BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA
FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS
COLEGIO DE MATEMÁTICAS

LA FÓRMULA DE AUSLANDER-BUCHSBAUM

TESIS
PRESENTADA COMO REQUISITO PARA OBTENER EL TÍTULO DE
LICENCIADO EN MATEMÁTICAS

PRESENTA
JORGE SÁNCHEZ MORALES

DIRECTOR DE TESIS
PROF. ÁNGEL CONTRERAS PÉREZ

PUEBLA, PUE.
MARZO DE 2011

A Carmen, Andrés, Vale y Ángel

Índice general

Introducción **1**

1. Módulos **3**
1.1. Módulos y morfismos de módulos 3
1.2. Sucesiones exactas 7
1.3. $Hom_R(M, N)$ 8
1.4. Suma y producto directo 11
1.5. Módulos libres 18
1.6. Módulos finitamente generados 20
1.7. Módulos noetherianos 23
1.8. Producto tensorial de módulos 28
1.9. Módulos proyectivos 36
1.10. Módulos inyectivos 38

2. Categorías **43**
2.1. Categorías y funtores 43

3. Homología **51**
3.1. Grupos de homología 51
3.2. Sucesiones exactas largas 55
3.3. Resoluciones 59
3.4. Funtores derivados 64
3.5. Dimensión proyectiva 74

4. Profundidad **77**
4.1. Sucesiones regulares 77
4.2. Sucesiones regulares maximales 82
4.3. Profundidad y codimensión 85
4.4. Fórmula de Auslander-Buchsbaum 87

A. Localización **93**

B. Descomposición Primaria **97**
B.1. Primos asociados 97
B.2. Descomposición primaria 99
B.3. Soporte de un módulo 102

Bibliografía **105**

Introducción

En su artículo de 1956, "A Theorem of Homological Algebra", Rees [15] introduce por vez primera el concepto de *grado* o *profundidad* de un ideal, concepto que es, después del de *dimensión*, tal vez el invariante numérico más importante de un ideal, y que se convirtió en una herramienta importante dentro del algebra homológica generando el desarrollo de nuevos campos de estudio. La profundidad estará definida en términos de sucesiones regulares y puede ser medida por la no anulación de ciertos elementos del funtor Ext. Esta conexión abre al álgebra conmutativa a la aplicación de métodos del álgebra homológica.

El número por el cual viene dada la profundidad de un ideal no puede considerarse en sí mismo como un ente aislado, pues de ser así, habría muy poco que decir acerca de él. Por lo tanto, las propiedades de este número consisten precisamente de sus relaciones con otros números. Así que mostraremos algunas relaciones entre profundidad y otros conceptos, tales como *codimensión* y *dimensión proyectiva*, el primero de ellos de naturaleza geométrica y el otro de naturaleza homológica. Una de estas relaciones se establece mediante la *Fórmula de Auslander-Buchsbaum*, la cual afirma que si $M \neq 0$ es un módulo finitamente generado sobre un anillo local noetheriano $(R, \mathfrak{m})$ y la dimensión proyectiva de M en R es finita, entonces ésta es igual a la profundidad de $\mathfrak{m}$ en R, menos la profundidad de $\mathfrak{m}$ en M.

En 1957-58, Serre impartió un curso de multiplicidades en el Collège de France, parte de ese curso se enfocó en la desigualdad $pd_R(M) \leq pd_R(S) + pd_S(M)$ para un módulo M sobre una R-álgebra S. Auslander y Buchsbaum notaron que los métodos de Serre podían ser utilizados para estudiar la conexión entre codimensión y multiplicidad sobre un anillo local. Esto los condujo a la fórmula mencionada.

El objetivo fundamental de esta tesis es demostrar la Fórmula de Auslander-Buchsbaum, y con el propósito de hacer autocontenido al máximo este trabajo, para que puedan usarlo como texto en un curso de álgebra homológica quienes tengan al menos los conocimientos básicos de teoría de grupos y teoría de anillos, se desarrolló de la siguiente manera. El capítulo 1 trata de la teoría básica de módulos y algunos módulos especiales, entre los que se encuentran los módulos libres, finitamente generados, noetherianos, proyectivos e inyectivos. El segundo y el tercer tipo de estos módulos aparecen nuevamente hasta la última sección del capítulo tres. A partir de ese momento es cuando se verá la importancia de las condiciones de finitud impuestas a los módulos que irán apareciendo. En el capítulo 2 se dan las nociones básicas del lenguaje categórico que se usan en los dos capítulos siguientes.

En el capítulo 3 se definen la categoría de complejos, la homotopía, los funtores de homología, las resoluciones proyectivas e inyectivas de módulos y se usan para definir los funtores derivados izquierdos y derechos, los funtores Ext y Tor, y por tanto a los grupos abelianos $Ext_R^n(M,N)$ y $Tor_n^R(M,N)$. La dimensión proyectiva de un módulo se estudia en la última sección de este capítulo, en donde se utiliza al funtor Tor para dar una equivalencia de la dimensión proyectiva.

En el capítulo 4 se muestra cómo están relacionadas las nociones de profundidad y codimensión, profundidad y dimensión de Krull, y se termina con la demostración de la Fórmula de Auslander-Buchsbaum. Además se incluyen dos apéndices para dar claridad a algunos conceptos y resultados que son utilizados únicamente en el capítulo 4.

Capítulo 1

Módulos

Al mencionar a un anillo R, convenimos en que se trata de un anillo conmutativo con elemento unitario, salvo aclaración.

1.1. Módulos y morfismos de módulos

Definición 1.1.1 *Sea R un anillo. M es un R-**módulo** (izquierdo) si M es un grupo abeliano y si hay una función de $R \times M$ en M tal que a $(r, m) \in R \times M$ le asocia $rm \in M$, y además para $r, s \in R$ y $m, n \in M$ se cumple que:*

(1) $r(m + n) = rm + rn.$

(2) $(r + s)m = rm + sm.$

(3) $(rs)m = r(sm).$

(4) $1m = m.$

Similarmente se definen los R-módulos derechos.

Ejemplos.

1. Si R es un campo, todo R-espacio vectorial es un R-módulo.
2. Si G es abeliano, G es un $\mathbb{Z}$-módulo.
3. Si R es un anillo e I un ideal de R, I es un R-módulo.

Definición 1.1.2 *Sean M un R-módulo y $N \subseteq M$. N es **submódulo** de M si N es un R-módulo con respecto a las operaciones que hacen de M un R-módulo.*

Ejemplos.

1. Si R es un anillo e $I \subseteq R$, entonces I es un submódulo de R si y sólo si I es un ideal de R.

2. Sea $(M_i)_{i\in I}$ una familia de submódulos de un R-módulo M. La **suma**

$$\sum_{i\in I} M_i = \Big\{ \sum_{i\in I} m_i : m_i \in M_i \text{ y } m_i = 0 \text{ para casi todo } i \in I \Big\}$$

   es un submódulo de M.

3. Si I es un ideal de R y M es un R-módulo, entonces

$$IM = \Big\{ \sum a_i m_i : a_i \in I,\ m_i \in M \ y \ a_i = 0 \text{ para casi todo i } \Big\}$$

   es un submódulo de M.

Definición 1.1.3 *Sean M y N dos R-módulos. Diremos que $f : M \to N$ es un* ***homomorfismo*** *o* ***morfismo*** *de R-módulos (R-morfismo) si satisface:*

(1) *f es un homomorfismo de grupos.*

(2) *Para cualesquiera $r \in R$ y $m \in M$, $f(rm) = rf(m)$.*

Ejemplos.

1. Si M es un R-módulo, $1_M : M \to M$ es un morfismo de R-módulos.

2. Si $f : M \to N$ y $g : N \to T$ son dos morfismos de R-módulos entonces $g \circ f : M \to T$ es un morfismo de R-módulos.

3. Si $f, g : M \to N$ son morfismos de R-módulos entonces $f + g : M \to N$ que a $m \in M$ le asigna $f(m) + g(m)$, es un morfismo de R-módulos y $rf : M \to N$ que a $m \in M$ le manda a $r(f(m))$ también es un morfismo de R-módulos.

Observación. Si $f : M \to N$ es un R-morfismo, entonces $\ker(f) = \{m \in M : f(m) = 0\}$ es un submódulo de M e $Im(f)$ es un submódulo de N. Más aún, si S es un submódulo de M, $f(S)$ es un submódulo de N, y si T es un submódulo de N entonces $f^{-1}(T)$ es un submódulo de M. Además, el grupo abeliano M/S admite una estructura de R-módulo definida por $r(m + N) = rm + N$, el cual es el **módulo cociente** de M por N.

Definición 1.1.4 *Un R-morfismo $f : M \to N$ es un* ***monomorfismo*** *si f es inyectivo;* ***epimorfismo*** *si f es suprayectivo e* ***isomorfismo*** *si f es una biyección.*

Proposición 1.1.5 *Sean M y N dos R-módulos y $f : M \to N$ un R-morfismo. Las siguientes afirmaciones son equivalentes:*

(1) *f es monomorfismo.*

(2) $\ker(f) = 0$.

(3) *Para todo R-módulo T y todo par de morfismos $g, h : T \to M$, $f \circ g = f \circ h$ implica $g = h$.*

(4) *Para todo R-módulo T y para todo morfismo $g : T \to M$, $f \circ g = 0$ implica $g = 0$.*

Demostración. (1) $\Rightarrow$ (2) Si $x \in \ker(f)$, $f(x) = 0 = f(0)$, entonces $x = 0$.

(2) $\Rightarrow$ (1) Sean $x, y \in M$ tales que $f(x) = f(y)$, lo que implica que $f(x-y) = 0$, entonces $x - y \in \ker(f) = 0$ y así $x = y$.

(2) $\Rightarrow$ (3) Si $x \in T$, $f(g(x)) = f(h(x))$, entonces $f(g(x) - h(x)) = f(g(x)) - f(h(x)) = 0$, o sea que $g(x) - h(x) \in \ker(f) = 0$ y de esto se sigue que $g(x) = h(x)$, es decir $g = h$.

(3) $\Rightarrow$ (4) Tomando el morfismo $h : T \to M$ que a todo $t \in T$ lo manda al cero en M tenemos que $g = 0$.

(4) $\Rightarrow$ (2) Si $x \in \ker(f)$, $f(x) = 0$. Haciendo $T = \ker(f)$ y tomando a g como el morfismo inclusión $i : \ker(f) \to M$ que es inyectivo tenemos que $f(i(x)) = f(x) = 0$, entonces $i = 0$. Luego, $\ker(f) \cong Im(i) = 0$. □

Observaciones.

1. La tercera afirmación es el concepto de monomorfismo categórico en la categoría de R-módulos, R-Mod. De aquí que la proposición afirma que la noción de monomorfismo dada aquí coincide con la noción de monomorfismo categórico.

2. En la categoría $\mathcal{C}$ de grupos abelianos divisibles (un grupo G es divisible si para todo $g \in G$ y para todo $s \in \mathbb{Z} - \{0\}$, hay un $g' \in G$ tal que $g = sg'$) y homomorfismos de grupos, hay monomorfismos los cuales no son inyectivos en los conjuntos subyacentes (considere el cociente natural $\mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$, donde $\mathbb{Q}$ y $\mathbb{Z}$ son considerados como grupos abelianos bajo la adición).

Proposición 1.1.6 *Sean M y N dos R-módulos y $f : M \to N$ un R-morfismo. Son equivalentes las siguientes afirmaciones:*

(1) *f es epimorfismo.*

(2) *$Coker(f) := N/Im(f) = 0$.*

(3) *Para todo R-módulo T y todo par de morfismos $g, h : N \to T$, $g \circ f = h \circ f$ implica $g = h$.*

(4) *Para todo R-módulo T y para todo morfismo $g : N \to T$, $g \circ f = 0$ implica $g = 0$.*

Demostración. (1) $\Leftrightarrow$ (2) f es epimorfismo si y sólo si $Im(f) = N$ que equivale a que $N/Im(f) = 0$.

(2) $\Rightarrow$ (3) Si $x \in N$, $x = f(m)$ para algún $m \in M$. Pero $g(f(m)) = h(f(m))$, entonces $g(x) = h(x)$, es decir, $g = h$.

(3) $\Rightarrow$ (4) Tomando $h = 0$ tenemos $g \circ f = 0 = h \circ f$, entonces $g = h = 0$.

(4) $\Rightarrow$ (1) Si hacemos $T = N/Im(f)$ y $g = \pi : N \to N/Im(f)$ que es la proyección canónica tenemos que $\pi \circ f = 0$, entonces $\pi = 0$, o sea que $N/Im(f) = \pi(N) = 0$. □

Observación. La tercera afirmación es el concepto de epimorfismo categórico en la categoría de R-módulos, R-Mod. De aquí que la proposición afirma que la noción de epimorfismo dada aquí coincide con la noción de epimorfismo categórico. Sin embargo, en la categoría de anillos y homomorfismos de anillos, Rng, hay epimorfismos que no son suprayectivos; por ejemplo, el encajamiento usual $\mathbb{Z} \xrightarrow{f} \mathbb{Q}$ es un epimorfismo que no es suprayectivo.

Proposición 1.1.7 *Sean $f : M \to N$ y $g : M \to T$ morfismos de R-módulos con g epimorfismo. Entonces hay un morfismo $h : T \to N$ que hace conmutar el diagrama*

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "g"'] & N \\ T \arrow[ur, dotted, "h"'] & \end{tikzcd}$$

si y sólo si $\ker(g) \subseteq \ker(f)$. *Además, h es único con tal propiedad.*

Demostración. ($\Rightarrow$) Sea $m \in M$ tal que $g(m) = 0$, entonces $f(m) = (h \circ g)(m) = h(g(m)) = h(0) = 0$.

($\Leftarrow$) Sea $t \in T$. Como g es un epimorfismo, existe $m \in M$ tal que $g(m) = t$. Definimos $h : T \to N$ por $h(t) := f(m)$.

Veamos que h está bien definida. Sean $m, m' \in M$ tales que $g(m) = g(m') = t$. Luego, $g(m-m') = 0$, esto es, $m-m' \in \ker(g) \subseteq \ker(f)$. Entonces $f(m-m') = 0$, y así, $f(m) = f(m')$. Además, h es un morfismo (porque está dada en términos de f que es un morfismo) tal que para cada $m \in M$, $f(m) = h(t) = h(g(m))$; es decir, $f = h \circ g$.

Finalmente veamos que h es único. Supongamos que $h' : T \to N$ es un morfismo tal que $f = h' \circ g$, entonces $h \circ g = h' \circ g$. Sea $t \in T$, entonces hay un $m \in M$ tal que $t = g(m)$. Luego, $h'(t) = h'(g(m)) = h(g(m)) = h(t)$. Por lo tanto, $h' = h$. □

Teorema 1.1.8 (Teorema fundamental de morfismos de R-módulos) *Si $f : M \to N$ es un epimorfismo de R-módulos, entonces $M/\ker(f) \cong N$.*

Demostración. Sabemos que $M/\ker(f) \cong N$ como grupos. Así que sólo hay que probar que tal morfismo es un R-morfismo. □

Teorema 1.1.9 (Teorema de correspondencia) *Si $f : M \to N$ es un epimorfismo, entonces hay una correspondencia biyectiva entre el conjunto de submódulos de N y el conjunto de submódulos de M que contienen a* $\ker(f)$.

Demostración. Para cada submódulo N' de N, sea $f^{-1}(N') = \{m \in M : f(m) \in N'\}$. Debemos probar que si M' es un submódulo de M tal que $\ker(f) \subseteq M'$, entonces $f^{-1}(f(M')) = M'$; y si N' es un submódulo de N, entonces $f(f^{-1}(N')) = N'$. Esto es, ambas aplicaciones son inversas una de la otra. $\square$

Observación. Sean M un R-módulo e I un ideal de R. Si $I \subseteq Ann(M) = \{r \in R : rM = 0\}$, entonces se puede considerar a M como un R/I-módulo de la siguiente forma: si $\overline{r} \in R/I$ y $m \in M$, $\overline{r}m = rm$. Esta operación es independiente de la elección del representante en $\overline{r}$, ya que $IM = 0$.

1.2. Sucesiones exactas

Definición 1.2.1 *Sea $(M_n)_{n\in\mathbb{Z}}$ una familia de R-modulos junto con morfismos $M_n \xrightarrow{f_n} M_{n-1}$. Diremos que la sucesión*

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

*es **exacta** en M_n si $Im(f_{n+1}) = \ker(f_n)$. Si la sucesión es exacta en cada M_n diremos que la sucesión es **exacta**.*

Observación. En una sucesión exacta la composición de R-morfismos sucesivos es el morfismo cero.

Ejemplo. Si $M \xrightarrow{f} N$ es un morfismo de R-módulos entonces tenemos la sucesión exacta

$$0 \longrightarrow \ker(f) \xrightarrow{i} M \xrightarrow{\pi} M/\ker(f) \longrightarrow 0,$$

donde i es la inclusión canónica y π es la proyección canónica. De modo análogo tenemos una sucesión exacta

$$0 \longrightarrow Im(f) \longrightarrow N \longrightarrow N/Im(f) \longrightarrow 0.$$

Definición 1.2.2 *Una sucesión **exacta corta** es una sucesión exacta del tipo*

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

Observaciones.

1. Decir que esta sucesión es exacta corta equivale a decir que f es monomorfismo, que g es epimorfismo y que $Im(f) = \ker(g)$.

2. Una sucesión exacta puede escindirse en sucesiones exactas cortas: si $N_i = Im(f_{i+1}) = \ker(f_i)$, tenemos sucesiones exactas cortas

$$0 \longrightarrow N_i \longrightarrow M_i \longrightarrow N_{i+1} \longrightarrow 0.$$

1.3. $Hom_R(M, N)$

En esta sección damos algunas propiedades de una de las operaciones que son fundamentales en álgebra homológica, la formación de grupos de homomorfismos.

Proposición 1.3.1 *Sea R un anillo conmutativo y sean M y N dos R-módulos. Entonces*

$$Hom_R(M, N) := \{f : \ f : M \to N \, es \ morfismo \ de \ R\text{-}módulos\}$$

es un R-módulo respecto a las operaciones:

$$\begin{array}{rcl} Hom_R(M, N) \times Hom_R(M, N) & \longrightarrow & Hom_R(M, N) \\ (f, g) & \longmapsto & f + g : \begin{array}{rcl} M & \longrightarrow & N \\ m & \longmapsto & f(m) + g(m), \end{array} \end{array}$$

$$\begin{array}{rcl} R \times Hom_R(M, N) & \longrightarrow & Hom_R(M, N) \\ (r, f) & \longmapsto & rf : \begin{array}{rcl} M & \longrightarrow & N \\ m & \longmapsto & r(f(m)). \end{array} \end{array}$$

Demostración. Es necesario verificar que estas operaciones están bien definidas y que se cumplen las propiedades que definen un R-módulo, teniendo en cuenta que si R es un anillo (no necesariamente conmutativo), entonces $Hom_R(M, N)$ es un grupo abeliano y por lo tanto es un $\mathbb{Z}$-módulo. □

Proposición 1.3.2 *Sean M, N y T R-módulos y sea $f : N \to T$ un R-morfismo. Entonces:*

$$(1) \quad \begin{array}{rcl} f^* = Hom_R(M, f) : Hom_R(M, N) & \longrightarrow & Hom_R(M, T) \\ g & \longmapsto & f \circ g \ , \end{array}$$

$$(2) \quad \begin{array}{rcl} f_* = Hom_R(f, M) : Hom_R(T, M) & \longrightarrow & Hom_R(N, M) \\ g & \longmapsto & g \circ f \ . \end{array}$$

son morfismos de grupos abelianos.

Demostración.

(1) Sean $g, h \in Hom_R(M, N)$, entonces

$$f^*(g + h) = f \circ (g + h) = f \circ g + f \circ h = f^*(g) + f^*(h).$$

(2) Es similar a la anterior.

□

Proposición 1.3.3 *Sea M un R-módulo. Entonces*

(1) *El grupo abeliano $Hom_R(R, M)$ es un R-módulo respecto a la ley de composición externa*

$$\begin{array}{rcl} R \times Hom_R(R,M) & \longrightarrow & Hom_R(R,M) \\ \\ (r,f) & \longmapsto & \begin{array}{rccl} rf: & R & \longrightarrow & M \\ & x & \longmapsto & (rf)(x) := f(xr). \end{array} \end{array}$$

(2) *$Hom_R(R, M) \cong M$ como R-módulos.*

Demostración.

(1) Directamente se prueba que esta operación está bien definida y que cumple con las propiedades que hacen del grupo abeliano $Hom_R(R, M)$ un R-módulo.

(2) Definimos $\rho : M \to Hom_R(R, M)$ de la siguiente forma: para cada $m \in M$, $\rho(m)$ es tal que para cada $r \in R$, $\rho(m)(r) = rm$. Definimos además $\theta : Hom_R(R, M) \to M$ que a $f \in Hom_R(R, M)$ le asocia $f(1)$. De acuerdo con esto, tenemos que $\rho(m) \in Hom_R(R, M)$, ρ y θ son R-morfismos y que $\theta \circ \rho = 1_M$ y $\rho \circ \theta = 1_{Hom_R(R,M)}$. Lo que implica que $Hom_R(R, M) \cong M$.

□

Proposición 1.3.4 *Sean $f_1 : N \to T$ y $f_2 : T \to U$ morfismos de R-módulos y M un R-módulo.*

(1) *Si $1_T : T \to T$ es la identidad, entonces 1_T^* es la identidad y 1_{T*} también es la identidad.*

(2) *$(f_2 \circ f_1)^* = f_2^* \circ f_1^*$ y $(f_2 \circ f_1)_* = f_{1*} \circ f_{2*}$.*

Demostración.

(1) Sea $h \in Hom_R(M, T)$ ($h \in Hom_R(T, M)$), entonces $1_T^*(h) = 1_T \circ h = h$ ($1_{T*}(h) = h \circ 1_T = h$).

(2) Sea $g \in Hom_R(M, N)$ ($g \in Hom_R(U, M)$), entonces

$$(f_2 \circ f_1)^*(g) = (f_2 \circ f_1) \circ g = f_2 \circ (f_1 \circ g) = f_2^*(f_1^*(g)) = (f_2^* \circ f_1^*)(g)$$

$$\big((f_2 \circ f_1)_*(g) = g \circ (f_2 \circ f_1) = (g \circ f_2) \circ f_1 = f_{1*}(f_{2*}(g)) = (f_{1*} \circ f_{2*})(g)\big).$$

□

Proposición 1.3.5 *La sucesión $0 \longrightarrow N \xrightarrow{u} T \xrightarrow{v} U$ de morfismos de R-módulos es exacta si y sólo si para todo R-módulo M, la sucesión*

$$0 \longrightarrow Hom_R(M, N) \xrightarrow{u^*} Hom_R(M, T) \xrightarrow{v^*} Hom_R(M, U)$$

es exacta.

Demostración. ($\Rightarrow$) Primero probaremos que $\ker(u^*) = 0$. Para esto, sea $f \in \ker(u^*)$, entonces $u \circ f = u^*(f) = 0$, o sea que para cada $m \in M$, $u(f(m)) = 0$, así, para cada $m \in M$, $f(m) \in \ker(u) = 0$, es decir, $f = 0$.

Ahora veamos que $Im(u^*) = \ker(v^*)$. Tomemos un $g \in Im(u^*)$, entonces existe $f \in Hom_R(M, N)$ tal que $u \circ f = u^*(f) = g$ y aplicando v^* tenemos que $v^*(g) = v^*(u \circ f) = v \circ (u \circ f) = 0$, así, $g \in \ker(v^*)$.

Por otro lado, sea $g \in \ker(v^*)$, luego, $v \circ g = v^*(g) = 0$, entonces para cada $m \in M$, $v(g(m)) = 0$, o sea que para cada $m \in M$, $g(m) \in \ker(v) = Im(u)$. Como u es inyectiva se sigue que para $m \in M$, hay un único $x_m \in N$ tal que $u(x_m) = g(m)$. Sin perder de vista que lo que queremos probar es que $g \in Im(u^*)$, o sea que existe un $f \in Hom_R(M, N)$ tal que $u \circ f = u^*(f) = g$; definimos $f : M \to N$ que a $m \in M$ le asocia x_m, entonces tenemos que para cada $m \in M$, $(u \circ f)(m) = u(f(m)) = u(x_m) = g(m)$.

($\Leftarrow$) Primero vamos a probar que u es un monomorfismo utilizando (3) $\Rightarrow$ (1) en 1.1.5. Sean f y g dos R-morfismos tales que $u \circ f = u \circ g$, o sea que $u^*(f) = u^*(g)$. Ahora bien, como u^* es monomorfismo se sigue que $f = g$.

Ahora sólo nos falta probar que $Im(u) = \ker(v)$. Por hipótesis, para cada R-módulo M, $v^* \circ u^* = 0$, lo que es equivalente a que para cada R-módulo M y para cada $f \in Hom_R(M, N)$, $v \circ u \circ f = (v^* \circ u^*)(f) = 0$. Entonces en particular para $M = N$ y $f = 1_N$, tenemos que $v \circ u = 0$, es decir, $Im(u) \subseteq \ker(v)$.

Para la otra contensión notemos lo siguiente:

$$\begin{aligned}\ker(v^*) &= \{f \in Hom_R(M, T) : v \circ f = 0\} \\ &= \{f \in Hom_R(M, T) : \text{para cada } m \in M, f(m) \in \ker(v)\}.\end{aligned}$$

De acuerdo con esto, sean $M = \ker(v)$ y $\ker(v) \overset{i}{\hookrightarrow} T$ el morfismo inclusión. De este modo $i \in \ker(v^*) = Im(u^*)$, o sea que hay un $f \in Hom_R(M, N)$, tal que $u^*(f) = u \circ f = i$. Además tenemos que $\ker(v) = Im(i)$.

Si $x \in Im(i) = M$, entonces $x = i(x) = u(f(x))$, o sea que $x \in Im(u)$, esto es, $Im(i) \subseteq Im(u)$. Por lo tanto, $\ker(v) \subseteq Im(u)$. $\square$

Proposición 1.3.6 *La sucesión* $N \xrightarrow{u} T \xrightarrow{v} U \longrightarrow 0$ *es exacta si y sólo si para todo R-módulo M, la sucesión*

$$0 \longrightarrow Hom_R(U, M) \xrightarrow{v_*} Hom_R(T, M) \xrightarrow{u_*} Hom_R(N, M)$$

es exacta.

Demostración. ($\Rightarrow$) Probemos que $\ker(v_*) = 0$.

Sea $f \in \ker(v_*)$, entonces $f \circ v = v_*(f) = 0$. Queremos mostrar que $f = 0$. Sea $u \in U = Im(v)$, existe $t \in T$, tal que $v(t) = u$ y así tenemos que $0 = f(v(t)) = f(u)$, o sea que $f = 0$.

Mostremos ahora que $Im(v_*) = \ker(u_*)$. Si $g \in Im(v_*)$, se sigue que hay un $f \in Hom_R(U, M)$, tal que $f \circ v = v_*(f) = g$. Pero al aplicar u_* a g tenemos que $u_*(g) = g \circ u = (f \circ v) \circ u = f \circ 0 = 0$, o sea que $g \in \ker(u_*)$.

Sea $g \in \ker(u_*)$, entonces $g \circ u = u_*(g) = 0$. Hay que mostrar que existe $f \in Hom_R(U, M)$ tal que $f \circ v = v_*(f) = g$. Entonces se nos presenta la siguiente situación:

$$\begin{tikzcd} T \arrow[r, "g"] \arrow[d, "v"'] & M \\ U \arrow[ur, dotted, "f"'] & \end{tikzcd}$$

y surge la pregunta de si $\ker(v) \subseteq \ker(g)$. Si $x \in \ker(v) = Im(u)$, se sigue que hay un $n \in N$ tal que $u(n) = x$, entonces $g(x) = g(u(n)) = 0$ y así $x \in \ker(g)$; o sea que $\ker(v) \subseteq \ker(g)$. Por lo tanto, hay un morfismo $U \xrightarrow{f} M$ tal que $g = f \circ v$.

($\Leftarrow$) Primero probaremos que v es un epimorfismo. Sea M un R-módulo y $f, g \in Hom_R(U, M)$ tales que $f \circ v = g \circ v$, es decir, $v_*(f) = v_*(g)$, lo cual implica que $f = g$, por ser v_* un monomorfismo. De esta manera v es un epimorfismo.

Probemos ahora que $Im(u) = \ker(v)$. Tenemos que $u_* \circ v_* = 0$, o sea que para toda $f \in Hom_R(U, M)$, $(u_* \circ v_*)(f) = u_*(v_*(f)) = u_*(f \circ v) = f \circ v \circ u = 0$. Si hacemos $M = U$ y $f = 1_U$, se sigue que $v \circ u = 0$, y de aquí, $Im(u) \subseteq \ker(v)$.

Para la otra contensión notemos que

$$\begin{aligned} \ker(u_*) &= \{f \in Hom_R(T, M) : u_*(f) = 0\} = \{f \in Hom_R(T, M) : f \circ u = 0\} \\ &= \{f \in Hom_R(T, M) : \text{para cada } n \in N, f(u(n)) = 0\}. \end{aligned}$$

Si hacemos $M = T/Im(u)$ y tomamos la proyección canónica $T \xrightarrow{\pi} M$, se sigue que $\pi \in \ker(u_*) = Im(v_*)$. Entonces existe $\psi \in Hom_R(U, M)$ tal que $\pi = v_*(\psi) = \psi \circ v$. Además $\ker(\pi) = Im(u)$ y $\ker(v) \subseteq \ker(\pi)$ (esto útimo es porque si $m \in \ker(v)$, $v(m) = 0$; entonces $\pi(m) = \psi(v(m)) = \psi(0) = 0$). Así $\ker(v) \subseteq Im(u)$. □

1.4. Suma y producto directo

Definición 1.4.1 *Sea $(M_i)_{i \in I}$ una familia de submódulos de un R-módulo M. Diremos que $\sum_{i \in I} M_i$ es la **suma directa interna** de $(M_i)_{i \in I}$ si*

$$0 = \sum_{i \in I} m_i \in \sum_{i \in I} M_i \textit{ implica que para cada } i \in I, m_i = 0.$$

Con $L = \sum_{\oplus} M_i$ denotaremos que $L = \sum M_i$ es la suma directa de (M_i). Si $I = \{1, \ldots, n\}$, entonces con $M_1 \oplus \cdots \oplus M_n$ denotamos a la suma directa de los M_i.

Ejemplos.

1. Si M es un R-módulo, M es suma directa de M y 0. Pero si $M \neq 0$, entonces M no es suma directa de M y M ya que al tomar un $m \in M$ con $m \neq 0$, se tiene que $m + (-m) = 0$.

2. Sea $M = \mathbb{R}^2$ visto como $\mathbb{R}$-espacio vectorial y sea M' un subespacio de M con $dim(M') = 1$, entonces $\mathbb{R}^2 = M' \oplus M''$, donde M'' es una recta que pasa por el origen y que no coincide con la recta M'.

Proposición 1.4.2 *Sea $(M_i)_{i\in I}$ una familia de submódulos de un R-módulo M. Entonces $\sum_{i\in I} M_i$ es suma directa si y sólo si $(\sum_{i\neq j} M_i) \cap M_j = 0$ para cada $j \in I$.*

Demostración. Sea $x \in (\sum_{i\neq j} M_i) \cap M_j$, entonces $x = \sum_{i\neq j} m_i$ y $x \in M_j$, luego $0 = \sum_{i\neq j} m_i + (-x) \in \sum_{i\in I} M_i$. Pero $\sum_{i\in I} M_i$ es suma directa, entonces para $i \neq j$, $m_i = 0$ y $-x = 0$, o sea que $x = 0$.

Ahora supongamos que $(\sum_{i\neq j} M_i) \cap M_j = 0$ y que $0 = \sum_{i\in I} m_i \in \sum_{i\in I} M_i$, entonces $m_i = 0$ para casi todo i. Fijémonos en la colección finita de los m_j que podrían no ser cero. Para cada uno de estos m_j, $\sum_{i\neq j} m_i + m_j = 0$, entonces $M_j \ni -m_j = \sum_{i\neq j} m_i \in \sum_{i\neq j} M_i$. Esto implica que $m_j \in (\sum_{i\neq j} M_i) \cap M_j = 0$. Entonces cada uno de los $m_j = 0$, o sea que para cada i, $m_i = 0$ y de este modo $\sum_{i\in I} M_i$ es suma directa. □

Corolario 1.4.3 *Sean N y T submódulos de M. Entonces $M = N \oplus T$ si y sólo si $M = N + T$ y $N \cap T = 0$.*

Definición 1.4.4 *Sea N un submódulo de un R-módulo M. Diremos que N es un **sumando directo** de M si hay un submódulo T de M tal que $M = N \oplus T$.*

Proposición 1.4.5 *Si $(M_i)_{i\in I}$ es una familia de R-módulos, entonces $\prod M_i$ es un R-módulo.*

Demostración. Se consideran las siguientes operaciones:

$$\text{Si } (f_i)_{i\in I}, (g_i)_{i\in I} \in \prod M_i \text{ y } r \in R, (f_i) + (g_i) = (f_i + g_i) \text{ y } r(f_i) = (rf_i).$$

□

Definición 1.4.6 *El R-módulo $\prod M_\alpha$ se llama **producto directo** de la familia $(M_i)_{i\in I}$.*

Definición 1.4.7 *El morfismo $\pi_j : \prod M_i \to M_j$ definido por $\pi_j((f_i)) = f_j$ se llama j-ésima **proyección** de $\prod M_i$. Y el morfismo $\mu_j : M_j \to \prod M_i$ definido por $\mu_j(x) = (f_i)$, donde $f_j = x$ y $f_i = 0$ si $i \neq j$; es llamado j-ésima **inclusión** de $\prod M_i$.*

Observación. π_j es un epimorfismo y μ_j es un monomorfismo.

Teorema 1.4.8 (Propiedad universal del producto directo) *Sea $(M_i)_{i\in I}$ una familia de R-módulos. Entonces $(\prod M_i, (\pi_i))$ es el único objeto (salvo isomorfismo) que cumple la siguiente propiedad: para toda pareja $(M, (\nu_i))$ (donde*

M es un R-módulo y para cada j, $\nu_j : M \to M_j$ es R-morfismo), existe un único morfismo $t : M \to \prod M_i$ tal que para todo $j \in I$, el diagrama

$$\begin{tikzcd} M \arrow[r, dotted, "t"] \arrow[dr, "\nu_j"'] & \prod M_i \arrow[d, "\pi_j"] \\ & M_j \end{tikzcd}$$

conmuta.

Demostración. Se define la aplicación $t : M \to \prod M_i$ por $t(m)(i) = \nu_i(m)$ para cada $m \in M$ y para cada $i \in I$, la cual es un morfismo ya que para cada $i \in I$, ν_i es un morfismo. Entonces para cada $j \in I$ y $m \in M$, $(\pi_j \circ t)(m) = \pi_j(t(m)) = t(m)_j = t(m)(j) = \nu_j(m)$, o sea que, $\pi_j \circ t = \nu_j$.

Veamos que t es único con esta propiedad. Supongamos que $t' : M \to \prod M_i$ es un morfismo tal que para cada $j \in I$, $\pi_j \circ t' = \nu_j$. Entonces para cada $m \in M$ y para cada $j \in I$, $t'(m)(j) = t'(m)_j = (\pi_j \circ t')(m) = \nu_j(m) = (\pi_j \circ t)(m) = t(m)_j = t(m)(j)$, o sea que, para cada $m \in M$, $t'(m) = t(m)$; y así, $t' = t$.

Ahora verifiquemos la unicidad de $(\prod M_i, (\pi_i))$ (hasta isomorfismo) con la propiedad enunciada. Para esto, supongamos que la pareja $(N, (\pi'_i))$, donde N es R-módulo y para cada $j \in I$, $\pi'_j : N \to M_j$ es un R-morfismo, cumple con las propiedades enunciadas.

De las propiedades de $(\prod M_i, (\pi_i))$ y $(N, (\pi'_i))$, tenemos que existen morfismos únicos θ y θ' tales que para cada $j \in I$, conmutan los diagramas

$$\begin{tikzcd} N \arrow[r, "\theta"] \arrow[dr, "\pi'_j"'] & \prod M_i \arrow[d, "\pi_j"] \\ & M_j \end{tikzcd} \qquad \begin{tikzcd} \prod M_i \arrow[r, "\theta'"] \arrow[dr, "\pi_j"'] & N \arrow[d, "\pi'_j"] \\ & M_j \end{tikzcd}$$

esto es, $\pi_j \circ \theta = \pi'_j$ y $\pi'_j \circ \theta' = \pi_j$. Entonces $(\pi_j \circ \theta) \circ \theta' = \pi'_j \circ \theta' = \pi_j$ y $(\pi'_j \circ \theta') \circ \theta = \pi_j \circ \theta = \pi'_j$; lo que nos dice que para cada $j \in I$, los diagramas

$$\begin{tikzcd} N \arrow[r, "\theta' \circ \theta"] \arrow[dr, "\pi'_j"'] & N \arrow[d, "\pi'_j"] \\ & M_j \end{tikzcd} \qquad \begin{tikzcd} \prod M_i \arrow[r, "\theta \circ \theta'"] \arrow[dr, "\pi_j"'] & \prod M_i \arrow[d, "\pi_j"] \\ & M_j \end{tikzcd}$$

conmutan. Pero también tenemos que para cada $j \in I$, los diagramas

$$\begin{tikzcd} N \arrow[r, "1_N"] \arrow[dr, "\pi'_j"'] & N \arrow[d, "\pi'_j"] \\ & M_j \end{tikzcd} \qquad \begin{tikzcd} \prod M_i \arrow[r, "1_{\prod M_i}"] \arrow[dr, "\pi_j"'] & \prod M_i \arrow[d, "\pi_j"] \\ & M_j \end{tikzcd}$$

conmutan. Entonces, $\theta' \circ \theta = 1_N$ y $\theta \circ \theta' = 1_{\prod M_i}$, y de este modo, θ es un isomorfismo con las propiedades requeridas. $\square$

Proposición 1.4.9 *Sea $(M_i)_{i\in I}$ una familia de R-módulos. Entonces*

$$S = \left\{(f_i)_{i\in I} \in \prod M_i : f_i = 0 \text{ para casi todo } i \in I\right\}$$

es un submódulo de $\prod M_i$.

Demostración. Es inmediata. $\square$

Definición 1.4.10 *El submódulo S en 1.4.9 es llamado* ***suma directa (externa)*** *de la familia $(M_i)_{i\in I}$ y se denota por $\bigoplus M_i$.*

Observación.

1. Si el conjunto de índices es finito, la suma directa externa coincide con el producto directo.

2. Si $f \in \bigoplus M_i$, entonces $f = \sum \mu_i(f_i)$, es decir, f se puede ver como una suma de funciones selectoras, porque las entradas de f son casi todas cero.

Teorema 1.4.11 (Propiedad universal de la suma directa) *Sea $(M_i)_{i\in I}$ una familia de R-módulos. Entonces $(\bigoplus M_i, (\mu_i))$ es el único objeto (salvo isomorfismo) que cumple la siguiente propiedad: para toda pareja $(M, (\nu_i))$ (donde M es un R-módulo y para cada j, $\nu_j : M_j \to M$ es R-morfismo), existe un único morfismo $u : \bigoplus M_i \to M$ tal que para todo $j \in I$, el diagrama*

$$\begin{tikzcd} M & \bigoplus M_i \arrow[l, dotted, "u"'] \\ & M_j \arrow[ul, "\nu_j"] \arrow[u, "\mu_j"'] \end{tikzcd}$$

conmuta.

Demostración. Se define la aplicación $u : \bigoplus M_i \to M$ por $u((f_i)) = \sum \nu_i(f_i)$, para cada $(f_i) \in \prod M_i$. Notemos que u está bien definida porque $f_i = 0$ para casi todo $i \in I$, y u es un morfismo porque ν_i es un morfismo. Así, tenemos que para cada $j \in I$ y $x \in M_j$, $(u \circ \mu_j)(x) = u(\mu_j(x)) = \sum \nu_i((\mu_i(x))) = \nu_i(x)$; es decir, para cada $j \in I$, $u \circ \mu_j = \nu_i$.

Veamos que u es único con esta propiedad. Supongamos que $u' : \bigoplus M_i \to M$ es un morfismo tal que para cada $j \in I$, $u' \circ \mu_j = \nu_j$; entonces para cada $(f_i) \in \bigoplus M_i$, $u((f_i)) = \sum \nu_i(f_i) = \sum (u' \circ \mu_i)(f_i) = \sum u'(\mu_i(f_i)) = u'(\sum \mu_i(f_i)) = u'((f_i))$. Así, $u' = u$.

La prueba de unicidad de $(\bigoplus M_i, \mu_i)$ (hasta isomorfismo) con la propiedad enunciada es análoga a la del producto. □

Sea (M_i) una familia de submódulos de M y sea para cada $i \in I$, $\mu'_i : M_i \to M$ el morfismo inclusión. La propiedad universal de la suma directa garantiza la existencia de un morfismo único $u : \bigoplus M_i \to M$ tal que para todo $i \in I$, $u \circ \mu_i = \mu'_i$.

Proposición 1.4.12 (1) *$Im(u) = \sum M_i$.*

(2) *$\sum M_i$ es suma directa si y sólo si u es un monomorfismo.*

Demostración.

(1) Sea $f \in \bigoplus M_i$. Luego, $f = \sum \mu_i(f_i)$ con $f_i = 0$ para casi todo $i \in I$. Aplicando u a f obtenemos que $u(f) = u(\sum \mu_i(f_i)) = \sum (u \circ \mu_i)(f_i) = \sum \mu'_i(f_i) = \sum f_i \in \sum M_i$. De esta forma $Im(u) = \sum M_i$.

(2) $(\Rightarrow)$ Sea $f \in \ker(u)$, entonces $0 = u(f) = u(\sum \mu_i(f_i)) = \sum f_i \in \sum M_i$. Como $\sum M_i$ es suma directa, $f_i = 0$ para cada $i \in I$, así $f = 0$.

$(\Leftarrow)$ Supongamos que $0 = \sum m_i \in \sum M_i$. Si $f = (m_i)_{i \in I} \in \bigoplus M_i$, entonces $u(f) = u(\sum \mu_i(m_i)) = \sum m_i = 0 = u(0)$. Como u es un monomorfismo, $f = 0$, esto es, para cada $i \in I$, $m_i = 0$. Así $\sum M_i$ es suma directa.

□

Observación.Si $M = \sum_{\oplus} M_i$, entonces de (1) tenemos que u es un epimorfismo, y por (2) u es un monomorfismo. Así, $\bigoplus M_i \cong \sum_{\oplus} M_i$.

Proposición 1.4.13 (1) *$Hom_R(M, \prod N_i) \cong \prod Hom_R(M, N_i)$.*

(2) *$Hom_R(\bigoplus M_i, N) \cong \prod Hom_R(M_i, N)$.*

Demostración.

(1) Para cada $j \in I$, la proyección $\pi_j : \prod N_i \to N_j$ induce un morfismo de grupos abelianos $\nu_j : Hom_R(M, \prod N_i) \to N_j$ definido por $\nu_j(f) := \pi_j \circ f$.

Entonces de 1.4.8, tenemos que hay un único morfismo t tal que para cada $j \in I$, el diagrama

$$\begin{tikzcd} Hom_R(M, \prod N_i) \arrow[r, "t"] \arrow[dr, "\nu_j"'] & \prod Hom_R(M, N_i) \arrow[d, "\pi_j"] \\ & N_j \end{tikzcd}$$

conmuta.

Afirmamos que t es un isomorfismo.

Sea $f \in \ker t$, entonces $0 = t(f)$, esto es, para cada $i \in I$, $0 = (t(f))_i = \pi_i(t(f)) = \nu_i(f) = \pi_i \circ f$. Entonces los diagramas

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[dr, "\nu_j(f)"'] & \prod N_i \arrow[d, "\pi_j"] \\ & N_j \end{tikzcd} \qquad \begin{tikzcd} M \arrow[r, "0"] \arrow[dr, "\nu_j(f)"'] & \prod N_i \arrow[d, "\pi_j"] \\ & N_j \end{tikzcd}$$

conmutan. Y por 1.4.8 obtenemos que $f = 0$.

