UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

ALGUNOS RESULTADOS EN LA TEORÍA DE V-ANILLOS Y ALGUNAS DE SUS GENERALIZACIONES

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

M A T E M Á T I C O

P R E S E N T A:

HÉBER UZZIEL CORONA PÉREZ

DIRECTOR DE TESIS:
DR. HUGO ALBERTO RINCÓN MEJÍA

2015

Ciudad Univeritaria, D. F.

1. Datos del alumno
Corona
Pérez
Héber Uzziel
56 18 82 75
Universidad Nacional Autónoma de México

Facultad de Ciencias
Matemáticas
411014199

2. Datos del Asesor
Dr.
Hugo Alberto
Rincón
Mejía

3. Datos del sinodal 1
Dra.
Bertha María
Tomé
Arreola

4. Datos del sinodal 2
Dr.
Alejandro
Alvarado
García

5. Datos del sinodal 3
Mat.
Alberto
Alcalá
Álvarez

6. Datos del sinodal 4
Mat.
Ernesto
Mayorga
Saucedo

7. Datos de la tesis.
Algunos Resultados en la Teoría de V-Anillos y Algunas de sus Generalizaciones
84 p.
2015

Algunos Resultados en la Teoría de V-Anillos y Algunas de sus Generalizaciones

23 de junio de 2015

Agradecimientos

Agradezco a mi familia que me apoyó durante toda mi carrera, a mi asesor de tesis que tanto me apoyó con la elaboración de este documento y a mi tía Rosa por cuidarme en su casa por todo el tiempo que estuve estudiando la licenciatura.

Introducción

El objetivo de este trabajo es, como menciona el título, trabajar con los V-anillos, los cuales son anillos tal que sus módulos simples son inyectivos, y con algunas de sus generalizaciones, como los DV-anillos (débilmente V-anillos) y los ΣV-anillos (que son casi como los V-anillos, sólo que los módulos simples no deben ser solamente inyectivos, sino Σ-inyectivos), para lo cual se desarrollará en un principio teoría, con el fin de que se pueda fundamentar de la mejor manera posible los resultados obtenidos en la Teoría de los V-anillos.

En el primer capítulo se trata el tema de los anillos, comenzando desde la definición de anillo (con uno), siguiendo por subanillos e ideales, y terminando con los homomorfismos. En el segundo capítulo se aborda el tema de módulos sobre un anillo R, submódulos y homomorfismos entre módulos. Después para dar más riqueza a los resultados en los capítulos consecuentes se ven las sumas y productos de módulos, después de esto, se introducen las sucesiones exactas, a fin de estudiar la proyectividad e inyectividad de los módulos, esta última es vital para la definición de los V-anillos. Se sigue con los módulos artinianos y neterianos, viendo sus definiciones, sus caracterizaciones y algunos resultados, además se aprovecha para introducir el zoclo y el radical de Jacobson de un módulo. Luego, con la intención de llegar a la dimensión de Goldie, la cual se utiliza para demostrar algunos resultados en la teoría de los V-anillos, se abordan los temas de anillos semilocales, donde se ve una aplicación interesante que tiene que ver con los anillos uniseriales (anillos donde se cumple que para cualesquiera dos ideales siempre uno está contenido en el otro), además se ve el Teorema de Krull-Schmidt-Remak. Ya con todo esto ahora sí se le entrará a los V-anillos, probando varios resultados, como algunas de sus caracterizaciones y la relación que tienen con los anillos Von Neumann regulares, y llegando a sus generalizaciones antes mencionadas.

Índice general

Capítulo 1

Anillos

1.1. Anillos, subanillos e ideales

Definición 1.1. Un anillo (con uno) es una quinteta $(R, +, \cdot, 0, 1)$, donde:
R es un conjunto,
$(R, +, 0)$ es un grupo abeliano,
$(R, \cdot, 1)$ es un monoide,
Se cumplen las leyes distributivas izquierda y derecha, es decir para cualesquiera $a, b, c \in R$ se cumple:
$a \cdot (b + c) = a \cdot b + a \cdot c$.
$(b + c) \cdot a = b \cdot a + c \cdot a$.

Definición 1.2. Un anillo conmutativo es un anillo $(R, +, \cdot, 0, 1)$, donde además la operación $\cdot$ es conmutativa.

Ejemplo 1.1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}_n$ son anillos conmutativos.

Ejemplo 1.2. M_n es un anillo (en general) no conmutativo con la suma y el producto de matrices usuales.

Definición 1.3. En un anillo conmutativo R se dice que $a \neq 0$ es un divisor de cero si existe un $b \in R$, distinto de cero tal que, $a \cdot b = 0$.

Ejemplo 1.3. Consideremos $\mathbb{Z}_4$ entonces tenemos que $\bar{2} \cdot \bar{2} = \bar{0}$ por lo tanto $\bar{2}$ es un divisor de cero en $\mathbb{Z}_4$.

Definición 1.4. Un dominio entero es un anillo conmutativo que no contiene divisores de cero.

Ejemplo 1.4. Como vimos en el ejemplo 1.3, $\mathbb{Z}_4$ tiene divisores de cero, por lo tanto no es un dominio entero, pero $\mathbb{Z}$ sí es un dominio entero.

Definición 1.5. Se dice que un anillo R es un anillo con división si todos sus elementos distintos de cero tienen inverso multiplicativo.

Ejemplo 1.5. $\mathbb{Z}$ tiene elementos que no tienen inverso multiplicativo (de hecho sólo 1 y -1 tienen inverso multiplicativo en $\mathbb{Z}$), por lo tanto $\mathbb{Z}$ no es un anillo con división, en cambio $\mathbb{Q}$ si es un anillo con división.

Definición 1.6. Un anillo conmutativo R es un campo si además es un anillo con división.

Ejemplo 1.6. $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son campos.

Definición 1.7. Sea $(R, +, \cdot, 0, 1)$ un anillo, un subanillo de R es un subconjunto $S \subseteq R$ tal que $(S, +, \cdot, 0, 1)$ tiene estructura de anillo donde las operaciones son las restricciones de las operaciones de R.

Proposición 1.1. *Sean R un anillo y $S \subseteq R$ entonces S es subanillo de R si y sólo si $1 \in S$ y para cualesquiera $a,\ b \in S$ se cumple que $a - b \in S$ y $a \cdot b \in S$.*

Demostración. Sean R un anillo y $S \subseteq R$.

Supongamos que S es un subanillo de R, entonces por definición de subanillo $1 \in S$, ahora, sean $a,\ b \in S$, por demostrar $a-b \in S$, como S es anillo, entonces $-b \in S$ y además por la cerradura de la suma tenemos que $a-b = a+(-b) \in S$, por lo tanto $a - b \in S$.

Ahora supongamos que $1 \in S$ y que para cualesquiera $a,\ b \in S$ se cumple que $a - b \in S$ y $a \cdot b \in S$. entonces $a + b = a + -(-b) \in S$, $0 = a - a \in S$ $\square$

Definición 1.8. Sea R un anillo, un ideal derecho (izquierdo) de R es un subconjunto $I \subseteq R$ tal que:

1) $0 \in I$
2) Para cualesquiera $a,\ b \in I$ se tiene que $a + b \in I$
3) $\forall a \in I$ se tiene que $\forall r \in R$ $a \cdot r \in I$ $(r \cdot a \in I)$

Si $I \subseteq R$ es un ideal derecho e izquierdo, entonces diremos que es un ideal bilateral.

Observación 1.1. Si $I \subseteq R$ es un ideal tal que $1 \in I$ entonces $I = R$, por (2) de la definición de ideal.

Ejemplo 1.7. $\{0\}$, R, y $aR = \{a \cdot r|\ a \in R \text{ fijo y } r \in R\}$ son ideales de R. De hecho este último tipo de ideales que son generados por un sólo elemento son llamados ideales principales, es decir aR es un ideal principal derecho, Ra es un ideal principal izquierdo, y en el caso de que R sea conmutativo diremos simplemente que $Ra = aR$ es un ideal principal.

Ejemplo 1.8. Existen anillos R especiales, que sólo tienen 2 ideales (los triviales) 0 y R, a estos anillos los llamaremos simples.

Proposición 1.2. *Si $I \subsetneq R$ es un ideal derecho, entonces se tiene que $\forall a \in I$ a no tiene inverso derecho.*

Demostración. Sean $I \subsetneq R$ y $a \in I$.

Por demostrar a no tiene inverso derecho, supongamos lo contrario, es decir, que a tiene inverso derecho, entonces $\exists b \in R$ tal que $ab = 1$, pero como I es un ideal y $a \in I$ entonces por definición de ideal derecho $1 = ab \in I$ y como $1 \in I$ entonces $R = 1R \subseteq I$, por lo tanto $R = I$, contradicción, ya que $I \subsetneq R$. Por lo tanto a no tiene inverso derecho. $\square$

Observación 1.2. Los casos donde $I \subsetneq R$ es un ideal izquierdo o bilateral son análogos a la proposición anterior

Observación 1.3. Con la proposición y la observación anterior nos damos cuenta de que si un ideal $I \subset R$ es distinto de R entonces I sólo contiene elementos no invertibles de R.

Observación 1.4. La intersección de ideales vuelve a ser ideal, ya que al estar el cero en todos los ideales va estar en la intersección, al sumar elementos de la intersección obtendremos otro elemento de la intersección ya que en un principio los elementos están dentro de un mismo ideal (por la definición de intersección), y por último la multiplicación de elementos de la intersección por elementos del anillo seguirán estando en la intersección ya que estos están en todos los ideales que se están intersectando (por la definición de ideal). Por otra parte la unión de ideales no necesariamente es un ideal.

Definición 1.9. Sea R un anillo, un elemento r del anillo se dice idempotente si $r^2 = r \cdot r = r$. Es claro que los neutros son idempotentes.

Definición 1.10. Un conjunto de elementos idempotentes E de un anillo R se dice ortogonal si para cualesquiera $e, f \in E$ distintos se tiene que $e \cdot f = 0$. Se dice que dos idempotentes e, f son ortogonales si $\{e, f\}$ es un conjunto ortogonal.

Definición 1.11. Un elemento idempotente e de un anillo R se dice primitivo si $e \neq 0$ y si se cumple que $e = e_1 + e_2$ con e_1, e_2 ortogonales implica que $e_1 = 0$ o $e_2 = 0$.

Definición 1.12. Un conjunto finito $\{e_1, e_2, ..., e_n\}$ de elementos idempotentes de R se dice completo si $e_1 + e_2 + ... + e_n = 1$.

Definición 1.13. En un anillo R se dice que $r \in R$ es nilpotente si existe algún entero positivo n tal que $r^n = 0$, y el menor entero positivo k que satisfaga que $r^k = 0$ será llamado índice de nilpotencia de r.

Ejemplo 1.9. En $\mathbb{Z}_4$ tenemos que $2^2 = 0$, entonces tenemos que 2 es un elemento nilpotente de $\mathbb{Z}_4$ con índice de nilpotencia 2.

Definición 1.14. Sean R un anillo e I un ideal bilateral de R, definimos el cociente R/I, que es otro anillo (anillo cociente), de la siguiente manera:

$r+I=\bar{r}=\{r+i|\ i\in I\}$, y $R/I=\{\bar{r}|\ r\in R\}$, con la suma $(r+I)+(r'+I)=(r+r')+I$ y el producto $(r+I)\cdot(r'+I)=rr'+I$.

Observemos que $\bar{0}=I$.

Ejemplo 1.10. Tomemos el anillo $\mathbb{Z}$ y al ideal $2\mathbb{Z}=\{x\in\mathbb{Z}|\ x=2z \text{ p. a. } z\in\mathbb{Z}\}$, es fácil ver que $2\mathbb{Z}$ es un ideal de $\mathbb{Z}$, tomemos $x,\ y\in 2\mathbb{Z}$ entonce existen $m,\ n\in\mathbb{Z}$ tal que $x=2m$ y $y=2n$ entonces $x+y=2m+2n=2(m+n)\in 2\mathbb{Z}$ y si tomamos un $z\in\mathbb{Z}$ cualquiera entonces $2mz=xz=zx=z2m=2zm\in 2\mathbb{Z}$, por lo tanto $2\mathbb{Z}$ es ideal de $\mathbb{Z}$, ahora hagamos cociente y obtendremos $\mathbb{Z}/2\mathbb{Z}$ (mejor conocido como $\mathbb{Z}_2$) en el cual sólo hay 2 elementos $\bar{0}$y $\bar{1}$

Observación 1.5. Se puede hacer lo mismo con cualquier n natural y obtendremos los conocidos $\mathbb{Z}_n=\{\bar{0},\ \bar{1},...,\ n\bar{-}1\}$

Proposición 1.3. *Todo dominio entero finito es un campo*

Demostración. Sea D un dominio entero finito entonces, basta mostrar que todo elemento distinto de cero tiene inverso. Al ser D finito entonces podemos decir que es un conjunto de n elementos, 0 y otros $n-1$ más, que llamaremos $z_1,\ z_2,...,\ z_{n-1}$, tomemos un elemento $x\in D$ distinto de cero, entonces tenemos su tabla de multiplicar $0=x0$ y otros $n-1$ elementos de la forma xz_i,donde de hecho ninguno se repite ya que si existieran m y n tal que $xz_m=xz_n$, $xz_m-xz_n=0$, $x(z_m-z_n)=0$, $z_m-z_n=0$, $z_m=z_n$ y $m=n$, entonces entre los $n-1$ elementos restantes de la tabla está el 1, por lo tanto existe un z_j tal que $xz_j=1$, por lo tanto x tiene inverso multiplicativo, por lo tanto D es un campo porque es un anillo con división y es conmutativo. □

Proposición 1.4. *$\mathbb{Z}_p$ con p primo es campo.*

Demostración. Basta mostrar que $\mathbb{Z}_p$ es dominio entero, vemos fácilmente que es un anillo conmutativo, así que basta demostrar que no tiene divisores de cero, pero esto también es fácil ya que $\bar{0}=\bar{p}$, supongamos que existe un elemento que es divisor propio de cero es decir existen $\bar{a}\bar{b}=\bar{0}=\bar{p}$ con $\bar{a}\neq\bar{p}\neq\bar{b}$, entonces $ab=p$, lo cual es una contradicción, ya que p es primo y por lo tanto no tiene divisores propios y tomamos $\bar{a}\neq\bar{p}\neq\bar{b}$, entonces $\mathbb{Z}_p$ es dominio entero finito y por lo tanto es un campo. □

Definición 1.15. Un ideal propio I de un anillo R se dice primo si cumple que para cualquier par de elementos $s,r\in R$ tales que $sr\in I$, entonces $s\in I$ o $r\in I$
.

Ejemplo 1.11. Por los resultados antes mostrados podemos ver que en $\mathbb{Z}$, los ideales del tipo $p\mathbb{Z}$ con p primo, son ideales primos.

1.2. Homomorfismos de anillos

Definición 1.16. Sean $(R, +_R, \cdot_R, 0_R, 1_R)$ y $(S, +_S, \cdot_S, 0_S, 1_S)$ anillos, un homomorfismo (morfismo) de anillos es una función $f : R \to S$ tal que:
1) $f(a +_R b) = f(a) +_S f(b)$
2) $f(a \cdot_R b) = f(a) \cdot_S f(b)$
3) $f(1_R) = 1_S$

El núcleo o kernel de un morfismo f es $Nuc(f)$=$\{r \in R|\ f(r) = 0_S\}$, la imagen de f es$Im(f)$=$\{s \in S|\ s = f(r)$ para algún $r \in R\}$, la preimagen de un elemento $s \in S$ la definimos por $f^{-1}(s) = \{r \in R|\ s = f(r)\}$ y la preimagen de un subconjunto $B \subseteq S$ lo definimos por $f^{-1}(B) = \cup_{s\in B} f^{-1}(s)$. En ocasiones nos interesará sólo la imagen de un subconjunto A de R, que se ve como $Im_f(A) = \{s \in S|\ s = f(a)$ para algún $a \in A\}$.

Ahora veamos algunas propiedades de los morfismos de anillos

Proposición 1.5. *Sea $f : R \to S$ un morfismo de anillos, entonces se cumple que:*
a) $f(0_R) = 0_S$.
b) Si I es un ideal derecho de S, entonces $f^{-1}(I)$ es un ideal derecho de R.
c) Si I es un ideal izquierdo de S, entonces $f^{-1}(I)$ es un ideal izquierdo de R.
d) Si I es un ideal bilateral de S, entonces $f^{-1}(I)$ es un ideal bilateral de R.
e) $Nuc(f) \subseteq R$ es un ideal bilateral de R.
f) $f(a - b) = f(a) - f(b)$
g) Si R' es subanillo de R, entonces $f(R')$ es subanillo de S.
h) Si S' es subanillo de S, entonces $f^{-1}(S')$ es subanillo de R.

Demostración. Sea $f : R \to S$ un morfismo de anillos

a) Sea $r \in R$, $f(r) = f(0_R +_R r) = f(0_R) +_S f(r)$, es decir $f(r) = f(0_R) +_S f(r)$, por lo tanto $f(0_R) = 0_S$.

b) Sea $I \subseteq S$ un ideal derecho, por demostrar $f^{-1}(I)$ es un ideal derecho de R. Primero como por el inciso anterior $f(0_R) = 0_S$ y como $0_S \in I$ entonces $0_R \in f^{-1}(I)$. Ahora tomemos $a,\ b \in f^{-1}(I)$ entonces $f(a +_R b) = (f(a) +_S f(b)) \in I$, ya que $f(a), f(b) \in I$, entonces $a + b \in f^{-1}(I)$, ahora tomemos un elemento $r \in R$, $f(a \cdot_R r) = (f(a) \cdot_S f(r)) \in I$, ya que $f(a) \in I$, entonces $a \cdot_R r \in f^{-1}(I)$. Por lo tanto $f^{-1}(I)$ es un ideal bilateral de R.

c) Es análogo a b).

d) juntando b) y c) obtenemos el resultado.

e) $Nuc(f)$ lo podemos ver como $f^{-1}(\{0\})$ por lo tanto es un caso particular de d). Por lo tanto $Nuc(f) \subseteq R$ es un ideal bilateral de R.

f) Como $f(0_R) = 0_S$, entonces $0 = f(0) = f(1_R +_R (-1_R)) = 1_S +_S f(-1_R)$, es decir $1_S +_S f(-1_R) = 0$, entonces $f(-1_R) = -1_S$, ahora si tomamos $a, b \in R$ entonces $f(a - b) = f(a) +_S f(-b) = f(a) +_S f(-1b) = f(a) +_S f(-1)f(b) = f(a) +_S (-f(b)) = f(a) - f(b)$

g) Sea R' es subanillo de R, entonces 1_R está en R' y por definición de morfismo $1_s \in f(R')$, ahora tomemos dos elementos $a,\ b \in f(R')$, por definición de imagen existen $m,\ n \in R'$ tal que $f(m) = a$ y $f(n) = b$, entonces $a - b = f(m) - f(n) = f(m +_R (-n))$ por definición de morfismo y $f(m +_R (-n)) \in f(R')$ y $a \cdot_S b = f(m) \cdot_S f(n) = f(m \cdot_R n)$ por definición de morfismo y $f(m \cdot_R n) \in f(R')$, por lo tanto $f(R')$ es un subanillo de S.

h) Sea S' es subanillo de S, entonces $1_S \in S'$, por definición de morfismo y preimagen $1_R \in f^{-1}(S')$, ahora tomemos $m,\ n \in f^{-1}(S')$, veamos que $m - n \in f^{-1}(S')$, $f(m-n) = f(m) - f(n)$ y $f(m) - f(n) \in S'$ ya que $m, n \in f^{-1}(S')$ y S' es subanillo, entonces $m - n \in f^{-1}(S')$ ahora veamos que $m \cdot_R n \in f^{-1}(S')$, $f(m \cdot_R n) = f(m) \cdot_S f(n)$ y $f(m) \cdot_S f(n) \in S'$ ya que $m, n \in f^{-1}(S')$ y S' es subanillo, entonces $m \cdot_R n \in f^{-1}(S')$, por lo tanto $f^{-1}(S')$ es subanillo de R. $\square$

Ahora veamos algunas propiedades de los morfismos.

Proposición 1.6. *La composición de morfismos de anillos vuelve a ser un morfismo de anillos.*

Demostración. Sean $f : R \to S$ y $g : S \to T$ morfismos de anillos, mostremos que $g \circ f : R \to T$ es un morfismo de anillos:

i) Sean $a,\ b \in R$, $g \circ f(a +_R b) = g(f(a +_R b)) = g(f(a) +_S f(b)) = g(f(a)) +_T g(f(b)) = g \circ f(a) +_T g \circ f(b)$ esto gracias a que g y f son morfismos de anillos.

ii) Sean $a,\ b \in R$, $g \circ f(a \cdot_R b) = g(f(a \cdot_R b)) = g(f(a) \cdot_S f(b)) = g(f(a)) \cdot_T g(f(b)) = g \circ f(a) \cdot_T g \circ f(b)$ esto gracias a que g y f son morfismos de anillos.

iii) $g \circ f(1_R) = g(f(1_R)) = g(1_S) = 1_T$ esto gracias a que g y f son morfismos de anillos.

Por lo tanto la composición de morfismos de anillos vuelve a ser un morfismo de anillos. $\square$

Definición 1.17. Un monomorfismo de anillos es un morfismo de anillos f que es cancelable por la izquierda, es decir, si $f \circ g = f \circ h$ implica $g = h$ con g y h morfismos de anillos.

Nota: en la teoría de anillos es lo mismo ser un monomorfismo de anillos a ser un un morfismo de anillos inyectivo.

Ejemplo 1.12. El morfismo $f : \mathbb{Z} \to \mathbb{Z}$ dado por $f(r) = r + n$ con $n \in \mathbb{N}$ y la inclusión de un subanillo $R' \subseteq R$ en R ($i : R' \to R$ dado por $i(r) = r$)) son monomorfismos, por ser inyectivos

Definición 1.18. Un epimorfismo de anillos es un morfismo de anillos f que es cancelable por la derecha, es decir, si $g \circ f = h \circ f$ implica $g = h$ con g y h morfismo de anillos.

Nota: en la teoría de anillos todo morfismo de anillos suprayectivo es epimorfismo, pero no todo epimorfismo es suprayectivo, como la inclusión de $\mathbb{Z}$ en $\mathbb{Q}$.

Ejemplo 1.13. El morfismo natural $f : R \to R/I$ dado por $f(r) = r + I$ es un epimorfismo, por ser suprayectivo.

Definición 1.19. Un isomorfismo de anillos es un morfismo de anillos f que tiene inverso, es decir, existe f^{-1}morfismo de anillos tal que $f \circ f^{-1}$ y $f^{-1} \circ f$ son las funciones identidades de los correspondientes anillos. Si existe un isomorfismo entre dos anillos R y S, entonces diremos que son isomorfos y lo denotaremos de la siguiente manera $R \cong S$.

Nota: en la teoría de anillos es lo mismo ser un isomorfismo de anillos a ser un morfismo de anillos biyectivo.

Ejemplo 1.14. La función identidad $f : R \to R$ dada por $f(r) = r$ es un isomorfismo. Si $g : R \to S$ es un monomorfismo entonces $R \cong g(R)$, por ser biyectivo.

Proposición 1.7. *Sea $f : R \to S$ un morfismo de anillos, entonces f es inyectivo si y sólo si $Nuc(f) = \{0\}$*

Demostración. Sea $f : R \to S$ un morfismo de anillos. Primero supongamos que f es inyectivo, por demostrar $Nuc(f) = \{0\}$, como f es inyectiva entonces el morfismo es uno a uno, entonces la preimagen del 0, mejor conocida como $Nuc(f)$ consta de un sólo elemento y por la proposición 1.5 sabemos que $f(0) = 0$, por lo tanto tenemos que $Nuc(f) = \{0\}$. Ahora supongamos que $Nuc(f) = \{0\}$ y mostremos que f es inyectivo, supongamos que no, entonces existen $r,\ r' \in R$ distintos, tales que $f(r) = f(r')$, entonces $f(r) - f(r') = 0$ y como f es morfismo tenemos que $f(r-r') = 0$, sea $a = r-r'$, entonces $a \neq 0$ y $a \in Nuc(f)$, contradicción ya que $Nuc(f) = \{0\}$, por lo tanto f es inyectivo. □

Veamos ahora los Teoremas de isomorfismo de anillos.

Teorema 1.1. *(Primer teorema de isomorfismos para anillos)*
Sea $f : R \to S$ un morfismo de anillos, entonces $R/Nuc(f) \cong Im(f)$

Demostración. Sea $f : R \to S$ un morfinismo de anillos, primero el cociente $R/Nuc(f)$ es un anillo bien definido porque $Nuc(f)$ es un ideal bilateral por la Proposición 1.5, además por esta misma proposición sabemos que $Im(f)$ es un anillo, ahora basta mostrar que existe un isomorfismo entre $R/Nuc(f)$ y $Im(f)$. Definamos $g : R/Nuc(f) \to Im(f)$ como $g(r + Nuc(f)) = f(r)$, veamos que g está bien definida, sean $r,\ r' \in R$ tal que $r + Nuc(f) = r' + Nuc(f)$, entonces $g(r + Nuc(f)) = g(r' + Nuc(f))$, entonces $\exists k \in Nuc(f)$ tal que $r = r' + k$, $g(r + Nuc(f)) = f(r) = f(r' + k) = f(r') + f(k) = f(r') = g(r' + Nuc(f))$. Veamos ahora que g es morfismo de anillos, sean $r + Nuc(f),\ r' + Nuc(f) \in R/Nuc(f)$, $g((r+Nuc(f))+(r'+Nuc(f)) = g((r+r')+Nuc(f)) = f(r+r') = f(r)+f(r') = g(r+Nuc(f))+g(r'+Nuc(f))$ y $g((r+Nuc(f))(r'+Nuc(f)) = g((rr') + Nuc(f)) = f(rr') = f(r)f(r') = g(r + Nuc(f))g(r' + Nuc(f))$, por último $g(1 + Nuc(f)) = f(1) = 1$, es decir el uno va a dar al uno, por lo tanto g es un morfismo de anillos. Veamos ahora la inyectividad, supongamos que $g(r + Nuc(f)) = g(r' + Nuc(f))$ entonces $f(r) = f(r')$, $0 = f(r) - f(r') = f(r-r')$, entonces $r - r' \in Nuc(f)$, por lo que $r' + Nuc(f) = r' + (r-r') = r = r + 0 = r + Nuc(f)$, por lo tanto g es inyectiva. Por último la suprayectividad de g es clara ya que todo elemento en $Im(f)$ es de la forma $f(r)$ con $r \in R$ y vendrá justamente de $r + Nuc(f)$. Por lo tanto g es biyectiva, con lo que hemos obtenido un isomorfismo entre $R/Nuc(f)$ y $Im(f)$. □

Teorema 1.2. *(Segundo Teorema de isomorfismos para anillos)*
Sean I un ideal bilateral del anillo R y S un subanillo del mismo, entonces:
i) $S + I = \{x + y |\ x \in S,\ y \in I\}$ es un subanillo de R;
ii) I es un ideal de $S + I$;
iii) $S \cap I$ es un ideal de S;
iv) $(S + I)/I \cong S/(S \cap I)$

Demostración. Sean I un ideal del anillo R y S un subanillo del mismo.

i) Primero como $1 \in S$ y $0 \in I$ entonces $1 = 1 + 0 \in S + I$, ahora tomemos dos elementos $x + y$, $x' + y' \in S + I$ y los multiplicamos $(x + y)(x' + y') = xx' + xy' + yx' + yy' = xx' + (xy' + yx' + yy')$ entonces como $xx' \in S$ porque es cerrado bajo multiplicación y $xy' + yx' + yy' \in I$ por la cerradura por elementos de R que tiene I y la cerradura de la suma de sus elementos obtenemos que $xx' + (xy' + yx' + yy') \in S + I$, por lo tanto $(x+y)(x'+y') \in S+I$ y además, por último hagamos $(x+y)-(x'+y') = x+y-x'-y' = (x-x')+(y-y') \in S+I$, esto gracias a que todos son elementos de R y la suma dentro de una anillo conmuta, con lo que concluimos que $(x + y) - (x' + y') \in S + I$ por lo tanto $S + I$ es un subanillo de R.

ii) Como I se puede ver como $0 + I$, entonces es claro que es un ideal de $S + I$, ya que para comprobar las propiedades de anillo sólo hace falta tomar las que ya tiene I y ponerle un cero al lado, por lo tanto I es un ideal de $S + I$

iii) Primero tenemos que $0 \in S \cap I$ ya que está en ambos por definición, ahora tomemos $m,\ n \in S \cap I$ y como $m + n \in S$ y $m + n \in I$ tenemos que $m+n \in S \cap I$, por último si tomamos un elemento $m \in S \cap I$ y lo multiplicamos por un elemento $s \in S$, entonces $ms \in S$ por su cerradura bajo la multiplicación y $ms \in I$ porque $m \in I$ e I es cerrado por elementos de S, por ser cerrado por elementos de R, por lo cual $ms \in S \cap I$, por lo tanto $S \cap I$ es un ideal de S.

iv) Ahora tomemos el morfismo natural $\pi : R \to R/I$ y consideremos su restricción a S con lo cual obtenemos el morfismo $\pi_0 : S \to \{a + I|$ con $a \in S\}$, es claro que como $Nuc(\pi) = I$ entonces $Nuc(\pi_0) = S \cap I$ por ser restricción a S, ahora mostremos que $\{a + I|$ con $a \in S\} = (S + I)/I$, pero esto es fácil ya que si tomamos un elemento $s \in S$ y $x \in I$ notamos que $(s + x) + I = s + I$ justamente por la definición de $s + I$, entonces tenemos el morfismo $\pi_0 : S \to (S + I)/I$ con $Nuc(\pi_0) = S \cap I$, entonces por el primer teorema de isomorfismos tenemos que $(S + I)/I \cong S/(S \cap I)$. □

Teorema 1.3. *(Tercer teorema de isomorfismos para anillos)*
Sean I y J ideales bilaterales del anillo R tal que $I \subseteq J$, entonces:
i) $J/I = \{j + I|\ j \in J\}$ es un ideal de R/I;
ii) $R/J \cong (R/I)/(J/I)$

Demostración. Sean I y J ideales del anillo R tal que $I \subseteq J$.

i) Primero como J es ideal de R, $0 \in J$ por lo cual $0 + I \in J/I$, además si tomamos $a, b \in I$ tenemos que $(a + I) + (b + I) = (a + b) + I \in J/I$ ya que J es cerrado bajo la suma. Ahora tomemos $r + I \in R/I$ y $j + I \in J/I$, entonces $(r + I)(j + I) = rj + I \in J/I$, ya que J es cerrado bajo la multiplicación por elementos de R. Por lo tanto $J/I = \{j + I |\ j \in J\}$ es un ideal de R/I

ii) Definamos el morfismo de anillos $f : R/I \to R/J$ dado por $f(a + I) = a + J$, veamos que f está bien definida, para esto, supongamos que $a + I = b + I$, esto quiere decir que $a - b \in I$ y como $I \subseteq J$, tenemos entonces que $a - b \in J$, por lo cual $a + J = b + J$, con lo cual queda bien definida, además es claro que es morfismo. Ahora $Nuc(f) = \{a + I |\ a + J = J\} = \{a + I |\ a \in J\} = J/I$, entonces tenemos un morfismo de anillos $f : R/I \to R/J$ con $Nuc(f) = J/I$, entonces por el primer teorema de isomorfismo de anillos tenemos que $R/J \cong (R/I)/(J/I)$. □

Teorema 1.4. *(Cuarto teorema de isomorfismos para anillos o Teorema de la correspondencia)*

Si I es un ideal bilateral del anillo R, entonces la función $f : S \to S/I$ determina tiene una correspondencia uno a uno entre el conjunto de todos los subanillos de R que contienen a I y el conjunto de todos los subanillos de R/I, del mismo modo determina una correspondencia uno a uno entre el conjunto de todos los ideales de de R que contienen a I y el conjunto de todos los ideales de R/I. La función inversa de f es $g : Q \to \pi^{-1}Q$ donde π es el morfismo canónico $\pi : R \to R/I$.

Demostración. El teorema de la correspondencia para grupos induce una correspondencia uno a uno entre los subgrupos aditivos de R que contienen a I y los subgrupos aditivos de R/I. Debemos mostrar que subanillos corresponden a subanillos e ideales a ideales. Si S es un subanillo de R, entonces S/I es cerrado bajo suma, resta y multiplicación, esto debido a las definiciones de suma y multiplicación de S/I, además como $1_R \in S$, por ser subanillo de R, entonces tenemos que $1_R + I \in S/I$, por lo cual S/I es un subanillo de R/I. Recíprocamente, si S/I es un subanillo de R/I, entonces S es cerrado bajo suma, resta y multiplicación, además se debe cumplir que $1_R \in S$, por lo que S es un subanillo de R.

Ahora si J es un ideal de R que contiene a I, entonces J/I es un ideal de R/I, por el tercer teorema de isomorfismos para anillos. Recíprocamente, sea J/I un ideal de R/I. Si $r \in R$ y $a \in J$ entonces $(x+I)(r+I) \in J/I$ entonces por la definición de producto obtenemos que $ar + I \in J/I$, por lo tanto para alguna $j \in J$ tenemos que $ar - j \in I \subseteq J$, entonces $ar \in J$, análogamente $ra \in J$ y de la definición de suma de J/I obtenemos que J es un subgrupo aditivo de R, por lo cual J es un ideal de R. □

Capítulo 2

Módulos

2.1. Módulos y submódulos

Definición 2.1. Dado un anillo R. Un R-módulo derecho es un grupo abeliano (aditivo) M equipado con un un producto por escalares $M \times R \to M$ dado por $(m, r) \mapsto mr$, tal que se cumplen las siguientes propiedades:
i) $m(rr') = (mr)r'$ asociatividad;
ii) $(m + m')r = mr + m'r$ distributividad;
iii) $m(r + r') = mr + mr'$ distributividad;
iv) $m1 = m$ neutro.
$\forall m,\ m' \in M$ y $\forall r,\ r' \in R$ y donde $1 \in R$ es el neutro multiplicativo de R.

La definición de R-módulo izquierdo es similar, sólo se cambia de lado el producto por escalares del anillo. Si es tanto módulo derecho como izquierdo, simplemente diremos que es un R-módulo.

Notación: Si M es un R-módulo derecho lo denotaremos M_R, y si es un R-módulo izquierdo lo denotaremos ${}_RM$, además en ocasiones a los elementos de R los llamaremos escalares.

Ejemplo 2.1. i) Todo grupo abeliano (aditivo) es un $\mathbb{Z}$-módulo derecho (e izquierdo).
ii) Todo espacio vectorial sobre un campo K es un K-módulo derecho (e izquierdo).
iii) Todo anillo R es un R-módulo derecho (e izquierdo) sobre sí mismo.

