Benemérita Universidad Autónoma de Puebla
Facultad de Ciencias Físico Matemáticas

TÍTULO DE LA TESIS:

FACTORIZACIÓN POR MATRICES: UNA TÉCNICA PARA FACTORIZAR POLINOMIOS IRREDUCIBLES

Tesis presentada para obtener el título de:

LICENCIADO EN MATEMÁTICAS

Presenta:

JOSÉ ALEJANDRO TENORIO VÁZQUEZ

Directores :
Dr. F. Agustín Romano Velázquez, UCIM-UNAM
Dr. César Cejudo Castilla, FCFM-BUAP

Febrero 2024

AGRADECIMIENTOS

Este trabajo no hubiera sido posible sin el apoyo de las personas que me acompañaron a lo largo del camino. A ellos quisiera expresarles mi más profundo agradecimiento.

En primer lugar, agradecer a mis asesores, el Dr. Agustín Romano Velázquez y el Dr. César Cejudo Castilla, por su invaluable orientación, paciencia y apoyo a lo largo de este proceso.

A mi familia, mis mas sinceros agradecimientos. A mis abuelos, Lorenza y Alejandro†, mi tía, Lorena, mi padre, Alejandro, y su esposa Angélica por el apoyo incondicional, su amor, sus consejos y por haberme enseñado a dar mi máximo esfuerzo. También, agradecer a mis hermanas, Michelle, Melina y Melany, y mi prima, Darina, por las risas y los momentos que hemos pasado juntos que sin duda fueron de ayuda para hacer mas alegre esta aventura.

Quiero expresar mi gratitud al proyecto Singularidades de superficies complejas: modificaciones, resoluciones y curvas polares (IN117523) del Programa de Apoyo a Proyectos de Investigación e Innovación Tecnológica (PAPIIT) por el apoyo económico que hicieron posible la realización de esta tesis. La cual no fue importante para el desarrollo de esta tesis, sino que también ha contribuido de manera significativa a mi crecimiento académico y profesional.

Finalmente, agradezco a todas esas personas que, de una u otra manera, han contribuido a la elaboración de esta tesis. A todos ustedes, les dedico este logro con gratitud y aprecio.

INTRODUCCIÓN

La noción de factorización se remonta a la antigua Grecia, cuando matemáticos de la época, como Euclides, comenzaron a estudiar propiedades de los números primos y fue precisamente Euclides quién desarrolló el algoritmo que hoy lleva su nombre para descomponer números en sus factores primos. Posteriormente, tras años de trabajo, en el siglo XIX se estableció y demostró el actual Teorema fundamental de la Aritmética. En este siglo, Kummer realizó contribuciones para demostrar un análogo del teorema mencionado para anillos de números algebraicos.

Continuando con la idea del surgimiento de la factorización tenemos a Cardano, Tartaglia y Viète quienes desarrollaron métodos para resolver ecuaciones polinomiales de grados específicos entre los siglos XVI y XVII, estos métodos muy frecuentemente implicaban la factorización de polinomios en raíces. Mas tarde, a finales del siglo XIX y principios del siglo XX, matemáticos como Richard Dedekind, David Hilbert y Emmy Noether desarrollaron la teoría de anillos y campos, la cual proporcionó una manera más general de estudiar la factorización de polinomios. Podríamos continuar con la historia que gira entorno a la factorización con el desarrollo de la Teoría de Galois en el siglo XIX o la teoría de ideales en el siglo XX. El ejemplo que motiva a seguir trabajando en hallar maneras de factorizar, son los polinomios irreducibles. Como mencionamos antes, el concepto de factorización se fue generalizando a través de los años, hasta llegar a la noción de polinomio irreducible, es decir, un polinomio que no se puede escribir como producto de polinomios de grado menor.

Un primer acercamiento a estos polinomios lo encontramos cuando se descubre la

existencia de los números complejos, cuando se demuestra que la ecuación $x^2 + 2 = 0$ no tiene soluciones reales. Si consideramos el polinomio $x^2 + 2$, no podremos escribirlo como el producto de polinomios de menor grado en $\mathbb{R}[x]$, pues de existir tendrían que ser polinomios de la forma $x - a$ donde $a \in \mathbb{R}$, lo cual implicaría que $a \in \mathbb{R}$ es una raíz de $x^2 + 2 = 0$. Gracias a una primera versión del que hoy conocemos como el Teorema Fundamental del Álgebra, surge la noción de la unidad imaginaria y junto a ella el campo de los números complejos, en el cual cualquier polinomio de una variable de grado mayor o igual a 1 se puede expresar como la multiplicación de polinomios de grado 1, es decir se puede factorizar. Esto es gracias a que el conjunto de los números complejos $\mathbb{C}$ es algebraicamente cerrado, es decir, todo polinomio de una variable con coeficientes en $\mathbb{C}$ tiene tantas raíces con multiplicidad en $\mathbb{C}$ como grado tenga el polinomio.

Sin embargo, a pesar de que $\mathbb{C}$ tenga la propiedad de ser algebraicamente cerrado, esto no implica que cualquier polinomio de n variables con coeficientes en $\mathbb{C}$ se pueda factorizar, como producto de polinomios de grado 1. Por ejemplo, los polinomios $x^n \pm y^m$, $x^n \pm z^m$ y $y^n \pm z^m$ con $n, m \in \mathbb{N}$ tales que $\mathrm{M.\,C.\,D}(n, m) = 1$ son irreducibles en $\mathbb{C}[x, y, z]$. Sin embargo, gracias al concepto de factorización por matrices, los polinomios anteriores tendrán una factorización que no está dada en términos de elementos del anillo de polinomios, si no en las matrices cuadradas con entradas en en $\mathbb{C}[x, y, z]$. Por ejemplo, el polinomio $x^3 + yz$ es irreducible en $\mathbb{C}[x, y, z]$, sin embargo usando el concepto de factorización por matrices tenemos que las matrices

$$A = \begin{pmatrix} y & x^2 \\ x & -z \end{pmatrix}, \quad B = \begin{pmatrix} z & x^2 \\ x & -y \end{pmatrix}$$

tiene las siguientes propiedades:

$$AB = \begin{pmatrix} y & x^2 \\ x & -z \end{pmatrix} \begin{pmatrix} z & x^2 \\ x & -y \end{pmatrix} = \begin{pmatrix} x^3 + yz & yx^2 - yx^2 \\ xz - zx & x^3 + yz \end{pmatrix} = x^3 + yz \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$BA = \begin{pmatrix} z & x^2 \\ x & -y \end{pmatrix} \begin{pmatrix} y & x^2 \\ x & -z \end{pmatrix} = \begin{pmatrix} x^3 + yz & yx^2 - yx^2 \\ xz - zx & x^3 + yz \end{pmatrix} = x^3 + yz \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Es decir que, de cierta manera, hemos "factorizado" al polinomio $x^3 + yz$.

En 1980, Eisenbud estudiando cuán diferentes eran un anillo conmutativo R y el cociente $R/(x)$, donde $x \in R$ no es un divisor de cero, introdujo el concepto de Factorización por Matrices, que hasta ese momento es utilizado por físicos teniendo un auge en la teoría de cuerdas. En su artículo [Eis80b], usa este concepto para probar que a cada una de las factorizaciones por matrices de $x \in R$, con R un anillo regular local Noetheriano, le corresponde un único $R/(x)$-módulo Cohen-Macaulay Maximal (sin sumandos directos libres).

Unos años después, Yoshino en su artículo [Yos98] utilizó un caso particular de anillo en la definición de Eisenbud, obteniendo así una gran herramienta de trabajo para los matemáticos y físicos contemporáneos. Yoshino, utiliza el anillo de polinomios $\mathbb{C}[x_1, \ldots, x_n]$, para fines prácticos de este trabajo unicamente utilizaremos el caso cuando $n = 3$. Pero, ¿porqué este concepto se volvió tan importante la actualidad? La respuesta es sencilla, el concepto de factorización por matrices ha sido de gran utilidad para definir invariantes topológicos y algebraicos. Además, ha sido parte crucial de conjeturas de física y en *homological mirror symmetry*.

Este trabajo tiene dos objetivos principales, el primero y por el cual se desarrolla la mayoría de teoría a lo largo del trabajo es demostrar el Teorema de Auslander-Buchsbaum (Teorema 3.32), el cual relaciona diversos conceptos de gran relevancia en álgebra conmutativa. El segundo, usando el Teorema antes mencionado, será probar que dado un R-módulo Cohen-Macaulay Maximal (donde R tiene características especiales) a este le corresponde una resolución libre periódica (de periodo 2) la cual es generada por una factorización por matrices.

Para poder llegar a cumplir los objetivos de este trabajo, como todo en matemáticas, es necesario introducir herramientas para poder entender como se comportan los objetos. Para ello, establecimos una estructura en el trabajo que esperamos permita al lector seguir de manera ordenada los conceptos, las consecuencias y las relaciones que hay entre estos.

En el primer capítulo desarrollaremos la teoría necesaria de anillos y módulos. Parti-

remos del concepto de anillo, del cual consideraremos ciertas características particulares como la localidad o la Noetheriedad. Psteriormente definiremos que es un módulo y veremos algunas propiedades como el producto tensorial de módulos y características relacionadas con las sucesiones exactas.

En el segundo capítulo, ahondaremos un poco en otra gran rama de las matemáticas, el Álgebra Homológica. En particular, mediante los conceptos de módulo libre, proyectivo e inyectivo definiremos dos conceptos relevantes que han sido de gran ayuda en el desarrollo de teoría moderna: los funtores Ext y Tor. Para esto, introduciremos conceptos de resoluciones libres, proyectivas e inyectivas.

En el capítulo tres, enunciaremos el concepto de sucesión regular y conceptos como el grado, la profundidad y dimensión proyectiva de un módulo, todo esto necesario para demostrar el teorema de Auslander-Buchsbaum (Teorema 3.32) el cual, como mencionamos anteriormente, es uno de nuestros objetivos del trabajo.

