28
2ej

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

ALGUNAS GENERALIZACIONES DE LAS PROPIEDADES DE LOS GRUPOS DIVISIBLES

T E S I S

Que para obtener el título de:

M A T E M A T I C O

presenta

MONICA PINTOS DE NEYMET

Ciudad Universitaria

México,D.F. 1993

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

INTRODUCCION

Una vez que definimos un objeto matemático y que conocemos sus propiedades, el cuestionamiento natural es: cuando podemos extender dicha definición y en donde siguen siendo válidas dichas propiedades. Responder a estas preguntas es un reto para cualquier estudioso de las matemáticas y la motivación de esta tesis.

Nuestra finalidad es encontrar la clase más general de anillos, en los cuales dos de las condiciones que definen Grupo Abeliano Divisible siguen siendo equivalentes.

En el capítulo uno daremos la definición de grupo abeliano divisible, a partir de algunas de sus equivalencias. Trataremos la primera generalización en el capítulo dos, donde estudiaremos los Dominios de Dedekind, ya que es sobre este tipo de anillos en donde son equivalentes los conceptos de módulo divisible y módulo inyectivo. En el capítulo tres encontraremos hipótesis suficientes y necesarias, para la equivalencia entre la inyectividad de un módulo Q y la condición de que sea cero todo morfismo con domino en Q y codominio en cualquier módulo simple.

CAPITULO UNO

Grupos Abelianos

El propósito de este primer capítulo es estudiar algunas condiciones equivalentes para que un grupo sea divisible.

Advertencia: Con la idea de no hacer reiterativa la redacción y la notación, durante este capítulo hablaremos de grupos y subgrupos refiriéndonos a los abelianos , excepto si se especifica lo contrario.

Definición 1.1 *Un conjunto no vacío de elementos G, se dice que forma un* ***grupo abeliano*** *si en G está definida una operación binaria denotada por +, tal que:*

1. $\forall a,b,c \in G\ a+(b+c)=(a+b)+c$ *(es asociativa)*
2. $\forall a,b \in G\ a+b=b+a$ *(es conmutativa)*
3. $\exists 0 \in G$ *tal que* $\forall a \in G\ a+0=a$ *(neutro)*
4. $\forall a \in G\ \exists -a \in G$ *tal que* $a+(-a)=0$ *(inversos).*

Definición 1.2 *Sea* $H \neq \varnothing$ *un subconjunto de G, decimos que H es* ***subgrupo*** *de G* ($H \triangleleft G$) *si para cualesquiera* $a,b \in H$ *se tiene que a + (-b)* $\in H$.

Nota : Debido a esta definición, H junto con la restricción a H de la operación de adición de G, resuta un grupo.

Ejemplos de subgrupos de G :

- {0}.
- G.
- $\langle a \rangle = \{na : n \in \mathbf{Z}\}$ el subgrupo generado por cualquier a en G.
- Dado K un subgrupo de G, definimos $\langle K,a \rangle = \{ k + na : k \in K \text{ y } n \in \mathbf{Z} \}$.

Donde llamaremos subgrupos impropios de G a los dos primeros.

Es ahora importante hablar de las relaciones que hay entre grupos, para ello estudiaremos a continuación los morfismos de grupos y sus propiedades.

Definición 1.3 *Una aplicación φ de un grupo G a un grupo H se dice que es un* ***morfismo*** *de grupos si para cualesquiera $a,b \in G$ se tiene $\varphi(a+b) = \varphi(a) + \varphi(b)$.*

Ejemplos de morfismos entre grupos son los siguientes:

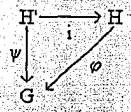
- $i : H \to G$ (la inclusión de un subgrupo).
- $Id : G \to G$ (la identidad).
- $0 : H \to G$ tal que $0 (h) = 0 \ \forall h \in H$.

Definición 1.4 *Dado un diagrama*

$$\begin{array}{ccc} G & \xrightarrow{\psi} & H \\ \varphi \downarrow & & \downarrow \varphi' \\ G' & \xrightarrow{\psi'} & H' \end{array}$$

de grupos y morfismos, se dice que conmuta cuando $\varphi' \psi = \psi' \varphi$.

En el caso particular de que se trate de la inclusión i:



diremos que φ extiende a ψ si el diagrama conmuta.

Definición 1.5 *Sea* $\cdots \to G_{k+1} \xrightarrow{\varphi_{k+1}} G_k \xrightarrow{\varphi_k} G_{k-1} \xrightarrow{\varphi_{k-1}} \cdots$ *una sucesión de grupos y morfismos, diremos que es exacta cuando* $\forall i \quad Im(\varphi_k) = Nuc(\varphi_{k+1})$.

Algunos ejemplos usuales de sucesiones exactas son los siguientes:

$0 \to H \xrightarrow{\varphi} G$ es exacta $\Leftrightarrow \varphi$ es monomorfismo

$G \xrightarrow{\psi} K \to 0$ es exacta $\Leftrightarrow \psi$ es epimorfismo

$0 \to H \xrightarrow{\varphi} G \to 0$ es exacta $\Leftrightarrow \varphi$ isomorfismo

Definición 1.6 *Si* $0 \to H \xrightarrow{\varphi} G \xrightarrow{\psi} K \to 0$ *es exacta entonces* G *es llamada extensión de* H *por* K.

Vamos a estudiar ahora una clase especial de grupos que son llamados simples.

Definición 1.7 *Un grupo* S *se llama* ***simple*** *si* $S \neq \langle 0 \rangle$ *y* S *sólo tiene los subgrupos impropios.*

La siguiente proposición caracteriza a los grupos simples.

Proposición 1.8 *S es simple* $\Leftrightarrow$ *S es finito de orden primo.*

Demostración. $\Rightarrow$) (Por reducción al absurdo). Supongamos que S tiene orden infinito, sea $0 \neq s \in S$, entonces $\langle s \rangle = S$ por lo tanto $\langle s \rangle$ es de orden infinito, así $\langle s^2 \rangle \neq \langle s \rangle$ lo cual contradice la hipótesis de que S es simple.

$\therefore$ S es finito.

Sea n el orden de s y sea p un primo tal que p|n, entonces $\left\langle s^{\frac{n}{p}} \right\rangle$ es un subgrupo de S con orden p, por lo que n=p.

$\Leftarrow$) Sea S un grupo de orden primo p, por el teorema de Lagrange, el orden de cualquier subgrupo de S divide a p, por lo que los únicos subgrupos de S son los impropios.

□

Un resultado inmediato de esta proposición es que los grupos abelianos simples son exactamente los grupos $\mathbf{Z}_p$ con p primo.

Definición 1.9 *Dado* $H \lhd G$ *diremos que es máximo si* $\nexists K$ *tal que* $H \lneq K \lneq G$.

Ejemplo: $n\mathbf{Z}$ es máximo en $\mathbf{Z}$ si y sólo si n es primo.

Otro concepto importante para el estudio de grupos es el de grupo cociente, a continuación trabajaremos con éste y veremos algunas de sus propiedades más importantes.

Vamos a denotar por $a + H = \{ a + x : x \in H \}$, el cual es llamado la clase de a módulo H.

Definición 1.9 *Dado $H \lhd G$ denotaremos por $G/H = \{\overline{a} : \overline{a} = a + H$ tal que $a \in H\}$ e introducimos una operación como sigue:*

$$\overline{a} + \overline{b} = (a+H) + (b+H) = (a+b)+H.$$

Se sigue directamente de la definición que G/H tiene estructura de grupo abeliano con esta operación. Sea π: $G \to G/H$ dado por $\pi(g) = g + H$, éste es conocido como el epimorfismo canónico .

Definición 1.10 *i)Denotaremos por $\prod_{k \in K} A_k$ al grupo formado por los elementos (a_n) en el producto cartesiano de $\{A_k / k \in K\}$ con la operación binaria $(a_n) + (b_n) = (a_n + b_n)$.*

ii) $\bigoplus_{k \in K} A_k$ es el subgrupo de $\prod_{k \in K} A_k$ donde casi todos los elementos de (a_n) son cero es decir sólo un número finito de elementos de (a_n) son distintos de cero.

iii) Dada $\{A_k / k \in K\}$ una familia de subgrupos de G, diremos que G es la ***suma directa*** *interna de $\{A_k\}$ cuando $G = \langle \bigcup A_i \rangle$ y para cada i $A_i \cap \left\langle \bigcup_{i \neq k} A_k \right\rangle = 0$.*

Proposición 1.11 *Sea $\{A_k / k \in K\}$ una familia de subgrupos de G, entonces son equivalentes:*

a) La familia de inclusiones $i_k : A_k \to G$ induce un isomorfismo $f : \bigoplus_{k \in K} A_k \to G$.

b) $\forall g \in G \quad \exists!$ *expresión* $g = \sum_{k \in K} a_k$ *tal que* $a_k \in A_k$ *y* $a_k = 0$ *para casi toda k.*

c) G es la suma directa interna de $\{ A_k \}$.

Demostración. c) $\Rightarrow$ b) Sea $g \in G$, entonces $g \in \left\langle \bigcup_{k \in K} A_k \right\rangle$ así $g = \sum_{k \in K} a_k$ con $a_k \in A_k$ y $a_k = 0$ para casi toda k.

Supongamos que $g = \sum_{k \in K} a_k = \sum_{k \in K} b_k$ y sea $i \in K$, entonces $a_i - b_i = \sum_{k \neq i} (a_k - b_k)$ de c) se sigue $\forall i \quad a_i = b_i$.

b) $\Rightarrow$ a) Supongamos b) y definamos un morfismo $\varphi : G \to \bigoplus_{k \in K} A_k$ por $\varphi(g) = (a_k)$ donde $g = \sum_{k \in K} a_k$, es fácil verificar que esta función es un isomorfismo.

a) $\Rightarrow$ c) Sea $g \in G$ y sea $(a_k) \in \bigoplus_{k \in K} A_k$ tal que $f((a_k)) = g$. De la definición de f se sigue inmediatamente que $g = \sum_{k \in K} a_k$ y que esta representación es única.

□

Proposición 1.12 *Sea V un espacio vectorial, entonces V es isomorfo a una suma directa de copias del campo.* $\left(V \cong F^{(x)} \right)$.

Demostración Sea $B = \{x_k / k \in K\}$ una base de V y $F_k = \langle x_k \rangle$ unidimensional, entonces $\forall k \in K \quad F_k \cong F$ y $V = \langle B \rangle$, así $\forall v \in V$ si $v \neq 0$ entonces $v = \sum_{i=1}^{n} f_{k_i} x_{k_i}$ con $0 \neq f_{k_i} \in F$ además $x_{k_i} \neq x_{k_j}$ si $i \neq j$ y $\forall i \quad f_{k_i} x_{k_i} \in F_{k_i}$.

□

Teorema 1.13 (De la correspondencia biyectiva para grupos abelianos)

Dado H un subgrupo de G se tiene una correspondecia biyectiva, que preserva el orden entre el conjunto de subgrupos de G que contienen a H y el conjunto de los subgrupos de G/H, dada como sigue: si H es un subgrupo de G que contiene a K, entonces el subgrupo de G/H que le corresponde es K/H.