Definición 2.2. Sea M_R un R-módulo derecho, un conjunto $N \subseteq M$ es un submódulo derecho de M si se cumple que:
i) $0_M \in N$
ii) $\forall n_1,\ n_2 \in N$, $n_1 + n_2 \in N$
iii) $\forall r \in R$ y $\forall n \in N$, $nr \in N$
La definición de submódulo izquierdo es análoga, y si no hay confusión con el lado sólo diremos submódulo.

Notación: denotaremos N_R submódulo de M_R por $N \leq M$.

Ejemplo 2.2. i) Tomemos un anillo R entonces todo ideal derecho de R es un submódulo derecho R_R, y de hecho todo submódulo derecho de R_R es un ideal derecho de R (análogamente con los izquierdos).

ii) Además $\forall M$ R-módulo se cumple que M_R y el $0_R = \{0_M\}$ (submódulo trivial cero) son submódulos de M.

Veamos ahora algunos módulos y submódulos relevantes.

Definición 2.3. Sea R un anillo, se dice que un R-módulo M es simple si sus únicos submódulos son el mismo y el submódulo cero.

Ejemplo 2.3. $\mathbb{Z}_2$ visto como $\mathbb{Z}$-módulo es un módulo simple, ya que por construcción sus únicos dos submódulos son él mismo y el submódulo cero.

Observación 2.1. De hecho todo campo C es un módulo simple sobre sí mismo, ya que los únicos ideales en un campo son el mismo y $\{0_C\}$, esto ya que todos sus elementos, a excepción del cero, son invertibles, por lo cual no puede tener submódulos propios distintos del trivial cero.

Definición 2.4. Dado un anillo R, diremos que un R-módulo derecho M es cíclico si $M = aR$ con $a \in M$, es decir, M es generado por un sólo elemento.

Ejemplo 2.4. Los ideales principales derechos de R son ejemplos de R-módulos derechos cíclicos.

Definición 2.5. Sean R un anillo y M_R un R-módulo derecho, se dice que un submódulo propio N de M es máximo si se cumple que N es el único submódulo propio de M que contiene a N.

Definición 2.6. Sean R un anillo y M_R un R-módulo derecho, se dice que un submódulo propio N de M es mayor si se cumple que $\forall L \lneqq M$ se tiene que $L \subset N$.

Observación 2.2. Todo submódulo mayor de M_R es máximo, ya que al contener a todos los submódulos propios de M él mismo es el único submódulo que lo contiene, de lo contrario obtendríamos una contradicción con la definición. Más aún si $N < M$ es el único submódulo máximo de M entonces N es mayor.

Definición 2.7. Sean R un anillo, M_R un R-módulo derecho y $N \leq M$ un submódulo de M, definimos el módulo cociente $\frac{M}{N} = \{m + N|\ m \in M\}$, con la suma $(m + N) + (m' + N) = (m + m') + N$ y el producto por elementos dela anillo $(m + N)r = mr + N$. Notación: en ocasiones denotaremos $m + N$ por $\bar{m}$

Observación 2.3. $\frac{M}{N}$ en efecto es un R-módulo, ya que:

i) si tomamos $r,\ r' \in R$ y $m+N \in \frac{M}{N}$ entonces $(m+N)rr' = (mr+N)r'$por la definición del producto por elementos del anillo en $\frac{M}{N}$.

ii) si tomamos $m+N,\ m'+N \in \frac{M}{N}$ y $r \in R$ entonces $((m+N)+(m'+N))r = ((m+m')+N)r = (m+m')r+N = (mr+m'r)+N = (mr+N)+(m'r+N)$ esto gracias a las definiciones de suma y producto por escalares de $\frac{M}{N}$ y el producto por escalares de M.

iii) si tomamos $r,\ r' \in R$ y $m+N \in \frac{M}{N}$ entonces $(m+N)(r+r') = m(r+r')+N = (mr+mr')+N = (mr+N)+(mr'+N)$ esto aplicando las mismas propiedades que en el inciso anterior.

iv) por último $(m+N)(1) = (m)(1)+N = m+N$, esto porque M es R-módulo derecho.

Proposición 2.1. *Sean M un R-módulo derecho e I un ideal bilateral de R tal que $MI = 0$, entonces M es un R/I-módulo derecho.*

Demostración. Sean M un R-módulo derecho e I un ideal bilateral de R tal que $MI = 0$, consideremos el anillo R/I, mostremos que M es un R/I-módulo con el producto por escalares $M \times R/I \to M$ dado por $(m, r+I) = mr$. Primero veamos que el producto está bien definido. Si tenemos que $r+I = s+I$ entonces $r-s \in I$ y como tenemos que $MI = 0$, entonces $\forall m \in M\ m(r-s) = 0$, por lo que $mr = ms$, por lo tanto el producto está bien definido, además dado que M es un R-módulo y al final de cuentas el producto que estamos dando es el mismo que tiene como R-módulo entonces los axiomas de módulo se cumplen y por lo tanto M es un R/I-módulo. □

2.2. Homomorfismos de módulos

Definición 2.8. Sean R un anillo y M y N dos R-módulos derechos sobre R, un R-morfismo de módulos es una función $f : M \to N$ tal que $\forall m,\ m \in M$ y $\forall r \in R$ se cumplen:

i) $f(m+m') = f(m)+f(m')$;

ii) $f(mr) = f(m)r$.

En otros momentos si no hay problema de confusión sobre que anillo se está basando el morfismo sólo diremos que es un morfismo de módulos, o morfismo simplemente. Como en los morfismos de anillos, tenemos que el núcleo o kernel de un morfismo de módulos f es $Nuc(f)$=$\{r \in M \mid f(r) = 0_N\}$, la imagen de f es $Im(f)$=$\{n \in N \mid n = f(m)$ para algún $m \in M\}$, la preimagen de un elemento $n \in N$ la definimos por $f^{-1}(n) = \{m \in R \mid n = f(m)\}$ y la preimagen de un subconjunto $L \subseteq N$ lo definimos por $f^{-1}(L) = \cup_{n \in L} f^{-1}(n)$. En ocasiones nos interesará sólo la imagen de un subconjunto K de M, que se ve como $Im(K) = \{n \in N \mid n = f(k)$ para algún $k \in K\}$.

Observación 2.4. También podemos ver $f(a-b) = f(a+(-b)) = f((a)+(b(-1))) = f(a)+f(b(-1)) = f(a)+f(b)(-1) = f(a)-f(b)$.

Ejemplo 2.5. i) Tomando dos R-módulos M y N tal que $N \leq M$ definimos la inclusión como $f : N \to M$ por $f(n) = n$, claramente este es un R-morfismo.

ii) Si tomamos dos R-módulos M y N podemos hacer el morfismo cero, $\bar{0} : M \to N$ donde $\bar{0}(m) = 0_N$ para todo $m \in M$, claramente en efecto es morfismo.

Proposición 2.2. *Si $f : M \to N$ es un R-morfismo de módulos, entonces:*
a) $f(0_M) = 0_N$;
b) Si $K \leq M$ tenemos que $f(K) \leq N$;
c) Si $L \leq N$ tenemos que $f^{-1}(L) \leq M$;
d) $Nuc(f) \leq M$;
e) $Im(f) \leq N$.

Demostración. Sea $f : M \to N$ es un R-morfismo de módulos.

a) $0_N + f(m) = f(m) = f(m + 0_M) = f(m) + f(0_M)$ por lo que $f(0_M) = 0_N$.

b) Sea $K \leq M$, mostremos que $f(K) \leq N$.

i) Como $K \leq M$ entonces $0_M \in K$ y por a) tenemos que $f(0_M) = 0_N \in f(K)$.

ii) Tomemos $n,\ n' \in f(K)$, por definición de imagen tenemos que existen $m,\ m' \in K$ tal que $n = f(m)$ y $n' = f(m')$, ahora $n + n' = f(m) + f(m') = f(m + m')$ ya que f es morfismo, como $K \leq M$ entonces $m + m' \in K$ y por lo tanto $n + n' = f(m) + f(m') = f(m + m') \in f(K)$.

iii) Tomemos $r \in R$ y $n \in f(K)$, por definición de imagen tenemos que existe $m \in K$ tal que $n = f(m)$, ahora $nr = f(m)r = f(mr)$ ya que f es morfismo, como $K \leq M$ entonces $mr \in K$ y por lo tanto $nr = f(mr) \in f(K)$.

c) Sea $L \leq N$, mostremos que $f^{\cdot -1}(L) \leq M$.

i) Como $L \leq N$ entonces $0_N \in L$ y como $f(0_M) = 0_N$, por a), entonces $0_M \in f^{-1}(L)$.

ii) Tomemos $m,\ m' \in f^{-1}(L)$, por definición de preimagen tenemos que existen $n,\ n' \in L$ tal que $n = f(m)$ y $n' = f(m')$, ahora como $L \leq N$ tenemos que $f(m + m') = f(m) + f(m') = n + n' \in L$ y por definición de preimagen concluimos que $m + m' \in f^{-1}(L)$.

iii) Tomemos $r \in R$ y $m \in f^{-1}(L)$, por definición de preimagen tenemos que existe $n \in L$ tal que $n = f(m)$, ahora como $L \leq N$ tenemos que $f(mr) = f(m)r = nr \in L$ y por definición de preimagen concluimos que $mr \in f^{-1}(L)$.

d) Como $Nuc(f) = f^{-1}(0_N)$ y $0_N \leq N$ entonces por c) concluimos que $Nuc(f) \leq M$.

e) como $Im(f) = Im(M)$ y $M \leq M$ entonces por b) $Im(f) \leq N$. □

Proposición 2.3. *Sean R un anillo y $f : M \to N$ un R-morfismo de módulos, entonces f es inyectivo si y sólo si $Nuc(f) = \{0_M\}$*

Demostración. Sean R un anillo y $f : M \to N$ un R-morfismo de módulos, primero supongamos que inyectiva, entonces $f^{-1}(0_N)$ tiene un sólo elemento y como sabemos que $f(0_M) = 0_N$, concluimos entonces que $Nuc(f) = \{0_M\}$.

Ahora supongamos que $Nuc(f) = \{0_M\}$, supongamos que $f(a) = f(b)$ entonces $f(a - b) = f(a) - f(b) = 0_N$, entonces $a - b \in Nuc(f) = \{0_M\}$, por lo que $a - b = 0_M$, $a = b$, por lo tanto f es inyectiva. □

Proposición 2.4. *La composición de morfismos de módulos vuelve a ser morfismo de módulos.*

Demostración. Sean $f : M \to N$ y $g : N \to L$ morfismos de módulos, mostremos que $g \circ f : M \to L$ es un morfismo de módulos.

i) Sean $a,\ b \in M$, $g \circ f(a +_M b) = g(f(a +_M b)) = g(f(a) +_N f(b)) = g(f(a)) +_L g(f(b)) = g \circ f(a) +_L g \circ f(b)$ esto gracias a que g y f son morfismos de módulos.

ii) Sean $m \in M$ y $r \in R$ $(g \circ f(mr)) = g(f(m)r) = g(f(m))r = (g \circ f(m))r$ esto gracias a que g y f son morfismos de anillos.

Por lo tanto la composición de morfismos de módulos vuelve a ser morfismo de módulos. $\square$

Proposición 2.5. *Sea M un R-módulo derecho y $N \leq M$, entonces la función $\pi : M \to \frac{M}{N}$ dada por $\pi(m) = m + N$ es un morfismo de módulos, cuyo núcleo es N*

Demostración. Sea M un R-módulo derecho y $N \leq M$, definamos la función $\pi : M \to \frac{M}{N}$ dada por $\pi(m) = m + N$, mostremos que π es un morfismo de módulos.

i) Sean $a,\ b \in M$, entonces $\pi(a + b) = (a + b) + N = (a + N) + (b + N) = \pi(a) + \pi(b)$, esto gracias a la definición de la suma de $\frac{M}{N}$.

i) Sean $m \in M$ y $r \in R$, entonces $\pi(mr) = mr + N = (m + N)r = \pi(m)r$, esto gracias a la definición del producto por elementos del anillo de $\frac{M}{N}$.

Por último mostremos que $Nuc(\pi) = N$, supongamos que $m \in M$ es tal que $\pi(m) = 0 + N$, esto quiere decir que $m + N = 0 + N$, por lo que $m + 0 \in N$, es decir, $m \in N$, además si tomamos $n \in N$, $\pi(n) = n + N = 0 + N$ por lo tanto $Nuc(\pi) = N$. $\square$

Definición 2.9. Como en el caso de los morfismos de anillos, un morfismo de módulos es un monomorfismo si es un morfismo de módulos cancelable por la izquierda.

Nota: en la teoría de módulos es lo mismo ser un monomorfismo de módulos a un morfismo de módulos inyectivo.

Ejemplo 2.6. Son ejemplos de monomorfismos de módulos:

i)La función identidad.

ii) Si $N \leq M$ entonces la inclusión de N en M dada por $i(n) = n$

Definición 2.10. También un epimorfismo si es un morfismo cancelable por derecha.

Nota: en la teoría de módulos es lo mismo ser un epimorfismo de módulos que un morfismo de módulos suprayectivo.

Ejemplo 2.7. Si $N \leq M$, entonces el morfismos $\pi : M \to \frac{M}{N}$ es un epimorfismo de módulos.

Definición 2.11. Por último, un isomorfismo de módulos es un morfismo de módulos que tiene inverso. Dos R-módulos se dicen isomorfos si existe un R-isomorfismo $f : M \to N$ entre ellos, y lo denotaremos $M \cong N$, y denotaremos a la función inversa por f^{-1}que también es un R-isomorfismo.

Nota: en la teoría de módulos es lo mismo ser un isomorfismo de módulos que un morfismo de módulos biyectivo.

Definición 2.12. Sean R y M un R-módulo, entonces un endomorfismo α de módulos es un R-morfismo que va de M a M, es decir, $\alpha : M \to M$. Si además α resulta ser un isomorfismo diremos que α es un automorfismo de M.

Ejemplo 2.8. Todo monomorfismo de módulos restringido a su imagen es un isomorfismo de módulos.

La inclusión siempre es un monomorfismo, el morfismo del cociente siempre es un epimorfismo y un monomorfismo restringido a la imagen es un isomorfismo.

Teorema 2.1. *(Primer Teorema de isomorfismos para módulos)*
Sea R un anillo y $f : M \to N$ un morfismo de R-módulos, entonces $M/Nuc(f) \cong Im(f)$

Demostración. Sea R un anillo y $f : M \to N$ un morfismo de R-módulos, Definamos $g : M/Nuc(f) \to Im(f)$ como $g(m+Nuc(f)) = f(m)$, veamos que g está bien definida, sean $m,\ m' \in R$ tal que $m+Nuc(f) = m'+Nuc(f)$, entonces $g(m + Nuc(f)) = g(m' + Nuc(f))$, entonces $\exists k \in Nuc(f)$ tal que $m = m' + k$, $g(m+Nuc(f)) = f(m) = f(m'+k) = f(m')+f(k) = f(m') = g(m'+Nuc(f))$. Veamos ahora que g es morfismo de módulos, sean $m+Nuc(f),\ m'+Nuc(f) \in M/Nuc(f)$, $g((m+Nuc(f))+(m'+Nuc(f)) = g((m+m')+Nuc(f)) = f(m+m') = f(m) + f(m') = g(m + Nuc(f)) + g(m' + Nuc(f))$ y $g(mr + Nuc(f)) = f(mr) = f(m)r = g((m+Nuc(f))r)$, por lo tanto g es un morfismo de módulos. Veamos ahora la inyectividad, supongamos que $g(m+Nuc(f)) = g(m'+Nuc(f))$ entonces $f(m) = f(m')$, $0 = f(m) - f(m') = f(m - m')$, entonces $m - m' \in Nuc(f)$, por lo tanto g es inyectiva. Por último la suprayectividad de g es clara ya que todo elemento en $Im(f)$ es de la forma $f(m)$ con $m \in M$ y vendrá justamente de $m+Nuc(f)$. Por lo tanto g es biyectiva, con lo que hemos obtenido un isomorfismo entre $M/Nuc(f)$ y $Im(f)$. □

Teorema 2.2. *(Segundo Teorema de isomorfismos para módulos)*
Sean R un anillo y $S,\ T \leq M$, entonces:
a)$S + T = \{s + t|\ s \in S,\ t \in T\}$ es submódulo de M;
b)$S \cap T$ es submódulo de M;
c) $(S + T)/T \cong S/(S \cap T)$.

Demostración. Sean R un anillo y $S,\ T \leq M$.

a) Consideremos $S+T = \{s+t|\ s \in S,\ t \in T\}$, mostremos que $S+T \leq M$.

i) Como $S,\ T \leq M$ entonces $0 \in S$ y $0 \in T$ por lo que $0 + 0 = 0 \in S + T$.

ii) Sean $s + t,\ s' + t' \in S + T$, entonces $(s + t) + (s' + t') = s + t + s' + t' = (s + s') + (t + t') \in S + T$, gracias a que todos son elementos de M y como tal conmutan en la suma.

iii) Sean $r \in R$ y $s + t \in S + T$, entonces $(s + t)r = sr + tr$ esto por la distributividad que tienen los R-módulos y como $S,\ T \leq M$ entonces $sr \in S$ y $tr \in T$, con lo que concluimos que $(s + t)r \in S + T$.

b) Mostremos que $S \cap T \leq M$.

i) Como $S,\ T \leq M$ entonces $0 \in S$ y $0 \in T$ por lo que $0 \in S \cap T$.

ii) Sean $s,\ t \in S \cap T$, entonces $s,\ t \in S$ y como $S \leq M$ tenemos que $s+t \in S$, usando el mismo razonamiento, obtenemos que $s+t \in T$, por lo que $s+t \in S \cap T$.

iii) Sean $r \in R$ y $n \in S \cap T$, entonces como $S \leq M$ tenemos que $nr \in S$, usando el mismo razonamiento, obtenemos que $nr \in T$, por lo que $nr \in S \cap T$.

c) Definamos la función $f : S \to M/T$ dada por $f(s) = s + T$, dado que ya sabemos que $\pi : M \to M/T$ es un R-morfismo de módulos (por la proposición 2.3) entonces f es un R-morfismo de módulos porque lo único que se hace es reducir el dominio a un submódulo, por lo que las propiedades de R-morfismo se seguirán cumpliendo, ahora dado que $Nuc(\pi) = T$, entonces $Nuc(f) = S \cap T$, y la imagen es $Im(f) = \{s + T|\ s \in S\} = (S + T)/T$, entonces aplicando el primer teorema de isomorfismo obtenemos que $S/S \cap T \cong S + T/T$. □

Teorema 2.3. *(Tercer Teorema de isomorfismos para módulos)*

Sean R un anillo, $M,\ N,\ L$ R-módulos tales que $L \leq N \leq M$, entonces $M/N \cong (M/L)/(N/L)$.

Demostración. Sean R un anillo, $M,\ N,\ L$ R-módulos tales que $L \leq N \leq M$, definamos el morfismo $f : M/L \to M/N$ dado por $f(m) = m+N$, ahora veamos que $Nuc(f) = \{m + L|\ m \in N\} = N/L$, además $Im(f) = \{m + N|\ m \in M\} = M/N$. Entonces por el primer teorema de isomorfismos de módulos tenemos que $(M/L)/(N/L) \cong M/N$. □

Teorema 2.4. *(Cuarto Teorema de isomorfismos para módulos o teorema de la correspondencia)*

Sea N un submódulo de un R-módulo M. La función $S \to S/N$, determina una correspondencia uno a uno entre el conjunto de submódulos de M que contienen a N y el conjunto submódulos de M/N, tiene su inversa que es $T \to \pi^{-1}(T)$, donde $\pi : M \to /N$ es el epimorfismo natural.

Demostración. El teorema de la correspondencia para grupos induce una correspondencia uno a uno entre los subgrupos aditivos de M que contienen a N y los subgrupos aditivos de M/N. Debemos mostrar que submódulos corresponden a submódulos, y para esto es suficiente mostrar que si $S_1/N \leq S_2/N$, entonces $S_1 \leq S_2$ (ya que el recíproco es inmediato). Si $x \in S_1$, entonces $x + N \in S_1/N \subseteq S_2/N$, entonces $x + N = y + N$ para algún $y \in S_2$. Por lo tanto $x - y \in N \subseteq S_2$, y como $y \in S_2$, entonces $x \in S_2$ también. por lo tanto $S_1 \leq S_2$. □

Capítulo 3

Suma y Producto de Anillos y Módulos.

3.1. Sumandos directos

En el capítulo pasado vimos que la intersección de módulos es módulo, ahora veremos otras operaciones que también nos producen módulos.

Por comodidad, de aquí en adelante denotaremos en algunas ocasiones al módulo trivial $\{0\}$ simplemente por 0.

Observación 3.1. Sabemos que la unión de R-módulos no necesariamente es un R-módulo, sin embargo si tenemos una cadena de módulos $M_1 \subseteq M_2 \subseteq ... \subseteq M_n$, entonces la $\cup_{i=1}^{n} M_i$ es un$R$-módulo, ya que $\cup_{i=1}^{n} M_i = M_n$, que es un R-módulo.

Definición 3.1. Sean R un anillo y M un R-módulo, entonces un $A \leq M$ es llamado sumando directo de M si existe $B \leq M$ tal que $A+B = M$ y $A \cap B = 0$, lo cual se denota por $M = A \bigoplus B$.

Observación 3.2. Si M es un R-módulo, entonces M y 0 son sumandos directos, ya que $M = M \bigoplus 0$.

Ejemplo 3.1. Un ejemplo bastante conocido de de sumandos directos se da en la teoría de espacios vectoriales, ya que si V_K es un espacio vectorial con base $\{x_1, x_2, ..., x_n\}$, tenemos que $V_K = \bigoplus_{i=1}^{n} x_i K$.

Definición 3.2. Sean R un anillo y M un R-módulo, decimos que M es directamente inescindible si M y 0 son lo únicos sumandos directos.

Ejemplo 3.2. Consideremos $\mathbb{Z}_{\mathbb{Z}}$, sus submódulos son de la forma $n\mathbb{Z}$, con $n \in \mathbb{N}$, entonces tenemos que $\mathbb{Z}_{\mathbb{Z}}$ es directamente inescindible, ya que $\forall n, m \in \mathbb{N}$ tenemos que $nm \in n\mathbb{Z} \cap m\mathbb{Z}$, es decir, la intersección de cualesquiera dos submódulos no cero de $\mathbb{Z}_{\mathbb{Z}}$ es distinta de cero. Por lo cual los únicos sumandos directos de $\mathbb{Z}_{\mathbb{Z}}$ son el mismo $\mathbb{Z}_{\mathbb{Z}}$ y 0.

Definición 3.3. Sean R un anillo y M un R-módulo, decimos que M es simple si M y 0 son lo únicos submódulos de M, y $M \neq 0$.

Claramente todo R-módulo simple es directamente inescindible.

Ejemplo 3.3. Todo K campo es un K-módulo simple, ya que como todo $x \in K$ es invertible, se tiene que los únicos ideales de K son el mismo y el ideal cero.

Definición 3.4. Sean R un anillo y M un R-módulo, decimos que M es semisimple si todo submódulo de M es sumando directo de M.

Proposición 3.1. *Son equivalentes para un R-módulo M:*
1) M es semisimple;
2) $M = \sum\{S \mid S \leq M, S \text{ simple}\}$;
3) $M = \bigoplus_{i \in I}\{S_i\}$ para alguna familia $\{S_i\}_{i \in I}$ de simples de M.

Demostración. Sea R un anillo y M un R-módulo.
1) $\Longrightarrow$ 2) Supongamos que M es semisimple, si consideramos $\{S_i\}_{i \in I}$ la familia de los submódulos simples de M, entonces todo S_i con $i \in I$ es sumando directo de M, entonces como $\sum\{S \mid S \leq M, S \text{ simple}\}$ es sumando directo de M existe un sumando N de M tal que $N + \sum\{S \mid S \leq M, S \text{ simple}\} = M$ y $N \cap \sum\{S \mid S \leq M, S \text{ simple}\} = 0$, pero como $\sum\{S \mid S \leq M, S \text{ simple}\}$ es una suma de simples, concluimos que $N = 0$, por lo tanto $M = \sum\{S \mid S \leq M, S \text{ simple}\}$.
2) $\Longrightarrow$ 3) Supongamos que $M = \sum\{S \mid S \leq M, S \text{ simple}\}$, ahora supongamos que N y L son submódulos simples de M, como los simples sólo tienen dos submódulos distintos, entonces $N \cap L = N = L$ en caso de que $N = L$, o $N \cap L = 0$ si $N \neq L$, por lo tanto la suma $\sum\{S \mid S \leq M, S \text{ simple}\}$ es directa, por lo tanto $M = \bigoplus_{i \in I}\{S_i\}$ donde $\{S_i\}_{i \in I}$ es la familia de los submódulos simples de M.
3) $\Longrightarrow$ 1) Supongamos que $M = \bigoplus_{i \in I}\{S_i\}$ para alguna familia $\{S_i\}_{i \in I}$ de simples de M, entonces todo submódulo de M es una suma directa de submódulos simples de M, es decir, si tomamos $N \leq M$ entonces existe un subconjunto $F \subseteq I$ tal que $N = \bigoplus_{i \in F}\{S_i\}$, por lo cual existe otro submódulo de M $N' = \bigoplus_{i \in I \setminus F}\{S_i\}$, tal que $N + N' = M$ y $N \cap N' = 0$, por lo que N resulta ser un sumando directo de M, por lo tanto todo submódulo de M es sumando directo suyo. $\square$

Ejemplo 3.4. Aquí tenemos otra vez el ejemplo de los espacios vectoriales ya que si V_K tiene base $\{x_i \mid i \in I\}$ entonces $V_K = \bigoplus_{i \in I} x_i K$, además como todo $x_i K \cong K$, entonces todo $x_i K$ es simple, por lo que $V_K = \bigoplus_{i \in I} x_i K$ es semisimple.

Proposición 3.2. *Sea R un anillo. La clase de los R-módulos semisimples es cerrada bajo submódulos, cocientes y sumas directas, es decir, todo submódulo de un semisimple es semisimple, todo cociente de un semisimple es semisimple y toda suma directa de semisimples es semisimple.*

Demostración. Sean R un anillo y S un R-módulo semisimple.

Primero tomemos M un submódulo de S y tomemos N un submódulo de M. Por definición M es sumando directo de S, por lo cual existe un submódulo de S M' tal que $M \bigoplus M' = S$. Supongamos que N no es sumando directo de M, entonces tomamos $L \leq M$ mínimo tal que $N + L = M$, pero $N \cap L \neq 0$, entonces obtenemos que $N + (L + M') = S$ tal que $N \cap (L + M') \neq 0$, lo cual es una contradicción ya que al ser N submódulo M es submódulo de S, por lo cual es un sumando directo de S. Por lo tanto todo submódulo de un semisimple es semisimple.

Ahora supongamos que M es un cociente de S, entonces M es de la forma S/N. Como S es semisimple entonces existe una familia de R-módulos simples $\{S_i\}_{i\in I}$ tal que $S = \bigoplus_{i\in I} S_i$, entonces tenemos que $N = \bigoplus_{i\in F} S_i$ con $F \subseteq I$, entonces $M = S/N = (\bigoplus_{i\in I} S_i)/(\bigoplus_{i\in F} S_i) = \bigoplus_{i\in I\setminus F} S_i$, es decir, M es una suma directa de simples, por lo tanto M es semisimple.

Por último supongamos que $\{S_i\}_{i\in I}$ es una familia de R-módulos semisimples, consideremos $\bigoplus_{i\in I} S_i$. Para cada S_i con $i \in I$, como es semisimple, existe una familia de módulos simples $\{N_{i_j}\}_{J_i}$ tal que $S_i = \bigoplus_{j\in J_j} N_{i_j}$. Entonces $\bigoplus_{i\in I} S_i = \bigoplus_{i\in I}(\bigoplus_{j\in J_i} N_{i_j})$, es decir $\bigoplus_{i\in I} S_i$ se ve como una suma directa de simples, por lo tanto $\bigoplus_{i\in I} S_i$ es semisimple. □

3.2. Productos y coproductos

Para la construcción de los productos primero recordemos algunos conceptos de la teoría de conjuntos.

Sea $\{A_i | \ i \in I \neq 0\}$ una familia de conjuntos, entonces el producto $\prod_{i\in I} A_i$ de la familia $\{A_i | \ i \in I \neq 0\}$ es el conjunto de funciones $\alpha : I \to \cup_{i\in I} A_i$ con $\alpha(i) \in A_i \ \forall i \in I$.

Notación.

i) Para ahorrar un poco llamemos $a_i = \alpha(i)$, la i-ésima componente de α.

ii) $(a_i) = (\alpha(i)) = \alpha$.

Por lo tanto obtenemos claramente que para todas $(\alpha_i), (\alpha'_i) \in \prod_{i\in I} A_i$ tenemos que $(a_i) = (a'_i)$ si y sólo si $\forall i \in I$ se tiene que $(a_i = a'_i)$.

Aquí observemos que I no es necesariamente numerable. Si I resulta numerable $(I = \{1, 2, 3, ...\})$ entonces usaremos la notación $(a_1a_2a_3...) = (a_i) = \alpha$, si además I resulta finito entonces usaremos $(a_1a_2a_3...a_n) = (a_i) = \alpha$.

Definición 3.5. Sean R un anillo y $\{A_i | \ i \in I\}$ una familia de R-módulos, definimos entonces el R-módulo $\prod_{i\in I} A_i$ con las operaciones:

suma: sean $(a_i), (b_i) \in \prod_{i\in I} A_i$ entonces $(a_i) + (b_i) = (a_i + b_i)$.

producto por escalares: $(a_i)r = (a_ir)$.

Si volvemos a reescribir $\alpha = (a_i)$ y $\beta = (b_i)$, tenemos entonces que $(\alpha + \beta)(i) = \alpha(i) + \beta(i)$ y $(ar)i = \alpha(i)r$. Además tenemos que $(0_i) \in \prod_{i\in I} A_i$, donde 0_i es el cero de A_i, es el neutro para la suma de $\prod_{i\in I} A_i$. Para los inversos aditivos si tomamos $\alpha = (a_i) \in \prod_{i\in I} A_i$ entonces $-\alpha = (-a_i)$, que claramente está en el producto.

Ya con todo esto es fácil ver que $\prod_{i\in I} A_i$ en efecto es un R-módulo.

Definición 3.6. Sean R un anillo y $\{A_i|\ i\in I\}$ una familia de R-módulos, entonces el R-módulo $\prod_{i\in I} A_i$ es llamado el producto directo de la familia $\{A_i|\ i\in I\}$.

Definición 3.7. Sean R un anillo y consideremos el R-módulo $\prod_{i\in I} A_i$, diremos entonces que un elemento $(a_i)\in\prod_{i\in I} A_i$ es de soporte finito si el conjunto $\{i\in I|\ a_i\neq 0\}$ es finito, aceptando el conjunto vació como finito.

Observación 3.3. El conjunto de todos los elementos de soporte finito de $\prod_{i\in I} A_i$ es un submódulo de $\prod_{i\in I} A_i$.

Definición 3.8. Sea R un anillo, si $\prod_{i\in I} A_i$ es el producto directo de la familia $\{A_i|\ i\in I\}$, entonces el submódulo de los elementos de soporte finito de $\prod_{i\in I} A_i$ es llamado suma directa externa de la familia $\{A_i|\ i\in I\}$ y es denotado por $\coprod_{i\in I} A_i$.

Observación 3.4. Es claro que sí I es finito entonces $\prod_{i\in I} A_i=\coprod_{i\in I} A_i$. ya que al ser I finito todo (a_i) sería de soporte finito.

Consideremos ahora algunos de R-morfismos importantes:
$\pi_j:\prod_{i\in I} A_i\to A_i$ dado por $\pi_j((a_i))=a_j\in A_j$.

$\sigma:\coprod_{i\in I} A_i\to\prod_{i\in I} A_i$ dado por $\sigma:\coprod_{i\in I} A_i\to\prod_{i\in I} A_i$ dado por $\sigma((a_i))=(a_i)$, es decir, σ es la inclusión de $\coprod_{i\in I} A_i$ en $\prod_{i\in I} A_i$.

$\eta_j:A_j\to\coprod_{i\in I} A_i$ dado por $\eta_j(a_j)=a_j\in\coprod_{i\in I} A_i$, con
$a_j(i)=\left\{\begin{array}{c} 0 \text{ para } i\neq j \\ a_j \text{ para } i=j\end{array}\right\}$ es decir, η_j es la inclusión de A_j en $\coprod_{i\in I} A_i$.

Proposición 3.3. *Sean R un anillo y si $\prod_{i\in I} A_i$ es el producto directo de la familia $\{A_i|\ i\in I\}$, entonces se cumple que:*
1) π_j y $\pi_j\circ\sigma$ son epimorfismos
2) η_j y $\sigma\circ\eta_j$ son monomorfismos.
3) $\pi_k\circ\sigma\circ\eta_j=\left\{\begin{array}{c} Id_{A_j} \text{ para } k=j \\ 0 \text{ para } k\neq j\end{array}\right.$
4) $(\sigma\circ\eta_j\circ\pi_j)\circ(\sigma\circ\eta_j\circ\pi_j)=\sigma\circ\eta_j\circ\pi_j$ *y* $(\eta_j\circ\pi_j\circ\sigma)\circ(\eta_j\circ\pi_j\circ\sigma)=\eta_j\circ\pi_j\circ\sigma$.

Demostración. Sean R un anillo y si $\prod_{i\in I} A_i$ es el producto directo de la familia $\{A_i|\ i\in I\}$
1) Mostremos que π_j es epimorfismo, sea $x\in A_j$, entonces
$(a_1,a_2,...a_{j-1},x,a_{j+1},...)\in\prod_{i\in I} A_i$ cumple con que
$\pi_j((a_1,a_2,...a_{j-1},x,a_{j+1},...))=x$, por lo que π_j resulta ser suprayectiva, es decir, π_j es epimorfismo. Ahora mostremos que $\pi_j\circ\sigma:\coprod_{i\in I} A_i\to A_j$, para esto tomemos nuevamente un $x\in A_j$, entonces $(0_1,0_2,...0_{j-1},x,0_{j+1},0,0...)\in\prod_{i\in I} A_i$, además vemos claramente que es de soporte finito, por lo que
$(0_1,0_2,...0_{j-1},x,0_{j+1},0,0...)\in\coprod_{i\in I} A_i$ y se cumple con que

$\pi_j \circ \sigma((0_1, 0_2, ...0_{j-1}, x, 0_{j+1}, ...)) = x$, por lo que $\pi_j \circ \sigma$ resulta ser suprayectiva, es decir, $\pi_j \circ \sigma$ es epimorfismo.