Finalmente, en el capítulo cuatro enunciaremos los conceptos de factorización de matrices y módulo Cohen-Macaulay Maximal, será en este capítulo donde demostraremos el teorema que nos propusimos como objetivo que relaciona los conceptos anteriormente mencionados. También, en este capítulo presentaremos algunos ejemplos de factorizaciones por matrices y enunciaremos el que se conoce como método estándar para hallarlas.

ÍNDICE GENERAL

1. Prelimiares **1**

1.1. Anillos y módulos 1

1.2. Sucesiones exactas 13

1.3. Producto tensorial 28

2. Funtores Ext **y** Tor **41**

2.1. Módulos proyectivos e inyectivos 41

2.2. Resoluciones 45

2.3. Tor y Ext 55

3. Teorema de Auslander-Buchsbaum **65**

3.1. Sucesiones regulares 65

3.2. Grado, profundidad y dimensión proyectiva 69

4. Factorización por matrices **85**

4.1. Factorización por matrices 85

4.2. Ejemplos de factorizaciones por matrices 89

4.3. Algoritmos para encontrar factorizaciones por matrices y más ejemplos 98

4.3.1. Método estándar 98

CAPÍTULO 1

PRELIMIARES

En el presente capítulo, se llevará a cabo una revisión concisa de los conceptos fundamentales de teoría de anillos que resultarán esenciales para el avance de la tesis. Paralelamente, se desarrollará de manera integral la teoría de módulos, la cual desempeñará un papel fundamental en la consecución de nuestros objetivos. Para una exploración más detallada de estos principios, se recomienda al lector consultar las obras [AM16, Capítulo 1], [DF91, Capítulos 7-9] que proporcionan un análisis exhaustivo.

1.1. Anillos y módulos

A lo largo de la tesis, unicamente consideraremos anillos conmutativos con unidad, por ello tenemos la siguiente definición.

Definición 1.1. *Un* anillo conmutativo con unidad R *es un conjunto con dos operaciones binarias (suma y multiplicación) tales que:*

(a) R *es un grupo abeliano respecto a la suma,*

(b) la multiplicación es asociativa y se distribuye sobre la suma,

(c) para todo $x, y \in R$ *se tiene que* $xy = yx$*, y*

(d) existe un elemento $1 \in R$ *tal que* $1x = x1 = x$ *para todo* $x \in R$*.*

Cuando mencionamos la palabra *anillo*, estamos haciendo referencia a aquellos men-

cionados en la definición previa. Uno de los objetos fundamentales en la teoría de anillos es el concepto de ideal, el cuál se define como sigue:

Definición 1.2. *Dado un anillo R e $I \subseteq R$. Diremos que I es un ideal de R si I es un subgrupo aditivo de R y para cualesquiera $r \in R$ y $x \in I$ se cumple que $rx \in I$.*

Existen diferentes tipo de ideales, por ejemplo tenemos:

Definición 1.3. *Sea R un anillo. Entonces:*

(a) Dado un ideal P de R, diremos que P es ideal primo si $P \neq R$ y $xy \in P$ implica que $x \in P$ o $y \in P$.

(b) Dado un ideal M de R, diremos que M es ideal máximo si $M \neq R$ y no existe ideal I de R tal que $M \subsetneq I \subsetneq R$.

Veamos algunos ejemplos de ideales primos e ideal máximos:

Ejemplo 1.4. Consideremos el anillo $\mathbb{Z}$. Entonces, dado p un número primo, tenemos que $p\mathbb{Z}$ es un ideal primo. En efecto, si $ab \in p\mathbb{Z}$ entonces $p \mid ab$ y como p es primo $p \mid a$ o $p \mid b$, es decir $a \in p\mathbb{Z}$ o $b \in p\mathbb{Z}$. También dado que $\mathbb{Z}$ es un dominio entero, el ideal cero también es primo.

De los ideales de $\mathbb{Z}$, unicamente los de la forma $p\mathbb{Z}$ con p primo son máximos. Primero es claro que $p\mathbb{Z} \neq \mathbb{Z}$; ahora, supongamos que existe un ideal I de $\mathbb{Z}$ tal que $p\mathbb{Z} \subsetneq I \subsetneq \mathbb{Z}$. Sea $a \in I$ tal que $a \notin p\mathbb{Z}$, entonces $p \nmid a$ como p es primo tenemos que $\mathrm{m.\,c.\,d}(a, p) = 1$. Así, por el lema de Bézout tenemos que existen α, $\beta \in \mathbb{Z}$ tal que $\alpha a + \beta p = 1$, sin embargo como $p \in I$ tenemos que $1 \in I$, es decir $I = \mathbb{Z}$ lo cual es absurdo, ya que $I \subsetneq R$.

De manera similar probaremos el siguiente ejemplo

Ejemplo 1.5. Consideremos el anillo de polinomios $\mathbb{C}[x]$. Afirmamos que los únicos ideales primos son el ideal cero y los de la forma $(x-\lambda)\mathbb{C}[x]$ con $\lambda \in \mathbb{C}$. El ideal cero es primo pues como $\mathbb{C}$ es un campo, $\mathbb{C}[x]$ es un dominio entero. Ahora si $fg \in (x-\lambda)\mathbb{C}[x]$ entonces $(x-\lambda) \mid fg$ como $x-\lambda$ es irreducible tenemos que $(x-\lambda) \mid f$ o $(x-\lambda) \mid g$ es decir $f \in (x-\lambda)\mathbb{C}[x]$ o $g \in (x-\lambda)\mathbb{C}[x]$.

Similar al ejemplo anterior tenemos que solo los ideales de la forma $(x-\lambda)\mathbb{C}[x]$ son máximos. Claramente $(x-\lambda)\mathbb{C}[x] \neq \mathbb{C}[x]$. Ahora, si suponemos que existe un ideal I

tal que $(x-\lambda)\mathbb{C}[x] \subsetneq I \subsetneq \mathbb{C}[x]$, tenemos que existe $f \in I$ tal que $f \notin (x-\lambda)\mathbb{C}[x]$, y así $\text{m. c. d.}(x-\lambda, f) = 1$. Nuevamente, por el lema de Bézout existen $u, v \in \mathbb{C}[x]$ tal que $u(x-\lambda) + v \cdot f = 1$, así $1 \in I$, es decir que $I = \mathbb{C}[x]$ lo cual es absurdo.

Proposición 1.6. *Sean R un anillo y $P_1, \ldots, P_r$ ideales primos de R. Si I es un ideal tal que $I \subseteq \bigcup_{i=1}^{r} P_i$, entonces $I \subseteq P_i$ para algún $1 \leq i \leq r$.*

Demostración:

Procedamos por inducción en r, y solo probaremos para el caso de $r = 2$, pues el paso inductivo es consecuencia de este. Supongamos que $I \subseteq P_1 \cup P_2$. Ahora, si $I \nsubseteq P_1$ debemos probar que $I \subseteq P_2$.

Primero, como $I \nsubseteq P_1$, entonces existe $x \in I$ tal que $x \notin P_1$. Ahora, supongamos que $I \nsubseteq P_2$, es decir, existe $y \in I$ tal que $y \notin P_2$. Como I es ideal, $x + y \in I$, y por hipótesis $I \subseteq P_1 \cup P_2$. Si $x + y \in P_1$, y dado que $y \in P_1$, entonces $x + y - y = x \in P_1$ lo cual es absurdo. Ahora, sí $x + y \in P_2$, y como $x \in P_2$ tenemos que $x + y - x = y \in P_2$ lo cual también es una contradicción. Por lo tanto, $I \subseteq P_2$.

■

Existen anillos con exactamente un ideal máximo, en este caso tenemos lo siguiente

Definición 1.7. *Dado un anillo R. Si este tiene solo un ideal máximo diremos que R es un anillo local.*

Veamos un ejemplo de anillo local:

Ejemplo 1.8. Consideremos el conjunto $\mathbb{C}[[x]] = \left\{\sum_{i\geq 0} z_i x^i : z_i \in \mathbb{C}\right\}$, el cual definiendo $1_{\mathbb{C}[[x]]} = 1 + \sum_{i\geq 1} 0$ y $0_{\mathbb{C}[[x]]} = \sum_{i\geq 0} 0$ y a las siguientes operaciones es un anillo, llamado el anillo de series formales:

$$\begin{aligned} + : \quad \mathbb{C}[[x]] \times \mathbb{C}[[x]] &\longrightarrow \mathbb{C}[[x]] \\ \left(\sum_{i\geq 0} z_i x^i, \sum_{i\geq 0} z_i' x^i\right) &\longmapsto \sum_{i\geq 0} (z_i + z_i') x^i \end{aligned}$$

$$\begin{aligned} \cdot : \quad \mathbb{C}[[x]] \times \mathbb{C}[[x]] &\longrightarrow \mathbb{C}[[x]] \\ \left(\sum_{i\geq 0} z_i x^i, \sum_{i\geq 0} z_i' x^i\right) &\longmapsto \sum_{i\geq 0} \left(\sum_{j=0}^{i} z_j z_{i-j}'\right) x^i. \end{aligned}$$

Notemos que dado $f = \sum_{i\geq 0} z_i x^i \in \mathbb{C}[[x]]$ con $z_0 \neq 0$, entonces, denotando por $f_1 = \sum_{i\geq 1} z_i x^i$ y usando el hecho de que

$$\frac{1}{1+x} = \sum_{i\geq 0}^{\infty} x^n (-1)^n,$$

definimos la siguiente serie formal:

$$g = \frac{1}{z_0} \cdot \frac{1}{1+\frac{f_1}{z_0}} = \frac{1}{z_0} \sum_{i\geq 0}^{\infty} \left(\frac{f_1}{z_0}\right)^n (-1)^n.$$

Entonces, tenemos que $f \cdot g = 1_{\mathbb{C}[[x]]}$.

