiente, si y sólo si ninguno de los vectores depende de sus predecesores.

Proposición 2.47. *Una sucesión* $M_1, M_2, M_3, ...$ *de submódulos de* M *es independiente si y sólo si para cada* $n \geq 1$

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

DEMOSTRACIÓN. ($\Rightarrow$) Por la Proposición 2.43.4, si $(M_\alpha)_{\alpha\in A}$ son independientes para todo subconjunto $\{1,2,...,n+1\} = F \subseteq A$ y ahora por Proposición 2.43.5, sí $B = \{n+1\}$ y $C = F - \{n+1\}$ se tiene lo deseado.

($\Leftarrow$) Si $0 = x_{n_1} + ... + x_{n_r}$ donde $x_{n_i} \in M_{n_i}$, $n_1 < n_2 ... < n_r$, y no todos cero. Podemos suponer $n_v = max\{n_i : \ x_{n_i} \neq 0\}$, entonces $0 = x_{n_1} + ... + x_{n_v}$ y $-\left(x_{n_1} + ... + x_{n_{v-1}}\right) \in M_{n_v} \cap \left(M_1 + ... + M_{n_{v-1}}\right) = \{0\}$, así que $x_{n_v} = 0$, lo cual es una contradicción. $\square$

El resultado siguiente es un enunciado formal del simple hecho de que grupos independientes de submódulos independientes forman un conjunto independiente de submódulos.

Proposición 2.48. *Sean $(M_\beta)_{\beta\in B}$ submódulos independientes de un módulo M. Para cada $\beta \in B$, sea $\left(L_{\alpha_\beta}\right)_{\alpha_\beta\in A_\beta}$, una clase indexada de submódulos de M_β. Sea A la unión ajena $A = \cup_B A_\beta$. Si $\left(L_{\alpha_\beta}\right)_{\alpha_\beta\in A_\beta}$ es independiente para cada $\beta \in B$, entonces $(L_\alpha)_{\alpha\in A} = \cup_{\beta\in B} \left(L_{\alpha_\beta}\right)_{\alpha_\beta\in A_B}$ es independiente.*

DEMOSTRACIÓN. Supongamos que existe $\alpha_1, ..., \alpha_n \in A$ un conjunto finito y $x_i \in L_{\alpha_i}$, con $x_1 + x_2 + ... + x_n = 0$, así asumimos que existe un k y un β con $\alpha_1, ..., \alpha_k \in A_\beta$ y $\alpha_{k+1}, ..., \alpha_n \notin A_\beta$. La independencia de los $(M_\beta)_{\beta\in B}$ implica que $x_1 + ... + x_k = 0 = x_{k+1} + ... + x_n$, y la independencia de $\left(L_{\alpha_\beta}\right)_{\alpha_\beta} \in A_\beta$ fuerza a que $x_1 = ... = x_k = 0$. $\square$

Corolario 2.49. *Sea $M = \Sigma_B M_\beta$, sea $M_\beta = \Sigma_{A_\beta} L_{\alpha_\beta}$ para cada $\beta \in B$ y sea A la unión ajena $A = \cup_B A_\beta$. Entonces $M = \oplus_A L_\alpha$ si y sólo si $M = \oplus_B M_\beta$ y $M_\beta = \oplus_{A_\beta} L_{\alpha_\beta}$.*

DEMOSTRACIÓN. ($\Leftarrow$) Si $M = \oplus_B M_\beta$ y $M_\beta = \oplus_{A_\beta} L_{\alpha_\beta}$ entonces se sigue que para $M_\lambda \cap \Sigma_{B-\{\lambda\}} M_\beta = \{0\}$ para cualquier $\lambda \in B$, análogamente también para $L_{\alpha_\lambda} \cap \Sigma_{A_\beta - \{\alpha_\lambda\}} L_{\alpha_\beta} = \{0\}$ son independientes y sea $A = \cap_{A_\alpha} L_{\alpha_\beta}$ es una unión disjunta entonces aplicando la Proposición 2.48, se concluye que $M = \oplus_A L_\alpha$.

($\Rightarrow$) Si $M = \oplus_A L_\alpha$ y $A = \cap_{A_\alpha} L_{\alpha_\beta}$ es la unión disjunta, entonces por la Proposición 2.43.5 y sabiendo que $M_\beta = \Sigma_{A_\beta} L_{\alpha_\beta}$ entonces $M = \oplus_{A_\beta} L_{\alpha_\beta}$ para cada M_β. Si $\beta' \in B$ se sabe que $M_{\beta'} \cap \Sigma_{B-\{\beta'\}} M_\beta = \{0\}$ entonces $M = \oplus_B M_\beta$. $\square$

Proposición 2.50. *Supongo que $(L_\alpha)_{\alpha\in A}$ es un conjunto de submódulos independientes de M. Si $(M_\alpha)_{\alpha\in A}$ es un conjunto de submódulos de M tal 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 $L_2 \trianglelefteq M_2$, tendremos $L_1 \cap M_2 = \{0\}$. Pero

$$(M_1 \cap M_2) \cap L_1 \leq L_1 \cap M_2 = \{0\}$$

Como $L_1 \trianglelefteq M_1$, $M_1 \cap M_2 = \{0\}$. Es decir, (M_1, M_2) es un conjunto independiente de submódulos de M. Por otra parte, por la Proposición 2.27.2, tenemos que $L_1 \oplus L_2 \trianglelefteq M_1 \oplus M_2$.

Si 1) y 2) se suponen para $F = \{\alpha_1, ..., \alpha_n\} \subseteq A$, entonces para cualquier $\alpha_{n+1} \in A \setminus F$ la suma

$$\Sigma_{i=1}^{n+1} M_{\alpha_i} = (\oplus_{i=1}^{n} M_{\alpha_i}) + M_{\alpha_{n+1}}$$

es directa, y

$$\oplus_{i=1}^{n+1} L_{\alpha_i} \trianglelefteq \oplus_{i=1}^{n+1} M_{\alpha_i}$$

. Por lo tanto, argumentando inductivamente, 1) y 2), se cumplen para cada subconjunto finito $F \subseteq A$; y por la Proposición 2.43.4, $(M_\alpha)_{\alpha\in A}$ son independientes. Veamos que $\oplus_{\alpha\in A} L_\alpha \leq \oplus_{\alpha\in A} M_\alpha$, si $0 \neq x \in \oplus_A M_\alpha$, entonces existe un subconjunto finito $F \subseteq A$ tal que $0 \neq x \in \oplus_F M_\alpha$. Así $\oplus_F L_\alpha \trianglelefteq \oplus_F M_\alpha$, y por el Lema 2.26 existe un $r \in R$ con

$$0 \neq rx \in \oplus_F L_\alpha \subseteq \oplus_A L_\alpha$$

y por lo tanto $\oplus_A L_\alpha \trianglelefteq \oplus_A M_\alpha$. □

2.2.5 Los Idempotentes para una Descomposición

Supongamos que M tiene una descomposición directa interna $M = \oplus_A M_\alpha$, entonces para cada $\alpha \in A$

$$M = M_\alpha \oplus (\Sigma_{\beta \neq \alpha} M_\beta)$$

Así aplicando la Proposicion 2.10, existe un único idempotente $e_\alpha \in End({}_R M)$ con $M_\alpha = Im\ e_\alpha$ y $\Sigma_{\beta \neq \alpha} M_\beta = Ker\ e_\alpha$.

Llamaremos a los idempotentes $(e_\alpha)_{\alpha \in A}$, los idempotentes para la descomposición $M = \oplus_A M_\alpha$, y para cada $\alpha \in A$, llamaremos e_α al idempotente, del cual M_α es su descomposición en M.

Proposición 2.51. *Sea $(M_\alpha)_{\alpha \in A}$ un conjunto de submódulos de un módulo M. Entonces $M = \oplus_A M_\alpha$ si y sólo si existe un (necesariamente único) conjunto indexado de $(e_\alpha)_{\alpha \in A}$ de endomorfismos idempotentes de M tal que para todo $\alpha \in A$, $M_\alpha = Im\ e_\alpha$ y $\Sigma_{\beta \neq \alpha} M_\beta = Ker\ e_\alpha$. Por otra parte, si tal endomorfismo idempotente de M existe, entonces e_α es el idempotente para M_α en la descomposición $M = \oplus_A M_\alpha$.*

Demostración. $\Leftarrow$) Supongamos que $(e_\alpha)_{\alpha \in A}$ satisface la condición establecida. Entonces por el Lema 2.9, donde $Im\ e_\alpha \cap Ker\ e_\alpha = \{0\}$ para cada $\alpha \in A$, se sigue que los $(M_\alpha)_{\alpha \in A}$ son independientes. Pero también por el Lema 2.9, $Im\ e_\alpha + Ker\ e_\alpha = M$. Claramente $(M_\alpha)_{\alpha \in A}$ generan a M. Por ultimo la unicidad se sigue de la Proposición 2.10.

$\Rightarrow$) Hay que notar que aplicando la Proposición 2.10, a cada submódulo M_α para todos los $\alpha \in A$ se tiene lo deseado. $\square$

Definición 2.52. *Un conjunto de idempotentes $(e_\alpha)_{\alpha \in A}$ en un anillo se dice que son ortogonales en el caso de que el conjunto sea por pares ortogonal, es decir,*

$$e_\alpha e_\beta = \delta_{\alpha\beta} e_\alpha$$

$(\alpha, \beta \in A)$

Corolario 2.53. *Los idempotentes $(e_\alpha)_{\alpha \in A}$ para una descomposición $M = \oplus_A M_\alpha$, son ortogonales. Además, si $x \in M$, entonces $xe_\alpha = 0$ para casi todos $\alpha \in A$ y $x = \Sigma_A x e_\alpha$.*

Demostración. Si $\alpha \neq \beta$, entonces $M_\beta \subseteq \Sigma_{\lambda\neq\alpha} M_\lambda = Ker\ e_\alpha$ y por lo tanto $Me_\beta e_\alpha = M_\beta e_\alpha = 0$. Por otra parte, escribiendo $x = \Sigma_A x_\alpha$ con los $x_\alpha \in M_\alpha = Me_\alpha$ cero para casi todos los $\alpha \in A$, tenemos

$$xe_\beta = \Sigma_A x_\alpha e_\beta = x_\beta e_\beta = x_\beta$$

para todo $\beta \in A$. □

Definición 2.54. *Un conjunto $\{e_1, ..., e_n\}$ ortogonal finito de idempotentes en un anillo* $\mathbf{R}$ *se dice que es completo en el caso en que*

$$e_1 + e_2 + ... + e_n = 1 \in \mathbf{R}$$

Corolario 2.55. *Sea $M_1, M_2, ..., M_n$ submódulos de M. entonces*

$$M = M_1 \oplus M_2 \oplus ... \oplus M_n$$

si y sólo si existe un (necesariamente único) conjunto completo de $e_1, e_2, ..., e_n$, idempotentes ortogonales en $End\left({}_RM\right)$ con $M_i = Me_i$, con $i \in \{1, 2, ..., n\}$.