2) Mostremos que η_j es monomorfismo, sean $x, y \in A_j$ tal que $\eta_j(x) = \eta_j(y)$, por lo que $\eta_j(x) - \eta_j(y) = 0$ y en particular en la j-ésima entrada tenemos que $x - y = 0$, es decir, $x = y$, por lo que η_j resulta ser inyectivo, es decir, η_j es monomorfismo. Ahora mostremos que $\sigma \circ \eta_j : A_j \to \prod_{i \in I} A_i$, para esto tomemos nuevamente $x, y \in A_j$, pero esta vez los tomaremos de forma que $x \neq y$, ahora aplicando η_j llegamos a $\eta_j(x)$ y a $\eta_j(y)$, si les aplicamos σ, por definición de σnos quedamos en $\eta_j(x)$ y $\eta_j(y)$, ahora como $x \neq y$, entonces $\eta_j(x)$ y $\eta_j(y)$ tienen la j-esima entrada distinta, por lo que $\eta_j(x) \neq \eta_j(y)$, es decir, $\sigma \circ \eta_j$ resulta inyectivo, es decir, $\sigma \circ \eta_j$ es un monomorfismo.

3) Sea $x \in A_j$ entonces $x \overset{\eta_j}{\mapsto} \begin{cases} x \text{ para } i = j \\ 0 \text{ para } i \neq j \end{cases} \overset{\sigma}{\mapsto} \begin{cases} x \text{ para } i = j \\ 0 \text{ para } i \neq j \end{cases} \overset{\pi_j}{\mapsto}$ $\begin{cases} x \text{ para } k = j \\ 0 \text{ para } k \neq j \end{cases}$, entonces si $k \neq j$ pues como $\eta_j(x) = 0 \ \forall i \neq j$, en particular la k-ésima entrada de$\eta_j(x)$ es cero, ya que $j \neq k$, entonces $\pi_k(\eta_j(x)) = 0$, entonces $\pi_k \circ \sigma \circ \eta_j$ en este caso es el morfismo cero, ahora si $k = j$, tenemos que la k-ésima entrada de $\eta_j(x)$ es x, por lo que $\pi_k(\eta_j(x)) = x$, es decir, en este caso $\pi_k \circ \sigma \circ \eta_j$ es la identidad en A_j, por lo tanto concluimos que $\pi_k \circ \sigma \circ \eta_j = \begin{cases} Id_{A_j} \text{ para } k = j \\ 0 \text{ para } k \neq j \end{cases}$.

4) sea $(a_i) \in \prod_{i \in I} A_i$ entonces

$(a_i) \overset{\pi_j}{\mapsto} a_j \overset{\eta_j}{\mapsto} \begin{cases} a_j \text{ para } i = j \\ 0 \text{ para } i \neq j \end{cases} \overset{\sigma}{\mapsto} \begin{cases} a_j \text{ para } i = j \\ 0 \text{ para } i \neq j \end{cases}$ y además

$(a_i) \overset{\pi_j}{\mapsto} a_j \overset{\eta_j}{\mapsto} \begin{cases} a_j \text{ para } i = j \\ 0 \text{ para } i \neq j \end{cases} \overset{\sigma}{\mapsto} \begin{cases} a_j \text{ para } i = j \\ 0 \text{ para } i \neq j \end{cases} \overset{\pi_j}{\mapsto} a_j \overset{\eta_j}{\mapsto}$ $\begin{cases} a_j \text{ para } i = j \\ 0 \text{ para } i \neq j \end{cases} \overset{\sigma}{\mapsto} \begin{cases} a_j \text{ para } i = j \\ 0 \text{ para } i \neq j \end{cases}$, por lo que concluimos que $(\sigma \circ \eta_j \circ \pi_j) \circ (\sigma \circ \eta_j \circ \pi_j) = \sigma \circ \eta_j \circ \pi_j$.

Ahora tomemos $(a_i) \in \coprod_{i \in I} A_i$, entonces

$(a_i) \overset{\sigma}{\mapsto} (a_i) \overset{\pi_j}{\mapsto} a_j \overset{\eta_j}{\mapsto} \begin{cases} a_j \text{ para } i = j \\ 0 \text{ para } i \neq j \end{cases} \overset{\sigma}{\mapsto} \begin{cases} a_j \text{ para } i = j \\ 0 \text{ para } i \neq j \end{cases}$ y además

$(a_i) \overset{\sigma}{\mapsto} (a_i) \overset{\pi_j}{\mapsto} a_j \overset{\eta_j}{\mapsto} \begin{cases} a_j \text{ para } i = j \\ 0 \text{ para } i \neq j \end{cases} \overset{\sigma}{\mapsto} \begin{cases} a_j \text{ para } i = j \\ 0 \text{ para } i \neq j \end{cases} \overset{\pi_j}{\mapsto} a_j \overset{\eta_j}{\mapsto}$

$\overset{\eta_j}{\mapsto} \begin{cases} a_j \text{ para } i = j \\ 0 \text{ para } i \neq j \end{cases}$, por lo que concluimos que $(\eta_j \circ \pi_j \circ \sigma) \circ (\eta_j \circ \pi_j \circ \sigma) = \eta_j \circ \pi_j \circ \sigma$. □

En el sentido categórico, el producto directo de una familia de R-módulos $\prod_{i \in I} A_i$ junto con el conjunto de las proyecciones $\{\pi_i : \prod_{i \in I} A_i \to A_i\}_{i \in I}$ cumple con ser un producto para la categoría de los R-módulos, es decir:

i) $\prod_{i\in I} A_i$ es un R-módulo.
ii) $\{\pi_i |\ i \in I\}$ es una familia de R-morfismos tal que $\pi_i : \prod_{i\in I} A_i \to A_i$ $\forall i \in I$.
iii) Para toda familia de R-morfismos $\{\gamma_i : C \to A_i\}_{i\in I}$ existe un único morfismo $\gamma : C \to \prod_{i\in I} A_i$ tal que $\gamma_i = \pi_i \circ \gamma$ $\forall i \in I$.

En el sentido categórico, el coproducto directo de una familia de R-módulos $\coprod_{i\in I} A_i$ junto con el conjunto de las proyecciones $\{\eta_i : A_i \to \coprod_{i\in I} A_i\}_{i\in I}$ cumple con ser un coproducto para la categoría de los R-módulos, es decir:
i) $\coprod_{i\in I} A_i$ es un R-módulo.
ii) $\{\eta_i |\ i \in I\}$ es una familia de R-morfismos tal que $\eta_i : A_i \to \coprod_{i\in I} A_i$ $\forall i \in I$.
iii) Para toda familia de R-morfismos $\{\gamma_i : A_i \to C\}_{i\in I}$ existe un único morfismo $\gamma : \coprod_{i\in I} A_i \to C$ tal que $\gamma_i = \gamma \circ \eta_i$ $\forall i \in I$.

Ahora un poco de notación, si I es un conjunto no vacío y M es un R-módulo entonces a:

$\prod_{i\in I} M_i$, con $M_i = M$ $\forall i \in I$, lo denotamos por M^I y

$\coprod_{i\in I} M_i$, con $M_i = M$ $\forall i \in I$, lo denotamos por $M^{(I)}$.

Entonces decimos que M^I es el producto directo de $|I|$ copias de M y que $M^{(I)}$ es la suma directa de $|I|$ copias de M.
Ahora recordando los morfismos η_j, llamemos $A'_j = \eta_j(A_j)$, con esto tenemos que $A'_j \cong A_j$, ya que si $I = \{1, 2, 3, ...\}$ entonces $A'_j = \{(0, ...0, a_j, 0, ...)|\ a_j \in A_j\}$, claramente a_j está en el j-ésimo lugar en $(0, ...0, a_j, 0, ...)$.

Proposición 3.4. *Sean R un anillo y $\{A_i |\ i \in I\}$ una familia de R-módulos, entonces tenemos que $\coprod_{i\in I} A_i = \bigoplus_{i\in I} A'_i$ donde $A_i \cong A'_i$ $\forall i \in I$.*

Demostración. Sean R un anillo y $\{A_i |\ i \in I\}$ una familia de R-módulos, entonces por la definición dada anteriormente de A'_i tenemos que $\sum_{i\in I} A'_i$ se incluye en $\coprod_{i\in I} A_i$. Tomemos ahora un elemento $0 \neq (a_i) \in \coprod_{i\in I} A_i$ donde $a_{i_1}, a_{i_2}, ..., a_{i_n}$ son los únicos distintos de cero, es decir, $a_i = 0$ $\forall i \in I\backslash\{i_1, ..., i_n\}$ y $a_{i_j} \neq 0$ $\forall j \in \{1, 2, ..., n\}$, de esto se sigue que $(a_i) \in A'_{i_1} + A'_{i_2} + ... + A'_{i_n}$, entonces $(a_i) \in \sum_{i\in I} A'_i$, es decir todo elemento de $\coprod_{i\in I} A'_i$ es elemento de $\sum_{i\in I} A'_i$, por lo tanto $\sum_{i\in I} A'_i = \coprod_{i\in I} A'_i$. Consideremos ahora A'_j con $j \in I$ y $\sum_{j\neq i\in I} A'_i$, entonces tenemos que si $(a_i) \in A'_j \cap \sum_{j\neq i\in I} A'_i$, entonces $a_i = 0$ $\forall i \neq j$, por la definición de A'_j. y además si $a_j = 0$, tenemos que $(a_i) = 0$, con lo cual la demostración queda completa. □

Definición 3.9. Sea R un anillo, decimos que una familia de R-módulos $\{U_i\}_{i\in I}$ genera al R-módulo M si existe un epimorfismo $\bigoplus_{i\in I} U_i \to M$.
Si el conjunto I resulta ser finito diremos que M es finitamente generado.

Ejemplo 3.5. Todo espacio vectorial ${}_FV$ es generado por una suma de copias de F, es decir, hay un epimorfismo de $F^{(I)} \to_F V$.

Observación 3.5. Si M_R es finitamente generado entonces todo submódulo propio de M_R está contenido en un submódulo máximo de M_R.

Definición 3.10. Sea R un anillo, decimos que una familia de R-módulos $\{U_i\}_{i\in I}$ cogenera al R-módulo M si existe un monomorfismo $M \to \prod_{i\in I} U_i$.

Definición 3.11. Diremos que un R-módulo M es finitamente cogenerado si se cumplen las siguientes afirmaciones equivalentes:

1) Si existe un monomorfismo $f : M \to \prod_{i\in I} U_i$, entonces existe un subconjunto finito $F \subseteq I$ tal que $M \xrightarrow{f'} \prod_{i\in I} U_i \xrightarrow{\pi_F} \prod_{i\in F} U_i$ es monomorfismo.

2) Si $\cap_{i\in I} N_i = 0$ para alguna familia de submódulos $\{N_i\}_{i\in I}$ de M entonces existe un subconjunto finito $F \subseteq I$ tal que $\cap_{i\in F} N_i = 0$.

Ejemplo 3.6. Todo módulo con un número finito de submódulos es finitamente cogenerado.

Definición 3.12. Sean R un anillo, M un R-módulo y $X \subseteq M$, se dice que X es una base de M si:

i) $Gen(X) = M$

ii) X es independiente, es decir, si $\sum_{x\in F \ finito} xr_x = 0$, implica $r_x = 0 \ \forall x \in F$.

Definición 3.13. Sea R un anillo, diremos que un R-módulo M es libre si es isomorfo a alguna suma directa de copias de R, es decir, $R^{(I)} \cong M$.

Ejemplo 3.7. Todo espacio vectorial es tiene base y es libre.

Capítulo 4

Sucesiones Exactas

4.1. Sucesiones exactas

Definición 4.1. Sean M, N, L tres R-módulos derechos, y $f : M \to N$, $g : N \to L$ dos R-morfismos entre ellos, se dice que la sucesión $M \xrightarrow{f} N \xrightarrow{g} L$ es exacta en N si $Im(f) = Nuc(g)$.

Observación 4.1. Otra forma de dar la definición anterior es diciendo que

$M \xrightarrow{f} N \xrightarrow{g} L$ es exacta en N si y sólo si $g \circ f = \{0\}$ y $Nuc(g) \subseteq Im(f)$.

Notación: Sean M y N dos R-módulos derechos, entonces $\bar{0} : M \to N$ es la función definida por $\bar{0}(m) = 0$, que claramente es un R-morfismo de módulos.

Ejemplo 4.1. Sean M y N dos R-módulos derechos, $f : M \to N$ un R-morfismo de módulos y consideremos el morfismo $\bar{0} : \{0\} \to M$. Entonces la sucesión $0 \xrightarrow{\bar{0}} M \xrightarrow{f} N$ es exacta en M si y sólo sí $Nuc(f) = \{0\}$, ya que $Im(\bar{0}) = \{0\}$.

Consideremos ahora los R-morfismos de módulos $f : M \to N$ y $\bar{0} : N \to \{0\}$. Entonces la sucesión $M \xrightarrow{f} N \xrightarrow{\bar{0}} 0$ es exacta en N si y sólo sí $Im(f) = N$, ya que $Nuc(\bar{0}) = N$.

Proposición 4.1. *Sean M y N dos R-módulos derechos y $f : M \to N$ un R-morfismo de módulos. Entonces:*

i) La sucesión $0 \xrightarrow{\bar{0}} M \xrightarrow{f} N$ es exacta en M si y sólo si f es inyectiva.

ii) La sucesión $M \xrightarrow{f} N \xrightarrow{\bar{0}} 0$ es exacta en N si y sólo si f es suprayectiva.

Demostración. Sean M y N dos R-módulos derechos y $f : M \to N$ un R-morfismo de módulos.

i) Supongamos que la sucesión $0 \xrightarrow{\bar{0}} M \xrightarrow{f} N$ es exacta entonces por ejemplo 4.1 $Nuc(f) = \{0\}$ por lo tanto f es inyectiva.

Supongamos ahora que f es inyectiva, entonces $Nuc(f) = \{0\}$ y como $Im(\bar{0}) = \{0\}$, entonces tenemos que $Nuc(f) = \{0\} = Im(\bar{0})$ por lo tanto la sucesión $0 \xrightarrow{\bar{0}} M \xrightarrow{f} N$ es exacta.

ii) Supongamos que la sucesión $M \xrightarrow{f} N \xrightarrow{\bar{0}} 0$ es exacta entonces por ejemplo 4.1 $Im(f) = N$ por lo tanto f es suprayectiva.

Supongamos ahora que f es suprayectiva, entonces $Im(f) = N$ y como $Nuc(\bar{0}) = N$, entonces tenemos que $Im(f) = N = Nuc(\bar{0})$ por lo tanto la sucesión $M \xrightarrow{f} N \xrightarrow{\bar{0}} 0$ es exacta. □

Observación 4.2. Sean M, N, L tres R-módulos derechos, entonces decimos que la sucesión $0 \xrightarrow{\bar{0}} M \xrightarrow{f} N \xrightarrow{g} L \xrightarrow{\bar{0}} 0$ es exacta si f es inyectiva, g es suprayectiva y se tiene que $Im(f) = Nuc(g)$. La exactitud en M y L se comprueba con la proposición anterior. y la condición de que $Im(f) = Nuc(g)$ nos da la exactitud en N. Para ahorrar un poco en las siguientes ocasiones dejaremos de poner $\bar{0}$, a menos de que sea completamente necesario, es decir, $0 \xrightarrow{\bar{0}} M \xrightarrow{f} N \xrightarrow{g} L \xrightarrow{\bar{0}} 0$ se convertirá en

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

Definición 4.2. Diremos que un diagrama
$$\begin{tikzcd} M \arrow[r, "f"] \arrow[dr, "\alpha"] & N \arrow[d, "\beta"] \\ & N' \end{tikzcd}$$
conmuta si $\beta(f(m)) = \alpha(m)$ $\forall m \in M$ y diremos que un diagrama
$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\alpha"] & N \arrow[d, "\beta"] \\ M' \arrow[r, "f'"] & N' \end{tikzcd}$$
conmuta si $\beta(f(m)) = f'(\alpha(m))$ $\forall m \in M$. En fin diremos que un diagrama conmuta si las distintas composiciones posibles resultan ser funciones iguales.

Lema 4.1. *(lema de los cinco)*

Si el siguiente diagrama de R-módulos y R-morfismos de módulos conmuta y tiene renglones exactos

$$\begin{tikzcd} M_1 \arrow[r, "f_1"] \arrow[d, "g_1"] & M_2 \arrow[r, "f_2"] \arrow[d, "g_2"] & M_3 \arrow[r, "f_3"] \arrow[d, "g_3"] & M_4 \arrow[r, "f_4"] \arrow[d, "g_4"] & M_5 \arrow[d, "g_5"] \\ N_1 \arrow[r, "h_1"] & N_2 \arrow[r, "h_2"] & N_3 \arrow[r, "h_3"] & N_4 \arrow[r, "h_4"] & N_5 \end{tikzcd}$$

entonces:

i) Si g_2 y g_4 son inyectivos y g_1 es suprayectivo entonces g_3 es inyectivo;

ii) Si g_2 y g_4 son suprayectivos y g_5 es inyectivo entonces g_3 es suprayectivo;

iii) Si g_1,g_2, g_4 y g_5 son isomorfismos entonces g_3 es isomorfismo.

Demostración. Sea

$$\begin{array}{ccccccccc} M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \xrightarrow{f_3} & M_4 & \xrightarrow{f_4} & M_5 \\ \downarrow{\scriptstyle g_1} & & \downarrow{\scriptstyle g_2} & & \downarrow{\scriptstyle g_3} & & \downarrow{\scriptstyle g_4} & & \downarrow{\scriptstyle g_5} \\ N_1 & \xrightarrow{h_1} & N_2 & \xrightarrow{h_2} & N_3 & \xrightarrow{h_3} & N_4 & \xrightarrow{h_4} & N_5 \end{array}$$

un diagrama conmutativo de R-módulos y R-morfismos de módulos con renglones exactos.

i) Supongamos que g_2 y g_4 son inyectivos y que g_1 es suprayectivo, tomemos $m_3 \in M_3$ tal que $g_3(m_3) = 0$, mostremos que $m_3 = 0$, $h_3(g_3(m_3)) = 0 = g_4(f_3(m_3))$, por la conmutatividad del diagrama y el hecho de que cero va a cero, ahora como $g_4$es inyectiva entonces $f(m_3) = 0$, por lo cual $m_3 \in Nuc(f_3) = Im(f_2)$ por exactitud, existe entonces un $m_2 \in M_2$ tal que $f_2(m_2) = m_3$y como $g_3(m_3) = 0$ por conmutatividad se tiene que $g_3(f_2(m_2)) = 0 = h_2(g_2(m_2))$, de donde obtenemos que $g_2(m_2) \in Nuc(h_2) = Im(h_1)$, con lo que existe $n_1 \in N_1$ tal que $h_1(n_1) = g_2(m_2)$, ahora como g_1 es suprayectiva entonces existe $m_1 \in M_1$ tal que $g_1(m_1) = n_1$, por lo que $g_2(m_2) = h_1(g_1(m_1)) = g_2(f_1(m_1))$, esta última igualdad por conmutatividad, después de todo esto quiere decir que $m_2 = f_1(m_1)$, con lo cual $m_3 = f_2(f_1(m_1)) = 0$ ya que la sucesión es exacta. Por lo tanto $g_3$es inyectiva.

ii) Supongamos que g_2 y g_4 son suprayectivos y que g_5 es inyectivo, tomemos $n_3 \in N_3$, entonces como g_4 es suprayectiva existe $m_4 \in M_4$tal que $h_3(n_3) = g_4(m_4)$, aplicando h_4 obtenemos que $0 = h_4(h_3(n_3)) = h_4(g_4(m_4)) = g_5(f_4(m_4))$, por la conmutatividad del diagrama, concluimos entonces que $f_4(m_4) = 0$ ya que g_5 es inyectiva, entonces $m_4 \in Nuc(f_4) = Im(f_3)$ por exactitud, existe entonces $m_3 \in M_3$ tal que $f_3(m_3) = m_4$, con lo que $g_4(f_3(m_3)) = g_4(m_4) = h_3(n_3)$, entonces por conmutatividad $h_3(g_3(m_3)) = h_3(n_3)$, entonces como h_3 es morfismo obtenemos que $n_3 - g_3(m_3) \in Nuc(h_3) = Im(h_2)$, existe entonces $n_2 \in N_2$ tal que $h_2(n_2) = n_3 - g_3(m_3)$, es decir, $n_3 = h_2(n_2) + g_3(m_3)$, además como g_2 es suprayectiva existe $m_2 \in M_2$ tal que $g_2(m_2) = n_2$, por lo que $n_3 = h_2(g_2(m_2)) + g_3(m_3) = g_3(f_2(m_2)) + g_3(m_3)$, esta última igualdad por conmutatividad, finalmente como g_3 es morfismo tenemos que $n_3 = g_3(f_2(m_2) + m_3) = g_3(f_2(m_2)) + g_3(m_3)$, por lo tanto $g_3$es suprayectiva.

iii) Supongamos que g_1,g_2, g_4 y g_5 son isomorfismos entonces se cumplen las condiciones necesarias para que se cumplan tanto i) como ii) ya que un isomorfismo de módulos es lo mismo que un morfismo de módulos biyectivo, en fin como se cumplen i) y ii) entonces g_3 es inyectivo y suprayectivo, por lo tanto g_3 es un isomorfismo de módulos. $\square$

Corolario 4.1. *Sean A, B, C, A', B', C' R-módulos derechos tales que*

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

son sucesiones exactas y se tiene el siguiente diagrama

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r] & 0 \end{tikzcd}$$ *conmutativo, entonces:*

i) Si α y γ son monomorfismos entonces β también es monomorfismo;
ii) Si α y γ son epimorfismos entonces β también es epimorfismo.
iii) Si α y γ son isomorfismos entonces β también es isomorfismo.

Demostración. Sean A, B, C, A', B', C' R-módulos derechos tales que

$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ y $0 \longrightarrow A' \xrightarrow{f'} B' \xrightarrow{g'} C' \longrightarrow 0$
son sucesiones exactas y se tiene el siguiente diagrama

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r] & 0 \end{tikzcd}$$ conmutativo, para mostrar las implicaciones sólo basta decir que consideramos la identidad $i : 0 \to 0$ la cual obviamente es un isomorfismo y entonces i) se debe al inciso i) del lema anterior, podemos hacer un razonamiento análogo para ii) y por último iii) lo podemos ver como una consecuencia de i) y ii), ya que como hemos dicho antes es lo mismo ser isomorfismo de módulos, que morfismo de módulos biyectivo. □

Definición 4.3. Se dice que el morfismo de R-módulos $f : A \to B$ es núcleo del morfismo de R-módulos $g : B \to C$ si $g \circ f = \bar{0}$ y si existe otro R-morfismo de módulos $h : D \to B$ tal que $g \circ h = \bar{0}$ entonces existe un único morfismo $\bar{h} : D \to A$ tal que el diagrama

$$\begin{tikzcd} A \arrow[r, "f"] & B \arrow[r, "g"] & C \\ & D \arrow[ul, "\bar{h}"] \arrow[u, "h"] \arrow[ur, "\bar{0}"'] & \end{tikzcd}$$

conmuta. En este caso por notación diremos que $f = nuc(g)$

Ejemplo 4.2. Sea $g : B \to C$ un R-morfismo de módulos, consideremos $Nuc(g)$, y la inclusión $i : Nuc(g) \to B$, entonces i es núcleo de g, primero claramente $g \circ i = \bar{0}$ ya que la composición lo que hace es restringir el dominio de g a $Nuc(g)$, ahora supongamos que existe otro R-morfismo de módulos $h : D \to B$ tal que $g \circ h = \bar{0}$ entonces sólo basta correstringir h a $Nuc(g)$ obteniendo el siguiente diagrama

$$\begin{tikzcd} Nuc(g) \arrow[r, "i"] & B \arrow[r, "g"] & C \\ & D \arrow[ul, "h|^{Nuc(g)}"] \arrow[u, "h"] \arrow[ur, "\bar{0}"'] & \end{tikzcd}$$

ya que si tomamos $d \in D$, $h(d) = b$ para alguna $b \in B$, pero como $g \circ h = 0$ entonces $b \in Nuc(g)$ $h(d) = h|^{Nuc(g)}(d) = b$ está bien definido entonces $h|^{Nuc(g)}$ y el diagrama conmuta.

Definición 4.4. Se dice que el morfismo de R-módulos $g : B \to C$ es conúcleo del morfismo de R-módulos $f : A \to B$ si $g \circ f = \bar{0}$ y si existe otro R-morfismo de módulos $h : B \to D$ tal que $h \circ f = \bar{0}$, entonces existe un único morfismo

$\bar{h}: C \to D$ tal que el diagrama
$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "\bar{0}"'] & B \arrow[r, "g"] \arrow[d, "h"] & C \arrow[dl, "\bar{h}"] \\ & D & \end{tikzcd}$$
conmuta. En este caso por notación diremos que $g = conuc(f)$.

Ejemplo 4.3. Tomemos un R-morfismo de módulos $f : A \to B$ y el cociente $\pi : B \to B/f(A)$, en este caso π resulta ser un conúcleo para f, ya que claramente $\pi \circ f = \bar{0}$, porque $f(A) = Nuc(\pi)$, ahora supongamos que existe otro morfismo de anillos $h : B \to D$ tal que $h \circ f = \bar{0}$, entonces existe un único morfismo $\bar{h} : B/f(A) \to D$ tal que el diagrama
$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "\bar{0}"'] & B \arrow[r, "g"] \arrow[d, "h"] & C \arrow[dl, "\bar{h}"] \\ & D & \end{tikzcd}$$
conmuta. Sólo definimos $\bar{h}$ por $\bar{h}(\bar{b}) = h(b)$, que está bien definido ya que como $h \circ f = \bar{0}$, $\bar{h}(\bar{b}) = h(b + f(A)) = h(b) + h(f(A)) = h(b)$.

Proposición 4.2. *El núcleo de un R-morfismo de módulos es único, salvo isomorfismo.*

Demostración. Sean $g : B \to C$ un R-morfismo de módulos y $f : A \to B$, $h : D \to B$ tales que ambos son núcleos de g, ahora consideremos a f, como $h : D \to B$ es tal que $g \circ h = \bar{0}$ entonces existe un único morfismo $\bar{h} : D \to A$ tal que el diagrama
$$\begin{tikzcd} A \arrow[r, "f"] & B \arrow[r, "g"] & C \\ & D \arrow[ul, "\bar{h}"] \arrow[u, "h"] \arrow[ur, "\bar{0}"'] & \end{tikzcd}$$
conmuta. Siguiendo el mismo razonamiento, pero ahora con h, como $f : A \to B$ es tal que $g \circ f = \bar{0}$ entonces existe un único morfismo $\bar{f} : D \to A$ tal que el diagrama ☐

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend left, "\bar{0}"] \arrow[dr, "\bar{f}"] & B \arrow[r, "g"] & C \\ & D \arrow[ul, "\bar{h}"] \arrow[u, "h"] \arrow[ur, "\bar{0}"'] & \end{tikzcd}$$
conmuta, luego tenemos que $f \circ \bar{h} \circ \bar{f} = f$ y que $h \circ \bar{f} \circ \bar{h} = h$,

de esto se sigue que $\bar{f} \circ \bar{h} = Id_A$ y que $\bar{h} \circ \bar{f} = Id_D$, por lo que $\bar{h}$ es isomorfismo.

Proposición 4.3. *El núcleo de un morfismo es monomorfismo.*

Demostración. Sean $g : B \to C$ un R-morfismo de módulos y $f : A \to B$ el núcleo de g, ahora consideremos dos morfismos $h : D \to A$ y $h' : D \to A$ tales que $f \circ h = f \circ h'$, entonces tenemos que $g \circ f \circ h = 0 = g \circ f \circ h'$, entonces por la definición de núcleo tenemos que $h = h'$, por lo tanto f es monomorfismo. ☐

Observación 4.3. Análogamente así como el núcleo de un morfismo es único y es monomorfismo, se tiene que el conúcleo de un morfismo es único y es epimorfismo.

Observación 4.4. En la sucesión exacta $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ f es $nuc(g)$ y g es $conuc(f)$

Lema 4.2. *(Lema de la serpiente)*

Supongamos que el siguiente diagrama de R-módulos y R-morfismos de módulos es conmutativo y que los renglones son exactos

$$\begin{tikzcd}
 & M_1 \arrow[r, "f_1"] \arrow[d, "t_1"] & M_2 \arrow[r, "f_2"] \arrow[d, "t_2"] & M_3 \arrow[r] \arrow[d, "t_3"] & 0 \\
0 \arrow[r] & N_1 \arrow[r, "h_1"] & N_2 \arrow[r, "h_2"] & N_3 &
\end{tikzcd}$$

Entonces existe una sucesión de la forma

$$Nuc(t_1) \xrightarrow{g_1} Nuc(t_2) \xrightarrow{g_2} Nuc(t_3) \xrightarrow{s} N_1/Im(t_1) \xrightarrow{p_1} N_2/Im(t_2) \ldots$$

$N_2/Im(t_2) \xrightarrow{p_2} N_3/Im(t_3)$ *donde* $s(k_3) = h_1^{-1}(t_2(f_2^{-1}(k_3))) + Im(t_1)$, *con* $k_3 \in Nuc(t_3)$.

Demostración. En el siguiente diagrama los morfismos l_i son inyecciones las j_i son morfismos de conúcleo como en el ejemplo 4.3.

$$\begin{tikzcd}
 & Nuc(t_1) \arrow[r, "g_1"] \arrow[d, "l_1"] & Nuc(t_2) \arrow[r, "g_2"] \arrow[d, "l_2"] & Nuc(t_3) \arrow[d, "l_3"] \arrow[dddll, "s"] & \\
 & M_1 \arrow[r, "f_1"] \arrow[d, "t_1"] & M_2 \arrow[r, "f_2"] \arrow[d, "t_2"] & M_3 \arrow[r] \arrow[d, "t_3"] & 0 \\
0 \arrow[r] & N_1 \arrow[r, "h_1"] \arrow[d, "j_1"] & N_2 \arrow[r, "h_2"] \arrow[d, "j_2"] & N_3 \arrow[d, "j_3"] & \\
 & N_1/Im(t_1) \arrow[r, "p_1"] & N_2/Im(t_2) \arrow[r, "p_2"] & N_3/Im(t_3) &
\end{tikzcd}$$

Entonces por construcción las columnas resultan ser exactas ya que son sucesiones como las de la observación 4.3. Hay que definir los morfismos g_i, p_i, $i = 1, 2$ y probar que la sucesión

$$Nuc(t_1) \xrightarrow{g_1} Nuc(t_2) \xrightarrow{g_2} Nuc(t_3) \xrightarrow{s} N_1/Im(t_1) \xrightarrow{p_1} N_2/Im(t_2) \ldots$$

$N_2/Im(t_2) \xrightarrow{p_2} N_3/Im(t_3)$ es exacta.

Primero veamos como son los g_i. Tomemos $k_1 \in Nuc(t_1)$, entonces $t_1(k_1) = 0$ y $h_1(t_1(k_1)) = 0 = t_2(f_1(k_1)$ por exactitud y la conmutatividad del diagrama, concluimos entonces que $f_1(k_1) \in Nuc(t_2)$. De la misma manera si tomamos $k_2 \in Nuc(t_2)$, entonces $t_2(k_2) = 0$ y $h_2(t_2(k_2)) = 0 = t_3(f_2(k_3)$ por exactitud y la conmutatividad del diagrama, concluimos entonces que $f_2(k_2) \in Nuc(t_3)$. Lo que nos permite definir a g_1 y g_2, de la siguiente manera: $g_1(k_1) = f_1(k_1)$

y $g_2(k_2) = f_2(k_2)$, es decir, que las g_i son las restricciones de las f_i a $Nuc(t_i)$, además por construcción $f_1 \circ l_1 = l_2 \circ g_1$ y $f_2 \circ l_2 = l_3 \circ g_2$, es decir, el diagrama conmuta en esa zona.

Ahora veamos como son los p_i, pues estos se definen de manera natural, es decir, $p_1(n_1 + Im(t_1)) = h_1(n_1) + Im(t_2)$ con $n_1 \in N_1$, análogamente $p_2(n_2 + Im(t_2)) = h_2(n_2) + Im(t_3)$ con $n_2 \in N_2$. Notemos además que por construcción $p_1 \circ j_1 = j_2 \circ h_1$ y $p_2 \circ j_1 = j_3 \circ h_2$.

Veamos que si definimos $s(k_3) = h_1^{-1}(t_2(f_2^{-1}(k_3))) + Im(t_1)$ entonces s está bien definido. Tomemos $k_3 \in Nuc(t_3) \subseteq M_3$, entonces existe $m_2 \in M_2$ tal que $f_2(m_2) = k_3$, por la exactitud del renglón, de donde $h_2(t_2(m_2)) = t_3(f_2(m_2)) = t_3(k_3) = 0$ por la conmutatividad del diagrama, lo cual implica que $t_2(m_2) \in Nuc(h_2) = Im(h_1)$ por la exactitud. Por lo que existe $n_1 \in N_1$ tal que $t_2(m_2) = h_1(n_1)$, entonces vemos que podemos definir $s(k_3) = n_1 + Im(t_1)$, con $h_1(n_1) = t_2(m_2)$ y $f_2(m_2) = k_3$, que se puede reescribir como $s(k_3) = h_1^{-1}(t_2(f_2^{-1}(k_3))) + Im(t_1)$. Ahora si $m_2' \in M_2$ es tal que $f_2(m_2') = k_3 = f_2(m_2)$, entonces $m_2 - m_2' \in Nuc(f_2) = Im(f_1)$, luego $m_2 - m_2' = f_1(m_1)$, con $m_1 \in M_1$, además, $h_2(t_2(m_2')) = t_3(f_2(m_2')) = t_3(k_3) = 0$, de donde $t_2(m_2') \in Nuc(h_2) = Im(h_1)$, por lo que existe $n_1' \in N_1$tal que $t_2(m_2') = h_1(n_1')$. Entonces restando resulta $0 = t_2(m_2) - t_2(m_2') = h_1(n_1) - h_1(n_1') = h_1(n_1 - n_1') = t_2(f_1(m_1)) = h_1(t_1(m_1))$, pero como $h_1$es inyectiva entonces $n_1 - n_1' = t_1(m_1) \in Im(t_1)$, con esto se muestra que s está bien definida.