Afirmamos que $\mathbb{C}[[x]]$ es un anillo local. Para probar este hecho, consideremos el conjunto $(x) = \left\{\sum_{i\geq 1} z_i x^i : z_i \in \mathbb{C}\right\}$ (las series sin término constante), veamos que este es el ideal máximo de $\mathbb{C}[[x]]$. No es complicado ver que en efecto (x) es un ideal. Veamos que este es máximo. Supongamos que existe J ideal de $\mathbb{C}[[x]]$ tal que $(x) \subsetneq J \subsetneq \mathbb{C}[[x]]$, es decir que existe $S \in J$ tal que $S = \sum_{i\geq 0} z_i x^i \notin (x)$, entonces su termino constante es distinto de cero, y por lo anterior, existe $S' \in \mathbb{C}[[x]]$ tal que $SS' = 1$, como J es ideal y $1 = SS' \in J$, así $J = \mathbb{C}[[x]]$, lo cual es absurdo. Es inmediato que (x) es el único ideal maximal, pues dada una serie formal sin término constante $S = \sum_{i\geq 1} z_i x^i$ entonces $S \in (x)$, es decir que cualquier otro ideal esta contenido en (x).

Definición 1.9. *Dados R un anillo e $\mathcal{I} := \{I_1, I_2 \ldots\}$ un conjunto de ideales de R. Diremos que $\mathcal{I}$ es una cadena ascendente de ideales si se cumple que $I_i \subseteq I_{i+1}$, es decir que se tiene lo siguiente:*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$$

Diremos que $\mathcal{I}$ se estaciona si existe $n \in \mathbb{N}$ tal que $I_n = I_{n+j}$ para toda $j \in \mathbb{N}$.

En caso de que cada I_j sea primo diremos que este es una cadena de ideales primos. Si $|\mathcal{I}| = n < \infty$ diremos que es una cadena de longitud n y definimos la dimensión de R como:

$$\dim(R) = \sup\{n : |\mathcal{I}| = n, \mathcal{I} \text{ es una cadena de ideales primos}\}.$$

Ejemplo 1.10. Como vimos anteriormente, los únicos ideal primos de $\mathbb{Z}$ son de la

forma $p\mathbb{Z}$ con p primos. Además, dados p y q primos distintos $p\mathbb{Z} \nsubseteq q\mathbb{Z}$ y $q\mathbb{Z} \nsubseteq p\mathbb{Z}$. Entonces, $\dim(\mathbb{Z}) = 1$.

Ejemplo 1.11. Dado un campo $\mathbb{F}$, tenemos que $\dim(\mathbb{F}) = 0$, pues no hay ideales primos.

Definición 1.12. *Dado un anillo R, diremos que R es Noetheriano si satisface alguna de las siguientes condiciones:*

(a) Cada conjunto no vacío de ideales de R tiene elemento maximal.

(b) Cada cadena ascendente de ideales de R se estaciona.

(c) Cada ideal de R es finitamente generado.

Podemos notar que las tres condiciones de la definición anterior son equivalentes, sin embargo no se probará pues no es el fin de este trabajo [AM16, Propisiciones 6.1 y 6.2, p. 74, 75].

Definición 1.13. *Dado R un anillo local con ideal máximo $\mathfrak{m}$, diremos que R es un anillo regular, o simplemente regular, si* $\dim(R) = \dim(\mathfrak{m}/\mathfrak{m}^2)$.

Ejemplo 1.14. Todo campo $\mathbb{F}$ es un anillo regular.

Ejemplo 1.15. Si $\mathbb{F}$ es un campo ($\mathbb{Z}$ o un dominio de ideales principales), entonces el anillo de polinomios $\mathbb{F}[x_1, \ldots, x_n]$ es un anillo regular (es una equivalencia del Corolario 3.33).

Definición 1.16. *Sea R un anillo. Un* R-módulo *es un grupo abeliano M y una función $R \times M \to M$ denotada por $(r, m) \mapsto rm$ (a la cual llamaremos ley de composición externa) tal que para cualesquiera $a, b \in R$ y $x, y \in M$ se cumple lo siguiente:*

(a) $a(x + y) = ax + ay$.

(b) $(a + b)x = ax + bx$.

(c) $(a \cdot b)x = a(bx)$.

(d) $1x = x$.

Consideremos ahora algunos ejemplos inmediatos basados en la definición anterior.

Ejemplo 1.17. Dado un anillo R, entonces R es un R-módulo con el producto de R como ley de composición externa.

Ejemplo 1.18. Dado M un grupo abeliano aditivo, tenemos que M es un $\mathbb{Z}$-módulo. Basta definir la ley de composición como sigue:

$$\begin{array}{ccc} \mathbb{Z} \times M & \longrightarrow & M \\ (z, m) & \longmapsto & zm = \begin{cases} \underbrace{(-m) + \ldots + (-m)}_{|z| \text{ veces}} & z < 0 \\ 0 & z = 0 \\ \underbrace{m + \ldots + m}_{z \text{ veces}} & z > 0 \end{cases} \end{array}$$

Ejemplo 1.19. Sea $\mathbb{F}$ un campo. Entonces cualquier espacio vectorial V sobre $\mathbb{F}$ es un $\mathbb{F}$-módulo. Tememos la ley de composición *multiplicar por escalares* y de ahí se obtiene el resultado.

Ejemplo 1.20. El conjunto $\mathbb{Q}[i] = \{p + qi : p, q \in \mathbb{Q}\}$ es un $\mathbb{Z}[i]$-módulo, donde $\mathbb{Z}[i] = \{x + yi : x, y \in \mathbb{Z}\}$. En efecto, basta definir la ley de composición externa como sigue:

$$\begin{array}{ccc} \mathbb{Z}[i] \times \mathbb{Q}[i] & \longrightarrow & \mathbb{Q}[i] \\ (x + yi, p + qi) & \longmapsto & (x + yi)(p + qi) = (xp - yq) + (xq + yp)i \end{array}$$

Definición 1.21. *Sean R un anillo y M un R-módulo. Decimos que M' es un* submódulo *de M si:*

(a) M' es subgrupo de M y

(b) para todo $r \in R$ y $m \in M'$ se tiene que $rm \in M'$.

Algunos ejemplos de submódulos son los siguientes:

Ejemplo 1.22. Para todo R-módulo M, se tiene que M y $\{0\}$ son submódulos de M. A estos submódulos los llamaremos *submódulos triviales*.

Ejemplo 1.23. Para todo anillo R, si I es un ideal de R, entonces R e I son R-módulos y por tanto I es submódulo de R.

Definición 1.24. *Sea R un anillo, I un ideal y M un R-módulo. Definimos el producto de I con M como sigue:*

$$IM = \left\{ \sum_{i=1}^{n} r_i x_i : n \in \mathbb{N},\ r_i \in I,\ x_i \in M \right\}.$$

Además, no es difícil verificar que IM es submódulo de M.

Definición 1.25. *Sean R un anillo, M un R-módulo. Dado $m \in M$ definimos el anulador de m como*

$$\mathrm{Ann}_R(m) = \{r \in R : rm = 0\}.$$

Similarmente definimos el anulador de M como

$$\mathrm{Ann}_R(M) = \{r \in R : rm = 0, \ \text{para todo } m \in M\}.$$

Definición 1.26. *Dados R un anillo y M un R-módulo. Si P es un ideal primo de R, diremos que P es asociado de M si existe un elemento no cero $m \in M$ tal que $P = \mathrm{Ann}_R(m)$. Al conjunto de los primos asociados de M lo denotaremos por $\mathrm{Ass}_R(M)$ o simplemente $\mathrm{Ass}(M)$ cuando no existe ambigüedad sobre el anillo en el que trabajamos.*

Definición 1.27. *Sean R un anillo, M un R-módulo y N, P submódulos de M. Definimos la suma de N y P como sigue:*

$$N + P = \{n + p : n \in N, p \in P\}.$$

Es inmediato que $N + P$ es submódulo de M.

Definición 1.28. *Sea R un anillo, M un R-módulo y $X \subseteq M$ no vacío. Al conjunto*

$$(X) := \left\{ \sum_{i=1}^{n} r_i x_i : r_i \in R, \, x_i \in X, \, n \in \mathbb{N} \right\},$$

lo llamaremos el generado por X, además no es complicado ver que este es un submódulo de M. Si X es finito y $(X) = M$, diremos que M es finitamente generado.

Observación. Si R un anillo Noetheriano y M un R-módulo finitamente generado. Entonces, $\mathrm{Ass}_R(M)$ es finito.

La demostración de la observación anterior puede ser consultada en [Eis95, Teorema 3.1, p. 90].

Definición 1.29. *Sean R un anillo, M un módulo y M' un submódulo de M. Definimos el R-módulo cociente de M y M' como el grupo abeliano M/M', con la operación $r(x + M') = rx + M'$.*

Definición 1.30. *Sean R un anillo y M y N R-módulos. Un mapeo $\varphi : M \to N$ es un* morfismo de R-módulos *(o simplemente R-*lineal*) si:*

(a) $\varphi(x+y) = \varphi(x) + \varphi(y)$ *para toda* $x, y \in M$,

(b) $\varphi(ax) = a\varphi(x)$ *para toda* $a \in R$ *y para toda* $x \in M$.

Algunos ejemplos básicos son:

Ejemplo 1.31. Dados un anillo R y M un R-módulo, la función identidad sobre M, a la cual denotaremos por 1_M o simplemente 1 cuando no haya ambigüedad sobre el módulo, dicha función es un morfismo de R-módulos.

Ejemplo 1.32. Dados un anillo R y M, N R-módulos, definimos $\tilde{0} : M \to N$ como $\tilde{0}(x) = 0$, este es un morfismo de R-módulos (lo llamaremos el morfismo cero).