Demostración. ($\Rightarrow$) Sean $e_1, ..., e_n$ los idempotentes para $M = M_1 \oplus ... \oplus M_n$. Por el Corolario 2.53, son ortogonales. Como para toda $x \in M$ $x = \Sigma_{i=1}^n xe_i = x\left(e_1 + ... + e_n\right)$, entonces $e_1 + ... + e_n = 1_M \in End\ \left({}_RM\right)$.

($\Leftarrow$) Sean $e_1, ..., e_n \in End\left(M\right)$ idempotentes ortogonales tal que $M_i = Me_i$, entonces para cada $x \in M$

$$x = x\left(e_1 + ... + e_n\right) = xe_1 + ... + xe_n,$$

claramente $M_i = Im\ e_i$, ahora

$$\Sigma_{j\neq i} M_j = Ker\ e_i,$$

ya que $y = y\left(e_1 + ... + e_n\right)$, entonces $y - \Sigma_{i\neq j} ye_j = ye_i$, entonces $y = \Sigma_{j\neq i} ye_j$ si y sólo si $ye_i = 0$. Ahora aplicando la Definición 2.52, si $i \neq j$ $M_i = Me_i \subseteq Ker\ e_j = \Sigma_{s\neq j} M_s$. Ahora $x \in M_j \cap \Sigma_{s\neq j} M_s$, entonces $x = \Sigma_{s\neq j} x_s$ con $x_s \in M_s$, entonces $xe_j = \Sigma_{s\neq j} x_s e_j = 0$. Por otro lado $x = ye_j$ con $y \in M$, por lo tanto $xe_j = ye_j e_j = ye_j$, entonces $x = 0$, concluimos que $\{Me_1, ..., Me_n\}$ son independientes. □

2.2.6 Una Caracterización de las Sumas Directas

Existe una variación de los resultados anteriores que proporcionan una útil caracterización de las sumas directas.

Proposición 2.56. *Sean* $(M_\alpha)_{\alpha\in A}$ *un conjunto indexado de módulos,* M *un módulo, y para cada* $\alpha \in A$*, sea* $j_\alpha : M_\alpha \to M$ *un homomorfismo. Entonces* $\left(M, (j_\alpha)_{\alpha\in A}\right)$ *es una suma directa de* $(M_\alpha)_{\alpha\in A}$ *si y sólo si existen (necesariamente únicos) homomorfismos* $q_\alpha : M \to M_\alpha$ $(\alpha \in A)$ *que satisfacen, para todo* $\alpha,\ \beta \in A$ *y toda* $x \in M$*,*

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

b) $q_\alpha(x) = 0$ *para casi todos los* $\alpha \in A$

c) $\Sigma_A j_\alpha q_\alpha(x) = x$

Por otra parte, si $\left(M, (j_\alpha)_{\alpha\in A}\right)$ *es una suma directa de* $(M_\alpha)_{\alpha\in A}$ *y si* $f_\alpha : M_\alpha \to N$ *son homomorfismos, entonces*

$$f : x \mapsto \Sigma_A f_\alpha q_\alpha(x) \ \text{ con } x \in M$$

es el único homomorfismo $f : M \to N$ *tal que* $f_\alpha = f j_\alpha$*, con* $\alpha \in A$*.*

Demostración. $(\Rightarrow)$ Supongamos que $\left(M, (j_\alpha)_{\alpha\in A}\right)$ es una suma directa de $(M_\alpha)_{\alpha\in A}$. La transformación suma directa $j = \oplus_A j_\alpha : \oplus_A M_\alpha \to M$ es un isomorfismo. Sean τ_α y π_α la usual transformación coordenada para la suma directa externa $\oplus_A M_\alpha$. Para cada $\alpha \in A$ sea

$$q_\alpha = \pi_\alpha j^{-1} : M \to M_\alpha.$$

Como $j_\alpha = j\tau_\alpha$ para cada $\alpha \in A$, es fácil ver que los q_α satisfacen a) y como $j^{-1}(x) \in \oplus M_\alpha$, se satisface b). Ahora para cada $x \in M$

$$x = jj^{-1}(x) = j\left(\Sigma_A \tau_\alpha \pi_\alpha j^{-1}(x)\right) = \Sigma_A j\tau_\alpha\pi_\alpha j^{-1}(x) = \Sigma_A j_\alpha q_\alpha(x)$$

. Por la Proposición 2.40, $M = \Sigma_A Im\ j_\alpha$, por lo que en vista de a), q_α es único. $(\Leftarrow)$ Si $(q_\alpha)_{\alpha\in A}$ que satisfacen las tres condiciones y $f_\alpha : M_\alpha \to N$, entonces se define $f : M \to N$ por

$$f(x) = \Sigma_A f_\alpha q_\alpha(x) \ \text{ con } x \in M$$

entonces para todo $\alpha \in A$ y toda $x_\alpha \in M_\alpha$,

$$fj_\alpha(x_\alpha) = \Sigma_{\beta\in A} f_\beta q_\beta (j_\alpha(x_\alpha)) = f_\alpha(x_\alpha)$$

. Por otro lado, si $g : M \to N$ con $gj_\alpha = f_\alpha$ para cada $\alpha \in A$, entonces para toda $x \in M$

$$g(x) = g(\Sigma_A j_\alpha q_\alpha(x)) = f(x)$$

□

Esta caracterización importante asume una forma particularmente interesante para el caso de las sumas directas finitas.

Corolario 2.57. *Sean $(M_1, ...M_n)$ una sucesión finita de módulos y $j_i : M_i \to M$ $(i = 1, 2, ...n)$ homomorfismos. Entonces $(M, (j_{1,...,j_n}))$ es una suma directa de $(M_1, ..., M_n)$ si y sólo si existen homomorfismos $q_i : M \to M_i$ tal que para todo $1 \leq k, i \leq n$*

$$q_k j_i = \delta_{ik} 1_{M_i} \ \ y \ \ \Sigma_{i=1}^{n} j_i q_i = 1_M$$

La demostración del Corolario es clara de la Proposición 2.56.

2.3 Clases de Generadores y Cogeneradores

Si $\Re$ una clase de módulos. Un módulo M es (finitamente) generado por $\Re$, en el caso que exista un conjunto (finito) indexado $(U_\alpha)_{\alpha\in A}$ en $\Re$ y un epimorfismo

$$\oplus_A U_\alpha \to M \to 0.$$

Si $\Re = \{U\}$ es un singular, entonces U genera a M, esto significa que existe un epimorfismo

$$U^{(A)} \to M \to 0$$

para algún conjunto finito A.

Teorema 2.58. *Si un módulo ${}_RM$ tiene un conjunto generador $X \subseteq M$, entonces existe epimorfismo $R^{(X)} \to M \to 0$. Además, R finitamente genera a M si y sólo si M tiene un conjunto generador finito.*

Demostración. Sea $X \subseteq M$ que genera a M. Para cada $x \in X$ la multiplicación a derecha dada por $\rho_x : r \mapsto rx$, es un R-homomorfismo izquierdo $\rho_x : R \to M$. Sea $\rho = \oplus_X \rho_x$ la suma directa de estos homomorfismos. Entonces $\rho : R^{(X)} \to M$ y $Im\ \rho = \Sigma_X Im\ \rho_x = \Sigma_X Rx = M$. Así ρ es epimorfismo. Así si ahora M es finitamente generado entonces X es finito que es este caso seria su conjunto generador. $\square$

Ejemplo 2.59. *Decimos que un grupo ${}_{\mathbb{Z}}M$ es de torsión en el caso en que cada elemento es de orden finito. Si ${}_{\mathbb{Z}}M$ es de torsión, entonces para cada $x \in M$ existe $0 < n(x) \in \mathbb{N}$ y un homomorfismo $f_x : \mathbb{Z}_{n(x)} \to M$ con $Im\ f_x = \mathbb{Z}x$ y la suma directa es un homomorfismo sobreyectivo $f = \oplus_M f_x$, $f : \oplus_M \mathbb{Z}_{n(x)} \to M$.*

Inversamente, si M es la imagen de un homomorfismo sobreyectivo de una suma directa de grupos cíclicos, generados por elementos de orden finito, así M es de torsión. En otros palabras un Grupo Abeliano es de torsión si y sólo si éste es generado por $\Re = \{\mathbb{Z}_n |\ n = 2, 3, ...\}$.

Observe también que esto es equivalente a ser generado por este grupo; $\oplus_{\mathbb{N}} \mathbb{Z}_n$.

La noción de generadores es categórica, pues sólo depende de los objetos y morfismo en la categoría M y no de los elementos de algún módulo M. Este concepto tiene un dual natural, simplemente invirtiendo flechas y cambiando epimorfismo por monomorfismo.

Sea $\Re$ una clase de módulos. Un módulo M es cogenerado (finitamente) por $\Re$ en caso de existir un conjunto indexado (finito) $(U_\alpha)_{\alpha \in A}$ en $\Re$ y un monomorfismo $0 \to M \to \Pi_A U_\alpha$.

Ejemplo 2.60. *Si M es un grupo abeliano libre de torsión entonces existe un monomorfismo $M \to \mathbb{Q}^M$; así, ${}_{\mathbb{Z}}M$ es cogenerado por ${}_{\mathbb{Z}}\mathbb{Q}$. en otras palabras, un grupo abeliano libre de torsión es precisamente un grupo abeliano cogenerado por $\mathbb{Q}$.*

Sea $\Re$ una clase de módulos. La clase de todos lo módulos generado por $\Re$ es denotada $Gen(\Re)$ y la clase de los cogenerados por $\Re$ denotada $Cog(\Re)$. También $FGen(\Re)$ y $FCog(\Re)$ denota las clases de los finitamente generados y finitamente cogenerados por $\Re$, respectivamente. Por ejemplo, si $\Re = \{\mathbb{Z}_n |\ n > 1\}$, entonces $Gen(\Re)$ es la clase de grupos de torsión, mientras $Cog(\mathbb{Q})$ es la clase de los grupos libres de torsión.