Ahora hay que ver las exactitudes:

i) Tomemos $g_1(k_1) \in Im(g_1)$, con $k_1 \in Nuc(t_1)$, entonces $g_2(g_1(k_1)) = g_2(f_1(k_1)) = f_2(f_1(k_1)) = 0$, gracias a la conmutatividad del diagrama, con lo que concluimos que $Im(g_1) \subseteq Nuc(g_2)$. Tomemos ahora $k_2 \in Nuc(g_2)$, con $k_2 \in Nuc(t_2)$, entonces $g_2(k_2) = 0 = f_2(k_2)$, por lo que $k_2 \in Nuc(f_2) = Im(f_1)$, de donde $k_2 = f_1(k_1)$, con $k_1 \in M_1$. Ahora si mostramos que $k_1 \in Nuc(t_1)$, entonces $k_2 = g_1(k_1) \in Im(g_1)$, con lo cual tendríamos $Nuc(g_2) \subseteq Im(g_1)$. Tomemos $h_1(t_1(k_1)) = t_2(f_1(k_1)) = t_2(k_2)$, pero como h_1 es inyectiva, entonces $t_1(k_1) = 0$. Por lo tanto $Im(g_1) = Nuc(g_2)$.

ii) Tomemos $k_3 = g_2(k_2) \in Im(g_2)$, con $k_2 \in Nuc(t_2) \subseteq M_2$, ya antes vimos que $g_2(k_2) = f_2(k_2)$, luego en la definición de s podemos tomar $m_2 = k_2$, entonces $t_2(m_2) = 0 = h_1(n_1)$, pero como h_1 es inyectivo, tenemos que $n_1 = 0$, de esta manera $s(k_3) = 0 + Im(t_1)$, por lo que $Im(g_2) \subseteq Nuc(s)$. Recíprocamente, tomemos $k_3 \in Nuc(s) \subseteq Nuc(t_3)$, entonces $n_1 \in Im(t_1)$, tomemos $m_1 \in M_1$ tal que $n_1 = t_1(m_1)$, luego $h_1(t_1(m_1)) = t_2(m_2)$, con $f_2(m_2) = k_3$, resulta entonces que, $t_2(m_2) = t_2(f_1(m_1))$ con lo cual $k_2 = m_2 - f_1(m_1) \in Nuc(t_2)$. De esto obtenemos que $f_2(k_2) = f_2(m_2 - f_1(m_1) = f_2(m_2) - f_2(f_1(m_1)) = f_2(m_2) - 0 = f_2(m_2) = k_3$, por la exactitud, con lo que concluimos que $k_3 = g_2(k_2) \in Im(g_2)$, ya que $g_2(k_2) = f_2(k_2)$. Por lo tanto $Im(g_2) = Nuc(s)$.

iii) Tomemos ahora $n_1 + Im(t_1) = s(k_3) \in Im(s)$ con $k_3 \in Nuc(t_3)$, entonces $p_1(n_1 + Im(t_1)) = h_1(n_1) + Im(t_2) = t_2(m_2) + Im(t_2) = 0 + Im(t_2)$, ya que $t_2(m_2) \in Im(t_2)$, con lo que concluimos que $Im(s) \subseteq Nuc(p_1)$. Tomemos $n_1 + Im(t_1) \in Nuc(p_1)$, con $n_1 \in N_1$, entonces $h_1(n_1) + Im(t_2) = 0 + Im(t_2)$, por lo que $h_1(n_1) \in Im(t_2)$, de donde $h_1(n_1) = t_2(m_2)$ con $m_2 \in M_2$. Sea $k_3 = f_2(m_2)$, pero notemos que $t_3(k_3) = t_3(f_2(m_2)) = h_2(t_2(m_2)) = h_2(h_1(n_1))=0$, gracias a la conmutatividad del diagrama y a la exactitud del renglón, concluimos entonces que $k_3 \in Nuc(t_3)$, con esto $s(k_3) = n_1 + Im(t_1)$, por lo que $Nuc(p_1) \subseteq Im(s)$. Por lo tanto $Im(s) = Nuc(p_1)$.

iv) Tomemos $p_1(n_1 + Im(t_1)) \in Im(p_1)$, con $n_1 \in N_1$, entonces $p_2(p_1(n_1 + Im(t_1))) = p_2(h_1(n_1) + Im(t_2)) = h_2(h_1(n_1)) + Im(t_3) = 0 + Im(t_3)$, es decir, $Im(p_1) \subseteq Nuc(p_2)$. Recíprocamente, sea $n_2 + Im(t_2) \in Nuc(p_2)$, con $n_2 \in N_2$, entonces $h_2(n_2) \in Im(t_3)$ y existe $m_2 \in M_3$ tal que $h_2(n_2) = t_3(m_3)$, como f_2 es suprayectivo existe entonces $m_2 \in M_2$ tal que $f_2(m_2) = m_3$, luego $h_2(n_2) = t_3(f_2(m_2)) = h_2(t_2(m_2))$ por conmutatividad del diagrama. Esto nos da que $n_2 - t_2(m_2) \in Nuc(h_2) = Im(h_1)$ por exactitud del renglón, con lo cual $n_2 - t_2(m_2) = h_1(n_1)$, con $n_1 \in N_1$, de lo que resulta que $n_2 - h_1(n_1) = t_2(m_2) \in Im(t_2)$, por lo que $n_2 + Im(t_2) = h_1(n_1) + Im(t_2) = p_1(n_1 + Im(t_1)) \in Im(p_1)$, con lo que obtenemos que $Nuc(p_2) \subseteq Im(p_1)$ y por lo tanto $Im(p_1) = Nuc(p_2)$.

Con esto queda demostrado el lema. □

Definición 4.5. Una sucesión exacta $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ de R-módulos

i) Se escinde por izquierda si existe un R-morfismo de módulos $\alpha : B \to A$ tal que $\alpha \circ f = Id_A$;

ii) Se escinde por derecha si existe un R-morfismo de módulos $\beta : C \to B$ tal que $g \circ \beta = Id_C$;

iii) Se escinde si se escinde por ambos lado.

Proposición 4.4. *Sea* $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *una sucesión exacta entonces son equivalentes:*

i) la sucesión se escinde por izquierda

ii) $B = f(A) \bigoplus C'$ *donde* $C' \cong C$

iii) la sucesión se escinde por derecha

Demostración. Sea $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ una sucesión exacta de R-módulos.

i) $\Longrightarrow$ ii) por hipótesis tenemos que existe $u : B \to A$ tal que $u \circ f = Id_A$, mostremos ahora que $B = f(A) \bigoplus Nuc(u)$, tomemos $b \in B$, entonces $b \overset{u}{\mapsto} u(b) \overset{f}{\mapsto} f(u(b)) \overset{u}{\mapsto} u(f(u(b))) = u(b)$ ya que $u \circ f = Id_A$, tenemos entonces que $u(f(u(b)) - b) = u(f(u(b))) - u(b) = 0$, por lo que $b - f(u(b)) \in Nuc(u)$, de esta manera $b \in Nuc(u) + f(u(b)) \subseteq Nuc(u) + f(A)$, por lo tanto $B \subseteq f(A) + Nuc(u)$. La otra contención es inmediata ya que $f(A) \subseteq B$ y $Nuc(u) \subseteq B$, por lo que $f(A) + Nuc(u) \subseteq B$, por lo tanto $B = f(A) + Nuc(u)$. Ahora veamos que la suma es directa, Tomemos $x \in f(A) \cap Nuc(u)$, entonces $x = f(a)$ para algún $a \in A$ y $u(x) = 0$, entonces tenemos $0 = u(x) = u(f(a)) = a$, por lo que $a = 0$ lo que implica que $0 = f(0) = f(a) = x$, entonces $x = 0$, por lo que $f(A) \cap Nuc(u) = 0$, por lo que la suma es directa, por lo tanto $B = f(A) \bigoplus Nuc(u)$. Ahora sólo falta mostrar que $Nuc(u) \cong C$, veamos que g restringida a $Nuc(u)$ es una biyección, como la sucesión $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ es exacta, tenemos entonces que $C = g(B) = g(f(A) \bigoplus Nuc(u)) = g(f(A)) + g(Nuc(u))$ y como $g \circ f = \bar{0}$,entonces $C = 0 + g(Nuc(u))$, con lo que concluimos que $C = g(Nuc(u))$, por lo cual $g|_{Nuc(u)} : Nuc(u) \to C$ es suprayectivo; veamos ahora que es inyectivo, tenemos que $Nuc(g|_{Nuc(u)}) = Nuc(u) \cap Nuc(g) = Nuc(u) \cap f(A) = 0$, por la exactitud de la sucesión, entonces $Nuc(g|_{Nuc(u)}) = 0$, por lo cual es inyectivo, por lo tanto $g|_{Nuc(u)}$ es biyectivo, es decir, $Nuc(u) \cong C$, por lo tanto $B = f(A) \bigoplus C'$ donde $Nuc(u) = C' \cong C$.

ii) $\Longrightarrow$ iii) Como por hipótesis $B = f(A) \bigoplus C'$ donde $C' \cong C$, podemos considerar la sucesión exacta $0 \longrightarrow A \xrightarrow{f} f(A) \bigoplus C' \xrightarrow{g} C \longrightarrow 0$, mostremos que existe $v : C \to f(A) \bigoplus C'$ tal que $g \circ v = Id_C$, consideremos entonces $g^{-1}|_{C'} : C \to C'$ la inversa de la restricción de g a C' y la inclusión $i : C' \to f(A) \bigoplus C'$, llamemos $v = i \circ (g|_{C'})^{-1}$ y mostremos que $g \circ v = Id_C$. Tomemos $x \in C$, entonces tenemos que $g \circ v(x) = g(v(x)) = g(i \circ (g|_{C'})^{-1}(x)) = g(i(g^{-1}(x))) = g(g^{-1}(x)) = x$, por lo que $g \circ v = Id_C$. por lo tanto la sucesión exacta se escinde por la derecha.

iii) $\Longrightarrow$ i) Supongamos que la sucesión $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$, es decir, existe $v : C \to B$ tal que $g \circ v = Id_C$, veamos que $B = f(A) \bigoplus v(C)$, tomemos $b \in B$, entonces $b \underset{\rightarrow}{g} g(b) \underset{\rightarrow}{v} v(g(b)) \underset{\rightarrow}{g} g(v(g(b))) = g(b)$ ya que $g \circ v = Id_C$, tenemos entonces que $g(v(g(b)) - b) = g(v(g(b))) - g(b) = 0$, entonces $v(g(b))) - b \in Nuc(g)$, por lo cual $b \in v(g(b)) + Nuc(g) = v(g(b)) + f(A)$ ya que la sucesión es exacta, concluimos entonces que $b \in Im(v) + Im(f)$, es decir, $B \subseteq f(A) + v(C)$, la otra contención es clara ya que $f(A) \subseteq B$ y $v(C) \subseteq B$, por lo que $f(A) + v(C) \subseteq B$, por lo tanto $B = f(A) + v(C)$. Ahora hay que ver que la suma es directa, para eso tomemos $x \in f(A) \cap v(C)$, entonces tenemos que $f(a) = x = v(c)$ para alguna $a \in A$ y alguna $c \in C$ y además tenemos que $g(x) = 0$, porque $x \in f(A) = Nuc(g)$ gracias a la exactitud de la sucesión, entonces $Id_C(c) = g(v(c)) = g(x) = 0$, por lo que la suma en efecto es exacta. Por último definamos $u : f(A) + v(C) \to A$ dado por $u(x) = u(f(a) + v(c)) = a$, entonces con esta definición $u \circ f = Id_A$, por lo que la sucesión se escinde por izquierda. □

Observación 4.5. Dada la proposición anterior, podemos decir que una sucesión exacta $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ se escinde, si se escinde por algún lado.

Proposición 4.5. *A es sumando directo de M si* $0 \longrightarrow A \xrightarrow{i} M$ *se escinde*

4.2. Proyectivos e inyectivos

Definición 4.6. Un R-módulo P es proyectivo si toda sucesión exacta

$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} P \longrightarrow 0$ se escinde.

Ejemplo 4.4. Los R-módulos libres son proyectivos.

Proposición 4.6. *Sea R un anillo, son equivalentes para un R-módulo P:*
i) P es proyectivo.

ii) Para toda sucesión exacta $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *y todo R-morfismo $h : P \to C$ existe un R-morfismo $\bar{h} : P \to B$ tal que el siguiente diagrama conmuta*

$$\begin{tikzcd} & & & P \arrow[dl, "\bar{h}"'] \arrow[d, "h"] & \\ 0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[r] & 0 \end{tikzcd}$$

Demostración. Sea R un anillo y P un R-módulo.
i) $\Longrightarrow$ ii) Consideremos el siguiente diagrama

$$\begin{tikzcd} & & & P \arrow[d, "h"] & \\ 0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[r] & 0 \end{tikzcd}$$

donde el segundo renglón es exacto y P es un módulo proyectivo. Mostremos que existe una función $\bar{h} : B \to Q$ tal que el diagrama

$$\begin{tikzcd} & & & P \arrow[dl, "\bar{h}"'] \arrow[d, "h"] & \\ 0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[r] & 0 \end{tikzcd}$$

conmuta, primero consideremos el R-modulo $B \bigoplus P$ y las proyecciones $\pi_B : B \bigoplus P \to B$, $\pi_P : B \bigoplus P \to P$ para con ellas obtener el R-módulo $Nuc(h\pi_P - g\pi_B)$, que en efecto es un R-módulo por ser el núcleo de un R-morfismo, hagamos la inyección, $i : Nuc(h\pi_P - g\pi_B) \to B \bigoplus P$, entonces definimos $\varphi = \pi_P \circ i : Nuc(h\pi_P - g\pi_B) \to P$ y $\psi = \pi_B \circ i : Nuc(h\pi_P - g\pi_B) \to B$ tal que el siguiente diagrama conmuta

$$\begin{tikzcd} & & Nuc(h\pi_P - g\pi_B) \arrow[rr, "\varphi"] \arrow[dd, "\psi"] \arrow[dr, "i"] & & P \arrow[dd, "h"] & \\ & & & B \bigoplus P \arrow[ur, "\pi_P"] \arrow[dl, "\pi_B"] & & \\ 0 \arrow[r] & A \arrow[r, "f"] & B \arrow[rr, "g"] & & C \arrow[r] & 0 \end{tikzcd}$$

Ahora veamos que el cuadrado

$$\begin{tikzcd} Nuc(h\pi_P - g\pi_B) \arrow[r, "\varphi"] \arrow[d, "\psi"] & P \arrow[d, "h"] \\ B \arrow[r, "g"] & C \end{tikzcd}$$

conmuta, es decir, $h \circ \varphi = g \circ \psi$. Tomemos un $x \in Nuc(h\pi_P - g\pi_B)$ entonces por un lado $x \overset{\varphi}{\mapsto} \pi_P(x) \overset{h}{\mapsto} h(\pi_P(x))$ y por el otro $x \overset{\psi}{\mapsto} \pi_B(x) \overset{g}{\mapsto} g(\pi_B(x))$ y como $x \in Nuc(h\pi_P - g\pi_B)$

entonces $(h\pi_P - g\pi_B)(x) = 0$, es decir, $h(\pi_P(x)) = g(\pi_B(x))$, por lo tanto el cuadrado conmuta. Ahora veamos que φ es suprayectiva, tomemos $m \in P$, si le aplicamos h llegamos a $h(m) \in C$, ahora como g es suprayectiva tenemos que existe $b \in B$ tal que $g(b) = h(m)$, por lo cual $h(m) - g(b) = 0$, es decir, $(b, m) \in Nuc(h\pi_P - g\pi_B)$, y es tal que $\varphi((b, m)) = m$, por lo tanto φ es suprayectiva, entonces basta completar el renglón superior con el núcleo de φ para obtener el siguiente diagrama conmutativo con los renglones exactos

$$\begin{tikzcd} 0 \arrow[r] & Nuc(\varphi) \arrow[r, "i"', "i"] & Nuc(h\pi_P - g\pi_B) \arrow[r, "\varphi"] \arrow[d, "\psi"] & P \arrow[r] \arrow[d, "h"] & 0 \\ 0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[r] & 0 \end{tikzcd}$$

Ahora como por hipótesis P es proyectivo, tenemos que φ se escinde, es decir, existe $\beta : P \to Nuc(h\pi_P - g\pi_B)$ tal que $\varphi \circ \beta = Id_P$. Por último mostremos que $g \circ \psi \circ \beta = h$, consideremos $g \circ \psi \circ \beta$, pero como $h \circ \varphi = g \circ \psi$, entonces $g \circ \psi \circ \beta = h \circ \varphi \circ \beta$, pero como $\varphi \circ \beta = Id_P$, entonces $h \circ \varphi \circ \beta = h \circ Id_P = h$, entonces definiendo $\bar{h} = h \circ \beta$, obtenemos una función tal que el diagrama

$$\begin{tikzcd} & & & P \arrow[dl, "\bar{h}"'] \arrow[d, "h"] & \\ 0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[r] & 0 \end{tikzcd}$$

conmuta.

ii) $\Longrightarrow$ i) Supongamos que P es proyectivo, consideremos el siguiente diagrama

$$\begin{tikzcd} & & & P \arrow[d, "i"] & \\ 0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & P \arrow[r] & 0 \end{tikzcd}$$

, con el segundo renglón exacto y $i : P \to P$ el morfismo identidad, ahora por hipótesis existe $\bar{i} : P \to B$ tal que el siguiente diagrama conmuta

$$\begin{tikzcd} & & & P \arrow[dl, "\bar{i}"'] \arrow[d, "i"] & \\ 0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & P \arrow[r] & 0 \end{tikzcd}$$

entonces $\bar{i} : P \to B$ hace que la sucesión exacta se escinda, por lo que P resulta proyectivo. $\square$

Proposición 4.7. *Sean R un anillo y P_1 y P_2 R-módulos, entonces P_1 y P_2 son proyectivos si y sólo si $P_1 \bigoplus P_2$ es proyectivo.*

Demostración. Sean R un anillo. Tomemos P_1 y P_2 dos R-módulos proyectivos. Sea

$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} P_1 \bigoplus P_2 \longrightarrow 0$ una sucesión exacta. Ahora consideremos los R-morfismos $g|^{P_1} : B \to P_1$ y $g|^{P_2} : B \to P_2$ con los cuales podemos construir las sucesiones exactas:

$0 \longrightarrow A_1 \xrightarrow{f_1} B \xrightarrow{g|^{P_1}} P_1 \longrightarrow 0$ y

$0 \longrightarrow A_2 \xrightarrow{f_2} B \xrightarrow{g|^{P_2}} P_2 \longrightarrow 0$, donde A_1 y A_2 están definidas de tal manera que las sucesiones son exactas (en particular podemos tomar los núcleos), además las tenemos que las sucesiones se escinden gracias a que P_1 y P_2 son proyectivos, sean entonces $\beta_1 : P_1 \to B$ y $\beta_2 : P_2 \to B$ las escisiones y definimos $\beta : P_1 \bigoplus P_2 \to B$ que es inducida justamente por β_1 y β_2, con lo cual obtenemos que la sucesión

$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} P_1 \bigoplus P_2 \longrightarrow 0$ se escinde, por lo tanto $P_1 \bigoplus P_2$ es proyectivo.

Para el regreso sólo basta tomar cualquier sucesión exacta de la forma

$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} P_1 \bigoplus P_2 \longrightarrow 0$ la cual, como $P_1 \bigoplus P_2$ es proyectivo, se escinde, es decir, existe $\beta : P_1 \bigoplus P_2 \to B$, sólo basta tomar las restricciones a P_1 y P_2 para obtener las escisiones deseadas con lo cual obtenemos que P_1 y P_2 son proyectivos. □

Como corolario a esta proposición tenemos que toda suma directa finita de R-módulos es proyectiva si y sólo si cada sumando lo es.

Definición 4.7. Un R-módulo Q es inyectivo si toda sucesión exacta

$0 \longrightarrow Q \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ se escinde.

Ejemplo 4.5. Los espacios vectoriales son inyectivos.

Proposición 4.8. *Sea R un anillo, son equivalentes para un R-módulo Q:*

i) Q es inyectivo.

ii) Para toda sucesión exacta $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ y todo R-morfismo $h : A \to Q$ existe un R-morfismo $\bar{h} : B \to Q$ tal que el siguiente diagrama conmuta

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "h"] & B \arrow[r, "g"] \arrow[dl, "\bar{h}"] & C \arrow[r] & 0 \\ & Q & & & \end{tikzcd}$$

Demostración. Sean R un anillo y Q un R-módulo.

i) $\Longrightarrow$ ii) Consideremos el siguiente diagrama

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "h"] & B \arrow[r, "g"] & C \arrow[r] & 0 \\ & Q & & & \end{tikzcd}$$

, con el primer renglón exacto y Q inyectivo. Mostremos que existe una función $\bar{h} : B \to Q$ tal que el diagrama

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "h"] & B \arrow[r, "g"] \arrow[dl, "\bar{h}"] & C \arrow[r] & 0 \\ & Q & & & \end{tikzcd}$$

conmuta, primero consideremos $Q \times B$ y las inclusiones $i_Q : Q \to Q \times B$, $i_B : B \to Q \times B$ y hagamos la proyección, $\pi : Q \times B \to Q \times B/(i_Q \circ h\text{-}i_B \circ f)(A)$, entonces definimos $\gamma : Q \to$

$Q \times B/((i_Q \circ h - i_B \circ f)(A))$ y $\beta : B \to Q \times B/((i_Q \circ h - i_B \circ f)(A))$ tal que el siguiente diagrama conmuta

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[rr, "f"] \arrow[dd, "h"] & & B \arrow[r, "g"] \arrow[dl, "i_B"'] \arrow[dd, "\beta"] & C \arrow[r] & 0 \\
& & Q \times B \arrow[dr, "\pi"] & & & \\
& Q \arrow[ur, "i_Q"] \arrow[rr, "\gamma"] & & Q \times B/((i_Q \circ h - i_B \circ f)(A)) & &
\end{tikzcd}$$

Primero veamos que el cuadrado

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "h"] & B \arrow[d, "\beta"] \\
Q \arrow[r, "\gamma"] & Q \times B/((i_Q \circ h - i_B \circ f)(A))
\end{tikzcd}$$

conmuta, tomemos un elemento $a \in A$, entonces $a \overset{f}{\mapsto} f(a) \overset{i_B}{\mapsto} (0, f(a)) \overset{\pi}{\mapsto} [(0, f(a)]$ y $a \overset{h}{\mapsto} h(a) \overset{i_Q}{\mapsto} (h(a), 0) \overset{\pi}{\mapsto} [(h(a), 0)]$ y como $[(0, f(a)] = [(h(a), 0)]$ concluimos que el cuadro en efecto conmuta.

Ahora veamos que γ es inyectivo, tomemos $x \in Q$ tal que $\gamma(x) = [0]$ entonces por conmutatividad tenemos que $x \overset{i_Q}{\mapsto} (x, 0) \overset{\pi}{\mapsto} [(x, 0)]$ entonces por la construcción de π tenemos que $(x, 0) \in (i_Q \circ h - i_B \circ f)(A)$, entonces existe $a \in A$ tal que $(x, 0) = (i_Q \circ h - i_B \circ f)(a) = (h(a), f(a))$, de aquí obtenemos que $h(a) = x$ y $f(a) = 0$, pero como, por hipótesis, f es inyectivo, nos resulta que $a = 0$, por último tenemos que $x = h(a) = h(0) = 0$, es decir obtenemos que si $\gamma(x) = [0]$ entonces $x = 0$, por lo que γ es inyectivo, con lo que agregando el conúcleo de γ y llamado $Q \times B/((i_Q \circ h - i_B \circ f)(A)) = M$ nos resulta el siguiente diagrama conmutativo

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[rr, "f"] \arrow[dd, "h"] & & B \arrow[r, "g"] \arrow[dl, "i_B"'] \arrow[dd, "\beta"] & C \arrow[r] & 0 \\
& & Q \times B \arrow[dr, "\pi"] & & & \\
0 \arrow[r] & Q \arrow[ur, "i_Q"] \arrow[rr, "\gamma"] & & M \arrow[r, "\pi'"] & M/\gamma(Q) \arrow[r] & 0
\end{tikzcd}$$

y como por hipótesis Q es inyectivo entonces obtenemos que γ se escinde, por lo cual podemos obtener un R-morfismo $\alpha : Q \times B/((i_Q \circ h - i_B \circ f)(A)) \to Q$ tal que $\alpha \circ \gamma = Id_Q$. Ahora solo basta ver que $h = \alpha \circ \beta \circ f$, pero $\alpha \circ \beta \circ f = \alpha \circ \gamma \circ h = Id_Q \circ h = h$, gracias que $\beta \circ f = \gamma \circ h$ y que α es escisión de γ. Por lo tanto definiendo $\bar{h} = \alpha \circ \beta$ tenemos que el diagrama

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "h"] & B \arrow[r, "g"] \arrow[dl, "\bar{h}"] & C \arrow[r] & 0 \\ & Q & & & \end{tikzcd}$$ conmuta.

ii) $\Longrightarrow$ i) Tomamos la sucesión exacta $0 \longrightarrow Q \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ y el morfismo identidad $i : Q \to Q$ entonces por hipótesis existe una función $\bar{i} : B \to Q$ tal que el siguiente diagrama conmuta

$$\begin{tikzcd} 0 \arrow[r] & Q \arrow[r, "f"] \arrow[d, "i"] & B \arrow[r, "g"] \arrow[dl, "\bar{i}"] & C \arrow[r] & 0 \\ & Q & & & \end{tikzcd}$$

entonces con $\bar{i} : B \to Q$ la sucesión $0 \longrightarrow Q \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ se escinde, es decir $\bar{i} \circ f = Id_Q$, por lo que Q resulta inyectivo. □

Lema 4.3. *(lema de Baer)*

Sea R un anillo, son equivalentes para un R-módulo Q:

i) Q es inyectivo.

ii) Para todo ideal I de R y toda función $f : I \to Q$ existe una función $\bar{f} : R \to Q$ tal que el siguiente diagrama conmuta

$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r, "i"] \arrow[d, "f"] & R \arrow[dl, "\bar{f}"] \\ & Q & \end{tikzcd}$$

Demostración. Sean R un anillo y Q un R-módulo.

i) $\Longrightarrow$ ii) Es claro ya que todo ideal de R se puede ver como un R-módulo y sólo falta falta completar la sucesión con R/I y 0, entonces conseguimos la sucesión exacta $0 \longrightarrow I \xrightarrow{i} R \xrightarrow{\pi} R/f(I) \longrightarrow 0$, entonces por la proposición anterior, entonces para toda función $f : I \to Q$ existe una función $\bar{f} : R \to Q$ tal que el siguiente diagrama conmuta

$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r, "i"] \arrow[d, "f"] & R \arrow[r, "\pi"] \arrow[dl, "\bar{f}"] & R/f(I) \arrow[r] & 0 \\ & Q & & & \end{tikzcd}$$

ii) $\Longrightarrow$ i) Consideremos el siguiente diagrama
$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "i"] \arrow[d, "f"] & B \\ & Q & \end{tikzcd}$$
con i inyección. Consideremos $S = \{(D, f_D| \ A \leq D \leq B$ y f_D extiende a $f\}$, para S definimos el orden $(X, f_x) \leq (Y, f_y)$ si y sólo si $X \leq Y$ y $f_X = f_Y|_X$, este orden resulta ser un orden parcial. Sea $C = \{(D_i, f_{D_i})\}_{i \in I}$ una cadena de S. Consideramos $(D', f'_{D'})$, donde $D' = \cup_{i \in I} D_i$ y $f'_{D'} = \cup_{i \in I} f_{D_i}$. Por construcción

$(D', f'_{D'})$ es cota superior de C, por lo cual a S se le puede aplicar el lema de Zorn, entonces existe (M, g) un elemento máximo en S. Sólo falta mostrar que $M = B$. Supongamos que no, entonces podemos encontrar un $x \in B \backslash M$ y podemos considerar $T = \{r \in R | \ xr \in M\}$, el cual es un ideal de R. Definamos $\alpha : T \to Q$ tal que $a(r) = g(rx)$ entonces por hipótesis existe $\bar{g} : B \to Q$ tal que el diagrama

$$\begin{tikzcd} 0 \arrow[r] & T \arrow[r, "i"] \arrow[d, "\alpha"] & B \arrow[dl, "\bar{\alpha}"] \\ & Q & \end{tikzcd}$$

conmuta. Ahora definamos $\bar{g} : M + xR \to Q$ dado por $\bar{g}(y + xr) = g(y) + \alpha(r)$ donde $y \in M$ y $r \in R$, observamos que claramente $g < \bar{g}$ (con el orden antes dado), pero esto es una contradicción con la condición máxima de g, por lo tanto $M = B$ y se obtiene que a $\bar{f} = g$ que hace que el diagrama

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "i"] \arrow[d, "f"] & B \arrow[dl, "\bar{f}"] \\ & Q & \end{tikzcd}$$

conmute, por lo tanto Q es inyectivo. □

Proposición 4.9. *Sean R un anillo y Q_1 y Q_2 R-módulos. Entonces Q_1 y Q_2 son inyectivos si y sólo si $Q_1 \bigoplus Q_2$ es inyectivo.*

Demostración. Sean R un anillo. Tomemos Q_1 y Q_2 dos R-módulos inyectivos. Sea

$0 \longrightarrow Q_1 \bigoplus Q_2 \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ una sucesión exacta. Ahora consideremos los R-morfismos $f|_{Q_1} : Q_1 \to B$ y $f|_{Q_2} : Q_2 \to B$ con los cuales podemos construir las sucesiones exactas:

$0 \longrightarrow Q_1 \xrightarrow{f|_{Q_1}} B \xrightarrow{g_1} C_1 \longrightarrow 0$ y

$0 \longrightarrow Q_2 \xrightarrow{f|_{Q_2}} B \xrightarrow{g_2} C_2 \longrightarrow 0$, donde C_1 y C_2 (en particular podemos tomar los conúcleos) están definidas de tal manera que las sucesiones son exactas, además las tenemos que las sucesiones se escinden gracias a que Q_1 y Q_2 son inyectivos, sean entonces $\alpha_1 : B \to Q_1$ y $\alpha_2 : B \to Q_2$ las escisiones y definimos $\alpha : B \to Q_1 \bigoplus Q_2$ que es inducida justamente por α_1 y α_2, con lo cual obtenemos que la sucesión

$0 \longrightarrow Q_1 \bigoplus Q_2 \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ se escinde, por lo tanto $Q_1 \bigoplus Q_2$ es inyectivo.

Para el regreso sólo basta tomar cualquier sucesión exacta de la forma

$0 \longrightarrow Q_1 \bigoplus Q_2 \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ la cual, como $Q_1 \bigoplus Q_2$ es inyectivo, se escinde, es decir, existe $\alpha : B \to Q_1 \bigoplus Q_2$, sólo basta tomar las correstricciones a Q_1 y Q_2 para obtener las escisiones deseadas con lo cual obtenemos que Q_1 y Q_2 son inyectivos. □

Como corolario a esta proposición tenemos que toda suma directa finita de R-módulos es inyectiva si y sólo si cada sumando lo es.

Definición 4.8. Sean R un anillo y M un R-módulo, un submódulo A de M es llamado superfluo en M si $\forall N \leq M$ se tiene que: $A + N = M$ implica $N = M$. denotaremos que A es superfluo en M por $A \ll M$.

Nota.- Decimos que ideal I es superfluo en un anillo R si lo es en el sentido de submódulo.

Proposición 4.10. *Sean R un anillo y L, N, M tres submódulos tales que $L \leq N$ y $N \ll M$, entonces $L \ll M$.*

Demostración. Sean R un anillo y L, N, M tres submódulos tales que $L \leq N$ y $N \ll M$, sea $U \leq M$ un submódulo de M tal que $L + U = M$, ahora como $L \leq N$, tenemos que $L + U \leq N + U$, y como tenemos que $N \ll M$, concluimos que $U = M$, por lo tanto $L \ll M$. □

En otras palabras los submódulos de submódulos superfluos son superfluos.

Definición 4.9. Sea R un anillo y M un R-módulo, un submódulo E de M es llamado esencial en M si $\forall N \leq M$ se tiene que: $E \cap N = 0$ implica $N = 0$. denotaremos que E es esencial en M por $E \leq_{es} M$. Además en estas condiciones diremos que M es extensión esencial de E.

Nota.- Decimos que ideal I es esencial en un anillo R si lo es en el sentido de submódulo.

Definición 4.10. Sea R un anillo y $\alpha : N \to M$ un R-morfismo de módulos, entonces decimos que α es esencial si $Im(\alpha) \leq_{es} M$.

Observación 4.6. Sea R un anillo y M un R-módulo, un submódulo E de M, entonces$E \leq_{es} M$ si y sólo si $\forall N \leq M$, $N \neq 0$ implica $(E \cap N) \neq 0$.

Ejemplo 4.6. $2\mathbb{Z}$es un módulo esencial en $\mathbb{Z}$ ya que $0 \neq 2n \in 2\mathbb{Z} \cap \mathrm{n}\mathbb{Z}$. En general tenemos que $n\mathbb{Z}$ es un módulo esencial en $\mathbb{Z}$.

Proposición 4.11. *Sean R un anillo y L, N, M tres submódulos tales que $L \leq_{es} N$ y $N \leq_{es} M$, entonces $L \leq_{es} M$.*

Demostración. Sean R un anillo y L, N, M tres submódulos tales que $L \leq_{es} N$ y $N \leq_{es} M$, sea $U \neq 0$ un submódulo de M, entonces como $N \leq_{es} M$, tenemos que $(N \cap U) \neq 0$, ahora como $N \cap U$ es un submódulo de N no cero, como $L \leq_{es} N$, tenemos que $((L \cap N) \cap U) = (L \cap (N \cap U)) \neq 0$, lo cual implica que $(L \cap U) \neq 0$, ya que $L \subseteq N$, por lo tanto $L \leq_{es} M$. □

En otras palabras la relación de ser submódulo esencial es transitiva.

Proposición 4.12. *Sean R un anillo, M un R-módulo y E_1, E_2 dos submódulos esenciales de M, entonces $E_1 \cap E_2 \leq_{es} M$.*

Demostración. Sean R un anillo, M un R-módulo y E_1, E_2 dos submódulos esenciales de M. De la definición de esencial concluimos que todo submódulo esencial de M es no cero, entonces $E_1 \cap E_2 \neq 0$ Tomemos N un submódulo de M tal que $(E_1 \cap E_2) \cap N = 0$, por asociatividad obtenemos que $E_1 \cap (E_2 \cap N) = 0$, como E_1es esencial concluimos que $(E_2 \cap N) = 0$ y como E_2 es esencial concluimos que $N = 0$. Por lo tanto $E_1 \cap E_2 \leq_{es} M$. $\square$

Como corolario a esta proposición obtenemos que la intersección finita de submódulos esenciales es esencial.