Ahora supongamos que $f = (f_i) \in \prod Hom_R(M, N_i)$, esto es, para cada $i \in I$, $f_i \in Hom_R(M, N_i)$. Nuevamente, por 1.4.8 se garantiza que hay un único morfismo θ tal que para cada $j \in I$, el diagrama

$$\begin{tikzcd} M \arrow[r, "\theta"] \arrow[dr, "f_j"'] & \prod N_i \arrow[d, "\pi_j"] \\ & N_j \end{tikzcd}$$

conmuta. Entonces para cada $i \in I$, $t(\theta)(i) = (t(\theta))_i = \pi_i(t(\theta)) = \nu_i(\theta) = \pi_i \circ \theta = f_i$, es decir, $t(\theta) = f$.

Por lo tanto, t es un isomorfismo.

(2) La prueba es análoga a la de (1).

$\square$

Definición 1.4.14 *Un morfismo de R-módulos $f : M \to N$ es:*

(1) *Una* ***sección*** *si hay un morfismo $g : N \to M$ tal que $g \circ f = 1_M$.*

(2) *Una* ***retracción*** *si hay un morfismo $g : N \to M$ tal que $f \circ g = 1_N$.*

Observaciones.

1. Si f es una sección, entonces f es un monomorfismo. Pero el recíproco no es necesariamente cierto. Considere el morfismo inclusión $2\mathbb{Z} \to \mathbb{Z}$, el cual es un monomorfismo que no es una sección.

2. Si f es una retracción, entonces f es epimorfismo. Pero el recíproco no es necesariamente cierto. Considere la proyección $\mathbb{Z} \to \mathbb{Z}_2$, el cual es un epimorfismo que no es una retracción.

Proposición 1.4.15 *Sea* $\mathcal{E}: \ 0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$ *una sucesión exacta corta. Las siguientes proposiciones son equivalentes:*

(1) *f es una sección.*

(2) *g es una retracción.*

(3) *Hay un isomorfismo $\varphi : N \to M \oplus T$ que hace conmutar los cuadrados del diagrama*

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "f"] \arrow[d, "1_M"'] & N \arrow[r, "g"] \arrow[d, "\varphi"'] & T \arrow[r] \arrow[d, "1_T"'] & 0 \\
0 \arrow[r] & M \arrow[r, "\mu_1"'] & M \oplus T \arrow[r, "\pi_2"'] & T \arrow[r] & 0,
\end{tikzcd}$$

donde μ_1 es la inclusión en M y π_2 es la proyección en T. Si se tiene alguna de estas tres condiciones, diremos que la sucesión $\mathcal{E}$ se ***divide****.*

Demostración. (3) $\Rightarrow$ (1) Tomando $\pi_1 : M \oplus T \to M$ como la proyección en M tenemos que $1_M = \pi_1 \circ \mu_1 = \pi_1 \circ (\varphi \circ f) = (\pi_1 \circ \varphi) \circ f$, o sea que f es una sección.

(3) $\Rightarrow$ (2) Tomando $\mu_2 : T \to M \oplus T$ como la inclusión en T tenemos que $1_T = \pi_2 \circ \mu_2 = (g \circ \varphi^{-1}) \circ \mu_2 = g \circ (\varphi^{-1} \circ \mu_2)$. De esta forma g es una retracción.

(1) $\Rightarrow$ (3) Como f es una sección, entonces, hay un morfismo $h : N \to M$ tal que $h \circ f = 1_M$. Definimos $\varphi : N \to M \oplus T$ por $\varphi(n) = (h(n), g(n))$, el cual es un R-morfismo porque h y g son R-morfismos.

Verifiquemos que φ es un isomorfismo.

Sea $n \in \ker(\varphi)$, esto es, $0 = \varphi(n) = (h(n), g(n))$; luego, $n \in \ker(g) = Im(f)$, o sea que existe un $m \in M$ tal que $f(m) = n$, lo cual implica que $m = h(f(m)) = h(n) = 0$, entonces $n = 0$; y de este modo tenemos que φ es inyectiva.

Ahora supongamos que $(m, t) \in M \oplus T$, entonces, hay un $n \in N$ tal que $g(n) = t$, pues g es suprayectiva. El elemento $f(m) - f(h(n)) + n \in N$ verifica que $\varphi(f(m) - f(h(n)) + n) = (m, t)$, es decir, que φ es suprayectiva.

Además, para cada $m \in M$ y cada $n \in N$, $(\varphi \circ f)(m) = \varphi(f(m)) = \big(h(f(m)), g(f(m))\big) = (m, 0) = \mu_1(m)$ y $g(n) = \pi_2(h(n), g(n)) = \pi_2(\varphi(n)) = (\pi_2 \circ \varphi)(n)$, o sea que los cuadrados del diagrama conmutan.

(2) $\Rightarrow$ (3) Como g es una retracción, hay un morfismo $h : T \to N$ tal que $g \circ h = 1_T$; entonces h es un monomorfismo, el cual induce el isomorfismo $h : T \to h(T)$.

Afirmamos que $N = \ker(g) \oplus h(T)$, esto es, $N = \ker(g) + h(T)$ y $\ker(g) \cap h(T) = 0$. Sea $n \in N$, entonces $n = (n - h(g(n))) + h(g(n))$, donde $(n - h(g(n))) \in \ker(g)$ y $h(g(n)) \in Im(h)$. Por otra parte, si $x \in \ker(g) \cap h(T)$, se sigue que hay un $t \in T$ tal que $g(x) = 0$ y $h(t) = x$, entonces $0 = g(x) = g(h(t)) = t$. Luego, $x = 0$.

Así tenemos que $N = \ker(g) \oplus h(T)$ con $T \cong h(T)$. Además, $\ker(g) = Im(f) \cong M$.

Finalmente verifiquemos que los cuadrados del diagrama conmutan. Como $N = \ker(g) \oplus h(T)$, entonces cada $n \in N$ tiene una expresión única de la forma $n = u + v$ con $u \in \ker(g) = Im(f)$ y $v \in h(T) \cong T$. De donde se tiene que existen $m \in M$ y $t \in T$ únicos tales que $u = f(m)$ y $v = h(t)$. Definimos la aplicación $\varphi : \ker(g) \oplus h(T) \to M \oplus T$ por $\varphi(n) = \varphi(u + v) = \varphi(f(m) + h(t)) = (m, t)$, la cual es un R-morfismo, es biyectiva y hace conmutar los cuadrados del diagrama. $\square$

Proposición 1.4.16 *La sucesión* $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$ *es exacta si* f *es un monomorfismo,* g *es un epimorfismo,* $g \circ f = 0$ *y* $N = f(M) \oplus h(T)$*, donde* $h : T \to N$ *es un morfismo tal que* $g \circ h = 1_T$*.*

Demostración. Sólo hay que probar que $\ker(g) \subseteq Im(f)$. Sea $x \in \ker(g) \subseteq N$, luego $0 = g(x)$ y $x = f(m) + h(t)$ para algún $m \in M$ y algún $t \in T$, entonces $0 = g(x) = g(f(m) + h(t)) = g(f(m)) + g(h(t)) = t$. Así $x = f(m) \in Im(f)$. Por lo tanto, $\ker(g) \subseteq Im(f)$. $\square$

1.5. Módulos libres

Definición 1.5.1 *Un* R*-módulo* F *es* ***libre*** *si es isomorfo a uno de la forma* $\bigoplus_{\alpha \in I} M_\alpha$*, donde* $M_\alpha \cong R$*.*

Observaciones.

1. $M_\alpha \cong R = \langle 1 \rangle$ implica que hay un $m_\alpha \in M_\alpha$ tal que $M_\alpha = \langle m_\alpha \rangle$.
2. Hay una aplicación inyectiva $\psi : I \to F$ que a $\alpha \in I$ le asocia $(u_\beta) \in F$ tal que $u_\beta = 1$ si $\beta = \alpha$ y $u_\beta = 0$ si $\beta \neq \alpha$.
3. $Im(\psi)$ es una base para F.
4. F es libre si y sólo si F tiene una base. En efecto, de la definición y la observación 1, $(m_\alpha)_{\alpha \in I}$ es una base de F.

Proposición 1.5.2 *Si* F *es un* R*-módulo libre y* $\mathcal{B}$ *es una base de* F*, entonces para todo* R*-módulo* M *y toda aplicación* $\varphi : \mathcal{B} \to M$*, existe un único morfismo*

$f : F \to M$ que hace conmutar el diagrama

$$\begin{tikzcd} M & F \arrow[l, dotted, "f"'] \\ & \mathcal{B} \arrow[ul, "\varphi"] \arrow[u, "i"'] \end{tikzcd}$$

Demostración. Como F es suma directa de los M_α y si para cada $\alpha \in I$, definimos morfismos $f_\alpha : M_\alpha \to M$ que a $x = rm_\alpha \in M_\alpha$ le asocia $r\varphi(m_\alpha) \in M$, entonces por la propiedad universal de la suma directa hay un único morfismo $f : F \to M$ que hace conmutar el diagrama

$$\begin{tikzcd} M & F \arrow[l, "f"'] \\ & M_\alpha \arrow[ul, "f_\alpha"] \arrow[u, "\mu_\alpha"'] \end{tikzcd}$$

Sea $(u_\beta) \in \mathcal{B}$, entonces $(f \circ i)((u_\beta)) = f(i((u_\beta))) = f((u_\beta))$, donde $u_\beta = m_\alpha$ si $\beta = \alpha$ y $u_\beta = 0$ cuando $\beta \neq \alpha$. Además $f((u_\beta)) = f(\mu_\alpha(m_\alpha)) = f_\alpha(m_\alpha) = \varphi((u_\beta))$. □

Proposición 1.5.3 *Si X es un conjunto, entonces hay un módulo libre F que tiene por base a X.*

Demostración. En el caso de que $X = \emptyset$, el módulo $F = 0$ es la suma de cero copias de R, de modo que F tiene por base a $\emptyset$. Si $X \neq \emptyset$, tomamos a F como la suma de $\mid X \mid$ copias de R. □

Observación. No todo módulo es libre. Por ejemplo, $\mathbb{Z}/2\mathbb{Z}$ no es $\mathbb{Z}$-libre, pues en caso contrario, $\bar{1}$ es una base para $\mathbb{Z}/2\mathbb{Z}$ y por tanto $\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}$, lo cual es falso. Esto también nos muestra que el cociente de un R-módulo libre no necesariamente es libre.

Proposición 1.5.4 *Todo R-módulo M es un cociente de un R-módulo libre.*

Demostración. Si M es un R-módulo libre y M' el conjunto subyacente de M, entonces hay un módulo libre F que tiene por base a M'. Si definimos la aplicación $\varphi : M' \to M$ que a $m \in M'$ le asocia $m \in M$ tenemos que hay un único morfismo $f : F \to M$ tal que el diagrama

$$\begin{tikzcd} M & F \arrow[l, dotted, "f"'] \\ & M' \arrow[ul, "\varphi"] \arrow[u, "i"'] \end{tikzcd}$$

conmuta. Como φ es suprayectiva, el morfismo f es suprayectivo. Entonces, por el teorema fundamental de morfismos de módulos, $M \cong F/\ker(f)$. □

1.6. Módulos finitamente generados

Definición 1.6.1 *Un R-módulo M es* ***finitamente generado*** *si existen elementos $m_1, \ldots, m_n \in M$ tales que para cada $m \in M$ existen $r_1 \ldots, r_n \in R$ tales que $m = \sum_{i=1}^{n} r_i m_i$, es decir, todo elemento de M es una* ***combinación lineal*** *de $m_1 \ldots, m_n$ con coeficientes en R. Si un R-módulo M es generado por $m_1 \ldots, m_n$, escribimos*

$$M = \langle m_1, \ldots, m_n \rangle = Rm_1 + \cdots + Rm_n.$$

Si $n = 1$, se dice que M es un ***módulo cíclico****.*

Observaciones.

1. Todo anillo R considerado como módulo sobre sí mismo es finitamente generado y tiene a 1 como generador.

2. Si M es un R-módulo cíclico, entonces M es isomorfo a un cociente de R (como módulo) por un ideal a la izquierda I de R. En efecto, si $M = \langle m \rangle$ y tomamos el epimorfismo $f : R \to M$ definido por $f(r) = rm$ para cada $r \in R$, entonces por el teorema fundamental de morfismos de módulos tenemos que $M \cong R/\ker(f)$. En conclusión, los módulos cíclicos se identifican con los módulos cocientes R/I, donde I es un ideal a la izquierda de R.

3. Si N y T son submódulos finitamente generados de un R-módulo M, entonces $N + T$ es finitamente generado.

4. Si V es un k-espacio vectorial finitamente generado, entonces todos sus subespacios también son de generación finita. Sin embargo, en el caso de módulos sobre un anillo arbitrario esta propiedad no necesariamente se hereda. Para algunos anillos R y ciertos R-módulos M, la propiedad de ser finitamente generados es hereditaria, por ejemplo: $\mathbb{Z}$ y $k[x]$, con k un campo; son dominios de ideales principales.

Ejemplo. El conjunto $R = \mathbb{R}^{[0,1]} = \{f : f : [0, 1] \to \mathbb{R} \text{ es función}\}$ bajo las operaciones usuales de suma y multiplicación de funciones, es un anillo con elemento unitario 1 (el 1 es la función constante 1), de lo cual resulta que R es un R-módulo cíclico con generador 1, por ejemplo. Vamos a probar que R tiene un submódulo (es decir, un ideal a la izquierda) que no es finitamente generado.

Sea $I = \{f \in R : \text{para casi todo } x \in [0, 1],\ f(x) = 0\}$. Probaremos que I es un ideal izquierdo de R. $I \neq \emptyset$, pues $f : [0, 1] \to \mathbb{R}$ definida por:

$$f(x) = 1 \ si \ x = 1 \ y \ f(x) = 0 \ si \ x \in [0, 1)$$

está en I. Ahora sean $h, g \in I$, entonces existen B y C subconjuntos finitos de $[0, 1]$ tales que para todo $b \in B$, $f(b) \neq 0$ y para todo $c \in C$, $g(c) \neq 0$. Entonces hay un subconjunto finito D de $B \cup C$ tal que para todo $x \in D$, $(g + h)(x) \neq 0$, o sea que $g + h \in I$. Además, para todo $b \in B$, $0 \neq -g(b) = (-g)(b)$, es decir,

$-g \in I$. También tenemos que $g+h = h+g$. De todo esto concluimos que I es abeliano.

Si $r \in R$ y para todo $b \in B$, $r(b) = 0$, entonces $rg \in I$. Si $r(b) \neq 0$ para algún $b \in B$, entonces haciendo $B' = \{b \in B : r(b) \neq 0\}$ tenemos que para todo $b \in B'$, $(rg)(b) \neq 0$, de donde se sigue que $rg \in I$. Luego I absorbe escalares por la izquierda y por lo tanto I es un ideal izquierdo de R.

Suponiendo que I es de generación finita, tenemos que existen $f_1 \ldots, f_n$ tales que $I = \langle f_1 \ldots, f_n \rangle$. Entonces para cada $i \in \{1, \ldots, n\}$, hacemos $J_i = \{x \in [0,1] \mid f_i(x) \neq 0\}$, de donde se sigue que para cada $i \in \{1, \ldots, n\}$, J_i es finito y así también $J = \bigcup_{i=1}^n J_i \subseteq [0,1]$ es finito, entonces hay un $x \in [0,1]$ tal que $x \notin J$. Sea $f_x : [0,1] \to \mathbb{R}$ tal que $f_x(x) = 1$ y $f_x(y) = 0$ si $y \neq x$, entonces $f_x \in I$, es decir, existen $g_1 \ldots, g_n \in R$ tal que $f_x = \sum_{i=1}^n g_i f_i$, lo que implica que $1 = f_x(x) = \sum g_i f_i(x) = 0$ que es una contradicción. Por lo tanto, I no es finitamente generado.

Proposición 1.6.2 *Si* $0 \longrightarrow M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$ *es una sucesión exacta corta de* R*-módulos. Entonces:*

(1) *Si* M_2 *finitamente generado, entonces* M_3 *es finitamente generado.*

(2) *Si* M_1 *y* M_3 *son finitamente generados, entonces* M_2 *es finitamente generado.*

Demostración.

(1) Sean $y_1, \ldots, y_n \in M_2$ tales que $M_2 = \langle y_1, \ldots, y_n \rangle$ y $z \in M_3$. Como g es un epimorfismo, hay un $y \in M_2$ tal que $g(y) = z$, entonces existen $r_1, \ldots, r_n \in R$ tales que $y = \sum r_i y_i$, de donde $z = g(y) = \sum r_i g(y_i)$, lo que implica que $M_3 = \langle g(y_1), \ldots, g(y_n) \rangle$.

(2) Sean $M_1 = \langle x_1, \ldots, x_r \rangle$ y $M_3 = \langle z_1, \ldots, z_s \rangle$. Como g es epimorfismo, para cada z_i con $i = 1, \ldots, s$, hay un $y_i \in M_2$ tal que $g(y_i) = z_i$.

Afirmamos que $M_2 = \langle f(x_1), \ldots, f(x_r), y_1, \ldots, y_s \rangle$.

Sea $y \in M_2$, luego $g(y) \in M_3$, entonces existen $r_1, \ldots, r_s \in R$ tales que $g(y) = \sum r_i z_i = \sum r_i g(y_i) = g(\sum r_i y_i)$, entonces $g(y) - g(\sum r_i y_i) = g(y - \sum r_i y_i) = 0$, de donde tenemos que $y - \sum r_i y_i \in \ker(g) = Im(f) \cong M_1$ vía f, lo que implica que $Im(f) = \langle f(x_1), \ldots, f(x_r) \rangle$, entonces existen $b_1, \ldots, b_r \in R$ tales que $y - \sum_{i=1}^s r_i y_i = \sum_{i=1}^r b_i f(x_i)$, con lo cual tenemos que $y = \sum_{i=1}^r b_i f(x_i) + \sum_{i=1}^s r_i y_i$.

□

Corolario 1.6.3 *Si* M *es un* R*-módulo finitamente generado y* N *es un submódulo de* M*, entonces* M/N *es un* R*-módulo finitamente generado.*

Demostración. Considere la sucesión exacta corta

$$0 \longrightarrow N \xrightarrow{i} M \xrightarrow{\pi} M/N \longrightarrow 0$$

donde i es la inclusión y π es la proyección canónica. □

Proposición 1.6.4 *Sea $J(R)$ el ideal de Jacobson, esto es, la intersección de todos los ideales maximales de R. Entonces $a \in J(R)$ si y sólo si para todo $r \in R$, $1 + ar$ es un unidad.*

Demostración. ($\Rightarrow$) Supongamos que hay un $r \in R$ tal que $1+ar$ no es una unidad, entonces $1 + ar$ genera un ideal propio, el cual está contenido en algún ideal maximal $\mathfrak{m}$. Luego, $1 + ar \in \mathfrak{m}$. Pero $a \in J(R) \subseteq \mathfrak{m}$, entonces $ar \in \mathfrak{m}$. Por lo tanto, $1 \in \mathfrak{m}$, que es una contradicción.

($\Leftarrow$) Supongamos que $a \notin J(R)$, entonces hay un ideal maximal $\mathfrak{m}$ tal que $a \notin \mathfrak{m}$ y el ideal $\mathfrak{m} + \langle a \rangle$ contiene a $\mathfrak{m}$. Luego $\mathfrak{m} + \langle a \rangle = R$. De esta manera, existen $b \in \mathfrak{m}$ y $s \in R$ tales que $b + as = 1$. Entonces $b = 1 - as \in \mathfrak{m}$ no es una unidad. Luego para $s = -r$, $1 + ar$ no es una unidad. □

Proposición 1.6.5 *Si M es un R-módulo finitamente generado e I es un ideal de R tal que $IM = M$, entonces existe un $a \in I$ tal que $(1 + a)M = 0$.*

Demostración. Sean $x_1, \ldots, x_n$ los generadores de M. Como $IM = M$, se sigue que para cada $i \in \{1, \ldots, n\}$, $x_i = \sum_{j=1}^n r_{ij}x_j$, donde los $r_{ij} \in I$. Entonces $x_i - \sum_{j=1}^n r_{ij}x_j = \sum_{j=1}^n (\delta_{ij} - r_{ij})x_j = 0$. Este sistema de ecuaciones se puede representar en forma matricial como sigue: $(\delta_{ij} - r_{ij})X = (1_n - (r_{ij}))X = 0$, donde 1_n es la matriz identidad $n \times n$ y X un vector columna cuyas entradas son los x_i. Multiplicando a la izquierda por la adjunta de $(1_n - (r_{ij}))$ obtenemos $0 = adj\big(1_n - (r_{ij})\big)\big((1_n - (r_{ij}))X\big) = \big(adj(1_n - (r_{ij}))(1_n - (r_{ij}))\big)X = (a_{ij})X$, donde $a_{ij} = det\big(1_n - (r_{ij})\big)$ si $i = j$ y $a_{ij} = 0$ si $i \neq j$. Entonces para cada $i \in \{1, \ldots, n\}$, $det\big(1_n - (r_{ij})\big)x_i = 0$; de aquí, $det\big(1_n - (r_{ij})\big)M = 0$. De aquí, $det\big(1_n - (r_{ij})\big)$ es de la forma $1 + a$, para algún $a \in I$. □

Proposición 1.6.6 (Lema de Nakayama) *Sean M un R-módulo finitamente generado e I un ideal de R tal que $I \subseteq J(R)$.*

(1) *Si $IM = M$, entonces $M = 0$.*

(2) *Si N es un submódulo de M y $M = IM + N$, entonces $M = N$.*

Demostración.

(1) De 1.6.5, tenemos que hay un $a \in I$ tal que $(1+a)M = 0$. Como $I \subseteq J(R)$, $1 + a$ es una unidad, de acuerdo con 1.6.4. Multiplicando la ecuación $(1 + a)M = 0$ por el inverso de $1 + a$ tenemos que $M = 0$.

(2) De 1.6.3, tenemos que M/N es finitamente generado.

Afirmamos que $I(M/N) = M/N$. Sabemos que $I(M/N)$ es un submódulo de M/N. Así que sólo hay que probar que $M/N \subseteq I(M/N)$. Sea $m + N \in M/N$. Como $m \in M = IM + N$, $m = \sum_{fin} r_i m_i + n$, con $r_i \in I$, $m_i \in M$ y $n \in N$. Entonces $m + N = (\sum_{fin} r_i m_i + n) + N = \sum_{fin} r_i m_i + N = \sum_{fin}(r_i m_i + N) = \sum_{fin} r_i(m_i + N) \in I(M/N)$. Así, $I(M/N) = M/N$. Luego, aplicando el inciso anterior tenemos que $M = N$.

□

Proposición 1.6.7 *Sea $(R, \mathfrak{m})$ un anillo local y M un R-módulo finitamente generado, entonces*

(1) *$M/\mathfrak{m}M$ es un $R/\mathfrak{m}$-espacio vectorial de dimensión finita.*

(2) *Si $\{x_1 + \mathfrak{m}M, \ldots, x_n + \mathfrak{m}M\}$ es una base para $M/\mathfrak{m}M$ sobre $R/\mathfrak{m}$, entonces $\{x_1, \ldots, x_n\}$ es un conjunto minimal de generadores para M.*

(3) *Cualesquiera dos conjuntos minimales generadores para M tienen la misma cardinalidad.*

Demostración.

(1) Como $\mathfrak{m} \subseteq Ann(M/\mathfrak{m}M)$, se puede considerar a $M/\mathfrak{m}M$ como $R/\mathfrak{m}$-módulo, esto es, como un $R/\mathfrak{m}$-espacio vectorial. Por hipótesis, M es finitamente generado, digamos $M = \langle x_1, \ldots, x_l \rangle$. Entonces, al tomar un elemento $m + \mathfrak{m}M \in M/\mathfrak{m}M$ tenemos que $m + \mathfrak{m}M = \sum_{i=1}^{l} r_i(x_i + \mathfrak{m}M) = \sum_{i=1}^{l}(r_i + \mathfrak{m})(x_i + \mathfrak{m}M)$, o sea que $M/\mathfrak{m}M$ es finitamente generado sobre $R/\mathfrak{m}$ y por lo tanto es finito dimensional.

(2) Considermos el submódulo $N = \langle x_1, \ldots, x_n \rangle$ de M.

   Afirmamos que $M = N + \mathfrak{m}M$. En efecto, si $m \in M$, entonces $m + \mathfrak{m}M = \sum_{i=1}^{n}(r_i + \mathfrak{m})(x_i + \mathfrak{m}M) = \sum_{i=1}^{n} r_i(x_i + \mathfrak{m}M) = \sum_{i=1}^{n}(r_i x_i + \mathfrak{m}M) = \sum_{i=1}^{n} r_i x_i + \mathfrak{m}M$, o sea que $m - \sum_{i=1}^{n} r_i x_i \in \mathfrak{m}M$ y por tanto $m \in N + \mathfrak{m}M$.

   Luego, de la afirmación y el lema de Nakayama se sigue que $M = N$.

   Ahora supongamos que un subconjunto propio de los x_i genera a M, entonces el conjunto correspondiente de las clases $x_i + \mathfrak{m}M$ genera a $M/\mathfrak{m}M$, lo cual contradice el hecho de que $M/\mathfrak{m}M$ es n-dimensional.

(3) Supongamos que S es un conjunto generador para M con más de n elementos, entonces S determina un conjunto generador para $M/\mathfrak{m}M$, el cual contiene una base con n elementos. Luego por (2), S no puede ser minimal.

□

1.7. Módulos noetherianos

Proposición 1.7.1 *Sea P un conjunto parcialmente ordenado. Las siguientes condiciones en P son equivalentes:*

(1) *Cada sucesión creciente $x_1 \leq x_2 \leq \ldots$ en P es estacionaria (es decir, existe un natural n tal que $x_n = x_{n+1} = \ldots$).*

(2) *Cada subconjunto no vacío de P tiene un elemento maximal.*

Demostración. (1) $\Rightarrow$ (2) Supongamos que hay un subconjunto T de P no vacío que no tiene elemento maximal, esto es, para cada $x \in T$ hay un $y \in T$ tal que $x \leq y$ y $x \neq y$. Así para $x_1 \in T$ hay un $x_2 \in T$ tal que $x_1 \leq x_2$ y $x_1 \neq x_2$. De este modo también tenemos que para x_2 hay un $x_3 \in T$ tal que $x_2 \leq x_3$ y $x_2 \neq x_3$, además $x_1 \neq x_3$, pues si $x_1 = x_3$ tendríamos que $x_1 \leq x_2$ y $x_2 \leq x_3 = x_1$ y así $x_1 = x_2$, lo cual es una contradicción. De este modo podemos construir inductivamente una sucesión en T estrictamente creciente que no termina.

(2) $\Rightarrow$ (1) Tomemos una sucesión creciente en P, $x_1 \leq x_2 \leq \ldots$, entonces el conjunto A de los x_m tiene un elemento maximal, esto es, hay un $m \in \mathbb{N}$ tal que para cada $n \in \mathbb{N}$ con $m \leq n$, $x_m \leq x_n$ implica que $x_m = x_n$. Así, $(x_m)_{m\in\mathbb{N}}$ es estacionaria. □

Observación. Si P es un conjunto de submódulos de un módulo M, ordenado por la relación $\subseteq$, entonces a la propiedad (1) le llamamos **condición de cadena ascendente** y a (2) la **condición maximal**.

Definición 1.7.2 *Un módulo que satisface una de estas dos condiciones se denomina **noetheriano**.*

Proposición 1.7.3 *M es un R-módulo noetheriano si y sólo si cada submódulo de M es finitamente generado.*

Demostración. Sean M es un R-módulo que verifica la condición maximal y N un submódulo de M. Queremos ver que N es finitamente generado, para esto, definimos $P = \{T : T \text{es submódulo de M de generación finita y } T \subseteq N\}$. Como $P \neq \emptyset$ (pues $\langle 0 \rangle \in P$), entonces existe $N_0 \in P$ tal que N_0 es maximal. Si $N_0 \neq N$, entonces hay un $x \in N - N_0$. Ahora, como N_0 y $\langle x \rangle$ están en P se sigue que $N_0 + \langle x \rangle \in P$ y $N_0 \subsetneq N_0 + \langle x \rangle$, ya que $x \in N_0 + \langle x \rangle$ y $x \notin N_0$, lo cual es una contradicción. Luego $N_0 = N$ y por lo tanto, N es de generación finita.

Para el recíproco tomamos una sucesión creciente $M_1 \subseteq M_2 \subseteq \ldots$ de submódulos de M, entonces $N = \bigcup M_i$ es un submódulo de M y por hipótesis N es finitamente generado. Supongamos que $N = \langle x_1, \ldots, x_r \rangle$, entonces para todo $i \in \{1, \ldots, r\}$, existe $n_i \in \mathbb{N}$ tal que $x_i \in M_{n_i}$. Sea $n = max\{n_1, \ldots, n_r\}$, entonces para todo $i \in \{1, \ldots, r\}$, $x_i \in M_n$ y de aquí tenemos que $N \subseteq M_n$ y $M_n \subseteq N$, es decir, $M_n = N$. Entonces para cada $m \in \mathbb{N}$ tal que $m \geq n$, $M_m \subseteq M_{m+1} \subseteq N \subseteq M_n \subseteq M_m$, así que, $M_m = M_{m+1}$, con lo cual tenemos que la sucesión (M_i) es estacionaria. □

Ejemplos.

1. Si M es el R-módulo nulo, $M = \langle 0 \rangle$ es noetheriano.

2. Si M es un R-módulo simple (esto es, los únicos submódulos de M son 0 y M) o si M tiene un número finito de submódulos, entonces M es noetheriano.

3. Si R es principal entonces R es un R-módulo noetheriano.

4. Si K es un campo, entonces un K-espacio vectorial V es noetheriano si y sólo si $dimV < \infty$.

Proposición 1.7.4 *Si N es un submódulo de un R-módulo M, entonces M es noetheriano si y sólo si N y M/N son noetherianos.*

Demostración. Primero mostraremos que N es noetheriano. Sí N' es un sub-módulo de N, entonces N' submódulo de M y de aquí tenemos que N' es finitamente generado. Luego N es noetheriano.

Ahora probemos que M/N es noetheriano. Sea $K_1 \subseteq K_2 \subseteq \dots$ una sucesión creciente de submódulos de M/N, entonces por 1.1.9 tenemos que hay una sucesión creciente $J_1 \subseteq J_2 \subseteq \dots$ de submódulos de M tal que cada J_i contiene a N y $K_i \cong J_i/N$ para cada i. Como M es noetheriano, la sucesión (J_i) es estacionaria. Luego la sucesión (K_i) es estacionaria.

Para el recíproco tomamos una sucesión (M_i) creciente de submódulos de M, entonces para la sucesión creciente $(M_i \cap N)$ de submódulos de N hay un $i \in \mathbb{N}$ tal que $M_i \cap N = M_{i+1} \cap N = \dots$ y para la sucesión creciente$((M_i + N)/N)$ de submódulos de M/N hay un $j \in \mathbb{N}$ tal que $(M_j + N)/N = (M_j + 1 + N)/N = \cdots$. Sean $k = max\{i, j\}$ y $a \in M_{k+1} \subseteq M_{k+1} + N$, entonces $a + N \in (M_{k+1} + N)/N = (M_k + N)/N$, lo que implica que $a \in M_k + N$ y de aquí tenemos que existen $b \in M_k \subseteq M_{k+1}$ y $c \in N$ tales que $a = b + c$. De esto se sigue que $a - b = c \in M_{k+1} \cap N = M_k \cap N \subseteq M_k$ y por tanto $b + c = a \in M_k$. □

Proposición 1.7.5 *Sea* $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$ *una sucesión exacta de R-módulos.*

(1) *Si N es noetheriano entonces M y T son noetherianos.*

(2) *Si M y T son noetherianos entonces N es noetheriano.*

Demostración.

(1) Como f es monomorfismo se sigue que $M \cong Im(f)$ es un submódulo de N y de aquí $M \cong Im(f)$ es noetheriano. Por otra parte, dado que g es epimorfismo tenemos que $T \cong N/\ker(g)$ es noetheriano por ser N noetheriano.

(2) Tomamos un submódulo U de N, entonces $f^{-1}(U)$ y $g(U)$ son submódulos de M y T, respectivamente. Ahora consideremos la sucesión exacta

$$0 \longrightarrow f^{-1}(U) \xrightarrow{f} U \xrightarrow{g} g(U) \longrightarrow 0.$$

Como M y T son noetherianos se sigue que $f^{-1}(U)$ y $g(T)$ son de generación finita, lo que implica que U también es de generación finita y por lo tanto N es noetheriano.

□

Corolario 1.7.6 *Si $\{M_i\}_{i=1}^n$ es una familia finita de R-módulos noetherianos, entonces también $\bigoplus_{i=1}^n M_i$ es noetheriano.*

Demostración. Aplicamos inducción y la proposición anterior a la sucesión exacta

$$0 \longrightarrow M_n \longrightarrow \bigoplus_{i=1}^{n} M_i \longrightarrow \bigoplus_{i=1}^{n-1} M_i \longrightarrow 0.$$

□

Observación. Ser noetheriano no se preserva por sumas directas infinitas ni por productos infinitos, por ejemplo, $\mathbb{Z}$ es un $\mathbb{Z}$-módulo noetheriano (ya que es principal), pero $\mathbb{Z}^{(\mathbb{N})}$ no es noetheriano, pues la sucesión creciente de submódulos $\langle e_1\rangle \subseteq \langle e_1, e_2\rangle \subseteq \langle e_1, e_2, e_3\rangle \subseteq \dots$, de $\mathbb{Z}^{(\mathbb{N})}$ (donde $e_i = (0, \dots, 0, 1, 0, \dots) \in \mathbb{Z}^{(\mathbb{N})}$ y el 1 está en el i-ésimo lugar) no es estacionaria. Además, como $\mathbb{Z}^{(\mathbb{N})}$ es un submódulo de $\mathbb{Z}^{\mathbb{N}}$, entonces $\mathbb{Z}^{\mathbb{N}}$ tampoco es noetheriano.

Definición 1.7.7 *Un anillo R es un **anillo noetheriano** si R es un R-módulo noetheriano.*

Ejemplos.

1. $\mathbb{Z}$ y $K[x]$ con K un campo, son anillos noetherianos por ser principales.

2. El anillo de polinomios $R = K[x_1, x_2, \dots]$ con un número infinito de indeterminadas, no es un anillo noetheriano, porque el ideal $\langle x_1, x_2, \dots\rangle$ generado por las indeterminadas no es finitamente generado, sin embargo, es un dominio entero, por lo que se le puede considerar como un subanillo de su campo de fracciones, el cual es un anillo noetheriano ya que sus únicos ideales son el cero y él mismo. Esto muestra que subanillos de anillos noetherianos no necesariamente son noetherianos.

Proposición 1.7.8 *Si R es un anillo noetheriano y M es un R-módulo finitamente generado, entonces M es noetheriano.*

Demostración. Supongamos que $M = \langle m_1, \dots, m_n\rangle$. Tomando el epimorfismo $f : \bigoplus_{i=1}^n R \to M$ que a $(r_1, \dots, r_n)$ le asocia $\sum_{i=1}^n r_i m_i$, tenemos que $M \cong (\bigoplus_{i=1}^n R)/\ker(f)$. Como R es noetheriano, $\bigoplus_{i=1}^n R$ es noetheriano. Luego $\bigoplus_{i=1}^n R/\ker(f)$ es noetheriano. □

Teorema 1.7.9 (de la base de Hilbert) *Si R un anillo noetheriano, entonces R[x] es un anillo noetheriano.*

Demostración. Sea J un ideal izquierdo de $R[x]$. Veamos que J es finitamente generado como $R[x]$-módulo.

Consideremos el siguiente conjunto

$$I = \left\{ r \in R : \text{para algún p(x)} \in J \subseteq R[x],\ p(x) = \sum_{i=0}^{m-1} r_i x^i + r x^m \right\}$$

y probemos que I es un ideal izquierdo de R.

$I \neq \emptyset$, pues $0 \in I$.

Ahora sean $r, s \in I$. Si $r = s$, entonces $r - s = 0 \in I$. Si $r \neq s$, existen $p(x), q(x) \in J$ tales que $p(x) = \sum_{i=1}^{m-1} r_i x^i + r x^m$ y $q(x) = \sum_{i=1}^{n-1} s_i x^i + s x^n$. Sin pérdida de generalidad, supongamos que $m \geq n$, entonces $x^{m-n} q(x) = \sum_{i=1}^{n-1} s_i x^{m-(n-i)} + s x^m \in J$ tiene a s como coeficiente principal, lo que implica que $p(x) - x^{m-n} q(x) \in J$ tiene a $r - s$ como coeficiente principal. Así que $r - s \in I$.

Si $s \in I$ y $r \in R$, entonces hay un $p(x) \in J$ tal que s es el coeficiente principal de $p(x)$ y de esto tenemos que $rp(x) \in J$ y rs es el coeficiente principal de $rp(x)$, lo que implica que $rs \in I$

Por lo tanto, I es un ideal izquierdo de R.

Ahora, como R es noetheriano, I es finitamente generado (como R-módulo), es decir, existen $a_1, \ldots, a_r \in I$ tales que $I = \langle a_1, \ldots, a_r \rangle$. Entonces para cada a_i, existe $p_i(x) \in J$ tal que a_i es el coeficiente principal de $p_i(x)$. Podemos suponer que todos los $p_i(x)$ son del mismo grado m (en caso contrario multiplicamos cada $p_i(x)$ por $x^{m - grad(p_i)}$, donde m es el máximo de los grados de los p_i).

Sea N el R-módulo cuyos elementos están en J y son de grado menor que m, es decir, $N = J \cap R_{<m}[x]$. Así tenemos que $R_{<m}[x]$ es un R-módulo de generación finita ($R_{<m}[x]$ está generado por $1, x, x^2, \ldots, x^{m-1}$) y R es noetheriano, entonces $R_{<m}[x]$ es un R-módulo noetheriano, lo que implica que $N \subseteq R_{<m}[x]$ es un submódulo finitamente generado. Sean $q_1(x), \ldots, q_s(x) \in N$ un sistema de generadores (sobre R) de N.

Afirmamos que J es generado por $p_1(x), \ldots, p_r(x), q_1(x), \ldots, q_s(x)$ como $R[x]$-módulo. Sea $p(x) \in J$.

Si $grad(p(x)) < m$, entonces $p(x) \in R_{<m}[x]$, lo que implica que $p(x) \in J$ y $p(x) \in R_{<m}[x]$ y así $p(x) \in N = \langle q_1(x), \ldots, q_s(x) \rangle_R \subseteq \langle q_1(x), \ldots, q_s(x) \rangle_{R[x]}$.

Si $grad(p(x)) = g \geq m$ razonaremos inductivamente (suponemos que para todo $t(x) \in J$ tal que $m \leq grad(t(x)) < g$, $t(x) \in \langle p_1(x), \ldots, p_r(x), q_1(x), \ldots, q_s(x) \rangle_{R[x]}$). Sea a el coeficiente principal de $p(x)$, entonces $a \in I$, lo que implica que $a = \sum_{i=1}^{r} \lambda_i a_i$, donde $\lambda_i \in R$. Consideremos el siguiente polinomio:

$$\begin{aligned}
\tilde{p}(x) &= x^{g-m} \sum_{i=1}^{r} \lambda_i p_i(x) = x^{g-m}[\lambda_1 p_1(x) + \cdots + \lambda_r p_r(x)] \\
&= x^{g-m}[\lambda_1(\sum_{i=0}^{m-1} a_{1i}x^i + a_1 x^m) + \cdots + \lambda_r(\sum_{i=0}^{m-1} a_{ri}x^i + a_r x^m)] \\
&= (\sum_{i=0}^{m-1} \lambda_1 a_{1i} x^{g-(m-i)} + \lambda_1 a_1 x^g) + \cdots + (\sum_{i=0}^{m-1} \lambda_r a_{ri} x^{g-(m-i)} + \lambda_r a_r x^g) \\
&= (\sum_{i=1}^{r} \lambda_i a_{i0}) x^{g-m} + (\sum_{i=1}^{r} \lambda_i a_{i1}) x^{g-(m-1)} + \cdots + (\sum_{i=1}^{r} \lambda_i a_i) x^g
\end{aligned}$$

el cual pertenece a J y tiene a a como coeficiente principal. Si tomamos el polinomio $p(x)-\tilde{p}(x)$, que es un polinomio en J (pues $p(x)$ y $\tilde{p}(x)$ están en J) tal que $grad(p(x)-\tilde{p}(x)) < grad(p(x))$ (no olvidemos que $grad(p(x)) = g = grad(\tilde{p}(x))$ y a es el coeficiente principal de ambos), entonces por la hipótesis de inducción, $p(x) - \tilde{p}(x) \in \langle p_1(x), \ldots, p_r(x), q_1(x), \ldots, q_s(x)\rangle_{R[x]}$. De aquí que $p(x) - \tilde{p}(x) = \sum_{i=1}^{r} u_i(x)p_i(x) + \sum_{i=1}^{s} v_i(x)q_i(x)$, o sea que $p(x) = \sum_{i=1}^{r} u_i(x)p_i(x) + \sum_{i=1}^{s} v_i(x)q_i(x) + \tilde{p}(x) \in \langle p_1(x), \ldots, p_r(x), q_1(x), \ldots, q_s(x)\rangle_{R[x]}$, ya que $\tilde{p}(x) \in \langle p_1(x), \ldots, p_r(x), q_1(x), \ldots, q_s(x)\rangle_{R[x]}$. □

Corolario 1.7.10 *Si R es un anillo noetheriano, entonces $R[x_1, \ldots, x_n]$ es un anillo noetheriano.*

Demostración. Escribimos $R[x_1, \ldots, x_n] = (R[x_1, \ldots, x_{n-1}])[x_n]$ y aplicamos inducción más el teorema de Hilbert. □

1.8. Producto tensorial de módulos

Definición 1.8.1 *Sean M un R-módulo derecho, N un R-módulo izquierdo y U un grupo abeliano. A una aplicación $f : M \times N \to U$ se le llama* ***R-balanceada*** *si para cada $m, m' \in M$; $n, n' \in N$ y $r \in R$ se cumplen las siguientes propiedades:*

(1) $f(m + m', n) = f(m, n) + f(m', n)$.

(2) $f(m, n + n') = f(m, n) + f(m, n')$.

(3) $f(mr, n) = f(m, rn)$.

Teorema 1.8.2 *Sean M un R-módulo derecho y N un R-módulo izquierdo. Entonces existe una única pareja (T, t), donde T es un grupo abeliano y $t : M \times N \to T$ es una aplicación R-balanceada tal que:*

(1) *Si $x \in T$ entonces $x = \sum_{fin} t(m_i, n_i)$.*

(2) *Si H es un grupo abeliano y $\varphi : M \times N \to H$ una aplicación R-balanceada, entonces existe un único morfismo $\theta : T \to H$ que hace conmutar el diagrama*

$$\begin{tikzcd} & T \arrow[d, dotted, "\theta"] \\ M \times N \arrow[ur, "t"] \arrow[r, "\varphi"'] & H \end{tikzcd}$$

Demostración. Primero mostraremos la existencia de (T, t).

Sea F el grupo abeliano ($\mathbb{Z}$-módulo) libre sobre $M \times N$, es decir, $F = \bigoplus_{M \times N} \mathbb{Z}$. Con $1_{m,n}$ denotaremos al elemento de F cuyo valor es uno en la entrada (m, n)-ésima y cero en todos los demás registros. La aplicación $i : M \times N \to F$ que a $(m, n) \in M \times N$ le asigna $1_{m,n} \in F$ es precisamente la que especifica a F como un grupo abeliano libre en $M \times N$. Sea G el subgrupo de F generado por elementos de la forma:

$$1_{m+m',n} - 1_{m,n} - 1_{m',n} \qquad 1_{m,n+n'} - 1_{m,n} - 1_{m,n'} \qquad 1_{mr,n} - 1_{m,rn}.$$

Como F es abeliano y G un subgrupo de F, entonces F/G es abeliano.

Sea $T := F/G$ y escribimos $m \otimes n$ para la clase de $1_{m,n}$ en T. Definimos la aplicación $t : M \times N \to T$ por $t(m, n) = m \otimes n = 1_{m,n} + G \in T$, la cual cumple que:

$t(m + m', n) - t(m, n) - t(m', n) = (m + m') \otimes n - m \otimes n - m' \otimes n = (1_{m+m',n}+G)-(1_{m,n}+G)-(1_{m',n}+G) = (1_{m+m',n}-1_{m,n}-1_{m',n})+G = 0,$

$t(m, n + n') - t(m, n) - t(m, n') = m \otimes (n + n') - m \otimes n - m \otimes n' = (1_{m,n+n'}+G)-(1_{m,n}+G)-(1_{m,n'}+G) = (1_{m,n+n'}-1_{m,n}-1_{m,n'})+G = 0,$

$t(mr, n) - t(m, rn) = mr \otimes n - m \otimes rn = (1_{mr,n} + G) - (1_{m,rn} + G) = (1_{mr,n} - 1_{m,rn}) + G = 0,$

o sea que t es R-balanceada.