Demostración. 1-1) Sean $H \lhd K \lhd G$ y $H \lhd S \lhd G$ tales que $K/H = S/H$, consideremos $s \in S$ así $s+H \in S/H$, entonces $\exists k \in K$ tal que $s+H = k+H$, por lo tanto $s-k \in H \subseteq K$, así que $s \in K$, lo cual prueba que $S \subseteq K$. Analogamente se verifica que $K \subseteq S$.

suprayectiva) Ahora sea $T \lhd G/H$, entonces definimos $S=\pi^{-1}(T)$, donde $\pi: G \to G/H$ es el epimorfismo canónico, de aquí que $T = S/H$.

orden) Es inmediato del hecho que π^{-1} preserva el orden.

□

Proposición 1.14 *G/H es simple $\Leftrightarrow$ H es máximo en G.*

Demostración. G/H es simple $\Leftrightarrow \nexists K/H \lhd G/H$ tal que $K/H \neq G/H$ y $K/H \neq 0 \Leftrightarrow \nexists K \lhd G$ tal que $H \neq K$ y $K \neq G$.

□

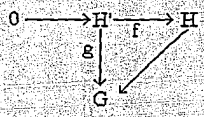
Definición 1.15 *Sean G, H grupos, denotaremos por **Hom(G,H)** al conjunto de morfismos de G en H.*

Teorema 1.16 *Sea G un grupo abeliano, entonces son equivalentes:*

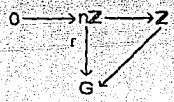
a) $\forall n \in \mathbf{Z}, n \neq 0$ *y* $\forall x \in G \; \exists y \in G$ *tal que* $x=ny$

b) $\forall p \in \mathbf{Z}$, *p primo y* $\forall x \in G \; \exists y \in G$ *tal que* $x=py$

c) Dados $0 \to H' \xrightarrow[f]{} H$ *exacta y* $H' \xrightarrow[g]{} G$ *un morfismo existe un diagrama conmutativo*



d) $\forall n \in \mathbf{N}$ *y* $n\mathbf{Z} \xrightarrow[r]{} G$ *existe un diagrama conmutativo*



e) Todo cociente $G/H \neq 0$ *es infinito.*

f) G no tiene subgrupos máximos.

g) $\forall S$ *simple* $Hom(G,S)=0$.

h) $\forall$ *K tal que* $G \lhd K$ *tenemos que G es sumando directo de K.*

Demostración. a) $\Rightarrow$b) Es un caso particular, ya que $p \in \mathbf{N}$ $\forall p$ primo.

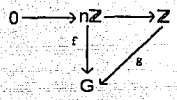
b) $\Rightarrow$a) Por hipótesis, $\forall p$ primo $pG=G$, sea $n \in \mathbf{N}$, por demostrar $nG=G$. $n = p_1 \cdots p_r$ con p_i primo para $i = 1,...,r$. Demostración por inducción sobre r.

i) $r = 1$, $n = p$ por hipótesis $pG = nG = G$.

Supongamos válido el resultado para $r = k$.

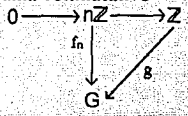
ii) si $r = k+1$ entonces $n = mp_{k+1}$ donde $m = p_1 \cdots p_k$ notemos que por hipótesis $p_{k+1}G = G$ y por hipótesis de inducción $mG=G$, se sigue que $nG = m(p_{k+1}G) = G$.

a) $\Rightarrow$d) Sean $n \in \mathbf{N}$, $n \neq 0$ y $f: n\mathbf{Z} \to G$, entonces si $f(n) = x$ tenemos que $\exists$ y tal que $x = ny$, definimos $g : \mathbf{Z} \to G$ por $g(m) = my$ $\forall\, m \in \mathbf{Z}$. Tenemos que el diagrama



conmuta.

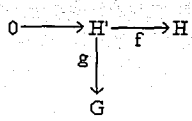
d) $\Rightarrow$a) Sean $n \in N$ y $x \in G$, definimos $f_n : n\mathbf{Z} \to G$ tal que $f_n(nm)=mx$ para cada $m \in \mathbf{N}$, por hipótesis existe un diagrama conmutativo



Si $y = g(1)$, entonces $ny = n\, g(1) = g(n) = x$. Lo cual demuestra a).

c) $\Rightarrow$d) Caso particular.

d) $\Rightarrow$c) Consideremos



supongamos, sin pérdida de generalidad, que $H' \lhd H$, y definamos $\wp$ como sigue:

$\wp = \{(K, f_k) : H' \lhd K \lhd H, f_k : K \to G \text{ tal que } f_k|_{H'} = f\}$ con el orden parcial $(K_1, f_{k_1}) \leq (K_2, f_{k_2})$ siempre que :

i) $K_1 \subseteq K_2$

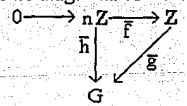
ii) $f_{k_2}|_{K_1} = f_{k_1}$

Sea $(K_1, f_{k_1}) \leq (K_2, f_{k_2}) \leq \cdots$ una cadena de elementos de $\wp$, si $K_0 \in \bigcup_{i \in N} K_i$, entonces $K_0 \lhd H$ tal que $H' \lhd K_0$ sea $f_0 : K_0 \to G$ definida como sigue: sea $x \in K_0$, entonces $\exists i \in \mathbf{N}$ tal que $x \in K_i$, así $f_0(x) = f_{k_i}(x)$.

Notemos que f_0 está bien definida ya que es la extensión de las f_{k_i}, así $f_0|_{H'} = f'$ por lo que $(K_0, f_0) \in \wp$ y $\forall i \in \mathbf{N}\ (K_i, f_{k_i}) \leq (K_0, f_0)$, así toda cadena ascendente tiene cota superior, entonces por el lema de Zorn (ver apéndice) $\exists (K, h)$ máximo en $(\wp, \leq)$.

Sabemos que $(H', f) \leq (K, h)$, falta ver que K=H, ésto se hará por reducción al absurdo: Supongamos que $K \lhd H$, sea $z \in$ H-K y $n = \min\{m \in \mathbf{N} : mz \in K\}$, entonces $n\mathbf{Z} = \{m \in \mathbf{Z} : mz \in K\}$ es un ideal de $\mathbf{Z}$, definamos para $m \in n\mathbf{Z}$, $\overline{h} : n\mathbf{Z} \to G$ tal que $\overline{h}(m) = h(mz)$ claramente es un morfismo ya que es la composición de morfismos.

Por hipótesis existe el siguiente diagrama conmutativo



Consideremos ahora $\langle K, z \rangle \lhd H$ tal que $\langle K, z \rangle = \{x + bz : x \in K \text{ y } b \in \mathbf{Z}\}$ así $K \lhd \langle K, z \rangle$, ya que $z \in \langle K, z \rangle$.

Definamos $h' : \langle K, z \rangle \to G$ tal que $h'(x + bx) = h(x) + b\overline{g}(1)$. Veamos que h' está bien definida; supongamos que $x + bz = z' + b'z$, ésto implica que $x - x' = (b' - b)z$ donde $x - x' \in K$ y $(b - b')z \in nZz$, además:

$\overline{h}(b'-b) = \overline{h}((b'-b)z) = h(x-x') = h(x) - h(x')$ y

$\overline{g}(b'-b) = \overline{g}(b) - \overline{g}(b) = b'(\overline{g}(1)) - b(\overline{g}(1))$ donde $\overline{h}(x) - \overline{h}(x') = b'(\overline{g}(1)) - b(\overline{g}(1))$

entonces $\overline{h}(b'-b) = \overline{g}(b'-b)$

$\therefore \quad \overline{h}(x) + b(\overline{g}(1)) = \overline{h}(x') + b'(\overline{g}(1))$

es decir $h'|_K = h$, lo que contradice que K es máximo.

$$\therefore K = H.$$

e) $\Rightarrow$f) Demostración por reducción al absurdo. Supongamos que K es máximo, entonces G/K es simple, por lo que G/K es finito, lo que contradice la hipótesis.

f) $\Rightarrow$g) Demostración por reducción al absurdo. Supongamos que G no tiene subgrupos máximos, sea S simple y $\varphi \in \mathrm{Hom}(G,S)$, entonces tenemos dos casos:

i) $\varphi = 0$ ✓

ii) $G \xrightarrow{\varphi} S \to 0$. Sea $H = \mathrm{Nuc}(\varphi)$, por lo que $S \cong G/H$, entonces G/H es simple. se sigue que H máximo lo que contradice la hipótesis.

g) $\Rightarrow$e) Demostración por reducción al absurdo. Supongamos que $\forall$ S simple $\mathrm{Hom}(G,S)=0$, y que $\exists$ $H \lhd G$ tal que $0 \neq G/H$ es finito, sea K/H un subgrupo máximo de G/H, entonces el epimorfismo canónico $\pi: G \to G/K$ contradice la hipótesis.

f) $\Rightarrow$b) Demostración por reducción al absurdo. Supongamos que G no tiene subgrupos máximos y que hay p primo tal que $pG \neq G$.

Consideremos $G/pG \neq 0$ como $\mathbf{Z}_p$-espacio vectorial con la operación: $(n + p\mathbf{Z})\, x = nx$.

Si $n + p\mathbf{Z} = m + p\mathbf{Z}$, entonces $n - m = kp$, asi :

$(n + p\mathbf{Z}) x = (m + p\mathbf{Z}) x = nx = mx$

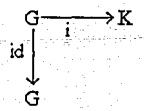
y $(n-m)x = (kp)x = (p\mathbf{Z})x$ y $x \neq 0$, se sigue que n=m, por lo tanto no importa la elección del representante, es decir, el espacio está bien definido.

. Por 1.12 $G/pG \cong \mathbf{Z}_p^X$. Sea $x \in X$ así $\mathbf{Z}_p^{X-\{x\}}$ es máximo en $\mathbf{Z}_p^X$, entonces $\mathbf{Z}_p^{X-\{x\}} \cong N/pG$ máximo en G/pG, así por 1.13 N es máximo en G, lo que contradice la hipótesis. Por lo tanto se cumple b).

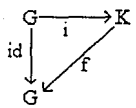
a) $\Rightarrow$f) Demostración por reducción al absurdo. Sea G con la propiedad a), supongamos que $\exists$ M $\lhd$ G máximo, así G/M es simple, por lo que $|G/M| < \infty$, entonces por 1.7, $\exists p \in \mathbf{N}$ tal que $G/M \cong \mathbf{Z}_p$, pero $\mathbf{Z}_p$ no cumple con la propiedad a), sea $0 \neq n \in \mathbf{Z}_p$, y $p \in \mathbf{N}$ entonces la ecuación $n = pm$ no tiene solución, entonces G/M no cumple con dicha propiedad, y por lo tanto G tampoco, lo que contradice la hipótesis.