Definición 4.11. Sea R un anillo y M un R-módulo. Un monomorfismo $\eta : M \to Q$ es llamado una cápsula inyectiva de M si y sólo si Q es inyectivo y η es un R-morfismo esencial. En algunos casos más adelante, si no hay posibilidad de confusión, diremos simplemente que Q es una cápsula de M sin mencionar a η. Ahora para la notación, denotaremos una cápsula inyectiva de M por $I(M)$.

Proposición 4.13. *Sea R un anillo, si los R-morfismos $\eta_i : M_i \to Q_i$ con son cápsulas inyectivas de M_i, con $i = 1, 2, ..., n$. Entonces $\bigoplus_{i=1}^n \eta_i : \bigoplus_{i=1}^n M_i \to \bigoplus_{i=1}^n Q_i$ es una cápsula inyectiva para $\bigoplus_{i=1}^n M_i$.*

Demostración. Sea R un anillo, supongamos que los R-morfismos $\eta_i : M_i \to Q_i$ con son cápsulas inyectivas de M_i, con $i = 1, 2, ..., n$. Consideremos entonces el R-morfismo $\bigoplus_{i=1}^n \eta_i : \bigoplus_{i=1}^n M_i \to \bigoplus_{i=1}^n Q_i$, primero como suma directa de inyectivos es inyectiva entonces $\bigoplus_{i=1}^n Q_i$ es inyectivo, además como $\bigoplus_{i=1}^n \eta_i$ es suma directa de R-morfismo inyectivos, el mismo $\bigoplus_{i=1}^n \eta_i$ resulta inyectivo, además $Im(\bigoplus_{i=1}^n \eta_i) \leq_{es} \bigoplus_{i=1}^n Q_i$. Por lo tanto $\bigoplus_{i=1}^n \eta_i : \bigoplus_{i=1}^n M_i \to \bigoplus_{i=1}^n Q_i$ es una cápsula inyectiva para $\bigoplus_{i=1}^n M_i$. $\square$

Capítulo 5

Artinianos y Neterianos

5.1. Artinianos, neterianos, zoclo y radical de Jacobson

Definición 5.1. Sean R un anillo y M un $R-módulo$ derecho. Se dice que M cumple con la condición de cadena ascendente en submódulos (CCA) si:

1) No hay cadenas ascendentes infinitas propias de submódulos, o equivalentemente

2) Para toda cadena ascendente de submódulos de M, $M_1 \leq M_2 \leq ... \leq M_k \leq M_{k+1} \leq ...$ existe un $k \in \mathbb{N}$ tal que la cadena se estaciona, es decir, $M_i = M_k \; \forall i \geq k$.

Definición 5.2. Sean R un anillo y M un $R-módulo$ derecho. Se dice que M cumple con la condición de cadena descendente en submódulos (CCD) si:

1) No hay cadenas descendentes infinitas propias de submódulos, o equivalentemente

2) Para toda cadena descendente de submódulos de M, $M_1 \geq M_2 \geq ... \geq M_k \geq M_{k+1} \geq ...$ existe un $k \in \mathbb{N}$ tal que la cadena se estaciona, es decir, $M_i = M_k \; \forall i \geq k$.

Definición 5.3. Sea R un anillo, un R-módulo M es neteriano si M cumple la condición de cadena ascendente en submódulos.

Nota: Se dice que un anillo R es neteriano, si es neteriano como módulo sobre sí mismo, es decir, cumple la condición de cadena ascendente en ideales.

Definición 5.4. Sea R un anillo, un R-módulo M es artiniano si M cumple la condición de cadena descendente en submódulos.

Nota: Se dice que un anillo R es artiniano, si es artiniano como módulo sobre el mismo, es decir, cumple la condición de cadena descendente en ideales.

Definición 5.5. Sean R un anillo y M un R-módulo derecho. Se dice que M cumple la condición máxima en submódulos si toda familia no vacía de submódulos de M tiene máximos.

Definición 5.6. Sean R un anillo y M un R-módulo derecho. Se dice que M cumple la condición mínima en submódulos si toda familia no vacía de submódulos de M tiene mínimos.

Ejemplo 5.1. Los módulos simples son artinianos y neterianos ya que al sólo tener dos submódulos cumplen trivialmente la condición de cadena ascendente y la condición de cadena descendente.

Proposición 5.1. *Sean R un anillo y M un R-módulo derecho. Las siguientes condiciones son equivalentes:*

i) M es neteriano;

ii) M tiene condición máxima en submódulos;

iii) Todo submódulo de M es finitamente generado.

Demostración. Sean R un anillo y M un R-módulo derecho.

i) $\Longrightarrow$ ii) Hagámoslo por contrapuesta. Supongamos que M no tiene condición máxima en submódulos. Sea $\{N_i\}_{i\in I} \neq \emptyset$ una familia de submódulos de M sin máximos, tomemos un N_{i_1}, como no es máximo, debe existir un N_{i_2} tal que $N_{i_1} \subsetneqq N_{i_2}$, como N_{i_2} tampoco es máximo, existe N_{i_3} tal que $N_{i_1} \subsetneqq N_{i_2} \subsetneqq N_{i_3}$ y siguiendo de esta manera podemos construir una cadena ascendente infinita de la forma $N_{i_1} \subsetneqq N_{i_2} \subsetneqq N_{i_3} \subsetneqq ...$, es decir, M no es neteriano.

ii) $\Longrightarrow$ i) Hagámoslo por contrapuesta. Supongamos que M no es neteriano. Tomemos una cadena ascendente infinita de submódulos de M de la forma $N_1 \subsetneqq N_2 \subsetneqq N_3 \subsetneqq ...$, entonces por construcción $\{N_i\}_{i\in\mathbb{N}}$ no tiene máximos, porque $\forall N_i \in \{N_i\}_{i\in\mathbb{N}}$ existe N_{i+1} tal que $N_i \subsetneqq N_{i+1}$, por lo tanto M no tiene condición máxima en submódulos.

i) $\Longrightarrow$ iii) Hagámoslo por contrapuesta. Si N es un R-módulo derecho de M que no es finitamente generado, entonces en particular $N \neq 0$, entonces también debe existir un $0 \neq x_1 \in N$ tal que $gen(x) \subsetneqq N$, por consiguiente debe existir $0 \neq x_2 \in N$ tal que $gen(x_1) \subsetneqq gen(x_1, x_2) \subsetneqq N$, continuando de esta manera debe existir una sucesión $x_1, x_2, ..., x_n, ...$ tal que podemos construir una cadena de la forma $gen(x_1) \subsetneqq gen(x_1, x_2) \subsetneqq gen(x_1, x_2, x_3) \subsetneqq ...$, es decir, una cadena ascendente de submódulos de N y por lo tanto de M que no se estaciona, por lo tanto M no es neteriano.

iii) $\Longrightarrow$ i) Sea $N_1 \subsetneqq N_2 \subsetneqq N_3 \subsetneqq ...$ una cadena ascendente de R-submódulos derechos de M, entonces $\cup_{i\in I} N_i$ es un R-submódulo derecho de M, justo por estar en cadena. Por hipótesis existe $\{x_1, x_2, ..., x_n\}$ tal que $gen(x_1, x_2, ..., x_n) = \cup_{i\in I} N_i$ con $x_i \in N_{j_i}$, de esta manera $gen(x_1, x_2, ..., x_n) \subseteq \cup_{i=1}^{n} N_{j_i} = N_l$ para algún $l \in \mathbb{N}$. Con ello tenemos que la cadena $N_1 \subsetneqq N_2 \subsetneqq N_3 \subsetneqq ...$ se estaciona, por lo tanto toda cadena ascendente de R-submódulos derechos de M se estaciona, es decir, M es neteriano. $\square$

Proposición 5.2. *La clase de los R-módulos finitamente generados es cerrada bajo cocientes (epimorfismos) y bajo extensiones, es decir si tenemos un sucesión exacta*

$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *con A y C finitamente generados, entonces B es finitamente generado.*

Demostración. Sean R un anillo y M un R módulo finitamente generado. Sea $\pi : M \to N$ un epimorfismo. Como M es finitamente generado entonces existe un epimorfismo $f : R^n \to M$, ahora consideremos la composición $\pi \circ f : R^n \to N$, la cual es un epimorfismo, por lo tanto N resulta ser finitamente generado.

Ahora supongamos que $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ con A y C finitamente generados, entonces tenemos que existen dos epimorfismo $\alpha : R^n \to A$ y $\gamma : R^m \to C$, entonces podemos construir la siguiente sucesión exacta $0 \longrightarrow R^n \xrightarrow{f} R^n \bigoplus R^m \xrightarrow{g} R^m \longrightarrow 0$, la cual se escinde ya que R^m es proyectivo, entonces existe $\gamma' : R^m \to B$ por la Proposición 4.6, además tal que

$$\begin{tikzcd} & & & R^m \arrow[dl, "\gamma'"'] \arrow[d, "\gamma"] & \\ 0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[r] & 0 \end{tikzcd}$$

conmuta.

Entonces $f \circ \alpha \bigoplus \gamma' : R^n \bigoplus R^m \to B$ es un morfismo tal que

$$\begin{tikzcd} 0 \arrow[r] & R^n \arrow[r] \arrow[d, "\alpha"] & R^n \bigoplus R^m \arrow[r] \arrow[d, "f\circ\alpha \bigoplus \gamma'"] & R^m \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[r] & 0 \end{tikzcd}$$

conmuta y como α y γ son epimorfismo entonces$f \circ \alpha \bigoplus \gamma'$ es epimorfismo gracias al lema de los cinco, por lo tanto B es finitamente generado. □

Proposición 5.3. *La clase de los R-módulos finitamente cogenerados es cerrada bajo submódulos.*

Demostración. Sean R un anillo, M un R-módulo finitamente cogenerado y N un submódulo de M. Consideremos una familia $\{L_i\}_{i\in I}$ de submódulos de N tal que $\cap_{i\in I} L_i = 0$. Como la relación de ser submódulo es transitiva, obtenemos que $\{L_i\}_{i\in I}$ es una familia de submódulos de M que cumple que $\cap_{i\in I} L_i = 0$, entonces como M es finitamente cogenerado existe un $F \subseteq I$ finito tal que $\cap_{i\in F} L_i = 0$, por lo cual N es finitamente cogenerado. □

Proposición 5.4. *Sean R un anillo y M un R-módulo derecho. Las siguientes condiciones son equivalentes:*

i) M es artiniano;

ii) M tiene condición mínima en submódulos.

Demostración. Sean R un anillo y M un R-módulo derecho.

i) $\Longrightarrow$ ii) Hagámoslo por contrapuesta. Supongamos que M no tiene condición mínima en submódulos. Sea $\{N_i\}_{i\in I} \neq \emptyset$ una familia de submódulos de

M sin mínimos, tomemos un N_{i_1}, ahora como no es mínimo, debe existir un N_{i_2} tal que $N_{i_1} \gneqq N_{i_2}$, ahora como N_{i_2} tampoco es mínimo, existe N_{i_3} tal que $N_{i_1} \gneqq N_{i_2} \gneqq N_{i_3}$ y siguiendo de esta manera podemos construir una cadena descendente infinita de la forma $N_{i_1} \gneqq N_{i_2} \gneqq N_{i_3} \gneqq ...$, es decir, M no es artiniano.

ii) $\Longrightarrow$ i) Hagámoslo por contrapuesta. Supongamos que M no es artiniano. Tomemos una cadena descendente infinita de submódulos de M de la forma $N_1 \gneqq N_2 \gneqq N_3 \gneqq ...$, entonces por construcción $\{N_i\}_{i\in\mathbb{N}}$ no tiene mínimos, porque $\forall N_i \in \{N_i\}_{i\in\mathbb{N}}$ existe N_{i+1} tal que $N_i \gneqq N_{i+1}$, por lo tanto M no tiene condición mínima en submódulos. □

Proposición 5.5. *La clase de los R-módulos artinianos es cerrada bajo submódulos y bajo cocientes, es decir, si M es un R-módulo artiniano, entonces todo submódulo y todo cociente suyo es artiniano.*

Demostración. Sean R un anillo y M un R-módulo artiniano

i) Sea N un submódulo de M, entonces si tomamos una cadena descendente $N_1 \geq N_2 \geq ...$ de submódulos de N, al ser $N \leq M$, entonces también la cadena $N_1 \geq N_2 \geq ...$ es una cadena descendente de submódulos de M, por lo cual se estaciona, ya que M es artiniano, con esto concluimos que toda cadena descendente de submódulos de N se estaciona, es decir, N es artiniano.

Por lo tanto submódulos de R-módulos artinianos son artinianos.

ii) Sea N un R-módulo tal que $f : M \to N$ es un epimorfismo de R-módulos, ahora como f es suprayectivo, por el teorema de la correspondencia para R-módulos, tenemos que hay una correspondencia biyectiva entre $[Nuc(f), M]$ y $[0, N]$ y como $[Nuc(f), M]$ tiene condición mínima en submódulos, por ser M artiniano, entonces $[0, N]$ tiene condición mínima en submódulos, por lo que N es artiniano.

Por lo tanto cocientes de R-módulos artinianos son artinianos. □

Definición 5.7. Sean R un anillo y M un R-módulo, definimos el zoclo de M como la suma de los submódulos mínimos (simples) de M. Denotaremos al zoclo de M por $zoc(M)$.

Proposición 5.6. *Sean R un anillo y M un R-módulo, entonces $zoc(M) = \cap\{L \leq M |\ L \leq_{es} M\}$*

Demostración. Sean R un anillo, M un R-módulo y S un submódulo simple de M. Si tomamos ahora $L \leq_{es} M$, como $S \neq 0$, entonces $S \cap L \neq 0$, y como S es simple concluimos que $S \leq L$, es decir, todo simple de M está contenido en todo submódulo esencial de M, por lo tanto la suma de todos los simples de M está contenido en la intersección de todos los submódulos esenciales de M, es decir, $zoc(M) \subseteq \cap\{L \leq M |\ L \leq_{es} M\}$.

Consideremos ahora $Z = \cap\{L \leq M |\ L \leq_{es} M\}$ y mostremos que Z es semisimple. Tomemos N un submódulo de M y N' su seudocomplemento, entonces $N + N' = N \bigoplus N'$, además $N \bigoplus N' \leq_{es} M$, ya que si existiera $0 \neq L \leq M$ tal que $N \bigoplus N' \cap L = 0$ implicaría que $N \cap (N' + L) = 0$, contradiciendo el hecho de que N' es máximo con esa propiedad. Entonces tenemos que $Z \subseteq N \bigoplus N'$, entonces $Z = Z \cap (N \bigoplus N') = N \bigoplus (Z \cap N')$, es decir, N es un sumando directo de Z. Por lo tanto Z es semisimple como queríamos. Concluimos entonces que $Z \subseteq zoc(M)$. Por lo tanto $zoc(M) = \cap\{L \leq M |\ L \leq_{es} M\}$. $\square$

Proposición 5.7. *Son equivalentes para un R-módulo semisimple M:*

i) $M = \bigoplus_{i=1}^{n} S_i$ con S_i simple $\forall i \in \{1, 2, ..., n\}$ (es decir M es una suma finita de simples)

ii) M es finitamente generado

iii) M es neteriano

iv) M es artiniano

v) M es finitamente cogenerado

Demostración. Sean R un anillo y $M = \bigoplus_{i \in I} S_i$ un R-módulo semisimple.

iv) $\Longrightarrow$ v) Supongamos que M es artiniano, y tomemos una familia $\{N_i\}_{i \in I}$ de submódulos de M tal que $\cap_{i \in I} N_i = 0$. Consideremos $S = \{\cap_{i \in J} N_i |\ J \subseteq I$, con J finito$\}$ y $F \subseteq I$ tal que $\cap_{i \in F} N_i$ es mínimo en S, el cual existe ya que M es artiniano por hipótesis y por lo tanto cumple la condición mínima en submódulos. Tomemos un $j \in I \backslash F$ entonces $N_j \cap (\cap_{i \in F} N_i)$ es un submódulo de $\cap_{i \in F} N_i$, este submódulo no puede ser propio en $\cap_{i \in F} N_i$, ya que si lo fuera nos daría una contradicción con la minimidad que tiene $\cap_{i \in F} N_i$ en S, concluimos entonces que $N_j \cap (\cap_{i \in F} N_i) = \cap_{i \in F} N_i$, por lo tanto $\cap_{i \in F} N_i = \cap_{i \in I} N_i = 0$, es decir, M es finitamente cogenerado.

v) $\Longrightarrow$ ii) Supongamos que M es finitamente cogenerado, sabemos que $M = \bigoplus_{i \in I} S_i$ es un submódulo de $\prod_{i \in I} S_i$ por definición. Ahora como M es finitamente cogenerado, existe un $F \subseteq I$ finito tal que hay un monomorfismo $f : M \to \prod_{i \in F} S_i = \bigoplus_{i \in F} S_i$. Entonces tenemos que M es sumando directo de $\bigoplus_{i \in F} S_i$, con lo cual obtenemos un epimorfismo hacia M desde una suma finita, por lo cual M es finitamente generado.

ii) $\Longrightarrow$ i) Supongamos que M es finitamente generado y como $M = \bigoplus_{i \in I} S_i$, entonces podemos tomar el epimorfismo (isomorfismo) $Id_M : \bigoplus_{i \in I} S_i \to M$. Ahora como M es finitamente generado, debe existir un $F \subseteq I$ finito tal que $Id_M : \bigoplus_{i \in F} S_i \to M$ es un epimorfismo, que por construcción es además inyectivo, por lo tanto $\bigoplus_{i \in F} S_i \cong M$, es decir, M es es una suma finita de simples.

i) $\Longrightarrow$ iv) Supongamos que M es una suma finita de simples, es decir, $M = \bigoplus_{i=1}^{n} S_i$ con S_i simple $\forall i \in \{1, 2, ..., n\}$, ahora como M es semisimple entonces todo submódulo de M es una suma de simples. Del Teorema de Wedderburn-Artin obtenemos que el número de sumandos en la descomposición de un semisimple es un invariante, por hipótesis M es una suma finita de simples, entonces todo submódulo de M también es una suma finita de simples, que tendrá n o menos sumandos simples en su descomposición. Por lo cual si tomamos una cadena descendente propia de submódulos $N_1 \gneqq N_2 \gneqq ...$, a lo más en un número finito de pasos llegaremos a 0, ya que el número de sumandos en las descomposiciones de los submódulos N_i de M será cada vez menor, y como M tiene sólo n sumandos simples que perder, pues entonces en algún paso $m \in \mathbb{N}$ la cadena llegara a 0, es decir, no hay cadenas descendentes propias en M, por lo tanto M es artiniano.

iv) $\implies$ i) Supongamos que M es artiniano, tomemos la cadena descendente propia $M = \bigoplus_{i\in I} S_i \gneqq \bigoplus_{i\in I\setminus\{i_1\}} S_i \gneqq \bigoplus_{i\in I\setminus\{i_1,i_2\}} S_i \gneqq ...$, esta cadena llega a 0 en un número finito de pasos, ya que como M es artiniano no puede haber cadenas descendentes propias infinitas, con lo cual concluimos que $M = \bigoplus_{j=1}^{n} S_{i_j}$, es decir, M es una suma finita de simples.

i) $\implies$ iii) Supongamos que M es una suma finita de simples, es decir, $M = \bigoplus_{i=1}^{n} S_i$ con S_i simple $\forall i \in \{1,2,...,n\}$, como M es semisimple entonces todo submódulo de M es una suma de simples, y como por hipótesis M es una suma finita de simples, entonces todo submódulo de M también es una suma finita de simples, esto es gracias como ya habíamos mencionado antes al Teorema de Wedderburn-Artin. Por lo cual si tomamos una cadena ascendente propia de submódulos $0 = N_1 \lneqq N_2 \lneqq ...$, a lo más en un número finito de pasos llegaremos a M, ya que el número de sumandos en las descomposiciones de los submódulos N_i de M será cada vez mayor y en algún momento alcanzarán al mismo M, entonces a lo más en un número finito de pasos la cadena llegara a M, es decir, no hay cadenas ascendentes propias en M, por lo tanto M es neteriano.

iv) $\implies$ i) Supongamos que M es neteriano, tomemos la cadena ascendente propia $0 = S_{i_1} \lneqq \bigoplus_{j=1}^{2} S_{i_j} \lneqq \bigoplus_{j=1}^{3} S_{i_j} \lneqq ...$, esta cadena llega a M en un número finito de pasos, ya que como M es neteriano no puede haber cadenas ascendentes propias infinitas, con lo cual concluimos que $M = \bigoplus_{j=1}^{n} S_{i_j}$, es decir, M es una suma finita de simples. □

Proposición 5.8. *Sean R un anillo y M un R-módulo, entonces M es finitamente cogenerado si y sólo si $zoc(M)$ es finitamente generado y es esencial en M.*

Demostración. Sean R un anillo y M un R-módulo.

Supongamos que M es finitamente cogenerado, como los módulos finitamente cogenerados son cerrados bajo submódulos, obtenemos que $zoc(M)$ es finitamente cogenerado y como $zoc(M)$ es semisimple por definición, entonces por la Proposición 5.7, $zoc(M)$ es finitamente generado. Ahora tomemos $K \leq M$ tal que $K \cap zoc(M) = 0$, pero como $zoc(M)$ es la intersección de todos los submódulos esenciales de M, puesto que M es finitamente cogenerado existe una familia finita $\{L_1, L_2..., L_n\}$ de submódulos esenciales de M tal que $(L_1 \cap L_2... \cap L_n) \cap K = 0$ y como $(L_1 \cap L_2... \cap L_n) \leq_{es} M$, entonces $K = 0$, lo que nos da que $zoc(M) \leq_{es} M$.

Ahora supongamos que $zoc(M)$ es finitamente generado y es esencial en M. Consideremos $\{N_i\}_{i\in I}$ una familia de submódulos de M tal que $\cap_{i\in I} N_i = 0$, entonces $\cap_{i\in I}\{(N_i \cap zoc(M)\} = 0$, y como $zoc(M)$ es finitamente cogenerado por ser semisimple y finitamente generado, concluimos que existe un $F \subseteq I$ tal que $\cap_{i\in F}\{(N_i \cap zoc(M)\} = 0$, es decir, $(\cap_{i\in F} N_i) \cap zoc(M) = 0$ y como $zoc(M) \leq_{es} M$, entonces $\cap_{i\in F} N_i = 0$, por lo tanto M resulta finitamente cogenerado. □

Proposición 5.9. *Sean R un anillo y M un R-módulo, entonces M es artiniano si y sólo si para todo epimorfismo de módulos $f : M \to N$, N es finitamente* *cogenerado. Es decir, M es artiniano si sus cocientes son finitamente cogenerados.*

Demostración. Sean R un anillo y M un R-módulo.

Supongamos que M es artiniano. Como la clase de los R-módulo artinianos es cerrado bajo cocientes, basta mostrar que todo artiniano es finitamente cogenerado. Consideremos el zoclo de M, entonces, por definición, es semisimple y además como es submódulo de M, obtenemos que el zoclo además es artiniano, ya que los artinianos son cerrados bajo submódulos. Por lo tanto $zoc(M)$ es semisimple artiniano, por lo que es finitamente generado.

Mostremos ahora que $zoc(M)$ es esencial en M, supongamos que no lo es, es decir, existe un submódulo U de M tal que $U \neq 0$ y $zoc(M) \cap U = 0$. Ahora como U también es un submódulo de un artiniano, resulta que U es artiniano. Por lo que U tiene condición mínima en submódulos. Por lo que debe existir un R-submódulo T de U tal que $T \neq 0$ y T mínimo. Así que para todo $0 \neq x \in T$ se tiene que $0 \neq xR$, es un submódulo de T. Como T es mínimo, obtenemos que $T = xR$, con lo cual concluimos que T es simple, con lo que $0 \neq T \subseteq zoc(M)$, lo que es una contradicción ya que Tes submódulo de U y teníamos que $zoc(M) \cap U = 0$. Concluimos que $zoc(M)$ es esencial en M. Juntando las cosas tenemos que $zoc(M)$ es finitamente generado y es submódulo esencial de M y por lo tanto M es finitamente cogenerado. Para terminar, si N es cociente de M artiniano, entonces N es artiniano y por lo que acabamos de ver, además es finitamente cogenerado.

Ahora para el regreso supongamos que tenemos que todo cociente de M es finitamente cogenerado, tomemos una cadena descendente de módulos $N_0 > N_1 > N_2 > ...$ y llamemos $L = \cap_{i \in \mathbb{I}} N_i$, ahora como M/L es finitamente cogenerado y $\cap_{i \in I}(N_i/L) = 0$, entonces existe un subconjunto finito $F \subset I$ tal que $\cap_{i \in F}(N_i/L) = 0$, entonces $\cap_{i \in I} N_i = L = \cap_{i \in F} N_i$, entonces como $\{N_i\}_{i \in I}$ resulta ser finita, la cadena descendente se estaciona, por lo tanto M es artiniano. □

Proposición 5.10. *La clase de los R-módulos finitamente cogenerados es cerrada bajo extensiones, es decir si tenemos un sucesión exacta*

$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *con A y C finitamente cogenerados, entonces B es finitamente cogenerado.*

Demostración. Sean R un anillo y $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ una sucesión exacta con A y C finitamente cogenerados, podemos pensar que f es una inclusión ya que todo morfismo inyectivo induce un isomorfismo al correstringirlo a la imagen. Entonces por la Proposición 5.8, tenemos que $zoc(A) \leq_{es} A$ y $zoc(C) \leq_{es} C$ además de ser finitamente generados. Consideremos $zoc(B)$, entonces podemos obtener el siguiente diagrama conmutativo

$$\begin{tikzcd}
0 \arrow[r] \arrow[dd] & zoc(A) \arrow[r] \arrow[dd] & zoc(B) \arrow[r] \arrow[dd] & g(zoc(B)) \arrow[r] \arrow[d] & 0 \\
 & & & zoc(C) \arrow[d] & \\
0 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[r] & 0
\end{tikzcd}$$ ya que como $A \leq B$

entonces $zoc(A) \leq zoc(B)$ y $g(zoc(B)) \leq zoc(C)$, y además $g(zoc(B))$ es finitamente cogenerado por ser submódulo de un finitamente cogenerado, además es semisimple y por lo tanto resulta ser finitamente generado y como los finitamente generados son cerrados bajo extensiones entonces $zoc(B)$ es finitamente bajo extensiones.

Ahora supongamos que $zoc(B)$ no es esencial en B, entonces existe $0 \neq N \leq B$ tal que $zoc(B) \cap N = 0$, como $zoc(B)$ es la suma de los simples de B, entonces $zoc(B) \cap B = zoc(N)$, por lo cual $zoc(N) = 0$, lo cual implica que $A \cap N = 0$, ya que $zoc(A) \leq_{es} A$ y $zoc(N) = 0$. Ahora considerando la restricción de g a N, $g|_N : N \to C$ es monomorfismo ya que $0 = A \cap N = Im(f) \cap N = Nuc(g) \cap N$ por la exactitud de la sucesión, de lo anterior concluimos que $g(N) \cong N$ y como $zoc(C) \leq_{es} C$ entonces $zoc(g(N)) \neq 0$, por lo que $zoc(N) \neq 0$, lo cual es una contradicción, por lo tanto $zoc(B) \leq_{es} B$, por lo tanto B es finitamente cogenerado. □

Proposición 5.11. *La clase de los R-módulos artinianos es cerrada bajo extensiones, es decir si tenemos una sucesión exacta*

$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *con A y C artinianos, entonces B es artiniano.*

Demostración. Sean R un anillo y $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ una sucesión exacta con A y C artinianos, consideremos $\beta : B \to D$ un epimorfismo y el siguiente diagrama conmutativo con renglones exactos

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & D \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & (\beta \circ f)(A) \arrow[r, "f'"] & D \arrow[r, "g'"] & D/(\beta \circ f)(A) \arrow[r] & 0
\end{tikzcd}$$

Ahora como A y C son artinianos, tenemos que $(\beta \circ f)(A)$ y $D/(\beta \circ f)(A)$ son finitamente cogenerados y dado que la clase de los módulos finitamente cogenerados son cerrados bajo extensiones entonces D es finitamente cogenerado, por lo tanto B es artiniano.

Por lo tanto la clase de los R-módulos artinianos es cerrada bajo extensiones. □

Definición 5.8. Sean R un anillo y M un R-módulo, definimos el radical de Jacobson de M como la intersección de los submódulos máximos de M. Denotaremos al radical de Jacobson por $J(M)$.

Notemos que el radical de Jacobson de un anillo es la intersección de sus ideales máximos.

Proposición 5.12. *Sea R un anillo e I un ideal de R, entonces $J(R/I) = 0$ si y sólo si I es intersección de ideales máximos de R.*

Demostración. Sea R un anillo e I un ideal de R.

Supongamos que $J(R/I) = 0$, Consideremos el epimorfismo natural $\pi : R \to R/I$, entonces por el Teorema de la correspondencia, hay una correspondencia biyectiva entre los ideales de R que contienen a I y los ideales de R/I, entonces como $J(R/I) = 0$, por definición tenemos que $\cap_{i\in I} M'_i = 0$ donde $\{M'_i\}_{i\in I}$ es el conjunto de ideales máximos de R/I, pero por el Teorema de la correspondencia $0 = \cap_{i\in I} M'_i = \cap_{i\in I}(M_i/I) = (\cap_{i\in I} M_i)/I$ donde $\{M_i\}_{i\in I}$ son los ideales máximos de R que contienen a I, al final nos resulta que $0 = (\cap_{i\in I} M_i)/I$, pero esto quiere decir que $I = \cap_{i\in I} M_i$. Por lo tanto I es intersección de ideales máximos de R.

Ahora supongamos que I es intersección de ideales máximos de R, es decir $I = \cap_{i\in I} M_i$ donde $\{M_i\}_{i\in I}$ es un conjunto de ideales máximos de R. Consideremos R/I y el epimorfismo natural $\pi : R \to R/I$, entonces por el Teorema de la correspondencia, hay una correspondencia biyectiva entre los ideales de R que contienen a I y los ideales de R/I. Por un lado $0 = \pi(I) = \pi(\cap_{i\in I} M_i)$, es decir $0 = (\cap_{i\in I} M_i)/I = \cap_{i\in I} M_i/I$, ya que por hipótesis los M_i contienen a I, de lo anterior concluimos que hay una intersección de máximos de R/I igual a cero, por lo que $J(R/I) \subseteq \cap_{i\in I} M_i/I = 0$. Por lo tanto $J(R/I) = 0$. □

Corolario 5.1. *Sea R un anillo entonces $J(R/J(R)) = 0$*

Demostración. Sea R un anillo, como por definición $J(R)$ es una intersección de ideales derechos máximos de R, entonces por la proposición anterior tenemos que $J(R/J(R)) = 0$, como se quería, observando que todo ideal máximo contiene a $J(R)$. □

Proposición 5.13. *Sea R un anillo artiniano, entonces $J(R)$ es la intersección de un número finito de ideales máximos.*

Demostración. Sea R un anillo artiniano, ahora tomemos los ideales máximos de R para formar la siguiente cadena intersectándolos, $M_1 \cap M_2 \supseteq M_1 \cap M_2 \cap M_3 \supseteq ...$, con $M_i \neq M_j$ si $i \neq j$. Esta es claramente una cadena de ideales descendente y como R es artiniano entonces se estaciona, es decir, existe $n \in \mathbb{N}$ tal que $M_1 \cap M_2 \cap ... \cap M_n \cap M_{n+1} = M_1 \cap M_2 \cap ... \cap M_n$, tenemos por consecuencia que la intersección de todos los ideales máximos de R es igual a $M_1 \cap M_2 \cap ... \cap M_n$, es decir, $J(R) = M_1 \cap M_2 \cap ... \cap M_n$, por lo tanto $J(R)$ es la intersección de un número finito de ideales máximos. □

Proposición 5.14. *Sea R un anillo artiniano, entonces R es semisimple si y sólo si $J(R) = 0$*

Demostración. Sea R un anillo artiniano.

Supongamos que R es semisimple, entonces R es una suma directa de simples (que es finita por la Proposición 5.7), es decir, $R \cong \bigoplus_{i=1}^{n} M_i$ con M_i simple $\forall i \in \{1, ..., n\}$ para algún $n \in \mathbb{N}$, entonces todo

$N_i = M_1 \bigoplus M_2 \bigoplus ... \bigoplus M_{i-1} \bigoplus M_{i+1} \bigoplus ... \bigoplus M_n$ es máximo de R. Ahora por definición de radical de Jacobson tenemos que $J(R) \subseteq \cap_{i=1}^{n} N_i$, pero en cada máximo estamos quitando uno de los simples que componen a R, uno por uno hasta que los agotamos todos, concluimos que $\cap_{i=1}^{n} N_i = 0$, por lo que $J(R) = 0$.

Ahora para el regreso tenemos que por la Proposición anterior $J(R) = \cap_{i \in I}^{n} M_i$ con $\{M_i\}_{i=1}^{n}$ máximos, entonces

$R/J(R) \cong R/M_1 \bigoplus R/M_2 \bigoplus ... \bigoplus R/M_n$, y como para todo $i \in \{1, 2, ..., n\}$ R/M_i es simple, entonces $R/J(R)$ es semisimple, y como por hipótesis $J(R) = 0$, entonces R es semisimple. $\square$

Capítulo 6

Anillos Locales y Seriales

6.1. Anillos locales y semilocales

Este capitulo está basado en el capítulo 1 del libro Module Theory de Alberto Facchini, por lo cual se toman algunas demostraciones de él.

Observación 6.1. Sea R un anillo, entonces el conjunto de morfismos que van de R a R (endomorfismos) forman un anillo con las operaciones de suma y composición, y cuyos elementos neutros son, respectivamente, el morfismo cero y la identidad. A dicho anillo lo denotaremos como $End(R)$.

Asimismo los endomorfismos de un R-módulo M forman un anillo, de forma análoga a la del caso de los endomorfismos de anillos. A dicho anillo lo denotaremos como $End(M)$.