Así tenemos una pareja (T, t) con T abeliano y t una aplicación R-balanceada.

Verifiquemos la propiedad (1). Sea $x \in T$, entonces $x = \sum_{fin} z_{kl}(m_k, n_l)+G$, donde $z_{kl} \in \mathbb{Z}$, $m_k \in M$ y $n_l \in N$. Luego, $x = \sum_{fin} z_{kl}(m_k, n_l) + G = \sum_{fin} z_{kl}[(m_k, n_l)+G] = \sum_{fin} z_{kl}t(m_k, n_l) = \sum_{fin} t(z_{kl}m_k, n_l)$ (la última igualdad se prueba primero haciendo $z = 0$, después para $z > 0$ usamos inducción y finalmente se prueba para $z < 0$).

Continuamos ahora con la prueba de (2). Sea H es un grupo abeliano y sea $\varphi : M \times N \to H$ es una aplicación R-balanceada, entonces como F es libre, se sigue que hay un único morfismo $f : F \to H$ que hace que el diagrama

$$\begin{tikzcd} H & F \arrow[l, "f"'] \\ & M \times N \arrow[ul, "\varphi"] \arrow[u, "i"'] \end{tikzcd}$$

conmute. Así, tenemos que el siguiente diagrama es conmutativo

$$
\begin{tikzcd}
F \arrow[r, "f"] \arrow[d, "\pi"'] & H \\
F/G \arrow[ur, dotted, "\theta"'] &
\end{tikzcd}
$$

ya que f anula a lo generadores de G, luego, f anula a $G = \ker(\pi)$ y así, $\ker(\pi) \subseteq \ker(f)$; lo que garantiza la existencia del morfismo θ. Entonces $\varphi = f \circ i = (\theta \circ \pi) \circ i = \theta \circ (\pi \circ i) = \theta \circ t$.

Veamos la unicidad del morfismo θ. Supongamos que $\theta' : T \to H$ es otro morfismo de grupos tal que $\theta' \circ t = \varphi$, entonces $\theta(t(m,m)) = \varphi(m,n) = (\theta' \circ t)(m,n) = \theta'(t(m,n))$; o sea que $\theta' = \theta$ en los generadores de T, por lo tanto, $\theta' = \theta$.

Finalmente verifiquemos que (T,t) es la única pareja con las propiedades (1) y (2). Supongamos que (U,t'), donde U es un grupo abeliano y $t' : M \times N \to U$ es una aplicación R-balanceada, cumple las condiciones del teorema 1.8.2. Veamos que $U \cong T$. Como (T,t) y (U,t') satisfacen las condiciones del teorema 1.8.2, entonces existen únicos morfismos de grupos $\psi : T \to U$ y $\psi' : U \to T$ tales que hacen conmutar los diagramas

$$
\begin{tikzcd}
 & T \arrow[d, dotted, "\psi"] \\
M \times N \arrow[ur, "t"] \arrow[r, "t'"'] & U
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
 & U \arrow[d, dotted, "\psi'"] \\
M \times N \arrow[ur, "t'"] \arrow[r, "t"'] & T
\end{tikzcd}
$$

Veamos qué ocurre al aplicar $\psi' \circ \psi$ a los generadores de $M \otimes_R N$.

$(\psi' \circ \psi)(t(m,n)) = \psi'((\psi \circ t)(m,n)) = \psi'(t'(m,n)) = t(m,n)$, o sea que $\psi' \circ \psi = 1_{M \otimes_R N}$.

Análogamente se prueba que $\psi \circ \psi' = 1_U$.

Por lo tanto, $U \cong T$. □

Notación. Con $M \otimes_R N$ o $M \otimes N$ se denota a T en el teorema anterior.

Definición 1.8.3 *Al grupo abeliano $M \otimes_R N$ se le llama **grupo producto tensorial** de M y N.*

Proposición 1.8.4 *Sea R un anillo conmutativo con elemento unitario. Si M es un R-módulo derecho, N es un R-módulo izquierdo y $r \in R$, entonces hay un único morfismo de grupos $\theta_r : M \otimes_R N \to M \otimes_R N$ definido por $\theta_r(m \otimes n) = mr \otimes n$.*

Demostración. Definimos la aplicación $\varphi : M \times N \to M \otimes_R N$ por $\varphi(m,n) := mr \otimes n$. Se verifica fácilmente que φ es R-balanceada teniendo en cuenta la conmutatividad de R. Entonces por 1.8.2, hay un único morfismo de grupos $\theta_r : M \otimes_R N \to M \otimes_R N$ tal que $\theta_r \circ t = \varphi$. Entonces $\theta_r(m \otimes n) = \theta_r(t(m,n)) = \varphi(m,n) = mr \otimes n$. □

Proposición 1.8.5 *Si R es un anillo conmutativo con elemento unitario, M un R-módulo derecho y N un R-módulo izquierdo, entonces $M \otimes_R N$ admite una estructura de R-módulo con el siguiente producto:*

$$r \sum_{fin} (m_i \otimes n_i) := \sum_{fin} (m_i r \otimes n_i).$$

Demostración. Primero veamos que el producto está bien definido. Para esto, sean $r \in R$ y $\sum_{fin}(m_i \otimes n_i) \in M \otimes_R N$. Luego por 1.8.4, existe un único morfismo de grupos $\theta_r : M \otimes_R N \to M \otimes_R N$ definido por $\theta_r(m \otimes n) = mr \otimes n$. Entonces $r \sum_{fin}(m_i \otimes n_i) = \sum_{fin}(m_i r \otimes n_i) = \sum_{fin} \theta_r(m_i \otimes n_i) = \theta_r(\sum_{fin}(m_i \otimes n_i)) \in M \otimes_R N$.

Fácilmente se verifica que $M \otimes_R N$ satisface las propiedades para ser un R-módulo, teniendo en cuenta que R es conmutativo. □

Proposición 1.8.6 *Sea R un anillo conmutativo con elemento unitario. Si $f : M \to M'$ es un morfismo de R-módulos derechos y $g : N \to N'$ es morfismo de R-módulos izquierdos, entonces hay un único morfismo de R-módulos $f \otimes g : M \otimes_R N \to M' \otimes_R N'$ definido por $(f \otimes g)(m \otimes n) := f(m) \otimes g(n)$ (si R no es conmutativo, $f \otimes g$ es un morfismo de grupos).*

Demostración. Definimos la aplicación $\varphi : M \times N \to M' \otimes_R N'$ por $\varphi(m,n) := f(m) \otimes g(n)$. Es fácil ver que φ es R-balanceada. Entonces de 1.8.2 se sigue que hay un único morfismo de grupos $f \otimes g : M \otimes_R N \to M' \otimes_R N'$ tal que $(f \otimes g) \circ t = \varphi$. Luego, $(f \otimes g)(m \otimes n) = (f \otimes g)(t(m,n)) = ((f \otimes g) \circ t)(m,n) = \varphi(m,n) = f(m) \otimes g(n)$.

Se puede mostrar sin mayor problema que si $r \in R$ y $\sum_{fin}(m_i \otimes n_i) \in M \otimes_R N$, entonces $r(f \otimes g)(\sum_{fin}(m_i \otimes n_i)) = (f \otimes g)(r \sum_{fin}(m_i \otimes n_i))$, es decir, $f \otimes g$ es un morfismo de R-módulos. □

Proposición 1.8.7 *Si $M \xrightarrow{f} M' \xrightarrow{f'} M''$ son morfismos de R-módulos derechos y $N \xrightarrow{g} N' \xrightarrow{g'} N''$ son morfismos de R-módulos izquierdos, entonces $(f' \otimes g') \circ (f \otimes g) = (f' \circ f) \otimes (g' \circ g)$.*

Demostración. Sean $m \in M$ y $n \in N$, entonces

$$\begin{aligned}((f' \otimes g') \circ (f \otimes g))(m,n) &= (f' \otimes g')((f \otimes g)(m,n)) \\ &= (f' \otimes g')(f(m) \otimes g(n)) = (f'(f(m)) \otimes g'(g(n))) \\ &= (f' \circ f)(m) \otimes (g' \circ g)(n) = ((f' \circ f) \otimes (g' \circ g))(m,n).\end{aligned}$$

Por lo tanto, $(f' \otimes g') \circ (f \otimes g) = (f' \circ f) \otimes (g' \circ g)$. □

Proposición 1.8.8 *Supongamos que M es un R-módulo izquierdo*

(1) *$R \otimes_R M \cong M$ como grupos abelianos.*

(2) *Si $f : M \to N$ es un morfismo de R-módulos, entonces conmuta el cuadrado del siguiente diagrama:*

$$\begin{tikzcd}
 & R \otimes_R M \arrow[r, "1_R \otimes f"] \arrow[d, "u"] & R \otimes_R N \arrow[d, "v"] & \\
R \times M \arrow[ur, "t_1"] \arrow[r, "t_1'"'] & M \arrow[r, "f"] & N & R \times N \arrow[ul, "t_2"'] \arrow[l, "t_2'"]
\end{tikzcd}$$

donde u y v son los isomorfismos que están garantizados por el inciso (1).

(3) *$(R/I) \otimes_R M \cong M/IM$ si I es un ideal derecho.*

Demostración.

(1) Mostraremos que M es un producto tensorial de R con M. Definimos la aplicación $t' : R \times M \to M$ por $t'(r, m) := rm$, de la cual se verifica fácilmente que es R-balanceada y que $Im(t')$ genera a M. Supongamos que H es un grupo abeliano y que $\varphi : R \times M \to H$ es una aplicación R-balanceada. Notemos que $\varphi(r, m) = \varphi(1r, m) = \varphi(1, rm)$; entonces definimos el morfismo de grupos $\theta : M \to H$ por $\theta(m) = \varphi(1, m)$. Así θ es el único morfismo de grupos que hace que el diagrama

$$\begin{tikzcd}
 & M \arrow[d, "\theta"] \\
R \times M \arrow[ur, "t'"] \arrow[r, "\varphi"'] & H
\end{tikzcd}$$

conmute, es decir, para cada $r \in R$ y $m \in M$, $(\theta \circ t')(r, m) = \theta(t'(r, m)) = \theta(rm) = \varphi(1, rm) = \varphi(r, m)$. Entonces $M \cong R \otimes_R M$ por 1.8.2.

(2) Sabemos que los triángulos en el diagrama conmutan, esto es, $u \circ t_1 = t_1'$ y $v \circ t_2 = t_2'$. Entonces, $(f \circ u)(r \otimes m) = f(u(r \otimes m)) = f(u(t_1(r, m))) = f((u \circ t_1)(r, m)) = f(t_1'(r, m)) = f(rm) = rf(m) = t_2'(r, f(m)) = (v \circ t_2)(r, f(m)) = v(t_2(r, f(m))) = v(r \otimes f(m)) = v((1_R \otimes f)(r \otimes m)) = (v \circ (1_R \otimes f))(r \otimes m)$, para cada $r \in R$ y cada $m \in M$. Por lo tanto, el cuadrado conmuta.

(3) Definimos $t' : (R/I) \times M \to M/IM$ por $t'(r + I, m) := rm + IM$. Fácilmente se verifica que t' está bien definida, que es R-balanceada y que $Im(t')$ genera a M/IM. Ahora supongamos que H es un grupo abeliano y que $\varphi : (R/I) \times M \to H$ es una aplicación R-balanceada. Sea la aplicación $t : R \times M \to M$ que a (r, m) le asocia rm. Notemos que $t' \circ (\pi \times 1_M) = \pi' \circ t$ y que $\varphi \circ (\pi \times 1_M)$ es R-balanceada. Además, del inciso 1 tenemos que

hay un único morfismo θ tal que $\theta \circ t = \varphi \circ (\pi \times 1_M)$. Así tenemos que el diagrama

$$\begin{tikzcd}
R \times M \arrow[r, "\pi \times 1_M"] \arrow[d, "t"'] & (R/I) \times M \arrow[d, "t'"] \arrow[ddr, "\varphi"] & \\
M \arrow[r, "\pi'"] \arrow[drr, dotted, "\theta"'] & M/IM & \\
 & & H
\end{tikzcd}$$

conmuta.

Afirmamos que $IM \subseteq \ker(\theta)$. En efecto, pues si $r \in I$ y $m \in M$, se sigue que $\theta(rm) = \theta(t(r,m)) = \varphi((\pi \times 1_M)(r,m)) = \varphi(r+I,m) = \varphi(0,m) = 0$. Luego la afirmación garantiza la existencia de un morfismo $\theta' : M/IM \to H$ tal que $\theta' \circ \pi' = \theta$. Entonces $\varphi \circ (\pi \times 1_M) = \theta \circ t = (\theta' \circ \pi') \circ t = \theta' \circ (\pi' \circ t) = \theta' \circ (t' \circ (\pi \times 1_M))$, y como $\pi \times 1_M$ es suprayectiva, se sigue que $\varphi = \theta' \circ t'$, esto es, el diagrama

$$\begin{tikzcd}
 & M/IM \arrow[d, "\theta'"] \\
(R/I) \times M \arrow[ur, "t'"] \arrow[r, "\varphi"'] & H
\end{tikzcd}$$

conmuta. Finalmente, θ' es único; ya que si $\theta'' : M/IM \to H$ es tal que $\theta'' \circ t' = \varphi$, entonces $\theta'' \circ \pi' \circ t = \theta'' \circ t' \circ (\pi \times 1_M) = \varphi \circ (\pi \times 1_M) = \theta \circ t = \theta' \circ \pi' \circ t$, y como $\pi' \circ t$ es suprayectiva se sigue que $\theta'' = \theta'$.

$\square$

Proposición 1.8.9 *Sea M un R-módulo derecho y $(N_i)_{i \in I}$ una familia de R-módulos izquierdos. Entonces $M \otimes_R (\bigoplus N_i) \cong \bigoplus (M \otimes_R N_i)$.*

Demostración. Probaremos que $M \otimes_R (\bigoplus N_i)$ es la suma directa de $(M \otimes_R N_i)_{i \in I}$. Sea $(\mu_i)_{i \in I}$ la familia de morfismos que especifican a $\bigoplus N_i$ como suma directa. Aplicando $M \otimes_R \_$ a los μ_j tenemos los morfismos de grupos $1_M \otimes \mu_j : M \otimes_R N_j \to M \otimes_R (\bigoplus N_i)$.

Debemos mostrar que para cada pareja $(G, (\nu_i)_{i \in I})$, donde G es un grupo abeliano y para cada $j \in I$, $\nu_j : M \otimes_R N_j \to G$ es un morfismo de grupos, hay un único θ tal que para cada $j \in I$, conmuta el diagrama

$$\begin{tikzcd}
G & M \otimes_R (\bigoplus N_i) \arrow[l, "\theta"'] \\
 & M \otimes_R N_j \arrow[ul, "\nu_j"] \arrow[u, "1_M \otimes \mu_j"']
\end{tikzcd}$$

Sean $t : M \times (\bigoplus N_i) \to M \otimes_R (\bigoplus N_i)$ y $t_i : M \times N_i \to M \otimes_R N_i$ las aplicaciones R-balanceadas que especifican a $M \otimes_R (\bigoplus N_i)$ y $M \otimes_R N_i$ como productos tensoriales. Entonces la aplicación $\nu_i \circ t_i : M \times N_i \to G$ es R-balanceada, por ser t_i R-balanceada. Después, consideramos la aplicación $\sum(\nu_i \circ t_i) : M \times (\bigoplus N_i) \to G$ definida por $(\sum(\nu_i \circ t_i))(m, (f_i)) := \sum(\nu_i \circ t_i)(m, f_i)$, la cual está bien definida porque los elementos de $\bigoplus N_i$ son funciones selectoras cuyas entradas son casi todas cero. Se verifica también fácilmente que $\sum(\nu_i \circ t_i)$ es R-balanceada. Entonces hay un morfismo único θ que hace que el diagrama

$$\begin{tikzcd}
 & M \otimes_R (\bigoplus N_i) \arrow[d, "\theta"] \\
M \times (\bigoplus N_i) \arrow[ur, "t"] \arrow[r, "\sum(\nu_i \circ t_i)"'] & G
\end{tikzcd}$$

conmute. Así tenemos el diagrama conmutativo

$$\begin{tikzcd}
M \times N_j \arrow[r, "t_j"] \arrow[d, "1_M \times \mu_j"'] & M \otimes_R N_j \arrow[d, "1_M \otimes \mu_j"] & \\
M \times (\bigoplus N_i) \arrow[r, "t"] \arrow[drr, "\sum(\nu_i \circ t_i)"'] & M \otimes_R (\bigoplus N_i) \arrow[dr, "\theta"] & \\
 & & G.
\end{tikzcd}$$

Entonces

$$\begin{aligned}
((\sum(\nu_i \circ t_i)) \circ (1_M \times \mu_j))(m, x) &= (\sum(\nu_i \circ t_i))(m, \mu_j(x)) \\
&= (\sum(\nu_i \circ t_i))(m, (f_i)) = \sum(\nu_i \circ t_i)(m, f_i) \\
&= \sum \nu_i(t_i(m, f_i)) = \nu_j(t_j(m, f_j)) = (\nu_j \circ t_j)(m, x)
\end{aligned}$$

esto es, $\theta \circ (1_M \otimes \mu_j) \circ t_j = (\sum(\nu_i \circ t_i)) \circ (1_M \times \mu_j) = \nu_j \circ t_j$.

Como $Im(t_j)$ genera a $M \otimes_R N_j$, se sigue que $\theta \circ (1_M \otimes \mu_j) = \nu_j$, es decir, el diagrama

$$\begin{tikzcd}
G & M \otimes_R (\bigoplus N_i) \arrow[l, dotted, "\theta"'] \\
 & M \otimes_R N_j \arrow[ul, "\nu_j"] \arrow[u, "1_M \otimes \mu_j"']
\end{tikzcd}$$

conmuta.

Sólo falta probar que θ es único con esta propiedad. Supongamos que θ' es tal que $\theta' \circ (1_M \otimes \mu_j) = \nu_j$, entonces $\theta' \circ (1_M \otimes \mu_j) \circ t_j = \theta' \circ t \circ (1_M \times \mu_j) = \nu_j \circ t_j = \theta \circ (1_M \otimes \mu_j) \circ t_j = \theta \circ t \circ (1_M \times \mu_j)$, esto es, $\theta' \circ t \circ (1_M \times \mu_j) = \theta \circ t \circ (1_M \times \mu_j)$. Así para cada $m \in M$ y para cada $j \in I$, $(\theta' \circ t)(m, \bullet)$ y $(\theta \circ t)(m, \bullet)$ coinciden en todo $Im(\mu_j) \subseteq \bigoplus N_i$. Como estas imágenes generan a $\bigoplus N_i$, $\theta' \circ t = \theta \circ t$. Sabemos además que $Im(t)$ genera a $M \otimes_R (\bigoplus N_i)$, luego $\theta' = \theta$. $\square$

Notemos que si M es un R-módulo derecho, podemos considerar a M como un $\mathbb{Z}$-módulo izquierdo. De aquí, si G es un grupo abeliano, podemos ver a $Hom_{\mathbb{Z}}(M, G)$ como un R-módulo izquierdo con el producto por escalar definido por $(rf)(m) := f(mr)$, para cada $r \in R$, $f \in Hom_{\mathbb{Z}}(M, G)$ y $m \in M$.

Proposición 1.8.10 *Suponga que M es un R-módulo derecho, N un R-módulo izquierdo y G un grupo abeliano. Entonces, como grupos abelianos,*

$$Hom_{\mathbb{Z}}(M \otimes_R N, G) \cong Hom_R(N, Hom_{\mathbb{Z}}(M, G)).$$

Demostración. Mostraremos que cada lado en esta relación es isomorfo a S, el grupo de las aplicaciones R-balanceadas de $M \times N$ en G.

Definimos la aplicación $\varphi : Hom_{\mathbb{Z}}(M \otimes_R N, G) \to S$ por $\varphi(f) := f \circ t$, donde t es la aplicación R-balanceada que especifica a $M \otimes_R N$ como producto tensorial. Notemos también que φ está bien definida -porque t es R-balanceada y f es un morfismo de grupos- y φ es un morfismo de grupos. Luego, la propiedad universal del producto tensorial garantiza que φ sea suprayectiva e inyectiva.

Resta probar que $S \cong Hom_R(N, Hom_{\mathbb{Z}}(M, G))$. Para esto, definimos la correspondencia como sigue:

$$\begin{array}{ccc} S & \longleftrightarrow & Hom_R(N, Hom_{\mathbb{Z}}(M, G)) \\ f & \longleftrightarrow & g \\ f(m,n) & = & g(n)(m) \end{array}$$

La linealidad de f en M hace que g tome valores en $Hom_{\mathbb{Z}}(M, G)$, esto es, para cada $n \in N$, $g(n) : M \to G$ es un morfismo de grupos. Mientras que la linealidad de f en N garantiza que g sea un morfismo de grupos. Aunado a esto, $f(mr, n) = f(m, rn)$ si y sólo si $(rg(n))(m) = g(n)(mr) = g(rn)(m)$. Entonces f es R-balanceada si y sólo si g es un morfismo de R-módulos. De esta forma tenemos el isomorfismo $S \cong Hom_R(N, Hom_{\mathbb{Z}}(M, G))$. $\square$

Proposición 1.8.11 *Si* $\mathcal{E} : N \xrightarrow{u} T \xrightarrow{v} U \longrightarrow 0$ *es una sucesión exacta de R-módulos izquierdos y M es un R-módulo derecho, entonces la sucesión*

$$M \otimes_R N \xrightarrow{1 \otimes u} M \otimes_R T \xrightarrow{1 \otimes v} M \otimes_R U \longrightarrow 0$$

es exacta.

Demostración. Sea G un grupo abeliano. Como $\mathcal{E}$ es exacta, se sigue de 1.3.6 que la sucesión

$$0 \longrightarrow Hom_R(U, Hom_{\mathbb{Z}}(M,G)) \longrightarrow Hom_R(T, Hom_{\mathbb{Z}}(M,G)) \longrightarrow Hom_R(N, Hom_{\mathbb{Z}}(M,G))$$

es exacta. Entonces por 1.8.10, la sucesión

$$0 \longrightarrow Hom_{\mathbb{Z}}(M \otimes_R U, G) \longrightarrow Hom_{\mathbb{Z}}(M \otimes_R T, G) \longrightarrow Hom_{\mathbb{Z}}(M \otimes_R N, G)$$

es exacta. Y nuevamente, por 1.3.6 tenemos que la sucesión

$$M \otimes_R N \xrightarrow{1 \otimes u} M \otimes_R T \xrightarrow{1 \otimes v} M \otimes_R U \longrightarrow 0$$

es exacta. □

Proposición 1.8.12 *Si M y N son módulos finitamente generados sobre un anillo local $(R, \mathfrak{m})$ y $M \otimes_R N = 0$, entonces $M = 0$ ó $N = 0$.*

Demostración. Si $M \neq 0$, el lema de Nakayama implica que $M/\mathfrak{m}M \neq 0$. Sabemos de 1.6.7, que $M/\mathfrak{m}M$ es un $R/\mathfrak{m}$-espacio vectorial finito dimensional. Entonces, al tomar la composición de alguna de las proyecciones de $M/\mathfrak{m}M \cong (R/\mathfrak{m})^n$ en $R/\mathfrak{m}$ y la proyección canónica de M en $M/\mathfrak{m}M$ obtenemos un epimorfismo $f : M \to R/\mathfrak{m}$. Entonces de la proposición anterior, $0 = M \otimes_R N \to (R/\mathfrak{m}) \otimes_R N$ es suprayectiva, lo cual implica que $0 = (R/\mathfrak{m}) \otimes_R N \cong N/(\mathfrak{m}N)$. Luego, por el lema de Nakayama, $N = 0$. □

1.9. Módulos proyectivos

Definición 1.9.1 *Un R-módulo P es **proyectivo** si dado el diagrama*

$$\begin{tikzcd} & P \arrow[dl, dotted, "h"'] \arrow[d, "\beta"] & \\ M \arrow[r, "f"'] & N \arrow[r] & 0 \end{tikzcd}$$

con fila exacta, existe un R-morfismo $h : P \to M$ que hace conmutar el diagrama.

Proposición 1.9.2 *Si P es un módulo libre, P es proyectivo.*

Demostración. Consideremos el diagrama

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

con fila exacta y P libre, entonces P tiene una base $X = \{x_\alpha\}$. Luego, para cada α, $f^{-1}(\beta(x_\alpha)) \neq \emptyset$. De este modo tenemos una familia $\{f^{-1}(\beta(x_\alpha))\}$ de conjuntos no vacíos, entonces por el axioma de elección hay una función $g : X \to M$ tal que para cada α, $g(x_\alpha) \in f^{-1}(\beta(x_\alpha))$. Teniendo en cuenta el diagrama

$$\begin{tikzcd} M & P \arrow[l, dotted, "h"'] \\ & X \arrow[ul, "g"] \arrow[u, "i"'] \end{tikzcd}$$

se sigue que hay un único morfismo $h : P \to M$ tal que $h \circ i = g$. Entonces para cada α, $(f \circ h)(x_\alpha) = f(h(x_\alpha)) = f(h(i(x_\alpha))) = f(g(x_\alpha)) = \beta(x_\alpha)$ (pues $g(x_\alpha) \in f^{-1}(\beta(x_\alpha)))$. Y como X es una base de P, $f \circ h = \beta$. $\square$

Observaciones.

1. El recíproco no necesariamente es cierto. Como ejemplo podemos tomar a $R = \mathbb{Z}_6$, que es un $\mathbb{Z}_6$-módulo libre, con base $\{1\}$. Además $\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$. Así, $\mathbb{Z}_2$ es un sumando directo de un libre, esto es, $\mathbb{Z}_2$ es $\mathbb{Z}_6$-proyectivo. Si $\mathbb{Z}_2$ es libre, $\mathbb{Z}_2 \cong \bigoplus_{i\in I} M_i$, donde $M_i \cong \mathbb{Z}_6$. En el mejor de los casos, podría pasar que $\mid I \mid < \infty$, entonces $\mathbb{Z}_2 \cong \bigoplus M_i = \prod M_i \cong \prod \mathbb{Z}_6$, que tiene $6^{|I|}$ elementos, lo cual es falso.

2. Bajo ciertas condiciones hay módulos proyectivos que son libres: todo módulo proyectivo sobre un anillo local es libre sobre este anillo (este resultado fue probado por Kaplansky en [13]).

Proposición 1.9.3 *Si P es un módulo proyectivo y $f : M \to P$ es un epimorfismo, entonces P es un sumando directo de M.*

Demostración. Consideremos el diagrama con fila exacta

$$\begin{tikzcd} & & & P \arrow[dl, dotted, "h"'] \arrow[d, "1_P"] & \\ 0 \arrow[r] & \ker(f) \arrow[r, "i"'] & M \arrow[r, "f"'] & P \arrow[r] & 0 \end{tikzcd}$$

Como P es proyectivo, existe un morfismo $h : P \to M$ tal que $f \circ h = 1_P$, esto es, f es una retracción. Entonces de 1.4.15, tenemos que P es un sumando directo de M. $\square$

Proposición 1.9.4 *Un módulo P es proyectivo si y sólo si P es un sumando directo de un libre.*

Demostración. ($\Rightarrow$) Supongamos que P es proyectivo. La prueba en 1.5.4, garantiza que hay un epimorfismo $f : F \to P$, con F libre. Luego, de la proposición anterior tenemos que P es un sumando directo de F.

($\Leftarrow$) Supongamos que hay un módulo libre F tal que para algún submódulo P' de F, $F = P \oplus P'$. Consideremos el diagrama con fila exacta

$$\begin{tikzcd} F \arrow[d, dotted, "h"'] \arrow[r, shift right, "j"'] & P \arrow[l, shift right, "i"'] \arrow[d, "\beta"] & \\ M \arrow[r, "f"'] & N \arrow[r] & 0, \end{tikzcd}$$

donde i es la inclusión y j la proyección en P. Como F es libre, F es proyectivo y por tanto hay un morfismo h tal que $f \circ h = \beta \circ j$. Si definimos el morfismo $\delta : P \to M$ por $\delta = h \circ i$, tenemos que $f \circ \delta = f \circ (h \circ i) = (f \circ h) \circ i = (\beta \circ j) \circ i = \beta \circ (j \circ i) = \beta \circ 1_P = \beta$. Por lo tanto, P es proyectivo. $\square$

1.10. Módulos inyectivos

Definición 1.10.1 *Un R-módulo E es* ***inyectivo*** *si dado el diagrama*

$$\begin{tikzcd} & E & \\ 0 \arrow[r] & M \arrow[u, "f"] \arrow[r, "\varphi"'] & N \arrow[ul, dotted, "g"'] \end{tikzcd}$$

con fila exacta, hay un morfismo $g : N \to E$ tal que $f = g \circ \varphi$.

Teorema 1.10.2 *Un R-módulo E es inyectivo si y sólo si para todo ideal I de R y para todo $f : I \to E$ morfismo de R-módulos, hay un morfismo $g : R \to E$ tal que $g\,|_I = f$.*

Demostración. Es claro que si E es inyectivo, entonces al considerar el diagrama

$$\begin{tikzcd} & E & \\ 0 \arrow[r] & I \arrow[u, "f"] \arrow[r, "i"'] & R \arrow[ul, dotted, "g"'] \end{tikzcd}$$

con fila exacta -donde I es un ideal de R e i es la inclusión- se tiene la propiedad requerida.

Ahora tomemos el diagrama con fila exacta

$$\begin{tikzcd} & E & \\ 0 \arrow[r] & M \arrow[u, "f"] \arrow[r, "\varphi"'] & N \end{tikzcd}$$

Podemos suponer que M es un submódulo de N y que φ es la inclusión. Usaremos el lema de Zorn. Para esto, se define

$$\mathcal{N} = \{(N', g') : \varphi(M) \subseteq N' \subseteq N,\ N' \text{ es un submódulo de } N \text{ y } g' : N' \to E \text{ es un morfismo tal que } g' \circ \varphi = f\},$$

el cual es no vacío, ya que $(\varphi(M), f \circ \varphi^{-1}) \in \mathcal{N}$. Si definimos en $\mathcal{N}$ un orden parcial "$\leq$" de la siguiente forma:

$$(N'', g'') \leq (N', g') \text{ si } N'' \subseteq N' \text{ y } g' \mid_{N''} = g''.$$

entonces toda cadena no vacía $\mathcal{N}'$ de $\mathcal{N}$ tiene a $(\bigcup_{(N',g')\in\mathcal{N}'} N', h)$ como cota superior, donde $h : \bigcup_{(N',g')\in\mathcal{N}'} N' \to E$ y $h(x) = g(x)$ si $x \in N'$ y $(N', g') \in \mathcal{N}'$. Por consiguiente, $\mathcal{N}$ tiene un elemento maximal (N_0, g_0). Basta probar que $N_0 = N$.

Supongamos que hay un $x \in N - N_0$ y sea $I = \{r \in R : rx \in N_0\}$ que es un ideal de R, entonces para el morfismo $\overline{f} : I \to E$ definido por $\overline{f}(r) = g_0(rx)$ para $r \in I$, existe un morfismo $\overline{g} : R \to E$ tal que para cada $r \in I$, $\overline{g}(r) = \overline{f}(r) = g_0(rx)$.

Sean $N'' = N_0 + Rx$ y $g'' : N'' \to E$ tal que $g''(b + rx) = g_0(b) + \overline{g}(r)$. $N'' \neq N_0$, pues $x \in N''$ y $x \neq N_0$. Además g'' está bien definida, ya que si $b+rx$, $b'+r'x \in N''$ y $b+rx = b'+r'x$, entonces $N_0 \ni b-b' = r'x-rx = (r'-r)x$. De aquí se sigue que $r' - r \in I$. Luego $g_0(b - b') = g_0(b) - g_0(b')$ y $g_0(b - b') = g_0((r' - r)x) = \overline{g}(r' - r) = \overline{g}(r') - \overline{g}(r)$. Entonces $g_0(b) + \overline{g}(r) = g_0(b') + \overline{g}(r')$, es decir, $g''(b + rx) = g''(b' + r'x)$. Además, g'' es un morfismo (pues g_0 y $\overline{g}$ son morfismos) tal que $g'' \mid_{N_0} = g_0$. Así, $(N'', g'') \in \mathcal{N}$ y $(N_0, g_0) \lneq (N'', g'')$, lo que contradice la maximalidad de (N_0, g_0). □

Definición 1.10.3 *Sean R un anillo con identidad y M un R-módulo. Si $r \in R$ y $m \in M$, diremos que m es* ***divisible*** *por r, si hay un $m' \in M$ tal que $m = rm'$; diremos que M es* ***divisible*** *si cada $m \in M$ es divisible por cualquier elemento de R que no sea divisor de cero.*

Ejemplos.

1. $\mathbb{Q}$ es divisible como $\mathbb{Z}$-módulo.

2. El $\mathbb{Z}$-módulo $\mathbb{Q}/\mathbb{Z}$ también es divisible. En efecto, ya que al tomar la proyección canónica $\pi : \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$, se sigue que para cualesquiera $\overline{x} \in \mathbb{Q}/\mathbb{Z}$ y $r \in \mathbb{Z}$ con $r \neq 0$, existen $p, q \in \mathbb{Q}$ tales que $\pi(p) = \overline{x}$ y $p = rq$. Así $\overline{x} = \pi(p) = \pi(rq) = r\pi(q)$.

Proposición 1.10.4 *Sea R un dominio de ideales principales. Un R-módulo E es divisible si y sólo si E es inyectivo.*

Demostración. Supongamos que E divisible y sean I un ideal de R y $f : I \to E$ un morfismo de $\mathbb{Z}$-módulos. Vamos a probar que hay un morfismo $g : R \to E$ que extiende a f.

Si $I = 0$ entonces f se puede extender por el morfismo cero.

Si $I \neq 0$, con $I = \langle r \rangle$, entonces como E es divisible se sigue que para algún $u \in E$, $f(r) = ru$. Definimos el morfismo $g : R \to E$ que a $s \in R$ le asocia su, entonces para cada $x \in I$, $g(x) = g(rs) = rsu = f(rs) = f(x)$. Por lo tanto, G es inyectivo.

Ahora supongamos que E es un R-módulo inyectivo y sean $r \in R - \{0\}$ y $u \in E$. Definimos un morfismo $f_u : R \to E$ por $f_u(s) = su$ y consideremos el monomorfismo $\varphi : R \to R$ que a $s \in R$ le asigna rs. Como M es inyectivo, existe un morfismo $g : R \to E$ tal que hace conmutar el diagrama

$$\begin{tikzcd} & E & \\ 0 \arrow[r] & R \arrow[u, "f_u"] \arrow[r, "\varphi"'] & R \arrow[ul, dotted, "g"'] \end{tikzcd} ,$$

o sea que para cada $s \in R$, $g(rs) = f_u(s) = su$. Así tenemos que $u = f_u(1) = g(r) = rg(1)$, es decir, M es divisible. $\square$

Proposición 1.10.5 *Si G es un grupo abeliano divisible, entonces $Hom_{\mathbb{Z}}(R, G)$ es un R-módulo inyectivo.*

Demostración. Supongamos que tenemos el diagrama de R-módulos

$$\begin{tikzcd} & Hom_{\mathbb{Z}}(R,G) & \\ 0 \arrow[r] & N \arrow[u, "h"] \arrow[r, "\varphi"'] & M \end{tikzcd}$$

con fila exacta.

Se define el morfismo de grupos $f : N \to G$ por $f(n) := h(n)(1)$. Como G es divisible, G es $\mathbb{Z}$-inyectivo y por tanto hay un morfismo de grupos f' que hace conmutar el diagrama

$$\begin{tikzcd} & G & \\ 0 \arrow[r] & N \arrow[u, "f"] \arrow[r, "\varphi"'] & M \arrow[ul, dotted, "f'"'] \end{tikzcd} .$$

Se define una aplicación $h' : M \to Hom_{\mathbb{Z}}(R, G)$ por $h'(m)(r) := f'(rm)$, de la cual es fácil verificar que está bien definida y que cumple las propiedades para ser un morfismo de R-módulos (teniendo en cuenta que si $\phi \in Hom_{\mathbb{Z}}(R, G)$ y $r, r' \in R$, entonces $(r\phi)(r') := \phi(r'r)$).

Sea $n \in N$, entonces $h'(n)(r) = f'(rn) = f(rn) = h(nr)(1) = (rh(n))(1) = h(n)(1r) = h(n)(r)$. $\square$

Proposición 1.10.6 *Si G es un grupo abeliano, entonces hay un grupo abeliano divisible D y un monomorfismo $g : G \to D$.*

Demostración. Supongamos que G es cíclico no nulo, entonces $G \cong \mathbb{Z}$ o $G \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ (observación 2 en 1.6.1). En el caso $G \cong \mathbb{Z}$ tomamos el morfismo inclusión de $\mathbb{Z}$ en $\mathbb{Q}$. Para el caso $G \cong \mathbb{Z}_n$ consideramos el monomorfismo $\phi : \mathbb{Z}_n \to \mathbb{Q}/\mathbb{Z}$ que a $\overline{1}$ le asocia $\overline{1/n}$.

Si G es un abeliano cualquiera y $x \in G$ con $x \neq 0$, entonces $\langle x \rangle$ es cíclico y por lo anterior se garantiza la existencia de un monomorfismo $f_x : \langle x \rangle \to D_x$, donde D_x es abeliano divisible. Luego D_x es inyectivo. Así, para cada $x \in G$ hay un morfismo $g_x : G \to D_x$ tal que el diagrama

$$\begin{tikzcd}
 & D_x & \\
0 \arrow[r] & \langle x \rangle \arrow[u, "f_x"] \arrow[r] & G \arrow[ul, dotted, "g_x"']
\end{tikzcd}$$

conmuta.

Consideremos el morfismo $g : G \to \prod_{x \in G-\{0\}} D_x$ que a $y \in G$ le asocia $\{g_x(y)\}_{x \in G-\{0\}}$. Como los D_x son $\mathbb{Z}$-inyectivos, entonces $\prod_{x \in G-\{0\}} D_x$ es $\mathbb{Z}$-inyectivo.

Afirmamos que $\ker(g) = 0$. Supongamos que existe un elemento $x_0 \neq 0$ en $\ker(g) = \bigcap_{x \in G-\{0\}} \ker(g_x) \subseteq \ker(g_{x_0})$, entonces $x_0 \in \ker(g_{x_0})$. Esto implica que $f_{x_0}(\langle x_0 \rangle) = g_{x_0}(\langle x_0 \rangle) = 0$ y por tanto $0 = \ker(f_{x_0}) = \langle x_0 \rangle$, lo cual es una contradicción. $\square$

Proposición 1.10.7 *Para todo R-módulo M, existe un módulo inyectivo E y un monomorfismo de $g : M \to E$.*

Demostración. Como M es abeliano, hay un grupo abeliano divisible E y un monomorfismo de grupos $g : M \to E$. Entonces $Hom_{\mathbb{Z}}(R, g) : Hom_{\mathbb{Z}}(R, M) \to Hom_{\mathbb{Z}}(R, E)$ es un monomorfismo de R-módulos.

Por otra parte, sabemos que $M \cong Hom_R(R, M)$. Se define una aplicación $f : Hom_R(R, M) \to Hom_{\mathbb{Z}}(R, M)$ por $f(h) := h$, la cual es un monomorfismo de R-módulos. De esta forma se tiene la siguiente cadena de monomorfismos

$$M \cong Hom_R(R, M) \to Hom_{\mathbb{Z}}(R, M) \to Hom_{\mathbb{Z}}(R, E),$$

donde $Hom_{\mathbb{Z}}(R, E)$ es un R-módulo inyectivo. $\square$

Capítulo 2

Categorías

2.1. Categorías y funtores

Definición 2.1.1 *Una* ***categoría*** *es un quíntuple* $\mathcal{C} = (\mathcal{O}, \mathcal{M}, dom, cod, \circ)$, *donde:*

(1) $\mathcal{O}$ *es una clase cuyos elementos son llamados* $\mathcal{C}$-***objetos****.*

(2) $\mathcal{M}$ *es una clase cuyos elementos son llamados* $\mathcal{C}$-***morfismos****.*

(3) *dom y cod son funciones de* $\mathcal{M}$ *a* $\mathcal{O}$ *y para* $f \in \mathcal{M}$, $dom(f)$ *es llamado el* ***dominio*** *de* f *y* $cod(f)$ *es llamado el* ***codominio*** *de* f.

(4) $\circ$ *es una función de* $D = \{(f,g) : f, g \in \mathcal{M} \text{ y } dom(f) = cod(g)\}$ *en* $\mathcal{M}$, *con* $f \circ g$ *usualmente se denota a* $\circ(f,g)$ *y se dice que* $f \circ g$ *está definida si y sólo si* $(f,g) \in D$. *La función* $\circ$ *se llama* ***ley de composición*** *de* $\mathcal{C}$ *y satisface las siguientes condiciones:*

   (i) *Si* $f \circ g$ *está definida, entonces* $dom(f \circ g) = dom(g)$ *y* $cod(f \circ g) = cod(f)$.

   (ii) *Si* $f \circ g$ *y* $h \circ f$ *están definidas, entonces* $h \circ (f \circ g) = (h \circ f) \circ g$.

   (iii) *Para cada* $\mathcal{C}$-*objeto* A *existe un* $\mathcal{C}$-*morfismo* e *tal que* $dom(e) = A = cod(e)$ *y*

      (a) $f \circ e = f$ *siempre que* $f \circ e$ *esté definido.*

      (b) $e \circ g = g$ *siempre que* $e \circ g$ *esté definido.*

   (iv) *Para cada pareja* (A, B) *de* $\mathcal{C}$-*objetos, la clase*

$$hom_{\mathcal{C}}(A,B) = \{f : f \in \mathcal{M},\ dom(f) = A \text{ y } cod(f) = B\}$$

   es un conjunto.

Observaciones.

1. $\mathcal{M} = \bigcup_{A,B\in\mathcal{O}} hom_{\mathcal{C}}(A,B)$ (unión ajena).
2. El $\mathcal{C} - morfismo\ e$ es único y se denota por 1_A.

Para una categoría dada $\mathcal{C}$, la clase de $\mathcal{C}$-objetos se denotará por $Ob(\mathcal{C})$, mientras que $Mor(\mathcal{C})$ denotará a la clase de $\mathcal{C}$-morfismos.

Ejemplos.

1. La categoría $\mathcal{C} = Set$ cuya clase de objetos es la clase $\mathcal{U}$ de todos los conjuntos, los conjuntos de morfismos $hom_{\mathcal{C}}(A,B)$ son los conjuntos de todas las funciones de A en B y cuya ley de composición es la composición usual de funciones.

2. Sea R un anillo con elemento unitario. Con R-Mod denotamos la categoría cuya clase de objetos es la clase de todos los R-módulos izquierdos, los conjuntos de morfismos $hom_{R\text{-}Mod}(M,N)$ son los conjuntos de todos los R-homomorfismos de M en N y donde la composición es la usual.

3. La categoría Ab cuya clase de objetos es la clase de todos los grupos abelianos, los conjuntos de morfismos $hom_{Ab}(G,H)$ son los conjuntos de morfismos de grupos de G en H y la ley de composición es la usual.

4. Dada una categoría $\mathcal{C}$, podemos formar la **categoría opuesta** $\mathcal{C}^{op}$, donde $Ob(\mathcal{C}^{op}) = Ob(\mathcal{C})$, $hom_{\mathcal{C}^{op}}(A,B) = hom_{\mathcal{C}}(B,A)$ y la composición está definida por $f \circ_{\mathcal{C}^{op}} g = g \circ_{\mathcal{C}} f$.