Proposición 2.61. *Sea $\Re$ la clase de módulos.*

1. *Si $M \in Gen(\Re)$ $(FGen(\Re))$, entonces también lo es cada imagen de M mediante un epimorfismo de M.*

2. *Si $(M_\alpha)_{\alpha\in A} \subseteq Gen(\Re)$ $((M_\alpha)_{\alpha\in A} \subseteq FGen(\Re)$ y finito), entonces $\oplus_A M_\alpha$ esta en $Gen(\Re)$ $(FGen(\Re))$.*

Demostración. (1) Si $f : \oplus_A U_\alpha \to M$ y $g : M \to M'$ son epimorfismos, entonces también la composición es un epimorfismo $gf : \oplus_A U_\alpha \to M'$.

(2) Sea $f_\alpha : \oplus_{B_\alpha} U_{\beta_\alpha} \to M_\alpha$, un epimorfismo para cada $\alpha \in A$. Entonces el suma directa $f = \oplus_A f_\alpha$ es un epimorfismo

$$f : \oplus_A (\oplus_{B_\alpha} U_{\beta_\alpha}) \to \oplus_A M_\alpha.$$

Pero si $C = \cup_A B_\alpha$ es unión ajena, entonces $\oplus_A (\oplus_{B_\alpha} U_{\beta_\alpha}) \cong \oplus_C U_\gamma$ □

Proposición 2.62. *Sea $\Re$ una clase de módulos.*

1. *Si M es un $Cog(\Re)$ $(FCog(\Re))$, y si $g : M' \to M$ es un monomorfismo, entonces M' es un $Cog(\Re)$ $(FCog(\Re))$.*

2. *Si $(M_\alpha)_{\alpha\in A}$ es un conjunto indexado en $Cog(\Re)$ $(FCog(\Re))$, entonces $\Pi_A M_\alpha$ es un elemento de $Cog(\Re)$ $(FCog(\Re))$.*

La demostración es dual a la Proposición 2.61.

Corolario 2.63. *Sean $\Re$ y $\Re'$ clases de módulos.*

1. *Si $\Re'$ esta contenido en $Gen(\Re)$ $(FGen(\Re))$, entonces $Gen(\Re') \subseteq Gen(\Re)$ $(FGen(\Re'))$.*

2. *Si $\Re'$ esta contenido en $Cog(\Re)$ $(FCog(\Re))$, entonces $Cog(\Re') \subseteq Cog(\Re)$ $(FCog(\Re'))$.*

Observación 2.64. *Es inmediato de la Proposición 2.40 y el Corolario 2.32, que:*

1. *La clase $\Re$ generará a M si y sólo si M es una suma de submódulos, cada uno imagen de un epimorfismo de algún módulo de $\Re$.*

2. *La clase de $\Re$ cogenera a M si y sólo si existe un conjunto $\mathcal{H}$, de submódulos de M tales que M/K esta inmerso en algún módulo de $\Re$, para cada $K \in \mathcal{H}$ y $\cap\, \mathcal{H} = \{0\}$.*

2.3.1 Generadores y Cogeneradores

Como consecuencia del Corolario 2.63, si $\Re$ y $\Re'$ son clases de módulos, que generan la misma clase de módulos, entoces $Gen\,(\Re) = Gen\,(\Re')$; en particular, $\Re$ y $\Re'$ podría ser distintas y generar las mismas clases. Así, dar un $\Re$ apropiado, es buscar algunas clases canónicas que también generen al $Gen\,(\Re)$.

Un conjunto $\mathcal{R} \subseteq \Re$ es una clase de representantes de los tipos de isomorfismos de $\Re$, en el caso en que cada $U \in \Re$ sea isomorfo a algún elemento de $\mathcal{R}$. Si además, no hay dos elementos de $\mathcal{R}$ que sean isomorfos, entonces la clase de representantes es irredundante. Claramente si $\mathcal{R}$ es una clase de representantes de $\Re$, entonces $Gen\,(\Re) = Gen\,(\mathcal{R})$ y $Cog\,(\Re) = Cog\,(\mathcal{R})$.

Dada una clase $\Re$, un módulo G es generador de $Gen\,(\Re)$ en caso de que $Gen\,(\Re) = Gen\,(G)$. Un módulo C es un cogenerador de $Cog\,(\Re)$, en el caso $Cog\,(\Re) = Cog\,(C)$.

Un generador (cogenerador) para la clase $_RM$ de todos los R-módulos izquierdos es usualmente llamada un R-generador (R-cogenerador) izquierdo, sin referencia a la clase; con base en esta terminología la primera parte del Teorema 2.58 puede ser remplazado por:

Corolario 2.65. *El módulo regular $_RR$ es un R-generador.*

Los Ejemplos 2.59 y 2.60, dicen que $\mathbb{Q}$ es un cogenerador para la clase de los grupos libres de torsión y que $G = \oplus_{n>1}\mathbb{Z}_n$ es un generador para la clase de grupos de torsión respectivamente.

Proposición 2.66. *Si $\Re$ tiene un conjunto $\{U_\alpha |\ \alpha \in A\}$ de representantes de $\Re$, entonces:*

1. *$\oplus_A U_\alpha$ es un generador para $Gen\,(\Re)$.*

2. *$\oplus_A U_\alpha$ y $\Pi_A U_\alpha$ son cogeneradores para $Cog\,(\Re)$.*

Demostración. Para la demostración de (1) ver la observación 2.64.1.

(2) Por la Proposición 2.62, $\Pi_A U_\alpha$ y el submódulo $\oplus_A U_\alpha$ estan en $Cog\,(\Re)$, así que

$$Cog\,(\oplus_A U_\alpha) \subseteq Cog\,(\Re) \text{ y } Cog\,(\Pi_A U_\alpha) \subseteq Cog\,(\Re)$$

La transformación $\tau_\alpha : U_\alpha \to \oplus_A U_\alpha$ es monomorfismo, también $\oplus_A U_\alpha$ cogenera cada U_α. Ahora si $T \in \Re$, $T \cong U_\alpha$ para algún $\alpha \in A$, $\mathcal{R} \subseteq Cog\,(U_\alpha) \subseteq Cog\,(\oplus_A U_\alpha)$, entonces $Cog\,(\Re) \subseteq Cog\,(\oplus_A U_\alpha)$, por tanto $\oplus_A U_\alpha$ cogenera $Cog\,(\Re)$. Trivialmente $\Pi_A U_\alpha$ cogenera a $\oplus_A U_\alpha$, así que $Cog\,(\Pi_A U_\alpha) \supseteq Cog\,(\oplus_A U_\alpha) = Cog\,(\Re)$, finalmente $Cog\,(\Pi_A) = Cog\,(\Re)$. □

Proposición 2.67. *Sean U y M módulos. Entonces*

1. *U (finitamente) genera a M si y sólo si existe un subconjunto (finito) $H \subseteq\ Hom_R\,(U, M)$ con $M = \Sigma_{h\in H} Im\ h$.*

2. *U (finitamente) cogenera a M si y sólo si existe un subconjunto (finito) $H \subseteq\ Hom_R\,(M, U)$ con $\{0\} = \cap_{h\in H} Ker\ h$.*

Demostración. (1) Supongamos que U genera a M, entonces podemos encontrar una familia (finita), de epimorfismos $h_\alpha : U \to M$ tal que $M = \Sigma_A Im\ h_\alpha$. Ahora, si $H \subseteq Hom\,(U, M)$ con

$$\Sigma_{h\in H} Imh = M\ \ (H finito)\,,$$

entonces existe $\oplus H : \oplus_H U_h \to M$, con $U_h = U$para todo h, como $Im(\oplus H) = \Sigma_{h\in H} Im\ h$ pero $\Sigma_{h\in H} Im\ h = M$, por tanto $\oplus H$ es epimorfismo.

(2) ($\Rightarrow$) Supongamos que U cogenera (cogenera finitamente) a M, entonces existe $f : M \to U^A$ monomorfismo (con A finito). Para cada $\alpha \in A$, $f_\alpha = \pi_\alpha f : M \to U$ es también un homomorfismo y $\cap_A Ker\ f_\alpha = \{0\}$.

($\Leftarrow$) Si $H \subseteq Hom_R\,(M, U)$, entonces el producto directo, $\Pi_H h : M \to U^H$ tiene núcleo $\cap_H Ker\ h = \{0\}$, entonces $\Pi_H h$ es monomorfismo. □

Corolario 2.68. *Sean U y M módulos. Entonces:*

1. *U genera a M si y sólo si para cada $f : M \to N$ homomorfismo, no cero existe un $h \in Hom_R(U, M)$ tal que $fh \neq 0$.*

2. *U cogenera a M si y sólo si para cada $f : N \to M$ homomorfismo no cero existe un $h \in Hom_R(M, U)$ tal que $hf \neq 0$.*

Demostración. Sean los conjuntos

$$H = Hom_R(U, M) \text{ y } T = \Sigma_H Im\ h \leq M$$

. 1) Sea $f : M \to N$ y supongamos que $fh = 0$ para cada $h \in H$, y que U genera a M entonces $T \leq Ker\ f$. Por otro lado T es el núcleo de la transformación $\eta_T : M \to M/T$, usando la Proposición 2.67 se tiene que $\eta_T = 0$ (ya que T=M), así $Ker\, f = M$, por tanto $f = 0$.

2) $\Rightarrow$) Sea $U = \Pi_A U_\alpha$ que cogenera a M y definamos $g : M \to \oplus_{A'} U_\alpha$ y la proyección $\pi_\alpha : \oplus_{A'} U_\alpha \to U_\alpha$, para un subconjunto $A' \subseteq A$, y sea $f : N \to M$ homomorfismo y supongamos que $(\pi_\alpha g) f = 0$ entonces $Ker(\pi_\alpha g) f = N$ y el $Im\ f \leq Ker\ \pi_\alpha g = \{0\}$, esto es por que U cogenera a M, luego $f = 0$, una contradicción, por tanto $(\pi_\alpha g) f \neq 0$.

$\Leftarrow$) Sean $f = \oplus h : M \to \oplus_A U_\alpha = U^A$ y $A = Hom_R(M, U)$ entonces, sea $i : Ker\ f \to M$ entonces se tiene que $i \neq 0$ y $h(Ker\ f) \neq \{0\}$, para algún $h \in A$ pero $Ker\ f \subseteq Ker\ h$ con $hi \neq 0$ por tanto U cogenera a M. □

2.3.2 La Traza y Reject

Sea $\Re$ una clase de módulos. De la Observación 2.64 es claro que no necesariamente genera $\Re$ a M, veremos que, existe un submódulo más grande de M generado por $\Re$. Y dualmente, existe un submódulo de M más chico tal que su cociente con M es cogenerado por $\Re$.