$\therefore \nexists$ M $\lhd$ G máximo.

c) $\Rightarrow$ h) Sea G un subgrupo de K y supongamos que G tiene la propiedad c), consideremos el diagrama



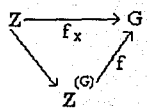
por hipótesis, existe un morfismo $f: K \rightarrow G$ tal que el diagrama



conmuta. Se obtiene de aquí que K es isomorfo a $G \oplus Nuc(f)$.

conmuta. Se obtiene de aquí que K es isomorfo a $G \oplus Nuc(f)$.

h) $\Rightarrow$ a) Sea G un grupo y $\forall\, x \in G$ definimos $f_x : \mathbf{Z} \to G$ por $f_x(n) = nx$, así por la propiedad universal de la suma directa $\exists$ f: $\mathbf{Z}^{(G)} \to G$ tal que conmuta el siguiente diagrama



para toda x. Claramente es un epimorfismo. Ahora, sea K el núcleo de este morfismo, entonces existe un monomorfismo $G \to {}^{Q^{(G)}}\!/_{K}$ inducido por la inclusión de $\mathbf{Z}$ en $\mathbf{Q}$. Si G satisface la propiedad h), entonces G es sumando directo de ${}^{Q^{(G)}}\!/_{K}$ y por lo tanto satisface la propiedad a).

□

Definición 1.17 *Diremos que G es* ***divisible*** *si cumple con las condiciones del teorema 1.16.*

CAPITULO DOS

Dominios Enteros

Tenemos en este capítulo dos objetivos: Primero definiremos el concepto de R-módulo divisible, para lo que debemos restringirnos a la categoría de dominios enteros. Con esta definición veremos cuando los conceptos de inyectivo y divisible siguen siendo equivalentes.

Advertencia: Durante el capítulo la notación que manejaremos es la siguiente: R es un anillo con 1 y D es un dominio entero, es decir, D es un anillo conmutativo con 1 y sin divisores de cero.

Definición 2.1 *Sea R un anillo con $1 \neq 0$, diremos que M es un* ***R-módulo*** *izquierdo, si $\langle M,+\rangle$ es un grupo abeliano y esta definida una operación escalar tal que $\forall m_1,m_2 \in M$ y $\forall r_1,r_2 \in R$ tenemos:*

i) $r_1(m_1 + m_2) = r_1m_1 + r_1m_2$

ii) $(r_1 + r_2)m_1 = r_1m_1 + r_2m_1$ *(es bilineal)*

iii) $(r_1r_2)m_1 = r_1(r_2m_1)$ *(es asociativa)*

iv) $1m_1 = m_1$ *(tiene neutro)*

Algunos ejemplos de módulos son:

- 0, el módulo que sólo tiene al cero.
- Los **Z**-módulos son los grupos abelianos.
- Si K es un campo, entonces los K-módulos son los K-espacios vectoriales.

Muchas definiciones y resultados de las categorías de grupos abelianos y espacios vectoriales se pueden generalizar a la teoría de módulos, por lo que algunos conceptos y propiedades no los trataremos aquí, para no ser reiterativos.

Definición 2.2 *Dados M,N R-módulos, $\varphi: M \to N$ es un* ***R-morfismo si:***

i) $\forall m_1, m_2 \quad \varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2)$

ii) $\forall m \in M \ \forall r \in R \quad \varphi(rm) = r\varphi(m)$

Los llamaremos sólo morfismos y tenemos para ellos las mismas definiciones y propiedades que para grupos abelianos con respecto a núcleos, imágenes, sucesiones, exactitud, etcetera.

Definición 2.3 *Diremos que la sucesión exacta* $0 \to M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \to 0$, *se* ***escinde****, si Im(φ) es sumando directo de M.*

Notemos que dada una sucesión exacta $0 \to M' \to M \to M'' \to 0$ que se escinde tenemos morfismos $M'' \to M \to M'$ que inducen una representación de M como suma directa.

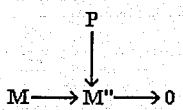
Definición 2.4 *Sea M un módulo y $X \subseteq M$, diremos que M es* ***libre con base X si:*** $\forall m \in M$ $\forall x \in X \; \exists r_x \in R$ *tal que* $\sum_{x \in X} r_x x = m$ *, donde* $r_x = 0$ *para casi toda* $x \in X$ *y esta representación es única.*

Observemos que el módulo $R^{(X)}$ es libre con base $\{e_x : x \in X\}$. Denotaremos a este módulo por L_X.

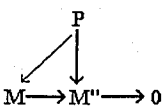
Proposición 2.5 *Dado M un R-módulo,* $\exists \; 0 \to R_M \to L_M \xrightarrow{\varphi} M \to 0$ *exacta, donde* $\varphi((r_x)) = \sum_{x \in M} r_x x$ *y* $R_M = Nuc(\varphi)$.

La demostración es inmediata de la definición de módulo libre.

Definición 2.6 *Sea P un R-módulo, diremos que P es* ***proyectivo*** *si dado el siguiente diagrama:*



existe



que hace conmutar el diagrama.

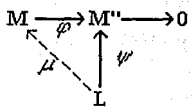
Es de gran interés ver que relaciones hay entre el concepto de proyectivo y los anteriores, es inmediato ver que una suma directa es proyectiva, si y sólo si cada sumando es proyectivo, en lo sucesivo veremos otras proposiciones con respecto a esto.

Proposición 2.7 *P es proyectivo* $\Leftrightarrow$ *P es sumando directo de un módulo libre.*

Demostración. $\Rightarrow$) Consideremos $0 \to R_P \to L_P \xrightarrow{\varphi} P \to 0$, como P es proyectivo entonces $\exists\ \psi : P \to L_P \ni \varphi\psi = id$ así la sucesión se escinde.

$\therefore$ P es sumando directo de L_P.

$\Leftarrow$) Basta demostrar que todo módulo libre es proyectivo. Consideremos



y definamos $\mu : L \to M$ como sigue para cada $x \in X$, donde X es la base de L elegimos un elemento $\mu(x) \in M$ con la propiedad que $\varphi(x) \in \varphi^{-1}(\psi(x))$. Esta función se extiende naturalmente a un morfismo $\mu : L \to M$.

□

Teorema 2.8: *Todo R-módulo M es el cociente de un proyectivo.*

Demostración. $0 \to R_M \to L_M \xrightarrow{\varphi} M \to 0$ es exacta y L_M es proyectivo.

□

Proposición 2.9 *Sea P un R-módulo izquierdo entonces son equivalentes:*

a) P es proyectivo.

b) $\forall 0 \to M' \to M \to P \to 0$ *exacta se escinde.*

c) $\exists\, X = \{x_i\} \subseteq P$ *y* $\exists \{\varphi_i : P \to R\}$ *tales que* $\forall\, p \in P \quad p = \sum_i (\varphi_i(p)) x_i$ *y* $\varphi_j(p) = 0$ *para casi toda j y para cada p.*

Demostración. a) $\Rightarrow$b) Idem 2.7.

b) $\Rightarrow$a) En particular $0 \to R_P \to L_P \to P \to 0$ se escinde, entonces P es sumando directo de L_P, por 2.7 concluimos que P es proyectivo.

a) $\Rightarrow$c) Sea $\psi : L \to P$ morfismo donde L es libre con base (e_α), definimos $m_i = \psi(e_i)$ entonces por la parte anterior $\varphi : P \to L \ni \varphi\psi = id$...(*), entonces se puede definir $\varphi(a) = \sum_\alpha (\varphi_\alpha(a)) e_\alpha$ donde $\varphi_\alpha : P \to R$ tal que $\varphi_\alpha(a) = 0$ para casi toda α por (*) tenemos que $\forall p \in P \quad p = \sum_\alpha (\varphi_\alpha(p)) x_\alpha$ y $\varphi_j(p) = 0$ para casi toda j y para cada p.

c) $\Rightarrow$a) Sea $f : L_X \to P$ dado por $f((r_{x_i})) = \sum_i r_{x_i} x_i$ el cual claramente es un epimorfismo. Ahora, sea $g : P \to L_X$ dado por $g(p) = (\varphi_i(p))$. Tenemos $fg = id$.

□

Definición 2.10 *Sea D un dominio entero y Q su campo de cocientes, diremos que* $I \leq D$ *es* ***invertible*** *si* $\exists \{a_1, a_2, \ldots, a_n\} \subseteq I$ *y* $\exists \{q_1, q_2, \ldots, q_n\} \subseteq Q$ *tales que:*

i) $\forall i \leq n$ *se tiene* $q_i\, I \subseteq D$

ii) $1 = \sum_{i=1}^{n} q_i\, a_i$

Son validas las siguientes condiciones:

1. Todo ideal principal diferente de cero es invertible, ya que si $I = Da$ entonces tomamos $a = a_1$, $\frac{1}{a} = q_1$ y $n=1$.

2. Si I es invertible tenemos que $I = < a_1, a_2, \ldots, a_n >$.

3. Otra forma de definir ideal invertible es la siguiente: $\forall I \; \exists M \leq Q$ tal que $IM = D$. (En el ejemplo 1 tenemos que la M correspondiente a Da debe ser Da^{-1}).

Veamos ahora más propiedades de estos ideales que necesitaremos para llegar al resultado central de este capítulo.

Proposición 2.11 *Si I invertible, entonces el submódulo M de Q tal que IM = D es único. Por lo que lo denotaremos por* I^{-1}.

Demostración. Supongamos que $I M = D$, entonces $M \subset [D : I]$, además $I [D : I] \subset D$ así, como M es un inverso de I, tenemos que $[D : I] = M I [D : I] \subset MD = M$.

Entonces $M = [D : I]$ y es único.

□

La proposición 2.11 nos da las condiciones suficientes y necesarias para encontrar el inverso de I, un corolario inmediato de dicha proposición es que I es invertible si y sólo si **$I [D : I] = D$.**

Definición 2.12 *Sea D un dominio entero y Q su campo de cocientes, consideremos J un D-submodulo de Q, diremos que es* ***fraccionario*** *cuando* $\exists d \in D$ *tal que* $dJ \leq D$.

Proposición 2.13 *Todo ideal fraccionario J, puede escribirse de la forma* $\frac{1}{d} I$ *donde* $d \in D$ *e I es un ideal de D.*

Demostración. Sea J un ideal fraccionario. Entonces $\exists\ d \in D$ tal que $dJ \leq D$, sea $I = \{dx \in D : x \in J\}$, tenemos entonces $dJ = I$ y claramente I es un ideal de D.

□

Proposición 2.14 *Si todo ideal diferente de cero es invertible, entonces todo ideal fraccionario es invertible.*

Demostración. Por la Proposición 2.12 tenemos que $J = \frac{1}{d} I$, donde I es un ideal de D y por hipotesis, I es invertible; sea I^{-1} su inverso, así $I^{-1}I = D \Rightarrow I^{-1}d\frac{1}{d}I = dI^{-1}J = D$.

$$\therefore J^{-1} = dI^{-1}$$

□

Proposición 2.15 *Si una familia* $\{I_\alpha\}$ *finita de ideales es tal que* $I = \prod_\alpha I_\alpha$ *es invertible, entonces, cada* I_α *es invertible.*

Demostración. Consideremos $I^{-1} \cdot \prod_\alpha I_\alpha = D$, se deduce que $I_\beta \cdot (I^{-1} \cdot \prod_{\alpha \neq \beta} I_\alpha) = D$, por lo tanto $(I^{-1} \cdot \prod_{\alpha \neq \beta} I_\alpha)$ es el inverso de I_β.