Ejemplo 1.33. Dados R un anillo, M un R-módulo y N un submódulo de M. El mapeo $\pi : M \to M/N$ dado por $\pi(x) = x + N$ es un morfismo de R-módulos, además resulta ser sobreyectivo. A lo anterior se le conoce como la sobreyección natural o canónica.

Ejemplo 1.34. Dados un anillo R, M un R-módulo y N submódulo de M. La función $i : N \to M$ dada por $i(x) = x$ es un morfismo (al cual llamaremos morfismo inclusión). De hecho podemos ver a i como la restricción de 1_M en N.

No es difícil verificar que dados M, N y P R-módulos y $\varphi : M \to N$ y $\psi : N \to P$ morfismos entonces $\psi \circ \varphi : M \to P$ resulta ser morfismo, a la composición simplemente la denotaremos por $\psi\varphi$.

Definición 1.35. *Sean R un anillo y M, N R-módulos. Dado $\varphi : M \to N$ un morfismo de R-módulos, decimos que:*

(a) El mapeo φ es monomorfismo si y solo si φ es inyectiva.

(b) El mapeo φ es epimorfismo si y solo si φ es sobreyectiva.

(c) El mapeo φ es isomorfismo si y solo si φ es biyectiva.

La definición anterior nos permite introducir la noción de isomorfismo.

Definición 1.36. *Sea R un anillo y M, N R-módulos, decimos que M y N son isomorfos si existe un isomorfismo $\varphi : M \to N$ y lo denotaremos por $M \cong N$.*

Proposición 1.37. *Sean R un anillo, M y N R-módulos. Al conjunto de todos los morfismos de M en N lo denotamos por* $\mathrm{Hom}_R(M, N)$. *Entonces,* $\mathrm{Hom}_R(M, N)$ *es un R-módulo con las siguientes operaciones:*

(a) $(\varphi_1 + \varphi_2)(x) = \varphi_1(x) + \varphi_2(x)$ *para todo* φ_1, $\varphi_2 \in \mathrm{Hom}_R(M, N)$*; esta operación convierte a* $\mathrm{Hom}_R(M, N)$ *en un grupo abeliano.*

(b) $(r\varphi)(x) = r\varphi(x)$ *para toda* $r \in R$ *y* $\varphi \in \mathrm{Hom}_R(M, N)$*; esta es la operación que lo convierte en un* R*-módulo.*

Escribiremos $\mathrm{Hom}(M, N)$ en lugar de $\mathrm{Hom}_R(M, N)$ cuando no exista ambigüedad del anillo en el que estamos trabajando.

En próximos capítulos, veremos que los anillos con los cuales trabajaremos tienen la característica de ser Noetherianos, y esperamos sean claras las razones por las cuales los consideramos de está manera. Una de ellas es la que se enuncia a continuación:

Proposición 1.38. *Sea* R *un anillo Noetheriano, y* M *un* R*-módulo. Entonces, los ideales máximos del conjunto* $\Gamma = \{\mathrm{Ann}_R(m) : m \in M,\ m \neq 0\}$ *son ideales primos de* R *(implícitamente estamos diciendo que son primos asociados).*

Demostración:
Sean $\mathrm{Ann}_R(m) \in \Gamma$ un ideal máximo de dicho conjunto y $rs \in \mathrm{Ann}_R(m)$. Supongamos que $s \notin \mathrm{Ann}_R(m)$, entonces dado que $sm \neq 0$. Luego, $\mathrm{Ann}_R(m) \subseteq \mathrm{Ann}_R(sm) \in \Gamma$, pues si $x \in \mathrm{Ann}_R(m)$ entonces $s(xm) = x(sm) = 0$. Pero, por hipótesis tenemos que $\mathrm{Ann}_R(m)$ es máximo, es decir que $\mathrm{Ann}_R(m) = \mathrm{Ann}_R(sm)$ y como $(rs)m = r(sm) = 0$, tenemos que $r \in \mathrm{Ann}_R(m)$. ■

Corolario 1.39. *Sea* R *un anillo Noetherioano y* M *un* R*-módulo. Entonces:*

(a) Para cada $m \in M$ *no cero, existe* $r \in R$ *tal que* $\mathrm{Ann}_R(rm)$ *es un primo asociado.*

(b) Si $M \neq 0$*, entonces* $\mathrm{Ass}_R(M) \neq \emptyset$*.*

Demostración:

(a) Sea $m \in M$ no cero. Consideremos $\Gamma_m = \{\mathrm{Ass}_R(rm) : r \in R, rm \neq 0\}$. El conjunto anterior es no vacío (basta tomar $r = 1$), entonces por la proposición anterior existe un ideal máximo de Γ_m, que además es primo y, por razones obvias, es un asociado de M.

(b) Como $M \neq 0$ existe $m \in M$ no cero y por lo anterior hay un asociado de M.

■

Los módulos que definiremos a continuación son esenciales para el desarrollo de la teoría, además de simplificar la notación.

Definición 1.40. *Dado $\varphi \in \mathrm{Hom}_R(M,N)$, definimos:*

(a) $\mathrm{Ker}(\varphi) = \{m \in M : \varphi(m) = 0\}$.

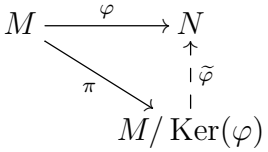
(b) $\mathrm{Im}(\varphi) = \{y \in N : \varphi(x) = y, \text{ para algún } x \in M\}$.

(c) $\mathrm{coker}(\varphi) = N/\mathrm{Im}(\varphi)$.

No es complicado ver que $\mathrm{Ker}(\varphi)$ y $\mathrm{Im}(\varphi)$ son submódulos de M y N, respectivamente.

Los resultados siguientes son importantes en la teoría de módulos (en general en cualquier estructura algebraica), sin embargo no serán demostrados, pues no es el objetivo del trabajo, pero pueden ser consultadas en [Mus99, pp. 135,136].

Teorema 1.41 (Primer teorema de isomorfismos de módulos)**.** *Sean R un anillo, M y N R-módulos y un epimorfismo $\varphi : M \to N$. Entonces existe un único isomorfismo $\widetilde{\varphi} : M/\mathrm{Ker}(\varphi) \to N$, tal que $\varphi = \widetilde{\varphi}\pi$, es decir, que el siguiente diagrama conmuta:*



Un resultado que se desprende del teorema anterior es el siguiente:

Proposición 1.42. *Dados R un anillo y P un ideal primo de R. Entonces, P es asociado de M si y solo si $R/P \cong N$ donde N es un submódulo de M (la segunda parte de la equivalencia es la definición de encaje, la cual es equivalente a que existe un morfismo inyectivo $\lambda : R/P \to M$).*

Demostración:

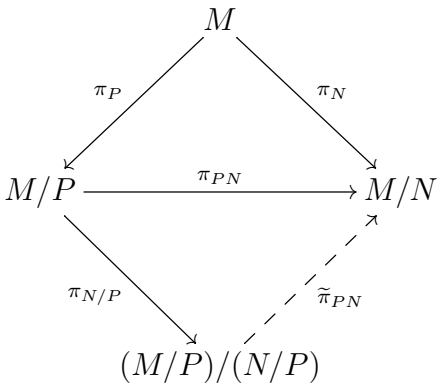
Supongamos que P es un asociado de M. Entonces $P = \mathrm{Ann}_R(m)$ para algún $m \in M$. Consideremos $N = Rm$ y $\lambda : R \to Rm$ el morfismo que manda 1 a m, este, claramente, es un epimorfismo. Así, por el Teorema 1.41 $R/\mathrm{Ker}(\lambda) \cong Rm$, no es complicado ver que $\mathrm{Ker}(\lambda) = \mathrm{Ann}_R(m) = P$.

Ahora supongamos que $R/P \cong N$ para algún submódulo N de M. Entonces, bajo el isomorfismo $n = 1 + P$ para algún $n \in N$. Luego tenemos que:

$$\begin{aligned}\mathrm{Ann}_R(n) &= \{r \in R : rn = 0\} \\ &= \{r \in R : r(1+P) = 0\} \\ &= \{r \in R : r \in P\} \\ &= P.\end{aligned}$$

■

Teorema 1.43 (Segundo teorema de isomorfismos de módulos)**.** *Sea R un anillo y M, N y P R-módulos tales que P es submódulo de N y N es submódulo de M. Entonces existe un isomorfismo natural de $(M/P)/(N/P)$ y M/N que hacen que el siguiente diagrama conmuta:*



Teorema 1.44 (Tercer teorema de isomorfismo de módulos)**.** *Sean R un anillo, M un R-módulo y N, P submódulos de M. Tenemos que$(B + C)/C \cong B/(B \cap C)$.*

Definición 1.45. *Sea R un anillo y $\{M_i\}_{i\in I}$ una familia de R-módulos. Definimos la suma directa de $\{M_i\}_{i\in I}$ como sigue:*

$$\bigoplus_{i\in I} M_i = \{(m_i)_{i\in I} : m_i \in M_i, \text{ y donde casi todos los } m_i \text{ son cero}\}.$$

Con las operaciones $(m_i)_{i\in I} + (n_i)_{i\in I} = (m_i + n_i)_{i\in I}$ y $r(m_i)_{i\in I} = (rm_i)_{i\in I}$ tenemos que $\bigoplus_{i\in I} M_i$ es un R-módulo.

En el caso donde I sea finito podemos definir $\bigoplus_{i\in I} M_i$ como el producto cartesiano usual, es decir, $\bigoplus_{i\in I} M_i = \prod_{i\in I} M_i$.