Definición 2.69. *Sea $\Re$ clase de módulos y M un módulo, definimos:*

1. *La traza de $\Re$ en M por;*

$$Tr_M(\Re) = \Sigma\{Im\ h|\ h : U \to M \text{ con } U \in \Re\}$$

2. *El Reject de $\Re$ en M por;*

$$Rej_M(\Re) = \cap\{Ker\ h|\ h : M \to U \text{ con } U \in \Re\}.$$

Observe que aunque la clase $\Re$ no sea un conjunto, ésta suma e intersección son tomadas sobre el conjunto de submódulos de M. Así, están bien definidos estos submódulos de M. En particular cuando $\Re = \{U\}$, entonces son de la forma

$$Tr_M(\Re) = \Sigma\{Im\ h|\ h \in Hom_R(U, M)\}$$

$$Rej_M(\Re) = \cap\{Ker\ h|\ h \in Hom_R(M, U)\}$$

Es fácil extender la Proposición 2.67, se tiene la siguiente Proposición:

Proposición 2.70. *Sea $\Re$ una clase de módulos y sea M un módulo. Entonces*

1. *$Tr_M(\Re) = L$ es el único submódulo más grande de M generado por $\Re$.*

2. *$Rej_M(\Re) = K$ es el único submódulo más chico de M tal que M/K es cogenerado por $\Re$.*

DEMOSTRACIÓN. (1) Sean $(U_\alpha)_{\alpha\in A}$ un conjunto indexado de $\Re$ y $h : \oplus_A U_\alpha \to N \subseteq M$, con $N = Im\ h = \Sigma_A Im(h\tau_\alpha) \leq Tr_M(\Re)$. Por lo que cada submódulo N de M $Gen(\Re)$ está contenido en $Tr_M(\Re)$. Por otro lado hay un conjunto indexado $(U_\alpha)_{\alpha\in A}$ y homomorfismos $h_\alpha : U_\alpha \to M$ con $Tr_M(\Re) = \Sigma_A Im\ h_\alpha$. Así $\oplus_A h_\alpha : \oplus_A U_\alpha \to M$ tiene imagen $Tr_M(\Re)$, también $Tr_M(\Re)$ es un elemento $Gen(\Re)$.

(2) Sea $(U_\alpha)_{\alpha\in A}$ un conjunto indexado en $\Re$, Sea $h : M \to \Pi_A U_\alpha$, y $K = Ker\ h$. Entonces $K = \cap_A Ker(\pi_\alpha h) \supseteq Rej_M(\Re)$ y por tanto, si M/K es cogenerado por $\Re$, $K \supseteq Rej_M(\Re)$. Por otro lado existe un conjunto indexado $(U_\alpha)_{\alpha\in A}$ en $\Re$ y $h_\alpha : M \to U_\alpha$ con $Rej_M(\Re) = \cap_A Ker\ h_\alpha$. Así $\Pi_A h_\alpha : M \to \Pi_A U_\alpha$ tiene núcleo $Rej_M(\Re)$ y, por tanto $M/Rej_M(\Re)$ es un $Cog(\Re)$. □

Corolario 2.71. *Sea M un módulo y sea $\Re$ una clase de módulos. Entonces*

1. *$\Re$ genera a M si y sólo si $Tr_M(\Re) = M$.*

2. *$\Re$ cogenera a M si y sólo si $Rej_M(\Re) = 0$.*

Corolario 2.72. *Sea M un módulo y sea $\Re$ una clase de módulos. Sea $K \leq M$. Entonces*

1. *$K = Tr_M(\Re)$ si y sólo si $K \geq Tr_M(\Re)$ y $K = Tr_K(\Re)$.*

2. *$K = Rej_M(\Re)$ si y sólo si $K \leq Rej_M(\Re)$ y $Rej_{M/K}(\Re) = 0$.*

En particular

$$K = Tr_{Tr_M(\Re)}(\Re) = Tr_M(\Re) \;\; y \;\; Rej_{M/Rej_M(\Re)}(\Re) = 0$$

Demostración. (1) $\Rightarrow$) Bastara demostrar que $K \leq Tr_K(\Re)$. Como $\Sigma\{Im\ h|\ h : U \to M$, con $U \in \Re\} = K$, entonces $Imh \leq K$ con $h : U \to M$ y $U \in \mathcal{R}$, entonces $K = Tr_M(\Re) \leq Tr_K(\Re)$.

$\Leftarrow$) Como $K \leq M$ y es generado por $\Re$ ($K = \Sigma\{Im\ h|\ h : U \to K \leq M\}$), $Tr_M(\Re) \geq K$ así $K = Tr_M(\Re)$.

(2) La demostración de es dual a (1).

□

Ejemplo 2.73. 1. *Si $\Re = \{\mathbb{Z}_n|\ n = 2, 3, ...\}$, entonces para cada grupo abeliano M, la Traza $Tr_M(\Re)$, es el grupo de torsión $T(M)$ de M. Por supuesto $T(M)$ es el único submódulo de torsión más grande que M, y $T(T(M)) = T(M)$.*

2. *Si M es un grupo abeliano, entonces $Rej_M(\mathbb{Q})$ es la intersección de todos $K \leq M$ con M/K libre de torsión. Por tanto $Rej_M(\mathbb{Q})$ es de nuevo sólo el subgrupo de torsión $T(M)$ de M, el único subgrupo más chico con $M/T(M)$ libre de torsión, y por supuesto que $T(M/T(M)) = 0$.*

Proposición 2.74. *Sea $\Re$ una clase de módulos. Sean dos módulos M y N y $f : M \to N$ un homomorfismo. Entonces*

$$f(Tr_M(\Re)) \leq Tr_N(\Re) \;\; y \;\; f(Rej_M(\Re)) \leq Rej_N(\Re).$$

En particular $Tr_M(\Re)$ y $Rej_M(\Re)$ son $End(_RM)$ bisubmódulos de M, R-izquierdo y R-derecho.

Demostración. Observemos para el primer caso que para cada $h \in Hom_R(U, M)$ con $U \in \Re$, tenemos que $fh \in Hom_R(U, N)$ y $f(Im\ h) = Im\ fh$.

Para el segundo caso, si $x \in Rej_M(\Re)$ y $h \in Hom_R(N, U)$ con $U \in \Re$, entonces $hf \in Hom_R(M, U)$, también $h(f(x)) = 0$. Sea

$f \in End\left({}_{R}M\right)$, $x \in Tr_M(\Re)$, $xf \in Tr_M(\Re)$. Así que $Tr_M(\Re)$ es un módulo derecho sobre $End\left({}_{R}M\right)$. $\square$

Corolario 2.75. *1. Si $f : M \to N$ es monomorfismo y $Tr_N(\Re) \subseteq Im\ f$, entonces $f\left(Tr_M(\Re)\right) = Tr_N(\Re)$.*

2. Si $f : M \to N$ es un epimorfismo y $Ker\ f \subseteq Rej_M(\Re)$, entonces $f\left(Rej_M(\Re)\right) = Rej_N(\Re)$.

Demostración. (1) Es dual de (2).

(2) Por la Proposición 2.74, $f\left(Rej_M(\Re)\right) \leq Rej_N(\Re)$, pero si f es epimorfismo con $Ker\ f \subseteq Rej_M(\Re)$, por el Teorema 1.42, existe un isomorfismo

$$M/Rej_M(\Re) \to N/f\left(Rej_M(\Re)\right).$$

Por el Corolario 2.72.2 los Reject de $\Re$ de ambos módulos son cero, es decir, $Rej_{N/f(Rej_M(\Re))}(\Re) = 0$. También por el Corolario 2.72.2, se sigue $f\left(Rej_M(\Re)\right) = Rej_N(\Re)$. $\square$

Proposición 2.76. *Si $\left(M_\alpha\right)_{\alpha\in A}$ es un conjunto indexado de módulos, entonces para cada módulo M*

1. $Tr_{\oplus_A M_\alpha}(\Re) = \oplus_A Tr_{M_\alpha}(\Re)$

2. $Rej_{\oplus_A M_\alpha}(\Re) = \oplus_A Rej_{M_\alpha}(\Re)$

Demostración. (1) Aplicando la Proposición 2.74 y las transformación inyección τ_α y proyección π_α tenemos

$$Tr_{\oplus_A M_\alpha}(\Re) = \Sigma\tau_\alpha\pi_\alpha\left(Tr_{\oplus_A M_\alpha}(\Re)\right) \leq \Sigma\tau_\alpha\left(Tr_{M_\alpha}(\Re)\right) \leq Tr_{\oplus_A M_\alpha}(\Re),$$

Así que $Tr_{\oplus_A M_\alpha}(\Re) = \Sigma\tau_\alpha\left(Tr_{M_\alpha}(\Re)\right)$.

Por tanto $\Sigma\tau_\alpha\left(Tr_{M_\alpha}(\Re)\right) = \oplus Tr_{M_\alpha}(\Re) = Tr_{\oplus_A M_\alpha}(\Re)$.

Es similar la prueba de (2) $\square$

Lema 2.77. *Sea $\Re$ y $\Re'$ clases de módulos.*

1. Si $\Re' \subseteq Gen(\Re)$, entonces $Tr_M(\Re') \leq Tr_M(\Re)$.

2. Si $\Re' \subseteq Cog(\Re)$, entonces $Rej_M(\Re) \leq Rej_M(\Re')$.

DEMOSTRACIÓN. (1) Si $\Re' \subseteq Gen(\Re)$ y sea $(M_\alpha)_{\alpha \in A} \subseteq \Re'$ y notemos que la $Tr_M(\Re') = \Sigma\{Im\ h | h : M_\alpha \to M \text{ con } M_\alpha \in \Re'\}$, ahora sean $h_{\alpha_\gamma} : M_{\alpha_\gamma} \to M_\alpha$ y los $M_{\alpha_\gamma} \in \Re$ y ahora tomando la composición de $h_\alpha h_{\alpha_\gamma}$ y la suma de estas imágenes entonces la suma esta contenida en $Tr_M(\Re)$, ahora es vidente que $Tr_M(\Re') \subseteq Tr_M(\Re)$.