Definición 2.1.2 *Sean $\mathcal{C}$ y $\mathcal{D}$ categorías. Diremos que $F : \mathcal{C} \to \mathcal{D}$ es un* ***funtor*** *o* ***funtor covariante*** *si satisface lo siguiente:*

(1) *A cada $A \in Ob(\mathcal{C})$ le asocia un único elemento $F(A) \in Ob(\mathcal{D})$.*

(2) *A cada $\mathcal{C}$-morfismo $A \xrightarrow{f} B$ le asocia un único $\mathcal{D}$-morfismo $F(A) \xrightarrow{F(f)} F(B)$.*

(3) *F* ***preserva la composición****: si $A \xrightarrow{f} B$ y $B \xrightarrow{g} C$ son $\mathcal{C}$-morfismos, entonces $F(g \circ f) = F(g) \circ F(f)$.*

(4) *F* ***preserva identidades****: para cada $A \in Ob(\mathcal{C})$, $F(1_A) = 1_{F(A)}$.*

Definición 2.1.3 *Sean $\mathcal{C}$ y $\mathcal{D}$ dos categorías. $F : \mathcal{C} \to \mathcal{D}$ es un* ***funtor contravariante*** *de $\mathcal{C}$ en $\mathcal{D}$ si satisface:*

(1) *A cada $A \in Ob(\mathcal{C})$ le asocia un único elemento $F(A) \in Ob(\mathcal{D})$.*

(2) *A cada $\mathcal{C}$-morfismo $A \xrightarrow{f} B$ le asocia un único $\mathcal{D}$-morfismo $F(B) \xrightarrow{F(f)} F(A)$.*

(3) *F* ***invierte la composición****: si $A \xrightarrow{f} B$ y $B \xrightarrow{g} C$ son $\mathcal{C}$-morfismos, entonces $F(g \circ f) = F(f) \circ F(g)$.*

(4) *F **preserva identidades**: para cada $A \in Ob(\mathcal{C})$, $F(1_A) = 1_{F(A)}$.*

Observación. Para definir un funtor covariante (contravariante) de $\mathcal{C}$ en $\mathcal{D}$ basta con definirlo en $\mathcal{C}$-objetos, en $\mathcal{C}$-morfismos y demostrar que preserva (invierte) la $\mathcal{C}$-composición y que preserva las $\mathcal{C}$-identidades.

Ejemplos:.

1. Sean R un anillo conmutativo con elemento unitario y M un R-módulo. Definimos $Hom(M, \_) : R\text{-}Mod \to R\text{-}Mod$ como sigue:

   Para cada R-módulo N, $Hom(M, \_)(N) := Hom_R(M, N) \in Ob(R\text{-}Mod)$ y si $N \xrightarrow{f} T$ es un R-morfismo, entonces

$$\begin{array}{rccc} Hom(M,\_)(f): & Hom_R(M,N) & \longrightarrow & Hom_R(M,T) \\ & g & \longmapsto & f \circ g. \end{array}$$

   De acuerdo con los resultados ya vistos referentes al módulo $Hom_R(M, N)$, tenemos que $Hom(M, \_)$ preserva la composición y las identidades. Por lo tanto, $Hom(M, \_)$ es un funtor covariante.

2. Dando definiciones análogas para $Hom(\_, M)$, se tiene que $Hom(\_, M)$ es un funtor contravariante.

3. Sean R un anillo conmutativo y M un R-módulo derecho. Definimos el funtor $M \otimes_R \_ : R\text{-}Mod \to R\text{-}Mod$ de la siguiente manera:

   Para cada $N \in Ob(R\text{-}Mod)$, $(M \otimes_R \_)(N) := M \otimes_R N$ y si $N \xrightarrow{f} T$ es un R-morfismo, entonces

$$\begin{array}{rccc} (M \otimes_R \_)(f) := 1_M \otimes f: & (M \otimes_R N) & \longrightarrow & (M \otimes_R T) \\ & m \otimes n & \longmapsto & m \otimes f(n). \end{array}$$

   Es fácil ver que $M \otimes_R \_$ preserva la composición y las identidades.

4. De forma similar tenemos que $\_ \otimes_R M$ es un funtor covariante de $Mod\text{-}R$ en $R\text{-}Mod$.

Definición 2.1.4 *Sean $F : R\text{-}Mod \to R\text{-}Mod$ un funtor covariante y*

$$0 \longrightarrow M \longrightarrow N \longrightarrow T \longrightarrow 0$$

una sucesión exacta en $R\text{-}Mod$.

(1) *Si $0 \longrightarrow F(M) \longrightarrow F(N) \longrightarrow F(T) \longrightarrow 0$ es exacta, entonces F es **exacto**.*

(2) *Si $0 \longrightarrow F(M) \longrightarrow F(N) \longrightarrow F(T)$ es exacta, entonces F es **exacto izquierdo**.*

(3) *Si* $F(M) \longrightarrow F(N) \longrightarrow F(T) \longrightarrow 0$ *es exacta, entonces* F *es* ***exacto derecho****.*

Definición 2.1.5 *Sean* $F : R\text{-}Mod \to R\text{-}Mod$ *un funtor contravariante y*

$$0 \longrightarrow M \longrightarrow N \longrightarrow T \longrightarrow 0$$

una sucesión exacta en $R\text{-}Mod$*.*

(1) *Si* $0 \longrightarrow F(T) \longrightarrow F(N) \longrightarrow F(M) \longrightarrow 0$ *es exacta, entonces* F *es* ***exacto****.*

(2) *Si* $0 \longrightarrow F(T) \longrightarrow F(N) \longrightarrow F(M)$ *es exacta, entonces* F *es* ***exacto izquierdo****.*

(3) *Si* $F(T) \longrightarrow F(N) \longrightarrow F(M) \longrightarrow 0$ *es exacta, entonces* F *es* ***exacto derecho****.*

Ejemplos.

1. De acuerdo con lo hecho en 1.3.5 y 1.3.6 tenemos que el funtor covariante $Hom(M, \_)$ es exacto izquierdo y el funtor contravariante $Hom(\_, M)$ también es exacto izquierdo.

2. Por lo hecho en 1.8.11 tenemos que el funtor covariante $M \otimes_R \_$ es exacto derecho. Así también lo es el funtor $\_ \otimes_R N$.

Proposición 2.1.6 *Un módulo* P *es proyectivo si y sólo si el funtor* $Hom(P, \_)$ *preserva epimorfismos.*

Demostración. ($\Rightarrow$) Supongamos que $f : M \to N$ es un epimorfismo. Debemos mostrar que $Hom_R(P, f) : Hom_R(P, M) \to Hom_R(P, N)$ es un epimorfismo.

Sea $g \in Hom_R(P, N)$. Como P es proyectivo, existe un morfismo $h : P \to M$ tal que $Hom_R(P, f)(h) = f \circ h = g$.

($\Leftarrow$) Supongamos que tenemos el diagrama con fila exacta

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

Como f es un epimorfismo, $Hom_R(P, f) : Hom_R(P, M) \to Hom_R(P, N)$ es un epimorfismo. Así, para el morfismo g, existe $h \in Hom_R(P, M)$ tal que $Hom_R(P, f)(h) = f \circ h = g$. □

Proposición 2.1.7 *Dada una familia de* R*-módulos* $(M_i)_{i \in I}$*,* $\bigoplus M_i$ *es proyectivo si y sólo si* M_i *es proyectivo.*

Demostración. Sea $0 \longrightarrow M \longrightarrow N \longrightarrow T \longrightarrow 0$ una sucesión exacta. Aplicando el funtor $Hom_R(\bigoplus M_i, \_)$ obtenemos el diagrama

$$\begin{array}{ccccccccc}
0 & \longrightarrow & Hom_R(\bigoplus M_i, M) & \longrightarrow & Hom_R(\bigoplus M_i, N) & \longrightarrow & Hom_R(\bigoplus M_i, T) & \longrightarrow & 0 \\
 & & \Big\| \wr & & \Big\| \wr & & \Big\| \wr & & \\
0 & \longrightarrow & \prod Hom_R(M_i, M) & \longrightarrow & \prod Hom_R(M_i, N) & \longrightarrow & \prod Hom_R(M_i, T) & \longrightarrow & 0
\end{array}$$

La fila superior es exacta si y sólo si la fila inferior es exacta, y esto ocurre si y sólo si para cada i,

$$0 \longrightarrow Hom_R(M_i, M) \longrightarrow Hom_R(M_i, N) \longrightarrow Hom_R(M_i, T) \longrightarrow 0$$

es exacta. □

Proposición 2.1.8 *Un módulo E es inyectivo si y sólo si el funtor $Hom_R(\_, E)$ manda monomorfismos en epimorfismos.*

Demostración. Es análoga a la prueba de 2.1.6. □

Proposición 2.1.9 *Sea $(E_i)_{i\in I}$ una familia de módulos. Entonces $\prod E_i$ es inyectivo si y sólo si cada E_i es inyectivo.*

Demostración. Es análoga a la prueba de 2.1.7. □

Definición 2.1.10 *Un R-módulo derecho M es **plano** si el funtor $M \otimes_R \_$ es exacto. De modo similar se define un R-módulo izquierdo plano.*

Proposición 2.1.11 *Si R es un anillo con elemento unitario, R es un módulo plano.*

Demostración. Sea $f : N \to T$ un monomorfismo, entonces del inciso 2 en 1.8.8 tenemos que el diagrama

$$\begin{array}{ccc}
R \otimes_R N & \xrightarrow{1_R \otimes f} & R \otimes_R T \\
{\scriptstyle u}\downarrow & & \downarrow{\scriptstyle v} \\
N & \xrightarrow[f]{} & T
\end{array}$$

conmuta. Debemos mostrar que $1_R \otimes f$ es un monomorfismo.

Sea $x \in R \otimes_R N$ tal que $(1_R \otimes f)(x) = 0$. Luego, $0 = v((1_R \otimes f)(x)) = (v \circ (1_R \otimes f))(x) = (f \circ u)(x)$. Como u y f son monomorfismos, $x = 0$. □

Proposición 2.1.12 *Sea $(M_i)_{i\in I}$ una familia de R-módulos derechos. Entonces $\bigoplus M_i$ es plano si y sólo si M_i es plano.*

Demostración. Sea $0 \longrightarrow N \longrightarrow T \longrightarrow U \longrightarrow 0$ una sucesión exacta. Luego, aplicando el funtor $\bigoplus M_i \otimes_R \_$ obtenemos el diagrama

$$\begin{tikzcd}
0 \arrow[r] & (\bigoplus M_i) \otimes_R N \arrow[r] \arrow[d, equal, "\sim"] & (\bigoplus M_i) \otimes_R T \arrow[r] \arrow[d, equal, "\sim"] & (\bigoplus M_i) \otimes_R U \arrow[r] \arrow[d, equal, "\sim"] & 0 \\
0 \arrow[r] & \bigoplus (M_i \otimes_R N) \arrow[r] & \bigoplus (M_i \otimes_R T) \arrow[r] & \bigoplus (M_i \otimes_R U) \arrow[r] & 0
\end{tikzcd}$$

La fila superior es exacta si y sólo si la fila inferior es exacta, esto ocurre si y sólo si para cada i,

$$0 \longrightarrow M_i \otimes_R N \longrightarrow M_i \otimes_R T \longrightarrow M_i \otimes_R U \longrightarrow 0$$

es exacta. $\square$

Corolario 2.1.13 *Cualquier R-módulo derecho libre es plano.*

Demostración. Sea F es un R-módulo derecho libre. Entonces F es suma directa de copias de R. Por 2.1.11 R es plano. Luego, de 2.1.12 se sigue que F es plano. $\square$

Definición 2.1.14 *Sean $F : \mathcal{A} \to \mathcal{B}$ y $G : \mathcal{A} \to \mathcal{B}$ funtores.*

(1) *Una **transformación natural** de F a G es una terna (F, η, G) donde $\eta : Ob(\mathcal{A}) \to Mor(\mathcal{B})$ es una función que satisface las siguientes propiedades:*

  (i) *Para cada $\mathcal{A}$-objeto A, $\eta(A)$ es un $\mathcal{B}$-morfismo $\eta_A : F(A) \to G(A)$ ($\eta(A) = \eta_A$).*

  (ii) *Para cada $\mathcal{A}$-morfismo $A \xrightarrow{f} A'$, el diagrama*

$$\begin{tikzcd}
F(A) \arrow[r, "\eta_A"] \arrow[d, "F(f)"'] & G(A) \arrow[d, "G(f)"] \\
F(A') \arrow[r, "\eta_{A'}"'] & G(A')
\end{tikzcd}$$

  conmuta.

(2) *Una transformación natural (F, η, G) es llamada un **isomorfismo natural** siempre que para cada $\mathcal{A}$-objeto A, η_A es un $\mathcal{B}$-isomorfismo, esto es, η_A tiene inverso izquierdo e inverso derecho en $\mathcal{B}$.*

(3) *F y G se dice que son **naturalmente isomorfos** y se denota por $F \cong G$, si hay un isomorfismo natural de F a G.*

Definición 2.1.15 (1) *Una* ***estructura aditiva*** (*resp.* ***estructura semiaditiva***) *en una categoría* $\mathcal{C}$ *es una función* $+$ *que asocia a cada par* (f, g) *de* $\mathcal{C}$*-morfismos con dominio común* A *y codominio común* B*, un* $\mathcal{C}$*-morfismo* $f + g$ *con dominio* A *y codominio* B *tal que las condiciones* (*A*1), (*A*2) *y* (*A*3) (*resp.* (*A*1′), (*A*2) *y* (*A*3)) *se cumplen:*

(A1) *Para cada par* (A, B) *de* $\mathcal{C}$*-objetos,* $+$ *induce en* $hom_{\mathcal{C}}(A, B)$ *la estructura de un grupo abeliano.*

(A1') *Para cada par* (A, B) *de* $\mathcal{C}$*-objetos,* $+$ *induce en* $hom_{\mathcal{C}}(A, B)$ *la estructura de un monoide conmutativo.*

(A2) *Si* $A \xrightarrow{k} B \overset{g}{\underset{h}{\rightrightarrows}} C \xrightarrow{f} D$ *son* $\mathcal{C}$*-morfismos, entonces*

$$f \circ (g + h) = (f \circ g) + (f \circ h) \text{ y } (g + h) \circ k = (g \circ k) + (h \circ k).$$

(A3) *Para cada* $\mathcal{C}$*-morfismo* f, $0 + f = f + 0 = f$.

(2) *Si* $+$ *es una estructura aditiva* (*resp. estructura semiaditiva*) *en una categoría* $\mathcal{C}$*, llamamos a* $\mathcal{C}$ *o* $(\mathcal{C}, +)$ *una* ***categoría aditiva*** (*resp.* ***categoría semiaditiva***).

Ejemplo. R-Mod es aditiva (para todo anillo R) y Grp no es aditiva.

Definición 2.1.16 *Si* $\mathcal{C}$ *y* $\mathcal{D}$ *son categorías semiaditivas, entonces* $F : \mathcal{C} \to \mathcal{D}$ *es un* ***funtor aditivo*** *si para cada pareja* (A, B) *de* $\mathcal{C}$*-objetos,* F *induce un homomorfismo de monoides de* $hom_{\mathcal{C}}(A, B)$ *en* $hom_{\mathcal{D}}(F(A), F(B))$.

Proposición 2.1.17 *Si* $F : R$-$Mod \to S$-Mod *es un funtor covariante aditivo, entonces* F *preserva sucesiones exactas cortas que se dividen.*

Demostración. Supongamos que F es un funtor covariante aditivo y sea

$$\mathcal{E} : \; 0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$$

una sucesión exacta corta que se divide. Aplicando F a $\mathcal{E}$ obtenemos la sucesión

$$F(\mathcal{E}) : \; 0 \longrightarrow F(M) \xrightarrow{F(f)} F(N) \xrightarrow{F(g)} F(T) \longrightarrow 0.$$

Como $\mathcal{E}$ se divide, existen morfismos $N \xrightarrow{h} M$ y $T \xrightarrow{k} N$ tales que $h \circ f = 1_M$ y $g \circ k = 1_T$. Además, en la prueba de la implicación (2) $\Rightarrow$ (3) en 1.4.15 vimos que $N = f(M) \oplus k(T)$. Sabemos también que F es covariante, así que $F(h) \circ F(f) = F(h \circ f) = F(1_M) = 1_{F(M)}$ y $F(g) \circ F(k) = F(g \circ k) = F(1_T) = 1_{F(T)}$ con $F(N) \overset{F(h)}{\to} F(M)$ y $F(T) \overset{F(k)}{\to} F(N)$. Nuevamente, de la prueba de la implicación (2) $\Rightarrow$ (3) en 1.4.15 tenemos que $F(N) = \ker(F(h)) \oplus F(f)(F(M))$, pues $F(h)$ es una retracción.

Se afirma que $1_N = (f \circ h) + (k \circ g)$. En efecto, ya que al tomar un $n \in N$, $n = f(m) + k(t)$ para algún $m \in M$ y algún $t \in T$, entonces $\big((f \circ h) + (k \circ g)\big)(n) = \big((f \circ h) + (k \circ g)\big)(f(m) + k(t)) = (f \circ h)\big(f(m) + k(t)\big) + (k \circ g)\big(f(m) + k(t)\big) =$

$f\big(h(f(m)+k(t))\big)+k\big(g(f(m)+k(t))\big)=f\big(h(f(m))+h(k(t))\big)+k\big(g(f(m))+g(k(t))\big)=f(m+0)+k(0+t)=f(m)+k(t)=n$, donde la igualdad $f\big(h(f(m))+h(k(t))\big)=f(m+0)$ se sigue de que al ser h una retracción, $N=\ker(h)\oplus f(M)$ (de acuerdo a lo hecho en la prueba de la implicación (2) $\Rightarrow$ (3) en 1.4.15). De esta forma obtenemos que $1_N=(f\circ h)+(k\circ g)$.

Se afirma también que $\ker(F(h))=F(k)(F(T))$. En efecto, pues si $x\in\ker(F(h))$, entonces $x=1_{F(N)}(x)=F(1_N)(x)=F\big((f\circ h)+(k\circ g)\big)(x)=\big(F(f\circ h)+F(k\circ g)\big)(x)=\big((F(f)\circ F(h))+(F(k)\circ F(g))\big)(x)=\big(F(f)\circ F(h)\big)(x)+\big(F(k)\circ F(g)\big)(x)=F(f)(F(h)(x))+F(k)(F(g)(x))=F(f)(0)+F(k)(F(g)(x))=F(f)(0)+F(k)(F(g)(x))\in F(k)(F(T))$. Recíprocamente, $F(k)(F(T))\subseteq\ker(F(h))$, ya que $F(h)\circ F(k)=F(h\circ k)=F(0)=0$.

Por todo esto tenemos que $F(N)=\ker(F(h))\oplus F(f)(F(M))=F(k)(f(T))\oplus F(f)(F(M))$ y podemos reescribir la sucesión $F(\mathcal{E})$ como sigue:

$$F(\mathcal{E}):\ 0\longrightarrow F(M)\longrightarrow F(k)(f(T))\oplus F(f)(F(M))\longrightarrow F(T)\longrightarrow 0.$$

Pero sabemos que $F(f)$ es un monomorfismo, $F(g)$ es un epimorfismo, $F(g)\circ F(f)=0$ y $F(k):F(T)\to F(N)$ es un morfismo tal que $F(g)\circ F(k)=1_{F(T)}$, así que por 1.4.16, la sucesión $F(\mathcal{E})$ es exacta corta y se divide. $\square$

Capítulo 3

Homología

3.1. Grupos de homología

En esta sección examinaremos algunas propiedades importantes de los grupos de homología de un complejo, las cuales proporcionan información sobre el grado en que el complejo se "desvía" de la exactitud.

Definición 3.1.1 *Un **complejo** o **complejo cadena** $(\mathcal{M}, d)$, es una sucesión de morfismos de R-módulos*

$$\mathcal{M}: \quad \cdots \longrightarrow M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \longrightarrow \cdots$$

tal que para cada $i \in \mathbb{Z}$, $d_i \circ d_{i+1} = 0$, esto es, $Im(d_{i+1}) \subseteq \ker(d_i)$.

Ejemplos.

1. Un R-módulo M puede ser visto como el complejo

$$\cdots \longrightarrow 0 \longrightarrow M \longrightarrow 0 \longrightarrow \cdots.$$

2. Sea R un anillo conmutativo y $x \in R$. La sucesión

$$0 \longrightarrow R \xrightarrow{x} R \longrightarrow 0,$$

donde el endomorfismo en R es multiplicación por x, es un complejo de R-módulos.

3. Supongamos que $\mathcal{M}: \quad \cdots \longrightarrow M_i \xrightarrow{d_i} M_{i-1} \longrightarrow \cdots$ es un complejo.

   a) Si $F: R\text{-}Mod \to S\text{-}Mod$ es un funtor covariante aditivo, entonces $F(\mathcal{M})$ es un complejo, ya que $F(d_i) \circ F(d_{i+1}) = F(d_i \circ d_{i+1}) = F(0) = 0$.

b) Si $F : R\text{-}Mod \to S\text{-}Mod$ es un funtor contravariante aditivo, entonces $F(\mathcal{M})$ es un complejo (la justificación es análoga a la dada en el inciso anterior, teniendo en mente que al aplicar el funtor a $\mathcal{M}$ las flechas se invierten y entonces hay que reetiquetar los subíndices).

Definición 3.1.2 *El **i-ésimo grupo de homología** de un complejo $\mathcal{M}$ es el grupo cociente,* $\ker(d_i)/Im(d_{i+1})$ *al cual denotaremos por $H_i(\mathcal{M})$.*

Observación. $\ker(d_i)/Im(d_{i+1})$ es un grupo abeliano, porque $\ker(d_i)$ es un grupo abeliano e $Im(d_{i+1})$ es un subgrupo de $\ker(d_i)$.

Ejemplo. En el complejo $0 \longrightarrow R \xrightarrow{x} R \longrightarrow 0$ tenemos que

$$H_0(\mathcal{M}) = \ker(d_0)/Im(d_1) = R/\langle x\rangle \quad y \quad H_1(\mathcal{M}) = \ker(d_1)/Im(d_2) = \ker(d_1).$$

Definición 3.1.3 *Sean $(\mathcal{M}, d)$ y $(\mathcal{N}, d')$ dos complejos. Una **aplicación de cadenas** $f : \mathcal{M} \to \mathcal{N}$ es una familia de morfismos $f = (f_i)_{i\in\mathbb{Z}}$ con $f_i : M_i \to N_i$ tales que hacen conmutar el diagrama siguiente:*

$$\begin{tikzcd}
\mathcal{M}: & \cdots \arrow[r] & M_{i+1} \arrow[r, "d_{i+1}"] \arrow[d, "f_{i+1}"'] & M_i \arrow[r, "d_i"] \arrow[d, "f_i"'] & M_{i-1} \arrow[r] \arrow[d, "f_{i-1}"'] & \cdots \\
\mathcal{N}: & \cdots \arrow[r] & N_{i+1} \arrow[r, "d'_{i+1}"'] & N_i \arrow[r, "d'_i"'] & N_{i-1} \arrow[r] & \cdots .
\end{tikzcd}$$

Al considerar dos aplicaciones de cadenas $f : \mathcal{M} \to \mathcal{N}$ y $g : \mathcal{M} \to \mathcal{N}$, tenemos que para cada i, $d'_i \circ f_i = f_{i-1} \circ d_i$ y $d'_i \circ g_i = g_{i-1} \circ d_i$. Por tanto $d'_i \circ (f_i + g_i) = (d'_i \circ f_i) + (d'_i \circ g_i) = (f_{i-1} \circ d_i) + (g_{i-1} \circ d_i) = (f_{i-1} \circ g_{i-1}) + d_i$, o sea que el diagrama

$$\begin{tikzcd}
\mathcal{M}: \cdots \arrow[r] & M_i \arrow[r, "d_i"] \arrow[d, "f_i+g_i"'] & M_{i-1} \arrow[r] \arrow[d, "f_{i-1}+g_{i-1}"] & \cdots \\
\mathcal{N}: \cdots \arrow[r] & N_i \arrow[r, "d'_i"'] & N_{i-1} \arrow[r] & \cdots
\end{tikzcd}$$

es conmutativo. De acuerdo con lo anterior podemos dar la siguiente definición.

Definición 3.1.4 *Si $f : \mathcal{M} \to \mathcal{N}$ y $g : \mathcal{M} \to \mathcal{N}$ son dos aplicaciones de cadenas, la **suma** de f y g es la aplicación de cadenas $f + g : \mathcal{M} \to \mathcal{N}$ que viene dada por la familia de morfismos $f_i + g_i : M_i \to N_i$.*

Si $(\mathcal{M}, d)$, $(\mathcal{N}, d')$ y $(\mathcal{T}, d'')$ son tres complejos y $f : \mathcal{M} \to \mathcal{N}$ y $g : \mathcal{N} \to \mathcal{T}$ son dos aplicaciones de cadenas, para cada i, $d'_i \circ f_i = f_{i-1} \circ d_i$ y $d''_i \circ g_i = g_{i-1} \circ d'_i$. Por tanto $d''_i \circ (g_i \circ f_i) = (d''_i \circ g_i) \circ f_i = (g_{i-1} \circ d'_i) \circ f_i = g_{i-1} \circ (d'_i \circ f_i) =$

$g_{i-1} \circ (f_{i-1} \circ d_i) = (g_{i-1} \circ f_{i-1}) \circ d_i$, lo que nos indica que el siguiente diagrama conmuta

$$\begin{tikzcd}
\mathcal{M}: \cdots \arrow[r] & M_i \arrow[r, "d_i"] \arrow[d, "g_i \circ f_i"'] & M_{i-1} \arrow[r] \arrow[d, "g_{i-1} \circ f_{i-1}"] & \cdots \\
\mathcal{T}: \cdots \arrow[r] & T_i \arrow[r, "d''_i"'] & T_{i-1} \arrow[r] & \cdots .
\end{tikzcd}$$

Esto nos permite dar la definición que sigue.

Definición 3.1.5 *Sean $f : \mathcal{M} \to \mathcal{N}$ y $g : \mathcal{N} \to \mathcal{T}$ dos aplicaciones de cadena. La* ***composición*** *de f y g es la aplicación de cadenas $g \circ f : \mathcal{M} \to \mathcal{N}$ que está dada por la familia de morfismos $g_i \circ f_i : M_i \to N_i$.*

Observación. La asociatividad de los morfismos de módulos implica la asociatividad de aplicaciones de cadenas. Además todos los complejos y todas las aplicaciones de cadenas con la composición definida anteriormente forman una categoría, la cual denotaremos por *Comp*.

Proposición 3.1.6 *La categoría Comp es una categoría aditiva.*

Demostración. Directamente se prueba que:

(1) Para cada pareja $(\mathcal{M},\mathcal{N})$ de objetos en la categoría *Comp*, $+$ induce en $hom_{Comp}(\mathcal{M},\mathcal{N})$ la estructura de un grupo abeliano.

(2) Si $\mathcal{M} \xrightarrow{k} \mathcal{N} \overset{g}{\underset{h}{\rightrightarrows}} \mathcal{T} \xrightarrow{f} \mathcal{U}$ son morfismos en *Comp*, entonces $f \circ (g + h) = (f \circ g) + (f \circ h)$ y $(g + h) \circ k = (g \circ k) + (h \circ k)$.

□

Proposición 3.1.7 *Si $f : \mathcal{M} \to \mathcal{N}$ es una aplicación de cadenas, como lo muestra el diagrama*

$$\begin{tikzcd}
\mathcal{M}: & \cdots \arrow[r] & M_{i+1} \arrow[r, "d_{i+1}"] \arrow[d, "f_{i+1}"'] & M_i \arrow[r, "d_i"] \arrow[d, "f_i"'] & M_{i-1} \arrow[r] \arrow[d, "f_{i-1}"'] & \cdots \\
\mathcal{N}: & \cdots \arrow[r] & N_{i+1} \arrow[r, "d'_{i+1}"'] & N_i \arrow[r, "d'_i"'] & N_{i-1} \arrow[r] & \cdots ,
\end{tikzcd}$$

entonces para cada i, $H_i(f) : H_i(\mathcal{M}) \to H_i(\mathcal{N})$, definido por $H_i(f)(\overline{m}) = \overline{f_i(m)}$ para cada $m \in \ker(d_i)$, es un morfismo de grupos abelianos.

Demostración. Debemos probar que $H_i(f)$ está bien definida.

Primero veamos que si $m \in \ker(d_i)$, entonces $f_i(m) \in \ker(d'_i)$. Si $m \in \ker(d_i)$, $d_i(m) = 0$, entonces $f_{i-1}(d_i(m)) = f_{i-1}(0) = 0$. Pero $0 = f_{i-1}(d_i(m)) = d'_i(f_i(m))$, así, $f_i(m) \in \ker(d'_i)$.

Ahora verifiquemos que si $m_1, m_2 \in \ker(d_i)$ y $\overline{m}_1 = \overline{m}_2$, se cumple que $H_i(f)(\overline{m}_1) = H_i(f)(\overline{m}_2)$, es decir, $f_i(m_1) - f_i(m_2) \in Im(d'_{i+1})$. Supongamos que $m_1, m_2 \in \ker(d_i)$ y $\overline{m}_1 = \overline{m}_2$, entonces $m_1 - m_2 \in Im(d_{i+1})$. Así que hay un $x_0 \in M_{i+1}$ tal que $d_{i+1}(x_0) = m_1 - m_2$ y por tanto $f_i(d_{i+1}(x_0)) = f_i(m_1 - m_2)$. Pero $f_i \circ d_{i+1} = d'_{i+1} \circ f_{i+1}$, entonces $d'_{i+1}(f_{i+1}(x_0)) = f_i(m_1 - m_2) = f_i(m_1) - f_i(m_2)$, es decir, $f_i(m_1) - f_i(m_2) \in Im(d'_{i+1})$.

Finalmente probemos que para cada i, $H_i(f)$ es un morfismo de grupos abelianos. Para esto, sean $m_1, m_2 \in \ker(d_i)$, entonces

$$H_i(f)(\overline{m}_1 + \overline{m}_2) = \overline{f_i(m_1 + m_2)} = \overline{f_i(m_1)} + \overline{f_i(m_2)} = H_i(f)(\overline{m}_1) + H_i(f)(\overline{m}_2).$$

□

Observación. La definición 3.1.2 junto con la proposición 3.1.7 nos definen para cada $i \in \mathbb{Z}$, una correspondencia H_i tal que a cada objeto en la categoría *Comp* le asocia un único objeto en la categoría *Ab* y a cada morfismo en *Comp* le asocia un único morfismo en *Ab*.

Proposición 3.1.8 *$H_i : Comp \to Ab$ es un funtor covariante aditivo.*

Demostración. Primero veamos que H_i preserva las composiciones. Sean $f : \mathcal{M} \to \mathcal{N}$ y $g : \mathcal{N} \to \mathcal{T}$ dos aplicaciones de cadenas. Hay que probar que $H_i(g \circ f) = H_i(g) \circ H_i(f)$, esto es, que para cada $x \in \ker(d_i)$, $H_i(g \circ f)(\overline{x}) = (H_i(g) \circ H_i(f))(\overline{x})$. Sea $x \in \ker(d_i)$, entonces $H_i(g \circ f)(\overline{x}) = \overline{(g \circ f)_i(x)} = \overline{(g_i \circ f_i)(x)} = \overline{g_i(f_i(x))} = H_i(g)(\overline{f_i(x)}) = H_i(g)(H_i(f)(\overline{x})) = (H_i(g) \circ H_i(f))(\overline{x})$.

Ahora vamos a probar que H_i preserva identidades, esto es, que para cada complejo $\mathcal{M}$, $H_i(1_{\mathcal{M}}) = 1_{H_i(\mathcal{M})}$, o sea que para cada $x \in \ker(d_i)$, $H_i(1_{\mathcal{M}})(\overline{x}) = 1_{H_i(\mathcal{M})}(\overline{x})$. Sea $\mathcal{M}$ un complejo y sea $x \in \ker(d_i)$, entonces $H_i(1_{\mathcal{M}})(\overline{x}) = \overline{1_{\mathcal{M}_i}(x)} = \overline{x} = 1_{H_i(\mathcal{M})}(\overline{x})$.

Finalmente veamos que H_i es aditivo. Sean $\mathcal{M}$ y $\mathcal{N}$ dos complejos y sean $f, g : \mathcal{M} \to \mathcal{N}$ dos aplicaciones de cadenas. Debemos mostrar que $H_i(f + g) = H_i(f) + H_i(g)$. Sea $x \in \ker(d_i)$, entonces $H_i(f + g)(\overline{x}) = \overline{(f + g)_i(x)} = \overline{(f_i + g_i)(x)} = \overline{f_i(x) + g_i(x)} = \overline{f_i(x)} + \overline{g_i(x)} = H_i(f)(\overline{x}) + H_i(g)(\overline{x})$. □

Definición 3.1.9 *Al funtor $H_i : Comp \to Ab$ se le llama **i-ésimo funtor de homología**.*

Definición 3.1.10 *Sean $\mathcal{M}$ y $\mathcal{N}$ dos complejos y sean $f, g : \mathcal{M} \to \mathcal{N}$ dos aplicaciones de cadenas*

$$\begin{tikzcd}
\mathcal{M}: & \cdots \arrow[r] & M_{i+1} \arrow[r, "d_{i+1}"] & M_i \arrow[r, "d_i"] \arrow[dl, dotted, "s_i"'] \arrow[d, shift right, "f_i"'] \arrow[d, shift left, "g_i"] & M_{i-1} \arrow[r] \arrow[dl, dotted, "s_{i-1}"] & \cdots \\
\mathcal{N}: & \cdots \arrow[r] & N_{i+1} \arrow[r, "d'_{i+1}"'] & N_i \arrow[r, "d'_i"'] & N_{i-1} \arrow[r] & \cdots .
\end{tikzcd}$$

*Diremos que f y g son **homotópicamente equivalentes** si hay una familia*

*$(s_i)_{i\in Z}$ de morfismos con $s_i : M_i \to N_{i+1}$ tales que $f_i - g_i = d'_{i+1} \circ s_i + s_{i-1} \circ d_i$ para cada i. La familia (s_i) es llamada una **homotopía**.*

Observación. El concepto de homotopía define una relación de equivalencia $\sim$ en las aplicaciones de cadena como sigue: si $f, g : \mathcal{M} \to \mathcal{N}$ son dos aplicaciones de cadenas, $f \sim g$ si y sólo si hay una homotopía entre ellas.

Proposición 3.1.11 *Sean $f, g : \mathcal{M} \to \mathcal{N}$ dos aplicaciones de cadenas. Si f y g son homotópicas, entonces para cada i, $H_i(f) = H_i(g) : H_i(\mathcal{M}) \to H_i(\mathcal{N})$.*

Demostración. Como f y g son homotópicas, entonces hay una familia de morfismos $(s_i : M_i \to N_{i+1})$ tal que para cada i, $f_i - g_i = d'_{i+1} \circ s_i + s_{i-1} \circ d_i$. Tomamos $\overline{z} \in H_i(\mathcal{M})$ con $z \in \ker(d_i)$, entonces

$$\begin{aligned}(H_i(f) - H_i(g))(\overline{z}) &= H_i(f)(\overline{z}) - H_i(g)(\overline{z}) = \overline{f_i(z)} - \overline{g_i(z)} \\ &= \overline{(f_i - g_i)(z)} = \overline{(d'_{i+1} \circ s_i + s_{i-1} \circ d_i)(z)} = \overline{(d'_{i+1} \circ s_i)(z) + (s_{i-1} \circ d_i)(z)} \\ &= \overline{d'_{i+1}(s_i(z)) + s_{i-1}(d_i(z))} = 0,\end{aligned}$$

pues $d'_{i+1}(s_i(z)) \in Im(d'_{i+1})$ y $z \in \ker(d_i)$. Por lo tanto, $H_i(f) = H_i(g)$. $\square$

Proposición 3.1.12 *Si $F : R\text{-}Mod \to S\text{-}Mod$ es un funtor covariante aditivo, entonces F preserva homotopías.*

Demostración. Supongamos que $f, g : \mathcal{M} \to \mathcal{N}$ son dos aplicaciones de cadenas que son homotópicas y sea $(M_i \xrightarrow{s_i} N_{i+1})$ una familia de morfismos tal que para cada i, $f_i - g_i = d'_{i+1} \circ s_i + s_{i-1} \circ d_i$, entonces $F(f_i) - F(g_i) = F(f_i - g_i) = F(d'_{i+1} \circ s_i + s_{i-1} \circ d_i) = F(d'_{i+1}) \circ F(s_i) + F(s_{i-1}) \circ F(d_i)$. $\square$

Proposición 3.1.13 *Si $F : R\text{-}Mod \to S\text{-}Mod$ es un funtor contravariante aditivo, entonces F preserva homotopías.*

Demostración. La prueba es semejante a la de la proposición anterior, no olvidando los cambios que hay que efectuar en los subíndices. $\square$

3.2. Sucesiones exactas largas

Definición 3.2.1 *Sean $f : \mathcal{M} \to \mathcal{N}$ y $g : \mathcal{N} \to \mathcal{T}$ dos aplicaciones de cadenas. Diremos que la sucesión*

$$0 \longrightarrow \mathcal{M} \xrightarrow{f} \mathcal{N} \xrightarrow{g} \mathcal{T} \longrightarrow 0$$

*es una **sucesión exacta corta de complejos** si para cada i hay una sucesión exacta corta dada por:*

$$0 \longrightarrow M_i \xrightarrow{f_i} N_i \xrightarrow{g_i} T_i \longrightarrow 0\ .$$

La sucesión exacta corta de complejos tiene una estructura como la que muestra el siguiente diagrama, cuyas filas son sucesiónes exactas cortas y las columnas son complejos.

$$\begin{tikzcd}
 & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \\
0 \arrow[r] & M_{i+1} \arrow[r, "f_{i+1}"] \arrow[d, "d_{i+1}"'] & N_{i+1} \arrow[r, "g_{i+1}"] \arrow[d, "d'_{i+1}"'] & T_{i+1} \arrow[r] \arrow[d, "d''_{i+1}"'] & 0 \\
0 \arrow[r] & M_{i} \arrow[r, "f_{i}"] \arrow[d, "d_{i}"'] & N_{i} \arrow[r, "g_{i}"] \arrow[d, "d'_{i}"'] & T_{i} \arrow[r] \arrow[d, "d''_{i}"'] & 0 \\
0 \arrow[r] & M_{i-1} \arrow[r, "f_{i-1}"] \arrow[d] & N_{i-1} \arrow[r, "g_{i-1}"] \arrow[d] & T_{i-1} \arrow[r] \arrow[d] & 0 \\
 & \vdots & \vdots & \vdots & .
\end{tikzcd}$$

Teorema 3.2.2 *Supongamos que tenemos una sucesión exacta corta de complejos:*

$$0 \longrightarrow \mathcal{M} \xrightarrow{f} \mathcal{N} \xrightarrow{g} \mathcal{T} \longrightarrow 0.$$

*Ésta induce una **sucesión exacta larga** de mapeos en homología*

$$\begin{tikzcd}
\cdots \arrow[r] & H_i(\mathcal{M}) \arrow[r, "H_i(f)"] & H_i(\mathcal{N}) \arrow[r, "H_i(g)"] & H_i(\mathcal{T}) \arrow[dll, rounded corners, "\delta_i"] & \\
 & H_{i-1}(\mathcal{M}) \arrow[r, "H_{i-1}(f)"] & H_{i-1}(\mathcal{N}) \arrow[r, "H_{i-1}(g)"] & H_{i-1}(\mathcal{T}) \arrow[r] & \cdots .
\end{tikzcd}$$

*Los mapeos $\delta_i : H_i(\mathcal{T}) \to H_{i-1}(\mathcal{M})$ son llamados **morfismos conectores**.*

Demostración. Ya vimos cómo para cada i se pueden definir morfismos entre los grupos abelianos $H_i(f)$ y $H_i(g)$. Así, lo que nos resta es definir δ_i, verificar que es un morfismo de grupos abelianos y verificar la exactitud en todos los puntos de la sucesión exacta larga.

Sea $x \in \ker(d''_i) \subseteq T_i$, entonces como g_i es suprayectiva, hay un $y \in N_i$ tal que $g_i(y) = x$. Luego

$$0 = (d''_i)(x) = (d''_i)(g_i(y)) = g_{i-1}(d'_i(y))$$

y por tanto $d'_i(y) \in \ker(g_{i-1}) = Im(f_{i-1})$. Así que existe un único $z \in M_{i-1}$ tal que $f_{i-1}(z) = (d'_i)(y)$ (esto último es porque f_{i-1} es inyectiva). Además

$$f_{i-2}(d_{i-1}(z)) = d'_{i-1}(f_{i-1}(z)) = d'_{i-1}(d'_i(y)) = 0,$$

y como f_{i-2} es inyectiva, $d_{i-1}(z) = 0$. Luego $f_{i-1}^{-1}(d'_i(y)) = z \in \ker(d_{i-1})$.

$$\begin{tikzcd}
 & \exists y \arrow[r, "g_i"] \arrow[d, "d'_i"'] & x \arrow[d, "d''_i"] \\
\exists ! z \arrow[r, "f_{i-1}"] \arrow[d, "d_{i-1}"'] & d'_i(y) \arrow[r, "g_{i-1}"] \arrow[d, "d'_{i-1}"'] & 0 \\
0 = d_{i-1}(z) \arrow[r, "f_{i-2}"'] & 0 &
\end{tikzcd}$$

Entonces definimos δ_i por $\delta_i(\overline{x}) = \overline{(f_{i-1}^{-1} \circ d'_i)(y)}$ para algún $y \in N_i$ tal que $g_i(y) = x$. Veamos que δ_i está bien definida.

Mostraremos que $\delta_i(\overline{x})$ es independiente de la elección de $y \in g_i^{-1}(x)$. Para esto, supongamos que $y' \in N_i$ es tal que $g_i(y') = x = g_i(y)$, entonces $0 = g_i(y - y')$, lo que implica que $y - y' \in \ker(g_i) = Im(f_i)$, o sea que hay un único $w \in M_i$ tal que $f_i(w) = y - y'$, de donde se sigue que $d'_i(y) - d'_i(y') = d'_i(y - y') = d'_i(f_i(w)) = f_{i-1}(d_i(w)) \in Im(f_{i-1})$. Luego $f_{i-1}^{-1}(d'_i(y)) - f_{i-1}^{-1}(d'_i(y')) = d_i(w) \in Im(d_i)$, es decir, $\overline{(f_{i-1}^{-1} \circ d'_i)(y)} = \overline{(f_{i-1}^{-1} \circ d'_i)(y')}$.

Ahora veamos que la elección de $\overline{(f_{i-1}^{-1} \circ d'_i)(y)}$ es independiente de la elección de los representantes en $\overline{x}$. Tomemos $x_1, x_2 \in \ker(d''_i)$ tales que $\overline{x_1} = \overline{x_2}$, o sea, $x_1 - x_2 \in Im(d''_{i+1})$. Hay que probar que $\delta_i(\overline{x}_1) = \delta_i(\overline{x}_2)$, lo cual equivale a que existan $y_1, y_2 \in N_i$ tales que $\overline{(f_{i-1}^{-1} \circ d'_i)(y_1)} = \overline{(f_{i-1}^{-1} \circ d'_i)(y_2)}$ con $g_i(y_1) = x_1$ y $g_i(y_2) = x_2$. Ahora bien, como $x_1 - x_2 \in Im(d''_{i+1})$ entonces hay un $u \in T_{i+1}$ tal que $d''_{i+1}(u) = x_1 - x_2$, lo que garantiza la existencia de $v \in N_{i+1}$ tal que $g_{i+1}(v) = u$, con lo cual tenemos que $x_1 - x_2 = d''_{i+1}(u) = d''_{i+1}(g_{i+1}(v)) = g_i(d'_{i+1}(v))$. Pero $d'_i(d'_{i+1}(v)) = 0 \in Im(f_{i-1})$, luego $(f_{i-1}^{-1} \circ d'_i)(d'_{i+1}(v)) = f_{i-1}^{-1}(0) = 0$, o sea que $\overline{(f_{i-1}^{-1} \circ d'_i)(d'_{i+1}(v))} = Im(d_i)$. Además, como $x_1, x_2 \in \ker(d''_i)$, existen $y_1, y_2 \in N_i$ tales que $g_i(y_1) = x_1$ y $g_i(y_2) = x_2$. Así que $g_i(y_1 - y_2) = x_1 - x_2$, lo que implica que $g_{i-1}(d'_i(y_1 - y_2)) = d''_i(g_i(y_1 - y_2)) = d''_i(x_1 - x_2) = 0$. Esto nos dice que $d'_i(y_1 - y_2) \in \ker(g_{i-1}) = Im(f_{i-1})$, y de esto se sigue que $f_{i-1}^{-1}(d'_i(y_1 - y_2)) = f_{i-1}^{-1}(d'_i(y_1) - d'_i(y_2)) =$

$f_{i-1}^{-1}(d'_i(y_1)) - f_{i-1}^{-1}(d'_i(y_2))$. Esto y que $\delta_i(\overline{x_1 - x_2})$ es independiente de la elección de los elementos en $g^{-1}(x_1 - x_2)$, implican que $\overline{(f_{i-1}^{-1} \circ d'_i)(y_1 - y_2)} = \overline{(f_{i-1}^{-1} \circ d'_i)(d'_{i+1}(v))}$ y por lo tanto $\overline{(f_{i-1}^{-1} \circ d'_i)(y_1)} = \overline{(f_{i-1}^{-1} \circ d'_i)(y_2)}$.