□

Teorema 2.16 *Sea D un dominio entero e* $I \leq D$ *entonces, I es proyectivo* $\Leftrightarrow$ *I es invertible.*

Demostración. $\Rightarrow$) Sean $\{x_i\}, \{\varphi_i\}$ como en 2.9 c). Así $\forall i\ a(\varphi_i(b)) = \varphi_i(ab) = b(\varphi_i(a))$, definamos para $x \neq 0\ \ q_i = \frac{\varphi_i(x)}{x}$ así $q_i \in Q$ y $\forall a \in I\ \ \varphi_i(a) = q_i a$ por lo tanto $q_i I \subset D$ y si $a \neq 0$ tenemos, para casi toda i, $\varphi_i(a) = q_i a = 0$.

Además si $a \neq 0$ tenemos $a = \sum_i (\varphi_i(a))x_i = \sum_i (q_i(a))x_i = a\sum_i q_i x_i$ lo que es equivalente a que $1 = \sum_i q_i x_i$ ya que D no tiene divisores de cero.

$\therefore$ I es invertible.

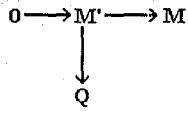
$\Leftarrow$) Definamos $\varphi_i(x)= q_i x$ con $x \in I$ entonces $\varphi_i : I \to D$ y $\sum_i (\varphi_i(x))x_i = \sum_i q_i x x_i = x \sum_i q_i x_i = x1 = x$.

$\therefore$ I es proyectivo.

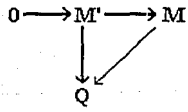
□

Definición 2.17 *Diremos que un D-módulo M es* ***divisible*** *cuando* $\forall m \in M$ $\forall r \in D$, $r \neq 0$ $\exists m' \in M$ *tal que* $m = rm'$.

Definición 2.18 *Dado Q, R-módulo diremos que es* ***inyectivo*** *si y sólo si, dado:*



existe



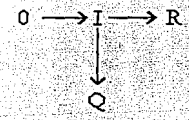
que hace conmutar el diagrama.

Se sigue de la definición que un producto directo es inyectivo si y sólo si cada factor es inyectivo, este es el concepto dual de módulo proyectivo y veremos ahora algunas de sus propiedades.

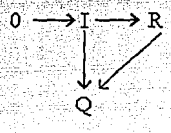
Teorema 2.19 (Criterio de Baer) *Sea Q un R-módulo entonces son equivalentes:*

a) *Q es inyectivo.*

b) $\forall I \leq R$ *dado el diagrama*

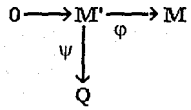


existe un diagrama conmutativo



Demostración. a) $\Rightarrow$b) Caso particular.

b) $\Rightarrow$a) Consideremos el diagrama



Primero encontraremos una extensión de ψ a un módulo mayor por lo que la prueba se hará en dos partes :

i) Sin pérdida de generalidad, supongamos que M'≤M, consideremos la familia $\delta=\{(K,\psi_K): M' \leq K \leq M,\ \psi_K : K \to Q,\ \psi_K|_{M'} = \psi\}$ con el orden ≤ definido como sigue: $(K_1,\psi_{K_1}) \leq (K_2,\psi_{K_2})$ cuando a) $K_1 \subseteq K_2$ y

b) $\psi_{K_2}|_{K_1} = \psi_{K_1}$.

Veamos que $(\delta,\leq)$ es inductivo (ver definición en el apendice), claramente por la definición del orden se trata de un orden parcial, ya que $\subseteq$ lo es, ahora consideremos $(K_1,\psi_{K_1}) \leq (K_2,\psi_{K_2}) \cdots$ una cadena ascendente de elementos de S, observemos que si $K_0 = \bigcup_{i\in N} K_i$ entonces K_0 es un submódulo de M tal que $M' \leq K_0 \leq M$, construyamos $\psi_0 : K_0 \to Q$ con la propiedad siguiente, dada $x \in K_0$ entonces $\exists i \in N$ tal que $x \in K_i$ así $\psi_0(x) = \psi_i(x)$. El morfismo ψ_0 esta bien definido, ya que $\forall i \in N\ \psi_0|_{Ki} = \psi_{K_i}$ y por lo tanto $\psi_0|_{M'} = \psi$, así $(K_0,\psi_0) \in \delta$ y además tenemos que $\forall i \in N\ (K_i,\psi_{K_i}) \leq (K_0,\psi_0)$, por lo tanto toda cadena de δ tiene cota superior, entonces usando el lema de Zorn (ver apendice) tenemos que $\exists (K,\varphi)$ máximo en $(\delta,\leq)$.

ii) Sabemos que $(M',\psi) \leq (K,\varphi)$, demostremos que K=M. La demostración la haremos por reducción al absurdo. Supongamos que $K \neq M$, así $K < M$ por lo que $\exists\ m \in M - K$. Consideremos $I=(K:m)=\{r \in R : rm \in K\}$ que es un ideal izquierdo de R y definamos $\overline{\phi} : I \to Q$ tal que $\overline{\phi}(r) = \varphi(r\,m)$, claramente $\overline{\phi}$ es un R-morfismo. Entonces $\exists \overline{\varphi} : R \to Q$ tal que $\overline{\varphi}\,|_I = \overline{\phi}$.

Sea $\langle K,m\rangle = \{x + r\,m : x \in K \text{ y } r \in R\} \leq M$ así $K < \langle K,m\rangle$ de hecho es el mínimo submódulo de M que contiene a K y a m, definamos entonces $\varphi' : \langle K,m\rangle \to Q$ tal que $\varphi'(x + r\,m) = \varphi(x) + r\overline{\varphi}(1)$, demostraremos que está bien definido: Supongamos que $x + r\,m = x' + r'\,m$ así $x - x' = (b' - b)\,m$ donde $x - x' \in K$ y $b' - b \in I$ ya que φ manda a m dentro de K. Entonces:

$\overline{\phi}(r' - r) = \varphi((r' - r)\,m) = \varphi(x' - x) = \varphi(x') - \varphi(x)$ y por otro lado

$\overline{\phi}(r' - r) = \overline{\varphi}(r' - r) = \overline{\varphi}(r') - \overline{\varphi}(r) = r'\,\overline{\varphi}(1) - r\,\overline{\varphi}(1)$ así

$\varphi(x) + r\,\overline{\varphi}(1) = \varphi(x') + r'\,\overline{\varphi}(1)$ y $\varphi'|_K = \varphi$ lo que contradice el hecho que K es máximo.

$\therefore\ K = M$

□

Esta es la generalización a la categoría de módulos de la equivalencia de los incisos c) y d) del teorema 1.16. Notemos que esta caracterización de módulos inyectivos, no es exclusiva de dominios enteros.

Lema 2.20 *Sea G un grupo divisible, entonces $Hom_Z(R,G)$ es un R-módulo izquierdo inyectivo.*

Demostración. Sea $0 \to M' \xrightarrow{f} M$ exacta y $M' \xrightarrow{} Hom_Z(R,G)$, definimos un morfismo $g': M' \to G$ por $g'(m) = g(m)(1)$, el cual es claramente aditivo. Dado que G es divisible, hay un morfismo $h' : M \to G$ tal que extiende a g', definimos un morfismo $h : M \to Hom_Z(R,G)$ por $h(m)(r) = h'(r\,m)$. Es fácil verificar que este morfismo extiende a g.

□

Proposición 2.21 *Dado M un R-módulo, hay un módulo Q inyectivo tal que $0 \to M \to Q$ es exacta. (e.d. Todo módulo M es submódulo de un inyectivo Q.)*

Demostración. Consideremos un monomorfismo de grupos abelianos $M \xrightarrow{f} G$ donde G es un grupo divisible (ver teorema 1.16). Ahora consideremos la siguiente sucesión de monomorfismos:

$$M \xrightarrow{\varphi} Hom_R(R,M) \xrightarrow{\psi} Hom_Z(R,M) \xrightarrow{\lambda} Hom_Z(R,G)$$

donde $\varphi(m)(r) = r\,m$, ψ es la inclusión natural y λ es el morfismo inducido por f. La composición de estos tres morfismos es el monomorfismo que buscamos.

□

Proposición 2.22 *$\forall Q$ inyectivo toda sucesión exacta* $0 \to Q \to M \to M'' \to 0$ *se escinde.*

Demostración. Es inmediato del hecho que la $id : Q \to Q$ se extiende a una función $f : M \to Q$ que nos da la escisión.

□

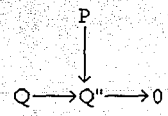
Proposición 2.23 *Dado M un D-módulo inyectivo se tiene que M es divisible.*

Demostración. Sea M inyectivo, $m \in M$ y $r \in D$ con $r \neq 0$, consideremos el ideal $I = rD$. Consideremos $\varphi : I \to M$ tal que $\varphi(ra) = r\,m$, el cual claramente está bien definido por ser D un domino entero y es un monomorfismo, sea $\psi : D \to M$ una extensión de φ y sea $n = \psi(1)$ así $m = \varphi(r) = \psi(r) = r\,n$.

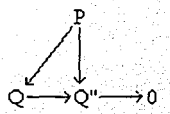
$\therefore$ M es divisible

□

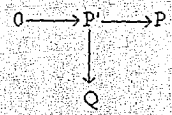
Proposición 2.24 *i) P proyectivo $\Leftrightarrow$ Dado*



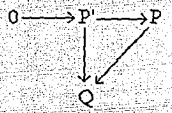
con Q inyectivo, existe un diagrama conmutativo



ii) Q inyectivo⇔ Dado

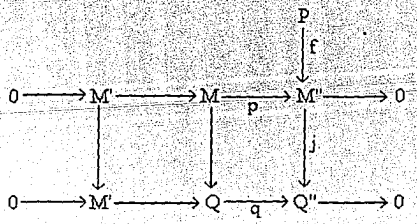


con P proyectivo, existe un diagrama conmutativo



Demostración. i) ⇒) Caso particular.

⇐) Sea $M' \leq M$, $M'' = M/M'$, $f : P \to M''$ un morfismo, $M \to Q$ una inclusión, donde Q es inyectivo y $Q'' = Q/M'$, tenemos entonces el siguiente diagrama conmutativo:



donde los renglones son exactos j es el monomorfismo inducido por la inclusión de M en Q.

Por hipótesis $\exists\, g : P \to Q$ tal que $q\, g = j\, f$.

Sea $x \in P$ y tomamos $y \in M$ tal que $p(y) = f(x)$.

Tenemos q (y) = j p (y) = j f (x) = q g (x), entonces z = g(x) - y ∈M', así g(x) = z + y ∈ M, es decir, el morfismo g se puede considerar como un morfismo de P en M.

∴ P es proyectivo.

ii) Se prueba analogamente.

□

Definición 2.25 *Un anillo R se llama* ***hereditario izquierdo*** *si todo ideal izquierdo I de R es proyectivo y es* ***semihereditario izquierdo*** *si todo ideal izquierdo de tipo finito es proyectivo.*

La siguiente proposición da varios ejemplos de anillos hereditarios:

Proposición 2.26 $\forall n \in \mathbf{Z}$ *son equivalentes:*

a) $\mathbf{Z}_n$ *es semisimple*

b) $\mathbf{Z}_n$ *es hereditario*

c) n es producto de primos distintos.

Demostración. a) $\Rightarrow$b) Caso particular.

b) $\Rightarrow$c) Sea $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, entonces $\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{r_1}} \times \cdots \times \mathbf{Z}_{p_k^{r_k}}$ y es claro que $\mathbf{Z}_n$ es hereditario si y sólo si cada factor lo es. Debemos probar entonces la implicación para $n = p^r$, es decir que $r = 1$.