Para (2) Supongamos que $x \notin Rej_M(\Re')$, entonces existe un homomorfismo $f : M \to V$ con $V \in \Re'$ y $x \notin Ker\ f$. Como $V \in Cog(\Re)$, existe un homomorfismo $h : V \to U$ con $U \in \Re$ y $f(x) \notin Ker\ h$. Así $hf : M \to U$, con $x \notin Ker\ hf$, luego $x \notin Rej_M(\Re)$. □

Proposición 2.78. *Sea G un generador para $Gen(\Re)$ y sea C un cogenerador para $Cog(\Re)$. Entonces para cada M, $Tr_M(\Re) = Tr_M(G)$ y $Rej_M(\Re) = Rej_M(C)$. En particular, si $(U_\alpha)_{\alpha \in A}$ es un conjunto indexado de módulos, $Tr_M(\oplus_A U_\alpha) = \Sigma_A Tr_M(U_\alpha)$ y*

$$Rej_M(\Pi_A U_\alpha) = \cap_A Rej_M(U_\alpha) = Rej_M(\oplus_A U_\alpha)$$

.

DEMOSTRACIÓN. Del Lema 2.77, tenemos que $Tr_M(G) \subseteq Tr_M(\Re)$, ahora si $x \in Tr_M(\Re)$, entonces $x = \Sigma_{i=1}^n h_{\alpha_i}(x_i)$ donde $x_i \in U_{\alpha_i} \in \Re$ y $h_{\alpha_i} : U_{\alpha_i} \to M$, cada $x_i = \Sigma J_{\alpha_{i_\beta}}(g_j)$, con $g_j \in G$, $x = \Sigma h_{\alpha_i} J_{\alpha_{i_\beta}}(g_j)$ entonces $x = Tr_M(G)$.

Ahora, si $\Re = \{U_\alpha\}$, $\oplus_A U_\alpha \in Gen\Re$, entonces $Tr_M(\oplus_A U_\alpha) = Tr_M(\Re) = \Sigma Tr_M(U_\alpha)$. □

Proposición 2.79. *Para cada clase $\Im$ de R-módulos izquierdos, la $Tr_R(\Im)$ es un ideal bilateral. Por otra parte, un $_RM$ módulo es un generador si y sólo si $Tr_R(M) = R$.*

La demostración viene dada en [4].

Capítulo 3

Condiciones Finitas para Módulos

En esta sección estudiaremos un poco de módulos que son generados por módulos simples. Estos son precisamente los que tienen una descomposición en suma directa de módulos simples. También los módulos semisimples forman la más importante clase de módulos y proporcionan el bloque básico de construcción de gran parte de esta teoría.

3.1 Módulos Semisimples, el Soclo y el Radical

Desde el punto de vista de la teoría de módulos una de las características más notables de un espacio vectorial es que este tiene una base, que la cardinalidad de esta base es una invariante del módulo. y que cualquier conjunto independiente puede ser extendido a una base agregando elementos de una base dada. Estas propiedades se pueden reformularse en términos de teoría de módulos, y como veremos más adelante en esta sección, lo anterior es corto en cualquier módulo generado por módulos simples.

3.1.1 Módulos Simples

Recalquemos que un módulo no cero ${}_RT$ es simple en el caso en que no tenga submódulos distintos de los triviales. Un módulo simple puede ser caracterizado como un módulo no cero T, tal que cada homomorfosmo no cero $T \to N$ $(N \to T)$ en ${}_RM$ es un monomorfismo (epimorfismo).

Proposición 3.1. *Un R-módulo izquierdo T es simple si y sólo si $T \cong R/M$ para algún ideal izquierdo maximal M de R.*

Demostración. $(\Leftarrow)$ Si $T \cong R/M$ donde M es ideal maximal de R, entonces por la Proposición 1.20, de ahí se tiene que T es simple.

3.1.2 Módulos Semisimples

Definición 3.2. *Sea $(T_\alpha)_{\alpha\in A}$ un conjunto indexado de submódulos simples de M. Si $M = \oplus_A T_\alpha$ entonces $(T_\alpha)_{\alpha\in A}$ es una descomposición semisimple de M.*

Definición 3.3. *Un módulo M es semisimple en el caso de tener una descomposición semisimple.*

Claramente un módulo simple es semisimple.

Lema 3.4. *Sea $(T_\alpha)_{\alpha\in A}$ un conjunto indexado de submódulos simples del R-módulo izquierdo M. Si $M = \Sigma_A T_\alpha$ entonces para cada submódulo K de M existe un subconjunto $B \subseteq A$ tal que $(T_\beta)_{\beta\in B}$ es independiente y $M = K \oplus (\oplus_B T_\beta)$.*

Demostración. Sea $K \leq M$, y tomando $\mathcal{C} = \{C \subset A : K \cap \Sigma_C T_\alpha = \{0\}, \{T_\alpha\}_{\alpha\in C}$ es independiente$\}$, parcialmente ordenado con la contención. El conjunto $\mathcal{C}$ es no vacío, ya que trivialmente $\emptyset \in \mathcal{C}$. Si $\{B_\gamma\}_{\gamma\in J}$ es una cadena en el conjunto parcialmente ordenado $\mathcal{C}$, entonces la unión $\cup_{\gamma\in J} B_\gamma$ está en el conjunto, ya que si $C = \cup_{\gamma\in J} B_\gamma$, debemos mostrar que a) $\{T_\alpha\}_{\alpha\in C}$ es independiente, b) $K \cap (\Sigma_{\alpha\in C} T_\alpha) = \{0\}$. Para a), si $x \neq 0$ y $x \in T_{\alpha_0} \cap (\Sigma_{\alpha\in C, \alpha\neq\alpha_0} T_\alpha)$, $x = x_{\alpha_1} + ... + x_{\alpha_n}$, existe un $\gamma' \in J$, con $\alpha_0, \alpha_1, ..., \alpha_n \in B_{\gamma'}$ entonces $x \in T_{\alpha_0} \cap \left(\Sigma_{\alpha\in B_{\gamma'}} T_\alpha\right)$ lo que es una contradicción, para b) es análogo. Aplicamos el Lema de Zorn y tomamos $B \subseteq A$ maximal con respecto a la condición, que $(T_\beta)_{\beta \in B}$ es independiente y $K \cap (\Sigma_B T_\beta) = \{0\}$, entonces la suma

$$N = K + (\Sigma_B T_\beta) = K \oplus (\oplus_B T_\beta)$$

es directa. Como, para cada $\alpha \in A$ el T_α es simple, entonces $T_\alpha \cap N = T_\alpha$ o $T_\alpha \cap N = \{0\}$. Si $T_\alpha \cap N = \{0\}$ y $C = B \cup \{\alpha\}$, $N = K \oplus (\oplus_C T_\gamma)$ por la maximalidad de B tenemos que $\alpha \in B$. Así que si $\alpha \in A \setminus B$, entonces pues $T_\alpha \leq N$, así que para cada $\alpha \in A$, $T_\alpha \leq N$, por tanto se sigue $N = M$. $\square$

Proposición 3.5. *Si un módulo M es generado por un conjunto indexado $(T_\alpha)_{\alpha \in A}$ de submódulos simples, entonces para algún $B \subseteq A$, $M = \oplus_B T_\beta$, es decir, M es semisimple.*

Demostración. Por hipótesis $M = \Sigma_A T_\alpha$, sea $K \leq M$ con $K = \{0\}$ y el Lema 3.4, entonces existe un $B \subseteq A$ tal que $M = \oplus_B T_\beta$ y por tanto M es semisimple. $\square$

Proposición 3.6. *Sea M un R-módulo izquierdo semisimple con la descomposición semisimple $M = \oplus_A T_\alpha$. Si*

$$0 \longrightarrow K \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0,$$

es una sucesión exacta de R-módulos, entonces la sucesión se parte, K y N son módulos semisimples; en efecto, existe un subconjunto $B \subseteq A$ tal que $N \cong \oplus_B T_\beta$ y $K \cong \oplus_{A-B} T_\alpha$.

Demostración. Sabemos que $Im\ f \leq M$ es un submódulo, por el Lema 3.4 existe un $B \subseteq A$ tal que $M = Im\ f \oplus (\oplus_B T_\beta)$, pero como es una sucesión exacta $N \cong M/Im\ f \cong \oplus_B T_\beta$, luego N es semisimple. También $M = \left(\oplus_{A \setminus B} T_\alpha\right) \oplus (\oplus_B T_\beta)$, entonces $p_K| \left(\oplus_{A \setminus B} T_\alpha\right) : \oplus_{A \setminus B} T_\alpha \to K$ es un isomorfismo, luego $K \cong Im\ f \cong \oplus_{A \setminus B} T_\alpha$ así K también es semisimple. $\square$

Corolario 3.7. *Sea $(T_\alpha)_{\alpha \in A}$ un conjunto indexado de submódulos simples de M. Si T es submódulo simple de M tal que $T \cap (\Sigma_A T_\alpha) \neq \{0\}$, entonces existe $\alpha \in A$ tal que $T \cong T_\alpha$.*

DEMOSTRACIÓN. Si T es simple y $T \cap (\Sigma_A T_\alpha) \neq \{0\}$ entonces $T \leq \Sigma_A T_\alpha$ es submódulo del generado pero por la Proposición 3.5, $\Sigma_{\alpha \in A} T_\alpha$ es semisimple y finalmente aplicando la Proposición 3.6, se concluye que $T \cong T_\alpha$ para algún $\alpha \in A$. □

Teorema 3.8. *Para un R-módulo izquierdo las siguientes afirmaciones son equivalentes:*

1. *M es semisimple.*
2. *M es generado por módulos simples.*
3. *M es la suma de algún conjunto de submódulos semisimples.*
4. *M es la suma de sus submódulos simples.*
5. *Cada submódulo de M es un sumando directo.*
6. *Cada sucesión exacta $0 \to K \to M \to N \to 0$ de R-módulos izquierdos es una sucesión que se parte.*

DEMOSTRACIÓN. La implicación 1) $\Rightarrow$ 6) por la Proposición 3.6.

La implicación 6) $\Rightarrow$ 5) es por la Proposición 2.5 y 2) $\Rightarrow$ 1) es por la Proposición 3.5. Las equivalencias 2) $\Leftrightarrow$ 3) $\Leftrightarrow$ 4) son triviales.

5) $\Rightarrow$ 4). Si M satisface que cada submódulo es un sumando directo, cada submódulo no cero de M tiene un submódulo simple. En efecto, si $x \in M$ y $x \neq 0$, entonces por el Lema 3.4, Rx tiene un submódulo maximal. Sea $H \subsetneq Rx$, tal submódulo maximal entonces $M = H \oplus H'$ para algún $H' \subsetneq M$, por la ley modular

$$Rx = Rx \cap M = Rx \cap (H \oplus H') = H \oplus (Rx \cap H')$$

y

$$Rx \cap H' \cong Rx/H.$$

Así que $Rx \cap H' \subsetneq Rx$ es simple.