Definición 1.46. *Dado un anillo R. Definimos el radical de Jacobson como la intersección de todos los ideales maximales de R.*

Proposición 1.47 (Lema de Nakayama)**.** *Sean R un anillo, I un ideal contenido en el radical de Jacobson de R y M un R-módulo finitamente generado. Si $IM = M$, entonces $M = 0$.*

Demostración:

Supongamos que $M \neq 0$. Como M es finitamente generado, consideremos $u_1, \ldots, u_n$ generadores de M y supongamos que es la cantidad mínima de estos. Como $M = IM$ y $u_n \in M$, tenemos que $u_n \in IM$. Por lo tanto, tenemos la siguiente expresión:

$$u_n = r_1u_1 + \ldots + r_nu_n \qquad r_i \in I,\ \forall i \in \{1, \ldots, n\}$$

luego

$$(1 - r_n)u_n = r_1u_1 + \ldots + r_{n-1}u_{n-1}$$

pero r_n es un elemento del radical de Jacobson, entonces afirmamos que $1 - r_n$ es una unidad. En efecto, pues de lo contrario $1 - r_n \in \mathfrak{m}$ con $\mathfrak{m}$ ideal maximal de R [AM16, Corolario 1.5, p. 4], pero r_n es un elemento del radical de Jacobson, entonces $1 \in \mathfrak{m}$ (i.e. $\mathfrak{m} = R$) lo cual es absurdo. Así u_n está generado $n - 1$ elementos, lo cual es absurdo ya que n era la cantidad mínima. Por tanto $M = 0$. ∎

Corolario 1.48. *Sean R un anillo, I un ideal de R contenido en el radical de Jacobson, M un R-módulo y N un submódulo de M. Entonces, si $M = IM + N$ se cumple que $N = M$.*

Demostración:

Supongamos que $M = IM + N$. Entonces

$$\begin{aligned} I(M/N) &= \left\{ \sum_{i=1}^{n} a_i(m_i + N) : n \in \mathbb{N},\ a_i \in I,\ m_i \in M \right\} \\ &= \left\{ \left(\sum_{i=1}^{n} a_i m_i + N \right) : n \in \mathbb{N},\ a_i \in I,\ m_i \in M \right\} \\ &= (IM + N)/N \\ &= M/N \end{aligned}$$

Entonces, por el lema de Nakayama tenemos que $M/N = 0$, es decir $M = N$. ■

Teorema 1.49. *Sean R un anillo local cuyo ideal máximo es $\mathfrak{m}$, M un R-módulo y $x_1, \ldots, x_n \in M$ tales que $\{x_1 + \mathfrak{m}M, \ldots, x_n + \mathfrak{m}M\}$ es una base del $R/\mathfrak{m}$-espacio vectorial $M/\mathfrak{m}M$. Entonces $x_1, \ldots, x_n$ generan a M.*

Demostración:
Consideremos N como el módulo generado por los elementos $x_1, \ldots, x_n$. Vamos a demostrar que $\mathfrak{m}M + N = M$, pues de cumplirse esto, por el corolario anterior tendríamos que $N = M$. Consideremos $m \in M$, si $m + \mathfrak{m}M = \mathfrak{m}M$ ya terminamos. En caso de que $m + \mathfrak{m}M \neq \mathfrak{m}M$, como $\{x_1 + \mathfrak{m}M, \ldots, x_n + \mathfrak{m}M\}$ es base de $M/\mathfrak{m}M$ tenemos que $m + \mathfrak{m}M = \sum_{i=1}^{n}(r_i + \mathfrak{m})(x_i + \mathfrak{m}M) = \sum_{i=1}^{n}(r_i x_i + \mathfrak{m}M)$. Denotemos a $m' = \sum_{i=1}^{n} r_i x_i \in N$, entonces $(m - m') + \mathfrak{m}M = \mathfrak{m}M$. Es decir, $m - m' \in \mathfrak{m}M$, por tanto existe $m'' \in \mathfrak{m}M$ tal que $m'' = m - m'$. Así tenemos que $m = m'' + m'$. Con esto se obtiene lo que deseamos. ■

Claramente, el recíproco del teorema se cumple, de esto tenemos la siguiente definición:

Definición 1.50. *Dados R un anillo local con ideal máximo $\mathfrak{m}$ y M un R-módulo finitamente generado. Decimos que $x_1, \ldots, x_n \in M$ son un sistema minimal de generadores si se cumple el teorema anterior. A la cantidad de estos elementos la denotaremos por $\mu(M)$, que no es más que la dimensión de $M/\mathfrak{m}M$ (la dimensión como espacio vectorial).*

Desde este punto en adelante, excluiremos la mención del anillo específico sobre el cual estemos calculando el módulo. En otras palabras, diremos que M es un R-módulo, y se dará por entendido que R representa el anillo en el que estaremos trabajando.

1.2. Sucesiones exactas

Definición 1.51. *Dada una sucesión de R-módulos y morfismos de R-módulos*

$$\ldots \longrightarrow M_{i-1} \xrightarrow{\varphi_i} M_i \xrightarrow{\varphi_{i+1}} M_{i+1} \longrightarrow \ldots$$

(a) Decimos que la sucesión es un complejo si $\mathrm{Im}(\varphi_i) \subseteq \mathrm{Ker}(\varphi_{i+1})$.

(b) Decimos que la sucesión es exacta si $\mathrm{Im}(\varphi_i) = \mathrm{Ker}(\varphi_{i+1})$.

A partir de ahora, a los objetos de la definición anterior simplemente diremos que son sucesiones de R-módulos.

Proposición 1.52. *Dados M, M' y M'' R-módulos. Entonces*

(a) La sucesión $0 \longrightarrow M' \xrightarrow{\varphi} M$ es exacta si y solo si φ es inyectiva.

(b) La sucesión $M \xrightarrow{\psi} M'' \longrightarrow 0$ es exacta si y solo si ψ es sobreyectiva.

(c) La sucesión $0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$ es exacta si y solo si φ es inyectiva, ψ es sobreyectiva y ψ induce un isomorfismo entre $\operatorname{coker}(\varphi)$ y M''.

Demostración:

(a) ($\Rightarrow$) Supongamos que $0 \xrightarrow{i} M' \xrightarrow{\varphi} M$ es exacta, donde i es el morfismo inclusión. Entonces, tenemos que $\operatorname{Ker}(\varphi) = \operatorname{Im}(i)$. Como $\operatorname{Im}(i) = 0$, tenemos que φ es inyectiva.
($\Leftarrow$) Supongamos que φ es inyectiva. Entonces $\operatorname{Ker}(\varphi) = 0$, pero $0 = \operatorname{Im}(i)$. Así la sucesión es exacta.

(b) ($\Rightarrow$) Supongamos que $M \xrightarrow{\psi} M'' \xrightarrow{\tilde{0}} 0$ es exacta. Entonces, tenemos que $\operatorname{Ker}(\tilde{0}) = \operatorname{Im}(\psi)$. Como $\operatorname{Ker}(\tilde{0}) = M''$, tenemos que ψ es sobreyectiva.
($\Leftarrow$) Supongamos que ψ es sobreyectiva. Esto es $\operatorname{Im}(\psi) = M''$ pero $M'' = \operatorname{Ker}(\tilde{0})$. Así la sucesión es exacta.

(c) ($\Rightarrow$) Supongamos que la sucesión $0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$ es exacta. De los incisos anteriores obtenemos que φ es inyectiva y ψ es sobreyectiva. Entonces, del Teorema 1.41, $M/\operatorname{Ker}(\psi) \cong M''$, dado que la sucesión es exacta, $\operatorname{coker}(\varphi) = M/\operatorname{Im}(\varphi) \cong M''$.
($\Leftarrow$) El recíproco es inmediato de los incisos anteriores.

■

Las sucesiones del estilo $0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$ son llamadas *sucesiones exactas cortas*. De hecho cualquier sucesión como en la Definición 1.51 puede dividirse en sucesiones exactas cortas, basta tomar $N_i = \operatorname{Im}(\varphi_i) = \operatorname{Ker}(\varphi_{i+1})$ para obtener la sucesión

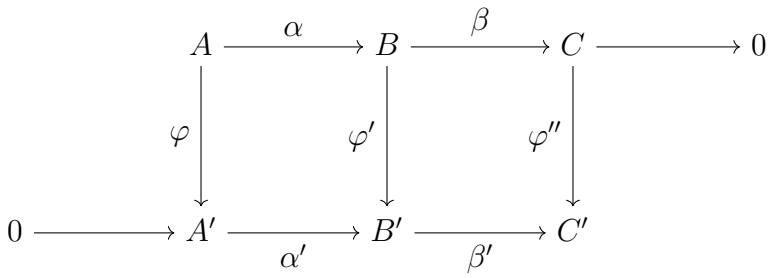
$$0 \longrightarrow N_i \longrightarrow M_i \longrightarrow N_{i+1} \longrightarrow 0\,.$$

Lema 1.53. *Si una sucesión $0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$ es exacta, entonces $\psi\varphi = 0$.*

Demostración:

Tomemos $x \in M'$, entonces $\varphi(x) \in \mathrm{Im}(\varphi)$. Como la sucesión es exacta, se tiene que $\varphi(x) \in \mathrm{Ker}(\psi)$ y por tanto $\psi(\varphi(x)) = (\psi\varphi)(x) = 0$. Por tanto, $\psi\varphi = 0$. ■

Teorema 1.54 (Lema de la Serpiente). *Sea R un anillo. Consideremos el siguiente diagrama conmutativo:*