Supongamos que $r > 1$, así el ideal $p\mathbf{Z}_{p^r}$ es esencial en el anillo, si fuese proyectivo el epimorfismo $\mathbf{Z}_{p^r} \to p\mathbf{Z}_{p^r}$ se escindiría, lo que implicaría que $p\mathbf{Z}_{p^r}$ es sumando directo de $\mathbf{Z}_{p^r}$ lo cual es una contradicción. Por lo tanto vale la condición c).

c) $\Rightarrow$a) Supongamos que $n = p_1 p_2 \cdots p_k$ con $p_i \neq p_j$ si $i \neq j$, entonces $\mathbf{Z}_n \cong \mathbf{Z}_{p_1} \times \cdots \times \mathbf{Z}_{p_k}$ con cada $\mathbf{Z}_{p_i}$ simple por 1.8 :

$\therefore \mathbf{Z}_n$ es semisimple.

□

Teorema 2.27 (Kaplansky) *Si R es hereditario L libre entonces* $\forall N \leq L$, *tenemos* $N = \oplus I_\alpha$ *donde* $\forall \alpha$ I_α *es un ideal de R.*

Demostración. $\Rightarrow$) Sea L libre con base $\{x_\alpha\}_{\alpha \in A}$ bien ordenada, definamos $\overline{L}_\alpha = \langle \{x_\beta \ / \ \beta \leq \alpha\} \rangle \leq L$ y $L_\alpha = \langle \{x_\beta \ / \ \beta < \alpha\} \rangle \leq L$, sea $N \leq L$ tenemos que $\forall a \in N \cap \overline{L}_\alpha$ $a = b + \lambda x_\alpha$ con $b \in L_\alpha$ y $\lambda \in R$. El morfismo $\varphi : N \cap \overline{L}_\alpha \to R$ tal que $\varphi(a) = \lambda$ tiene como imagen un ideal I_α de R que tiene que ser proyectivo, es claro que $N \cap L_\alpha = \ker(\varphi)$, entonces $N \cap \overline{L}_\alpha \cong (N \cap L_\alpha) \oplus I_\alpha$.

Es claro que $N \cap L_\beta = \bigcup_{\gamma < \beta} N \cap \overline{L}_\gamma$ y por lo tanto $N \cap L_\beta \cong \bigoplus_{\gamma < \beta} I_\gamma$, asi $N \cap \overline{L}_\beta \cong \bigoplus_{\gamma \leq \beta} I_\gamma$. Sea $\alpha \in A$ la menor tal que $N \cap \overline{L}_\alpha = N$, de aqui que $N \cong \oplus I_\alpha$

□

Teorema 2.28 *Dado R un anillo, son equivalentes:*

a) *R es hereditario*

b) $\forall_R$ $M \leq_R P$ *proyectivo* $\Rightarrow$ *M proyectivo*

c) $\forall_R$ (Q/N) *con Q inyectivo* $\Rightarrow Q/N$ *inyectivo.*

Demostración. a) $\Rightarrow$b) Sea $M \leq P$ proyectivo, entonces $P \leq L$ con L libre, entonces por 2.27 M es suma directa de proyectivos, por lo tanto M es proyectivo.

b) $\Rightarrow$c) Considremos ahora el siguiente diagrama con renglones exactos

$$\begin{array}{ccccccc} P & \xleftarrow{\alpha} & P' & \leftarrow & 0 \\ & & \downarrow & \varphi & \\ Q & \xrightarrow[\beta]{} & Q'' & \rightarrow & 0 \end{array}$$

con P proyectivo y Q inyectivo, ahora

P' proyectivo $\Rightarrow \exists\, \psi' : P' \to Q \ni \beta\psi' = \varphi$ y Q inyectivo $\Rightarrow \exists \psi : P \to Q$ tal que $\beta\psi\alpha = \varphi$. El morfismo que buscamos es $\beta\psi$

$\therefore$ Q'' es inyectivo.

c) $\Rightarrow$a) Sea I un ideal izquierdo de R y consideremos el diagrama

$$\begin{array}{ccccccc} R & \xleftarrow{\alpha} & I & \leftarrow & 0 \\ & & \downarrow & \varphi & \\ Q & \xrightarrow[\beta]{} & Q'' & \rightarrow & 0 \end{array}$$

donde los renglones son exactos y Q es inyectivo, por la proposición 2.20 la existencia de un morfismo de I en Q que haga el diagrama conmutativo probará que I es proyectivo.

Q'' es inyectivo por c), entonces $\exists \psi$: $R \to Q''$ tal que $\psi\alpha = \varphi$. Ahora, como R es proyectivo $\exists \psi'$: $R \to Q$ tal que $\beta\psi' = \psi$, entonces el morfismo $\psi'\alpha$ es el que buscamos.

□

Nota: Estas equivalencias son válidas para cualquier anillo, es decir que no es necesario restringirnos a dominios enteros.

Definición 2.29 *Diremos que N es noetheriano si $\forall M \leq N$ se tiene que M es de tipo finito.*

Diremos que un anillo es neteriano izquierdo si visto como R-módulo izquierdo es neteriano.

Proposición 2.30 *R neteriano izquierdo* $\Rightarrow \forall_R N$ *de tipo finito se tiene N neteriano.*

Demostración. Sea $\{x_1, x_2, \ldots, x_n\}$ un conjunto que genera a N y $M \leq N$, la prueba se hará por inducción:

i) $n = 1 \Rightarrow N \cong {}_R/_I$ para algún $I \leq R$, entonces $M \cong {}_I/_J$ $I \leq J \leq R$, con J de tipo finito, por lo tanto M es de tipo finito.

ii) Si $n>1$ consideremos $N' = \langle x_1 \rangle$ entonces $0 \to N' \to N \to N'' \to 0$ es exacta y N', N" están generados por menos de n elementos, así inducimos:

$$\begin{array}{ccccccccc} 0 & \to & N' & \to & N & \to & N'' & \to & 0 \\ & & \cup & & \cup & & \cup & & \\ 0 & \to & M' & \to & M & \to & M'' & \to & 0 \end{array}$$

con $M' = N' \cap M$ y $M'' = {}_M/_{M'}$ que son finitamente generados

$\therefore$ M es de tipo finito.

□

Proposición 2.31 *Sea M un R-módulo izquierdo entonces son equivalentes:*

a) M es neteriano

b) $\forall M_1 \leq M_2 \leq \ldots$ *cadena ascendente de módulos de M,* $\exists n \in \mathbf{N}$ *tal que* $\forall k \in \mathbf{N}$ *tenemos* $M_n = M_{n+k}$

c) Toda familia no vacía de submódulos de M tiene elementos máximos.

Demostración. a) $\Rightarrow$b) Sea $M_1 \leq M_2 \leq \ldots$una cadena ascendente de módulos de M y $M_0 = \bigcup_{n\in N} M_i$, así $M_0 \leq M$, por lo cual M_0 es de tipo finito. Consideremos $\{x_1, x_2, \ldots, x_r\}$ un conjunto de generadores de M_0, por lo que $\forall j \leq r \; x_j \in M_0$ y por definición $\forall j \leq r \; \exists i_j$ tal que $x_j \in M_{i_j}$, sea $n = \max\{i_1, \ldots, i_k\}$, entonces $x_j \in M_n$, por lo tanto $M_0 \leq M_n$, así $M_0 = M_n$.

$$\therefore \forall k \; M_0 = M_n = M_{n+k}$$

b) $\Rightarrow$c) Inmediato, usando el lema de Zorn. (Ver apéndice)

c) $\Rightarrow$ a) Sean $0 \neq N \leq M$ y $S = \{K \leq N : K \text{ es de tipo finito}\}$, como $\{0\} \in S$ tenemos que $S \neq \emptyset$, por hipótesis $\exists M_0 \in S$ máximo, así M_0 es de tipo finito y $M_0 \leq N$. Demostremos que $M_0 = N$. Supongamos que $M_0 \neq N$ y sea $x \in N - M_0$, así $\langle M_0, x\rangle \leq N$ y es de tipo finito, pero $M_0 \lneq \langle M_0, x\rangle$, lo que contradice que M_0 sea máximo. Por lo tanto $M_0 = N$

$$\therefore N \text{ es de tipo finito.}$$

□

Definición 2.32 *Sea $P \leq D$ diremos que P es un* ***ideal primo*** *si $\forall r, s \in D$ tales que $rs \in P$ se tiene que $r \in P$ ó $s \in P$.*

Es un resultado conocido que todo ideal máximo es primo.

Proposición 2.33 *Si I es un ideal primo invertible de D, entonces su factorización en ideales primos es única.*

Demostración. Supongamos que $I = \prod_{\beta} Q_\beta$ y que $I = \prod_{\alpha} P_\alpha$, donde cada P_α y Q_β son ideales primos, sin pérdida de generalidad tomamos P_1 un mínimo en el conjunto de las P_α. Como $\prod_{\beta} Q_\beta \leq P_1$, entonces alguna $Q_\beta \leq P_1$, analogamente, alguna $P_\alpha \leq Q_1$, de lo que se

deduce, $Q_i = P_i$. Ahora tenemos que $\prod_{\beta \neq i} Q_\beta = \prod_{\alpha \neq j} P_\alpha$, por hipotesis de inducción se debe tener el resultado.

Proposición 2.34 *Sea D neteriano e I⊴D entonces I contiene un producto de ideales primos.*

Demostración. Consideremos la familia $\mathcal{J}$= { I ⊴ D / I no contiene productos de primos} y supongamos que $\mathcal{J} \neq \varnothing$, por 2.31 podemos considerar L un ideal máximo en $\mathcal{J}$ entonces L no es primo, se sigue que hay I, J ideales de D con $L \subseteq I$, J tales que $IJ \subseteq L$, ya que L es máximo en $\mathcal{J}$, sabemos que $I, J \notin \mathcal{J}$ entonces I, J contienen productos de primos, así L tiene un producto de primos, por lo que $L \notin \mathcal{J}$ lo que contradice la elección de L.

$$\therefore \mathcal{J} = \varnothing$$

□

Proposición 2.35 *Sea R un anillo neteriano e I y J ideales de R tales que I ≠R, entonces I = (I : J) si y sólo si J no esta contenido en ningún ideal primo de I.*

Demostración. Sea $I = \bigcap_i Q_i$ una representación primaria irreducible de I y sean P_i los radicales de cada Q_i.

⇐) Si J no esta contenido en ningún P_i, entonces de (I : J) J ≤ I ≤ Q_i se deduce que (I : J) ≤ Q_i y por lo tanto (I : J) = I ya que la otra contención es obvia.

⇒) Supongamos que (I : J) = I, entonces tenemos que ∀ s (I : J^s) = I. Haremos la demostración por reducción al absurdo, supongamos que ∃ j tal que J ≤ P_j ∃ r tal que $J^r \leq P_j^r \leq Q_j$ ya que cada P_i es de tipo finito. Ahora (Q_j : J^r) = R, por lo tanto

$I = (I : J^r) = \bigcap_i (Q_i : P^r) = \bigcap_{i \neq j} (Q_i : P^r) \geq \bigcap_{i \neq j} Q_i \geq I$, lo que implica que $I = \bigcap_{i \neq j} Q_i$, que es una contradicción.