El que δ_i sea un morfismo se sigue del hecho de que $f_{i-1}^{-1} \circ d'_i$ es un morfismo.

Ahora vamos a probar la exactitud en $H_i(\mathcal{N})$, es decir, vamos a probar que $Im(H_i(f)) = \ker(H_i(g))$. Sea $\overline{x} \in H_i(\mathcal{M})$, entonces $H_i(g)(H_i(f)(\overline{x})) = H_i(g)(\overline{f_i(x)}) = \overline{g_i(f_i(x))} = \overline{0}$, lo que indica que $Im(H_i(f)) \subseteq \ker(H_i(g))$. Recíprocamente, si $\overline{x} \in \ker(H_i(g)) \subseteq H_i(\mathcal{N})$, entonces $H_i(g)(\overline{x}) = \overline{g_i(x)} = 0$, o sea que $g_i(x) \in Im(d''_{i+1})$, lo que implica que hay un $u \in T_{i+1}$ tal que $d''_{i+1}(u) = g_i(x)$. Luego hay un $v \in N_{i+1}$ que cumple que $g_{i+1}(v) = u$, y al aplicar d''_{i+1} tenemos que $g_i(d'_{i+1}(v)) = d''_{i+1}(g_{i+1}(v)) = d''_{i+1}(u) = g_i(x)$, de lo cual se sigue que $0 = g_i(x) - g_i(d'_{i+1}(v)) = g_i(x - d'_{i+1}(v))$. Así $x - d'_{i+1}(v) \in \ker(g_i) = Im(f_i)$ y de este modo hay un $w \in M_i$ tal que $f_i(w) = x - d'_{i+1}(v)$. Probar que $\overline{x} \in Im(H_i(f))$ equivale a probar que para algún $w \in \ker(d_i)$, $H_i(f)(\overline{w}) = \overline{x}$. Además, $w \in \ker(d_i)$ equivale a que $f_{i-1}(d_i(w)) = 0$.

Como $f_{i-1}(d_i(w)) = d'_i(f_i(w)) = d'_i(x - d'_{i+1}(v)) = d'_i(x) = 0$ (ya que por definición $x \in \ker(d'_i)$). Por lo tanto, $w \in \ker(d_i)$ y $f_i(w) - x = -d'_{i+1}(v) = d'_{i+1}(-v)$.

En esta parte probaremos la exactitud en $H_i(\mathcal{T})$, esto es, probaremos que $Im(H_i(g)) = \ker(\delta_i)$. Sea $\overline{x} \in H_i(N)$, entonces $\delta_i(H_i(g)(\overline{x})) = \overline{(f_{i-1}^{-1} \circ d'_i)(y)}$ para algún $y \in N_i$ tal que $g_i(y) = g_i(x)$. Queremos probar que $\delta_i(H_i(g)(\overline{x})) = 0$, esto es, queremos probar que $\delta_i(\overline{g_i(x)}) = \overline{(f_{i-1}^{-1} \circ d'_i)(y)} = 0$ para algún $y \in N_i$ tal que $g_i(y) = g_i(x)$. En particular, si hacemos $y = x$ tenemos que $\delta_i(H_i(g)(\overline{x})) = \overline{(f_{i-1}^{-1} \circ d'_i)(x)} = \overline{f_{i-1}^{-1}(0)} = 0$. Recíprocamente, si $\overline{x} \in \ker(\delta_i)$, entonces $\delta_i(\overline{x}) = \overline{(f_{i-1}^{-1} \circ d'_i)(y)} = 0$ para algún $y \in N_i$ tal que $g_i(y) = x$ y de esto tenemos que $(f_{i-1}^{-1} \circ d'_i)(y) \in Im(d_i)$. De aquí que haya un $m \in M_i$ tal que $d_i(m) = (f_{i-1}^{-1} \circ d'_i)(y)$ y aplicando f_{i-1} tenemos que $d'_i(f_i(m)) = f_{i-1}(d_i(m)) = d'_i(y)$, lo cual implica que $0 = d'_i(y) - d'_i(f_i(m)) = d'_i(y - f_i(m))$ y así tenemos que $y - f_i(m) \in \ker(d'_i)$. Hay que probar que $\overline{x} \in Im(H_i(g))$, esto es, probar que hay un $u \in \ker(d'_i)$ tal que $\overline{g_i(u)} = \overline{x}$, es decir, probar que hay un $u \in \ker(d'_i)$ tal que $g_i(u) - x \in Im(d''_{i-1})$. Como $g_i(y - f_i(m)) - x = g_i(y) - g_i(f_i(m)) - x = g_i(y) - x = x - x = 0$, implica que $\overline{g_i(y - f_i(m))} = \overline{x}$, basta tomar $u = y - f_i(m)$.

Únicamente falta probar la exactitud en $H_{i-1}(\mathcal{M})$, esto es, sólo falta probar que $Im(\delta_i) = \ker(H_{i-1}(f))$. Sea $\overline{x} \in H_i(\mathcal{T})$, entonces $H_{i-1}(f)(\delta_i(\overline{x})) = H_{i-1}(f)(\overline{(f_{i-1}^{-1} \circ d'_i)(y)}) = \overline{d'_i(y)}$ para algún $y \in N_i$ tal que $g_i(y) = x$. Además $\overline{d'_i(y)} = 0$, pues $d'_i(y) \in Im(d'_i)$. Finalmente, sea $\overline{x} \in \ker(H_{i-1}(f))$, entonces $H_{i-1}(f)(\overline{x}) = \overline{f_{i-1}(x)} = 0 = Im(d'_i)$, es decir, $f_{i-1}(x) \in Im(d'_i)$ lo cual garantiza que hay un $y \in N_i$ tal que $d'_i(y) = f_{i-1}(x)$ y aplicando g_{i-1} tenemos que $d''_i(g_i(y)) = g_{i-1}(d'_i(y)) = g_{i-1}(f_{i-1}(x)) = 0$, o sea que $g_i(y) \in \ker(d''_i)$, lo cual implica que $\delta_i(\overline{g_i(y)}) = \overline{(f_{i-1}^{-1} \circ d'_i)(y)} = \overline{(f_{i-1}^{-1}(f_{i-1}(x)))} = \overline{x}$. Pero $\overline{x} \in Im(\delta_i)$ si y sólo si hay un $u \in \ker(d''_i)$ tal que $\delta_i(\overline{u}) = \overline{x}$. Esto equivale a que hay un $u \in \ker(d''_i)$ tal que $\overline{(f_{i-1}^{-1} \circ d'_i)(y)} = \overline{x}$ para algún $y \in M_i$ tal que $g_i(y) = u$. Así, tomamos $u = g_i(y)$. $\square$

3.3. Resoluciones

Definición 3.3.1 (1) *Una **resolución proyectiva** de un R-módulo M es un complejo exacto de la forma*

$$\mathcal{P}: \; \cdots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} M \longrightarrow 0,$$

*donde $P_0, P_1, \ldots$ son módulos proyectivos. Si $P_0, P_1, \ldots$ son módulos libres, entonces la resolución es una **resolución libre** de M.*

$$\mathcal{P}_M: \; \cdots \longrightarrow P_3 \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \longrightarrow 0$$

*se llama **complejo recortado** de $\mathcal{P}$.*

(2) *Una **resolución inyectiva** de un R-módulo M es un complejo exacto de la forma*

$$\mathcal{E}: \; 0 \longrightarrow M \xrightarrow{d_0} E_0 \xrightarrow{d_1} E_1 \xrightarrow{d_2} E_2 \longrightarrow \cdots,$$

donde $E_0, E_1, \ldots$ son módulos inyectivos.

$$\mathcal{E}_M: \; 0 \longrightarrow E_0 \xrightarrow{d_1} E_1 \xrightarrow{d_2} E_2 \xrightarrow{d_3} E_3 \longrightarrow \cdots$$

*se llama **complejo recortado** de $\mathcal{E}$.*

Proposición 3.3.2 *Todo R-módulo M tiene una resolución proyectiva.*

Demostración. Sea M un R-módulo. Cuando probamos que todo R-módulo es un cociente de un libre, vimos también que hay un epimorfismo $h_1 : F_1 \to M$, con F_1 libre. Así, la sucesión

$$0 \longrightarrow \ker(h_1) \xrightarrow{i_1} F_1 \xrightarrow{h_1} M \longrightarrow 0$$

es exacta (donde i_1 es la inclusión). Si $h_1 := d_1$ y $F_0 := \ker(h_0) := M$, entonces siguiendo un razonamiento inductivo, tenemos que para cada $n \in \mathbb{N}$, hay una sucesión exacta

$$0 \longrightarrow \ker(h_h) \xrightarrow{i_n} F_n \xrightarrow{h_n} \ker(h_{n-1}) \longrightarrow 0$$

donde F_n es libre, i_n es la inclusión y h_n es un epimorfismo. Considerando el siguiente diagrama:

$$\begin{tikzcd}
 & \cdots \arrow[r] & F_{n+1} \arrow[rr, "d_{n+1}"] \arrow[dr, "h_{n+1}"] & & F_n \arrow[r, "d_n"] & F_{n-1} \arrow[r] & \cdots \\
 & \ker(h_{n+1}) \arrow[ur, "i_{n+1}"] & & \ker(h_n) \arrow[ur, "i_n"] \arrow[dr] & & & \\
0 \arrow[ur] & & 0 \arrow[ur] & & 0, & &
\end{tikzcd}$$

hacemos para cada $n \geq 2$, $d_n = i_{n-1} \circ h_n$.

Así tenemos que $d_1 \circ d_2 = d_1 \circ (i_1 \circ h_2) = (d_1 \circ i_1) \circ h_2 = 0 \circ h_2 = 0$ y $d_n \circ d_{n+1} = (i_{n-1} \circ h_n) \circ (i_n \circ h_{n+1}) = i_{n-1} \circ (h_n \circ i_n) \circ h_{n+1} = i_{n-1} \circ 0 \circ h_{n+1} = 0$, o sea que para cada $n \in \mathbb{N}$, $Im(d_{n+1}) \subseteq \ker(d_n)$.

Por otra parte, al tomar $x \in \ker(d_n) = \ker(i_{n-1} \circ h_n)$, se sigue que $(i_{n-1} \circ h_n)(x) = i_{n-1}(h_n(x)) = 0$, lo cual implica que $h_n(x) = 0$. Luego $x \in \ker(h_n)$. Como h_{n+1} es suprayectiva, hay un $y \in F_{n+1}$ tal que $h_{n+1}(y) = x$. De esto se sigue que $d_{n+1}(y) = i_n \circ h_{n+1}(y) = i_n(h_{n+1}(y)) = i_n(x) = x$, lo cual nos dice que $x \in Im(d_{n+1})$. Por tanto $\ker(d_n) \subseteq Im(d_{n+1})$.

De esta forma M tiene una resolución libre y por lo tanto proyectiva. $\square$

Proposición 3.3.3 *Todo R-módulo M tiene una resolución inyectiva.*

Demostración. De 1.10.7 sabemos que hay una sucesión exacta

$$0 \longrightarrow M \xrightarrow{d_0} E_0 \xrightarrow{p_1} E_0/Im(d_0) \longrightarrow 0,$$

donde E_0 es un módulo inyectivo. De manera análoga a como se hizo en la prueba anterior se construye una resolución inyectiva para M. $\square$

Proposición 3.3.4 *Supongamos que tenemos dos complejos como se muestra en el diagrama:*

$$\begin{tikzcd}
\cdots \arrow[r] & P_2 \arrow[r, "d_2"] \arrow[d, dotted, "f_2"'] & P_1 \arrow[r, "d_1"] \arrow[d, dotted, "f_1"'] & P_0 \arrow[r, "d_0"] \arrow[d, dotted, "f_0"'] & N \arrow[r] \arrow[d, "\varphi"] & 0 \\
\cdots \arrow[r] & M_2 \arrow[r, "d'_2"] & M_1 \arrow[r, "d'_1"] & M_0 \arrow[r, "d'_0"] & M \arrow[r] & 0,
\end{tikzcd}$$

donde los P_i son proyectivos, la fila inferior es exacta y $\varphi : N \to M$ es un morfismo. Entonces hay una aplicación de cadenas $f = \{P_i \xrightarrow{f_i} M_i\}$ inducida por φ. Si $f' = \{P_i \xrightarrow{f'_i} M_i\}$ es otra aplicación de cadenas inducida por φ, entonces f y f' son homotópicamente equivalentes.

Demostración. Como $\varphi \circ d_0$ es un R-morfismo, d'_0 es un epimorfismo y P_0 es proyectivo se sigue que hay un morfismo $f_0 : P_0 \to M_0$ tal que $d'_0 \circ f_0 = \varphi \circ d_0$.

Ahora procedemos inductivamente. Supongamos que para $j < n$, hay un morfismo $f_j : P_j \to M_j$ tal que $d'_j \circ f_j = f_{j-1} \circ d_j$, entonces

$$d'_j \circ (f_j \circ d_{j+1}) = (d'_j \circ f_j) \circ d_{j+1} = (f_{j-1} \circ d_j) \circ d_{j+1} = f_{j-1} \circ (d_j \circ d_{j+1}) = 0.$$

De esto tenemos que $Im(f_j \circ d_{j+1}) \subseteq \ker(d'_j) = Im(d'_{j+1})$. Consideremos el siguiente diagrama:

$$\begin{tikzcd}
 & P_{j+1} \arrow[dl, dotted, "f_{j+1}"'] \arrow[d, "f_j \circ d_{j+1}"] & \\
M_{j+1} \arrow[r, "d'_{j+1}"'] & Im(d'_{j+1}) \arrow[r] & 0.
\end{tikzcd}$$

Como P_{j+1} es proyectivo y $d'_{j+1} : M_{j+1} \to Im(d'_{j+1})$ es suprayectiva, tenemos que hay un morfismo $f_{j+1} : P_{j+1} \to M_{j+1}$ tal que

$$d'_{j+1} \circ f_{j+1} = f_j \circ d_{j+1}.$$

Esto completa el paso inductivo y queda garantizada la existencia de la aplicación de cadenas f.

Ahora supongamos que f y f' son dos aplicaciones de cadenas tales que $d'_i \circ f_i = f_{i-1} \circ d_i$ y $d'_i \circ f'_i = f'_{i-1} \circ d_i$. Debemos probar que hay morfismos $s_i : P_i \to M_{i+1}$ tales que $f_i - f'_i = d'_{i+1} \circ s_i + s_{i-1} \circ d_i$. Haremos la prueba usando inducción.

Para $i < 0$, definimos s_i como el morfismo cero. De este modo tenemos que para cada $i < 0$, $0 = f_i - f'_i = d'_{i+1} \circ s_i + s_{i-1} \circ d_i$.

Ahora supongamos que para cada $i < n$ $(n \geq 0)$ hay morfismos $s_i : P_i \to M_{i+1}$ tales que $f_i - f'_i = d'_{i+1} \circ s_i + s_{i-1} \circ d_i$ y consideremos el siguiente diagrama

$$\begin{tikzcd}
\cdots \arrow[r] & P_{i+1} \arrow[r, "d_{i+1}"] & P_i \arrow[r, "d_i"] \arrow[dl, dotted, "s_i"'] \arrow[d, shift right, "f'_i"'] \arrow[d, shift left, "f_i"] & P_{i-1} \arrow[r] \arrow[dl, dotted, "s_{i-1}"] & \cdots \\
\cdots \arrow[r] & M_{i+1} \arrow[r, "d'_{i+1}"'] & M_i \arrow[r, "d'_i"'] & M_{i-1} \arrow[r] & \cdots,
\end{tikzcd}$$

entonces

$$\begin{aligned}
&d'_{i+1} \circ ((f_{i+1} - f'_{i+1}) - (s_i \circ d_{i+1})) = \\
&\quad = (d'_{i+1} \circ (f_{i+1} - f'_{i+1})) - (d'_{i+1} \circ (s_i \circ d_{i+1})) \\
&\quad = (d'_{i+1} \circ (f_{i+1} - f'_{i+1})) - ((d'_{i+1} \circ s_i) \circ d_{i+1}) \\
&\quad = (d'_{i+1} \circ (f_{i+1} - f'_{i+1})) - (((f_i - f'_i) - (s_{i-1} \circ d_i)) \circ d_{i+1}) \\
&\quad = (d'_{i+1} \circ (f_{i+1} - f'_{i+1})) - ((f_i - f'_i) \circ d_{i+1}) - ((s_{i-1} \circ d_i) \circ d_{i+1}) \\
&\quad = (d'_{i+1} \circ (f_{i+1} - f'_{i+1})) - ((f_i - f'_i) \circ d_{i+1}) \\
&\quad = d'_{i+1} \circ f_{i+1} - d'_{i+1} \circ f'_{i+1} - (f_i \circ d_{i+1} - f'_i \circ d_{i+1}) = 0.
\end{aligned}$$

De aquí obtenemos que $Im((f_{i+1} - f'_{i+1}) - (s_i \circ d_{i+1})) \subseteq ker(d_{i+1}) = Im(d'_{i+2})$. Del diagrama

$$\begin{tikzcd}
 & P_{i+1} \arrow[dl, dotted, "s_{i+1}"'] \arrow[d, "(f_{i+1} - f'_{i+1}) - (s_i \circ d_{i+1})"] & \\
M_{i+2} \arrow[r, "d'_{i+2}"'] & Im(d'_{i+2}) \arrow[r] & 0,
\end{tikzcd}$$

donde d'_{i+2} es un epimorfismo y P_{i+1} es proyectivo, se sigue que hay un morfismo $s_{i+1} : P_{i+1} \to M_{i+1}$ tal que $d'_{i+2} \circ s_{i+1} = (f_{i+1} - f'_{i+1}) - (s_i \circ d_{i+1})$. Luego $f_{i+1} - f'_{i+1} = d'_{i+2} \circ s_{i+1} + s_i \circ d_{i+1}$. Por lo tanto, f y f' son homotópicamente equivalentes. $\square$

Proposición 3.3.5 *Supongamos que tenemos dos complejos como se muestra en el diagrama:*

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r, "d_0"] & E_0 \arrow[r, "d_1"] & E_1 \arrow[r, "d_2"] & E_2 \arrow[r] & \cdots \\
0 \arrow[r] & M \arrow[u, "\varphi"'] \arrow[r, "d'_0"] & M_0 \arrow[u, dotted, "f_0"] \arrow[r, "d'_1"] & M_1 \arrow[u, dotted, "f_1"] \arrow[r, "d'_2"] & M_2 \arrow[u, dotted, "f_2"] \arrow[r] & \cdots ,
\end{tikzcd}$$

donde los E_i son inyectivos, la fila inferior es exacta y $\varphi : M \to N$ es un morfismo. Entonces hay una aplicación de cadenas $f = \{M_i \xrightarrow{f_i} E_i\}$ inducida por φ. Más aún, si $f' = \{M_i \xrightarrow{f'_i} E_i\}$ es otra aplicación de cadenas inducida por φ, entonces f y f' son homotópicamente equivalentes.

Demostración. Como $d_0 \circ \varphi$ es un R-morfismo, d'_0 es un monomorfismo y E_0 es inyectivo se sigue que hay un morfismo $f_0 : M_0 \to E_0$ tal que $f_0 \circ d'_0 = d_0 \circ \varphi$.

Ahora procedemos inductivamente. Supongamos que para $j < n$, hay un morfismo $f_j : M_j \to E_j$ tal que $f_j \circ d'_j = d_j \circ f_{j-1}$. Consideremos la aplicación $\overline{d'}_{j+1} : M_j / \ker(d'_{j+1}) \to M_{j+1}$ definida por $\overline{d'}_{j+1}(\overline{x}) := d'_{j+1}(x)$. Directamente se verifica que dicha aplicación está bien definida y que es un monomorfismo.

Sea $\overline{d_{j+1} \circ f_j} : M_j / \ker(d'_{j+1}) \to E_{j+1}$ que está definida por $\overline{d_{j+1} \circ f_j}(\overline{x}) := (d_{j+1} \circ f_j)(x)$. Veamos que $\overline{d_{j+1} \circ f_j}$ está bien definida y que es un morfismo.

Sean $\overline{x}$ y $\overline{x'}$ en $M_j / \ker(d'_{j+1})$ tales que $\overline{x} = \overline{x'}$, entonces $x - x' \in \ker(d'_{j+1}) = Im(d'_j)$, lo cual implica que para algún $y \in M_{j-1}$, $d'_j(y) = x - x'$. Entonces $(d_{j+1} \circ f_j)(x - x') = (d_{j+1} \circ f_j)(d'_j(y)) = ((d_{j+1} \circ f_j) \circ d'_j)(y) = (d_{j+1} \circ (f_j \circ d'_j))(y) = (d_{j+1} \circ (d_j \circ f_{j-1}))(y) = 0$ (la penúltima igualdad se da por la hipótesis de inducción). Así tenemos que $\overline{d_{j+1} \circ f_j}(\overline{x}) = (d_{j+1} \circ f_j)(x) = (d_{j+1} \circ f_j)(x') = \overline{d_{j+1} \circ f_j}(\overline{x'})$.

Que $\overline{d_{j+1} \circ f_j}$ sea un morfismo se sigue de que $(d_{j+1} \circ f_j)$ es un morfismo.

De esta forma, por ser E_{j+1} inyectivo tenemos que hay un morfismo $f_{j+1} : M_{j+1} \to E_{j+1}$ tal que el diagrama

$$\begin{tikzcd}
 & E_{j+1} & \\
0 \arrow[r] & M_j / \ker(d'_{j+1}) \arrow[u, "\overline{d_{j+1} \circ f_j}"] \arrow[r, "\overline{d'}_{j+1}"'] & M_{j+1} \arrow[ul, "f_{j+1}"']
\end{tikzcd}$$

conmuta, esto es, $f_{j+1} \circ \overline{d'}_{j+1} = \overline{d_{j+1} \circ f_j}$.

Luego, para cada $x \in M_j$, $(f_{j+1} \circ d'_{j+1})(x) = f_{j+1}(d'_{j+1}(x)) = f_{j+1}(\overline{d'}_{j+1}(\overline{x})) = (f_{j+1} \circ \overline{d'}_{j+1})(\overline{x}) = \overline{d_{j+1} \circ f_j}(\overline{x}) = (d_{j+1} \circ f_j)(x)$, o sea que $f_{j+1} \circ d'_{j+1} = d_{j+1} \circ f_j$.

De esta forma se garantiza la existencia de la aplicación de cadenas f.

Ahora suponemos que f y f' son dos aplicaciones de cadenas tales que $f_j \circ d'_j = d_j \circ f_{j-1}$ y $f'_j \circ d'_j = d_j \circ f'_{j-1}$. Mostraremos que hay una familia de morfismos $(M_j \xrightarrow{s_j} E_{j-1})$ tal que $f_j - f'_j = d_j \circ s_j + s_{j+1} \circ d'_{j+1}$. Haremos la prueba por inducción.

Para $j \leq 0$ definimos $s_j : M_j \to E_{j-1}$ como el morfismo cero. Entonces $0 = f_j - f'_j = d_j \circ s_j + s_{j+1} \circ d'_{j+1}$ para $j < 0$.

Ahora supongamos que para cada $j < n$ $(n \geq 0)$, existen morfismos $s_j : M_j \to E_{j-1}$ tales que $f_j - f'_j = d_j \circ s_j + s_{j+1} \circ d'_{j+1}$. Consideremos el siguiente diagrama

$$\begin{tikzcd}
\cdots \arrow[r] & E_{j-1} \arrow[r, "d_j"] & E_j \arrow[r, "d_{j+1}"] & E_{j+1} \arrow[r] & \cdots \\
\cdots \arrow[r] & M_{j-1} \arrow[u, "f_{j-1}-f'_{j-1}"] \arrow[r, "d'_j"'] & M_j \arrow[u, "f_j-f'_j"'] \arrow[ul, dotted, "s_j"] \arrow[r, "d'_{j+1}"'] & M_{j+1} \arrow[u, "f_{j+1}-f'_{j+1}"'] \arrow[ul, dotted, "s_{j+1}"] \arrow[r] & \cdots .
\end{tikzcd}$$

Definimos una aplicación $\overline{f_j - f'_j - (d_j \circ s_j)} : M_j / \ker(d'_{j+1}) \to E_j$ como sigue: $\overline{f_j - f'_j - (d_j \circ s_j)}(\overline{x}) := (f_j - f'_j - (d_j \circ s_j))(x)$. Veamos que está aplicación está bien definida. Sean $\overline{x}$ y $\overline{x'}$ en $M_j / \ker(d'_{j+1})$ tales que $\overline{x} = \overline{x'}$, entonces $x - x' \in \ker(d'_{j+1}) = Im(d'_j)$, lo cual implica que para algún $y \in M_{j-1}$, $d'_j(y) = x - x'$. Aplicando $f_j - f'_j - (d_j \circ s_j)$, por la hipótesis inductiva y por ser $f - f'$ una aplicación de cadenas obtenemos que

$$\begin{aligned}
\big(f_j - f'_j - (d_j \circ s_j)\big)(x - x') &= \big(f_j - f'_j - (d_j \circ s_j)\big)(d'_j(y)) \\
&= \Big(\big(f_j - f'_j - (d_j \circ s_j)\big) \circ d'_j\Big)(y) = \Big(\big((f_j - f'_j) \circ d'_j\big) - \big((d_j \circ s_j) \circ d'_j\big)\Big)(y) \\
&= \Big(\big((f_j - f'_j) \circ d'_j\big) - \big(d_j \circ (s_j \circ d'_j)\big)\Big)(y) \\
&= \Big(\big((f_j - f'_j) \circ d'_j\big) - \big(d_j \circ (f_{j-1} - f'_{j-1} - (d_{j-1} \circ s_{j-1}))\big)\Big)(y) \\
&= \Big(\big((f_j - f'_j) \circ d'_j\big) - \big((d_j \circ (f_{j-1} - f'_{j-1})) - (d_j \circ (d_{j-1} \circ s_{j-1}))\big)\Big)(y) \\
&= \Big(\big((f_j - f'_j) \circ d'_j\big) - \big(d_j \circ (f_{j-1} - f'_{j-1})\big)\Big)(y) = 0
\end{aligned}$$

y por tanto $\overline{\big(f_j - f'_j - (d_j \circ s_j)\big)}(\overline{x}) = \big(f_j - f'_j - (d_j \circ s_j)\big)(x) = \big(f_j - f'_j - (d_j \circ s_j)\big)(x') = \overline{\big(f_j - f'_j - (d_j \circ s_j)\big)}(\overline{x'})$. Así, $\overline{\big(f_j - f'_j - (d_j \circ s_j)\big)}$ está bien definida.

El que $\overline{\big(f_j - f'_j - (d_j \circ s_j)\big)}$ sea un morfismo es porque $\big(f_j - f'_j - (d_j \circ s_j)\big)$ es un morfismo.

De esta forma tenemos que hay un morfismo $s_{i+1} : M_{i+1} \to E_i$ tal que $\overline{\big(f_j - f'_j - (d_j \circ s_j)\big)} = s_{i+1} \circ \overline{d'}_{j+1}$.

Sea $x \in M_i$, entonces $\big(f_j - f'_j - (d_j \circ s_j)\big)(x) = \overline{\big(f_j - f'_j - (d_j \circ s_j)\big)}(\overline{x}) = s_{i+1} \circ \overline{d'}_{j+1}(\overline{x}) = s_{i+1}(\overline{d'}_{j+1}(\overline{x})) = s_{i+1}(d'_{j+1}(x)) = (s_{i+1} \circ d'_{j+1})(x)$, o sea que, $f_j - f'_j = s_{i+1} \circ d'_{j+1} + d_j \circ s_j$. Por lo tanto, f y f' son homotópicas. $\square$

3.4. Funtores derivados

Consideremos ahora un funtor covariante $F : R\text{-}Mod \to S\text{-}Mod$ y sea N un R-módulo izquierdo. Sabemos que N tiene una resolución proyectiva, digamos

$$\mathcal{P} : \ \cdots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} N \longrightarrow 0.$$

Aplicando el funtor F al recortado $\mathcal{P}_N$ del complejo $\mathcal{P}$, obtenemos el complejo

$$F(\mathcal{P}_N) : \ \cdots \longrightarrow F(P_2) \xrightarrow{F(d_2)} F(P_1) \xrightarrow{F(d_1)} F(P_0) \longrightarrow 0$$

Para cada $n \in \mathbb{Z}$ definimos $L_nF : R\text{-}Mod \to Ab$ de la siguiente manera:

(1) En objetos: si $N \in Ob(R\text{-}Mod)$,

$$L_nF(N) := H_n(F(\mathcal{P}_N)) = \ker(F(d_n))/Im(F(d_{n+1})).$$

(2) En morfismos: si $\varphi : N \to T$ es un morfismo en $R\text{-}Mod$, entonces de 3.3.4 se sigue que hay una aplicación de cadenas $f : \mathcal{P}_N \to \mathcal{P}_T$ inducida por φ (con $\mathcal{P}_N = (\mathcal{P}_N, d)$ y $\mathcal{P}_T = (\mathcal{P}_T, d')$). Si $L_nF(\varphi) := H_n(F(f))$, donde $F(f) = (F(f_n))$, entonces el morfismo $L_nF(\varphi) : H_n(F(\mathcal{P}_N)) \to H_n(F(\mathcal{P}_T))$ es el que a $u_n + Im(F(d_{n+1}))$ le asocia $F(f_n)(u_n) + Im(F(d'_{n+1}))$.

Observaciones.

1. $L_nF(\varphi)$ no depende de la elección de la aplicación de cadenas sobre φ, ya que si tomamos otra aplicación de cadenas $f' : \mathcal{P}_N \to \mathcal{P}_T$ sobre φ, entonces las aplicaciones de cadenas sobre $F(\varphi)$, $F(f)$ y $F(f')$ son homotópicas, de acuerdo con 3.3.4. Luego, de 3.1.11 se sigue que $H_n(F(f)) = H_n(F(f'))$.

2. Como $L_nF(N) = 0$ para cada $N \in Ob(R\text{-}Mod)$ y cada $n < 0$, se sigue que si $\varphi : N \to T$ es un morfismo en $R\text{-}Mod$, entonces $L_nF(\varphi) = 0$ para cada $n < 0$.

Proposición 3.4.1 *$L_nF : R\text{-}Mod \to Ab$ es un funtor covariante.*

Demostración. Ya hemos definido la aplicación $L_nF : R\text{-}Mod \to Ab$ en objetos y en morfismos, así que sólo nos resta mostrar que preserva composiciones e identidades.

Sean $\varphi : N \to T$, $\psi : T \to U$ morfismos en $R\text{-}Mod$ y sean $f : \mathcal{P}_N \to \mathcal{P}_T$, $f' : \mathcal{P}_T \to \mathcal{P}_U$ aplicaciones de cadenas sobre φ y ψ, respectivamente. Entonces $f' \circ f : \mathcal{P}_N \to \mathcal{P}_U$ es una aplicación de cadenas sobre $\psi \circ \varphi$, y como F y H_n son funtores covariantes tenemos que $L_nF(\psi \circ \varphi) = H_n(F(f' \circ f)) = H_n(F(f') \circ F(f)) = H_n(F(f')) \circ H_n(F(f)) = L_nF(\psi) \circ L_nF(\varphi)$.

Ahora tomemos $N \in Ob(R\text{-}Mod)$. Como $1_{\mathcal{P}_N} : \mathcal{P}_N \to \mathcal{P}_N$ es una aplicación de cadenas sobre $1_N : N \to N$, y F y H_n son funtores covariantes se sigue que $L_nF(1_N) = H_n(F(1_{\mathcal{P}_N})) = H_n(1_{F(\mathcal{P}_N)}) = 1_{H_n(F(\mathcal{P}_N))} = 1_{L_nF(N)}$. □

Notemos que la definición de los funtores L_nF depende, hasta el momento, de la elección de la resolución proyectiva elegida de inicio para un R-módulo N. Pues al tomar otra resolución proyectiva para N, digamos

$$\mathcal{P}' : \cdots \longrightarrow P_2' \xrightarrow{d_2'} P_1' \xrightarrow{d_1'} P_0' \xrightarrow{d_0'} N \longrightarrow 0$$

tendríamos otra familia de funtores $L_n'F$.

Proposición 3.4.2 *Los funtores L_nF y $L_n'F$ son naturalmente isomorfos.*

Demostración. Debemos probar que existe $(L_nF, \eta, L_n'F)$, transformación natural, tal que para cada $N \in Ob(R\text{-}Mod)$, η_N es un isomorfismo en Ab.

Consideremos el diagrama

$$\begin{tikzcd}
\mathcal{P} : \cdots \arrow[r] & P_2 \arrow[r, "d_2"] \arrow[d, dotted, "f_2"'] & P_1 \arrow[r, "d_1"] \arrow[d, dotted, "f_1"'] & P_0 \arrow[r, "d_0"] \arrow[d, dotted, "f_0"'] & N \arrow[r] \arrow[d, "1_N"] & 0 \\
\mathcal{P}' : \cdots \arrow[r] & P_2' \arrow[r, "d_2'"] \arrow[d, dotted, "f_2'"'] & P_1' \arrow[r, "d_1'"] \arrow[d, dotted, "f_1'"'] & P_0' \arrow[r, "d_0'"] \arrow[d, dotted, "f_0'"'] & N \arrow[r] \arrow[d, "1_N"] & 0 \\
\mathcal{P} : \cdots \arrow[r] & P_2 \arrow[r, "d_2"] & P_1 \arrow[r, "d_1"] & P_0 \arrow[r, "d_0"] & N \arrow[r] & 0,
\end{tikzcd}$$

donde $\mathcal{P}$ y $\mathcal{P}'$ son las resoluciones proyectivas sobre N que definen respectivamente a los funtores L_nF y $L_n'F$. Entonces existen aplicaciones de cadenas $f : \mathcal{P}_N \to \mathcal{P}_N'$ y $f' : \mathcal{P}_N' \to \mathcal{P}_N$ inducidas por 1_N. Entonces $f' \circ f$ y $f \circ f'$ son aplicaciones de cadenas sobre 1_N. Luego, $F(f' \circ f)$, $F(1_{\mathcal{P}_N})$, $F(f \circ f')$ y $F(1_{\mathcal{P}_N'})$ son aplicaciones de cadenas sobre $F(1_N)$. De 3.3.4 tenemos que $F(f' \circ f)$ es homotópica a $F(1_{\mathcal{P}_N})$, y $F(f \circ f')$ es homotópica a $F(1_{\mathcal{P}_N'})$. Además, 3.1.11 garantiza que $H_n(F(f' \circ f)) = H_n(F(1_{\mathcal{P}_N}))$ y $H_n(F(f \circ f')) = H_n(F(1_{\mathcal{P}_N'}))$. Pero F y H_n son covariantes, entonces

$$H_n(F(f')) \circ H_n(F(f)) = H_n(F(1_{\mathcal{P}_N})) \text{ y } H_n(F(f)) \circ H_n(F(f')) = H_n(1_{F(\mathcal{P}_N')}).$$

O sea que $H_n(F(f)) : H_n(F(\mathcal{P}_N)) \to H_n(F(\mathcal{P}_N'))$ es un isomorfismo. Así, tomamos $\eta_N = H_n(F(f)) : L_nF(N) \to L_n'F(N)$.

Finalmente, veamos que si $\varphi : N \to T$ es un morfismo en R-Mod, entonces el diagrama

$$\begin{tikzcd}
L_nF(N) \arrow[r, "\eta_N"] \arrow[d, "L_nF(\varphi)"'] & L_n'F(N) \arrow[d, "L_n'F(\varphi)"] \\
L_nF(T) \arrow[r, "\eta_T"'] & L_n'F(T)
\end{tikzcd}$$

conmuta.

Sean $\mathcal{P}$ y $\mathcal{P}'$ dos resoluciones proyectivas sobre N y sean $\mathcal{Q}$ y $\mathcal{Q}'$ dos resoluciones proyectivas sobre T. Entonces existen $f : \mathcal{P}_N \to \mathcal{P}'_N$ y $g : \mathcal{Q}_T \to \mathcal{Q}'_T$ aplicaciones de cadenas sobre 1_N y 1_T, respectivamente. También tenemos que existen $h : \mathcal{P}_N \to \mathcal{Q}_T$ y $h' : \mathcal{P}'_N \to \mathcal{Q}'_T$ aplicaciones de cadenas sobre φ. Entonces $g \circ h$ y $h' \circ f$ son aplicaciones de cadenas sobre φ. Aplicando el funtor F tenemos que $F(g \circ h)$ y $F(h' \circ f)$ son aplicaciones de cadenas sobre $F(\varphi)$. Entonces por 3.3.4, $F(g \circ h)$ y $F(h' \circ f)$ son homotópicas y por 3.1.11 tenemos que $H_n(F(g \circ h)) = H_n(F(h' \circ f))$. Luego, de la forma en que se definió η_N y por ser F y H_n covariantes tenemos que

$$\eta_T \circ L_n F(\varphi) = H_n(F(g)) \circ H_n(F(h)) = H_n(F(h')) \circ H_n(F(f)) = L'_n F(\varphi) \circ \eta_N.$$

□

Definición 3.4.3 *Al funtor L_nF se le denomina **n-ésimo funtor derivado izquierdo** de F.*

Proposición 3.4.4 *Si $F : R\text{-}Mod \to S\text{-}Mod$ es un funtor covariante aditivo, entonces el funtor covariante $L_nF : R\text{-}Mod \to Ab$ es aditivo.*

Demostración. Sean $\varphi,\ \psi : N \to T$ morfismos en R-Mod, entonces existen $\mathcal{P}$ y $\mathcal{Q}$ resoluciones proyectivas para N y T, respectivamente. Luego existen $f,\ g : \mathcal{P}_N \to \mathcal{Q}_T$ aplicaciones de cadenas sobre φ y ψ, respectivamente. Como $f + g$ es una aplicación de cadenas sobre $\varphi + \psi$, se sigue que $L_nF(\varphi + \psi) = H_n(F(f + g)) = H_n(F(f)) + H_n(F(g)) = L_nF(\varphi) + L_nF(\psi)$. □

Definición 3.4.5 *Si $F = M \otimes_R \_$, entonces para cada $n \in \mathbb{Z}$, $Tor_n^R(M, \_) := L_nF$. A la familia de funtores $(Tor_n^R(M, \_))_{n\in\mathbb{Z}}$ se le denomina **funtor Tor** con respecto a M.*

Consideremos ahora un funtor covariante $F : R\text{-}Mod \to S\text{-}Mod$ y sea N un R-módulo izquierdo. Sabemos que N tiene una resolución inyectiva, digamos

$$\mathcal{E} :\ 0 \longrightarrow N \longrightarrow E_0 \xrightarrow{d_0} E_{-1} \xrightarrow{d_{-1}} E_{-2} \longrightarrow \cdots .$$

Aplicando el funtor F al recortado $\mathcal{E}_N$ del complejo $\mathcal{E}$, obtenemos el complejo

$$F(\mathcal{E}_N) :\ 0 \longrightarrow F(E_0) \xrightarrow{F(d_0)} F(E_{-1}) \xrightarrow{F(d_{-1})} F(E_{-2}) \longrightarrow \cdots .$$

Para cada $n \in \mathbb{Z}$ definimos la aplicación $R^nF : R\text{-}Mod \to Ab$ de la siguiente manera:

(1) En objetos: si $N \in Ob(R\text{-}Mod)$.

$$R^nF(N) := H_{-n}(F(\mathcal{E}_N)) = \ker(F(d_{-n}))/Im(F(d_{-n+1})).$$

(2) En morfismos: si $\varphi : N \to T$ es un morfismo en R-Mod, entonces de 3.3.5 se sigue que hay una aplicación de cadenas $f : \mathcal{E}_N \to \mathcal{E}_T$ inducida por φ (con $\mathcal{E}_N = (\mathcal{E}_N, d)$ y $\mathcal{E}_T = (\mathcal{E}_T, d'))$. Si $R^nF(\varphi) := H_{-n}(F(f))$, donde $F(f) = \{F(f_{-n})\}$, entonces el morfismo $R^nF(\varphi) : H_{-n}(F(\mathcal{E}_N)) \to H_{-n}(F(\mathcal{E}_T))$ es el que a $u_{-n} + Im(F(d_{-n+1}))$ le asocia $F(f_{-n})(u_{-n}) + Im(F(d'_{-n+1}))$.

Observaciones.

1. $R^nF(\varphi)$ no depende de la elección de la aplicación de cadenas sobre φ.

2. Como $R^nF(N) = 0$ para cada $N \in Ob(R\text{-}Mod)$ y cada $n < 0$, se sigue que si $\varphi : N \to T$ es un morfismo en R-Mod, entonces $R^nF(\varphi) = 0$ para cada $n < 0$.

Proposición 3.4.6 *$R^nF : R\text{-}Mod \to Ab$ es un funtor covariante.*

Demostración. Es análoga a la prueba de 3.4.1. □

Notemos que la definición de los funtores R^nF depende, hasta aquí, de la elección de la resolución inyectiva elegida de inicio para un R-módulo N. Pues al tomar otra resolución inyectiva para N, digamos

$$\mathcal{E}' :\ 0 \longrightarrow N \longrightarrow E'_0 \xrightarrow{d_0} E'_{-1} \xrightarrow{d_{-1}} E_{-2} \longrightarrow \cdots$$

tendríamos otra familia de funtores R'^nF.

Proposición 3.4.7 *Los funtores R^nF y R'^nF son naturalmente isomorfos.*

Demostración. Es similar a la prueba en 3.4.2, teniendo en cuenta que se utiliza 3.3.5. □

Definición 3.4.8 *Al funtor R^nF se le denomina **n-ésimo funtor derivado derecho** de F.*

Proposición 3.4.9 *Si $F : R\text{-}Mod \to S\text{-}Mod$ es un funtor covariante aditivo, entonces el funtor covariante $R^nF : R\text{-}Mod \to Ab$ es aditivo.*

Demostración. Es análoga a la prueba de 3.4.4. □

Definición 3.4.10 *Si $F = Hom_R(M, \_)$, entonces para cada n, $Ext^n_R(M, \_) := R^nF$. A la familia de funtores $Ext^n_R(M, \_)$ se le denomina **funtor Ext** (covariante) con respecto a M.*

Ejemplos.

1. Sean R un anillo, M un R-módulo y x un elemento en R que no es divisor de cero. Entonces

$$0 \longrightarrow R \xrightarrow{x} R \longrightarrow R/\langle x\rangle \longrightarrow 0$$

es una resolución proyectiva de $R/\langle x\rangle$. Aplicando el funtor $\_\otimes M$ al complejo recortado de $R/\langle x\rangle$ obtenemos el complejo

$$0 \longrightarrow R\otimes_R M \xrightarrow{x\otimes 1} R\otimes_R M \longrightarrow 0,$$

el cual vía los isomorfismos $R\otimes_R M\cong M$ y $R/\langle x\rangle\otimes_R M\cong M/\langle x\rangle M$ es isomorfo al complejo

$$0\longrightarrow M\xrightarrow{x} M\longrightarrow 0.$$

De este modo tenemos que $Tor_0^R(R/\mathfrak{m},M)=M/\langle x\rangle M$, $Tor_1^R(R/\mathfrak{m},M)=\{m\in M : xm=0\}$ y para cualquier otro n, $Tor_n^R(R/\mathfrak{m},M)=0$.

2. Si ahora aplicamos el funtor $Hom_R(\_,M)$ al complejo recortado de $R/\langle x\rangle$ de 1, obtenemos el complejo

$$0\longrightarrow Hom_R(R,M)\xrightarrow{x_*} Hom_R(R,M)\longrightarrow 0,$$

que es isomorfo al complejo

$$0\longrightarrow M\xrightarrow{x} M\longrightarrow 0,$$

ya que $Hom_R(R,M)\cong M$ y x_* es sólo multiplicación por x (pues si $f\in Hom_R(R,M)$, entonces para cada $r\in R$, $x_*(f)(r)=f(xr)=xf(r)$). Al tomar la homología de este complejo obtenemos que $Ext_R^0(R/\langle x\rangle,M)\cong\{m\in M : xm=0\}$, $Ext_R^1(R/\langle x\rangle,M)\cong M/\langle x\rangle M$ y para todos los demás i, $Ext_R^i(R/\langle x\rangle,M)=0$.