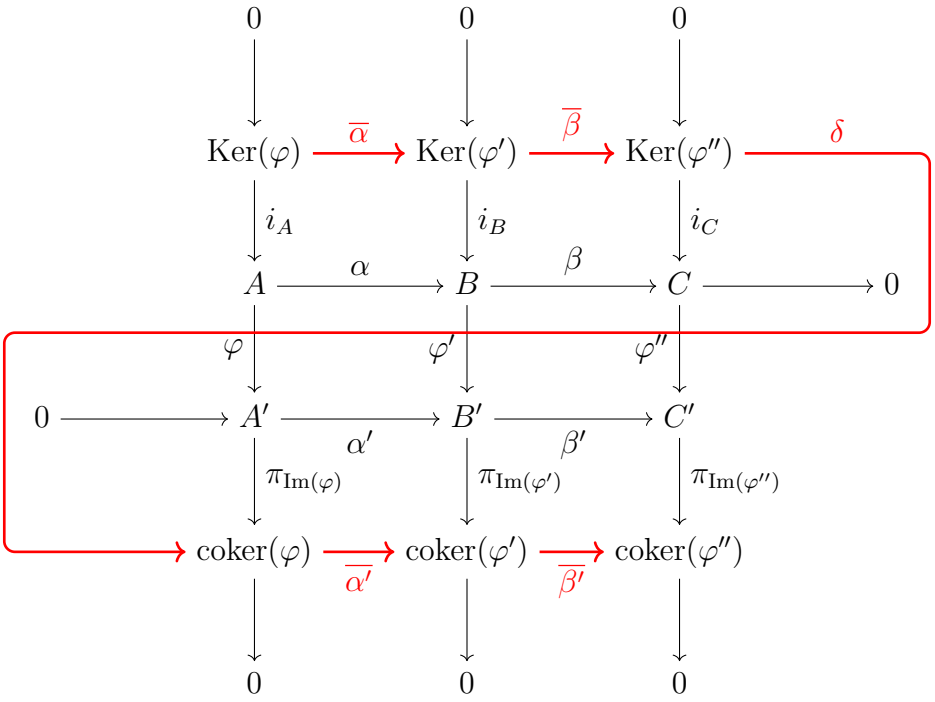


donde las filas son exactas. Tenemos que la siguiente sucesión es exacta:

$$\mathrm{Ker}(\varphi) \xrightarrow{\overline{\alpha}} \mathrm{Ker}(\varphi') \xrightarrow{\overline{\beta}} \mathrm{Ker}(\varphi'') \xrightarrow{\delta} \mathrm{coker}(\varphi) \xrightarrow{\overline{\alpha'}} \mathrm{coker}(\varphi') \xrightarrow{\overline{\beta'}} \mathrm{coker}(\varphi'') \ .$$

Demostración:

Primero, veamos como se define cada uno de los morfismos inducidos, para ello consideremos el siguiente diagrama:



$\overline{\alpha}$: Definimos a $\overline{\alpha} : \mathrm{Ker}(\varphi) \to \mathrm{Ker}(\varphi')$ como $\overline{\alpha}(x) = \alpha i_A(x)$ para toda $x \in \mathrm{Ker}(\varphi)$. Veamos que la función tiene sentido, dado $x \in \mathrm{Ker}(\varphi)$ tenemos que:

$$\begin{aligned}\varphi'(\overline{\alpha}(x)) &= \varphi'(\alpha i_A(x)) \\ &= \varphi'(\alpha(x)) \\ &= \alpha'(\varphi(x)) \\ &= \alpha'(0) \\ &= 0\end{aligned}$$

Por tanto $\overline{\alpha}$ está bien definida.

$\overline{\beta}$: De manera similar, definimos a $\overline{\beta} : \mathrm{Ker}(\varphi') \to \mathrm{Ker}(\varphi'')$ como $\overline{\beta}(x) = \beta i_B(x)$ para toda $x \in \mathrm{Ker}(\varphi')$. Por argumentos similares a los anteriores tenemos que $\overline{\beta}$ tiene sentido.

$\overline{\alpha'}$: Definamos a $\overline{\alpha'} : \mathrm{coker}(\varphi) \to \mathrm{coker}(\varphi')$ como $\overline{\alpha'}(x + \mathrm{Im}(\varphi)) = \alpha'(x) + \mathrm{Im}(\varphi')$ para toda $x + \mathrm{Im}(\varphi) \in \mathrm{coker}(\varphi)$. Veamos que $\overline{\alpha'}$ está bien definida, sean $x + \mathrm{Im}(\varphi)$, $y + \mathrm{Im}(\varphi) \in \mathrm{coker}(\varphi)$ tales que $x + \mathrm{Im}(\varphi) = y + \mathrm{Im}(\varphi)$, entonces $x - y \in \mathrm{Im}(\varphi)$. Es decir que existe $a \in A$ tal que $\varphi(a) = x - y$. Luego, $\alpha'\varphi(a) = \alpha'(x - y)$, lo que implica que $\varphi'\alpha(a) = \alpha'(x - y)$ por lo tanto, $\alpha'(x - y) \in \mathrm{Im}(\varphi')$, es decir $\alpha'(x) + \mathrm{Im}\,\varphi' = \alpha'(y) + \mathrm{Im}(\varphi')$. Así $\overline{\alpha'}$ está bien definida.

$\overline{\beta'}$: Análogamente, si definimos a $\overline{\beta'} : \mathrm{coker}(\varphi') \to \mathrm{coker}(\varphi'')$ como el mapeo $\overline{\beta'}(x + \mathrm{Im}(\varphi')) = \beta'(x) + \mathrm{Im}(\varphi'')$ para toda $x + \mathrm{Im}(\varphi') \in \mathrm{coker}(\varphi')$, usando argumentos similares a los anteriores, tenemos que $\overline{\beta'}$ está bien definida.

δ: Por último, veamos como se define $\delta : \mathrm{Ker}(\varphi'') \to \mathrm{coker}(\varphi)$. Sea $x \in \mathrm{Ker}(\varphi'')$, entonces tenemos que $i_C(x) \in C$. Dado que β es suprayectiva, existe $b \in B$ tal que $\beta(b) = i_C(x)$.

Como $0 = \varphi''(x) = \varphi i_C(x) = \varphi''\beta(b)$ y usando la conmutatividad del diagrama tenemos que $\beta'\varphi'(b) = 0$ es decir que $\varphi'(b) \in \mathrm{Ker}(\beta')$ y como el la sucesión es exacta $\varphi'(b) \in \mathrm{Im}(\alpha')$, es decir que $\varphi'(b) = \alpha'(a')$ con $a' \in A'$ y dado que α' es inyectiva tenemos que dicho elemento es único. De manera análoga, si tomamos b' otro elemento tal que $\beta(b') = x$ tenemos que $\varphi'(b') = \alpha'(a'')$ con $a'' \in A'$.

Luego, $\alpha'(a''-a') = \varphi'(b'-b) = \alpha'\varphi(a)$ donde $\varphi(a) = b'-b$, dado que α' es inyectiva tenemos que $a''-a' = \varphi(a)$. Luego, $\pi_{\mathrm{Im}(\varphi)}(a''-a') = \pi_{\mathrm{Im}(\varphi)}\varphi(a) = 0$. Es decir que $a''+\mathrm{Im}(\varphi) = a'+\mathrm{Im}(\varphi)$.

Por lo tanto, si definimos a δ como $\delta(x) = a'+\mathrm{Im}(\varphi)$ tenemos que está bien definido y además es inmediato que δ es morfismo.

Ahora, vamos a verificar la exactitud en cada uno de los módulos:

Exactitud en $\mathrm{Ker}(\varphi')$: Primero, sea $x \in \mathrm{Im}(\overline{\alpha})$. Entonces, existe $y \in \mathrm{Ker}(\varphi)$ tal que $\overline{\alpha}(y) = x$. Luego $\overline{\beta'}(x) = \overline{\beta'}\overline{\alpha}(y) = \beta\alpha(z) = 0$. Así, $x \in \mathrm{Ker}(\overline{\beta'})$.

Ahora, consideremos un elemento $x \in \mathrm{Ker}(\overline{\beta})$, es decir $\overline{\beta}(x) = \beta i_B(x) = \beta(x) = 0$, así $x \in \mathrm{Ker}(\beta) = \mathrm{Im}(\alpha)$, es decir que existe $a \in A$ tal que $x = \alpha(a)$. Luego, $0 = \varphi'(x) = \varphi'\alpha(a) = \alpha'\varphi(a)$ como α' es inyectiva $\varphi(a) = 0$, es decir $a \in \mathrm{Ker}(\varphi)$ y por tanto $a = i_A(a)$. Como $\alpha(a) = x$, tenemos que $\alpha(i_A(a)) = \overline{\alpha}(a) = x$. Por tanto, $x \in \mathrm{Im}(\overline{\alpha})$. Esto prueba que en efecto existe exactitud en $\mathrm{Ker}(\varphi')$.

Exactitud en $\mathrm{coker}(\varphi')$: Tomemos $x+\mathrm{Im}(\varphi')$ un elemento de $\mathrm{Im}(\overline{\alpha'})$. Entonces, existe $y+\mathrm{Im}(\varphi) \in \mathrm{coker}(\varphi)$ tal que $x+\mathrm{Im}(\varphi') = \overline{\alpha'}(y+\mathrm{Im}(\varphi)) = \alpha'(y)+\mathrm{Im}(\varphi')$. Finalmente, $\overline{\beta'}(x+\mathrm{Im}(\varphi')) = \overline{\beta'}(\alpha'(y)+\mathrm{Im}(\varphi')) = \beta'\alpha'(y)+\mathrm{Im}(\varphi'') = 0$. Por lo tanto, $x+\mathrm{Im}(\varphi') \in \mathrm{Ker}(\overline{\beta'})$.