□

Proposición 2.36 *Si D es un dominio entero donde todo ideal es producto de primos, entonces todo ideal fraccionario J≠0 de D es invertible y se puede escribir de forma única:*

$$J = \prod_{P \text{ primo}} P^{n_p(I)}$$

donde cada $n_p(I)$ es un entero tal que: dado I un ideal de D hay un número finito de $n_p(I) \neq 0$, además $I \leq K$ si y sólo si $n_p(K) \leq n_p(I)$ para cualquier P y se tienen las siguientes relaciones:

1. $n_p(I + K) = min\,[n_p(I), n_p(K)]$
2. $n_p(I \cap K) = max\,[n_p(I), n_p(K)]$
3. $n_p(IK) = n_p(I) + n_p(K)$
4. $n_p(I:K) = n_p(IK^{-1}) = n_p(I) - n_p(K)$

Demostración. Sea J un ideal fraccionario de D, primero daremos una descomposición de J y veremos que es invertible. Por 2.12 $\exists\, I \leq D$ y $\exists\, d \in D$ tales que $J = \frac{1}{d} I$ y sea $K = Dd$, así $J = I K^{-1}$, por hipótesis I y K^{-1} son productos de primos y son invertibles, por lo tanto $J = \prod_i P_i \prod_j Q_j^{-1}$ donde cada P_i y cada Q_j son ideales primos y J es invertible.

Ahora veamos que esta descomposición es única. Sin pérdida de generalidad podemos suponer que $\forall$ i, j $P_i \neq Q_j$, ahora si $J = \prod_s P'_s \prod_t Q'^{-1}_t$ con cada $P'_s \neq Q'_t$ para toda s y para toda t, entonces tenemos $\prod_s P'_s \prod_j Q_j = \prod_t Q'_t \prod_i P_i$ y por la unicidad de la factorización de I y K (corolario de la equivalencia de los incisos a) y e) del teorema 2.42) se sigue que $\prod_s P'_s = \prod_i P_i$ y que $\prod_j Q_j = \prod_t Q'_t$, lo que demuestra la unicidad.

Como K es invertible, tenemos que $I K^{-1} \leq K K^{-1}$ esto es equivalente a que $\forall P$ ideal primo de D tenemos $n_p(IK^{-1}) \geq 0$ por que $\forall P\ n_p(K) \geq 0$, lo que prueba que si $I \leq K$ es equivalente a que $n_p(I) - n_p(K) \geq 0$, de aquí se sigue que $\prod_P P^{\nu(P)}$ donde $\nu(P) = \min(n_p(I), n_p(K))$ es el menor ideal que contiene a I y a K, ademas que $\prod_P P^{\mu(P)}$ donde $\mu(P) = \max(n_p(I), n_p(K))$ es el mayor ideal contenido en I y en K, esto prueba los puntos 1. y 2. El punto 3. es directo.

Se vió que $K^{-1} = (D : K)$, asi $I K^{-1} = I(D : K) \leq (I : K)$, y por otro lado, tenemos que $D = (D : K) K$, entonces $(I : K) = (I : K) K (D : K) \leq I (D : K)$. Por lo que se concluye $I(D : K) = (I : K)$ y esto prueba el punto 4.

□

Definición 2.37 *Sean R un anillo y A un subanillo tal que $1 \in A$. Un elemento $x \in R$ se dice que es entero sobre A si x es una raiz de un polinomio mónico con coeficientes en A. Es decir si x satiface una ecuación de la forma $x^n + a_1 x^{n-1} + \ldots + a_n = 0$ donde $a_i \in A$.*

Proposición 2.38 *Sean E un dominio entero, D un subanillo de E, M un E-módulo de tipo finito e I un ideal de D. Si $x \in E$ y es tal que :*

i) $xM \subset IM$

ii) Si $\forall z \in M$ tenemos que $yz = 0$ con $y \in D[x]$, entonces $y = 0$

entonces x es raiz de un polinomio de la forma $x^n + i_{n-1}x^{n-1} + \cdots + i_0 = 0$
donde $\forall j\ i_j \in I$.

Demostración. Podemos escribir $M = \sum_j D\, m_j$, asi $xM \subset \sum_j D\, I\, m_j = \sum_j I\, m_j$ en particular $\exists \{i_{kj}\} \subset I$ tal que $xm_j = \sum_j i_{kj} m_j$ y este es un sistema lineal homogeneo, entonces podemos escribirlo $\sum_j (\delta_{kj}\, x - i_{kj})\, m_j = 0$ donde las δ_{kj} son las de Kronecker.

Sea d = det $\left(\delta_{kj}\, x - i_{kj}\right)$ entonces $\forall j$ $dm_j = 0$ y por lo tanto d M = 0 lo que implica por la hipótesis que d = 0. Se sigue fácilmente que det $\left(\delta_{kj}\, x - i_{kj}\right) = 0$ es el polinomio que buscamos.

□

Proposición 2.39 *Sean E y D dominios enteros tales que $D \subseteq E$, sea $x \in E$, entonces son equivalentes:*

a) x es un elemento entero sobre D.

b) El anillo D[x] es un E-módulo de tipo finito.

c) El anillo D[x] está contenido en un subanillo F de E de tipo finito.

d) $\exists M$ un E-módulo de tipo finito tal que:

i) $xM \subset M$

ii) Si $\forall z \in M$ tenemos $yz = 0$ con $y \in D[x]$, entonces $y = 0$.

Demostración. a) $\Rightarrow$ b) Tenemos que $x^n \in \sum_{i=0}^{n-1} Dx^i$, asi $x^{n+q} \in \sum_{i=0}^{n-1} Dx^{i+q}$, por lo que se sigue que $x^{n+q} \in \sum_{i=0}^{n-1} Dx^i$, por lo tanto $\{1, x, \cdots, x^{n-1}\}$ es un conjunto de generadores de D[x].

Las implicaciones b) $\Rightarrow$ c) y c) $\Rightarrow$ d) son claras y d) $\Rightarrow$ a) es inmediata de la proposición 2.37.

□

Proposición 2.40 *El conjunto C de elementos enteros sobre A es un subanillo de D tal que $A \subseteq C$.*

Demostración. Sean a,b∈C entonces A[a,b] es un A-módulo finitamente generado. Por lo tanto a + b y a b son enteros sobre A.

□

Definición 2.41 *El anillo C de 2.31 se denomina la* ***cerradura entera*** *de A en D, si A coincide con C, entonces diremos que A es* ***enteramente cerrado.***

Teorema 2.42 *Sea D un dominio entero, entonces son equivalentes:*

a) $\forall I \leq D$ *se tiene que I es invertible.*

b) D es hereditario.

c) D es neteriano y semihereditario.

d) D es 1) neteriano,

2) enteramente cerrado,

3) todo ideal primo es máximo.

e) $\forall I \leq D$ *I es producto de primos.*

f) $\forall_D M \leq_D P$ *P proyectivo* $\Rightarrow$ *M proyectivo.*

g) $\forall_D (\mathbb{Q}/\mathbb{N})$ *con Q inyectivo* $\Rightarrow$ $\mathbb{Q}/\mathbb{N}$ *inyectivo.*

h) $\forall_D M$ *M divisible* $\Leftrightarrow$ *M inyectivo.*

i) El conjunto $\mathfrak{I}$ *de los ideales fraccionarios de D es ungrupo bajo la multiplicación.*

Demostración a) $\Rightarrow$b) Inmediato por 2.11.

b) $\Rightarrow$c) Por la proposición 2.11, sabemos que todo ideal I es invertible, además sabemos que todo ideal invertible es de tipo finito, lo cual prueba c).

c) $\Rightarrow$b) Como D es neteriano todo ideal de D es finitamente generado, además D es semihereditario por lo que todo ideal finitamente generado, es decir, todo ideal de D es proyectivo

$\therefore$ D es hereditario.

b) y c) $\Rightarrow$i) Como D es neteriano por 2.34 sabemos que todo ideal I de D contiene un producto de primos, por ser D hereditario I es proyectivo y por la proposición 2.11, tenemos que I es invertible, y por la proposición 2.13 tenemos que $\mathcal{J}$ es un grupo.

Las equivalencias de b), f) y g) fueron dadas en la proposición 2.29

h) $\Rightarrow$g) Supongamos que todo módulo M divisible es inyectivo. Consideremos M divisible y M/N un cociente, sabemos que $\forall\, 0 \neq a \in D$ $aM = M$ entonces $aM/N = aM/N = M/N$ y por lo tanto M/N es divisible.

Como el cociente de todo divisible es divisible, entonces el cociente de todo inyectivo es inyectivo.

e) $\Rightarrow$a) 1) Consideremos I ideal primo e invertible, demostremos que es máximo. Sea $r \in R$ con $r \neq 0$, por hipótesis, podemos escribir $I+Rr = \prod_{\alpha=1}^{n} P_\alpha$ y $I+Rr^2 = \prod_{\beta=1}^{m} Q_\beta$, donde cada P_α y cada Q_β son ideales primos. Sea $\overline{R} = R/I$, y $\overline{r}$ la clase residual de r. Así $\overline{R}\cdot\overline{r} = \prod_{\alpha=1}^{n}(P_\alpha/I)$ y $\overline{R}\cdot\overline{r}^2 = \prod_{\beta=1}^{m}(Q_\beta/I)$, donde cada P_α/I y cada Q_β/I son ideales primos y por lo tanto son invertibles. Ahora como $\overline{R}\cdot\overline{r}^2 = (\overline{R}\cdot\overline{r})^2 = \prod_{\alpha=1}^{n}(P_\alpha/I)^2$, entonces $m = 2n$ y podemos remnumerar cada Q_β de tal forma que $Q_{2\beta}/I = Q_{2\beta-1}/I = P_\beta/I$, lo que nos dice que $Q_{2\beta} = Q_{2\beta} = P_\beta$, y tenemos también; $I+Rr^2 = (I+Rr)^2$, entonces $I \subset (I+Rr)^2 \subset I^2 + Rr$.

Por lo tanto toda $x \in I$ se puede escribir de la forma $x = y + z\,r$ con $y \in I^2$ y $z \in R$, es decir, $z\,r \in I$ pero $r \notin I$, entonces $z \in I$ e $I \subseteq I^2 + Ir$, y como $I^2 + Ir \subseteq I$ se sigue que $I = I^2 + Ir = I(I + Rr)$, por hipótesis I es invertible, así $I^{-1}I = I^{-1}(I^2 + Ir) = I^{-1}I(I + Rr)$ por lo que $R = I + Rr$.

Como r fue arbitrario, esto prueba que I es máximo.

2) Para demostrar que I es invertible tomemos $a \in I$ tal que $a \neq 0$, y consideremos $Ra = \prod_{\alpha} P_\alpha$ donde cada P_α es un ideal primo, como $\prod_{\alpha} P_\alpha \subseteq I$, entonces alguna $P_\beta \subseteq I$, pero por la proposición 2.14, sabemos que cada P_α es invertible, y por la parte 1) tenemos que todo P_α es máximo, por lo que se tiene $P_\beta = I$.