A continuación enunciamos algunas propiedades que involucran al funtor Ext y que utilizaremos en el siguiente capítulo. En [10] se pueden encontrar más propiedades para Ext y sus correspondientes duales para Tor.

Proposición 3.4.11 *Consideremos el diagrama*

$$\begin{tikzcd}
 & 0 \arrow[d] & & 0 \arrow[d] & \\
0 \arrow[r] & M \arrow[r, "\mu"] \arrow[d, "\varphi'"'] & N \arrow[r, "\pi"] & T \arrow[r] \arrow[d, "\varphi''"] & 0 \\
 & E'_0 \arrow[d, "d'_0"'] & & E''_0 \arrow[d, "d''_0"] & \\
 & E'_{-1} \arrow[d, "d'_{-1}"'] & & E''_{-1} \arrow[d, "d''_{-1}"] & \\
 & \vdots & & \vdots &
\end{tikzcd}$$

con fila exacta y donde las columnas son resoluciones inyectivas de M y T, respectivamente. Entonces hay una resolución inyectiva de N y aplicaciones de cadenas tales que las columnas forman una sucesión exacta de complejos.

Demostración. Para cada $n \in \mathbb{N}_{-} \cup \{0\}$, hacemos $E_n = E'_n \oplus E''_n$. Sean $\mu : E'_n \to E_n$ y $\pi_n : E_n \to E''_n$ la inclusión y la proyección, respectivamente, entonces para cada $n \in \mathbb{N}_{-} \cup \{0\}$, la sucesión

$$\begin{tikzcd} 0 \arrow[r] & E'_n \arrow[r, "\mu_n"] & E_n \arrow[r, "\pi_n"] & E''_n \arrow[r] & 0 \end{tikzcd}$$

es exacta. En este caso, el producto y la suma directa coinciden, y como E'_n y E''_n son inyectivos se sigue que E_n es inyectivo.

Falta definir a los morfismos $\varphi : N \to E_0$ y $d_n : E_n \to E_{n-1}$ para cada $n \leq 0$.

Fijémonos en el diagrama siguiente:

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "\varphi'"] & E'_0 \arrow[r, "d'_0"] & E'_{-1} \arrow[r, "d'_{-1}"] & E'_{-2} \arrow[r, "d'_{-2}"] & \cdots \\ 0 \arrow[r] & M \arrow[r, "\mu"'] \arrow[u, "1_M"] & N \arrow[r, "-(\varphi'' \circ \pi)"'] \arrow[u, dotted, "f_0"] & E''_0 \arrow[r, "-d''_0"'] \arrow[u, dotted, "f_{-1}"] & E''_{-1} \arrow[r, "-d''_{-1}"'] \arrow[u, dotted, "f_{-2}"] & \cdots . \end{tikzcd}$$

Se comprueba fácilmente que la fila inferior en tal diagrama es exacta. Entonces hay una aplicación de cadenas $f = (f_n)$ de la fila inferior en la fila superior inducida por 1_M, que hace que los cuadrados en el diagrama conmuten.

Definimos los morfismos $\varphi : N \to E_0$ por $\varphi(x) = (f_0(x), (\varphi'' \circ \pi)(x))$, y para cada $n \leq 0$, $d_n : E_n \to E_{n-1}$ por $d_n(u, v) = (d'_n(u) + f_{n-1}(v), d''_n(v))$. Notemos que φ y los d_n son morfismos porque están definidas en términos de otros morfismos. Y así obtenemos el diagrama

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & M \arrow[r, "\mu"] \arrow[d, "\varphi'"'] & N \arrow[r, "\pi"] \arrow[d, "\varphi"'] & T \arrow[r] \arrow[d, "\varphi''"] & 0 \\
0 \arrow[r] & E'_0 \arrow[r, "\mu_0"] \arrow[d, "d'_0"'] & E_0 \arrow[r, "\pi_0"] \arrow[d, "d_0"'] & E''_0 \arrow[r] \arrow[d, "d''_0"] & 0 \\
0 \arrow[r] & E'_{-1} \arrow[r, "\mu_{-1}"] \arrow[d, "d'_{-1}"'] & E_{-1} \arrow[r, "\pi_{-1}"] \arrow[d, "d_{-1}"'] & E''_{-1} \arrow[r] \arrow[d, "d''_{-1}"] & 0 \\
 & \vdots & \vdots & \vdots & .
\end{tikzcd}$$

Veamos que la columna central es un complejo.

φ es inyectiva, pues si $x \in \ker(\varphi)$, $0 = \varphi(x) = \big(f_0(x), (\varphi'' \circ \pi)(x)\big)$, esto es, $x \in \ker(f_0)$ y $\pi(x) \in \ker(\varphi'') = 0$. Luego $x \in \ker(\pi) = Im(\mu)$, es decir, $x = \mu(m)$ para algún $m \in M$. Por tanto $0 = f_0(x) = f_0(\mu(m)) = \varphi'(1_M(m)) = \varphi'(m)$, lo cual nos dice que $m \in \ker(\varphi') = 0$, o sea que, $x = \mu(m) = \mu(0) = 0$.

$d_0 \circ \varphi = 0$, ya que al tomar un $x \in N$, $(d_0 \circ \varphi)(x) = d_0(\varphi(x)) = d_0\big(f_0(x), (\varphi'' \circ \pi)(x)\big) = \big(d'_0(f_0(x)) + f_{-1}((\varphi'' \circ \pi)(x)), d''_0((\varphi'' \circ \pi)(x))\big) = \big(f_{-1}((-(\varphi'' \circ \pi))(x)) + f_{-1}((\varphi'' \circ \pi)(x)), 0\big) = 0$.

$d_{n-1} \circ d_n = 0$ para $n < 0$, porque si $(u, v) \in E_n$, entonces $(d_{n-1} \circ d_n)(u, v) = d_{n-1}(d_n(u, v)) = d_{n-1}\big(d'_n(u) + f_{n-1}(v), d''_n(v)\big)$
$= \big(d'_{n-1}(d'_n(u) + f_{n-1}(v)) + f_{n-2}(d''_n(v)), d''_{n-1}(d''_n(v))\big)$
$= \big(d'_{n-1}(d'_n(u)) + d'_{n-1}(f_{n-1}(v)) + f_{n-2}(d''_n(v)), 0\big)$
$= \big(f_{n-2}(-d''_n(v)) + f_{n-2}(d''_n(v)), 0\big) = 0$.

Ahora verifiquemos que los cuadrados del diagrama conmutan.

Si $m \in M$, entonces $(\varphi \circ \mu)(m) = \varphi(\mu(m)) = \big(f_0(\mu(m)), (\varphi'' \circ \pi)(\mu(m))\big) = \big(\varphi'(1_M(m)), 0\big) = (\varphi'(m), 0) = \mu_0(\varphi'(m)) = (\mu_0 \circ \varphi')(m)$. Luego $\varphi \circ \mu = \mu_0 \circ \varphi'$.

Si $x \in N$, $(\pi_0 \circ \varphi)(x) = \pi_0(\varphi(x)) = \pi_0\big(f_0(x), (\varphi'' \circ \pi)(x)\big) = (\varphi'' \circ \pi)(x)$. Entonces $\pi_0 \circ \varphi = \varphi'' \circ \pi$.

Si $x \in E'_n$, $(d_n \circ \mu_n)(x) = d_n(\mu_n(x)) = d_n(x, 0) = \big(d'_n(x) + f_{n-1}(0), d''_n(0)\big) = (d'_n(x), 0) = \mu_{n-1}(d'_n(x)) = (\mu \circ d'_n)(x)$. Con lo cual tenemos que para cada $n \leq 0$, $d_n \circ \mu_n = \mu \circ d'_n$.

Supongamos que $(x, y) \in E_n$, entonces $(\pi_{n-1} \circ d_n)(x, y) = \pi_{n-1}(d_n(x, y)) = \pi_{n-1}(d'_n(x) + f_{n-1}(y), d''_n(y)) = d''_n((y)) = d''_n(\pi_n(x, y)) = (d''_n \circ \pi_n)(x, y)$. Por lo tanto, $d''_n \circ \pi_n = \pi_{n-1} \circ d_n$.

Finalmente veamos que la columna central en el diagrama es exacta. Denotamos con $\mathcal{E}'$, $\mathcal{E}$ y $\mathcal{E}''$ a los complejos asociados con M, N y T, respectivamente. Como $\mathcal{E}'$ y $\mathcal{E}''$ son resoluciones inyectivas, tenemos que

$$0 \longrightarrow \mathcal{E}' \longrightarrow \mathcal{E} \longrightarrow \mathcal{E}'' \longrightarrow 0$$

es una sucesión exacta corta de complejos, la cual induce una sucesión exacta de mapeos en Ab

$$\begin{tikzcd}
\cdots \arrow[r] & H_n(\mathcal{E}') \arrow[r] & H_n(\mathcal{E}) \arrow[r] & H_n(\mathcal{E}'') \arrow[dll, "\delta_n"] \\
& H_{n-1}(\mathcal{E}') \arrow[r] & H_{n-1}(\mathcal{E}) \arrow[r] & H_{n-1}(\mathcal{E}'') \arrow[r] & \cdots .
\end{tikzcd}$$

Sabemos que $\mathcal{E}'$ y $\mathcal{E}''$ son complejos exactos; por lo cual, $H_n(\mathcal{E}') = 0$ y $H_n(\mathcal{E}'') = 0$ para cada $n \leq 0$, entonces $H_n(\mathcal{E}) = 0$ para cada $n \leq 0$. De este modo, $Im(\varphi) = \ker(d_0)$ e $Im(d_n) = \ker(d_{n-1})$ para cada $n \leq 0$. Con lo cual tenemos que $\mathcal{E}$ es la resolución inyectiva que buscamos. $\square$

Proposición 3.4.12 *Sea M un R-módulo. Entonces para cada R-módulo N, $Ext^0_R(M, N) \cong Hom_R(M, N)$.*

Demostración. Sea $0 \longrightarrow N \xrightarrow{\varphi} E_0 \xrightarrow{d_0} E_{-1} \xrightarrow{d_{-1}} \cdots$ una resolución inyectiva de un R-módulo dado N. Como el funtor covariante $F = Hom_R(M, \_)$ es exacto izquierdo, la sucesión

$$0 \longrightarrow Hom_R(M, N) \xrightarrow{F(\varphi)} Hom_R(M, E_0) \xrightarrow{F(d_0)} Hom_R(M, E_{-1})$$

es exacta. Entonces, $Ext^0_R(M, N) = \ker(F(d_0))/Im(f(d_1)) = \ker(F(d_0))/0 = \ker(F(d_0)) = Im(F(\varphi)) \cong Hom_R(M, N)$. $\square$

Proposición 3.4.13 *Si $0 \longrightarrow N \xrightarrow{\mu} T \xrightarrow{\pi} U \longrightarrow 0$ es una sucesión exacta corta de R-módulos, entonces para cada R-módulo M existe una sucesión exacta larga*

$$
\begin{tikzcd}
0 \arrow[r] & Hom_R(M,N) \arrow[r] & Hom_R(M,T) \arrow[r] & Hom_R(M,U) \arrow[dlll, rounded corners, "\delta_0"] & \\
 Ext^1_R(M,N) \arrow[r] & Ext^1_R(M,T) \arrow[r] & Ext^1_R(M,U) \arrow[r] & \cdots .
\end{tikzcd}
$$

Demostración. Sean

$$\mathcal{E}': \ 0 \longrightarrow N \longrightarrow E'_0 \longrightarrow E'_{-1} \longrightarrow \cdots$$

$$\mathcal{E}'': \ 0 \longrightarrow U \longrightarrow E''_0 \longrightarrow E''_{-1} \longrightarrow \cdots$$

resoluciones inyectivas de N y U, respectivamente. Entonces de 3.4.11 se sigue que hay una resolución inyectiva de T,

$$\mathcal{E}: \ 0 \longrightarrow T \longrightarrow E_0 \longrightarrow E_{-1} \longrightarrow \cdots$$

tal que

$$0 \longrightarrow \mathcal{E}' \longrightarrow \mathcal{E} \longrightarrow \mathcal{E}'' \longrightarrow 0$$

es una sucesión exacta corta de complejos, o sea que para cada n,

$$0 \longrightarrow E'_n \xrightarrow{\mu_n} E_n \xrightarrow{\pi_n} E''_n \longrightarrow 0$$

es una sucesión exacta corta. Como E'_n es inyectivo, μ_n es una sección, o sea que esta sucesión exacta se divide. Luego, por ser $F = Hom_R(M,\_\,)$ un funtor covariante aditivo, la proposición 2.1.17 garantiza que para cada n, la sucesión

$$0 \longrightarrow F(E'_n) \longrightarrow F(E_n) \longrightarrow F(E''_n) \longrightarrow 0$$

es exacta y se divide. De esta forma, la sucesión de complejos

$$0 \longrightarrow F(\mathcal{E}'_N) \longrightarrow F(\mathcal{E}_T) \longrightarrow F(\mathcal{E}''_U) \longrightarrow 0$$

es exacta. Entonces por 3.2.2, existe una sucesión exacta larga

$$
\begin{tikzcd}
\cdots \arrow[r] & H_{-n}(F(\mathcal{E}'_N)) \arrow[r] & H_{-n}(F(\mathcal{E}_T)) \arrow[r] & H_{-n}(F(\mathcal{E}''_U)) \arrow[dll, rounded corners, "\delta_{-n}"] & \\
 & H_{-n-1}(F(\mathcal{E}'_N)) \arrow[r] & H_{-n-1}(F(\mathcal{E}_T)) \arrow[r] & H_{-n-1}(F(\mathcal{E}''_U)) \arrow[r] & \cdots .
\end{tikzcd}
$$

Luego, por la definición de los $Ext^n_R(M,\_\,)$ tenemos la sucesión exacta larga

$$\begin{tikzcd}
\cdots \arrow[r] & Ext^n_R(M,N) \arrow[r] & Ext^n_R(M,T) \arrow[r] & Ext^n_R(M,U) \arrow[dll, "\delta_n"] \\
& Ext^{n+1}_R(M,N) \arrow[r] & Ext^{n+1}_R(M,T) \arrow[r] & Ext^{n+1}_R(M,U) \arrow[r] & \cdots,
\end{tikzcd}$$

la cual inicia en cero porque para cada $n < 0$, $Ext^n_R(M,\_\,) = 0$. Además $Ext^0_R(M,N) \cong Hom_R(M,N)$, análogamente $Ext^0_R(M,T)$ y $Ext^0_R(M,U)$. $\square$

Proposición 3.4.14 *Sea R un anillo conmutativo con identidad. Si $\mu : N \to N$ es multiplicación por $r \in R$, entonces $\mu^* : Ext^n_R(M,N) \to Ext^n_R(M,N)$ es multiplicación por r.*

Demostración. Sea $0 \longrightarrow N \xrightarrow{\varphi} E_0 \xrightarrow{d_0} E_{-1} \xrightarrow{d_{-1}} \cdots$ una resolución inyectiva de N. Si para cada n definimos $f_n : E_n \to E_n$ como multiplicación por r, obtenemos el diagrama conmutativo

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r, "\varphi"] \arrow[d, "\mu"] & E_0 \arrow[r, "d_0"] \arrow[d, "f_0"] & E_{-1} \arrow[r, "d_{-1}"] \arrow[d, "f_{-1}"] & \cdots \\
0 \arrow[r] & N \arrow[r, "\varphi"] & E_0 \arrow[r, "d_0"] & E_{-1} \arrow[r, "d_{-1}"] & \cdots .
\end{tikzcd}$$

Así, $f = (f_n)$ es una aplicación de cadenas sobre μ. Aplicando $Hom_R(M,\_\,)$ al diagrama anterior se tiene el siguiente diagrama conmutativo:

$$\begin{tikzcd}
0 \arrow[r] & Hom_R(M,N) \arrow[r, "\varphi^*"] \arrow[d, "\mu^*"] & Hom_R(M,E_0) \arrow[r, "d_0^*"] \arrow[d, "f_0^*"] & Hom_R(M,E_{-1}) \arrow[r, "d_{-1}^*"] \arrow[d, "f_{-1}^*"] & \cdots \\
0 \arrow[r] & Hom_R(M,N) \arrow[r, "\varphi^*"] & Hom_R(M,E_0) \arrow[r, "d_0^*"] & Hom_R(M,E_{-1}) \arrow[r, "d_{-1}^*"] & \cdots .
\end{tikzcd}$$

Como $Ext^n_R(M,\mu)$ no depende de la aplicación de cadenas sobre μ, entonces $\mu^* : Ext^n_R(M,N) \to Ext^n_R(M,N)$ se define por $z_{-n} + Im(d^*_{-n+1}) \mapsto (f^*_{-n})(z_{-n}) + Im(d^*_{-n+1})$. Pero $(f^*_{-n})(z_{-n})(x) = (f_{-n} \circ z_{-n})(x) = f_{-n}(z_{-n}(x)) = r(z_{-n}(x))$ para cada $x \in M$, es decir, $(f^*_n)(z_{-n}) = rz_{-n}$. De este modo μ^* está definido por $z_{-n} + Im(d^*_{-n+1}) \mapsto rz_{-n} + Im(d^*_{-n+1}) = r(z_{-n} + Im(d^*_{-n+1}))$, esto es, μ^* es multiplicación por r. $\square$

Definición 3.4.15 *Sean*

$$\mathcal{M} : \quad \cdots \longrightarrow M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \longrightarrow \cdots$$

$$\mathcal{N} : \quad \cdots \longrightarrow N_{i+1} \xrightarrow[d'_{i+1}]{} N_i \xrightarrow[d'_i]{} N_{i-1} \longrightarrow \cdots$$

dos complejos. La ***suma directa*** *de $\mathcal{M}$ y $\mathcal{N}$ es el complejo*

$$\mathcal{M}\oplus\mathcal{N}\colon \cdots \longrightarrow M_{i+1}\oplus N_{i+1} \xrightarrow{(d_{n+1},\,d'_{n+1})} M_i\oplus N_i \xrightarrow{(d_n,\,d'_n)} M_{i-1}\oplus N_{i-1} \longrightarrow \cdots .$$

Observación. Se verifica directamente que $\mathcal{M}\oplus\mathcal{N}$ es un complejo y que $H_n(\mathcal{M}\oplus\mathcal{N}) = H_n(\mathcal{M})\oplus H_n(\mathcal{N})$.

Proposición 3.4.16 *Para cada $n \geq 0$ y módulos $M, N_1, \ldots, N_r$ sobre un anillo R, $Ext^n_R(M, \bigoplus_{i=1}^r N_i) \cong \bigoplus_{i=1}^r Ext^n_R(M, N_i)$.*

Demostración. La prueba es por inducción, pero sólo mostraremos el caso base $n = 2$, ya que este es el paso importante en la demostración.

Sea $\mathcal{P} : \cdots \longrightarrow P_1 \xrightarrow{d_1} P_0 \longrightarrow M \longrightarrow 0$ una resolución proyectiva de M. Aplicando los funtores $Hom_R(\_, N_1)$ y $Hom_R(\_, N_2)$ al complejo recortado $\mathcal{P}_M$ obtenemos los complejos

$$Hom_R(\mathcal{P}_M, N_1) : \ 0 \longrightarrow Hom_R(P_0, N_1) \longrightarrow Hom_R(P_1, N_1) \longrightarrow Hom_R(P_2, N_1) \longrightarrow \cdots$$

$$Hom_R(\mathcal{P}_M, N_2) : \ 0 \longrightarrow Hom_R(P_0, N_2) \longrightarrow Hom_R(P_1, N_2) \longrightarrow Hom_R(P_2, N_2) \longrightarrow \cdots$$

y podemos definir el complejo $Hom_R(\mathcal{P}_M, N_1) \oplus Hom_R(\mathcal{P}_M, N_2)$ como sigue:

$$\begin{aligned} &\big(Hom_R(\mathcal{P}_M, N_1) \oplus Hom_R(\mathcal{P}_M, N_2)\big)_{-n} \\ &= \big(Hom_R(\mathcal{P}_M, N_1)\big)_{-n} \oplus \big(Hom_R(\mathcal{P}_M, N_2)\big)_{-n} \\ &= Hom_R(P_n, N_1) \oplus Hom_R(P_n, N_2) \cong Hom_R(P_n, N_1 \oplus N_2). \end{aligned}$$

Entonces $Ext^n_R(M, N_1 \oplus N_2) = H_{-n}\big(Hom_R(\mathcal{P}_M, N_1) \oplus Hom_R(\mathcal{P}_M, N_2)\big) = H_{-n}\big(Hom_R(\mathcal{P}_M, N_1)\big) \oplus H_{-n}\big(Hom_R(\mathcal{P}_M, N_2)\big) = Ext^n_R(M, N_1) \oplus Ext^n_R(M, N_2)$.
□

3.5. Dimensión proyectiva

Definición 3.5.1 *La* ***dimensión proyectiva*** *o* ***dimensión homológica*** *de un R-módulo M, denotada por $\mathrm{pd}_R(M)$, es el menor entero no negativo n para el cual hay una resolución proyectiva de M de longitud n. Si tal entero no existe, la dimensión se define como ∞.*

Proposición 3.5.2 *$pd_R(M) = 0$ si y sólo si M es proyectivo.*

Demostración. Si $0 \longrightarrow X_0 \longrightarrow M \longrightarrow 0$ es una resolución proyectiva de M, entonces $M \cong X_0$, así M es proyectivo. Recíprocamente, si M es proyectivo, entonces $0 \longrightarrow X_0 = M \longrightarrow M \longrightarrow 0$ es una resolución proyectiva de M, donde el endomorfismo en M es la identidad. □

Si en lugar de empezar una resolución libre de un módulo M seleccionando un conjunto arbitrario de generadores de M, parece razonable el escoger un conjunto minimal de generadores, obteniendo de esta forma un morfismo "minimal" de un módulo libre F a M. Podemos continuar eligiendo ahora un conjunto minimal de generadores para el kernel, y así sucesivamente, y de esta forma conseguir una resolución libre "minimal". Sin embargo, esta idea no es útil en general, ya que los conjuntos generadores minimales no tienen propiedades de unicidad (por ejemplo, en los enteros, $\langle 5\rangle = \langle 10, 15\rangle$). Pero sobre un anillo local, donde el lema de Nakayama hace más accesible la noción de un conjunto minimal de generadores, deja ver que cada módulo sobre un anillo local tiene una única resolución libre "minimal".

Definición 3.5.3 *Un complejo de R-módulos*

$$\mathcal{M}: \quad \cdots \longrightarrow M_{n+1} \xrightarrow{d_{n+1}} M_n \xrightarrow{d_n} M_{n-1} \longrightarrow \cdots$$

*sobre un anillo local $(R,\mathfrak{m})$, es **minimal** si para cada n, $d_n(M_n) \subseteq \mathfrak{m}M_{n-1}$.*

Observaciones.

1. La condición de que $d_n(M_n) \subseteq \mathfrak{m}M_{n-1}$ es equivalente a que los morfismos en el complejo $(R/\mathfrak{m}) \otimes \mathcal{M}$ son todos cero. En efecto, pues para cada n, el morfismo

$$M_n/\mathfrak{m}M_n \cong (R/\mathfrak{m}) \otimes_R M_n \stackrel{1\otimes d_n}{\longrightarrow} (R/\mathfrak{m}) \otimes_R M_{n-1} \cong M_{n-1}/\mathfrak{m}M_{n-1}$$

   asocia a $\overline{x} \in M_n/\mathfrak{m}M_n$ con $\overline{d_n(x)} = 0$.

2. Si los módulos en el complejo son libres y de rango finito, los morfismos d_n pueden representarse por matrices sobre R y la minimalidad indica que las entradas de tales matrices están contenidas en $\mathfrak{m}$.

Proposición 3.5.4 *Sean $(R,\mathfrak{m})$ un anillo local noetheriano y M un R-módulo finitamente generado. entonces M tiene una resolución libre minimal.*

Demostración. Como $(R,\mathfrak{m})$ es local y M es finitamente generado, se sigue que $M/\mathfrak{m}M$ es un $R/\mathfrak{m}$-espacio vectorial de dimensión finita. Sea $\{\overline{m}_1, \ldots, \overline{m}_n\}$ una base para $M/\mathfrak{m}M \cong (R/\mathfrak{m})\otimes_R M$ sobre $R/\mathfrak{m}$, entonces $\{m_1, \ldots, m_n\}$ es un conjunto minimal de generadores para M. Así, podemos definir un epimorfismo $\varphi_0 : R^n \to M$ por $\varphi(e_i) = m_i$, donde $e_1, \ldots, e_n$ es la base canónica de R^n. De este modo obtenemos la sucesión exacta:

$$0 \longrightarrow \ker(\varphi_0) \xrightarrow{i} R^n \xrightarrow{\varphi_0} M \longrightarrow 0.$$

Por otro lado tenemos que si $x \in \ker(\varphi_0)$, entonces hay una única expresión para x de la forma $\sum_{i=1}^n r_i e_i$, donde los $r_i \in R$ y $0 = \varphi_0(x) = \sum_{i=1}^n r_i\varphi_0(e_i) = \sum_{i=1}^n r_i m_i \in \mathfrak{m}M$, entonces los $r_i \in \mathfrak{m}$ y por lo tanto, $x = \sum_{i=1}^n r_i e_i \in \mathfrak{m}R^n$,o sea que $\ker(\varphi_0) \subseteq \mathfrak{m}R^n$.

Esta construcción junto con la que se hizo para probar que todo R-módulo tiene una resolución libre nos permite concluir que M tiene una resolución libre minimal. □

Teorema 3.5.5 *Si* $(R, \mathfrak{m})$ *es un anillo local noetheriano y* M *un* R*-módulo no cero finitamente generado, entonces cualquier resolución libre minimal de* M *tiene longitud igual a* $pd_R(M)$. *Más aún,*

$$pd_R(M) = sup\{i : Tor_i^R(R/\mathfrak{m}, M) \neq 0\}.$$

Demostración. Supongamos que $pd_R(M) = n$, entonces hay una resolución proyectiva $\mathcal{P}$ de M de longitud n, o sea que para $i > n$, $P_i = 0$. Como la definición de Tor es independiente de la resolución proyectiva de M, se sigue que para $i > n$, $Tor_i^R(R/\mathfrak{m}, M) = 0$, con lo cual tenemos que $n \geq a = sup\{i : Tor_i^R(R/\mathfrak{m}, M) \neq 0\}$.

Supongamos que $\mathcal{F}$ es una resolución libre minimal de M. Por la minimalidad de $\mathcal{F}$, los morfismos en el complejo $R/\mathfrak{m} \otimes \mathcal{F}$ son cero. Entonces para cada i, $Tor_i^R(R/\mathfrak{m}, M) = (R/\mathfrak{m}) \otimes_R F_i$. Pero los F_i y $R/\mathfrak{m}$ son finitamente generados (no olvidemos que $R/\mathfrak{m}$ es noetheriano por ser R noetheriano), entonces $(R/\mathfrak{m}) \otimes_R F_i = 0$ si y sólo si $F_i = 0$. En particular, para F_n que es distinto de cero tenemos que $0 \neq (R/\mathfrak{m}) \otimes_R F_n = Tor_n^R(R/\mathfrak{m}, M)$ y por tanto $a \geq n$. Así que $a = n$. $\square$

Capítulo 4

Profundidad

4.1. Sucesiones regulares

Medir el tamaño de un ideal en un anillo es un problema en el que pueden intervenir ideas que incluyen nociones geométricas tales como dimensión o codimensión o algunas otras que involucran aspectos homológicos, vía los funtores Ext y Tor, como lo es la dimensión proyectiva. Otra idea en este tenor es la de profundidad de un ideal, la cual fue trabajada por Ress en [15] y desarrollada con más detalle por él mismo en [16] y que es la que consideraremos aquí.

El concepto de profundidad estará basado en la noción de sucesión regular y en términos del funtor Ext, lo cual muestra la naturaleza homológica del concepto de profundidad.

Después mostraremos algunas relaciones que hay entre profundidad y otros conceptos que pueden ser usados para medir el tamaño de un ideal, tales como dimensión proyectiva, dimensión de Krull y codimensión.

Definición 4.1.1 *Sea M un R-modulo.*

(1) $x \in R$ *es* ***M-regular*** *si* $xm = 0$ *con* $m \in M$ *implica que* $m = 0$. *En caso contrario diremos que* x *es un* ***divisor de cero de*** M.

(2) *Una sucesión* $x_1, \ldots, x_n \in R$ *es una* ***sucesión M-regular*** *o una* ***M-sucesión****, si se cumplen las siguientes condiciones:*

   (i) x_1 *es M-regular y para cada* $i = 2, \ldots, n$, x_i *es* $M/\langle x_1, \ldots, x_{i-1}\rangle M$*-regular.*

   (ii) $M/\langle x_1, \ldots, x_n\rangle M \neq 0$.

(3) *Una sucesión* $x_1, \ldots, x_n \in R$ *que cumple con la condición* (i) *del inciso* (2) *es una* ***M-sucesión débil****.*

Ejemplos.

1. En el anillo de polinomios $R = K[x_1, \ldots, x_n]$ la sucesión de indeterminadas $x_1, \ldots, x_n$ es una R-sucesión.
2. En el anillo de polinomios $R = K[x_1, x_2]$, la sucesión x_1^2, x_1 no es una R-sucesión, ya que x_1 es un divisor de cero de $R/\langle x_1^2\rangle R$.

Proposición 4.1.2 *$x_1, \ldots, x_n \in R$ es una sucesión M-regular si y sólo si para cada $s = 1, \ldots, n-1$, $x_1, \ldots, x_s$ es una sucesión M-regular y $x_{s+1}, \ldots, x_n$ es una sucesión $M/\langle x_1, \ldots, x_s\rangle M$-regular.*

Demostración. Por hipótesis x_1 es M-regular y para cada $i = 2, \ldots, n$, x_i es $M/\langle x_1, \ldots, x_{i-1}\rangle M$-regular. Entonces para cada $i = 2, \ldots, s$ con $s < n$, x_i es $M/\langle x_1, \ldots, x_{i-1}\rangle M$-regular. Como $\langle x_1, \ldots, x_s\rangle \subseteq \langle x_1, \ldots, x_n\rangle$ entonces $\langle x_1, \ldots, x_s\rangle M \subseteq \langle x_1, \ldots, x_n\rangle M \neq M$. Así, $x_1, \ldots, x_s$ es una M-sucesión.

Para el resto de la demostración hacemos $N = M/\langle x_1, \ldots, x_s\rangle M$. De acuerdo con esto tenemos que x_{s+1} es N-regular y para $k = s+2, \ldots, n$, x_k es $M/\langle x_1, \ldots, x_{k-1}\rangle M$-regular. Al tomar los epimorfismos $M \xrightarrow{\pi_1} N$ y $N \xrightarrow{\pi_2} N/\langle x_{s+1}, \ldots, x_{k-1}\rangle N$ tenemos que $\pi_2 \circ \pi_1$ es un epimorfismo, entonces

$$M/\ker(\pi_2 \circ \pi_1) \cong N/\langle x_{s+1}, \ldots, x_{k-1}\rangle N \ .$$

Afirmamos que $\ker(\pi_2 \circ \pi_1) = \langle x_1, \ldots, x_{k-1}\rangle M$, porque $m \in \ker(\pi_2 \circ \pi_1)$ si y sólo si $\pi_2(\pi_1(m)) = \pi_2([m]) = [m] + \langle x_{s+1}, \ldots, x_{k-1}\rangle N = 0$ si y sólo si $[m] \in \langle x_{s+1}, \ldots, x_{k-1}\rangle N$ si y sólo si

$$\begin{aligned}
[m] &= \sum_{fin} \big((\sum_{j=s+1}^{k-1} a_{ij}x_j)(m_i + \langle x_1, \ldots, x_s\rangle M)\big), \ (a_{ij} \in R \ y \ m_i \in M) \\
&= \sum_{fin} \big((\sum_{j=s+1}^{k-1} a_{ij}x_j)m_i + \langle x_1, \ldots, x_s\rangle M\big) \\
&= \big(\sum_{fin} (\sum_{j=s+1}^{k-1} a_{ij}x_j)m_i\big) + \langle x_1, \ldots, x_s\rangle M
\end{aligned}$$

si y sólo si $m - \sum_{fin}(\sum_{j=s+1}^{k-1} a_{ij}x_j)m_i = \sum_{fin}(\sum_{j=1}^{s} b_{ij}x_j)m_i$ (con $b_{ij} \in R$ y $m_i \in M$) si y sólo si $m = \sum_{fin}(\sum_{j=1}^{k-1} c_{ij}x_j)m_i$. Entonces $\ker(\pi_2 \circ \pi_1) = \langle x_1, \ldots, x_{k-1}\rangle M$. Así tenemos que $M/\langle x_1, \ldots, x_{k-1}\rangle M \cong N/\langle x_{s+1}, \ldots, x_{k-1}\rangle N$. Entonces para $k = s+2, \ldots, n$, x_k es $N/\langle x_{s+1}, \ldots, x_{k-1}\rangle N$-regular.

Nos falta probar que $N/\langle x_{s+1}, \ldots, x_n\rangle N \neq 0$. Si $N/\langle x_{s+1}, \ldots, x_n\rangle N = 0$ entonces para todo $m \in M$ tenemos que $(m + \langle x_1, \ldots, x_s\rangle M) + \langle x_{s+1}, \ldots, x_n\rangle N = \langle x_{s+1}, \ldots, x_n\rangle N$, lo que implica que $m + \langle x_1, \ldots, x_s\rangle M \in \langle x_{s+1}, \ldots, x_n\rangle N$. Luego, haciendo lo mismo que en la anterior cadena de equivalencias llegamos a que para cada $m \in M$, $m \in \langle x_1, \ldots, x_n\rangle M$, es decir, $M = \langle x_1, \ldots, x_n\rangle M$, lo cual es una contradicción.

Para el recíproco tenemos que x_1 es M-regular, x_{s+1} es N-regular y para $k = s+2, \ldots, n$, x_k es $N/\langle x_{s+1}, \ldots, x_{k-1}\rangle N$-regular, entonces por lo hecho anteriormente tenemos que x_k es $M/\langle x_1, \ldots, x_{k-1}\rangle M$-regular. $\square$

Proposición 4.1.3 *Sean M un R-módulo y $X = (x_1, \ldots, x_n)$ una M-sucesión débil. Entonces una sucesión exacta de R-módulos*

$$\mathcal{M} : M_2 \xrightarrow{d_2} M_1 \xrightarrow{d_1} M_0 \xrightarrow{d_0} M \longrightarrow 0$$

induce una sucesión exacta

$$\overline{\mathcal{M}} : \overline{M}_2 \xrightarrow{\overline{d}_2} \overline{M}_1 \xrightarrow{\overline{d}_1} \overline{M}_0 \xrightarrow{\overline{d}_0} \overline{M} \longrightarrow 0,$$

donde $\overline{M}_i = M_i/\langle X\rangle M_i$

Demostración. Usaremos inducción sobre la longitud de la sucesión X.

Supongamos que X consiste de un único elemento x_1, el cual es M-regular. Aplicando el funtor aditivo $(R/\langle x_1\rangle) \otimes \_$ a $\mathcal{M}$ obtenemos el complejo

$$\overline{M}_2 \xrightarrow{\overline{d}_2} \overline{M}_1 \xrightarrow{\overline{d}_1} \overline{M}_0 \xrightarrow{\overline{d}_0} \overline{M} \longrightarrow 0.$$

Como el funtor $(R/\langle x_1\rangle) \otimes \_$ es exacto derecho, sólo falta probar que $\ker(\overline{d}_1) \subseteq Im(\overline{d}_2)$ para mostrar que $\overline{\mathcal{M}}$ es un complejo exacto. Para esto, sea $\overline{y} \in \ker(\overline{d}_1)$, es decir, $0 = \overline{d}_1(\overline{y}) = \overline{d_1(y)}$, luego $d_1(y) \in \langle x_1\rangle M_0$, entonces $d_1(y)$ se puede expresar como $d_1(y) = \sum_{fin}(r_i x_1)m_i = x_1 \sum_{fin} r_i m_i$. Entonces $0 = d_0(d_1(y)) = x_1 d_0(\sum_{fin} r_i m_i)$. Pero x_1 es M-regular, luego $d_0(\sum_{fin} r_i m_i) = 0$, o sea que $\sum_{fin} r_i m_i \in \ker(d_0) = Im(d_1)$. Por tanto hay un $z_1 \in M_1$ tal que $d_1(z_1) = \sum_{fin} r_i m_i$.

Debemos mostrar que $\overline{y} \in Im(\overline{d}_2)$, es decir, mostrar que hay un $z_2 \in M_2$ tal que $\overline{d_2(z_2)} = \overline{y}$ lo que equivale a probar que $y - d_2(z_2) \in \langle x_1\rangle M_1$ para algún $z_2 \in M_2$.

Tenemos que $0 = d_1(y) - x_1 d_1(z_1)$, entonces $y - x_1 z_1 \in \ker(d_1) = Im(d_2)$. Así que hay un $z_2 \in M_2$ tal que $d_2(z_2) = y - x_1 z_1$, de donde $y - d_2(z_2) = x_1 z_1 \in \langle x_1\rangle M_1$.

Así queda establecido el caso base (primer paso del principio de inducción matemática).

Ahora supongamos que para toda M-sucesión débil de longitud k, con $1 \leq k < n$, $\mathcal{M}$ induce una sucesión exacta

$$\overline{M}_2 \xrightarrow{\overline{d}_2} \overline{M}_1 \xrightarrow{\overline{d}_1} \overline{M}_0 \xrightarrow{\overline{d}_0} \overline{M} \longrightarrow 0.$$

Al tomar una M-sucesión débil $x_1, \ldots, x_n$, se sigue que $x_1, \ldots, x_{n-1}$ es una M-sucesión débil y x_n es $M/\langle x_1, \ldots, x_{n-1}\rangle M$-regular, entonces por la hipótesis de inducción, $\mathcal{M}$ bajo $(x_1, \ldots, x_{n-1})$ induce una sucesión exacta

$$\overline{M}_2 \xrightarrow{\overline{d}_2} \overline{M}_1 \xrightarrow{\overline{d}_1} \overline{M}_0 \xrightarrow{\overline{d}_0} \overline{M} \longrightarrow 0,$$

la cual por el caso base y por ser x_n $M/\langle x_1, \ldots, x_{n-1}\rangle M$-regular, induce una sucesión exacta

$$\frac{\overline{M}_2}{\langle x_n\rangle \overline{M}_2} \longrightarrow \frac{\overline{M}_1}{\langle x_n\rangle \overline{M}_1} \longrightarrow \frac{\overline{M}_0}{\langle x_n\rangle \overline{M}_0} \longrightarrow \frac{\overline{M}}{\langle x_n\rangle \overline{M}} \longrightarrow 0,$$

y de acuerdo con lo hecho en la prueba de la proposición anterior tenemos el isomorfismo $\overline{M}_i/\langle x_n\rangle\overline{M}_i = (M_i/\langle x_1,\ldots,x_{n-1}\rangle M_i)/\langle x_n\rangle(M_i/\langle x_1,\ldots,x_{n-1}\rangle M_i) \cong M_i/\langle x_1,\ldots,x_n\rangle M_i$. $\square$

Proposición 4.1.4 *Sea*

$$\mathcal{M}:\cdots \longrightarrow M_2 \xrightarrow{d_2} M_1 \xrightarrow{d_1} M_0 \xrightarrow{d_0} M_{-1} \longrightarrow 0$$

un complejo de R-módulos. Si $X=(x_1,\ldots,x_n)$ es una M_i-sucesión débil para cada i, entonces $R/\langle X\rangle\otimes\mathcal{M}$ es un complejo exacto.

Demostración. Usaremos inducción sobre la longitud de X.

Supongamos que X es de longitud uno. Sea $X=x_1$ que es M_i-regular, entonces x_1 también es regular en $Im(d_{i+1})$. Luego podemos aplicar la proposición anterior a la sucesión exacta

$$M_{i+3} \longrightarrow M_{i+2} \longrightarrow M_{i+1} \longrightarrow Im(d_{i+1}) \longrightarrow 0$$

para obtener la sucesión exacta

$$\overline{M}_{i+3} \longrightarrow \overline{M}_{i+2} \longrightarrow \overline{M}_{i+1} \longrightarrow \overline{Im(d_{i+1})} \longrightarrow 0.$$

Haciendo esto para cada i, obtenemos el diagrama con fila exacta

$$\begin{tikzcd}
 & & & & & 0 \\
 & & & & \overline{Im(d_{i+1})} \arrow[ur] & \\
\cdots \arrow[r] & \overline{M}_{i+3} \arrow[r] & \overline{M}_{i+2} \arrow[r] & \overline{M}_{i+1} \arrow[r] \arrow[ur] & \overline{M}_i \arrow[r] & \cdots .
\end{tikzcd}$$

De este modo queda establecido el caso base y el argumento que sigue para completar la prueba es análogo al de la proposición anterior.

Así podemos concluir que $R/\langle X\rangle\otimes\mathcal{M}$ es un complejo exacto. $\square$

Proposición 4.1.5 *Sea M un R-módulo finitamente generado y suponga que x_1, x_2 es una M-sucesión. Entonces*

(1) *x_2, x_1 es una M-sucesión si y sólo si x_2 no es divisor de cero en M.*

(2) *Si $(R,\mathfrak{m})$ es un anillo local noetheriano entonces x_2 no es divisor de cero en M.*

Demostración. La prueba de la primera implicación en (1) es inmediata.

Para el recíproco hay que probar $\langle x_2, x_1\rangle M \neq M$ y que x_1 no es divisor de cero en $M/\langle x_2\rangle M$.

Tenemos que $\langle x_2, x_1\rangle M = \langle x_1, x_2\rangle M \neq M$. Ahora supongamos que x_1 es divisor de cero en $M/\langle x_2\rangle M$, entonces hay un $m \in M - \langle x_2\rangle M$ tal que $x_1(m + \langle x_2\rangle M) = \langle x_2\rangle M$, así, $x_1 m \in \langle x_2\rangle M$. De aquí se sigue que $x_1 m = \sum_{fin}(a_i x_2)m_i = \sum_{fin}(x_2 a_i)m_i = \sum_{fin} x_2(a_i m_i) = x_2 \sum_{fin}(a_i m_i) = x_2 n$, donde $a_i \in R$, $m_i \in M$ y $n = \sum_{fin} a_i m_i$. Si $n \in \langle x_1\rangle M$, se sigue que $n = x_1 m'$ para algún $m' \in M$, entonces $x_1 m = x_2(x_1 m')$ y por tanto $x_1(m - x_2 m') = 0$. Como x_1 no es divisor de cero en M, $m = x_2 m' \in \langle x_2\rangle M$, lo cual es una contradicción. Por lo tanto $n \notin \langle x_1\rangle M$. Ahora bien, como $x_2 n = x_1 m \in \langle x_1\rangle M$, entonces $x_2(n+\langle x_1\rangle M) = \langle x_1\rangle M$, es decir, x_2 es un divisor de cero en $M/\langle x_1\rangle M$, lo que contradice el que x_1, x_2 sea una M-sucesión. Entonces x_1 no puede ser divisor de cero en $M/\langle x_2\rangle M$.