Ahora, dado $x+\mathrm{Im}(\varphi') \in \mathrm{Ker}(\overline{\beta'})$. Entonces, $\overline{\beta'}(x+\mathrm{Im}(\varphi')) = \beta'(x)+\mathrm{Im}(\varphi'') = 0$, es decir que $\beta'(x) \in \mathrm{Im}(\varphi'')$. Así, existe $c \in C$ tal que $\varphi''(c) = \beta'(x)$. Como β es suprayectiva, existe $b \in B$ tal que $c = \beta(b)$, así:

$$\begin{aligned}
\varphi''(c) = \beta'(x) &\Rightarrow \varphi''\beta(b) = \beta'(x) \\
&\Rightarrow \beta'\varphi'(b) = \beta'(x) \\
&\Rightarrow \beta'(x-\varphi'(b)) = 0 \\
&\Rightarrow x-\varphi'(b) \in \mathrm{Ker}(\beta').
\end{aligned}$$

Luego, dado que la sucesión es exacta, tenemos que $x-\varphi'(b) \in \mathrm{Im}(\alpha')$, es decir que existe $a \in A'$ tal que $x-\varphi'(b) = \varphi'(a)$. Finalmente, observemos que $\alpha'(a)+\mathrm{Im}(\varphi') =$

$x + \mathrm{Im}(\varphi')$, por lo tanto $x + \mathrm{Im}(\varphi') \in \mathrm{Im}(\overline{\alpha'})$. Con esto hemos probado la exactitud en $\mathrm{coker}(\varphi')$.

Exactitud en $\mathrm{coker}(\varphi)$: Ahora, dado $x + \mathrm{Im}(\varphi') \in \mathrm{Im}(\delta)$ existe $y \in \mathrm{Ker}(\varphi'')$ tal que $\delta(y) = x + \mathrm{Im}(\varphi')$. Primero, consideremos $b \in B$ tal que $\beta(b) = y$ y $a \in A'$ tal que $\alpha'(a) = \varphi'(b)$ y por tanto $\delta(y) = a + \mathrm{Im}(\varphi)$. Luego

$$\begin{aligned} \overline{\alpha'}(x + \mathrm{Im}(\varphi)) &= \overline{\alpha'}(a + \mathrm{Im}(\varphi)) \\ &= \alpha'(a) + \mathrm{Im}(\varphi') \\ &= \varphi'(b) + \mathrm{Im}(\varphi') \\ &= 0. \end{aligned}$$

Por lo tanto, $x + \mathrm{Im}(\varphi) \in \mathrm{Ker}(\overline{\alpha'})$.

Por otro lado, consideremos $x + \mathrm{Im}(\varphi)$ un elemento de $\mathrm{Ker}(\overline{\alpha'})$, es decir que $\overline{\alpha'}(x + \mathrm{Im}(\varphi)) = \alpha'(x) + \mathrm{Im}(\varphi') = 0$. Entonces, $\alpha'(x) = \varphi'(b)$ para algún $b \in B$. Así, obtenemos las siguientes igualdades $0 = \beta'\alpha'(x) = \beta'\varphi'(b) = \varphi''\beta(b)$, es decir que $\beta(b) \in \mathrm{Ker}(\varphi'')$. Finalmente, $\delta(\beta(b)) = x + \mathrm{Im}(\varphi)$, así $x + \mathrm{Im}(\varphi) \in \mathrm{Im}(\delta)$. Con esto se prueba la exactitud en $\mathrm{coker}(\varphi)$.

Exactitud en $\mathrm{Ker}(\varphi'')$: Sea $x \in \mathrm{Im}(\overline{\beta})$. Entonces, existe $y \in \mathrm{Ker}(\varphi)$ tal que $\overline{\beta}(y) = x$. Entonces $\delta(x) = a + \mathrm{Im}(\varphi)$, donde $a \in A'$ es tal que $\alpha'(a) = \varphi'(y)$ (pues ya vimos que es independiente de la elección del elemento en B), es decir que $\alpha'(a) = 0$ y como α' es inyectiva $a = 0$ por lo tanto $\delta(x) = 0$. Así, $x \in \mathrm{Ker}(\delta)$.

Finalmente, dado $x \in \mathrm{Ker}(\delta)$ tenemos que $\delta(x) = 0$. Ahora, consideremos $b \in B$ tal que $\beta(b) = x$ y $a \in A$ tal que $\alpha'(a) = \varphi'(b)$. Entonces, de nuestra hipótesis obtenemos que $a \in \mathrm{Im}(\varphi)$, es decir que $a = \varphi(r)$ para algún $r \in A$. Así, obtenemos que $\varphi'\alpha(r) = \alpha'\varphi(r) = \alpha'(a) = \varphi'(b)$, lo que implica que $b - \alpha(r) \in \mathrm{Ker}(\varphi')$. Por último, $\overline{\beta}(b - \alpha(r)) = \beta(b) - \beta(\alpha(r)) = \beta(b) = x$. Así, $x \in \mathrm{Im}(\overline{\beta})$ y con esto hemos probado la exactitud en $\mathrm{Ker}(\varphi'')$. ■

Teorema 1.55. *Sea R un anillo. Consideremos el siguiente diagrama conmutativo:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi'} & & \downarrow{\scriptstyle \varphi''} & & \\ 0 & \longrightarrow & A' & \xrightarrow[\alpha']{} & B' & \xrightarrow[\beta']{} & C' & \longrightarrow & 0 \end{array}$$

donde las filas son exactas. Tenemos que la siguiente sucesión es exacta:

$$0 \longrightarrow \operatorname{Ker}(\varphi) \xrightarrow{\overline{\alpha}} \operatorname{Ker}(\varphi') \xrightarrow{\overline{\beta}} \operatorname{Ker}(\varphi'') \xrightarrow{\delta} \operatorname{coker}(\varphi) \xrightarrow{\overline{\alpha'}} \operatorname{coker}(\varphi') \xrightarrow{\overline{\beta'}} \operatorname{coker}(\varphi'') \longrightarrow 0 \cdot$$

Demostración:

Solo resta probar la exactitud en $\operatorname{Ker}(\varphi)$ y $\operatorname{coker}(\varphi'')$, pues del teorema anterior tenemos las exactitud en todo lo demás.

Exactitud en $\operatorname{Ker}(\varphi)$: Para esto solo debemos probar que $\overline{\alpha}$ es inyectiva. Sea $x \in \operatorname{Ker}(\overline{\alpha})$, entonces $\overline{\alpha}(x) = \alpha(x) = 0$ y como α es inyectiva $x = 0$. Por tanto, $\overline{\alpha}$ es inyectiva.

Exactitud en $\operatorname{coker}(\varphi'')$: Análogamente probaremos que $\overline{\beta'}$ es suprayectiva. Sea $x + \operatorname{Im}(\varphi'') \in \operatorname{coker}(\varphi'')$. En particular tenemos que $x \in C'$ y como β' es suprayectiva obtenemos que $x = \beta'(b)$ para algún $b \in B$. Finalmente, consideremos $b + \operatorname{Im}(\varphi') \in \operatorname{coker}(\varphi')$, entonces $\overline{\beta'}(b+\operatorname{Im}(\varphi')) = \beta'(b)+\operatorname{Im}(\varphi'') = x+\operatorname{Im}(\varphi'')$. Así $\overline{\beta'}$ es suprayectiva. ■

Proposición 1.56. *Dada*

$$M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0 \tag{1.1}$$

una sucesión de R-módulos. Entonces, la sucesión anterior es exacta si y solo si para cualesquier R-módulo N, la sucesión

$$0 \longrightarrow \operatorname{Hom}(M'', N) \xrightarrow{\overline{v}} \operatorname{Hom}(M, N) \xrightarrow{\overline{u}} \operatorname{Hom}(M', N) \tag{1.2}$$

es exacta.

Pasar de la la sucesión en (1.1) a la sucesión en (1.2) se le conoce como aplicarle el funtor $\operatorname{Hom}(-, N)$, el término funtor se suele encontrar en la literatura de álgebra

homológica y de categorías sin embargo para fines prácticos del trabajo no nos sumergiremos en dichas áreas.

Antes de proceder con la demostración, debemos aclarar quienes son $\overline{u}$ y $\overline{v}$, los cuales se definen como sigue:

$$\begin{array}{rccc} \overline{u}: & \mathrm{Hom}(M,N) & \longrightarrow & \mathrm{Hom}(M',N) \\ & \varphi & \longmapsto & \varphi u \end{array} \qquad \begin{array}{rccc} \overline{v}: & \mathrm{Hom}(M'',N) & \longrightarrow & \mathrm{Hom}(M,N) \\ & \psi & \longmapsto & \psi v \end{array}$$

Demostración:

($\Rightarrow$) Supongamos que $M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$ es exacta.

Primero, vamos a verificar que la sucesión (1.2) es exacta en $\mathrm{Hom}(M'',N)$. Para ello usaremos la Proposición 1.52, es decir, vamos a verificar que $\overline{v}$ es inyectiva. Sean $\varphi, \psi \in \mathrm{Hom}(M'',N)$ tales que $\overline{v}(\varphi) = \overline{v}(\psi)$, es decir que $\varphi v = \psi v$. Verifiquemos que $\varphi = \psi$, para esto tomemos $x \in M''$, como v es sobreyectiva (pues la sucesión (1.1) es exacta), entonces existe $y \in M$ tal que $x = v(y)$. Así

$$\begin{aligned} \varphi(x) &= \varphi(v(y)) \\ &= (\varphi v)(y) \\ &= (\psi v)(y) \\ &= \psi(v(y)) \\ &= \psi(x). \end{aligned}$$

Por lo tanto $\overline{v}$ es inyectiva.