Teorema 6.1. *Teorema. Son equivalentes para un anillo R:*
(a) $R/J(R)$ es un anillo con división;
(b) R_R es un módulo local (R tiene un único ideal máximo);
(c) La suma de 2 elementos no invertibles es no invertible;
(d) $J(R)$ es un ideal máximo derecho;
(e) $J(R)$ es el conjunto de todos los elementos no invertibles de R

Demostración. Sea R un anillo

a) $\implies$ b) Supongamos que $R/J(R)$ es un anillo con división, esto implica que todos los elementos no invertibles de R están en $J(R)$, entonces por la observación 1.3 $\forall I \subset R$ se tiene que $I \subset J(R)$, entonces $J(R)$ es un ideal mayor, entonces es el único ideal máximo de R, por lo tanto R es un anillo local.

b) $\implies$ c) Supongamos que R es local, por demostrar la suma de 2 elementos no invertibles es no invertible. Consideremos A=$\{r \in R|\ r$ es no invertible$\}$, sea M el único ideal máximo de R, tenemos por otra parte que $\forall a \in A$, aR es un ideal de R y todo ideal está contenido en algún máximo entonces $\forall a \in A$ no invertible $a \in M$ y entonces $A = M$ y como M es ideal entonces A es cerrado bajo la suma.

c) $\Longrightarrow$ d) Supongamos que la suma de 2 no invertibles es no invertible, por demostrar $J(R)$ es un ideal máximo. Consideremos A=$\{r \in R|$ r es no invertible$\}$, por demostrar A es ideal. Por hipótesis suma de no invertibles es no invertible, por lo que sólo basta demostrar que A es cerrado bajo multiplicación por elementos de R. Sea $a \in A$ y $r \in R$, por demostrar $ar \in A$. Supongamos que $ar \notin A$ entonces $\exists s \in R$ tal que $ars = 1$ entonces $a(rs) = 1$, esto es una contradicción ya que $a \in A$ y por lo tanto no es invertible. por lo tanto A es cerrado bajo multiplicación por elementos de R. Por lo tanto A es un ideal y por la observación 1.3, A es un ideal mayor (en otras palabras el único ideal máximo de R), entonces $J(R) = A$ por definición de $J(R)$, por lo tanto $J(R)$ es un ideal máximo.

d) $\Longrightarrow$ e) Supongamos que $J(R)$ es un ideal máximo derecho, por demostrar $J(R)$ es el conjunto de todos los elementos no invertibles de R. Consideremos A=$\{r \in R|$ r es no invertible$\}$, por demostrar $A = J(R)$. Sabemos que$\forall a \in A$, aR es un ideal de R y todo ideal está contenido en algún máximo entonces $\forall a \in A$ no invertible $a \in J(R)$ entonces por la observación 1.3 $J(R) = A$.

e) $\Longrightarrow$a) Supongamos que $J(R)$ es el conjunto de todos los elementos no invertibles de R, por demostrar $R/J(R)$ es anillo con división. Dado que todo elemento no invertible de R está en $J(R)$ entonces todo elemento de $R/J(R)$ es invertible y por lo tanto $R/(R)$ es un anillo con división. $\square$

La siguiente proposición fue tomada del libro Module Theory de Alberto Facchini.

Proposición 6.1. *Si $e \in R$ es idempotente, entonces eRe es local si y sólo si el $R-$ módulo eR es local.*

Demostración. Supongamos que eRe es un anillo local, entonces $e \neq 0$. El ideal eR tiene un submódulo máximo N. Basta demostrar que N es superfluo en eR. Asumamos lo contrario, es decir, supongamos que $\exists K \subset eR$ tal que $K+N = eR$. Ahora haciendo cociente con N $eR/N = K + N/N \cong K/K \cap N$ (por segundo teorema de isomorfismo) entonces existe un isomorfismo $\phi : eR/N \to K/K \cap N$. Sea $\pi : eR \to eR/N$ y $\pi' : K \to K/K \cap N$ las proyecciones canónicas. El módulo eR es proyectivo. por lo tanto existe un morfismo $\psi : eR \to K$ tal que $\phi\pi = \pi'\psi$. Puesto que K es submódulo propio de eR, entonces ψ puede verse como un elemento no invertible del anillo local $End(eR) \cong eRe$, esto quieres decir que, ψ es multiplicar por la izquierda por un elemento de $J(eRe) = eJ(R)e$ (ya que $J(eRe)$ contiene a lo elementos no invertibles de eRe por localidad). Por lo tanto, $\exists r \in J(R)$ tal que $\psi(et) = eret$ $\forall t \in R$. Ahora $K/K \cap N = \phi\pi(eR) = \pi'\psi(eR) = ereR + K \cap N/K \cap N$, y $ereR \nsubseteq K \cap N$. Puesto que $ereR \subseteq K$, tenemos que $ereR \nsubseteq N$. Pero $ereR \subseteq eJ(R) = rad(eR) \subseteq N$, contradicción. Entonces $N \ll eR$ y por lo tanto eR es local.

Ahora supongamos que eR es un R-módulo con un submódulo máximo N. Por demostrar $eRe \cong End(eR)$es local, es suficiente probar que la suma de dos elementos no invertibles de $End(eR)$ es no invertible, para esto es suficiente mostrar que si $f \in End(eR)$, entonces f es no invertible si y sólo si $f(eR) \subseteq N$.Es claro que si $f(eR) \subseteq N$ entonces f es no invertible. Ahora, (contrapositiva) supongamos que $f(eR) \nsubseteq N$, entonces $f(eR) = eR$, entonces $f : eR \to eR$ es suprayectiva. Puesto que eR es proyectivo, $ker(f)$ es un sumando directo de eR. Pero todo módulo local es inescindible, y por lo tanto $f = 0$ o f es inyectiva. Si $f = 0$, entonces $eR = 0$ lo cual no es posible porque eR es local. Entonces f es inyectiva, y por lo tanto es un elemento invertible de $End(eR)$. Por lo tanto eRe es un anillo local □

Definición 6.1. Sea R un anillo, decimos que R es semilocal si $R/J(R)$ es un anillo semisimple.

Proposición 6.2. *Sea R un anillo, entonces son equivalentes:*
i) R es semilocal
ii) $R/J(R)$ es artiniano

Demostración. Sea R un anillo.

i) $\Longrightarrow$ ii) Supongamos que R es semilocal, entonces por definición $R/J(R)$ es semisimple y como $J(R/J(R)) = 0$, entonces $R/J(R)$ es artiniano.

ii) $\Longrightarrow$ i) Supongamos que $R/J(R)$ es artiniano. Si le sacamos el radical de Jacobson a $R/J(R)$, sabemos que $J(R/J(R)) = 0$, por lo que $R/J(R)$ resulta ser un anillo y artiniano tal que su radical es cero, por lo tanto $R/J(R)$ es semisimple, entonces por definición, R resulta ser semilocal. □

Proposición 6.3. *Todo anillo R local es semilocal.*

Demostración. Sea R un anillo local, entonces $R/J(R)$ es un anillo con división, por lo cual cumple la condición de cadena descendente trivialmente en ideales, ya que sólo tiene dos ideales, por lo tanto $R/J(R)$ es artiniano y por la Proposición 6.2 concluimos que R es semilocal. □

Ejemplo 6.1. Todo anillo artiniano es semilocal, ya que si tenemos que un anillo R es artiniano, entonces como los artinianos son cerrados bajo cocientes, obtendremos que $R/J(R)$ es artiniano y por lo tanto semilocal.

La siguiente proposición fue tomada del libro Module Theory de Alberto Facchini.

Proposición 6.4. *Si R es un anillo semilocal y e es un idempotente no cero de R, entonces eRe es un anillo semilocal.*

Demostración. Denotemos por $L(R/J(R))$ la retícula de todos los ideales derechos del anillo $R/J(R)$, y por $L(eRe/J(eRe))$ la retícula de todos los ideales derechos del anillo $eRe/J(eRe)$.

Para mostrar que la semilocalidad de R implica la semilocalidad de eRe, es suficiente mostrar que si $L(R/J(R))$ es un copo artiniano entonces

$L(eRe/J(eRe))$ es un copo artiniano, y para esto es suficiente probar que existe un morfismo inyectivo (monomorfismo) $L(eRe/J(eRe)) \to L(R/J(R))$. (preserva orden)

Por lo tanto la proposición será demostrada si mostramos que

$(IR + J(R)) \bigcap eRe = I \ \forall I \subset eRe$ ideal derecho, contiene a $J(eRe)$. Sea $\sum_k i_k r_k + j = ere$ un elemento de $(IR + J(R)) \cap eRe$, con $i_k \in I$, $r, r_k \in R$ y $j \in J(R)$. Entonces (multiplicando e por izquierda y por derecha) $ere = e(\sum_k i_k r_k + j)e = \sum_k e i_k e r_k e + eje \in IeRe + eJ(R)e \subseteq I$, y como$eJ(R)e = J(eRe)$, entonces $J(eRe) \subset I$ ya que $\forall I \subset eRe$ ideal derecho. Por lo tanto la semilocalidad de R implica la localidad de eRe. □

Definición 6.2. Un módulo M es de *longitud* finita si tiene una cadena de submódulos $0 = M_0 \subset M_1 \subset M_2 \subset ... \subset M_n = M$, que no tiene refinamiento. En este caso el entero n es llamado la *longitud* de M.

Proposición 6.5. *Un módulo M es de longitud finita si y sólo si es artiniano y neteriano.*

Demostración. Sea M un módulo

Supongamos que M es de es de *longitud* finita. Por demostrar que M es artiniano y neteriano. Como M es de longitud finita entonces toda cadena de submódulos de 0 a M es finita y por lo tanto estacionaria, tanto descendente, como ascendentemente. Por lo tanto M es artiniano y neteriano.

Supongamos que M es ariniano y neteriano, por demostrar que M es de longitud finita, construyamos una serie de composición de M empezando con $M = M_0$, como M es neteriano, entonces la familia $\{N | \ N \lneqq M\}$ tiene un elemento máximo $M_1 \lneqq M_0$, repitiendo el proceso obtenemos una cadena descendente $M = M_0 \gneqq M_1 \gneqq M_2 \gneqq ...$ y como M es artiniano entonces esta cadena descendente se estaciona, que existe $n \in \mathbb{N}$ tal que $M = M_0 \gneqq M_1 \gneqq M_2 \gneqq ... \gneqq M_n = M$. Por lo tanto M es de longitud finita. □

El siguiente lema está basado en el lema 1.14 del libro Module Theory de Alberto Facchini.

Lema 6.1. *Sean R un anillo semilocal y M R-módulo finitamente generado. Entonces:*

(a) $M/MJ(R)$ es un $R-$módulo semisimple de longitud finita.

(b) M es local si y sólo si $M/MJ(R)$ es simple.

(c) M es una suma directa de módulos inescindibles.

Demostración. Sean R un anillo semilocal y M R-módulo de longitud finita.

(a) Por demostrar $M/MJ(R)$ es un $R - módulo$ semisimple de longitud finita. Como R es semilocal entonces $R/J(R)$ es semisimple entonces $M/MJ(R)$ es semisimple y como M es finitamente generado entones $M/MJ(R)$ es suma de un número finito de simples, por lo tanto de longitud finita.

(b) Si M es local, $M/MJ(R)$ es un módulo local sobre el anillo $R/J(R)$ que es semisimple artiniano (ya que R es semilocal). Por lo tanto $M/MJ(R)$ es simple. Ahora, si $M/MJ(R)$ es simple, $MJ(R)$ es un submódulo máximo de M, entonces $MJ(R) \subseteq rad(M)$. Puesto que M es finitamente generado, $rad(M) \subsetneq M$, entonces $MJ(R) = rad(M)$ es el único ideal máximo de M y por lo tanto M es local.

(c) supongamos que no, entonces el conjunto de sumandos directos de M para los cuales (c) es falso es no vacío. Por lo tanto éste tiene un elemento N tal que el R-módulo $N/NJ(R)$ es de longitud mínima. Puesto que N no es una suma directa de módulos inescindibles, N mismo no es inescindible, entonces tenemos que $N = N' \bigoplus N''$, donde N' y N'' son R-módulos no cero finitamente generados. Entonces

$N/NJ(R) \cong (N'/N'J(R)) \bigoplus (N''/N''J(R))$ y los módulos semisimples

$N'/N'J(R)$ y $N''/N''J(R)$ tienen longitud no cero por el Lema de Nakayama, entonces N' y N'' son sumas directas de módulos inescindibles, por lo que N mismo resulta ser una suma directa de módulos inescindibles, lo cual es una contradicción. Por lo tanto M es una suma directa de módulos inescindibles. □

6.2. Anillos y módulos seriales

Definición 6.3. Un R-módulo M es llamado uniserial si para cualesquiera $A, B \subset M$ tenemos que $A \subseteq B$ o $B \subseteq A$. Por lo tanto un módulo M es uniserial si y sólo si la retícula $L(M)$ de submódulos está linealmente ordenada bajo la contención de conjuntos.

Observación 6.2. Todo submódulo y toda imagen de un módulo uniserial es uniserial.

Definición 6.4. Un módulo uniserial M es encogible si M es isomorfo a K/H para algunos submódulos $0 \subset H \subset K \subset M$. En caso contrario diremos que el módulo uniserial M es no encogible.

Ejemplo 6.2. Módulos uniseriales artinianos y módulos uniseriales neterianos son no encogibles.

De hecho, si M es un módulo uniserial artiniano, su retícula de submódulos $L(M)$ está bien bien ordenada bajo contención, es decir, su orden es isomorfo a un número ordinal α. Si M es encogible, entonces existe un ordinal β no cero tal que $\beta + \alpha + \gamma = \alpha$. Esto no es posible por la definición de suma en ordinales, por lo tanto M es no encogible.

Analogamente para los neterianos.

Ejemplo 6.3. Existen módulos uniseriales encogibles.

Sea $\mathbb{Z}$ (el conjunto de los enteros), p y q dos números primo distintos, consideramos $\mathbb{Z}_{(p)}$ y $\mathbb{Z}_{(q)}$, y $\mathbb{Q}$ el campo de los racionales. Donde $\mathbb{Z}_{(p)} = \{a/b |\ a \in \mathbb{Z},\ b \in \mathbb{Z}\ y\ p \nmid b\}$.

Consideremos el anillo

$R = \begin{pmatrix} \mathbb{Z}_{(p)} & 0 \\ \mathbb{Q} & \mathbb{Z}_{(q)} \end{pmatrix}$

y este ideal derecho

$H = \begin{pmatrix} \mathbb{Z}_{(p)} & 0 \\ \mathbb{Z}_{(p)} & 0 \end{pmatrix}$

Las operaciones en el anillo son las operaciones de suma y multiplicación de matrices ordinarias. Es fácil ver que los ideales de R que contienen a H son los ideales de la forma
$\begin{pmatrix} \mathbb{Z}_{(p)} & 0 \\ J & 0 \end{pmatrix}$ y $\begin{pmatrix} \mathbb{Z}_{(p)} & 0 \\ \mathbb{Q} & I \end{pmatrix}$
donde J es cualquier $\mathbb{Z}_{(p)}$-submódulo de $\mathbb{Q}$ que contiene a $\mathbb{Z}_{(p)}$ e I es cualquier ideal de $\mathbb{Z}_{(q)}$

Por lo tanto R/H es un R-módulo derecho uniserial.

Ahora mostraremos que R/H es encogible, consideremos el elemento $t = \begin{pmatrix} 1 & 0 \\ 0 & q/p \end{pmatrix} \in R$

y el endomorfismo $\varphi : R_R \to R_R$ dado por la multipliación por izquierda por t. Es fácil ver que $tH = \begin{pmatrix} \mathbb{Z}_{(p)} & 0 \\ p^{-1}\mathbb{Z}_{(p)} & 0 \end{pmatrix}$ y $tR = \begin{pmatrix} \mathbb{Z}_{(p)} & 0 \\ \mathbb{Q} & q\mathbb{Z}_{(q)} \end{pmatrix}$,

entonces tenemos que $H \subset tH \subset tR \subset R$. Puesto que $\varphi^{-1}(tH) = H$, φ induce un isomorfismo de R-módulos $R/H \to tR/tH$. Por lo tanto R/H es un R-módulo uniserial encogible.

El siguiente lema está basado en el lema 1.17 del libro Module Theory de Alberto Facchini.

Lema 6.2. *Todo módulo derecho uniserial encogible contiene un submódulo cíclico encogible.*

Demostración. Sea M un módulo derecho uniserial encogible sobre un anillo R, entonces por definición de encogible existen $0 \subset H \subset K \subset M$ submódulos de M tal que existe un isomorfismo $\varphi : M \to K/H$. Fijemos un elemento $x \in M$, tal que $x \notin K$ y supongamos que $\varphi(x) = y + H$, entonces φ induce un isomorfismo $\varphi' : xR \to yR/H$ y $H \subset yR \subset K \subset xR$. Por lo tanto xR es un R-módulo cíclico encogible, contenido en M ya que $x \in M$. □

La siguiente proposición fue tomada del libro Module Theory de Alberto Facchini.

Proposición 6.6. *Sea R un anillo que es conmutativo o neteriano derecho. Entonces todo R-módulo uniserial es no encogible.*

Demostración. Sea M un R-módulo derecho uniserial encogible, entonces por el lema anterior M contiene un submódulo cíclico encogible, llamémosle N.

Si R es neteriano derecho, entonces N es un módulo uniserial encogible derecho, lo cual es una contradicción con el *ejemplo 6.2.*

Si R es conmutativo, entonces $N \cong R/I$ para algún ideal $I \subset R$, y $R/I \cong xR/J$ para algunos ideales $I \subset J \subset xR \subset R$, porque$N$ es encogible. Sea $r \in J$ tal que $r \notin I$, entonces r anula xR/J, pero no anula a R/I. Esto es una contraticcción con el hecho de que $xR/J \cong R/I$. □

Definición 6.5. Diremos que un anillo R es un anillo cadena derecho si es un módulo uniserial como módulo dereho sobre si mismo.

Análogamente podemos definir lo que es un anillo cadena izquierdo.

Un anillo es un anillo cadena si es anillo cadena derecho e izquierdo. Un anillo valuación es un anillo cadena conmutativo, no necesariamente un dominio.

El siguiente lema fue tomado del libro Module Theory de Alberto Facchini.

Lema 6.3. *Sean R un anillo y $e \in R$ un elemento idempotente no cero. Si el módulo eR es uniserial, entonces el anillo eRe es un anillo cadena derecho.*

Demostración. Sean R un anillo y $e \in R$ un elemento idempotente no cero y $eaeRe$, $ebeRe$ dos ideales principales derechos del anillo eRe, $a, b \in R$. Es suficiente probar que $eaeRe \subseteq ebeRe$ o $ebeRe \subseteq eaeRe$. Si eR es un módulo uniserial entonces como $eaeRe$,$ebeRe \subset eR$ tenemos justamente que $eaeRe \subseteq ebeRe$ o $ebeRe \subseteq eaeRe$. Por lo tanto eR es un anillo cadena derecho. □

Definición 6.6. Un módulo serial es un módulo que es una suma directa de módulos uniseriales. Un anillo R es serial derecho (izquierdo) si es un módulo serial derecho (izquierdo) sobre sí mismo. Si es serial derecho e izquierdo entonces diremos que R es serial.

Ejemplo 6.4. Todo módulo simple es uniserial, entonces todo módulo semisimple es uniserial. Por lo tanto todo anillo artiniano semisimple es un anillo serial.

Recordemos que un elemento idempotente e de un anillo R es primitivo si es no cero y no puede ser escrito como la suma de dos idempotentes ortogonales no cero. Equivalentemente, e es primitivo si y sólo si el sumando directo de eR de $R_R$es inescindible, si y sólo si el sumando directo Re de ${}_RR$ es inescindible. También recordemos que conjunto de idempotentes ortogonales completo de R es un conjunto finito $\{e_1, e_2, ..., e_n\}$ de idempotentes de R tal que $e_ie_j = 0$ con $i \neq j$ y $e_1+e_2+...+e_n = 1$ (equivalentemente, tal que $R_R = e_1R \bigoplus e_2R \bigoplus ... \bigoplus e_nR$).

Observación 6.3. *Sea R un anillo derecho serial, puesto que $R_R$es serial, existe a un conjunto $\{e_1, e_2, ..., e_n\}$ de idempotentes ortogonales completo en R para los cuales e_iR es uniserial como R-módulo, de esto se sigue que $e_1, e_2, ..., e_n$ son idempotentes primitivos, por definición.*

Proposición 6.7. *Toda imagen homomorfa de un anillo serial derecho R es un anillo serial derecho.*

Demostración. Sea R un anillo serial derecho, entonces como observamos anteriormente, debe existir un conjunto de elementos idempotentes ortogonales completo, sea $\{e_1, e_2, ..., e_n\}$ dicho conjunto, entonces tenemos que

$R_R = e_1R \bigoplus e_2R \bigoplus ... \bigoplus e_nR$ donde cada e_iR es uniserial como R-módulo derecho. Ahora si tomamos un ideal bilateral I de R obtendremos que

$R/I \cong R_R = (e_1R/e_1I) \bigoplus (e_2R/e_2I) \bigoplus ... \bigoplus (e_nR/e_nI)$. Cada (e_iR/e_iI) es una imagen homomorfa del módulo uniserial derecho e_iR, por lo que el mismo (e_iR/e_iI) es uniserial, por lo tanto R/I es serial derecho y como para todo morfismo de anillos f se tiene que $R/Nuc(f) \cong \}Im(f)$ por el primer teorema de isomorfismos para anillos. Entonces por todo lo anterior tendremos que $f(R)$ es serial con f un morfismo de anillos. □

Ahora mostraremos un resultado que une la defininción de anillo serial con la de anillo semilocal, cuya demostración se basa en la escrita en el libro Module Theory de Alberto Facchini.

Proposición 6.8. *Todo anillo serial derecho es un anillo semilocal.*

Demostración. Sean R un anillo serial derecho y $\{e_1, e_2, ..., e_n\}$ un conjunto de elementos idempotentes ortogonales completo en R tal que

$R_R = e_1R \bigoplus e_2R \bigoplus ... \bigoplus e_nR$ donde cada e_iR es uniserial, entonces como $J(R)$ es un ideal bilateral de R tenemos que

$R/J(R) \cong (e_1R/e_1J(R)) \bigoplus (e_2R/e_2J(R)) \bigoplus ... \bigoplus (e_nR/e_nJ(R))$ donde cada $(e_iR/e_iJ(R))$ es un R-módulo derecho simple, por lo tanto $R/J(R)$ es un R-módulo semisimple de longitud finita, por lo tanto R es semilocal. $\square$

Capítulo 7

Krull-Schmidt-Remak y Goldie

7.1. Teorema de Krull-Schmidt-Remak

En esta sección, con la intención de probar el teorema de Krull-Schmidt-Remak primero se probará una serie de lemas con tal de hacer más sencilla la demostración.

Lema 7.1. *Sea R un anillo y $M = \bigoplus_{i\in I} M_i$ un R-módulo derecho tal que $End(M_i)$ es local $\forall i \in I$ y $\sigma, \tau \in End(M)$ con $Id_M = \sigma + \tau$. Entonces $\forall j \in I$ existe un $U_j \leq M$ y un isomorfismo $\varphi : M_j \to U_j$, el cual es inducido por σ o por τ (es decir $\varphi(x) = \sigma(x)$ $\forall x \in M_j$ o $\varphi(x) = \tau(x)$ $\forall x \in M_j$), entonces tenemos nosotros que $M = U_j \bigoplus(\bigoplus_{j\neq i\in I} M_i)$.*

Demostración. Sea R un anillo y $M = \bigoplus_{i\in I} M_i$ un R-módulo derecho tal que $End(M_i)$ es local $\forall i \in I$ y $\sigma, \tau \in End(M)$ con $Id_M = \sigma + \tau$. Consideremos las proyecciones $\pi_i : M \to M_i$ y las inyecciones $\iota_i : M_i \to M$ $\forall i \in I$. Ahora puesto que $Id_M = \sigma + \tau$ tenemos que, tomando las anteriores proyecciones e inyecciones, $Id_{M_i} = \pi_i Id_M \iota_i = \pi_i(\sigma + \tau)\iota_i = \pi_i\sigma\iota_i + \pi_i\tau\iota_i$. Anteriormente se probó, en el capítulo de anillos locales, que los elementos no invertibles de un anillo local forman un ideal propio, entonces como Id_M es un elemento invertible en $End(M_i)$ tenemos que $\pi_i\sigma\iota_i$ o $\pi_i\tau\iota_i$ es invertible, ya que de lo contrario el ideal de los no invertibles sería igual al anillo por lo de que $Id_{Mi} = \pi_i\sigma\iota_i + \pi_i\tau\iota_i$, en otras palabras tenemos que $\pi_i\sigma\iota_i$ o $\pi_i\tau\iota_i$ es automorfismo de M_i. Sin pérdida de generalida digamos que $\pi_j\sigma\iota_j$ es un automorfismo de M_j, entonces definimos el R-módulo $U_j = \sigma\iota_j(M_j) = \sigma(M_i)$, los R-morfismos de módulos $\varphi : M_j \to U_j$ tal que $\forall x \in M_j$ se tiene que $\varphi(x) = \sigma(x)$ y la inyección$\iota'_j : U_j \to M$, es decir, $\iota'_j(y) = y$. Ahora como $\pi_j\sigma\iota_j$ es automorfismo, entonces en particular tenemos que φ_j es epimorfismo. Tomemos ahora $x \in M_j$, entonces tenemos que $\iota'_j\varphi_j(x) = \varphi_j(x) = \sigma(x) = \sigma\iota_j(x)$, es decir, $\iota'_j\varphi_j = \sigma\iota_j$, lo cual implica que $\pi_j\iota'_j\varphi_j = \pi_j\sigma\iota_j$ con lo cual obtenemos que el siguiente diagrama conmuta

$$\begin{tikzcd}
M \arrow[rr, "\sigma"] & & M \arrow[dd, "\pi_j"] \\
& U_j \arrow[ur, "\iota'_j"] & \\
M_j \arrow[uu, "\iota_j"] \arrow[ur, "\varphi_j"] \arrow[rr, "\pi_j\sigma\iota_j"] & & M_j
\end{tikzcd}$$

Entonces con esto tenemos que, por el primer teorema de isomorfismo de módulos, $M = Im(\iota'_j\varphi_j)\bigoplus Nuc(\pi_j)$ y como $\iota'_j\varphi_j$es espimorfismo tenemos entonces $Im(\iota'_j\varphi_j)\bigoplus Nuc(\pi_j) = U_j\bigoplus(\bigoplus_{j\neq i\in I} M_i)$, por lo tanto concluimos que $M = U_j\bigoplus(\bigoplus_{j\neq i\in I} M_i)$. □

Lema 7.2. *Sea R un anillo y $M = \bigoplus_{i\in I} M_i$ un R-módulo derecho tal que $End(M_i)$ es local $\forall i \in I$ y $\sigma, \tau \in End(M)$ con $Id_M = \sigma + \tau$. Entonces $\forall j \in I$ existe un $U_j \leq M$ y un isomorfismo $\varphi : M_j \to U_j$, el cual es inducido por σ o por τ (es decir $\varphi(x) = \sigma(x)\ \forall x \in M_j$ o $\varphi(x) = \tau(x)\ \forall x \in M_j$). Además sea $E = \{i_1 i_2, ..., i_t\} \subset I$. Entonces existen R-módulos $C_{i_j} \leq M$, con $j = 1, ..., t$, e isomorfismos $\gamma_{i_j} : M_{i_j} \to C_{i_j}$ los cuales son inducidos por σ o por τ, con lo cual al último tendríamos que $M = C_{i_1}\bigoplus C_{i_2}\bigoplus ...\bigoplus C_{i_t}\bigoplus(\bigoplus\limits_{i\in I, i\notin E} M_i)$.*

Demostración. Sea R un anillo y $M = \bigoplus_{i\in I} M_i$ un R-módulo derecho tal que $End(M_i)$ es local $\forall i \in I$ y $\sigma, \tau \in End(M)$ con $Id_M = \sigma + \tau$. Entonces $\forall j \in I$ existe un $U_j \leq M$ y un isomorfismo $\varphi : M_j \to U_j$, el cual es inducido por σ o por τ (es decir $\varphi(x) = \sigma(x)\ \forall x \in M_j$ o $\varphi(x) = \tau(x)\ \forall x \in M_j$). Además sea $E = \{i_1 i_2, ..., i_t\} \subset I$. Ahora con esto tenemos que los C_{i_j} están determinados sucesivamente con ayuda del lema anterior, entonces para $i_j = j$ sea $C_{i_j} = U_{i_1}$, con lo cual por el lema anterior tenemos que $C_{i_1}\bigoplus(\bigoplus_{i_1\neq i\in I} M_i)$. Ahora como $M_{i_1} \cong C_{i_1}$, tenemos que $End(C_{i_1})$ también es local. Ahora tomamos la descomposición antes dada y siguiendo un razonamiento análogo al de C_{i_1}podemos reemplazar a M_{i_2} por un C_{i_2}, de tal manera que obtenemos $C_{i_1}\bigoplus C_{i_2}\bigoplus(\bigoplus_{1,2\neq i\in I} M_i)$, por último siguiendo de esta manera al final obtenemos que $C_{i_1}\bigoplus C_{i_2}\bigoplus ...\bigoplus C_{i_t}\bigoplus(\bigoplus\limits_{i\in I, i\notin E} M_i)$ como se quería. □

Lema 7.3. *Sean R un anillo y $M = \bigoplus_{i\in I} M_i$ un R-módulo derecho tal que $End(M_i)$ es local $\forall i \in I$ y $M = A\bigoplus B$ donde $A \neq 0$ es «inescindible», sea $\pi' : M \to A$ la proyacción de M a A. Entonces existe un $k \in I$ tal que π' induce un isomorfismo de M_k sobre A y además $M = M_k\bigoplus B$.*

Demostración. Sean R un anillo y $M = \bigoplus_{i\in I} M_i$ un R-módulo derecho tal que $End(M_i)$ es local $\forall i \in I$ y $M = A\bigoplus B$ donde $A \neq 0$ es inescindible, sea $\pi' : M \to A$ la proyacción de M a A, además consideremos $\iota : A \to M$ la inclusión de A en M, con esto definamos $\iota\pi'\pi : M \to M$. Ahora como por construcción $Id_M = \pi + (Id_M - \pi)$, entonces podemos aplicar el lema 7.1 con $\sigma = \pi$ y $\tau = Id_M - \pi$. Como $A \neq 0$ entonces existe $0 \neq a \in A$ tal que $\pi(a) = a$, entonces se sigue que $(Id_M - \pi)(a) = 0$. Sea $a = \sum_{j=1}^{t} m_{i_j}$ con

$0 \neq m_{i_j} \in M_{i_j}, i_j \in I$ la única representación de a en $M = \bigoplus_{i \in I} M_i$. Ahora recordando el lema anterior tomamos los módulos C_{i_j} y los isomorfismos γ_{i_j} determinados. Supongamos que todos los γ_{i_j} fueron inducido por $Id_M - \pi$, entonces de esto se seguiría que $0 = (Id_M - \pi)(a) = \sum_{j=1}^{t}(Id_M - \pi)(m_{i_j})$ con $(Id_M - \pi)(m_{i_j}) = \gamma_{i_j}(m_{i_j}) \in C_{i_j}$, ahora como la suma de los C_{i_j} es directa, se sigue que $\gamma_{i_j}(m_{i_j}) = 0$, por lo que $m_{i_j} = 0$ y finalmente resulta $a = 0$, lo cual es una contradicción ya que escogimos $0 \neq a$. Por lo tanto al menos un ι_{i_j}es tal que γ_{i_j} es inducido por π, denotemos a este morfismo por γ_k, entonces $\gamma_k : M_k \to C_k$con $\gamma_k(x) = \pi(x)$, por lo que resulta entonces ser un isomorfismo, como en el lema anterior, además justamente además tenemos que C_k es un sumando directo de M, podemos entonces escribir $M = C_k \bigoplus L$. Por todo lo anteriro tenemos que $C_k = \pi(M_k) \hookrightarrow \pi(M) = A$, de esto se sigue que $A = M \cap A = (C_k \bigoplus L) \cap A = C_k \bigoplus (L \cap A)$, ahora como A es directamente inescindible y $C_k \neq 0$ (ya qe $M_k \neq 0$ y $M_k \cong C_k$), concluimos finalmente que $A = C_k$, si hacemos $\iota : M_k \to M$ la inclusión de M_k en M podemos considerar el digrama conmutativo

$$\begin{tikzcd} M_k \arrow[rr, "\iota"] \arrow[dr, "\gamma_k"'] & & M \arrow[dl, "\pi'"] \\ & A = C_k & \end{tikzcd}$$

, entonces por el primer teorema de isomomorfismos para módulos tenemos que $M = M_k \bigoplus Nuc(\pi') = M_k \bigoplus B$, es decir, $M = M_k \bigoplus B$ como se quería. $\square$

El siguiente Teorema fue tomado del libro Modules and Rings de F. Kasch, y se exhibe aquí para la comodidad del lector.

Teorema 7.1. *(Teorema de Krull-Schmidt-Remak)*

Sean R un anillo y $M = \bigoplus_{i \in I} M_i$ un R-módulo derecho tal que $End(M_i)$ es local $\forall i \in I$ y $M = \bigoplus_{j \in J} N_j$ donde N_j es inescindible y distinto de de 0 $\forall j \in J$. Entonces existe una biyección $\beta : I \to J$ tal que $M_i \cong N_{\beta(i)}$ $\forall i \in I$.

Demostración. Sean R un anillo y $M = \bigoplus_{i \in I} M_i$ un R-módulo derecho tal que $End(M_i)$ es local $\forall i \in I$ y $M = \bigoplus_{j \in J} N_j$ donde N_j es inescindible y distinto de de 0 $\forall j \in J$. Ahora por el lema anterior tenemos que N_j es isomorfo a un M_i, entonces los $End(N_j)$ son locales $\forall j \in J$. Demos ahora unas relaciones de equivalencia; 1) $i_1 \sim i_2$ si y sólo si $M_{i_1} \cong M_{i_2} (i_1, i_2 \in I)$ y 2) $j_1 \sim j_2$ si y sólo si $N_{j_1} \cong N_{j_2}$ $(j_1, j_2 \in J$. Estas realciones en efecto son de equivalencia, porque la relación de isomorfía entre módulos lo es. Consideremos entonces $\bar{i}$ la clase de equivalencia determinda por $i \in I$ y llamemos $\bar{I}$ al conjunto de todas las clases de equivalencia, análagomente llamemos $\bar{j}$ a la clase de equivalencia de $j \in J$ y $\bar{J}$ al conjunto de todas las clases de equivalencia. Definamos entonces la función $\Phi : \bar{I} \to \bar{J}$ dada por $\Phi(i) = j$,si $M_i \cong N_j$. Mostremos que Φ es una función biyectiva.

Φ es función: Φ está defnida en $\bar{I}$, puesto que por el lema 7.3 (aplicado a $A = M_i$ y $M = \bigoplus N_j$ en lugar de $M = \bigoplus M_{ii}$) tenemos que existe una $j \in J$ con $N_j \cong M_i$. Puesto que, como ya dijimos, el isomorfismo es una relación de equivalencia Φ es independiente de los representantes que se tomen en $\bar{I}$ y $\bar{J}$, es decir, Φ en efecto es una función.