Para la prueba de (2) supongamos que para algún $m \in M$, $x_2 m = 0 \in \langle x_1\rangle M$, entonces $x_2(m + \langle x_1\rangle M) = x_2 m + \langle x_1\rangle M = \langle x_1\rangle M$, o sea que $m + \langle x_1\rangle M = \langle x_1\rangle M$ (pues x_2 no es divisor de cero en $M/\langle x_1\rangle M$). Esto implica que $m \in \langle x_1\rangle M$, es decir, que $m = x_1 m'$ para algún $m' \in M$. Como $0 = x_2 m = x_2(x_1 m') = x_1(x_2 m')$, se sigue que $x_2 m' = 0$ (ya que x_1 no es divisor de cero en M). Sea $L = \{m \in M : x_2 m = 0\}$, el cual es un submódulo de M. Además $\langle x_1\rangle L$ es un submódulo de L tal que $L \subseteq \langle x_1\rangle L$. Entonces $L = \langle x_1\rangle L \subseteq \mathfrak{m}L \subseteq L$ (porque todo ideal propio está contenido en un ideal maximal), así que $\mathfrak{m}L = L$. Como R es noetheriano y M finitamente generado, entonces M es noetheriano y así L es finitamente generado. Luego, por el lema de Nakayama, $L = 0$. Por lo tanto x_2 no es divisor de cero en M. $\square$

Proposición 4.1.6 *Si $(R, \mathfrak{m})$ es un anillo local noetheriano y M es un R-módulo finitamente generado, entonces cualquier permutación de una M-sucesión también es una M-sucesión.*

Demostración. Sea $x_1, \ldots, x_n$ una M-sucesión. Como toda permutación es un producto de transposiciones de elementos consecutivos, basta probar que todas las transposiciones de la forma $(i, i+1)$ aplicadas a $x_1, \ldots, x_n$ da una M-sucesión.

$x_1, \ldots, x_{i-1}, x_{i+1}, x_i, x_{i+2}, \ldots, x_n$ es una M-sucesión si sólo si $x_1, \ldots, x_{i-1}, x_{i+1}, x_i$ es una M-sucesión y $x_{i+2}, \ldots, x_n$ es una $M/\langle x_1, \ldots, x_{i-1}, x_{i+1}, x_i\rangle M$-sucesión, lo cual equivale a que $x_1, \ldots, x_{i-1}$ es una M-sucesión, x_{i+1}, x_i es una $M/\langle x_1, \ldots, x_{i-1}\rangle M$-sucesión y $x_{i+2}, \ldots, x_n$ es una $M/\langle x_1, \ldots, x_{i-1}, x_{i+1}, x_i\rangle M$-sucesión.

Como $x_1, \ldots, x_n$ es una M-sucesión, entonces $x_1, \ldots, x_{i+1}$ es una M-sucesión y $x_{i+2}, \ldots, x_n$ es una $M/\langle x_1, \ldots, x_{i+1}\rangle M$-sucesión, entonces $x_1, \ldots, x_{i-1}$ es una M-sucesión, x_i, x_{i+1} es una $M/\langle x_1, \ldots, x_{i-1}\rangle M$-sucesión y $x_{i+2}, \ldots, x_n$ es una $M/\langle x_1, \ldots, x_{i+1}\rangle M$-sucesión.

Que x_i, x_{i+1} es una $M/\langle x_1, \ldots, x_{i-1}\rangle M$-sucesión, implica por (2) de la proposición anterior que x_{i+1} no es divisor de cero en $M/\langle x_1, \ldots, x_{i-1}\rangle M$, luego por (1) de la misma proposición, x_{i+1}, x_i es una $M/\langle x_1, \ldots, x_{i-1}\rangle M$-sucesión.

Entonces de lo hecho en los dos párafos anteriores se sigue que $x_1, \ldots, x_{i-1}$ es una M-sucesión, x_{i+1}, x_i es una $M/\langle x_1, \ldots, x_{i-1}\rangle M$-sucesión y $x_{i+2}, \ldots, x_n$ es una $M/\langle x_1, \ldots, x_{i-1}, x_{i+1}, x_1\rangle M$-sucesión, que es justamente lo que se tiene al final de la cadena de equivalencias desarrollada arriba. Por lo tanto $x_1, \ldots, x_{i-1}, x_{i+1}, x_i, x_{i+2}, \ldots, x_n$ es una M-sucesión. □

4.2. Sucesiones regulares maximales

Proposición 4.2.1 *Si R es un anillo noetheriano y M un R-módulo, entonces toda sucesión regular en M es finita.*

Demostración. Supongamos que hay una M-sucesión infinita $x_1, x_2, \ldots$ de elementos en R. Ahora consideremos la sucesión de ideales de R

$$\langle x_1 \rangle \subseteq \langle x_1, x_2 \rangle \subseteq \langle x_1, x_2, x_3 \rangle \subseteq \ldots$$

ordenada por la inclusión.

Afirmamos que todas las inclusiones se dan en sentido estricto, pues de lo contrario, existiría un $k \in \mathbb{N}$ tal que $\langle x_1, \ldots x_k \rangle = \langle x_1, \ldots, x_{k+1} \rangle$ y $x_{k+1} \in \langle x_1, \ldots x_k \rangle$. Luego, para cada $m \in M$, $x_{k+1}m \in \langle x_1, \ldots x_k \rangle M$, lo que implica que $x_{k+1}(m + \langle x_1, \ldots x_k \rangle M) = \langle x_1, \ldots x_k \rangle M$, de donde para cada $m \in M$, $m + \langle x_1, \ldots x_k \rangle M = \langle x_1, \ldots x_k \rangle M$, por ser x_{k+1} $M/\langle x_1, \ldots x_k \rangle M$-regular. De aquí se sigue que para cada $m \in M$, $m \in \langle x_1, \ldots x_k \rangle M$, o sea que $M = \langle x_1, \ldots x_k \rangle M$, lo cual contradice el hecho de que $x_1, \ldots x_k$ es una M-sucesión. Por lo tanto, las inclusiones son estrictas.

De este modo tenemos una sucesión creciente de ideales en el anillo noetheriano R. Entonces por la condición de cadena ascendente, hay un $k \in N$ tal que $\langle x_1, \ldots x_k \rangle = \langle x_1, \ldots, x_{k+1} \rangle$, lo que ya vimos nos lleva a una contradicción.

Por lo tanto, toda M-sucesión en R noetheriano es finita. □

Definición 4.2.2 *Sea M un R-módulo. Una M-sucesión $x_1, \ldots, x_n$ es una **sucesión regular maximal en** M si para todo $r \in R$, la sucesión $x_1, \ldots, x_n, r$ no es una M-sucesión.*

Proposición 4.2.3 *Sean M y N R-módulos y $x_1, \ldots, x_n$ una M-sucesión. Si $x_n \in Ann_R(N)$ entonces $Hom_R(N, M/\langle x_1, \ldots, x_{n-1} \rangle M) = 0$.*

Demostración. Sean $h \in Hom_R(N, M/\langle x_1, \ldots, x_{n-1} \rangle M)$ y $x \in N$, entonces $x_n x = 0$, lo que implica que $x_n h(x) = h(x_n x) = h(0) = 0$. Como x_n es $M/\langle x_1, \ldots, x_{n-1} \rangle M$-regular entonces $h(x) = 0$. □

Proposición 4.2.4 *Sean M y N R-módulos y $x_1, \ldots, x_n$ una M-sucesión en $Ann(N)$. Entonces*

$$Hom_R(N, M/\langle x_1, \ldots, x_n \rangle M) \cong Ext_R^n(N, M).$$

Demostración. Haremos la prueba usando inducción sobre n.

Para $n = 0$, $Ext_R^n(N, M) \cong Hom_R(N, M) = Hom_R(N, M_0)$, con lo cual queda establecido el caso base.

Supongamos que para $0 \leq j < n$, al tomar la M-sucesión $x_1, \ldots, x_j$ se cumple que $Hom_R(N, M/\langle x_1, \ldots, x_j \rangle M) \cong Ext_R^j(N, M)$. Veamos qué ocurre al considerar la M-sucesión $x_1, \ldots, x_{j+1}$.

Como $x_{j+1} \in Ann(N)$, entonces por la proposición anterior, $Ext_R^j(N, M) \cong Hom_R(N, M/\langle x_1, \ldots, x_j \rangle M) = 0$, y del hecho de que x_1 es M-regular se sigue que la sucesión

$$0 \longrightarrow M \xrightarrow{x_1} M \longrightarrow M/x_1M \longrightarrow 0$$

es exacta, donde el morfismo $M \xrightarrow{x_1} M$ es multiplicación por x_1 y el morfismo $M \to M/x_1M$ es el canónico. Entonces esta sucesión garantiza la existencia de la sucesión exacta larga

$$\begin{tikzcd}
\cdots \arrow[r] & Ext_R^j(N,M) \arrow[r, "x_1"] & Ext_R^j(N,M) \arrow[r] & Ext_R^j(N,M/x_1M) \arrow[dll, "\delta_j"] \\
& Ext_R^{j+1}(N,M) \arrow[r, "x_1"] & Ext_R^{j+1}(N,M) \arrow[r] & Ext_R^{j+1}(N,M/x_1M) \arrow[r] & \cdots,
\end{tikzcd}$$

donde $Ext_R^j(N, M) = 0$ y el morfismo $Ext_R^{j+1}(N, M) \xrightarrow{x_1} Ext_R^{j+1}(N, M)$ es multiplicación por x_1.

Afirmamos que x_1 anula $Ext_R^{j+1}(N, M) = H_{j+1}(Hom_R(N, E_M))$.

Para esto tomamos una resolución inyectiva de M

$$0 \longrightarrow M \longrightarrow E_0 \xrightarrow{\psi_0} E_1 \xrightarrow{\psi_1} E_2 \longrightarrow \cdots$$

y le aplicamos el funtor $Hom_R(N, \_\,)$ al recortado E_M de M para obtener el complejo

$$0 \longrightarrow Hom_R(N, E_0) \xrightarrow{\psi_0^*} Hom_R(N, E_1) \xrightarrow{\psi_1^*} Hom_R(N, E_2) \longrightarrow \ldots$$

Como $x_1 \in Ann(N)$, entonces es claro que para todo j, x_1 anula a $Hom_R(N, E_j)$, y ya que $\ker(\psi_{j+1}^*) \subseteq Hom_R(N, E_{j+1})$, x_1 anula a $Ext_R^{j+1}(N, M)$. Por esto, la sucesión exacta larga se reduce a la sucesión exacta

$$0 \longrightarrow Ext_R^j(N, M/x_1M) \xrightarrow{\delta_j} Ext_R^{j+1}(N, M) \longrightarrow 0,$$

de donde resulta que δ_j es a la vez inyectiva y suprayectiva. Así $Ext_R^{j+1}(N, M) \cong Ext_R^j(N, M/x_1M)$. Luego, por la hipótesis de inductiva $Ext_R^j(N, M/x_1M) \cong Hom_R(N, (M/x_1M)/\langle x_2, \ldots, x_{j+1} \rangle (M/x_1M))$ ya que $x_2, \ldots, x_{j+1}$ es una sucesión M/x_1M-regular. Entonces por lo hecho en la prueba de 4.1.2,

$$(M/x_1M)/\langle x_2, \ldots, x_{j+1} \rangle (M/x_1M) \cong M/\langle x_1, \ldots, x_{j+1} \rangle M.$$

Luego,

$$Ext_R^{j+1}(N, M) \cong Hom_R(N, M/\langle x_1, \ldots, x_{j+1} \rangle M),$$

lo cual completa la prueba inductiva. □

Proposición 4.2.5 *Supongamos que M es un R-módulo e I un ideal de R. Entonces $Hom_R(R/I, M) \neq 0$ si y sólo si hay un $x \in M$ con $x \neq 0$ tal que $I = Ann(x)$.*

Demostración. ($\Rightarrow$) $Hom_R(R/I, M) \neq 0$ implica que hay un $f \neq 0$ en $Hom_R(R/I, M)$, entonces existe un $r \in R - I$ tal que $f(r + I) \neq 0$. Sea $x = f(r + I) \in M$ y tomemos un $a \in I$, entonces $ax = af(r + I) = f(ar + I) = f(I) = 0$. Así tenemos que I anula a x.

($\Leftarrow$) Supongamos que hay un $x \in M$ con $x \neq 0$ tal que I anula a x. Definimos un R-morfismo $f : R/I \to M$ que a $r + I$ le asocia rx. Es claro que f está bien definido porque I anula a x y $f \neq 0$, pues $f(1 + I) \neq 0$. □

Observaciones.

1. La segunda parte, en la equivalencia de la proposición anterior nos dice que los elementos de I son divisores de cero de M.
2. Si a la hipótesis de la proposición anterior añadimos que R sea un anillo noetheriano, entonces $\bigcup_{P \in AP(M)} P = ZD_R(M) \supseteq I$ (la igualdad se garantiza por B.1.6).

Proposición 4.2.6 *Si R es un anillo noetheriano, M un R-módulo de generación finita e I un ideal de R tal que $IM \neq M$, entonces cualesquiera dos M-sucesiones maximales en I tienen la misma longitud, a saber,*

$$inf\{i : Ext^i_R(R/I, M) \neq 0\}.$$

Demostración. Sea $x_1, \ldots, x_n$ una M-sucesión maximal en I. Es claro que los x_i están en $Ann(R/I)$. Entonces por 4.2.3 y 4.2.4, para cualquier k con $1 \leq k \leq n$,

$$Ext^{k-1}_R(R/I, M) \cong Hom_R(R/I, M/\langle x_1, \ldots, x_{k-1}\rangle M) = 0$$

Veamos qué pasa con $Ext^n_R(R/I, M)$.

$Ext^n_R(R/I, M) = 0$ si y sólo si $Hom_R(R/I, M/\langle x_1, \ldots, x_n\rangle M) = 0$ si y sólo si $I \nsubseteq \bigcup AP(M/\langle x_1, \ldots, x_n\rangle M)$ si y sólo si hay un $a \in I$ tal que $a \notin P$ para todo $P \in AP(M/\langle x_1, \ldots, x_n\rangle M)$, o sea que a no es divisor de cero de $M/\langle x_1, \ldots, x_n\rangle M$, es decir, a es $M/\langle x_1, \ldots, x_n\rangle M$-regular. Entonces la sucesión $x_1, \ldots, x_n, a$ es M-regular y está contenida en I, lo que contradice la maximalidad de la sucesión $x_1, \ldots, x_n$. Así $Ext^n_R(R/I, M) \neq 0$. Por lo tanto, la longitud de la M-sucesión maximal $x_1, \ldots, x_n$ es igual a $inf\{i : Ext^i_R(R/I, M) \neq 0\}$.
□

Proposición 4.2.7 *Toda M-sucesión en R puede ser completada a una M-sucesión maximal.*

Demostración. Supongamos que la longitud de cualquier M-sucesión maximal en R es n y sea $x_1, \ldots, x_p$ una M-sucesión tal que $p < n$, entonces esta

M-sucesión no es maximal, así que hay un $r_1 \in R$ tal que $x_1, \ldots, x_p, r_1$ es una M-sucesión. De la misma manera podemos encontrar $r_1, \ldots, r_{n-p} \in R$ tal que $x_1, \ldots, x_p, r_1, \ldots, r_{n-p}$ es una M-sucesión de longitud n y que por lo tanto es maximal. $\square$

Definición 4.2.8 *Sean R un anillo noetheriano, M un R-módulo finitamente generado e I un ideal propio de R tal que $IM \neq M$. Definimos la* ***profundidad*** *de I en M, denotada por $depth(I, M)$, como la longitud de cualquier M-sucesión maximal contenida en I.*

Ejemplo. Sean $(R, \mathfrak{m})$ un anillo local noetheriano y $M \neq 0$ un R-módulo finitamente generado. Entonces

$$depth(\mathfrak{m}, M) = 0 \text{ si y sólo si } \mathfrak{m} \in AP(M).$$

En efecto, pues si $depth(\mathfrak{m}, M) = 0$, entonces la longitud de cualquier M-sucesión maximal contenida en $\mathfrak{m}$ es cero, o sea que todo elemento de $\mathfrak{m}$ es divisor de cero de M. Así, $\mathfrak{m} \subseteq ZD_R(M)$. Pero R es noetheriano, así que $ZD_R(M) = \bigcup_{P \in AP(M)} P$ y por tanto $\mathfrak{m} \in AP_R(M)$.

El recíproco es inmediato.

4.3. Profundidad y codimensión

Señalamos al inicio de este capítulo que la profundidad puede ser relacionada con otros invariantes de un ideal I. En esta sección trataremos principalmente a la relación que hay entre profundidad y codimensión, y profundidad y dimensión de Krull.

Definición 4.3.1 *Sean R un anillo e I un ideal en R. La* ***codimensión*** *de I en R, denotada por $codim(I)$, se define como el supremo de las longitudes de cadenas, ordenadas por la inclusión, de ideales primos de R que están contenidos en I.*

Ejemplo. En un campo K tenemos que 0 y K son sus únicos ideales. Como se sabe que el ideal 0 es primo si y sólo si $R = K$ es un dominio entero, entonces $codim(0) = 0 = codim(K)$.

Proposición 4.3.2 *Sea M un módulo finitamente generado sobre un anillo noetheriano R. Si $r \in R$ es M-regular, entonces $r \notin P$ para todos los elementos minimales de $Supp(M)$.*

Demostración. Supongamos que hay un P minimal en $Supp(M)$ tal que $r \in P$. De B.3.9 tenemos que $P \in AP(M)$, entonces hay un $m \neq 0$ en M tal que $P = Ann(m)$. Luego, $rm = 0$. Como r es M-regular, se sigue que $m = 0$, lo cual es una contradicción. $\square$

Proposición 4.3.3 *Sea I un ideal de un anillo noetheriano R, entonces*

$$depth(I,R) \leq codim(I).$$

Demostración. Haremos la prueba por inducción sobre $depth(I,R)$. Supongamos que $depth(I,R) = 0$. Al ser $codim(I,R) \geq 0$ se sigue que $depth(I,R) \leq codim(I,R)$.

Como hipótesis inductiva, suponemos que siempre que $depth(I,R) < k$, entonces $depth(I,R) \leq codim(I)$.

Ahora consideremos el caso en que $depth(I,R) = k$.

Al tomar una R-sucesión maximal $x_1, \ldots, x_k$ en I, tenemos que x_1 es R-regular, entonces para cualquier P minimal en $Supp(R)$, $x_1 \notin P$.

Veamos qué ocurre con $codim(I/\langle x_1 \rangle)$ (visto $I/\langle x_1 \rangle$ como un ideal de $R/\langle x_1 \rangle$).

Como hay una correspondencia biyectiva entre los ideales primos en $R/\langle x_1 \rangle$ y los ideales primos en R que contienen a $\langle x_1 \rangle$, entonces cualquier cadena de ideales primos del anillo $R/\langle x_1 \rangle$ contenida en $I/\langle x_1 \rangle$ está asociada con una cadena de ideales primos en R contenida en I y que contiene a $\langle x_1 \rangle$. Pero $\langle x_1 \rangle \nsubseteq P$ para todo P minimal en $Supp(R)$, así que para cualquiera de tales cadenas de ideales primos en R podemos encontrar al menos un ideal primo que se añade a dicha cadena. Así que $codim(I/\langle x_1 \rangle) < codim(I)$. Luego, de la maximalidad de la R-sucesión $x_1, \ldots, x_k$ se sigue que

$$depth(I/\langle x_1 \rangle, R/\langle x_1 \rangle) = k - 1,$$

y por la hipótesis de inducción tenemos que

$$depth(I,R) - 1 = k - 1 = depth(I/\langle x_1 \rangle, R/\langle x_1 \rangle) \leq codim(I/\langle x_1 \rangle) < codim(I),$$

y así, $depth(I,R) \leq codim(I)$. □

Definición 4.3.4 *La **dimensión de Krull** de un anillo R, denotada por $dim(R)$, es el supremo de las longitudes de cadenas de ideales primos en R, donde la longitud de una cadena es el número de contensiones propias en ésta (por ejemplo, la cadena $P_0 \subseteq P_1 \subseteq \cdots \subseteq P_n$ tiene longitud n).*

Ejemplo. Un dominio de ideales principales R tiene dimensión a lo más uno.

Para esto, tomemos dos ideales primos $\langle p \rangle \neq 0$ y $\langle q \rangle \neq 0$ en R tales que $\langle p \rangle \subseteq \langle q \rangle$. Tenemos que $p \in \langle q \rangle$, entonces $p = rq \in \langle p \rangle$ y por tanto $r \in \langle p \rangle$ o $q \in \langle p \rangle$. Si $r \in \langle p \rangle$, $r = tp$. Entonces $p = rq = (tp)q = (tq)p$, lo que implica que $tq = 1$ y de esto se sigue que $\langle q \rangle = R$, lo cual es una contradicción. Así que $q \in \langle p \rangle$ y por tanto $\langle q \rangle \subseteq \langle p \rangle$. Luego $\langle p \rangle = \langle q \rangle$. Así, la cadena más larga de contensiones propias de ideales primos es $0 \subsetneq \langle p \rangle$.

Observación. En un anillo local $(R, \mathfrak{m})$, $depth(\mathfrak{m}, R) \leq dim(R)$, ya que $dim(R)$ es el número de contensiones de cualquier cadena maximal de ideales primos en R, de hecho, tales cadenas maximales de ideales primos están contenidas en $\mathfrak{m}$ (pues cualquier ideal propio de un anillo está contenido en algún ideal maximal $\mathfrak{m}$), así que $dim(R) = codim(\mathfrak{m})$.

4.4. Fórmula de Auslander-Buchsbaum

Proposición 4.4.1 *Sea R un anillo noetheriano e I un ideal de R. Si*

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$$

es una sucesión exacta de R-módulos, entonces se cumplen las siguientes desigualdades (suponiendo que se cumplen las condiciones para que las expresiones que intervienen en dichas desigualdades tengan sentido):

(1) $depth(I,N) \geq min\{depth(I,M),\ depth(I,T)\}$.

(2) $depth(I,M) \geq min\{depth(I,N),\ depth(I,T)+1\}$.

(3) $depth(I,T) \geq min\{depth(I,M)-1,\ depth(I,N)\}$.

Demostración. Haremos sólo la prueba para (2), pues las demostraciones para (1) y (3) se hacen de manera análoga.

La sucesión exacta corta $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} T \longrightarrow 0$ induce la sucesión exacta larga

$$\begin{tikzcd}
\cdots \arrow[r] & Ext_R^j(R/I,M) \arrow[r] & Ext_R^j(R/I,N) \arrow[r] & Ext_R^j(R/I,T) \arrow[dll, rounded corners, "\delta_j"] & \\
& Ext_R^{j+1}(R/I,M) \arrow[r] & Ext_R^{j+1}(R/I,N) \arrow[r] & Ext_R^{j+1}(R/I,T) \arrow[r] & \cdots .
\end{tikzcd}$$

Sean $a = depth(I,M)$, $b = depth(I,N)$ y $c = depth(I,T)$, entonces $b \leq c+1$ o $c+1 < b$. Supongamos además que $a < min\{b,\ c+1\}$.

Si $b \leq c+1$ y $a < b$, entonces $a < b$ y $a-1 < c$, lo cual implica que $Ext_R^a(R/I,N) = 0$ y $Ext_R^{a-1}(R/I,T) = 0$. Entonces por la exactitud de la sucesión exacta larga se sigue que $Ext_R^a(R/I,M) = 0$, lo cual es una contradicción.

Si $c+1 < b$ y $a < c+1$, entonces $a-1 < c$ y $a < b$, que es lo mismo que obtuvimos anteriormente y que nos llevará a una contradicción.

Por lo tanto $depth(I,M) \geq min\{depth(I,N),\ depth(I,T)+1\}$. □

Proposición 4.4.2 *Sean R un anillo noetheriano, I un ideal de R, M un R-módulo finitamente generado y $X = (x_1, \ldots, x_n)$ una M-sucesión en I. Entonces son equivalentes:*

(1) $IM = M$.

(2) $I(M/\langle X\rangle M) = M/\langle X\rangle M$.

(3) $(I/\langle X\rangle)(M/\langle X\rangle M) = M/\langle X\rangle M$.

Demostración. Sean $\overline{R} = R/\langle X\rangle$, $\overline{I} = I/\langle X\rangle$ y $\overline{M} = M/\langle X\rangle M$.

Para mostrar que (1) implica (2) sólo hay que probar que $I\overline{M} \supseteq \overline{M}$ pues ya sabemos que $I\overline{M}$ es un submódulo de $\overline{M}$. Sea $\overline{m} \in \overline{M}$, entonces como $IM = M$, $m = \sum_{fin} r_i m_i$, donde $r_i \in I$ y $m_i \in M$. Luego, $\overline{m} = \overline{\sum_{fin} r_i m_i} = \sum_{fin} \overline{r_i m_i} = \sum_{fin} r_i \overline{m}_i \in I\overline{M}$.

Ahora veamos que (2) implica (3). En (3) implícitamente se nos está indicando que $\overline{M}$ tiene una estructura de $\overline{R}$-módulo. Veamos que efectivamente es así. Ya que

$$\begin{aligned} Ann_R(\overline{M}) &= \{r \in R : r\overline{M} = 0\} = \{r \in R : \text{para cada } m \in M,\ r\overline{m} = 0\} \\ &= \{r \in R : \text{para cada } m \in M,\ \overline{rm} = 0\} \\ &= \{r \in R : \text{para cada } m \in M,\ rm \in \langle X\rangle M\} = \langle X\rangle, \end{aligned}$$

$\overline{M}$ se puede considerar como un $\overline{R}$-módulo, donde $\overline{r}\,\overline{m} = r\overline{m}$.

Como $\overline{I}\,\overline{M}$ es un submódulo del $\overline{R}$-módulo $\overline{M}$, únicamente falta probar que $\overline{M} \subseteq \overline{I}\,\overline{M}$. Sea $\overline{m} \in \overline{M} = I\overline{M}$, entonces $\overline{m} = \sum_{fin} r_i \overline{m}_i = \sum_{fin} \overline{r}_i\,\overline{m}_i$, donde $r_i \in I$ y $m_i \in M$, con lo cual tenemos que $\overline{m} \in \overline{I}\,\overline{M}$.

Finalmente probemos que (3) implica (1), en donde al igual que en los casos anteriores, sólo hay probar que $M \subseteq IM$. Sea $m \in M$ y consideremos su clase $\overline{m} \in \overline{M} = \overline{I}\,\overline{M}$, entonces $\overline{m} = \sum_{fin} \overline{r}_i\,\overline{m}_i = \sum_{fin} r_i \overline{m}_i = \overline{\sum_{fin} r_i m_i}$, luego, $m - \sum_{fin} r_i m_i \in \langle X\rangle M$, o sea que, $m - \sum_{fin} r_i m_i = \sum_{fin}(\sum_{j=1}^{n} s_{kj} x_j) m_k$, es decir, $m \in IM$. □

Proposición 4.4.3 *Sean M un módulo finitamente generado sobre un anillo noetheriano R, I un ideal de R con $IM \neq M$ y $X = (x_1, \ldots, x_n)$ una M-sucesión en I, entonces*

$$depth(\overline{I}, \overline{M}) = depth(I, \overline{M}) = depth(I, M) - n.$$

Demostración. Sea $Y = (y_1, \ldots, y_m)$ una $\overline{M}$-sucesión maximal en I. Entonces haciendo el mismo tipo de cálculos que en la proposición anterior junto con el hecho de que para cada $i \in \{1, \ldots, m\}$, y_i es $\overline{M}/\langle y_1, \ldots, y_{i-1}\rangle\overline{M}$-regular, se sigue directamente que $\overline{y}_i$ es $\overline{M}/\langle\overline{y}_1, \ldots, \overline{y}_{i-1}\rangle\overline{M}$ -regular.

Por otra parte, como $y_1, \ldots, y_m$ es una $\overline{M}$-sucesión en I, $\langle y_1, \ldots, y_m\rangle\overline{M} \neq \overline{M}$. Así que $\langle\overline{y}_1, \ldots, \overline{y}_m\rangle\overline{M} \neq \overline{M}$, de acuerdo con la proposición 4.4.2. De este modo $\overline{y}_1, \ldots, \overline{y}_m$ es una $\overline{M}$-sucesión en $\overline{I}$.

Ahora supongamos que $\overline{y}_1, \ldots, \overline{y}_m$ no es una $\overline{M}$-sucesión maximal en $\overline{I}$, entonces hay un $r_0 \in I$ tal que $\overline{y}_1, \ldots, \overline{y}_m, \overline{r}_0$ es una $\overline{M}$-sucesión y de aquí tenemos que $\overline{r}_0$ es $\overline{M}/\langle\overline{y}_1, \ldots, \overline{y}_m\rangle\overline{M}$ -regular. Y nuevamente con el mismo tipo de cálculos que en la proposición anterior llegamos a que r_0 es $\overline{M}/\langle y_1, \ldots, y_m\rangle\overline{M}$-regular. Pero $\overline{y}_1, \ldots, \overline{y}_m, \overline{r}_0$ es una $\overline{M}$-sucesión, entonces $\langle\overline{y}_1, \ldots, \overline{y}_m, \overline{r}_0\rangle\overline{M} \neq \overline{M}$, que implica que $\langle y_1, \ldots, y_m, r_0\rangle\overline{M} \neq \overline{M}$ y de aquí se sigue que $y_1, \ldots, y_m, r_0$ es una $\overline{M}$-sucesión en $\overline{I}$, lo que contradice la maximalidad de $y_1, \ldots, y_m$. Así $\overline{y}_1, \ldots, \overline{y}_m$ es una $\overline{M}$-sucesión maximal en $\overline{I}$. Por lo tanto, $depth(\overline{I}, \overline{M}) = depth(I, \overline{M})$.

Para la segunda igualdad tenemos que la M-sucesión en I, $x_1, \ldots, x_n$ puede ser completada a una M-sucesión maximal en I, digamos $x_1, \ldots, x_n, \ldots, x_m$.

Entonces por la proposición 4.1.2, $x_1, \ldots, x_n$ es una M-sucesión y $x_{n+}1, \ldots, x_m$ es una $\overline{M}$-sucesión.

Veamos que $x_{n+}1, \ldots, x_m$ es una $\overline{M}$-sucesión maximal.

Supongamos que $x_{n+}1, \ldots, x_m$ no es maximal, entonces hay un $r_0 \in R$ tal que $x_{n+}1, \ldots, x_m, r_0$ es una $\overline{M}$-sucesión. Esto último junto con el hecho de que $x_1, \ldots, x_n$ es una M-sucesión implican que $x_1, \ldots, x_n, x_{n+1} \ldots, x_m, r_0$ es una M-sucesión, lo que contradice la maximalidad de $x_1, \ldots, x_n, \ldots, x_m$. Así, $depth(I, \overline{M}) = depth(I, M) - n$. $\square$

Proposición 4.4.4 *Sea $f : F \to G$ un monomorfismo de módulos finitamente generados sobre un anillo local $(R, \mathfrak{m})$ y supongamos además que F es libre y que $\mathfrak{m} \in AP_R(R)$. Entonces $1_k \otimes f$ es inyectiva, donde $k = R/\mathfrak{m}$.*

Demostración. $\mathfrak{m} \in AP_R(R)$ implica por B.1.3 que hay un monomorfismo de R-módulos $\varphi : k \to R$. Por otra parte, como F es libre se sigue de 2.1.13 que F es plano, entonces $\varphi \otimes 1_F : k \otimes_R F \to R \otimes_R F$ es inyectiva. Así obtenemos el diagrama conmutativo

$$\begin{array}{ccc} k \otimes_R F & \xrightarrow{\varphi \otimes 1_F} & R \otimes_R F \cong F \\ \Big\downarrow{\scriptstyle 1_k \otimes f} & & \Big\downarrow{\scriptstyle 1_R \otimes f} \\ k \otimes_R G & \xrightarrow{\varphi \otimes 1_G} & R \otimes_R G \cong G\ . \end{array}$$

Como $\varphi \otimes 1_F$ y $1_R \otimes f$ son inyectivas, entonces $(1_R \otimes f) \circ (\varphi \otimes 1_F) = (\varphi \otimes 1_G) \circ (1_k \otimes f)$ es inyectiva, luego $1_k \otimes f$ es inyectiva. $\square$

Proposición 4.4.5 *Sean $(R, \mathfrak{m})$ un anillo local noetheriano y M un R-módulo finitamente generado. Si $x \in \mathfrak{m}$ es R-regular y M-regular, entonces*

$$pd_R(M) = pd_{R/\langle x \rangle}(M/\langle x \rangle M).$$

Demostración. Sea $\mathcal{F}$ una resolución libre minimal de M.

Veamos que x es F_i-regular. Sea $y \in F_i$ tal que $xy = 0$. Como F_i es libre, F_i tiene una base, digamos $\{b_j\}$. Entonces y se puede expresar de manera única como $y = \sum r_j b_j$, donde $r_j \in R$ y $r_j = 0$ para casi todo j. Luego, $xy = x \sum r_j b_j = \sum (x r_j) b_j = 0$. Entonces para todo j, $x r_j = 0$. Pero x es R-regular, así que para todo j, $r_j = 0$, o sea que $y = 0$. Por lo tanto, x es F_i-regular.

Por lo tanto, por 4.1.4, el complejo $R/\langle x \rangle \otimes \mathcal{F}$ es exacto.

También tenemos que cada R-módulo en $R/\langle x \rangle \otimes \mathcal{F}$ admite una estructura de $R/\langle x \rangle$-módulo, pues $\langle x \rangle \subseteq Ann(M/\langle x \rangle M)$ y $\langle x \rangle \subseteq Ann(F_i/\langle x \rangle F_i)$. Además $R/\langle x \rangle \otimes_R F_i \cong R/\langle x \rangle \otimes_R (\bigoplus R) \cong \bigoplus (R/\langle x \rangle \otimes_R R) \cong \bigoplus R/\langle x \rangle$ y como $R/\langle x \rangle \otimes_R F_i$ admite una estructura de $R/\langle x \rangle$-módulo, entonces $R/\langle x \rangle \otimes_R F_i$ es $R/\langle x \rangle$-libre. Más aún, $R/\langle x \rangle \otimes \mathcal{F}$ es una resolución libre minimal de $M/\langle x \rangle M$ sobre $R/\langle x \rangle$, ya que los morfismos $\overline{d}_i$ en el complejo $R/\mathfrak{m} \otimes \mathcal{F}$ son todos cero. $\square$

Observación.

1. $\mathfrak{m}/\langle x\rangle$ es un ideal maximal de $R/\langle x\rangle$ si y sólo si $(R/\langle x\rangle)/(\mathfrak{m}/\langle x\rangle) \cong R/\mathfrak{m}$ es un campo.

2. $(R/\langle x\rangle, \mathfrak{m}/\langle x\rangle)$ es un anillo local.

Proposición 4.4.6 *Dado un anillo local noetheriano* $(R, \mathfrak{m})$*, para cada* R*-módulo libre finitamente generado* F*,* $depth(\mathfrak{m}, R) = depth(\mathfrak{m}, F)$*.*

Demostración. Como F es libre y finitamente generado, $F \cong \bigoplus_{i=1}^{n} R$ para algún $n > 0$.

$depth(\mathfrak{m}, R) = depth(\mathfrak{m}, F)$ si y sólo si $inf\{i : Ext_R^i(R/\mathfrak{m}, R) \neq 0\} = inf\{i : Ext_R^i(R/\mathfrak{m}, F) \neq 0\}$.

Tenemos que $Ext_R^i(R/\mathfrak{m}, F) \cong Ext_R^i(R/\mathfrak{m}, \bigoplus_{i=1}^{n} R) \cong \bigoplus Ext_R^i(R/\mathfrak{m}, R) = (Ext_R^i(R/\mathfrak{m}, R))^n$. Entonces $Ext_R^i(R/\mathfrak{m}, F) = 0$ si y sólo si $Ext_R^i(R/\mathfrak{m}, R) = 0$. Por lo tanto $depth(\mathfrak{m}, R) = depth(\mathfrak{m}, F)$. □

Teorema 4.4.7 (Fórmula de Auslander-Buchsbaum) *Si* $(R, \mathfrak{m})$ *es un anillo local noetheriano y* $M \neq 0$ *es un* R*-módulo finitamente generado con dimensión proyectiva finita, entonces*

$$pd_R(M) = depth(\mathfrak{m}, R) - depth(\mathfrak{m}, M).$$

Demostración. Usaremos inducción sobre $depth(\mathfrak{m}, R)$.

Supongamos que $depth(\mathfrak{m}, R) = 0$. Por hipótesis M tiene una resolución libre minimal

$$\mathcal{F} : 0 \longrightarrow F_n \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{d_1} F_0 \xrightarrow{\varphi} M \longrightarrow 0$$

con $n = pd_R(M)$.

Supongamos que $n \geq 1$. Como $depth(\mathfrak{m}, R) = 0$, entonces del ejemplo dado después de la definición 4.2.8, se sigue que $\mathfrak{m} \in AP(R)$. Además d_n es un monomorfismo, entonces por 4.4.4, $1_{R/\mathfrak{m}} \otimes d_n$ es inyectiva, es decir, $\ker(1_{R/\mathfrak{m}} \otimes d_n) = 0$, pero $0 \neq Tor_n^R(R/\mathfrak{m}, M) = \ker(1_{R/\mathfrak{m}} \otimes d_n)$, lo cual es una contradicción. Luego $n = 0$ y de esto se sigue que M es proyectivo sobre $(R, \mathfrak{m})$, lo cual implica que M es libre. Así por 4.4.6, $depth(\mathfrak{m}, R) = depth(\mathfrak{m}, M)$.

Ahora supongamos que $depth(\mathfrak{m}, R) > 0$ y siempre que $(R', \mathfrak{m}')$ es un anillo local noetheriano y $N \neq 0$ un R'-módulo finitamente generado con dimensión proyectiva finita tal que $depth(\mathfrak{m}', R') < depth(\mathfrak{m}, R)$, entonces

$$pd_{R'}(N) = depth(\mathfrak{m}', R') - depth(\mathfrak{m}', N).$$

Al considerar el caso $depth(\mathfrak{m}, M) > 0$, se sigue, del ejemplo dado después de la definición 4.2.8, que $\mathfrak{m} \notin AP(R)$ y $\mathfrak{m} \notin AP(M)$.

Afirmación. Hay un $x \in \mathfrak{m}$ tal que x es R-regular y M-regular.

En efecto, supongamos que para todo $x \in \mathfrak{m}$, $x \in ZD(R) = \bigcup_{P \in AP(R)} P$ o $x \in ZD(M) = \bigcup_{P \in AP(M)} P$, es decir, $\mathfrak{m} \subseteq (\bigcup_{P \in AP(R)} P) \bigcup (\bigcup_{P \in AP(M)} P)$. De B.2.9 tenemos que $AP(R)$ y $AP(M)$ son finitos, entonces por B.1.1 se sigue que

$\mathfrak{m} \in AP(R)$ o que $\mathfrak{m} \in AP(M)$, lo cual es una contradicción.

La afirmación junto con 4.4.3 y 4.4.5 nos da que

$$depth(\mathfrak{m}/\langle x\rangle, M\langle x\rangle M) = depth(\mathfrak{m}, M/\langle x\rangle M) = depth(\mathfrak{m}, M) - 1$$

$$depth(\mathfrak{m}/\langle x\rangle, R/\langle x\rangle) = depth(\mathfrak{m}, R/\langle x\rangle) = depth(\mathfrak{m}, R) - 1,$$

$$pd_R(M) = pd_{R/\langle x\rangle}(M/\langle x\rangle M).$$

Luego, por la hipótesis de inducción tenemos que

$$\begin{aligned} pd_R(M) &= pd_{R/\langle x\rangle}(M/\langle x\rangle M) \\ &= depth(\mathfrak{m}/\langle x\rangle, R/\langle x\rangle) - depth(\mathfrak{m}/\langle x\rangle, M\langle x\rangle M) \\ &= depth(\mathfrak{m}, R) - 1 - depth(\mathfrak{m}, M) + 1. \end{aligned}$$

Finalmente consideremos el caso $depth(\mathfrak{m}, M) = 0$.
Al tomar la sucesión exacta corta

$$0 \longrightarrow K \xrightarrow{i} F_0 \xrightarrow{\varphi} M \longrightarrow 0,$$

donde $K = \ker(\varphi)$ e i es la inclusión, tenemos por 4.4.6 que $depth(\mathfrak{m}, F_0) = depth(\mathfrak{m}, R) > 0$. Entonces por 4.4.1,

$$0 = depth(\mathfrak{m}, M) \geq min\{depth(\mathfrak{m}, K) - 1,\ depth(\mathfrak{m}, F_0)\} = depth(\mathfrak{m}, K) - 1$$

$$y\ depth(\mathfrak{m}, K) \geq min\{depth(\mathfrak{m}, F_0),\ depth(\mathfrak{m}, M) + 1\} = 1.$$

Así que $depth(\mathfrak{m}, K) = 1$.
(Notemos que $K \neq 0$, por lo cual tiene sentido hablar de $depth(\mathfrak{m}, K)$, pues si $K = 0$, entonces M es proyectivo, y de aquí $depth(\mathfrak{m}, M) = depth(\mathfrak{m}, R) > 0$, lo cual es una contradicción).

Ahora fijémonos en el complejo

$$0 \longrightarrow F_n \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{d_1} K \longrightarrow 0,$$

el cual es una resolución libre de K, entonces $pd(K) \leq n - 1 = pd(M) - 1$.

Supongamos que $pd(K) = j < n - 1$ para algún $j \in \mathbb{N} \cup \{0\}$, o sea que hay una resolución libre de K

$$0 \longrightarrow F'_j \longrightarrow \cdots \longrightarrow F'_1 \xrightarrow{d'_1} F'_0 \xrightarrow{\varphi'} K \longrightarrow 0,$$

la cual nos da otra resolución libre de M, a saber:

$$0 \longrightarrow F'_j \longrightarrow \cdots \longrightarrow F'_1 \xrightarrow{d'_1} F'_0 \xrightarrow{i \circ \varphi'} F_0 \longrightarrow M \longrightarrow 0.$$

De este modo tenemos una resolución proyectiva de M de longitud $j + 1 < n = pd(M)$, lo que contradice la definición de dimensión proyectiva. Por lo tanto, $pd(K) = pd(M) - 1$.

Al igual que como se hizo en el caso $depth(\mathfrak{m}, M) > 0$, tenemos que $pd(K) = depth(\mathfrak{m}, R) - depth(\mathfrak{m}, K)$. Luego

$$pd(M) - 1 = depth(\mathfrak{m}, R) - depth(\mathfrak{m}, M) - 1.$$

□

Observación. La teoría de profundidad nos prepara para el estudio del *Teorema de Hilbert-Burch*, el cual establece lo siguiente:

Sea R un anillo noetheriano e $I \neq 0$ un ideal propio de R con una resolución libre de longitud 1, $0 \longrightarrow F_1 \xrightarrow{\varphi_1} F_0 \longrightarrow I \longrightarrow 0$ *. Si $rango(F_1) = t$, entonces $rango(F_0) = t + 1$. Fijando bases para F_0 y F_1, entonces φ_1 puede representarse por una matriz $(t+1) \times t$. Haciendo $d_i = (-1)^i D_i$, donde D_i es el determinante de la matriz $t \times t$ que se forma eliminando la i-ésima fila de la matriz φ_1, entonces $I_t(\varphi_1) = \langle d_1, \ldots, d_{t+1} \rangle$. Se garantiza también que existe $a \in R$ tal que a no es divisor de cero e $I = aI_t(\varphi_1)$. Más aún, $depth(I_t(\varphi_1)) = 2$.*

Recíprocamente, si $a \in R$ no es divisor de cero y φ es una matriz $(t+1) \times t$ con entradas en R tal que $depth(I_t(\varphi)) \geq 2$, entonces el ideal $I = aI_t(\varphi)$ tiene una resolución libre de longitud 1.

Si bien el teorema no trata con ideales de dimensión proyectiva mayor que 1, éste ha encontrado aplicaciones, por ejemplo, en el Problema de Levantamiento de Grothendieck, en la teoría de singularidades racionales, en teoría de deformación y en la teoría de eslabonamiento. Todas estas aplicaciones descansan en el hecho de que el Teorema de Hilbert-Burch da un tipo de “forma genérica” para ideales perfectos de profundidad 2.

Apéndice A

Localización

Se generaliza el proceso por medio del cual se construye el campo de fracciones de un dominio entero.

Sea R un anillo y sea S un subcojunto multiplicativamente cerrado de R, es decir, $1 \in S$ y S es cerrado respecto a la multiplicación. Se define en $R \times S$ una relación $\sim$ de la siguiente forma:

$$(r, s) \sim (r', s') \text{ si y sólo si } u(s'r - sr') = 0 \text{ para algún } u \in S.$$

Dicha relación es una relación de equivalencia. Con r/s se denota a la clase de equivalencia de (r, s) y con $S^{-1}R$ al conjunto de las clases de equivalencia. Se definen operaciones en $S^{-1}R$ para hacer de él un anillo del modo siguiente:

$$(r/s) + (r'/s') = (s'r + sr')/ss' \qquad \text{y} \qquad (r/s)(r'/s') = rr'/ss',$$

donde el neutro aditivo es $0/1$, el cual coincide con $0/s$ para cada $s \in S$. El inverso aditivo de r/s es $-(r/s) = (-r)/s$ y el elemento unitario es $1/1$, que coincide con s/s para cada $s \in S$. El anillo $S^{-1}R$ se denomina **anillo de fracciones**. Hay además un morfismo de anillos $f : R \to S^{-1}R$ que está definido por $f(r) := r/1$, que en general no es inyectivo.