Sea N la suma de todos los submódulos simples de M, entonces $M = N \oplus N'$, para algún $N' \subsetneq M$, pero también $N \cap N' = \{0\}$, si $N' \neq \{0\}$ existiría $T \subsetneq N'$ submódulo simple , pero $T \subsetneq N$ así que $T \subsetneq N \cap N'$ así que $N \cap N' \neq \{0\}$, lo cual no puede ser. Esto sólo significa que $N' = 0$ y por lo tanto $N = M$. □

3.1.3 El Soclo

De la equivalencia 1) y 2) de la Proposición 3.8, se obtiene que la clase de R-módulos izquierdos semisimples es precisamente la clase de $Gen(\Re)$ de módulos generado por las clases de los R-módulos simple $\Re$.

Definición 3.9. *Sea M un módulo y $\Re$ la clase de los R-módulos simples. El submódulo $H = Tr_M(\Re)$, que es el máximo submódulo semisimple de M, se llamará el Soclo y se denotará como $H = SocM$.*

Es claro ahora que si M es semisimple si y sólo si $M = SocM$.

Proposición 3.10. *Si M es un R-módulo izquierdo entonces*

$$SocM = \Sigma\{K \leq M |\ K \text{ es minimal de } M\} = \cap\{L \leq M |\ L \trianglelefteq M\}$$

Demostración. La primera igualdad se sigue de la definición de Soclo, pues notemos que

$$Tr_M(\Re) = \Sigma\{Im\ h |\ h \in Hom_R(U, M) \text{ con } U \text{ simple}\},$$

es fácil ver que $Im\ h$ es cero o es minimal en M, ya que $Im\ h$ es cero o simple.

Para la otra igualdad, sea T un módulo simple de M. Si $L \trianglelefteq M$, entonces $T \cap L \neq \{0\}$, así $T \leq L$, entonces $SocM$ está contenido en cada módulo esencial de M, por tanto $SocM \subseteq \cap\{L \leq M |\ L \trianglelefteq M\}$. Por otro lado sea $H = \cap\{L \leq M |\ L \trianglelefteq M\}$ afirmamos que H es semisimple, sea $N \leq H$. Si $H' \leq M$ es un complemento de N, entonces $H' + N = H' \oplus N \trianglelefteq M$, por la Proposición 2.30. Como $N \leq H \leq H' \oplus N$, por la ley modular $H = H \cap (H' \oplus N) = N \oplus (H \cap H')$. Entonces N es un sumando directo de H, por la Proposición 3.8.5, H es semisimple; se sigue $H \subseteq SocM$ por lo tanto se da la igualdad. □

Proposición 3.11. *Sean M y N R-módulos izquierdos y sea $f : M \to N$ un R-homomorfismo entonces*

$$f(SocM) \leq SocN.$$

En particular, $SocM$ es un submódulo R-izquierdo $End({}_RM)$-derecho de M.

Demostración. Se sigue de la Proposición 2.74. $\square$

Corolario 3.12. *Sea M un módulo y sea $K \leq M$ entonces*

$$SocK = K \cap SocM$$

en particular,

$$Soc\,(SocM) = SocM$$

Demostración. Por la Proposición 3.11, y tomando a f como la inclusión entonces $SocK \leq SocM$, es claro $Soc\ K \subseteq K$, así que $Soc\ K \leq K \cap Soc\ M$. Por la Proposición 3.6, como $K \cap Soc\ M \leq K$ y $K \cap Soc\ M \leq Soc\ M$, entonces $K \cap Soc\ M$ es semisimple, así que esta contenido en $SocK$. $\square$

Se obtiene que el $SocM$ de M es el submódulo más grande de M contenido en cada submódulo esencial de M. Pero en general $Soc\,M$ puede no ser esencial de M, pues puede suceder el caso en que un módulo sea distinto de cero y el $Soc\,M = \{0\}$ cuando M es cualquier módulo simple.

Corolario 3.13. *Sea M un R-módulo izquierdo, entonces $SocM \trianglelefteq M$ si y sólo si cada submódulo no cero de M contiene un submódulo minimal de M.*

Demostración. La demostración se sigue de la Proposición 3.10 y el Corolario 3.12. Ya que si $Soc\ M \trianglelefteq M$ y $K \neq \{0\}$, entonces $K \cap Soc\ M \neq \{0\}$ entonces $Soc\ K \neq \{0\}$ existe $K_0 \neq \{0\}$ minimal en K, y también es minimal en M. Ahora si $K \neq \{0\}$ y $L \subseteq K$ minimal de M, entonces $L \subseteq Soc\ K = K \cap Soc\ M$ entonces $K \cap Soc\ M \neq \{0\}$ entonces $Soc\ M \trianglelefteq M$ $\square$

Proposición 3.14. *Sea $\eth$ un conjunto representantes de los R-módulos simples, entonces para cada ${}_RM$*

$$SocM = Tr_M\,(\eth) = Tr_M\,(\oplus_{\eth}T) = \Sigma_{\eth}Tr_M\,(T)$$

Demostración. La demostración se sigue de la Proposición 2.78. $\square$

Una consecuencia de la Proposición 3.14, es que la clase de R-módulos semisimples tiene un generador semisimple, el módulo $\oplus_{\eth}T$.

Definición 3.15. *Si T es simple entonces $Tr_M(T)$, es llamada la componente T-homogénea de $SocM$.*

Es claro que $Tr_M(T)$ es generado por un módulo simple, por lo que es semisimple, en $SocM$, por la Proposición 3.10 cada submódulo simple de $Tr_M(T)$ es isomorfo a T. Por ejemplo: la componente $\mathbb{Z}_p$-homogénea de $SocM$ donde M es un grupo abeliano, es el conjunto de los elementos de orden p.

Definición 3.16. *Un módulo semisimple H es T-homogéneo en el caso en que $H = Tr_H(T)$*

Es claro que para cualquier módulo M, la componente T-homogenea del $SocM$ es el único submódulo simple más largo T-homogeneo de M. Si M no tiene un submódulo simple isomorfo a T, entonces la componente T-homogénea de $SocM$ es cero.

3.1.4 El Radical

El radical es el dual del $Soc\,M$ de un R-módulo izquierdo M. Para cada M existe un único módulo cociente más grande generado por $\Re$ (donde $\Re$ es la clase de módulos simples) que coresponde al reject de $\Re$ en M.

Definición 3.17. *Sea $\Re$ la clase de los R-módulos izquierdos simples. Para cada R-módulo izquierdo M el radical de M (Jacobson) es el $Rej_M(\Re) = RadM$*

Proposición 3.18. *Sea M un R-módulo izquierdo, entonces*

$$RadM = \cap\{K \leq M |\ K\ es\ maximal\ en\ M\} = \Sigma\{L \leq M |\ L \ll M\}$$

Demostración. Como $K \leq M$ es maximal de M si y sólo si M/K es simple, la primera igualdad es inmediata de la definición de $Rej_M(\Re) = \cap\{Ker\ h | h : M \to U\ , U \in \Re\}$ (si $h \neq 0$, $U \cong M/Ker\ h$ así que $Ker\ h$ es maximal).

Para la segunda igualdad, sea $L \leq M$ tal que $L \ll M$. Si K es un submódulo maximal de M, y si $L \nleq K$, entonces $K + L = M$, pero como L es superfluo, entonces $K = M$, que contradice la maximalidad de K, entonces $L \subseteq K$. Por lo tanto, cualquier superfluo esta contenido en $RadM$.

Para la otra contención, sea $x \in M$, si $N \leq M$ con $Rx + N = M$, entonces $N = M$ o $N \lneq M$. Si $N \lneq M$, entonces $N \leq K$ con K submódulo maximal. Si $x \in K$ entonces $Rx + N = K = M$ una contradicción, por tanto $x \notin K$. Ahora, si $x \in RadM$, entonces $x \in K$, así que $N = M$. Entonces $Rx \ll M$, por tanto se consigue la igualdad. □

Proposición 3.19. *Sea M y N R-módulos izquierdos y sea $f : M \to N$ un R-homomorfismo, entonces*

$$f\,(RadM) \leq RadN$$

en particular, $RadM$ es un izquierdo R-derecho $End\,({}_RM)$-submódulo de M.

La demostración de se sigue de la Proposición 2.74 y de la Proposición 3.19.

Proposición 3.20. *Si $f : M \to N$ es un epimorfismo y si $Ker\ f \leq RadM$, entonces $Rad\ N = f\,(Rad\ M)$, en particular*

$$Rad\,(M/Rad\ N) = \{0\}.$$

Recordemos que $SocM = M$ si y sólo si M es un módulo semisimple, así también se tiene un resultado dual.

Proposición 3.21. *Sea M un R-módulo izquierdo, entonces $Rad\,M = 0$ si y sólo si M es cogenerado por la clase de módulos semisimple, en particular, si M es semisimple entonces $Rad\,M = \{0\}$.*

Proposición 3.22. *Sea $\Re$ un conjunto representante de R-módulos izquierdo simples, entonces para cada ${}_RM$*

$$Rad\,M = Rej_M\,(\pi_{\Re}T) = Rej_M\,(\oplus_{\Re}T) = \cap_{\Re}Rej_M\,(T)$$

□

El radical de M es el submódulo de M más pequeño que contiene a todos los submódulos superfluos de M, pero el radical no siempre es un submódulo superfluo de M.

Proposición 3.23. *Si cada submódulo superfluo de M está contenido en un submódulo maximal de M, entonces $Rad\,M$ es el único submódulo superfluo más grande de M.*

Demostración. Sea L un submódulo propio de M, y sea K un submódulo maximal con $L \leq K$ entonces por la Proposición 3.18 $L + Rad\,M \leq K \neq M$. Y en otro caso, contiene a todos los superfluos. $\square$

Proposición 3.24. *Si $(M_\alpha)_{\alpha \in A}$ un conjunto indexado de submódulos de M, con $M = \oplus_A M_\alpha$, entonces*

$$SocM = \oplus_A Soc\,M_\alpha \;\; y \;\; Rad\,M = \oplus_A Rad\,M_\alpha$$

$\square$

3.1.5 Módulos Finitamente Generados y Finitamente Cogenerados

Definición 3.25. *Un módulo M es finitamente generado en el caso en que para cada conjunto Ψ de submódulos de M que genera a M, existe un conjunto finito $\Phi \subseteq \Psi$ que genera a M; es decir,*

$$\Sigma\Psi = M \;\; entonces \;\; \Sigma\Phi = M$$

para algún conjunto finito $\Phi \subseteq \Psi$.