Φ es inyectiva y suprayectiva: Sean $\Phi(\bar{i_1}) = \bar{j_i} = \bar{j_2} = \Phi(\bar{i_2})$, de esto se sigue por definición que $M_{i_1} \cong N_{j_1} \cong N_{j_2} \cong M_{i_2}$, que por transitividad nos da $M_{i_1} \cong M_{i_2}$, por lo que $\bar{i_1} = \bar{i_2}$, es decir, Φ es inyectiva. Además por el lema 7.3 Φ resulta también suprayectiva.

Entonces en efecto Φ es una función biyectiva, ahora sólo falta mostrar que $\forall i \in I$ existe una biyección $\beta_{\bar{i}} : \bar{i} \to \Phi(\bar{i})$. Ya que $\beta : I \to J$ dada por $\beta(i) = \beta_{\bar{i}}(i)$ sería la biyeción deseada.

Ahora por el teorema de Schröder-Bernstein que se puede encontrar en el libro A. G. Hamilton. Numbers, sets and axiom: the apparatus of mathematics, nos es suficiente mostrar que existen funciones inyectivas $\bar{i} \to \Phi(\bar{i})$ y $\Phi(\bar{i}) \to \bar{i}$. Por la simetría de las afirmaciones, solamente es necesario encontrar la existencia de alguna inyección, por ejemplo, sólo basta mostrar la de $\Phi(\bar{i}) \to \bar{i}$. Dividiremos esto en casos.

Caso 1.- $\bar{i}$ es finito. Sea t el número de elementos de $\bar{i}$, llamemos $E = \{j_1, j_2, ..., j_s\} \subset \Phi$. Por el lema 7.3 (con $A = N_{j_1}$) existe un M_{i_1} tal que $M_{i_1} \cong N_{j_i}$, es decir, $i_1 \in \bar{i}$ y $M = M_{i_1} \bigoplus (\bigoplus_{j_1 \neq j \in J} N_j)$. También por el lema 7.3 (pero ahora con $A = N_{j_2}$ y $B = M_{i_1} \bigoplus (\bigoplus_{j_1, j_2 \neq j \in J} N_j))$ existe otra vez un M_{i_2} tal que $M_{i_2} \cong N_{j_2}$, es decir, $i_2 \in \bar{i}$ y $M = M_{i_1} \bigoplus M_{i_2} \bigoplus (\bigoplus_{j_1 \neq j \in J} N_j)$. Siguiendo esta misma idea obtenemos sucesivamente $M = M_{i_1} \bigoplus M_{i_2} \bigoplus ... \bigoplus M_{i_t} (\bigoplus\limits_{j \in J, j \notin E} N_j)$ con $M_{i_l} \cong N_{j_l}$ para $l = 1, 2, ..., s$. Puesto que la suma es directa, los

$M_{i_1}, M_{i_2}, ..., M_{i_s}$ son diferentes por pares, por lo tanto debemos tener que $s \leq t$. De esta manera aseguramos que el número de elementos de $\Phi(\bar{i}) \leq t$ y la afirmación es clara, es decir, existe la inyección.

Caso 2.- $\bar{i}$ es infinito. Sea $\pi'_j : M \to N_j$ la proyección natural, y sea para $k \in I$ $E(k) = \{j |\ j \in J$ y π'_j induce un isomorfismo de M_k sobre $N_j\}$.

Afirmación.- $E(k)$ es finito $\forall k \in I$.

Sea $0 \neq m \in M_k$ y $m = \sum_{l=1}^{t} n_{j_l}$, $0 \neq n_{j_l} \in N_{j_l}$, lo cual implica que $\pi'_{j_l}(m) = n_{j_l}$. Ahora para ver lo del isomorfismo, debemos tener que $\pi'_j(m) \neq 0$, es decir, $j \in \{j_1, j_2, ..., j_l\}$.

Afirmación.- $\Phi(\bar{i}) = \cup_{k \in \bar{i}} E(k)$.

Veamos que $\Phi(\bar{i}) \supset \cup_{k \in \bar{i}} E(k)$. Sea $k \in \bar{i}$ y $j \in E(k)$. Entonces $k \in \bar{i}$ implica que $M_k \cong M_i$, ademas $j \in E(k)$ implica $M_k \cong N_j$,juntando estas dos implicaciones obtenemos por transitividad que $M_i \cong N_j$, lo cual implica que $j \in \Phi(\bar{i})$.

Veamos ahora que $\Phi(\bar{i}) \subset \cup_{k \in \bar{i}} E(k)$. Sea $j \in \Phi(\bar{i})$, de entrada esto implica que $M_{i_1} \cong N_j$, además por el lema 7.3 existe un $k \in I$ tal que π'_j induce un isomorfismo de M_k sobre N_j, lo cual nos una que $M_k \cong N_j \cong M_i$, es decir, $M_k \cong M_i$, lo cual implica que $k \in \bar{i}$ y que $j \in E(k)$. Sea $\sqcup_{k \in \bar{i}} E(k)$ la unión disjunta de los conjuntos $E(k)$, entonces existe una inyección $\Phi(\bar{i}) = \cup_{k \in \bar{i}} E(k) \to \sqcup_{k \in \bar{i}} E(k)$. Puesto que $E(k)$ es finito, para todo $E(k)$ existe una inyección sobre $\mathbb{N}$, entonces existe una inyección $\sqcup_{k \in \bar{i}} E(k) \to \bar{i} \times \mathbb{N}$. Puesto que $\bar{i}$ es infinito, por un conocido resultado de la teoría de conjuntos existe una biyección entre $\bar{i} \times \mathbb{N}$ y $\bar{i}$. Todas estas inyecciones juntas nos producen una inyección $\Phi(\bar{i}) \to \bar{i}$. Por lo que el segundo caso que completo.

Por lo tanto queda demostrado el teorema de Krull-Schmidt-Remak. $\square$

7.2. Dimensión de Goldie

Ya demostrado el teorema de Krull-Schmidt-Remak podemos hablar de la dimensión de Goldie.

Definición 7.1. Sea R un anillo, decimos que un R-módulo M es uniforme si todo submódulo no cero de M es esencial.

Observación 7.1. Que un R-módulo M sea uniforme es equivalente a que la intersección de cualesquiera dos submódulos no cero de M sea distinta de cero.

Definición 7.2. La dimensión de Goldie (o dimensión uniforme) de un R-módulo M es el cardinal de una suma $\bigoplus_{i\in I} U_i$, tal que $\bigoplus_{i\in I} U_i$ es esencial en M y $\forall i \in I$ U_i es inescindible, es decir, si una suma directa de submódulos inescindibles de M $\bigoplus_{i\in I} U_i$ es esencial en M, entonces la dimensión de Goldie de M es $|I|$. Denotaremos la dimensión de Goldie por $Gdim$.

Observación 7.2. La dimensión de Goldie de un R-módulo está bien definida ya que si se tiene que $\bigoplus_{i\in I} U_i$ y $\bigoplus_{j\in J} V_j$ son esenciales en M, entonces $|I|$=|J|, esto gracias al teorema de Krull-Schmidt-Remak.

Observación 7.3. Si un R-módulo M es tal que $Gdim(M) = 1$, entonces M es uniforme.

Observación 7.4. Para que la dimensión de Goldie de un R-módulo M sea infinita se debe de tener que M contiene una suma infinita de submódulos no cero de M, por lo que si M es neteriano o artiniano se tiene que M tiene dimensión de Goldie finita.

Definición 7.3. Sea R un anillo, decimos que un R-módulo M es un módulo hueco si todo submódulo propio de M es superfluo.

Observación 7.5. Que un R-módulo M sea un módulo hueco es equivalente a que si al tomar $N_1, N_2 \leq M$ tales que $N_1 + N_2 = M$ se tiene que $N_1 = M$ o $N_2 = M$.

Capítulo 8

V-anillos

8.1. V-anillos

Definición 8.1. Un anillo R es llamado V-anillo si todo R-módulo derecho simple es inyectivo.

Nota: La clase de los V-anillos fue introducida por Villamayor.

Teorema 8.1. *Son equivalentes para un anillo R:*
i) R es V-anillo;
ii) Para todo R-módulo M se tiene que $J(M) = 0$;
iii) Todo ideal derecho propio $I < R$ es una intersección de ideales máximos.

Demostración. Sea R un anillo:
i) $\Longrightarrow$ ii) Supongamos que R es V-anillo, tomemos un R-módulo derecho M. Mostremos que la intersección de todos los submódulos máximos de M ($J(M)$) es cero. Sea $0 \neq x \in M$, consideremos el R-módulo derecho xR, sea N un submódulo máximo de xR y construyamos $S = xR/N$ que es un R-módulo simple, por hipótesis inyectivo. Consideramos el epimorfismo canónico $f : xR \to S$, ahora como S es inyectivo f puede ser extendido a $\bar{f} : M \to S = xR/N$, entonces $Nuc(\bar{f})$ es un submódulo máximo de M tal que $x \notin Nuc(\bar{f})$, por lo que x no puede estar en la intersección de todos los submódulos máximos de M, es decir, $J(M) = 0$.
ii) $\Longrightarrow$ iii) Sea $I < R$ un ideal derecho propio de R. Puesto que $J(R/I) = 0$, por la Proposición 5.12 concluimos que I es una intersección de ideales máximos de R.
iii) $\Longrightarrow$ i) Sean S un R-módulo derecho simple e I un ideal de R. Consideremos un morfismo no cero $f : I \to S$, por el Lema de Baer para mostrar la inyectividad de S, basta mostrar que f se puede extender a un morfismo $\bar{f} : R \to S$. Tomemos un elemento $x \in I \backslash Nuc(f)$, como $Nuc(f)$ resulta ser un ideal derecho de R, entonces por hipótesis, $Nuc(f)$ es una intersección de una familia de ideales derechos máximos de R, ahora como tenemos que $x \notin Nuc(f)$, entonces existe un ideal máximo $M \supseteq Nuc(f)$ tal que $x \notin M$. Ahora puesto

que $I\backslash Nuc(f) \cong S$ (primer teorema de isomorfismo para módulos) es simple, tenemos que $M \cap I = Nuc(f)$. Claramente $I + M = R$. Ahora extendemos f a $\bar{f} : R \to S$ definida por $\bar{f}(a+m) = f(a)$ $\forall a \in I$ y $\forall m \in M$. Con esto mostramos que todo R-módulo simple es inyectivo, es decir, R es V-anillo. □

Ejemplo 8.1. Todo campo K cumple con ser V-anillo, ya que al sólo tener dos ideales (0 y K) cumple trivialmente que todo ideal $I < K$ es intersección de máximos.

Definición 8.2. Un ideal I, de un anillo R, se llama primitivo si es el anulador de un R-módulo simple. De la misma manera un anillo cociente R/I será llamado primitivo justo cuando el ideal I sea primitivo.

Observación 8.1. Todo ideal primitivo es primo.

Proposición 8.1. *Son equivalentes para un anillo R:*
i) R es un V-anillo;
ii)Todo ideal I de R es idempotente, es decir, $I^2 = I$ y todos los anillos cocientes primitivos de R son V-anillos.

Demostración. Sea R un anillo:
i) $\Longrightarrow$ ii) Supongamos que R es un V-anillo, claramente todo anillo cociente de R es V-anillo. Ahora supongamos que I es un ideal derecho de R tal que $I \neq I^2$. Por la proposición anterior I e I^2 son intersección de ideales derechos máximos y como son distintos debe existir un ideal máximo M tal que $I^2 \subseteq M$ y $I \nsubseteq M$, entonces $R = M + I$, por lo cual deben existir $m \in M$ e $i \in I$ tal que $1 = m + i$, con lo cual se tiene que $I = (m+i)I \subseteq mI + iI \subseteq M + I^2 = M$, lo cual es una contradicción, porque teníamos que $I \nsubseteq M$, por lo que $I = I^2$.
ii) $\Longrightarrow$ i) Sean S un R-módulo derecho simple, E una extensión esencial de S y $A = ann(S)$. Puesto que R/A es un anillo primitivo, entonces por hipótesis, R/A es un V-anillo. Veamos ahora que $A = ann(E)$, ya que si suponemos que $A \neq ann(E)$, entonces existiría un elemento $x \in E$ tal que $xA \neq 0$. Puesto que E es una extensión esencial de S que es simple, nosotros tenemos que $S \subseteq xA$, por lo tanto existe un ideal derecho I de R tal que $I \subseteq A$ y $xI = S$, ya que si consideramos la inyección $\iota : S \to xA$ obtendremos que $S = Im(\iota) = xI$. Ahora $S = xI = xI^2 = SI \subseteq SA = 0$, lo cual es una contradicción, por lo tanto $A = ann(E)$. Ahora E es un R/A -módulo que es extensión esencial del R/A-módulo simple S. Puesto que por hipótesis R/A es un V-anillo, se tiene que $S = E$. Por lo tanto S es inyectivo y R resulta V-anillo. □

Definición 8.3. Un anillo R es llamado Von Neumann regular si para todo $r \in R$ existe un $s \in R$ tal que $r = rsr$.

Proposición 8.2. *Sea R un anillo, entonces R es Von Neumann regular si y sólo si todo ideal principal (cíclico) es generado por un elemento idempotente.*

Demostración. Sea R un anillo.

Supongamos que R es Von Neumann regular y tomemos un ideal principal aR de R, entonces como R es Von Neumann regular, existe $x \in R$ tal que $a = axa$, ahora multiplicando por x la igualdad obtenemos que $ax = axax = (ax)(ax) = (ax)^2$, es decir, ax es idempotente y además $aR = axR$.

Ahora supongamos que todo ideal principal está generado por un idempotente. Tomemos $a \in R$, entonces por hipótesis $aR = eR$ para algún $e \in R$ idempotente, entonces $a = ex$ para alguna $x \in R$ y $a = ea = axa$. □

Proposición 8.3. *Sea R un anillo Von Neumann regular, entonces todo ideal I de R es idempotente.*

Demostración. Sean R un anillo Von Neumann regular e I un ideal de R, sea $a \in I$, entonces por la proposición anterior tenemos que $aR = e_aR$ con $e_a \in R$ idempotente, entonces $a = e_ar$ para alguna $r \in R$, esto implica que $e_aa = e_ae_ar = e_a(e_ar) = (e_ae_a)r = e_ar = a$, con esto tenemos que $e_a \in I$ y además $a = e_a(e_ar)$ donde $e_a, e_ar \in I$, por lo tanto $a \in I^2$, por lo tanto $I = I^2$. □

Proposición 8.4. *Un anillo conmutativo R es un V-anillo si y sólo si es un anillo Von Neumann regular.*

Demostración. Sea R un anillo Von Neumann regular conmutativo, puesto que es conmutativo, todo anillo cociente primitivo es un campo, ya que todo ideal primitivo es primo, además todo ideal derecho de un anillo Von Neumann regular es idempotente, entonces por la Proposición 8.1 obtenemos que R es V-anillo.

Ahora supongamos que R es V-anillo conmutativo, entonces por la Proposición 8.1 todo ideal de R es idempotente. Tomemos ahora $r \in R$, entonces $rR = (rR)^2 = r^2R$, entonces existe un elemento $s \in R$ tal que $r = r^2s = rsr$ por la conmutatividad, entonces con esto concluimos que R es un anillo Von Neumann regular. □

8.2. DV-anillos

Definición 8.4. Un anillo R es un débil-V-anillo (DV-anillo para abreviar) si todo R-módulo simple derecho es R/I-inyectivo para todo ideal derecho I tal que $R/I \ncong R$, es decir, R/I es propio.

Ejemplo 8.2. Un ejemplo de un DV-anillo que no es V-anillo es $\mathbb{Z}_{p^2}$ con p primo

Lema 8.1. *Sean R un DV-anillo y R/A y R/B dos R-módulos cíclicos distintos de R tal que $A \cap B = 0$, entonces R es un V-anillo.*

Demostración. Sean R un DV-anillo y R/A y R/B dos R-módulos cíclicos distintos de R tal que $A \cap B = 0$, ahora dado que R es DV-anillo, cualquier R-módulo derecho simple es $(R/A) \times (R/B)$ inyectivo, ya que por definición es R/A y R/B inyectivo, ahora como se tiene que $A \cap B = 0$ entonces R_R se sumerge en $(R/A) \times (R/B)$, ya que un elemento $x \in R$ está en R/A o R/B, de lo contrario x estaría en $A \cap B$, pero $A \cap B = 0$, por lo que todo R-módulo es R_R, es decir R es V-anillo. □

El siguiente Teorema fue tomado del libro Cyclic Modules and the Structure of Rings de S. K. Jain, Ashish K. Srivastava, Askar A. Tuganbaev, y se exhibe aquí para la comodidad del lector.

Proposición 8.5. *Sea R un DV-anillo que no es V-anillo, entonces R debe ser uniforme derecho.*

Demostración. Sea R un DV-anillo.

Supongamos que R es de dimensión de Goldie infinita, entonces R contiene una suma directa $A \bigoplus B$ tal que A y B son sumas directas infinitas de ideales derechos no cero. Si $R/A \cong R$, entonces R/A es proyectivo, entonces existe un ideal derecho C de R tal que $R = C \bigoplus A$, pero el módulo cíclico R/C es isomorfo a una suma directa infinita de ideales no cero, lo cual es una contradicción, por lo tanto R/A es R-módulo propio derecho, siguiendo un razonamiento similar obtenemos que R/B también es propio. Entonces por el lema anterior obtenemos que R es V-anillo.

Supongamos que la dimensión de Goldie de R está en $\mathbb{N} \backslash \{1\}$, es decir, $Gdim(R) = n > 1$ entonces existen ideales derechos uniformes U_i tal que $\bigoplus_{i=1}^{n} U_i \subset_{es} R$. Ahora tenemos entonces que

$Gdim(R/U_1) = n - 1 = Gdim(R/U_2)$, por lo que R/U_1 y R/U_2 son propios y como la suma de los $U_i's$ es directa tenemos entonces que $U_1 \cap U_2 = 0$, entonces por el lema anterior tenemos que R es V-anillo.

Por lo tanto concluimos que si un anillo R es DV-anillo, pero no es V-anillo entonces se tiene que $Gdim(R) = 1$, es decir, R es uniforme derecho. □

Proposición 8.6. *Sea R un anillo tal que R/I es propio para todo ideal derecho no cero I, entonces son equivalentes:*

i) R es un DV-anillo derecho;

ii) $J(R/I) = 0$ para todo ideal derecho no cero I de R;

iii) Todo ideal derecho no cero $I \neq R$ es una intersección de ideales derechos máximos.

Nota: en particular los enunciados anteriores son equivalentes cuando R es uniforme derecho.

Demostración. Sea R un anillo tal que R/I es propio para todo ideal derecho no cero I.

i) $\Longrightarrow$ ii) Supongamos que R es DV-anillo, entonces por definición R-módulo simple es R/I-inyectivo, donde I es un ideal no cero de R, lo cual por hipótesis implica que $R/I \neq R$, entonces de esto concluimos que todo R/I es V-anillo, por lo cual, gracias al Teorema 8.1, todo R/I-módulo M tiene $J(M) = 0$, en particular R/I es un R/I-módulo, con lo cual concluimos que $J(R/I) = 0$.

ii) $\Longrightarrow$ iii) Tomemos un ideal derecho no cero $I \neq R$, entonces por hipótesis tenemos que $J(R/I) = 0$, con lo cual concluimos que I es una intersección de máximos.

iii) $\Longrightarrow$ i) Supongamos que todo ideal derecho no cero $I \neq R$ es una intersección de ideales derechos máximos, como por hipótesis R/I es propio, porque I es no cero, entonces de esto concluimos que R/I es V-anillo, entonces todo R/I-módulo simple es R/I-inyectivo, con lo cual podemos concluir que todo R-módulo simple es R/I-inyectivo, es decir, R es DV-anillo. $\square$

Corolario 8.1. *Si R es un DV-anillo derecho, entonces $R/J(R)$ es un V-anillo derecho.*

Demostración. Si R es un V-anillo, entonces claramente $R/J(R)$ es un V-anillo ya que por la proposición 8.1 se tendría que $J(R) = 0$ por lo que $R/J(R) = R$. Entonces supongamos que R no es un V-anillo derecho, entonces por la proposición 8.4 se tiene que R es uniforme derecho, ahora por la proposición anterior tenemos que todo ideal derecho no cero $I \neq R$ es intersección de ideales derechos máximos. Ahora si tuviéramos que $J(R) = 0$ entonces tendríamos que el ideal cero también es una intersección de ideales máximos por lo que $R = R/J(R)$ es un V-anillo. Ahora si $J(R) \neq 0$ entonces todos lo ideales derecho de $R/J(R)$ distintos de $R/J(R)$ son intersección de ideales derechos máximos, entonces por la proposición 8.1 se tiene que $R/J(R)$ es un V-anillo. $\square$

Nota: Con esto tenemos que, en particular, un anillo DV-anillo que además es Von Neumann regular derecho resulta ser un V-anillo derecho.

Proposición 8.7. *Si R es un DV-anillo derecho, entonces para todo ideal derecho de R se tiene que $I^2 = 0$ o $I^2 = I$.*

Demostración. Sea R es un DV-anillo derecho.

Primero si R además es un V-anillo entonces por la proposición 8.2 para todo ideal derecho de R se tiene que $I^2 = I$.

Asumamos entonces que R no es V-anillo, entonces por la proposición 8.4 R resulta uniforme derecho. Tomemos ahora un ideal derecho $I \neq R$ y supongamos que $I^2 \neq 0$, entonces por la proposición 8.5 se tiene que tanto I como I^2son intersección de ideales derechos máximos, si $I^2 \neq I$ entonces debe existir un ideal derecho máximo M tal que $I^2 \subseteq M$, pero $I \nsubseteq M$, entonces tenemos que $R = I + M$ y podemos escribir $1 = i + m$ para algunos $i \in I$ y $m \in M$, esto nos da $I = (i+m)I \subseteq iI + mI \subseteq I^2 + M = M$, lo cual es una contradicción ya que teníamos que $I \nsubseteq M$, por lo que $I = I^2$. Todo esto se dio teniendo en mente que $I^2 \neq 0$, por lo tanto podes concluir que para todo ideal derecho I de R se tiene que $I^2 = 0$ o $I = I^2$. $\square$

Proposición 8.8. *Si R es un DV-anillo derecho que además es un dominio entero, entonces R es simple.*

Demostración. Sea R es un DV-anillo derecho que además R es un dominio entero, tomemos un elemento $0 \neq a \in R$, ahora como R dominio entero, obtenemos que $(aR)^2 \neq 0$, ya que en los dominios enteros no hay divisores propios de cero, ahora como $(aR)^2 \neq 0$, por la proposición anterior, concluimos que $(aR)^2 = aR$, es decir, $aRaR = aR$, y puesto que R es dominio entero obtenemos que $RaR = R$, ya que se vale la ley de la cancelación, esto muestra que

R es el único ideal no cero de R, por lo tanto concluimos que R es un anillo simple. $\square$

Corolario 8.2. *Si R es un DV-dominio, entonces R es un V-dominio.*

Demostración. Sea R un DV-dominio, entonces por la proposición anterior, tenemos que R es simple, entonces sólo tiene dos ideales, R y 0, por lo que, al ser DV-anillo en particular, se cumple trivialmente que R es V-anillo. $\square$

8.3. ΣV-anillos

Definición 8.5. Sean R un anillo y M un R-módulo, se dice que M es Σ-inyectivo si $M^{(\alpha)}$ es inyectivo para cualquier cardinal α.

El siguiente Teorema fue tomado del libro Cyclic Modules and the Structure of Rings de S. K. Jain, Ashish K. Srivastava, Askar A. Tuganbaev, y se exhibe aquí para la comodidad del lector.

Teorema 8.2. *Sea R un anillo, entonces son equivalentes para un R-módulo inyectivo M:*
i) M es Σ-inyectivo
ii) $M^{(\aleph_0)}$ es inyectivo
iii) Toda extensión esencial de $M^{(\aleph_0)}$ es una suma directa de módulos que son proyectivos o inyectivos.

Demostración. Sean R un anillo y M un R-módulo inyectivo
iii) $\implies$ i) Supongamos que toda extensión esencial de $M^{(\aleph_0)}$ es una suma directa de módulos que son proyectivos o inyectivos, procedamos por contradicción. Supongamos que M no es Σ-inyectivo, entonces $\bigoplus_{i\in I} M_i$ $(M_i \cong M)$ no es inyectivo, para algún conjunto de índices infinito I, por lo tanto por el Teorema de Baer, existe un ideal derecho A de R y un R-morfismo $g : A \to \bigoplus_{i\in I} M_i$ tal que el conjunto $I' = \{j \in I | \ \pi_j \circ g \neq 0\}$ es infinito, donde $\pi_j : \bigoplus_{i\in I} M_i \to M_j$ es la proyección canónica, ya que de otra manera $Im(g)$ estaría contenida en una subsuma directa finita de $\bigoplus_{i\in I} M_i$ y puesto que toda suma directa finita de módulos inyectivos es inyectivo, entonces g se extendería a R, contradiciendo el hecho de que tomamos $\bigoplus_{i\in I} M_i$ no inyectivo. Sea J un subconjunto infinito numerable de I'. Ahora, escogemos un elemento $a_j \in A$ y definimos $b_j = g(a_j)$ y $N_j = b_j R$. Entonces tenemos que N_j es un submódulo cíclico de M_j, y puesto que J es numerable y todo N_j es cíclico, tenemos que $\bigoplus_{j\in J} N_j$ es numerablemente generado. Ahora denotamos por Q_j una cápsula inyectiva de N_j en M_j y tomamos $Q = E(\bigoplus_{j\in J} Q_j)$ una cápsula inyectiva de $\bigoplus_{j\in J} Q_j$. Sea $\pi : \bigoplus_{i\in I} M_i \to \bigoplus_{j\in J} Q_j$ el epimorfismo que manda todo M_i a cero si $i \in I \backslash J$; mientras que $\forall i \in J$, la restricción de π a M_i es tal que $\pi|_{M_i} = \beta \circ \alpha$, donde $\alpha : M_i \to Q_i$ es la proyección natural y $\beta : Q_i \to \bigoplus_{j\in J} Q_j$ es el monomorfismo canónico. Ahora afirmamos que el morfismo $f = \pi \circ g : A \to \bigoplus_{j\in J} Q_j$ no puede ser extendido a un morfismo $h : R \to \bigoplus_{j\in J} Q_j$ a lo largo del monomorfismo $\mu : A \to R$. En particular afirmamos que $\bigoplus_{j\in J} Q_j$ no es inyectivo. Supongamos

lo contrario, es decir, supongamos que f admite una extensión h. Puesto que $h(1)$ está contenido en una subsuma directa finita de $\bigoplus_{j\in J} Q_j$, entonces $Im(f)$ está contenida en $\bigoplus_{j\in F} Q_j$ para algún conjunto finito F de J, por lo tanto $\pi_j \circ f = 0$ para cada $j \in J\backslash F$. Pero esto no es posible ya que $\pi \circ f : A \to Q_j$ y toda Q_j es una cápsula inyectiva de N_j en M_j, por lo que nuestra afirmación es correcta.

Consideremos ahora el conjunto Ω de submódulos P de Q que satisfacen las tres siguientes condiciones:

1) $\bigoplus_{j\in J} Q_j \subseteq P \subseteq Q$.

2) P es una suma directa de submódulos inyectivos de Q.

3) $f = \pi \circ g : A \to \bigoplus_{j\in J} Q_j \subseteq P$ no puede ser extendido a un morfismo $h : R \to P$ a lo largo del monomorfismo $\mu : A \to R$.

Claramente Ω no es vacío ya que $\bigoplus_{j\in J} Q_j \in \Omega$. Definamos ahora un orden parcial en Ω por $P_1 \leq P_2$ si y sólo si $P_1 \subseteq P_2$. Afirmamos que Ω es un conjunto inductivo bajo este el orden parcial. Sea $\{P_k\}_{k\in K}$ una cadena en Ω. Sea $P = \cup_{k\in K} P_k$. Como tenemos que $\bigoplus_{j\in J} Q_j \subseteq_{es} Q = E(\bigoplus_{j\in J} Q_j)$, tenemos que $\bigoplus_{j\in J} Q_j \subseteq_{es} P$. Por lo tanto $\bigoplus_{j\in J} M_j \subseteq_{es} P$, entonces por hipótesis $P = (\bigoplus_{u\in U} C_u) \bigoplus (\bigoplus_{v\in U'} C'_v)$ donde todo C_u es inyectivo y todo D_v es proyectivo. Entonces por un Teorema de I. Kaplansky que se puede encontrar en el libro de Anderson y Fuller, sabemos que todo módulo proyectivo es una suma directa de módulos numerablemente generados. Por lo tanto, tenemos que $P = (\bigoplus_{u\in U} C_u) \bigoplus (\bigoplus_{v\in V} D_v)$, donde todo C_u es inyectivo y todo D_v es un módulo numerablemente generado, además los conjuntos U y V son numerables ya que P contiene un submódulo numerablemente generado $\bigoplus_{j\in J} N_j \subseteq_{es} P$. Por lo tanto, $D = \bigoplus_{v\in V} D_v$ es numerablemente generado. Podemos entonces escribir $D = \sum_{n\in\mathbb{N}} D'_n$ como una suma numerable de módulos finitamente generados. Puesto que D'_1 es finitamente generado $D'_1 \subset \cup_{k\in F'} P_k$ para algún subconjunto finito $F' \subset K$. Además, puesto que todo P_k es una suma directa de módulos inyectivos, P contiene una cápsula inyectiva $E(D'_1)$ de D'_1y más aun, $E(D'_1) \cap (\bigoplus_{u\in U} C_u) = 0$, porque $D'_1 \cap (\bigoplus_{u\in U} C_u) = 0$. Por lo tanto

$$E(D'_1) \cong \frac{(\bigoplus_{u\in U} C_u) \bigoplus E(D'_1)}{(\bigoplus_{u\in U} C_u)} \subseteq \frac{(\bigoplus_{u\in U} C_u) \bigoplus (\bigoplus_{v\in V} D_v)}{(\bigoplus_{u\in U} C_u)} \cong (\bigoplus_{v\in V} D_v) = D$$

Por lo tanto, D contiene una cápsula inyectiva $E(D'_1)$ de D'_1, con lo cual obtenemos la siguiente descomposición $D = E(D'_1) \bigoplus D''_1$, ahora denotemos $D'_{1,n}$ a la imagen de D'_n bajo la proyección natural sobre D''_1 para $n \geq 2$, escribamos $D'_{1,1} = D'_1$, para simplificar un poco. Es fácil ver que $D = E(D'_1) \bigoplus \sum_{n\geq 2} D'_{1,n}$, por como han sido definidos los $D'_{1,n}$. Esto nos produce una descomposición $P = (\bigoplus_{u\in U} C_u) \bigoplus E(D'_{1,1}) \bigoplus \sum_{n\geq 2} D'_{1,n}$. Ahora podemos aplicar el mismo proceso a P, pero ahora con $D'_{1,2}$, con lo cual obtendríamos que:

$P = (\bigoplus_{u\in U} C_u) \bigoplus E(D'_{1,1}) \bigoplus E(D'_{2,2}) \bigoplus \sum_{n\geq 3} D'_{2,n}$, y si repetimos el proceso infinitamente, construimos un conjunto infinito $\{E(D'_{n,n})\}_{n\in\mathbb{N}}$ de submódulos inyectivos de P tal que para cada $m \in \mathbb{N}$ tenemos que:

$(\bigoplus_{u\in U} C_u) \bigoplus (\bigoplus_{n=1}^{m} E(D'_{n,n}) \subseteq P$. Entonces, por construcción:

$D'_m \subseteq \bigoplus_{n=1}^{m} E(D'_{n,n})$, $\forall m \in \mathbb{N}$. Como consecuencia de esto tenemos que, $D \subseteq \bigoplus_{n\in\mathbb{N}} E(D'_{n,n})$, por lo que $P = (\bigoplus_{u\in U} C_u) \bigoplus (\bigoplus_{n\in\mathbb{N}} E(D'_{n,n})$, por lo que P satisface (2). Finalmente, veamos que el morfismo $f = \pi \circ g : A \to \bigoplus_{j\in J} Q_j \subseteq$

P no puede ser extendido a un morfismo $h : R \to P$ a lo largo del monomorfismo $\mu : A \to R$. Supongamos, si es posible, que g admite una extensión h. Puesto que $Im(h)$ es finitamente generado y $\{P_k\}_{k\in K}$ es una cadena, existe un $k \in K$ tal que $Im(h) \subseteq P_k$. Esto nos da una contradicción, porque $P_k \in \Omega$, y por lo tanto, por definición de Ω, f no puede ser extendido a un morfismo con dominio R, por lo tanto $P \in \Omega$. Esto prueba nuestra afirmación de que Ω es un conjunto inductivo. Por el lema de Zorn, tenemos que Ω tiene un elemento máximo, llamémosle P_0, por hipótesis $P_0 = \bigoplus_{t\in T} W_t$, donde todo W_t es inyectivo. Sean $\varphi_t : P_0 \to W_t$ las proyecciones canónicas. Puesto que, por hipótesis, f no puede ser extendido a un morfimos $h : R \to P_0$, existe un subconjunto infinito $T' \subseteq T$ tal que $\varphi_t \circ f \neq 0$, para toda $t \in T'$, porque de otra manera $Im(f)$ podría ser extendida a un morfismo $R \to \bigoplus_{t\in F} W_t \subseteq P_0$, lo cual nos daría una contradicción. Escribamos T como una unión ajena de conjuntos infinitos T_1 y T_2 y denotemos $\varphi_{T_1} : \bigoplus_{t\in T} W_t \to \bigoplus_{t\in T_1} W_t$ y $\varphi_{T_2} : \bigoplus_{t\in T} W_t \to \bigoplus_{t\in T_2} W_t$, notemos que $\varphi_{T_i} \circ f : A \to \bigoplus_{t\in T_i} W_t$ no puede ser extendido a un morfismo $h : R \to \bigoplus_{t\in T_i} W_t$ para $i \in \{1, 2\}$, ya que de otro modo $Im(h) \subset \bigoplus_{t\in F} W_t$, donde F es un conjunto finito, y por lo tanto $\varphi \circ f = \varphi \circ \varphi_{T_i} \circ f = 0$, para cada $t \in T_i \backslash F$, lo cual es una contradicción. Esto implica que $\bigoplus_{t\in T_1} W_t$ no es inyectivo y por lo tanto $\bigoplus_{t\in T_1} W_t \neq E(\bigoplus_{t\in T_1} W_t)$. Por lo tanto $P_0 = \bigoplus_{t\in T} W_t \subsetneq E(\bigoplus_{t\in T_1} W_t) \bigoplus (\bigoplus_{t\in T_2} W_t)$, de aquí podemos ver que f no puede ser extendida a un morfismo $R \to E(\bigoplus_{t\in T_1} W_t) \bigoplus (\bigoplus_{t\in T_2} W_t)$, porque de otra manera $\varphi_{T_2} \circ f$ podría ser extendido a un morfismo $R \to \bigoplus_{t\in T_2} W_t$, lo cual es una contradicción. Concluimos entonces que $E(\bigoplus_{t\in T_1} W_t) \bigoplus (\bigoplus_{t\in T_2} W_t) \in \Omega$, pero esto es una contradicción con el hecho de que P_0 es el elemento máximo de Ω. Por lo tanto M debe ser Σ-inyectivo.

i) $\Longrightarrow$ ii) Es claro ya que si M es Σ-inyectivo, entonces $M^{(\aleph_0)}$ es inyectivo

i) $\Longrightarrow$ iii) Es claro ya que si M es Σ-inyectivo, entonces $M^{(\aleph_0)}$ es inyectivo, por lo cual no tiene una extensión esencial propia, por lo cual el hecho de que $M^{(\aleph_0)}$ sea una suma directa de módulos inyectivos o proyectivos se cumple trivialmente.

ii) $\Longrightarrow$ iii) Es claro ya que si $M^{(\aleph_0)}$ es inyectivo, no tiene una extensión esencial propia, por lo cual el hecho de que $M^{(\aleph_0)}$ sea una suma directa de módulos inyectivos o proyectivos se cumple trivialmente. $\square$

Definición 8.6. Un anillo R es llamado ΣV-anillo derecho si todo R-módulo derecho simple es Σ-inyectivo.