Si P es un ideal primo de R, el conjunto $S = R - P$ es multiplicativamente cerrado. En este caso $S^{-1}R$ se denota por R_P, el cual es un anillo local. El proceso de pasar de R a R_P se denomina **localización** en P.

La construcción de $S^{-1}R$ se puede hacer sobre un R-módulo M en lugar del anillo R, para obtener el $S^{-1}R$-módulo $S^{-1}M$ con las operaciones de suma y producto por escalar siguientes:

$$(m/s) + (m'/s') = (s'm + sm')/ss' \qquad \text{y} \qquad (r/s)(m/s') = rm/ss'.$$

Nuevamente, si P es primo, se escribe M_P en lugar de $S^{-1}M$, donde $S = R - P$.

Concluimos esta serie de comentarios con lo siguiente: si $u : M \to N$ es un morfismo de R-módulos, entonces la aplicación $S^{-1}u : S^{-1}M \to S^{-1}N$ definida por $S^{-1}u(m/s) = u(m)/s$, es un morfismo de $S^{-1}R$-módulos y $S^{-1}(v \circ u) = S^{-1}v \circ S^{-1}u$.

Proposición A.0.1 *Si la sucesión de R-módulos* $M \xrightarrow{u} N \xrightarrow{v} T$ *es exacta en* N*, entonces* $S^{-1}M \xrightarrow{S^{-1}u} S^{-1}N \xrightarrow{S^{-1}v} S^{-1}T$ *es exacta en* $S^{-1}N$*.*

Demostración. Demostración. Como $v \circ u = 0$, entonces $0 = S^{-1}(0) = S^{-1}(v \circ u) = S^{-1}v \circ S^{-1}u$, esto es, $Im(S^{-1}u) \subseteq \ker(S^{-1}v)$.

Sólo falta probar que $\ker(S^{-1}v) \subseteq Im(S^{-1}u)$. Si $n/s \in \ker(S^{-1}v)$, $0 = S^{-1}v(n/s) = v(n)/s$, esto es, $(v(n), s) \sim (0, 1)$. Entonces hay un $w \in S$ tal que $wv(n) = v(wn) = 0$, o sea que , $wn \in \ker(v) = Im(u)$. De esto se obtiene que $wn = u(m)$ para algún $m \in M$. Así, $n/s = wn/ws = u(m)/ws \in Im(S^{-1}u)$. $\square$

Proposición A.0.2 *Si* N *es un submódulo de* M*, la aplicación* $S^{-1}N \to S^{-1}M$ *es inyectiva y por lo tanto* $S^{-1}N$ *puede considerarse como un submódulo de* $S^{-1}M$*.*

Demostración. Como la sucesión $0 \longrightarrow N \xrightarrow{i} M$ es exacta, entonces la sucesión $0 \longrightarrow S^{-1}N \xrightarrow{S^{-1}i} S^{-1}M$ es exacta. De esta forma, $S^{-1}N$ es isomorfo a un submódulo de $S^{-1}M$. $\square$

Proposición A.0.3 *Sea* I *un ideal de* R *y sean* N *y* T *submódulos de un R-módulo* M*, entonces*

(1) $S^{-1}(N + T) = S^{-1}N + S^{-1}T$.

(2) $S^{-1}(N \cap T) = S^{-1}N \cap S^{-1}T$.

(3) *Los* $S^{-1}R$*-módulos* $S^{-1}(M/N)$ *y* $(S^{-1}M)/(S^{-1}R)$ *son isomorfos.*

(4) $S^{-1}I$ *es isomorfo a un ideal propio de* $S^{-1}R$ *si y sólo si* $S \cap I = \emptyset$*.*

Demostración.

(1) Sea $x/s \in S^{-1}(N + T)$, con $x \in N + T$ y $s \in S$. Entonces $x = n + t$ con $n \in N$ y $t \in T$. Luego, $x/s = (n + t)/s = (n/s) + (t/s) \in S^{-1}N + S^{-1}T$. Recíprocamente, sea $x/s \in S^{-1}N + S^{-1}T$ con $x \in M$ y $s \in S$. Entonces $x/s = (n/s_1) + (t/s_2)$ con $n \in N$, $t \in T$ y $s_1, s_2 \in S$. $(n/s_1) + (t/s_2) = (s_2n + s_1t)/s_1s_2 \in S^{-1}(N + T)$.

(2) $N \cap T$ es un submódulo de N y de T. De la proposición anterior tenemos que $S^{-1}(N \cap T) \subseteq S^{-1}N$ y $S^{-1}(N \cap T) \subseteq S^{-1}T$. Entonces $S^{-1}(N \cap T) \subseteq S^{-1}N \cap S^{-1}T$. Recíprocamente, si $x \in S^{-1}N \cap S^{-1}T$, $x \in S^{-1}N$ y $x \in S^{-1}T$. Entonces $x = n/s$ y $x = t/s'$ con $n \in N$, $t \in T$ y $s, s' \in S$. De esto se sigue que hay un $u \in S$ tal que $u(s'n - st) = 0$. Luego, $n/s = us'n/us's = ust/us's \in S^{-1}(N \cap T)$.

(3) Como $0 \longrightarrow N \xrightarrow{i} M \xrightarrow{\pi} M/N \longrightarrow 0$ es una sucesión exacta, entonces la sucesión

$$0 \longrightarrow S^{-1}N \xrightarrow{S^{-1}i} S^{-1}M \xrightarrow{S^{-1}\pi} S^{-1}(M/N) \longrightarrow 0$$

es exacta. Así, $S^{-1}N \cong Im(S^{-1}i) = \ker(S^{-1}\pi)$ y por tanto $S^{-1}(M/N) \cong (S^{-1}M)/(S^{-1}N)$.

(4) ($\Rightarrow$) Supongamos que $s \in R$ tal que $s \in S \cap I$, entonces $1/1 = s/s \in S^{-1}I$. Luego, $S^{-1}I = S^{-1}R$.

($\Leftarrow$) Supongamos que $S^{-1}I = S^{-1}R$, entonces $1/1 = r/s$ para algún $r \in I$ y $s \in S$. De esto se sigue que hay un $s' \in S$ tal que $s'(s-r) = 0$, es decir, $S \ni s's = s'r \in I$,o sea que $S \cap I \neq \emptyset$.

□

Proposición A.0.4 *Si J es un ideal de $S^{-1}R$, entonces $J = S^{-1}I$, donde $I = f^{-1}(J)$.*

Demostración. Sea $r/s \in J$ con $r \in R$ y $s \in S$, entonces $f(r) = r/1 = (s/1)(r/s) \in J$ y por tanto $r \in f^{-1}(J) = I$. Así, $r/s \in S^{-1}I$. Recíprocamente, sea $r/s \in S^{-1}I$ con $r \in I$ y $s \in S$. Entonces $f(r) = r/1 \in J$. Luego, $r/s = (1/s)(r/1) \in J$. □

Proposición A.0.5 *Si P es un ideal de R, entonces $P \subseteq f^{-1}(S^{-1}P)$. La igualdad es válida si P es primo y $P \cap S = \emptyset$.*

Demostración. Si $x \in P$, $f(x) = x/1 \in S^{-1}P$. Ahora supongamos que P es primo y $P \cap S = \emptyset$, y sea $x \in f^{-1}(S^{-1}P)$. Entonces $f(x) = x/1 \in S^{-1}P$. Luego, existen $r \in P$ y $s \in S$ tales que $x/1 = r/s$, de lo cual se sigue que hay un $u \in S$ tal que $u(sx - r) = 0$. Así, $usx = ur \in P$, pero $us \notin P$ ya que $P \cap S = \emptyset$. Como P es primo, $x \in P$. □

Proposición A.0.6 *Si P es un ideal primo de R con $P \cap S = \emptyset$, entonces $S^{-1}P$ es un ideal primo de $S^{-1}R$.*

Demostración. Del inciso 4 en A.0.3 tenemos que $S^{-1}P$ es un ideal propio de $S^{-1}R$.

Sean x/s y x'/s' en $S^{-1}R$ tales que $(x/s)(x'/s') = xx'/ss' \in S^{-1}P$, entonces existen $r \in P$ y $u \in S$ tales que $xx'/ss' = r/u$. Luego hay un $v \in S$ tal que $v(uxx' - ss'r) = 0$ y por tanto $vuxx' = vss'r \in P$, con $vu \in S - P$. Entonces $xx' \in P$ con P primo, de donde $x \in P$ o $x' \in P$. Y de esto obtenemos que $x/s \in S^{-1}P$ o $x'/s' \in S^{-1}P$. □

Teorema A.0.7 *Hay una aplicación biyectiva entre el conjunto de ideales primos P de R que son ajenos con S y el conjunto de ideales primos Q de $S^{-1}R$, dada por*

$$P \to S^{-1}P \qquad y \qquad Q \to f^{-1}(Q).$$

Demostración. Sea P un ideal primo de R tal que $P \cap S = \emptyset$, entonces por la proposición anterior, $S^{-1}P$ es un ideal primo en $S^{-1}R$. Luego, por A.0.5, $f^{-1}(S^{-1}P) = P$.

Sea Q un ideal primo en $S^{-1}R$, entonces $f^{-1}(Q)$ es un ideal primo en R.

Veamos que $f^{-1}(Q) \cap S = \emptyset$. Supongamos que $f^{-1}(Q) \cap S \neq \emptyset$, entonces $Q = S^{-1}(f^{-1}(Q)) = S^{-1}R$ (la primera igualdad se da por A.0.4 y la segunda por (4) en A.0.3), lo cual es una contradicción.

Así, las aplicaciones $P \to S^{-1}P$ y $Q \to f^{-1}(Q)$ son inversa una de la otra. $\square$

Corolario A.0.8 *Si P es un ideal primo de R, los ideales primos del anillo local R_P están en correspondencia biyectiva con los ideales primos de R contenidos en P.*

Demostración. Basta tomar $S = R - P$ en el teorema anterior. $\square$

Proposición A.0.9 *Sea M un R-módulo. Son equivalentes:*

(1) $M = 0$.

(2) $M_P = 0$ *para todo ideal primo* P *de* R.

(3) $M_{\mathfrak{m}} = 0$ *para todo ideal maximal* $\mathfrak{m}$ *de* R.

Demostración. (1) $\Rightarrow$ (2) $\Rightarrow$ (3) son evidentes. Probemos que (3) $\Rightarrow$ (1). Supongamos que $M \neq 0$. Sea $m \neq 0$ en M y consideremos el ideal $Ann(m)$. Como $0 \neq m = 1m$, entonces $1 \notin Ann(m)$. Así, $Ann(m)$ es un ideal propio de R y por tanto hay un ideal maximal $\mathfrak{m}$ de R tal que $Ann(m) \subseteq \mathfrak{m}$. Pero $m/1 \in M_{\mathfrak{m}} = 0$, o sea que $m/1 = 0/1$. Entonces hay un $r \in R - \mathfrak{m}$ tal que $rm = 0$, lo cual nos dice que $r \in Ann(m)$. Además, $r \notin \mathfrak{m} \supseteq Ann(m)$, lo cual es una contradicción. $\square$

Apéndice B

Descomposición Primaria

B.1. Primos asociados

Teorema B.1.1 *Sean $P_1, P_2, \ldots, P_s$ $(s \geq 2)$ ideales en un anillo R, con P_1 y P_2 no necesariamente primos, pero $P_3, \ldots, P_s$ primos $(s \geq 3)$ y sea I un ideal de R. Si $I \subseteq \bigcup_{i=1}^{s} P_i$, entonces hay un i tal que $I \subseteq P_i$.*

Demostración. Supongamos que para todo i, $I \nsubseteq P_i$.

Afirmamos que I no está contenido en la unión de cualquier colección más pequeña de los P_i. Usemos inducción para probar esta afirmación.

El caso base es obvio por la suposición inicial en la demostración.

Supongamos que cualquier colección de cardinalidad mayor o igual a uno y menor que $s-1$ cumple lo dicho.

Ahora tomemos una colección con $s-1$ de los P_i, digamos $P_{i_1}, \ldots, P_{i_{s-1}}$; entonces $I \nsubseteq P_{i_1}$ e $I \nsubseteq \bigcup_{j=2}^{s-1} P_{i_j}$, o sea que existen $x_1, x_2 \in I$ tales que $x_1 \notin P_{i_1}$ y $x_2 \notin \bigcup_{j=2}^{s-1} P_{i_j}$. Si $I \subseteq \bigcup_{j=1}^{s-1} P_{i_j} = P_{i_1} \cup (\bigcup_{j=1}^{s-1} P_{i_j})$, entonces $x_1 \notin P_{i_1}$, $x_2 \in P_{i_1}$, $x_1 \in \bigcup_{j=2}^{s-1} P_{i_j}$ y $x_2 \notin \bigcup_{j=2}^{s-1} P_{i_j}$. Esto implica que $x_1 + x_2 \notin P_{i_1}$ y $x_1 + x_2 \notin \bigcup_{j=2}^{s-1} P_{i_j}$, de donde, $x_1 + x_2 \notin I$, lo cual es una contradicción. Por lo tanto $I \nsubseteq \bigcup_{j=1}^{s-1} P_{i_j}$.

De la afirmación se sigue que para cada i, hay un $x_i \in I$ tal que $x_i \notin \bigcup_{j \neq i} P_j$, pero $I \subseteq \bigcup_{i=1}^{s} P_i$, así que $x_i \in P_i$.

Si $s = 2$, $I \nsubseteq P_1$ e $I \nsubseteq P_2$ implica que $x_1 \in P_1$, $x_2 \notin P_1$, $x_1 \notin P_2$ y $x_2 \in P_2$. De esto se sigue que $x_1 + x_2 \notin P_1$ y $x_1 + x_2 \notin P_2$. Luego $x_1 + x_2 \notin P_1 \cup P_2 \supseteq I$, lo cual es una contradicción.

Supongamos que $s > 2$. Para cada $i \in \{1, \ldots, s-1\}$, $x_1 x_2 \cdots x_{s-1} \in P_i$ y $x_s \notin P_i$, entonces para cada $i \in \{1, \ldots, s-1\}$, $a = (x_1 x_2 \cdots x_{s-1}) + x_s \notin P_i$, esto es, $a \notin \bigcup_{i=1}^{s-1} P_i$. También tenemos que para cada $i \in \{1, \ldots, s-1\}$, $x_i \notin P_s$, entonces $x_1 x_2 \cdots x_{s-1} \notin P_s$, porque P_s es primo. Pero $x_s \in P_s$, entonces $a \notin P_s$. Luego, $a \notin \bigcup_{i=1}^{s} P_i \supseteq I$, lo cual es una contradicción. □

Definición B.1.2 *Sean M un R-módulo y P un ideal primo de R. Diremos* *que P es un* ***primo asociado*** *de M si P es el anulador de algún $x \in M$ con $x \neq 0$. El conjunto de primos asociados de M es denotado por $AP(M)$.*

Proposición B.1.3 *Un ideal primo P es un primo asociado de M si y sólo si hay un morfismo de R-módulos inyectivo de R/P a M. Por consiguiente, si N es un submódulo de M entonces $AP(N) \subseteq AP(M)$.*

Demostración. Para la primera implicación tomamos a P un ideal primo tal que $P = Ann(x)$ para algún $x \in M$ con $x \neq 0$. El morfismo buscado es el que a $r + P \in R/P$ le asigna rx.

Para el recíproco suponemos que hay un R-morfismo inyectivo $\varphi : R/P \to M$ y sea $x = \varphi(1 + P)$. Como P es primo, $1 + P \neq 0$ y por tanto $x \neq 0$.

Veamos que $P = Ann(x)$

Si $r \in P$, entonces $0 = \varphi(r + P) = r\varphi(1 + P) = rx$, o sea que $r \in Ann(x)$.

Si $r \in Ann(x)$, se sigue que $0 = rx = r\varphi(1 + P) = \varphi(r + P)$, entonces $r + P = 0$, es decir, $r \in P$.

Por lo tanto, $P = Ann(x)$.

Por otra parte, $P \in AP(N)$ implica que hay un morfismo inyectivo $\varphi : R/P \to N$, entonces $i \circ \varphi : R/P \to M$ es un R-morfismo inyectivo (donde i es la inclusión de N en M). Así, $P \in AP(M)$. □

Proposición B.1.4 *Si $M = 0$ entonces $AP(M) = \emptyset$. El recíproco se cumple si R es un anillo noetheriano.*

Demostración. Como no hay elementos distintos de cero en el módulo cero, entonces M no tiene primos asociados. Ahora supongamos que R es noetheriano y que $M \neq 0$, entonces para cada $x \in M$ con $x \neq 0$ siempre es posible hablar del anulador de x, es decir, para todo $x \in M$ con $x \neq 0$, $Ann(x) \neq \emptyset$. Como R es noetheriano, se cumple la condición maximal, esto es, el conjunto $C = \{I : I = Ann(x)$ para algún $x \in M$ con $x \neq 0\}$ tiene un elemento maximal I.

Veamos que $I \neq R$ y que I es un ideal primo de R.

Si $Ann(x) = I = R$, entonces $x = 1x = 0$, lo cual es una contradicción.

Supongamos que $ab \in I$ con $a \notin I$, entonces $abx = 0$ y $ax \neq 0$, lo que implica que $b \in Ann(ax)$. Pero $I = Ann(x) \subseteq Ann(ax)$ e I es maximal en C, entonces $b \in I$.

De esta forma tenemos que I es primo y por lo tanto $AP(M) \neq \emptyset$. □

Proposición B.1.5 *Para todo ideal primo P de R, $AP(R/P) = \{P\}$.*

Demostración. Al tomar el morfismo identidad en R/P, tenemos por B.1.3 que $P \in AP(R/P)$. Ahora tomemos un $I \in AP(R/P)$, luego existe $r \in R - P$ tal que $I = Ann(r+P)$. Entonces $x \in I$ si y sólo si $xr \in P$ si y sólo si $x \in P$. □

Observación. Si $r \in R - P$, entonces $Ann(r + P) = \{s \in R \mid sr \in P\} = P$.

Proposición B.1.6 *Sea $ZD(M) = \{r \in R : rm = 0$ para algún $m \in M$ con $m \neq 0\}$ el conjunto de* ***divisores de cero*** *de M. Entonces $\bigcup_{P \in AP(M)} P \subseteq Z(M)$. La igualdad es válida si R es noetheriano.*

Demostración. La inclusión primera se sigue directamente de la definición de primo asociado.

Ahora supongamos que R es noetheriano y que $r \in ZD_R(M)$, entonces hay un $m \in M$ con $m \neq 0$ tal que $rm = 0$, así $\langle m \rangle \neq 0$. Entonces por B.1.4, existe un ideal primo P de R tal que P es primo asociado de $\langle m \rangle$, o sea que $P = Ann(sm)$ para algún $s \in R$ y $s \neq 0$. Pero también tenemos que $rm = 0$, luego $rsm = 0$, de donde se sigue que $r \in Ann(sm) = P \in AP\langle m \rangle \subseteq AP(M)$ (la última contensión se garantiza por B.1.3). Por lo tanto, $r \in \bigcup_{P \in AP(M)} P$. □

B.2. Descomposición primaria

Sea N un submódulo de un R-módulo M y sea $r \in R$. Definimos $\lambda_r : M/N \to M/N$ como multiplicación por r.

Definición B.2.1 *N es un **submódulo primario** de M si $N \neq M$ y para cada $r \in R$, λ_r es inyectiva o nilpotente.*

Observación.

1. La inyectividad de λ_r significa que $N = \ker(\lambda_r) = \{m+N : rm \in N\}$, esto es, para cada $m \in M$, $rm \in N$ implica $m \in N$. Mientras que la nilpotencia de λ_r indica que hay un $n \in \mathbb{N}$ tal que para cada $m \in M$, $r^n(m+N) = 0$. Esto equivale a que $r^n \in Ann(M/N)$, o sea que $r \in rad(Ann(M/N))$, donde $rad(Ann(M/N)) := \{r \in R : r^n \in Ann(M/N) \text{ para algún } n \in \mathbb{N}\}$ y es un ideal de R.

2. λ_r no puede ser inyectiva y nilpotente a un mismo tiempo, ya que de ser así, la nilpotencia nos dice que $r^n M = r(r^{n-1}M) \subseteq N$, y de esto, la inyectividad implica que $r^{n-1}M \subseteq N$. Luego, siguiendo un argumento inductivo se sigue que $M = N$, lo que contradice que N sea un submódulo propio. De esta forma tenemos que si N es un submódulo primario de M, entonces $rad(Ann(M/N)) = \{r \in R \mid \lambda_r \text{ no es inyectiva }\}$.

Proposición B.2.2 *$rad(Ann(M/N))$ es un ideal primo.*

Demostración. $rad(Ann(M/N)) \neq R$, ya que $1 \notin rad(Ann(M/N))$. Sean $r, r' \in R$ tales que $r \notin rad(Ann(M/N))$ y $r' \notin rad(Ann(M/N))$, es decir, λ_r y $\lambda_{r'}$ son inyectivas. Entonces $\lambda_r \circ \lambda_{r'} = \lambda_{rr'}$ es inyectiva. o sea que, $rr' \notin rad(Ann(M/N))$. □

Definición B.2.3 *Si $P = rad(Ann(M/N))$, diremos que N es P-**primario**.*

Definición B.2.4 *Una **descomposición primaria** de un submódulo N de M es una expresión de N como una intersección finita, $\cap_{i=1}^r N_i$, donde los N_i son submódulos P_i-primarios. La descomposición es **reducida** si los P_i son distintos y si ninguna de las componentes N_i pueden omitirse de la intersección, es decir, si $N_i \not\supseteq \cap_{j \neq i} N_j$ $(1 \leq i \leq r)$.*

Proposición B.2.5 *Si $N_1, \dots, N_r$ son P-primarios, entonces $\cap_{i=1}^{r} N_i$ es P-primario.*

Demostración. Hagamos la prueba por inducción.

El caso base es obvio.

Supongamos que para cualquier familia finita $N_1, \dots, N_j$ $(j < t)$ de submódulos P-primarios, $\cap_{i=1}^{j} N_i$ es P-primario.

Sea $N_1, \dots, N_t$ una familia de submódulos P-primarios de M. Hacemos $N = \cap_{i=1}^{t-1} N_i$. Por hipótesis, $rad(Ann(M/N)) = rad(Ann(M/N_t)) = P$.

Debemos probar que para cada $r \in R$, $\lambda_r : M/(N \cap N_t) \to M/(N \cap N_t)$ es inyectiva o nilpotente. Sea $r \in R$ y supongamos que λ_r no es nilpotente. Sea $m \in M$ tal que $rm \in N \cap N_t$. Como N y N_t son P-primarios, $m \in N \cap N_t$, y así, λ_r es inyectiva.

Sólo falta probar que $rad(Ann(M/N \cap N_t)) = P$.

Sea $x \in rad(Ann(M/N \cap N_t))$, entonces hay un $n \in \mathbb{N}$ tal que $x^n M \subseteq N \cap N_t$, lo cual implica que $x^n M \subseteq N$ y $x^n M \subseteq N_t$. De aquí se sigue que $x \in rad(Ann(M/N))$ y $x \in rad(Ann(M/N_t))$. Luego $x \in P$.

Sea $x \in P$, entonces existen $n_1, n_2 \in \mathbb{N}$ tales que $x^{n_1} M \subseteq N$ y $x^{n_2} M \subseteq N_t$. Luego, $x^{n_1+n_2} M \subseteq N \cap N_t$, o sea que $x \in rad(Ann(M/N \cap N_t))$. $\square$

Definición B.2.6 *El submódulo propio N de M es **irreducible** si N no puede ser expresado como $N_1 \cap N_2$, con N contenido propiamente en los submódulos N_1 y N_2.*

Proposición B.2.7 *Si N es un submódulo irreducible de un módulo noetheriano M, entonces N es primario.*

Demostración. Haremos la prueba por contraposición. Supongamos que N no es primario, esto es, para algún $r \in R$, $\lambda_r : M/N \to M/N$ no es inyectiva y no es nilpotente. Entonces, $\ker(\lambda_r) \neq 0$ y para cada $n \in \mathbb{N}$, $\lambda_r^n \neq 0$. Entonces hay un $m_0 \in M - N$ tal que $rm_0 \in N$. Luego, $r^2 m_0 \in N$, esto es, $m_0 \in \ker(\lambda_r^2)$. Siguiendo de esta forma tenemos que $m_0 \in \ker(\lambda_r^n)$ para cada $n \in \mathbb{N}$. Más aún, para cada $m \in \ker(\lambda_r)$, $m \in \ker(\lambda_r^n)$ para cada $n \in \mathbb{N}$. De esta forma se tiene una sucesión creciente de submódulos de M/N

$$\ker(\lambda_r) \subseteq \ker(\lambda_r^2) \subseteq \ker(\lambda_r^3) \subseteq \cdots .$$

Como M es noetheriano, se sigue que M/N es noetheriano, entonces hay un $n_0 \in \mathbb{N}$ tal que $\ker(\lambda_r^{n_0}) = \ker(\lambda_r^{n_0+1}) = \cdots$. Sean $\varphi = \lambda_r^{n_0}$ y $\pi : M \to M/N$ la proyección canónica y sean $N_1 = \pi^{-1}(\ker(\varphi))$ y $N_2 = \pi^{-1}(Im(\varphi))$. Afirmamos que $N = N_1 \cap N_2$, $N \subsetneq N_1$ y $N \subsetneq N_2$.

Sea $x \in N$, entonces $\pi(x) = 0 \in \ker(\lambda_r^{n_0}) \cap Im(\lambda_r^{n_0})$. Recíprocamente, $x \in N_1 \cap N_2$ implica que $\pi(x) \in \ker(\varphi) \cap Im(\varphi)$. Luego, $\varphi(\pi(x)) = 0$ y $\pi(x) = \varphi(y)$ para algún $y \in M/N$. Entonces $0 = \varphi(\pi(x)) = \varphi(\varphi(y)) = \varphi^2(y)$. De esto se sigue que $y \in \ker(\varphi^2) = \ker(\varphi)$, es decir, $0 = \varphi(y) = \pi(x)$. Así que, $x \in N$. Por lo tanto, $N = N_1 \cap N_2$.

Sabemos también que $\ker(\varphi) \neq 0$ e $Im(\varphi) \neq 0$. Así podemos tomar un $y \neq 0$ en $\ker(\varphi)$, entonces hay un $x \in M$ tal que $\pi(x) = y$, esto es, $x \in \pi^{-1}(y) \subseteq \pi^{-1}(\ker(\varphi)) = N_1$. Además, $x \notin N$, porque $\pi(x) = y \neq 0$.

Análogamente se prueba que $N \subsetneq N_2$. □

Teorema B.2.8 *Si N es un submódulo propio de un módulo noetheriano M, entonces N tiene una descomposición primaria. Más aún, N tiene una descomposición primaria reducida.*

Demostración. Mostraremos que N puede ser expresado como una intersección finita de submódulos irreducibles de M.

Sea S la familia de submódulos de M que no admiten una representación de esta forma. Si $S \neq \emptyset$, S tiene un elemento maximal N, porque M es noetheriano. Por la definición de S, N no es irreducible, o sea que puede ser expresado como $N = N_1 \cap N_2$ con $N \subsetneq N_1$ y $N \subsetneq N_2$. Luego, por la maximalidad de N, N_1 y N_2 pueden ser expresados como intersecciones finitas de submódulos irreducibles de M. Y así, N también puede expresarse de esta forma, lo que contradice que $N \in S$. Por lo tanto, $S = \emptyset$. De esta forma, todo submódulo propio N de M admite una representación como $N = \cap_{i=1}^{r} N_i$, donde los N_i son irreducibles. Luego, de la proposición anterior, los N_i son P_i-primarios. Además, la irreducibilidad de los N_i garantiza la minimalidad de dicha intersección, esto es, que N no puede expresarse como una intersección de una subcolección propia de los N_i. Sabemos también de B.2.5 que la intersección de submódulos P-primarios es P-primaria, así que la minimalidad de tal intersección implica que los P_i son distintos. □

Teorema B.2.9 *Si M es un módulo finitamente generado sobre un anillo noetheriano R, entonces $AP(M)$ es finito.*

Demostración. Si $M = 0$, $AP(M) = \emptyset$.

Supongamos que $M \neq 0$. Del teorema anterior se sigue que 0 tiene una descomposición primaria reducida $\cap_{i=1}^{r} N_i$, donde N_i es P_i-primario.

Se afirma que $AP(M) = \{P_1, \ldots, P_r\}$. Sea $P \in AP(M)$, entonces hay un $m \neq 0$ en M tal que $P = Ann(m)$. Como $m \neq 0$, $m \notin \cap_{i=1}^{r} N_i$, o sea que hay un N_{i_0} tal que $x \notin N_{i_0}$. Reordenando a los N_i, de modo que $N_1, \ldots, N_j$ sea la subcolección de los N_i que no contienen a m. Sabemos que los N_i son P_i-primarios, esto es, $P_i = rad(Ann(M/N_i))$. Como P_i es finitamente generado, entonces hay un $n_i \in \mathbb{N}$ tal que $P_i^{n_i} M \subseteq N_i$. Luego, $(\cap_{i=1}^{j} P_i^{n_i}) m \subseteq \cap_{i=1}^{r} N_i = 0$, (no olvidando que $m \in \cap_{i=j+1}^{r} N_i$) y así, $\cap_{i=1}^{j} P_i^{n_i} \subseteq Ann(m) = P$, el cual es primo. De esto obtenemos que para algún $1 \leq i_1 \leq j$, $P_{i_1} \subseteq P$.

Veamos que $P_{i_1} = P$, es decir, que $P \subseteq P_{i_1}$.

Sea $x \in P$, entonces $xm = 0$. Como $m \notin P_{i_1}$, $\lambda_x : M/N_{i_1} \to M/N_{i_1}$ no es inyectiva, o sea que $x \in rad(Ann(M/N_{i_1})) = P_{i_1}$.

Ahora mostremos que cada P_i está en $AP(M)$. Sin pérdida de generalidad, tomemos a P_1. Como la descomposición es reducida, $N_1 \not\supseteq \cap_{i=2}^{r} N_i$. Sea $x \in \cap_{i=2}^{r} N_i$ tal que $x \notin N_1$. Análogamente a lo hecho en la primera parte de la prueba, tenemos que el conjunto $A = \{n \in \mathbb{N} : P_1^n x \subseteq N_1\} \neq \emptyset$, entonces A

tiene mínimo. Sea $n_0 = min(A)$. Luego, $P_1^{n_0-1}M \nsubseteq N_1$. Sea $y \in P_1^{n_0-1}x - N_1$, de aquí, $y \neq 0$ y $P_1 y \subseteq P_1^{n_0-1}x \subseteq N_1$.

Se afirma que $P_1 = Ann(y)$.

Como $x \in \cap_{i=2}^{r} N_i$, $P_1^{n_0}x \subseteq \cap_{i=2}^{r} N_i$. Entonces $P_1 y \subseteq \cap_{i=1}^{r} N_i = 0$, esto es, $P_1 \subseteq Ann(y)$. Por otra parte, si $x \in Ann(y)$, $xy = 0$. Además, $y \notin N_1$, entonces $\lambda_x : M/N_1 \to M/N_1$ no es inyectiva, o sea que $x \in rad(Ann(M/N_1)) = P_1$. □

B.3. Soporte de un módulo

Definición B.3.1 *El **soporte** de un R-módulo M, denotado por $Supp(M)$, es el conjunto de todos los ideales primos P de R tales que $M_P \neq 0$.*

Observación. $Supp(M) = \emptyset$ si y sólo si $M_P = 0$ para todo ideal primo P si y sólo si $M = 0$ (la útima igualdad se da por A.0.9).

Si I es un ideal de R, sea $V(I)$ el conjunto de todos los ideales primos que contienen a I.

Proposición B.3.2 *$Supp(R/I) = V(I)$.*

Demostración. Si $P \in V(I)$, P es un ideal primo de R tal que $I \subseteq P$. Entonces, por A.0.2 y A.0.8, $I_P = S^{-1}I \subseteq S^{-1}P \neq R_P$. Luego, por A.0.3, $0 \neq (R_P/I_P) \cong (R/I)_P$, es decir, $P \in Supp(R/I)$.

Si $P \in Supp(R/I)$, $S^{-1}I = I_P \neq R_P$. Luego, $I_P \subseteq \mathfrak{m}$, donde $\mathfrak{m}$ es el ideal maximal de R_P. Como $\mathfrak{m}$ es primo en R_P, $f^{-1}(\mathfrak{m})$ es un ideal primo de R y por A.0.8, $f^{-1}(\mathfrak{m}) \subseteq P$. Entonces, $\mathfrak{m} = S^{-1}(f^{-1}(\mathfrak{m})) \subseteq S^{-1}P$. Como $\mathfrak{m}$ es maximal en R_P, $\mathfrak{m} = S^{-1}P$. Sea $r \in I$, entonces $r/1 \in I_P \subseteq \mathfrak{m} = S^{-1}P$, lo cual implica que existen $r' \in P$ y $s \in R - P$ tales que $r/1 = r'/s$. De esto se sigue que $u(sr - r') = 0$ para algún $u \in R - P$, esto es, $usr = ur' \in P$ con $us \in R - P$. Como P es primo, $r \in P$. □

Proposición B.3.3 *Si $0 \longrightarrow M \xrightarrow{u} N \xrightarrow{v} T \longrightarrow 0$ es una sucesión exacta, entonces $Supp(N) = Supp(M) \cup Supp(T)$.*

Demostración. Como $0 \longrightarrow M \xrightarrow{u} N \xrightarrow{v} T \longrightarrow 0$ es una sucesión exacta, entonces $0 \longrightarrow M_P \xrightarrow{S^{-1}u} N_P \xrightarrow{S^{-1}v} T_P \longrightarrow 0$ también es una sucesión exacta. Sea $P \in Supp(N) - Supp(M)$, entonces $N_P \neq 0$ y $M_P = 0$. De esto se sigue que $S^{-1}v$ es inyectiva, luego, $S^{-1}v$ es un isomorfismo. Esto implica que $T_P \neq 0$, o sea que, $P \in Supp(T)$.

Ahora supongamos que $P \in Supp(M) \cup Supp(T)$. Si $P \in Supp(M)$, $M_P \neq 0$. Además M_P es isomorfo a un submódulo de N_P, luego, $N_P \neq 0$, esto es, $P \in Supp(N)$. Por otra parte, si $P \in Supp(T)$, $T_P \neq 0$, entonces $N_P \neq 0$, o sea que $P \in Supp(N)$. □

Proposición B.3.4 *Si $M = \sum M_i$, entonces $Supp(M) = \bigcup Supp(M_i)$.*

Demostración. Sea $P \in Supp(M)$, entonces $0 \neq M_P = (\sum M_i)_P = \sum (M_i)_P$ (la última igualdad es válida porque los elementos en $\sum M_i$ y $\sum (M_i)_P$ son sumas finitas). Entonces no todos los $(M_i)_P$ son cero, así que $P \in Supp(M_i)$ para algún i, esto es, $P \in \bigcup Supp(M_i)$.

Sea $P \in \bigcup Supp(M_i)$, entonces para algún i, $0 \neq (M_i)_P \subseteq \sum (M_i)_P = (\sum M_i)_P = M_P$. De esta forma $P \in Supp(M)$. □

Teorema B.3.5 *Si M es un R-módulo finitamente generado, entonces*

$$Supp(M) = V(Ann(M)).$$

Demostración. Sea $M = Rm_1 + \cdots + Rm_n$. Entonces por B.3.4, $Supp(M) = \bigcup_{i=1}^n Supp(Rm_i)$. Tomando el epimorfismo $f_i : R \to Rm_i$ que viene dado por $f_i(r) = rm_i$, tenemos que $R/Ann(m_i) \cong Rm_i$, pues $Ann(m_i) = \ker(f_i)$. De esto y B.3.2,

$$Supp(M) = \bigcup_{i=1}^n Supp(Rm_i) = \bigcup_{i=1}^n Supp(R/Ann(m_i)) = \bigcup_{i=1}^n V(Ann(m_i)).$$

Más aún, $\bigcup_{i=1}^n V(Ann(m_i)) = V(Ann(M))$. En efecto, si $P \in V(Ann(m_i))$ para algún i, entonces $P \supseteq Ann(m_i) \supseteq Ann(M)$. Recíprocamente, si $P \in V(Ann(M))$, se sigue $P \supseteq Ann(M) = \bigcap_{i=1}^n Ann(m_i) \supseteq Ann(m_1) \cdots Ann(m_n)$. Entonces $P \supseteq Ann(m_i)$ para algún i. □

Proposición B.3.6 *Si M es un módulo finitamente generado sobre un anillo noetheriano R, entonces $\bigcap_{P \in AP(M)} P = rad(Ann(M))$.*

Demostración. Si $M = 0$, $AP(M) = \emptyset$. Así que

$$\bigcap_{P \in AP(M)} P = \{r \in R \mid \text{para cada } P \in AP(M),\ r \in P\} = R \qquad \text{y}$$

$$rad(Ann(M)) = \{r \in R \mid r^n M = 0 \text{ para algún } n \in \mathbb{N}\} = R.$$

Sea $M \neq 0$. Sabemos que el módulo cero tiene una descomposición primaria reducida, $0 = \bigcap_{i=1}^r N_i$, donde cada N_i es P_i-primario y $AP(M) = \{P_1, \ldots, P_r\}$.

Si $x \in \bigcap_{P \in AP(M)} P$, se sigue que para cada i, $x \in P_i = rad(Ann(M/N_i))$. Entonces, para cada i, hay un $n_i \in \mathbb{N}$ tal que $x^{n_i} M \subseteq N_i$. Sea $n = max\{n_i\}$, entonces $x^n M \subseteq N_i$ para cada i. Luego, $x^n M \subseteq \bigcap_{i=1}^r N_i = 0$, es decir, $x \in rad(Ann(M))$.

Recíprocamente, si $x \in rad(Ann(M))$, se sigue que hay un $n \in \mathbb{N}$ tal que $x^n M = 0 = \bigcap_{i=1}^r N_i$. Luego, para cada i, $x^n M \subseteq N_i$. Entonces, para cada i, $x \in rad(Ann(M/N_i)) = P_i$, que son los elementos de $AP(M)$. □

Proposición B.3.7 *Sea M es un módulo finitamente generado sobre un anillo noetheriano R y sea P un idea primo de R. Las siguientes condiciones son equivalentes:*

(1) *$P \in Supp(M)$.*

(2) *Hay un $Q \in AP(M)$ tal que $Q \subseteq P$.*

(3) *$Ann(M) \subseteq P$.*

Demostración. (1) $\Rightarrow$ (2) Sea $P \in Supp(M)$ y supongamos que para todo $Q \in AP(M) = \{P_1, \ldots, P_r\}$, $Q \nsubseteq P$, esto es, que para todo $i \in \{1, \ldots, r\}$, hay un $a_i \in Q$ y $a_i \notin P$. Como P es primo, $\bigcap_{i=1}^r P_i \ni a_1 \cdots a_r \notin P$, que implica $\bigcap_{i=1}^r P_i \nsubseteq P$ con $\bigcap_{i=1}^r P_i = rad(Ann(M)) \supseteq Ann(M)$. Entonces $Ann(M) \nsubseteq P \in Supp(M)$, lo cual es una contradicción.

(2) $\Rightarrow$ (3) Por hipótesis hay un $P_i \in AP(M) = \{P_1, \ldots, P_r\}$ tal que $P \supseteq P_i$. Tenemos también que $P_i \supseteq \bigcap_{i=1}^r P_i = rad(Ann(M)) \supseteq Ann(M)$. Así, $P \supseteq Ann(M)$.

(3) $\Rightarrow$ (1) Se sigue de B.3.5. □

Definición B.3.8 *Sea $N = \bigcap_{i=1}^r N_i$ una descomposición primaria reducida, donde N_i es P_i-primario. Diremos que P_i es **minimal** si no contiene propiamente a ningún P_j, con $j \neq i$.*

Teorema B.3.9 *Sea M es un módulo finitamente generado sobre un anillo noetheriano R. Entonces $AP(M) \subseteq Supp(M)$ y los elementos minimales de $AP(M)$ y $Supp(M)$ son los mismos.*

Demostración. Sea $P \in AP(M)$ y haciendo $Q = P$ en la implicación (2) $\Rightarrow$ (1), de la proposición anterior, tenemos que $P \in Supp(M)$.

Supongamos que P es minimal en $Supp(M)$, entonces la implicación (1) $\Rightarrow$ (2), en la proposición anterior, nos dice que hay un $Q \in AP(M) \subseteq Supp(M)$ tal que $Q \subseteq P$. Por la minimalidad de P, $Q = P$. Así, $P \in AP(M)$. Más aún, P es minimal en $AP(M)$, pues en caso contrario, hay un $Q \in AP(M) \subseteq Supp(M)$ tal que $Q \subsetneq P$ y por tanto P no es minimal en $Supp(M)$, lo cual es una contradicción.

Sea P minimal en $AP(M)$ y supongamos que P no es minimal en $Supp(M)$. Entonces hay un ideal $Q \in Supp(M)$ tal que $Q \subsetneq P$. Luego, por la implicación (1) $\Rightarrow$ (2), en la proposición anterior, hay un $P' \in AP(M)$ tal que $P' \subseteq Q$. Entonces $P' \subsetneq P$, o sea que P no es minimal en $AP(M)$, lo cual es falso. □

Bibliografía

[1] Aleksandrov, A. D. et al., *Mathematics, its content, methods and meaning*, vol. 1, the M. I. T. Press, Cambridge, Massachusetts, 1981.

[2] Arumugam, M. *A Theorem of Homological Algebra: The Hilbert-Burch Theorem*, School of Mathematics, The University of New South Wales, 2005.

[3] Ash, R. B. *A Course in Commutative Algebra*, 2003,
www.math.uiuc.edu/ r-ash

[4] Atiyah, M. F. y Macdonald, I. G. *Introducción al Algebra Conmutativa*, Reverté, España, 1980.

[5] Auslander, M. and Buchsbaum, D. A. *Homological Dimension in Local Rings*, Transactions of the American Mathematical Society, vol.85, part 2, 1957.

[6] Bruns, W. and Herzog, J. *Cohen-Macaulay Rings*, Cambridge Studies in Advanced Mathematics no. 39, Cambridge University Press, 1996.

[7] Burch, L. *On Ideals of Finite Homological Dimension in Local Rings*, Proceedings of the Cambridge Philosophical Society, vol.64, part 4, 1968.

[8] Cartan, H. and Eilenberg, S. *Homological Algebra*, Princeton Mathematical Series no. 19, Springer, 1973.

[9] Chan, D. *Homology and Homological Algebra*, 2005,
www.maths.unsw.edu.au/ danielch/homology05b/halec.pdf

[10] Contreras, A. *Los Funtores Ext y Tor y Algunas de sus Propiedades*, Universidad Autónoma de Puebla, Tesis de Licenciatura, 1988.

[11] Eisenbud, D. *Commutative Algebra, with a View Toward Algebraic Geometry*, Graduate Texts in Mathematics no. 150, Springer-Verlag, New York, 1995.

[12] Herrlich, H. and Strecker, G. E. *Category Theory, An introduction*, Allyn and Bacon, United States of America, 1973.

[13] Kaplansky, I. *Projective Modules*, Annals of Mathematics, vol. 68, no.2, September 1958.

[14] Osborne, M. S. *Basic Homological Algebra*, Graduate Texts in Mathematics no. 196, Springer-Verlag, New York, 2000.

[15] Rees, D. *A Theorem of Homological Algebra*, Proceedings of the Cambridge Philosophical Society, vol.52, part 4, 1956.

[16] Rees, D. *The Grade of an Ideal or Module*, Proceedings of the Cambridge Philosophical Society, vol.53, part 1, 1957.

[17] Simon, J. *The Formula of Auslander and Buchsbaum*, A talk at Summer School: Homological conjectures for finite dimensional algebras; Nordfjordeid, Norway, 2001,

www.math.ntnu.edu/ oyvinso/Nordfjordeid/Transparencies/simontalk.ps

[18] Weibel, C. A. *History of Homological Algebra*, Department of Mathematics, Rutgers University, U. S. A.

www.math.rutgers.edu/ weibel/history.dvi