Proposición 3.26. *Sea M un R-módulo. Las siguientes afirmaciones son equivalentes:*

1. *M es finitamente generado.*

2. *Para cada conjunto $f_\alpha : U_\alpha \to M$ $(\alpha \in A)$ con $M = \Sigma_A Im\, f_\alpha$, existe un conjunto finito $F \subseteq A$ con $M = \Sigma_F Im\, f_\alpha$.*

3. *Para cada conjunto indexado* $(U_\alpha)_{\alpha\in A}$ *y epimorfismo* $\oplus_A U_\alpha \to M \to 0$, *existe un conjunto finito* $F \subseteq A$ *y un epimorfismo* $\oplus_F U_\alpha \to M \to 0$.

4. *Cada módulo que genera a* M *finitamente lo genera.*

5. M *contiene un conjunto generador finito.*

Demostración. Las implicaciones 1)⇒2) y 3)⇒4) son claras.

2)⇒3) Por la Proposición 2.40, si $f : \oplus_A U_\alpha \to M$ es un epimorfismo si y sólo si $\Sigma_A Im\, f\tau_\alpha = M$, y se tiene $f\tau_\alpha : U_\alpha \to M$ para toda $\alpha \in A$. Sea $\oplus_{\alpha\in F} f_{\tau_\alpha} : \oplus_F U_\alpha \to M$ como $Im \oplus_{\alpha\in F} f_{\tau_\alpha} = \Sigma_{\alpha\in F} Im\ f_{\tau_\alpha} = M$ entonces $\oplus_{\alpha\in F} f_{\tau_\alpha}$ es B_i.

4)⇒5) Se sigue de la Proposición 2.58. 5)⇒1) Supongamos que $\{x_1, ..., x_n\}$ es un conjunto finito generador de M y supongamos que Ξ es un conjunto de submódulos de M con $M = \Sigma\Xi$, entonces para cada x_i existe un subconjunto finito $\Psi_i \subseteq \Xi$ con $x_i \in \Sigma\Psi_i$, sea el conjunto $\Psi = \Psi_1 \cup ... \cup \Psi_n$, entonces Ψ es finito y donde $\Sigma\Psi$ es un submódulo de M que contiene un conjunto generador de M, es decir, M es finitamente generado. □

Definición 3.27. *Un módulo* M *es finitamente cogenerado en el caso en que cada conjunto* Ψ *de submódulos de* M

$$\cap\Psi = \{0\} \ \textit{entonces} \ \cap\Phi = \{0\}$$

para un conjunto finito $\Phi \subseteq \Psi$.

Esta definición es dual a la definición de finitamente generado.

Proposición 3.28. *Sea* M *un* R*-módulo. Las siguientes afirmaciones son equivalentes:*

1. M *es finitamente cogenerado.*

2. *Para cada conjunto* $f_\alpha : M \to U_\alpha$ $(\alpha \in A)$ *con* $\cap_A Ker\, f_\alpha = \{0\}$, *existe un conjunto finito* $F \subseteq A$ *con* $\cap_F Ker\, f_\alpha = \{0\}$.

3. *Para cada conjunto indexado* $(U_\alpha)_{\alpha\in A}$ *y monomorfismo* $0 \to M \to \Pi_A U_\alpha$, *existe un conjunto finito* $F \subseteq A$ *y un monomorfismo* $0 \to M \to \Pi_F U_\alpha$.

Demostración. 1)⇒2) Es clara de la definición. 2)⇒1) Sea $\{M_\alpha |\ \alpha \in A\}$ submódulos de M tal que $\cap_A M_\alpha = \{0\}$, aplicando 2) para los homomorfismos naturales $f_\alpha : M \to M/M_\alpha$ para cada $\alpha \in A$ se sigue 1).

2)⇒3) Supongamos que $f : M \to \Pi_A U_\alpha$ es un monomorfismo, entonces por el Corolario 2.32 $\cap_A Ker\, \pi_\alpha f = \{0\}$. Pero por 2) existe un conjunto finito $L \subseteq A$ tal que $\cap_L Ker\, \pi_\alpha f = \{0\}$, y usando nuevamente el Corolario 2.32, se tiene que $\pi_L f : M \to \Pi_F U_\alpha$ es un monomorfismo. □

Notar que no obtenemos afirmaciones duales de la Proposición 3.26,4 y 5; de hecho no existen como tales, sólo tenemos el siguiente Corolario, ver [4] página 124.

Corolario 3.29. *Si M es finitamente cogenerado, entonces cada módulo que cogenere a M cogenera finitamente a M.*

Demostración. Se sigue de la Proposición 3.28. implicación 2)⇒3). □

Teorema 3.30. *Sea M un R-módulo. Entonces*

1. *M es finitamente generado si y sólo si $M/Rad\, M$ es finitamente generado y el epimorfismo natural*

$$M \to M/Rad\ M \to 0$$

es superfluo, es decir, $Rad\, M \ll M$.

2. *M es finitamente cogenerado si y sólo si $Soc\, M$ es finitamente cogenerado y la inclusión natural*

$$0 \to Soc\, M \to M$$

es esencial, es decir, $Soc\, M \trianglelefteq M$.

Demostración. Probaremos 2). (⇒) Claramente un submódulo de un módulo M finitamente cogenerado es finitamente cogenerado. Será suficiente probar que si M es finitamente cogenerado entonces $Soc\, M \trianglelefteq M$. Supongamos que $K \subseteq M$ tal que $(Soc\, M) \cap K = \{0\}$, como el $Soc\, M$ es la intersección de todos submódulos esenciales de M, pero como M es finitamente cogenerado entonces existen submódulos esenciales $L_1, L_2, ..., L_n$ de M tal que $L_1 \cap ... \cap L_n \cap K = \{0\}$, entonces $(L_1 \cap ... \cap L_n) \trianglelefteq M$ por la Proposición 2.23.2, por lo tanto $K = \{0\}$.

($\Leftarrow$) Sea $Soc\, M$ finitamente cogenerado y $Soc\ M \trianglelefteq M$. Sea Ψ cualquier conjunto de submódulos de M con $\cap\Psi = \{0\}$, entonces $\cap\{A \cap Soc\, M |\ A \in \Psi\} = \{0\}$, entonces

$$(A_1 \cap ... \cap A_n) \cap Soc\, M = (A_1 \cap Soc\, M) \cap ... \cap (A_n \cap Soc\, M) = \{0\}$$

para algunos $A_1, ..., A_n \in \Psi$, pero como $Soc\ M \trianglelefteq M$ entonces $A_1 \cap ... \cap A_n = \{0\}$ □

Corolario 3.31. *Sea M un módulo no cero.*

1. *Si M es finitamente generado, entonces M tiene un submódulo maximal.*

2. *Si M es finitamente cogenerado, entonces M tiene un submódulo minimal.*

Demostración. (1) Sea $\mathcal{H}$ el conjunto de todos los submódulos propios de M, ordenados parcialmente por la inclusión. Sea $\mathcal{T} \subseteq \mathcal{H}$ conjunto totalmente ordenado. Sea L' la suma de todas $L \in \mathcal{T}$, si mostramos que $L' \neq M$ entonces será un límite superior de $\mathcal{T}$ en M y aplicando el Lema de Zorn, encontramos un submódulo propio maximal de M.

Si $L' = M$, entonces L' es finitamente generado por lo tanto existen $x_1, x_2, ..., x_n \in M$ que generan a L', pero cada x_i se encontrará en un módulo que pertenece a $\mathcal{T}$ y por lo tanto $\{x_1, ..., x_n\} \subseteq L_1$ para algún $L_1 \in \mathcal{T}$ entonces $L_1 = M$ una contradicción. □

Proposición 3.32. *Sea M un módulo semisimple, entonces las siguientes afirmaciones son equivalentes:*

a) M es finitamente cogenerado.

b) $M = T_1 \oplus ... \oplus T_n$, con T_i módulos simples para $1 \leqslant i \leqslant n$.

c) M es finitamente generado.

Demostración. (a)⇒(b) Claramente M puede ser encajado en un producto de módulos simples y por la Proposición 3.28.3, entonces M puede ser cogenerado por un producto finito de módulos simples. Es decir, tenemos una sucesión exacta

$$0 \to M \xrightarrow{f} \Pi_{i=1}^{n} T_i = \oplus_{i=1}^{n} T_i \xrightarrow{g} \oplus_{i=1}^{n} T_i / Im\ f \longrightarrow 0,$$

por tanto $M \cong \oplus_{j=1}^{m} T_{i_j}$.

(b)⇒(c) M es generado por un conjunto finito. (Aplicando la Proposición 3.26.1).

(c)⇒(a) Como M es semisimple, es generado por submódulos simples, luego exiten $T_1, T_2, ..., T_n$ submódulos simples que lo generan por (c). Probaremos (a) por inducción sobre n. Para $n = 1$ entonces M es simple y es finitamente cogenerado; asumiendo que se vale para todo $n \geq 2$, es decir, cualquier otro módulo generado por m módulos simples con $m < n$, es finitamente cogenerado. Ahora supongamos que $\Im$ es un conjunto de submódulos de M tal que $\cap \Im = \{0\}$. Entonces $T_n \cap L_0 = \{0\}$ para algún $L_0 \in \Im$, ya que si $T_n \cap L \neq \{0\}$ para todo $L \in \Im$, entonces $T_n \subseteq L$ para toda $L \in \Im$ entonces $T_n \subseteq \cap \Im$, entonces $\cap \Im \neq 0$. Por la Proposición 3.8, como

$$0 \to L_0 \to M \to M/L_0 \to 0$$

es exacta, entonces $L_0 = S_1 \oplus ... \oplus S_m$ con cada S_i submódulo simple para $1 \leq i \leq m$ y $m \leq n-1$, así que L_0 es finitamente cogenerado por hipótesis de inducción. Sea $\Im' = \{N \cap L_0 |\ N \in \Im\}$, notemos que $\Im'$ es un conjunto de submódulos de L_0 con $\cap \Im' = \{0\}$. Por lo que existe un conjunto finito $\{N_1, ..., N_k\} \subseteq \Im$,

$$L_0 \cap N_1 \cap ... \cap N_k = \{0\}$$

y así, M es finitamente cogenerado. □

Proposición 3.33. *Un módulo M es finitamente cogenerado si y sólo si el $Soc(M)$ es esencial y finitamente generado.*

Demostración. Por el Teorema 3.30.2 y la Proposición 3.32 es clara la proposición. □

Proposición 3.34. *Sea $M = M_1 \oplus ... \oplus M_n$. Entonces M es finitamente generado (finitamente cogenerado) si y sólo si cada M_i es finitamente generado (finitamente cogenerados) para $1 \leq i \leq n$.*

Demostración. Notemos que la unión de los conjuntos generadores de los M_i $(1 \leq i \leq n)$, es un conjunto generador de M y es finito, M es finitamente generado por la Proposición 3.26. Ahora mostraremos que los M_i son finitamente cogenerados cuando M lo es. Sabemos por la Proposición 3.24 que

$$Soc\, M = Soc\, M_1 \oplus ... \oplus Soc\, M_n$$

donde los M_i son finitamente cogenerados, cada $Soc\, M_i$ es finitamente generado por la Proposición 3.33, entonces $Soc\ M$ también es finitamente generado. También por 3.33 cada $Soc\, M_i \trianglelefteq M_i$ de donde por la Proposición 2.50 $Soc\, M \trianglelefteq M$. Finalmente aplicando nuevamente 3.33 se obtiene que M es finitamente cogenerado. □

3.2 Condiciones de Cadena

Los módulos para los cuales cada submódulo y cada módulo factor es finitamente generado y finitamente cogenerado respectivamante se pueden caracterizar en términos de las llamadas condiciones de cadena.