$\therefore$ I es invertible

a) $\Rightarrow$h) La proposición 2.24 dice que todo inyectivo es divisible, por lo que debemos demostrar que todo divisible es inyectivo. Supongamos que $\forall I \leq D$ I es invertible. Consideremos M un D-modulo divisible, sea $I \leq D$ y $\varphi: I \to M$ entonces $\exists \{a_1, a_2, \ldots, a_n\} \subseteq I$ y $\exists \{q_1, q_2, \ldots, q_n\} \subseteq Q$ tales que: $\forall i \leq n$ se tiene $q_i\, I \subseteq R$ y $1 = \sum_{i=1}^{n} q_i a_i$, así $\exists m_i \in M$ y $\forall i\ \varphi(a_i) = a_i m_i$ entonces para $a \in D$ tenemos:

$\varphi a = \varphi(\sum_i q_i a_i)a = \sum_i (q_i a)\varphi(a_i) = \sum_i (q_i a a_i)m_i = a\sum_i (q_i a_i)m_i$ así $m = \sum_i (q_i a_i)m_i$ cumple con que $\varphi(a) = am$ entonces φ se puede extender a D.

$\therefore$ M es inyectivo

i) $\Rightarrow$e) Como por hipótesis todo ideal $I \neq 0$ de D es invertible, se sigue que todo ideal es de tipo finito, es decir D es neteriano. Demostraremos por reducción al absurdo que todo ideal propio I de D es producto de ideales máximos. Sean $\mathcal{P} = \{J \leq D : J$ no es producto de ideales máximos$\}$ y J_0 un máximo en $\mathcal{P}$, así J_0 no es máximo en D, entonces $\exists\, J_0 < I \leq D$ tal que I en máximo en D, por hipótesis $\exists\, I^{-1}$ así $J_0 < I^{-1}J_0$, ya que suponer que $J_0 = J_0 I^{-1}$, nos lleva a una contradicción. Por lo tanto $I^{-1}J_0$ es producto de máximos y

$J_0 = I\, I^{-1} J_0$ es también un producto de máximos, lo que contradice que $J_0 \in \wp$, por lo que concluimos que $\wp = \varnothing$

$\therefore$ todo ideal de D es producto de primos.

d) $\Rightarrow$e) Dada la hipótesis de que D es neteriano, sólo hace falta demostrar que todo ideal P primo y propio es invertible, para tener una demostración análoga a la anterior. Sea $0 \neq x \in P$, entonces Dx contiene un producto de ideales primos propios, por lo tanto P contiene alguno de estos ideales primos propios, digamos Q, como Q es máximo tenemos que $P = Q$.

Por lo anterior es suficiente demostrar que todo ideal primo propio de un ideal principal es invertible. Como P es un ideal primo de Dx tenemos que $(Dx : P) \neq Dx$, consideremos $y \in (Dx : P) - Dx$, así $\left(\frac{y}{x}\right)P \leq D$ y $\left(\frac{y}{x}\right) \notin D$, por lo que $(Dx : P) \neq D$.

Supongamos que P no es invertible, así $P \leq P (D : P) < D$ y como P es máximo $P = P (D : P)$, ahora $(0) \neq P$ es un D-módulo de tipo finito ya que D es neteriano, y por $P \leq P (D : P)$ sabemos que $\forall\, z \in (D : P)$ z es entero sobre D y $z \in D$ ya que D es enteramente cerrado, por lo que $(Dx : P) \leq D$ lo que contradice el hecho que $(Dx : P) \neq D$. Por lo tanto P es invertible.

e) $\Rightarrow$d) 1. y 3. se siguen inmediatamente de las implicaciones i) $\Rightarrow$e) y e) $\Rightarrow$ a) y de la proposición 2.31. Sólo falta ver que D es enteramente cerrado. Sea K el campo de cocientes de D y $x \in K$, como K es entero sobre D $\exists\, 0 \neq d \in D$ un común denominador tal que $\forall\, n \neq 0$ tenemos que $dx^n \in D$, ahora $v_p(d)$ y $v_p(x)$ son enteros (ver demostración

de la proposición 2.36), entonces $v_P(x) \geq 0$ y por lo tanto $v_P(Dx) \geq 0$ y ésto para todo ideal primo P, por lo tanto $x \in D$.

□

Definición 2.36 *Un dominio entero se llama* ***dominio de Dedekind*** *si cumple con las condiciones del teorema 2.35.*

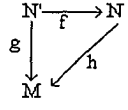
CAPITULO TRES

Módulos inyectivos y módulos simples

Los incisos c) y g) del teorema 1.16 son generalizables a cualquier categoría de módulos, como sigue:

1. $\forall S$ simple $Hom(M,S)=0$

2. Dados $0 \to N' \xrightarrow{f} N$ y $N' \xrightarrow{g} M$ entonces existe un diagrama conmutativo



El objeto de este capítulo es encontrar condiciones suficientes y necesarias sobre un anillo R para mantener la equivalencia de estos dos conceptos en la categoría R-$\mathcal{MOD}$.

Para ésto debemos revisar algunas definiciones y propiedades en la categoría R-$\mathcal{MOD}$. Primero veamos con detenimiento el concepto de Hom y algunas de sus propiedades.

Definición 3.1 *Dada $\mathcal{C}$ una categoría y dados $A,B \in obj(\mathcal{C})$ definimos* **Hom (A,B)** *como* $\{\varphi \in mor(\mathcal{C}): \varphi : A \to B\}$.

Hom(A,B) es en general, una clase. Pero en el caso particular que la categoría $\mathcal{C}$ sea R-$\mathcal{MOD}$, entonces se verifica fácilmente que Hom(A,B) es un grupo abeliano con la operación usual de suma de morfismos.

Definición 3.2 *Dadas $\mathcal{C}$ y $\mathcal{D}$ dos categorías, un funtor $T:\mathcal{C} \to \mathcal{D}$ es una función que satisface:*

1. $\forall C \in obj(\mathcal{C})$, *se tiene que* $FC \in obj(\mathcal{D})$
2. $\forall \varphi : C \to D \in mor(\mathcal{C})$, *se tiene que* $F\varphi : FA \to FB \in mor(\mathcal{D})$
3. *Dado* $A \xrightarrow[\varphi]{} B \xrightarrow[\psi]{} C$, *se tiene que* $F(\psi\varphi) = F\psi F\varphi$
4. $\forall C \in obj(\mathcal{C})$, *se tiene que* $F(1_C) = 1_{FC}$

Definición 3.3 *Para un objeto fijo $A \in obj(\mathcal{C})$, definimos $FC = Hom(A,C)$, dado $\varphi : B \to C$* $F(\varphi) = \varphi_* : Hom(A,B) \to Hom(A,C)$ *y es tal que* $\forall \psi \in Hom(A,B)$ $\varphi_*(\psi) = \varphi\,\psi$.

Definición 3.4 *Un funtor F es exacto izquierdo cuando, dada una sucesión exacta* $0 \to A \xrightarrow[\varphi]{} B \xrightarrow[\psi]{} C$, *tenemos que la sucesión* $0 \to FA \xrightarrow[F\varphi]{} FB \xrightarrow[F\psi]{} FC$ *es exacta.*

Proposición 3.5 *Dado M un R-módulo, se tiene que Hom(M,_) es exacto izquierdo.*

Demostración. Consideremos $0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C$ exacta, demostremos que $0 \to \mathrm{Hom}(M,A) \xrightarrow{\varphi_*} \mathrm{Hom}(M,B) \xrightarrow{\psi_*} \mathrm{Hom}(M,C)$ es exacta.

i) Demostremos que φ_* es monomorfismo. Supongamos que $\varphi_*(f) = 0$, entonces $\varphi f = 0$, φ es un monomorfismo.

$$\therefore f = 0$$

ii) Demostremos que $\mathrm{Im}(\varphi_*) \subseteq \mathrm{Nuc}(\psi_*)$. Supongamos que $g \in \mathrm{Im}(\varphi_*)$, entonces $\exists\, f \in \mathrm{Hom}(M,A)$ tal que $g = \varphi_*(f) = \varphi f$, así $\psi_*(g) = \psi g = (\psi\varphi)f = 0$, por lo que se sigue que $\psi\varphi = 0$.

iii) Demostremos que $\mathrm{Nuc}(\psi_*) \subseteq \mathrm{Im}(\varphi_*)$. Supongamos que $g \in \mathrm{Hom}(M,B)$ y es tal que $\psi g = 0$, veamos que $\exists\, f: M \to A$ tal que $g = \varphi f$. Sea $m \in M$, así $\psi g(m) = 0$, por lo que $g(m) \in \mathrm{Nuc}(\psi) = \mathrm{Im}(\varphi)$ y φ es monomorfismo, de aquí que $\exists!\, a \in A$ tal que $\varphi(a) = g(m)$, entonces definimos $f: M \to A$ como sigue: $f(m) = a$, por construcción se tiene que $\varphi f = g$.

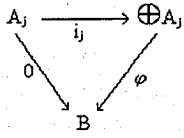
□

Proposición 3.6 *Dado B un módulo e* $i_j : A_j \to \bigoplus A_k$ *entonces hay un isomorfismo* $\theta : Hom(\bigoplus A_k, B) \to \prod Hom(A_k, B)$ *definido por* $\forall j\ \pi_j\ \theta(\varphi) = \varphi\, i_j$ *, donde* π_j *es la proyección canónica.*

Demostración. Es claro que θ es un morfismo de grupos abelianos.

i) Demostremos que θ es epimorfismo. Sea $(f_j) \in \prod \mathrm{Hom}(A_j, B)$, entonces $\forall j \ f_j : A_j \to B$, por la propiedad universal de la suma directa tenemos que $\exists\, \varphi : \bigoplus A_j \to B$ tal que $\varphi\, i_j = f_j$, es decir que $\theta(\varphi) = (f_j)$.

ii) Demostremos que θ es monomorfismo. Supongamos que $\theta(\varphi) = 0 = \varphi\, i_j$, es decir que cada $\varphi\, i_j = 0$, entonces φ hace que el siguiente diagrama sea conmutativo:



por la propiedad universal de la suma directa tenemos que φ es única, pero 0 también hace conmutar el diagrama, por lo tanto $\varphi = 0$.

□

Definición 3.7 *Dado* $0 \to M' \xrightarrow{\varphi} M$ *es esencial si* $\forall N \leq M$, $N \neq 0$, *tenemos que* $N \cap \mathrm{Im}(\varphi) \neq 0$

Vimos en 2.18 que todo módulo se puede sumergir en un inyectivo, la pregunta ahora es acerca de la existencia de mínimos inyectivos que contienen a M.

Definición 3.8 *Sea M un R-módulo, diremos que EM es su* ***cápsula inyectiva*** *cuando* $\exists\ M \to EM$ *es un monomorfismo esencial y EM es inyectivo.*

De acuerdo con la definición, diremos que ER es la cápsula inyectiva del anillo R considerado como R-módulo izquierdo, observemos también que para cualquier módulo M $M \cong EM$ si y sólo si M es inyectivo.