Observación 8.2. Es claro que todo ΣV-anillo R es V-anillo, porque todo R-módulo simple S lo podemos ver como $S^{(1)}$, por lo que S resulta inyectivo.

Definición 8.7. Una suma directa interna $\bigoplus_{i\in I} A_i$ de submódulos de un R-módulo M es llamada sumando local de M si, dado cualquier conjunto finito F de I, la suma directa $\bigoplus_{i\in F} A_i$ es un sumando directo de M.

Definición 8.8. Sean R un anillo y $M = \bigoplus_{i\in I} M_i$ un R-módulo donde ningún M_i es cero. Se dice que la descomposición $\bigoplus_{i\in I} M_i$ complementa sumandos directos si, siempre que se tiene una suma directa A de sumandos de M, existe una subconjunto $J \subseteq I$ para el cual se cumple que $M = (\bigoplus_{i\in J} M_j) \bigoplus A$.

El siguiente Corolario está basado en el Corolario 6.18 del libro Cyclic Modules and the Structure of Rings de S. K. Jain, Ashish K. Srivastava, Askar A. Tuganbaev, y se exhibe aquí para la comodidad del lector.

Corolario 8.3. *Sea R un anillo, entonces un R-módulo M es Σ-inyectivo si y sólo si toda extensión esencial de $M^{(\aleph_0)}$ es una suma directa de módulos inyectivos.*

Demostración. Sean R un anillo y M un R-módulo.

Supongamos que toda extensión esencial de $M^{(\aleph_0)}$ es una suma directa de módulos inyectivos, sea E una cápsula inyectiva de M, tenemos entonces que $M^{(\aleph_0)} \subseteq_{es} E^{(\aleph_0)}$, por hipótesis, el mismo $M^{(\aleph_0)}$ es una suma directa de módulos inyectivos, por lo tanto $M^{(\aleph_0)}$ es un sumando local de $E^{(\aleph_0)}$. Por el teorema anterior, E es Σ-inyectivo, entonces también lo es $E^{(\aleph_0)}$, por lo tanto $E^{(\aleph_0)}$ tiene una descomposición inescindible que complementa sumandos directos, entonces cualquier sumando local de $E^{(\aleph_0)}$ es un sumando directo, por lo tanto $M^{(\aleph_0)}$es un sumando directo de $E^{(\aleph_0)}$, con lo cual concluimos que $M^{(\aleph_0)}$ es inyectivo y por lo tanto M es Σ-inyectivo.

El regreso es claro ya que si M es Σ-inyectivo, entonces $M^{(\aleph_0)}$ es inyectivo, por lo cual no tiene una extensión esencial propia, por lo cual el hecho de que $M^{(\aleph_0)}$ sea una suma directa de módulos inyectivos se cumple trivialmente. □

Teorema 8.3. *Un anillo R es ΣV-anillo derecho si y sólo si para todo R-módulo derecho simple S se cumple que toda extensión esencial finita de $S^{(\aleph_0)}$es una suma directa de módulos inyectivos.*

Demostración. Sea R un anillo. supongamos que todo R-módulo derecho simple S cumple que toda extensión esencial finita de $S^{(\aleph_0)}$es una suma directa de módulos inyectivos, entonces por el corolario anterior, todo R-módulo derecho simple S es Σ-inyectivo, por lo tanto R es ΣV-anillo derecho.

El regreso es claro ya que si suponemos que R es ΣV-anillo derecho, entonces todo R-módulo simple derecho S es Σ-inyectivo, entonces $S^{(\aleph_0)}$ es inyectivo, por lo cual no tiene una extensión esencial propia, por lo cual el hecho de que $S^{(\aleph_0)}$ sea una suma directa de módulos inyectivos se cumple trivialmente. □

Definición 8.9. Un anillo R es llamado c. f. d. (cociente finito-dimensional) relativo a un módulo M si ningún R-módulo derecho cíclico contiene una suma directa infinita de módulos isomorfos a submódulos de M.

Proposición 8.9. *Si un R-módulo derecho M es Σ-inyectivo, entonces R es c. f. d. relativo a M.*

Demostración. Sea R un anillo y M un R-módulo Σ-inyectivo. Supongamos que R no es c. f. d. relativo a M, entonces existe un R-módulo derecho cíclico C que contiene una suma directa infinita de módulos $\bigoplus_{i\in I} V_i$ isomorfos a submódulos de M, tomemos $M_i = M\ \forall i \in I$. Puesto que M es Σ-inyectivo, $\bigoplus_{i\in I} M_i$ es inyectivo, entonces el monomorfismo $\varphi : \bigoplus_{i\in I} V_i \to \bigoplus_{i\in I} M_i$ que incluye a V_i en M_i, se extiende a un monomorfismo $f : C \to \bigoplus_{i\in I} M_i$. Ahora puesto que C es cíclico, existe un subconjunto finito $J \subseteq I$ tal que $f(C) \subseteq \bigoplus_{j\in J} M_j$. Por lo tanto $f(V_k) \cap M_k \subseteq f(C) \cap M_k = 0$ para toda k que no pertenece a J, lo cual es una contradicción con el hecho de que $f(V_i) = \varphi(V_i) \subseteq M_i$ para toda $i \in I$. Por lo tanto R es es c. f. d. relativo a M. $\square$

Proposición 8.10. *Sean R un ΣV-anillo derecho y S un R-módulo simple, entonces R es c. f. d. relativo a S.*

Demostración. Sean R un ΣV-anillo derecho y S un R-módulo simple, entonces S es Σ-inyectivo, por lo tanto por la proposición anterior R es c. f. d. relativo a S. $\square$

Capítulo 9

Apéndice. Ordinales

Definición 9.1. Sea R una relación binaria en un conjunto X, decimos que:
R es reflexiva si $\forall a \in X$ tenemos que aRa;
R es simétrica si $\forall a, b \in X$ tenemos que aRb implica bRa;
R es antisimétrica si $\forall a, b \in X$ tenemos que aRb y $a \neq b$ implica $\neg bRa$;
R es conectada si $\forall a, b \in X$ tenemos que aRb o bRa;
R es transitiva si $\forall a, b, c \in X$ tenemos que aRb y bRc implica aRc.

Definición 9.2. Un orden parcial de un conjunto X es una relación binaria en X que es reflexiva, antisimétrica y transitiva. Usualmente los ordenes parciales se denotan con el símbolo $\leq$.

Un conjunto parcialmente ordenado (copo) consiste de un conjunto X y un orden parcial $\leq$ en el conjunto X, se denota como el par ordenado $(X, \leq)$.

Definición 9.3. Tomemos ahora un copo $(X, \leq)$ y $Y \subseteq X$. Un elemento $a \in Y$ es un elemento mínimo si y sólo si $\nexists b \in Y$ tal que $b < a$.

Un copo $(X, \leq)$ es llamado bien fundado si todo subconjunto no vacío de X tiene elemento mínimo (en este caso diremos que la relación es bien fundada).

Lema 9.1. *Sea $(X, \leq)$ un copo. $(X, \leq)$ es bien fundado si y sólo si no hay sucesiones $\{a_n\}_{n=0}^{\infty}$ de elementos de X tal que $a_{n+1} < a_n$ para todo n, es decir, no hay sucesiones $\{a_n\}_{n=0}^{\infty}$tal que $a_0 > a_1 > a_2 > ...$*

Demostración. Sea $(X, \leq)$ un copo. Supongamos que el copo no es bien fundado. Sea $Y \subseteq X$ tal que Y no tiene elemento mínimo. Sea $a_o \in Y$. Como a_0 no es elemento mínimo en Y, podemos encontrar $a_1 \in Y$ tal que $a_o < a_1$, otra vez $a_1$no es elemento mínimo en Y entonces podemos encontrar un $a_2 \in Y$ tal que $a_2 < a_1$, entonces procediendo de esta manera podemos obtener una sucesión $\{a_n\}_{n=0}^{\infty}$ tal que $a_0 > a_1 > a_2 > ...$

Ahora supongamos que existe una sucesión$\{a_n\}_{n=0}^{\infty}$tal que $a_0 > a_1 > a_2 > ...$ Sea $Y = \{a_n\}_{n=0}^{\infty}$, entonces claramente por construcción $Y \subseteq X$ no tiene elemento mínimo, y por lo tanto $(X, \leq)$ no es bien fundado. □

Teorema 9.1. *Sea $(X, \leq)$ un copo. Entonces existe un conjunto Y de subconjuntos de X tal que $(X, \leq) \cong (Y, \subseteq)$.*

Demostración. Sea $(X, \leq)$ un copo, para cada $a \in X$ definamos $z_a = \{b \in X | b \leq a\}$, y $Y = \{z_a | a \in X\}$. Definamos la función $\pi : X \to Y$ por $\pi(a) = z_a$. Veamos que πes una biyección, simplemente por construcción de Y, π es sobre, supongamos ahora que $z_a = z_b$ entonces por definición de z_a tenemos que $b \leq a$ y análogamente por definición de z_b tenemos que $a \leq b$, entonces $a = b$, entonces πes inyectiva y por lo tanto biyectiva. Más aún por, por definición, tenemos que si $a_1 \leq a_2 \Longleftrightarrow z_{a_1} \subseteq z_{a_2}$, por lo tanto π es un isomorfismo entre X y Y. □

Definición 9.4. Un orden total (u orden lineal) de un conjunto X es un orden parcial conectado de X. Un conjunto totalmente ordenado (coto) es una pareja $(X, \leq)$ tal que $\leq$ es un orden total de X.

Definición 9.5. Un buen orden de un conjunto X es un orden total bien fundado del conjunto X. Un conjunto bien ordenado (cobo) es una pareja $(X, \leq)$ tal que $\leq$ es un buen orden de X.

Observemos que en un coto $(X, \leq)$ los elementos mínimos de conjuntos no vacíos $Y \subseteq X$ son únicos, en este caso diremos que son elementos menores. Esto gracias a que en un coto la relación es conectada.

Teorema 9.2. *Sean $(X, \leq)$ un cobo y $E \subseteq X$ tal que:*
(i) el elemento menor de X pertenece a E;
(ii) para cualquier $x \in X$, si $\forall y \in X$ tal que $y < x$ implica $y \in E$, entonces $x \in E$.
Entonces $E = X$.

Demostración. Sean $(X, \leq)$ un cobo y $E \subseteq X$ tal que se cumplen (i) y (ii). Supongamos que $E \neq X$. Consideremos el conjunto $X - E$, como $(X, \leq)$ es cobo entonces $X - E$ tiene elemento menor, sea x dicho elemento menor, ahora por (i) x no es el elemento menor de X y por la elección de x tenemos que si $y < x$ entonces $y \in E$, entonces por (ii) $x \in E$, contradicción ya que $x \in X - E$.

Sean $(X, \leq)$, $(X', \leq')$ cobos, una función $f : X \to X'$ es un isomorfismo de orden si y sólo si f es biyectiva y $x < y \Longrightarrow f(x) <' f(y)$. En caso de que dicho isomorfismo exista lo denotaremos por $f : X \cong X'$. □

Teorema 9.3. *Sean $(X, \leq)$ un cobo, $Y \subseteq X$, $f : X \cong Y$. Entonces $\forall x \in X$, $x \leq f(x)$.*

Demostración. Sean $(X, \leq)$ un cobo, $Y \subseteq X$ tal que $f : X \cong Y$ y $E = \{x \in X | f(x) < x\}$. Por demostrar que $E = \emptyset$. Supongamos lo contrario, entonces, como $(X, \leq)$ es cobo y $\emptyset \neq E \subseteq X$, E tiene elemento menor, x_0. Como $x_0 \in E$ tenemos que $f(x_0) < x_0$. Sea $x_1 = f(x_0)$. Como $x_1 < x_0$aplicando f tenemos que $f(x_1) < f(x_0)$ ya que f es isomorfismo de orden, sustituyendo tenemos que $f(x_1) < x_1$. entonces $x_1 \in E$, pero $x_1 < x_0$, lo que contradice la elección de x_0 como el elemento menor de E. Por lo tanto $E = \emptyset$ y $\forall x \in X, x \leq f(x)$. □

Teorema 9.4. *Sean $(X, \leq)$, $(X', \leq')$ cobos. Si $(X, \leq) \cong (X', \leq')$, entonces existe un único isomorfismo de orden $f : X \cong X'$.*

Demostración. Sean $(X, \leq)$, $(X', \leq')$ cobos tal que $(X, \leq) \cong (X', \leq')$ supongamos que $f : X \cong X'$ y $g : X \cong X'$. Sea $h = f^{-1} \circ g$. Claramente $h : X \cong X$. Entonces por el teorema anterior $x \leq h(x)$ $\forall x \in X$. Entonces aplicando f, tenemos que para cualquier $x \in X$, $f(x) \leq f(h(x)) = g(x)$,entonces $f(x) \leq g(x)$, análogamente obtendremos que $g(x) \leq f(x)$ $\forall x \in X$. Por lo tanto $f = g$. $\square$

Definición 9.6. Sea $(X, \leq)$ un cobo, $a \in X$. Definiremos el segmento X_a de X como $X_a = \{x \in X | x < a\}$.

Teorema 9.5. *Sea $(X, \leq)$ un cobo. Entonces no existe ningún isomorfismo de X sobre un segmento de X.*

Demostración. Sea $(X, \leq)$ un cobo. Supongamos que $f : X \cong X_a$ para algún $a \in X$. entonces por un *resultado anterior* tenemos que $x \leq f(x)$ $\forall x \in X$. En particular, $a \leq f(a)$, pero $ran(f) = X_a$ entonces $f(a) \in X_a$ y por definición de X_a tenemos que $f(a) < a$, contradicción. $\square$

Teorema 9.6. *Sean $(X, \leq)$ un cobo y $A = \{X_a | a \in X\}$. Entonces $(X, \leq) \cong (A, \subseteq)$.*

Demostración. Sean $(X, \leq)$ un cobo y $A = \{X_a | a \in X\}$, definamos $f : X \to A$ por $f(a) = X_a$. Por demostrar f es un isomorfismo de orden. Simplemente por construcción de A la función es sobre. Sean $a, b \in X$ tal que $a \neq b$, como $(X, \leq)$es cobo sin pérdida de generalidad, supongamos que $a < b$ entonces $X_a \subset X_b$, por definición de segmento, entonces $X_a \neq X_b$, entonces f es inyectiva, por lo tanto f es biyectiva y además también es de orden, como se vio en la demostración de la inyectividad. Por lo tanto f es isomorfismo de orden. $\square$

Definición 9.7. Un ordinal es un cobo $(X, \leq)$ tal que $X_a = a$ $\forall a \in X$.

Observación 9.1. Sea $(X, \leq)$ un ordinal. Entonces $\forall a, b \in X$, tenemos que $a < b$ si y sólo si $X_a \subset X_b$si y sólo si $a \subset b$.

La primera equivalencia se da gracias a la definición de segmento (de hecho basta con que$(X, \leq)$ sea cobo), y la segunda se da gracias a la definición de ordinal.

Teorema 9.7. *Sea $(X, \leq)$ un ordinal. Si $a \in X$, entonces X_a es un ordinal.*

Demostración. Sean $(X, \leq)$ un ordinal, $a \in X$ y $b \in X_a$. Entonces se define $(X_a)_b$ por $(X_a)_b = \{x \in X_a | x < b\} = \{x \in X | x < a \wedge x < b\}$ y como $a < b$ tenemos que $\{x \in X | x < a \wedge x < b\} = \{x \in X | x < b\} = X_b = b$ ya que $(X, \leq)$ es ordinal, entonces con estos vemos que $(X_a)_b = X_b = b$, por lo tanto X_a es un ordinal. $\square$

Teorema 9.8. *Sea $(X, \leq)$ un ordinal. Si $Y \subset X$. Si Y es un ordinal, entonces $Y = X_a$ para algún $a \in X$.*

Demostración. Sean $(X, \leq)$ un ordinal y $Y \subset X$. Supongamos que Y es un ordinal, sea $a \in X$ el elemento menor de $X - Y$ (que existe ya que X es cobo), entonces $X_a \subseteq Y$ por definición de segmento, ahora tomemos $b \in Y$, entonces como Y es ordinal tenemos que $Y_b = b = X_b$, entonces si $a < b$ tenemos que $a \in X_b$, entonces $a \in Y_b$ y por lo tanto $a \in Y$, pero eso no puede ser ya que $a \in X - Y$. Por lo tanto $b \leq a$, pero $b \neq a$ ya que $b \in Y$ y $a \in X - Y$, entonces $b < a$ y $b \in X_a$, esto muestra que $Y \subseteq X_a$, y como a es el elemento menor de $X - Y$, podemos concluir que $Y = X_a$. □

Teorema 9.9. *Si X, Y son ordinales, entonces $X \cap Y$ es un ordinal.*

Demostración. Sean X, Y ordinales y $a \in X \cap Y$, entonces $X_a = a = Y_a$, es decir, $\{x \in X | x < a\} = a = \{y \in Y | y < a\}$, entonces $a = \{z \in X \cap Y | z < a\} = (X \cap Y)_a$, por lo tanto $X \cap Y$ es un ordinal. □

Teorema 9.10. *Sean X, Y son ordinales, si $X \neq Y$, entonces uno es segmento del otro.*

Demostración. Sean X, Y son ordinales tales que $X \neq Y$, si $X \subset Y$ o $Y \subset X$ como ambos son ordinales entonces *por un resultado anterior*, obtendríamos que uno es segmento del otro. Entonces supongamos lo contrario, consideremos ahora $X \cap Y$, por el teorema anterior $X \cap Y$ es un ordinal y como está contenido en X y Y, tenemos que es segmento de ambos, es decir, para algunos $a \in X$ y $b \in Y$ tenemos $a = X_a = X \cap Y = Y_b = b$, entonces $a = b$, pero $a \in X$ y $b \in Y$, por lo tanto $a = b \in X \cap Y$, pero $X_a = X \cap Y$, entonces $\forall z \in X \cap Y$ $z < a$, en particular $a < a$, contradicción. Por lo tanto si $X \neq Y$ ordinales tenemos que uno es subconjunto del otro y por lo tanto segmento. □

Teorema 9.11. *Si X, Y son ordinales isomorfos, entonces son iguales.*

Demostración. Sean X y Y cardinales tales que $f : X \cong Y$, probaremos ahora que $f = id_x$, consideremos $E = \{x \in X | f(x) \neq x\}$ y probemos que $E = \emptyset$. Supongamos lo contrario, entonces como E es un subconjunto no vacío de un cobo, tiene elemento menor, sea $a \in E$ dicho elemento, entonces si $x < a$ tenemos que $f(x) = x$, entonce $X_a = Y_{f(a)}$, pero $a = X_a = Y_{f(a)} = f(a)$, es decir, $a = f(a)$, contradicción ya que $a \in E$. Por lo tanto $E = \emptyset$ y $f = id_x$, lo que muestra que si dos ordinales son isomorfos, entonces son iguales. □

Teorema 9.12. *Sea $(X, \leq)$ un cobo tal que $\forall a \in X$, X_a es isomorfo a un ordinal. Entonces X es isomorfo a un ordinal.*

Demostración. Sea $(X, \leq)$ un cobo tal que $\forall a \in X$, X_a es isomorfo a un ordinal, entonces $\forall a \in X$ tenemos el isomorfismo $g_a : X_a \cong Z(a)$ con $Z(a)$ ordinal. *Por un resultado anterior* $Z(a)$ es único y por lo tanto g_a también. Entonces esto define una función de X a $W = \{Z(a) | a \in X\}$ de la siguiente manera: sea $f : X \to W$ tal que $f(a) = Z(a)$. Afirmación: si $x, y \in X$, entonces $x < y$ implica $Z(x) \subset Z(y)$.

Prueba de la afirmación: Sean $x, y \in X$, tal que $x < y$. Consideremos el isomorfismo $g_x : X_x \cong Z(x)$. Puesto que $X_x = \{z \in X | z < x\} = \{z \in X | z <$

$x \wedge z < y\}$ ya que $x < y$, además $\{z \in X | z < x \wedge z < y\} = \{z \in X_y | z < x\} = (X_y)_x$ por definición de segmento, entonces podemos tomar $g_{(y,x)} : X_x \cong (Z(y))_{g_y(x)}$. Ahora, como $Z(y)$ es un ordinal y $(Z(y))_{g_y(x)}$ es un segmento de $Z(y)$, entonces $(Z(y))_{g_y(x)}$ es un ordinal, por lo tanto $(Z(y))_{g_y(x)} = Z(x)$, ya que ambos ordinales son isomorfos a X_x y por lo tanto entre sí y habíamos visto que si dos ordinales son isomorfos, entonces son iguales. Por lo tanto al ser $Z(x)$ un segmento de $(Z(y))_{g_y(x)}$ tenemos que $Z(x) \subset Z(y)$, con esto queda demostrada la afirmación.

Entonces por construcción de f, esta es biyectiva y por la afirmación, concluimos que f es un isomorfismo de orden entre $(X, \leq)$ y $(W, \subseteq)$. Por lo tanto en particular $(W, \subseteq)$ es un cobo. Para terminar la demostración, sólo hace falta ver que W es un ordinal.

Sea $y \in X$, como $Z(y)$ es un ordinal, tenemos que $x < y$ implica $(Z(y))_{g_y(x)} = g_y(x)$ (por definición de ordinal) y como $(Z(y))_{g_y(x)} = Z(x)$, entonces $x < y$ implica $Z(x) = g_y(x)$. Por lo tanto $W_{z(y)} = \{Z(x) | Z(x) \subset Z(y)\} = \{Z(x) | x < y\} = \{g_y(x) | x < y\} = g_y(X_y) = Z(y)$, es decir, $W_{z(y)} = Z(y)$, entonces W es un ordinal, ya que $Z(y)$ era un elemento cualquiera de W. Con esto queda terminada la demostración. □

Teorema 9.13. *Todo cobo es isomorfo a un único ordinal.*

Demostración. Sea $(X, \leq)$ un cobo, la unicidad se sigue de que dos ordinales isomorfos son iguales, por lo que sólo falta demostrar la existencia del ordinal isomorfo a $(X, \leq)$, y para esto sólo basta mostrar que $\forall a \in X$, X_a es isomorfo a un ordinal (por el teorema anterior).

Sea$E = \{a \in X |\ X_a \text{ no es isomorfo a un ordinal}\}$, probemos que $E = \emptyset$. Supongamos lo contrario, otra vez E tiene elemento menor, sea $a \in E$ dicho elemento, entonces, si $x < a$ se tiene que X_x es isomorfo a un ordinal, pero si $x < a$ entonces $X_x = (X_a)_x$, con esto vemos que todo segmento de X_a es un ordinal y por el teorema anterior el mismo X_a es un ordinal, contradicción con el hecho de que $a \in E$. Por lo tanto $E = \emptyset$ y todo segmento de X es isomorfo a un ordinal y por lo tanto el mismo X también. □

Ahora dado que todo cobo es isomorfo a un único ordinal, esto les da un cierto tipo de «medida» o «longitud». Así que podríamos decir que la longitud de un cobo es igual al ordinal al que es isomorfo.

Un poco de notación, contemporáneamente es común usar letras griegas minúsculas para denotar a los ordinales, así que seguiremos esa notación en general.

Observación 9.2. Usando los teoremas anteriores ahora podemos notar lo siguiente:

Para α y β ordinales son equivalentes:

i) $\alpha \subset \beta$

ii) $a < \beta$

iii) $\alpha = \beta_a$ para algún $a \in \beta$

iv) $\alpha = a$ para algún $a \in \beta$

v) $\alpha \in \beta$

Observación 9.3. Todo ordinal $\alpha = \{\beta | \beta < \alpha\}$

En otras palabras, un ordinal es el conjunto de todos los ordinales menores a él.

Podemos ver entonces ahora que el primer ordinal no debe tener ordinales menores a él, por lo tanto el primer ordinal debe ser el conjunto vacío ($\emptyset$) y lo denotaremos por 0 ($0 = \emptyset$). Ahora el segundo ordinal tener al primero como el elemento y nada más, entonces el segundo debe ser $\{0\}$y lo denotaremos por 1 ($1 = \{0\}$). De la misma manera el tercer ordinal debe ser $\{0, 1\}$ y lo denotaremos por 2 ($2 = \{0, 1\}$) y finalmente siguiendo este proceso inductivamente por demos decir quien es el n-ésimo ordinal y será nada menos que $\{0, 1, 2, ..., n-1\}$ ($n = \{0, 1, 2, ..., n-1\}$). Podemos notar que el ordinal n tiene justamente n elementos, sin embargo todos estos ordinales son finitos, así que podemos preguntarnos por el primer ordinal infinito y resulta ser justamente $\{01, 2, 3, ..., n, n+1, ...\}$ al cual denotaremos por ω ($\omega = \{01, 2, 3, ..., n, n+1, ...\}$), ahora quien será el siguiente, pues siguiendo el razonamiento usado para el caso de los ordinales finitos obtenemos que que el siguiente ordinal debe ser $\{\{01, 2, 3, ..., n, n+1, ..., \omega\}$.

Ya con esto en general, podemos decir que si α es un ordinal, entonces el siguiente a él será $\alpha \cup \{\alpha\}$. Por notación, diremos que el primer ordinal siguiente a α será $\alpha + 1$, el (ordinal) sucesor a α. Por lo tanto $\alpha + 1 = \alpha \cup \{\alpha\}$.

Ahora observando a ω nos damos cuenta de que no tiene elemento máximo, entonces no puede ser el sucesor de otro ordinal, con esto nos damos cuenta de que no todos lo ordinales son sucesores de algún otro, a estos ordinales que son como ω los llamaremos ordinales límite. En caso de que sean el sucesor de algún otro ordinal los llamaremos ordinales sucesor.

Ahora definamos lo que es una sucesión, una sucesión es una función que tiene como dominio un ordinal. Si f es una sucesión y $dom(f) = \alpha$, entonces diremos que f es una $\alpha -$ *secuencia*. Si $f(\beta) = x_\beta \ \forall \beta < \alpha$, entonces podemos denotar a f por $\{x_\beta | \beta < \alpha\}$. Además si $\gamma < \alpha$, $\{x_\beta | \beta < \gamma\}$ denota $f(\gamma)$.

En particular podemos observar que $\{a_n\}_{n=0}^{\infty} = \{a_n | n < \omega\}$.

Una variación de transitividad, diremos que un conjunto X es transitivo si y sólo si $x \in X$ y a$\in x$ implican $a \in X$.

Veamos una caracterización de los ordinales.

Lema 9.2. *Un conjunto X es un ordinal si y sólo si es transitivo y totalmente ordenado por $\in$.*

Demostración. Primero supongamos que X es un ordinal, es decir, $(X, \subset)$ es un cobo y se cumple que a, $a = X_a$. Puesto que $x \in X$ implica $x \subseteq X$, entonces X es transitivo, y sabemos que X al ser ordinal está totalmente ordenado por $\in$.

Ahora, supongamos que X es un conjunto transitivo totalmente ordenado por $\in$. Por el axioma de fundación, X es bien ordenado por $\in$. Tomemos $x \in X$, puesto que X es transitivo, $a \in b$ implica $a \in X$, entonces $b = \{a \in X | a \in b\}$, es decir, $b = X_b$. Por lo tanto X es un ordinal. $\square$

Lema 9.3. *Si α es un ordinal, entonces $\alpha \cup \{\alpha\}$es un ordinal, es decir, el ordinal sucesor en efecto es un ordinal.*

Demostración. Sea αun ordinal. Dado que α es totalmente ordenado por $\in$, entonces $\alpha \cup \{\alpha\}$, además claramente sigue siendo transitivo, entonces por el lema anterior $\alpha \cup \{\alpha\}$ es un ordinal. □

Lema 9.4. *Si A es un conjunto de ordinales, entonces $\cup A$ es un ordinal.*

Demostración. Sean A un conjunto de ordinales y $x \in a \in \cup A$. Tenemos que para algunos $b \in A$, $a \in b$. Puesto que b es un ordinal, tenemos que $x \in a \in b$ implica $x \in b$. Por lo tanto $x \in \cup A$, es decir se cumple la transitividad.

Tomemos ahora $x, y \in \cup A$. Escogemos $a, b \in A$ tal que $x \in a$ y $y \in b$, sin pérdida de generalidad supongamos que $a \subseteq b$, entonces $x, y \in b$. Por lo tanto tenemos que $x \in y$ o $y \in x$ (o incluso $x = y$). Por lo tanto $\cup A$ es totalmente ordenado por $\in$. Por lo tanto $\cup A$ es un ordinal. □

Esto aunado a los axiomas de Zermelo-Fraenkel nos garantiza la existencia de los ordinales infinitos, entonces nuestros anteriores resultados quedan bien fundados.

Definición 9.8. Dados dos ordinales α y β, definimos el ordinal suma $\alpha + \beta$ como el ordinal que continua con α y continua más allá de α justamente β pasos.

Formalmente se usa $A = (\alpha \times \{0\}) \cup (\beta \times \{1\})$, se define un buen orden de A de la siguiente manera: $(\mu, i) <_A (\nu, j)$ si y sólo sí $(i < j)$ o $(i = j$ y $\mu < \nu)$

Entonces $\alpha + \beta$ es el ordinal isomorfo a $(A, <_A)$.

Podemos observar que esta definición de suma con la que habíamos usado para referirnos al ordinal sucesor.

Lema 9.5. *La suma de ordinales es asociativa, es decir, $\alpha+(\beta+\gamma) = (\alpha+\beta)+\gamma$*

Demostración. Sean α, β y γ ordinales, por demostrar $\alpha+(\beta+\gamma) = (\alpha+\beta)+\gamma$.

$\alpha + (\beta + \gamma)$ lo podemos asociar con $A = (\alpha \times \{0\}) \cup ((\beta \times \{1\}) \cup (\gamma \times \{2\}))$ y a $(\alpha + \beta) + \gamma$ lo podemos asociar con $A' = ((\alpha \times \{0\}) \cup (\beta \times \{1\})) \cup (\gamma \times \{2\})$ y como sabemos que la unión es asociativa entonces $A = A'$ y por lo tanto los ordinales isomorfos a $(A, <_A)$ y a $(A', <_{A'})$ son iguales, es decir, $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$. □

Observación 9.4. La suma de ordinales no es conmutativa. Un ejemplo de esto es:

$1 + \omega \neq \omega + 1$ ya que $1 + \omega = \omega$ y $\omega + 1 > \omega$, esto gracias a que $\forall n \in \mathbb{N}$ tenemos que $n + \omega = \omega$, justo por la infinitud de ω.

Por último veamos los principios de inducción sobre ordinales.

Teorema 9.14. *(Principio de Inducción Transfinita) Sea $P(x)$ una propiedad. Supongamos que, para todos los números ordinales α,*

si $P(\beta)$ se cumple para todo $\beta < \alpha$, entonces $P(\alpha)$ se cumple.

Entonces $P(\alpha)$ su cumple para todos los ordinales α.

Demostración. Supongamos que $P(\alpha)$ falla para algún ordinal α. Sea $A = \{\beta \leq \alpha | P(\beta) \text{ falla}\}$, entonces $A \neq \emptyset$ y por lo tanto tiene un primer elemento β_0. Entonces tenemos que $P(\beta_0)$ falla, pero $P(\gamma)$ se cumple $\forall \gamma < \beta_0$, lo cual contradice el hecho de que «si $P(\beta)$ se cumple para todo $\beta < \alpha$, entonces $P(\alpha)$ se cumple». $\square$

Teorema 9.15. *(Segunda Versión del Principio de Inducción Transfinita) Sea $P(x)$ una propiedad. Supongamos que:*

(a) $P(0)$ se cumple

(b) $P(\alpha)$ implica $P(\alpha + 1)$ para todos los ordinales α

(c) Para todo ordinal límite $\alpha \neq 0$, si $P(\beta)$ su cumple para todo $\beta < \alpha$, entonces se cumple $P(\alpha)$.

Entonces $P(\alpha)$ se cumple para todo los ordinales α.

Demostración. Basta ver que (a), (b) y (c) implican la hipótesis del principio original. Sea α un ordinal tal que $P(\beta)$ se cumple $\forall \beta < \alpha$. Si $\alpha = 0$, entonces $P(\alpha)$ se cumple por (a). Si α es ordinal sucesor, entonces $\exists \beta$ tal que $\alpha = \beta + 1$, por hipótesis $P(\beta)$ se cumple y por (b) $P(\alpha)$ también se cumple. Por último si α es un ordinal límite distinto de 0, entonces $P(\alpha)$ se cumple por (c). $\square$

Bibliografía

[1] F.Kasch. Modules and Rings. Academic Press. 1982

[2] Anderson, Fuller. Rings and Categories of Modules. Springer-Verlag. 1992

[3] Alberto Facchini. Module Theory Endomorphism Rings and Direct Sum Decompositions in Some Classes of Modules. Springer-Basel. 2012

[4] S. K. Jain, Ashish K. Srivastava, Askar A. Tuganbaev. Cyclic Modules and the Structure of Rings. Oxford University Press, USA. 2012

[5] Robert B. Ash. Abstract Algebra: The Basic Graduate Year. Dover Publicatons. 2006

[6] Wisbauer, R. Foundations of Module and Ring Theory,Gordon and Breach Science Publishers, 1991.