Definición 3.35. *Sea $\Re$ un conjunto de submódulos de M. R satisface una condición de cadena ascendente (descendente) si para cada cadena*

$$L_1 \leq L_2 \leq ... \leq L_n \leq ... (L_1 \geq L_2 \geq ... \geq L_n \geq ...)$$

en $\Re$, existe un $n \in \mathbb{N}$ tal que $L_n = L_{n+i}$ $(i = 1, 2, ...)$

Definición 3.36. *Un módulo M es Noetheriano en el caso en que la familia de todos los submódulos de M satisface la condición de cadena ascendente.*

Definición 3.37. *Un módulo M es Artiniano en el caso en que la familia de todos los submódulos de M satisface la condición de cadena descendente.*

Proposición 3.38. *Para un módulo M las siguientes afirmaciones son equivalentes*

a) M es Artiniano.

b) Cada módulo cociente de M es finitamente cogenerado.

c) Cada conjunto no vacío de submódulos de M tiene un elemento minimal.

DEMOSTRACIÓN. a) $\Rightarrow$ c) Sea $\Re$ un conjunto no vacío de submódulos de M y supongamos que $\Re$ no tiene elemento minimal, entonces para cada $L \in \Re$ el conjunto $\{L' \in \Re |\ L' < L\}$ es no vacío. Por el axioma de elección, existe una función de $L \longmapsto L'$ con $L > L'$ para cada $L \in \Re$. Por tanto para cada $L \in \Re$ se tiene

$$L > L' > L'' > ...$$

es una cadena descendente infinita de submódulos de M.

c) $\Rightarrow$ b) Por la correspondencia que existe entre los submódulos de un módulo M y los submódulos del módulo cociente basta ver que si $K \leq M$ y si $\Re$ es una colección de submódulos de M con $K = \cap\Re$, entonces $K = \cap\Im$ para algún subconjunto finito $\Im \subseteq \Re$. Pero el conjunto $\Psi = \{\cap\Im |\ \Im \subseteq \Re\ es\ finito\}$ es no vacío, luego tiene elemento minimal, $\cap\Im_0$. Veamos que $\cap\Im_0 = K$; es claro que $K = \cap\Re \subseteq \cap\Im_0$; si existiera $x \in \cap\Im_0$ tal que $x \notin K$, existe $\tau \in \Re$ tal que $x \notin \tau$ así que $x \notin \cap\Im_1$, donde $\Im_1 = \Im_0 \cup \{\tau\}$ (notar que $\cap\Im_1 \in \Psi$), pero $\cap\Im_1 \subsetneq \cap\Im_0$, lo que contradice que $\cap\Im_0$ es minimal en Ψ.

b) $\Rightarrow$ a) Supongamos que M tiene una cadena descendente

$$L_1 \geq L_2 \geq ... \geq L_n \geq ...$$

de submódulos. definamos $K = \cap_{\mathbb{N}} L_n$. Como M/K es finitamente cogenerado, entonces existe $n \in \mathbb{N}$ tal que $K = L_n$ con la propiedad $L_{n+i} = L_n$ para toda $i \in \mathbb{N}$. $\square$

Resaltaremos que el Axioma de Elección es equivalente al Lema de Zorn 2.29, y puede se consultado en la página 2 de preliminares en [4].

Proposición 3.39. *Para un módulo M las siguientes afirmaciones son equivalentes:*

a) M es Noetheriano.

b) Cada submódulo de M es finitamente generado.

c) Cada conjunto no vacío de submódulos de M tiene elemento maximal.

DEMOSTRACIÓN. La demostración es dual a la Proposición 3.38. □

Corolario 3.40. *Sea M un módulo no cero:*

1. *Si M es Artiniano, entonces M tiene un submódulo simple; el $\operatorname{Soc} M$ es un submódulo esencial de M.*

2. *Si M es Noetheriano, entonces M tiene un submódulo maximal, el $\operatorname{Rad} M$ es un módulo superfluo.*

□

Proposición 3.41. *Sea*

$$0 \longrightarrow K \longrightarrow M \longrightarrow N \longrightarrow 0$$

una sucesión exacta corta de R-módulos. Entonces M es Artiniano (Noetheriano) si y sólo si ambos K y N son Artinianos (Noetherianos).

DEMOSTRACIÓN. ($\Rightarrow$) Sea M un módulo Artiniano. Entonces notemos que K es isomorfo a un submódulo de M, K es Artiniano, se sigue de la definición. También cada módulo cociente de N es isomorfo a un módulo cociente de M, por el Teorema de isomorfismos, y por la Proposición 3.38 es Artiniano.

($\Leftarrow$) Supongamos que K y N son Artinianos. Claramente se tienen las relaciones $K \leq M$ y $M/K = N$, ahora supongamos que

$$L_1 \geq L_2 \geq ... \geq L_n \geq ...$$

es una cadena descendente de submódulos de M. Como $M/K \cong N$ es Artiniano, existe un entero m tal que $L_m + K = L_{m+i} + K$ con $i \in \mathbb{N}$, como K también Artiniano, existe un $n \in \mathbb{N}$ con $n \geq m$ tal que

$$L_n \cap K = L_{n+i} \cap K \ \ con\ i \in \mathbb{N}$$

luego usando la ley modular y sabiendo que $L_n \geq L_{n+i}$, nosotros tenemos que para cada $i \in \mathbb{N}$.

$$L_n = L_n \cap (L_n + K) = L_n \cap (L_{n+i} + K) = L_{n+i} + (L_n \cap K)$$

$$= L_{n+i} + (L_{n+i} \cap K) = L_{n+i}$$

entonces M es Artiniano. La demostración de Noetheriano es dual a ésta. □

Corolario 3.42. *Sea $M = M_1 \oplus ... \oplus M_n$ entonces M es Artiniano (Noetheriano) si y sólo si cada M_i con $1 \leq i \leq n$ es Artiniano (Noetheriano).* □

Proposición 3.43. *Sea M un módulo no cero que tiene una condición de cadena ascendente o descendente sobre sumandos directos, entonces M es el suma directa*

$$M = M_1 \oplus ... \oplus M_n$$

de un conjunto finito de módulos indescomponibles.

Demostración. Para cada módulo no cero M que no tiene una descomposición finita de indescomponible, se escoje una descomposición propia $M = N' \oplus M'$ tal que M' no tiene una descomposición finita de indescomponible y supongamos que M es no cero y que no es una suma directa finita de módulos indescomponibles, entonces $M = N' \oplus M'$, $M' = N'' \oplus M''$,... es una sucesión propia de módulos descomponibles. También existe cadenas infinitas

$$N' < N' \oplus N'' < ... \; y \; M > M' > M'' > ...$$

de sumandos directos de M. Así que es una suma finita de idescomponible. □

Proposición 3.44. *Para cada módulo M las siguientes afirmaciones son equivalentes:*

a) $Rad\, M = 0$ *y M es Artiniano.*

b) *Rad* $M = 0$ *y* M *es finitamente cogenerado.*

c) M *es semisimple y finitamente generado.*

d) M *es semisimple y Noetheriano.*

e) M *es un sumando directo de un conjunto finito de submódulos simples.*

Demostración. a) $\Rightarrow$ b) Ya se tienes que *Rad* $M = \{0\}$ y como es Artiniano por la Proposición 3.38, cada módulo cociente de M es finitamente cogenerado y se sabe que $M \cong M/(Rad\ M)$ luego M es finitamante cogenerado.

b) $\Rightarrow$ c) Como *Rad* $M = \{0\}$ entonces M es semisimple y también M es finitamente cogenerado y por la Propocisión 3.32 entonces M es finitamente generado.

c) $\Rightarrow$ d) M es semisimple y finitamante generado entonces por la Proposición 3.39 M es Noetheriano.

d) $\Rightarrow$ e) M es semisimple y Noetheriano, entonces por la Proposición 3.39 M es finitamante genrado así apricando la Proposición 3.32, $M = \oplus_B T_\beta$ donde $\beta \in B$ y es finito.

e) $\Rightarrow$ a) Si $M = \oplus_B T_\beta$ con B finito entonces es por definición semisimple y cada T_β es simple entonces es Artiniano para cada $\beta \in B$ entonces por el Corolario 3.42 se obtine que M es Artiniano, y si un módulo es semisimple entonces *Rad* $M = \{0\}$. □

Corolario 3.45. *Para cada* M *módulo semisimple las siguientes afirmaciones son equivalentes:*

a) M *es Artiniano.*

b) M *es Noetheriano.*

c) M *es finitamente generado.*

d) M *es finitamente cogenerado.* □

Bibliografía

[1] Herstein I. N., *Topics in Algebra*, John Wiley and Sons, 2nd edition, 1975.

[2] Oscar Zariski and Pierre Samuel *Conmutative Algebra I*, Samuel, Reprinted febrary, 1965.

[3] M. F. Atiyah, I. G. Macdonald, *Introducción al Álgebra Conmutativa*, edición en español, 1980.

[4] Frank W. Anderson, Kent R. Fuller, *Rings and Categories of Módules*, Second Edition, 1991.

[5] Felipe Zaldivar, *Teoría de Galois*, Primera Edición, 1996.

[6] Oswaldo Lezama,*Cuadeno de Álgebra, No. 4, Módulos* , 30 de mayo 2013

www.matematicas.unal.edu.co/sac2/cuadernos/algebralineal.pdf