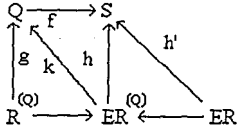
Lema 3.9 *Sea R un anillo, entonces son equivalentes:*

a) ∀Q inyectivo, ∀S simple Hom(Q,S)=0

b) ∀S simple Hom(ER,S)=0

Demostración a) ⇒b) Caso particular.

b) ⇒a) Demostración por contrapositiva. Supongamos que Hom(Q,S)≠0, entonces $\exists f : Q \xrightarrow{\neq 0} S$, consideremos el siguiente diagrama conmutativo:



donde $g((r_x)) = \sum_{x \in Q} r_x x$ es claramente un epimorfismo; como Q es inyectivo existe k y si h es la composición de k con f entonces h es también un epimorfismo, h' es entonces la composición de h con una de las inclusiones de tal forma que resulte diferente de cero.

□

Con el objeto de mantener una redacción ágil, definiremos las siguientes clases:

$\mathcal{J}$ = { **M : Hom(M,S) = 0 ∀ S simple** }

$\mathcal{E}$ = { **Q : Q es inyectivo** }

Así tenemos que el propósito de este capítulo es ver cuando $\mathcal{E} = \mathcal{J}$, para lo cual estudiaremos en lo siguiente estas clases. Hagamos las siguientes observaciones de $\mathcal{J}$:

Proposición 3.10 $\mathcal{J}$ *es cerrada bajo cocientes.*

Demostración. Consideremos $M \in \mathcal{J}$ y una sucesión exacta $M \to M'' \to 0$. Sea S simple, entonces $0 \to \text{Hom}(M'',S) \to \text{Hom}(M,S)$ es exacta y por hipótesis $\text{Hom}(M,S) = 0$, por lo que $0 \to \text{Hom}(M'',S) \to 0$ es exacta, por lo tanto $\text{Hom}(M'',S) = 0$.

$$\therefore M'' \in \mathcal{J}.$$

□

Proposición 3.11 $\mathcal{J}$ *es cerrada bajo extensiones.*

Demostración. Sean $M', M'' \in \mathcal{J}$ y la sucesión exacta $0 \to M' \to M \to M'' \to 0$, entonces $0 \to \text{Hom}(M'',S) \to \text{Hom}(M,S) \to \text{Hom}(M',S)$ es exacta y por hipótesis $\text{Hom}(M', S) = 0$ y $\text{Hom}(M'', S) = 0$, entonces $0 \to \text{Hom}(M,S) \to 0$ es exacta, por lo tanto $\text{Hom}(M, S) = 0$.

$$\therefore M \in \mathcal{J}.$$

□

Proposición 3.12 $\mathcal{J}$ *es cerrada bajo sumas directas.*

Demostración. Sea $\{M_\alpha\} \subseteq \mathcal{J}$, por 3.6 sabemos que $\text{Hom}(\oplus M_\alpha, S) \cong \prod \text{Hom}(M_\alpha, S)$ y tenemos por hipótesis que $\forall \alpha \ \text{Hom}(M_\alpha, S) = 0$, entonces $\prod \text{Hom}(M_\alpha, S) = 0$, por lo tanto $\text{Hom}(\oplus M_\alpha, S) = 0$.

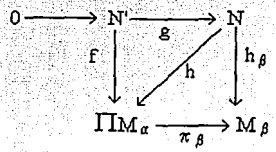
$$\therefore \oplus M_\alpha \in \mathcal{J}.$$

□

Ahora veamos que pasa con $\mathcal{E}$:

Proposición 3.13 $\mathcal{E}$ *es cerrado bajo productos directos.*

Demostración. Sea $\{M_\alpha\} \subseteq \mathcal{E}$, consideremos el siguiente diagrama conmutativo



donde f y g están dados, $\exists h_\beta$ que hace el cuadro conmutativo, ya que $\forall \beta$ M_β es inyectivo. Ahora, por la propiedad universal del producto directo existe h que hace conmutar el diagrama.

$$\therefore \prod M_\alpha \in \mathcal{E}$$

□

Proposición 3.14 $\mathcal{E} = \mathcal{J}$ *implica que R es hereditario y noetheriano.*

Demostración. Ver proposición 2.29 para deducir que R es hereditario.
El hecho que $\mathcal{E} = \mathcal{J}$ implica que $\mathcal{E}$ es cerrada bajo sumas directas, ahora por [3 prop 18.13.] obtenemos que R es noetheriano.

□

El recíproco de 3.14 no es verdadero. Consideremos K un campo, entonces tenemos $K\text{-}\mathcal{MOD} = \mathcal{E}$ y $\mathcal{J} = \{0\}$.

Sea $\mathcal{S}$ = {S} una familia de representantes de los simples, es decir, si T es simple entonces $\exists$ S $\in \mathcal{S}$ tal que T $\cong$ S y sea $\mathbf{C} = \prod_{S \in \mathcal{S}} S$.

Teorema 3.15 *Sea R un anillo, entonces son equivalentes:*

a) i) $\forall S$ simple $Hom(ER,S)=0$.

ii) Si $M \neq EM$ entonces $\exists\ f: M \to C$ tal que $f \neq 0$.

b) $\mathcal{E} = \mathcal{J}$

Demostración a) $\Rightarrow$b) $\mathcal{E} \subseteq \mathcal{J}$ es inmediato, dada la proposición 3.9.

Demostremos $\mathcal{E} \supseteq \mathcal{J}$. Demostración por reducción al absurdo. Supongamos $\mathcal{E} \neq \mathcal{J}$, por la contención anterior tenemos que $\exists\ M \in \mathcal{J}$, pero $M \notin \mathcal{E}$, así $M \neq EM$, por hipótesis sabemos que $\exists\ f: M \to C$ tal que $f \neq 0$, entonces $\exists\ m \in M$ y $\exists\ (c) \in C$ tal que $f(m) = (c)$, tomando una coordenada j distinta de cero tenemos que $\pi_j\ f: M \to S_j$ y $\pi_j\ f \neq 0$ con S_j simple, entonces $M \notin \mathcal{J}$, lo que es una contradicción. Por lo tanto $\exists M \in \mathcal{J}$ tal que $M \notin \mathcal{E}$.

$$\therefore \mathcal{E} = \mathcal{J}$$

b) $\Rightarrow$a) i) Es un caso particular, ya que ER es inyectivo y por hipótesis tenemos que $\forall S$ simple $\forall Q$ inyectivo $Hom(Q,S) = 0$.

ii) Demostración por reducción al absurdo. Sean $M \in \mathcal{E} = \mathcal{J}$ y $C = \prod_{s \in b} S$, suponga-mos que $\exists\ f: M \to C$ con $f \neq 0$, entonces $\exists\ m \in M$ y $m \neq 0$ tal que $f(m) \neq 0$, tomando una coordenada j distinta de cero de $f(m)$ tenemos que $\pi_j\ f: M \to S_j$ y $\pi_j\ f \neq 0$ con S_j simple, entonces, por un lado sabemos que $M = EM$ y por otro que $M \notin \mathcal{J}$, lo que contradice la hipótesis. Por lo tanto se cumple ii).

□

APENDICE

Teoría de conjuntos

Una relación R sobre un conjunto A es un subconjunto del producto cartesiano AxA, donde diremos que $(a,b) \in R$ cuando a está R-relacionado con b, la notación más usual es a R b.

Definición A.1 *Dado $A \neq \emptyset$, una relación binaria $\leq$ es un orden parcial o un preorden de A cuando para cualquier $a,b,c, \in A$, tenemos:*

1. $a \leq a$ *(es reflexiva)*
2. $a \leq b$ y $b \leq a \Rightarrow a = b$ *(es antisimétrica)*
3. $a \leq b$ y $b \leq c \Rightarrow a \leq c$ *(es transitiva)*

Ejemplos de ordenes parciales son:

- $\leq$ sobre **N, Z, Q, R.**
- $\subseteq$ sobre una familia de conjuntos.

Este último ejemplo se utiliza en algunas demostraciones de los capitulos 1 y 2, por lo que lo demostraremos aqui:

Demostración. Sea $\mathcal{C}$ una familia de conjuntos y $A,B,C \in \mathcal{C}$.

1. Es una tautología que $a \in A \Leftrightarrow a \in A$, por lo que se concluye que $A \subseteq A$.

2. Supongamos que $A \subseteq B$ y $B \subseteq A$, entonces es verdadero por definición $\forall a\,(a \in A \Leftrightarrow a \in B)$, por lo tanto $A = B$.

3. Supongamos que $A \subseteq B$ y $B \subseteq C$, entonces $\forall a\,(a \in A \Rightarrow a \in B)$ y $\forall a\,(a \in B \Rightarrow a \in C)$, de lo que se concluye que $\forall a\,(a \in A \Rightarrow a \in C)$ y por lo tanto $A \subseteq C$.

□

Definición A.2 *Dado $(A,\leq)$ un preorden diremos que es total, lineal o simple si :*

4. $\forall a,b \in A \quad a \leq b \text{ o } b \leq a$. *(es dicotómica)*

Diremos que un subconjunto $\mathcal{C}$ de una familia $(A,\leq_A)$ es una cadena cuando $(\mathcal{C},\leq_{\mathcal{C}})$ es un orden total, donde $\leq_{\mathcal{C}}$ es el orden de A restringido a $\mathcal{C}$.

Definición A.3 *Dado $\mathcal{C}$ totalmente ordenado por $\leq$ diremos que c_0 es una cota superior de $\mathcal{C}$ si cumple con $\forall c \in \mathcal{C} \quad c \leq c_0$.*

Ahora, c_0 no necesariamente está en $\mathcal{C}$, cuando esto sucede llamaremos a c_0 máximo y no necesariamente es único.

Lema A.4 (Lema de Zorn) *Sea A un conjunto parcialmente ordenado tal que, cada cadena $\mathcal{C} \subseteq A$ tiene cota superior, entonces A tiene elementos máximos.*

El lema de Zorn es lógicamente equivalente a una serie de principios y axiomas intuitivos que se han demostrado como indecidibles, es decir la teoría de conjuntos mantiene su consistencia tomandolos como verdaderos o admitiendo su negación.

Algunas de estas equivalencias son:

- El axioma de elección; existen funciones de elección.
- El principio del buen orden; Dado un conjunto A distinto del vacío, existe un preorden que lo bien ordena.
- El teorema de Tychonoff; El producto de compactos es compacto.
- El producto cartesiano de conjuntos no vacíos es no vacío.

Las pruebas de estas equivalencias y otras más, además de no ser triviales están fuera de nuestro tema de estudio, por lo que las omitiremos aquí.[1]

Definición A.5 *Dado un conjunto A una operación $*$ n-aria definida en A es una función* $*: \prod_{n} A \to A$.

Diremos que la operación es cerrada cuando la función está bien definida y llamaremos operaciones binarias a las de aridad 2.

[1] Estas demostraciones y otras se pueden encontrar en P.R. ALMOS, Naïve set theory, Van Nostrand, 1960.

BIBLIOGRAFIA

1.- ROTMAN J.J., The theory of groups *an introduction*,
Allin & Bacon,USA, segunda ed., 1980, 342 pp

2.- CARTAN & EILENBERG, Homological algebra,
Princeton University Press, USA, 1956, 390 pp

3.- ANDERSON & FULLER, Rings and categories of modules,
USA, 1974, 356 pp

4.- ZARISKI & SAMUEL, Commutative algebra,
Editorial Board, USA, 1965, 329 pp

5.- ROTMAN J.J., An introduction to homological algebra,
Academic Press inc., USA, 1979, 374 pp