Ahora, lo que debemos demostrar es que $\mathrm{Ker}(\overline{u}) = \mathrm{Im}(\overline{v})$. Sea $\varphi \in \mathrm{Ker}(\overline{u})$, es decir $\overline{u}(\varphi) = \varphi u = 0$. Definamos la siguiente función

$$\begin{array}{rccc} \alpha: & M'' & \longrightarrow & N \\ & x & \longmapsto & \varphi(y) \end{array}$$

donde $y \in M$ es tal que $x = v(y)$, pues v es sobreyectiva. Debido a que α depende de la existencia de un elemento en M, que no necesariamente es único, debemos verificar que la función está bien definida. Supongamos que para $x \in M''$ existen y_1, $y_2 \in M$

tales que $v(y_1) = x = v(y_2)$. Entonces $v(y_1 - y_2) = 0$, es decir $y_1 - y_2 \in \mathrm{Ker}(v)$. Por hipótesis tenemos que $\mathrm{Ker}(v) = \mathrm{Im}(u)$, luego $y_1 - y_2 = u(z)$ para algún $z \in M'$. Por tanto, tenemos lo siguiente:

$$\begin{aligned}
\varphi(y_1) &= \varphi(y_1 - y_2 + y_2) \\
&= \varphi(y_1 - y_2) + \varphi(y_2) \\
&= \varphi(u(z)) + \varphi(y_2) \\
&= (\varphi u)(z) + \varphi(y_2) \\
&= 0 + \varphi(y_2) \\
&= \varphi(y_2).
\end{aligned}$$

Es decir, que α no depende de dicho elemento, además por la forma en la que lo definimos $\alpha \in \mathrm{Hom}(M'', N)$.

Ahora, tenemos lo siguiente: dado $y \in M$

$$\begin{aligned}
\overline{v}(\alpha)(y) &= (\alpha v)(y) \\
&= \alpha(v(y)) \\
&= \varphi(y) && \text{(por la definición de } \alpha)
\end{aligned}$$

Por tanto, $\varphi \in \mathrm{Im}(\overline{v})$.

Ahora, sea $\varphi \in \mathrm{Im}(\overline{v})$. Entonces $\overline{v}(\psi) = \varphi$ con $\psi \in \mathrm{Hom}(M, N)$, luego

$$\begin{aligned}
\overline{v}(\varphi) &= \overline{u}(\overline{v}(\psi)) \\
&= \overline{u}(\psi v) \\
&= (\psi v)u \\
&= \psi(vu) && \text{(pues la sucesión (1.1)) es exacta} \\
&= \psi 0 \\
&= 0
\end{aligned}$$

Es decir que $\varphi \in \mathrm{Ker}(u)$.

Por lo tanto $0 \longrightarrow \mathrm{Hom}(M'', N) \xrightarrow{\overline{v}} \mathrm{Hom}(M, N) \xrightarrow{\overline{u}} \mathrm{Hom}(M', N)$ es exacta.

($\Leftarrow$) Supongamos que $0 \longrightarrow \mathrm{Hom}(M'', N) \xrightarrow{\overline{v}} \mathrm{Hom}(M, N) \xrightarrow{\overline{u}} \mathrm{Hom}(M', N)$ es exacta para cualquier R-módulo N.

Verifiquemos que la sucesión (1.1) es exacta en M'', por la Proposición 1.52, basta probar que v es sobreyectiva. Supongamos que v no es suprayectiva, entonces $\mathrm{Im}(v)$ es submódulo propio de M''. Así, el epimorfismo canónico $\pi : M'' \to M''/\mathrm{Im}(v)$ no es cero. Denotemos por $N = M''/\mathrm{Im}(v)$. Aplicando $\mathrm{Hom}(-, N)$ a la sucesión (1.1) y usando la hipótesis tenemos que $\overline{v}(\pi) \neq 0$. Sin embargo, dado que $\mathrm{Im}(v) \subseteq \mathrm{Ker}(\pi)$ se tiene que $\overline{v}(\pi) = \pi v = 0$, lo que es una contradicción. Por tanto v es suprayectivo.

Ahora, debemos verificar que $\mathrm{Im}(u) = \mathrm{Ker}(v)$. Para esto, podemos considerar $1_{M''} \in \mathrm{Hom}(M'', M'')$, por el Lema 1.53 tenemos que $\overline{uv}(f) = fvu = 0$, y como $1_{M''}$, en particular, es inyectiva, tenemos que $vu = 0$, por tanto $\mathrm{Im}(u) \subseteq \mathrm{Ker}(v)$. Para ver la igualdad, consideremos $N = M/\mathrm{Im}(u)$ y $\pi : M \to N$. Notemos que $\pi \in \mathrm{Ker}(\overline{u})$, y como $\mathrm{Ker}(\overline{u}) = \mathrm{Im}(\overline{v})$, existe un morfismo $\psi : M'' \to N$ tal que $\overline{v}(\psi) = \psi v = \pi$, es decir que $\mathrm{Ker}(\pi) \subseteq \mathrm{Ker}(v)$. Pero, $\mathrm{Ker}(\pi) = \mathrm{Im}(u)$, así $\mathrm{Im}(u) \subseteq \mathrm{Ker}(v)$. Por lo tanto, $M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$ es exacta. ■

Análogamente se puede probar el siguiente resultado.

Proposición 1.57. *Dada*

$$0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \tag{1.3}$$

una sucesión de R-módulos y R-morfismos. Entonces, la sucesión anterior es exacta si y solo si para cualesquier R-módulo N, la sucesión

$$0 \longrightarrow \mathrm{Hom}(N, M') \xrightarrow{\overline{u}} \mathrm{Hom}(N, M) \xrightarrow{\overline{v}} \mathrm{Hom}(N, M'') \tag{1.4}$$

es exacta.

La demostración es análoga a la anterior, unicamente debemos tener en cuenta que, ahora $\overline{u}$ y $\overline{v}$ se definen como sigue:

$$\begin{array}{rccc} \overline{u}: & \mathrm{Hom}(N,M') & \longrightarrow & \mathrm{Hom}(N,M) \\ & \varphi & \longmapsto & u\varphi \end{array} \qquad \begin{array}{rccc} \overline{v}: & \mathrm{Hom}(N,M) & \longrightarrow & \mathrm{Hom}(N,M'') \\ & \psi & \longmapsto & v\psi \end{array}$$

De manera similar, pasar de la sucesión (1.3) a la sucesión (1.4) se le conoce como aplicar el funtor $\mathrm{Hom}(N,-)$.

Naturalmente uno puede preguntarse si lo mismo pasa en cualquier tipo de sucesiones exactas, los siguientes lemas nos ayudaran a resolver este cuestionamiento.

Lema 1.58. *Dada una sucesión de R-módulos exacta*

$$\ldots \xrightarrow{\varphi_3} M_3 \xrightarrow{\varphi_2} M_2 \xrightarrow{\varphi_1} M_1 \longrightarrow 0\,.$$

Entonces para cualquier R-módulo N tenemos que

$$0 \longrightarrow \mathrm{Hom}(M_1,N) \xrightarrow{\overline{\varphi_1}} \mathrm{Hom}(M_2,N) \xrightarrow{\overline{\varphi_2}} \mathrm{Hom}(M_3,N) \xrightarrow{\overline{\varphi_3}} \ldots$$

es un complejo.

Demostración:
Sea $\psi \in \mathrm{Im}(\overline{\varphi_i})$. Entonces, existe $\rho \in \mathrm{Hom}(M_{i-1},N)$ tal que $\overline{\varphi_i}(\rho)=\psi$, luego tenemos lo siguiente:

$$\begin{aligned} \overline{\varphi_{i+1}}(\psi) &= \overline{\varphi_{i+1}}(\overline{\varphi_i}(\rho)) \\ &= \overline{\varphi_{i+1}}(\rho\varphi_i) \\ &= (\rho\varphi_i)\varphi_{i+1} \\ &= \rho(\varphi_i\varphi_{i+1}) \\ &= \rho(\tilde{0}) \\ &= \tilde{0} \end{aligned}$$

Por lo tanto, $\mathrm{Im}(\overline{\varphi_i}) \subseteq \mathrm{Ker}(\overline{\varphi_{i+1}})$. Es decir que la sucesión es un complejo. ■

Lema 1.59. *Dada una sucesión de R-módulos exacta (larga)*

$$0 \longrightarrow M_1 \xrightarrow{\varphi_2} M_2 \xrightarrow{\varphi_3} M_3 \longrightarrow \ldots\,.$$

Entonces para cualquier R-módulo N tenemos que

$$0 \longrightarrow \mathrm{Hom}(N, M_1) \xrightarrow{\overline{\varphi_1}} \mathrm{Hom}(N, M_2) \xrightarrow{\overline{\varphi_2}} \mathrm{Hom}(N, M_3) \xrightarrow{\overline{\varphi_3}} \dots$$

es un complejo.

Demostración:
Sea $\psi \in \mathrm{Im}(\overline{\varphi_i})$. Entonces, existe $\rho \in \mathrm{Hom}(M_i, N)$ tal que $\overline{\varphi_i}(\rho) = \psi$, luego tenemos lo siguiente:

$$\begin{aligned}
\overline{\varphi_{i+1}}(\psi) &= \overline{\varphi_{i+1}}(\overline{\varphi_i}(\rho)) \\
&= \overline{\varphi_{i+1}}(\varphi_i \rho) \\
&= \varphi_{i+1}(\varphi_i \rho) \\
&= (\varphi_{i+1}\varphi_i)\rho \\
&= \tilde{0}\rho \\
&= \tilde{0}
\end{aligned}$$

Por lo tanto, $\mathrm{Im}(\overline{\varphi_i}) \subseteq \mathrm{Ker}(\overline{\varphi_{i+1}})$. Es decir que la sucesión es un complejo. ■

Definición 1.60. *Dado F un R-módulo y $X \subseteq F$, diremos que X es una base si cumple lo siguiente:*

(a) el conjunto X genera a F, y

(b) para cada subconjunto finito $\{x_1, \dots, x_n\}$ de X se tiene que: si $\sum_{i=1}^{n} r_i x_i = 0$ entonces $r_i = 0$ para toda $i = 1, \dots, n$.

Diremos que F es libre si este posee una base.

Si la cardinalidad de dicha base es $n \in \mathbb{N}$, diremos que el rango de F es n y lo denotaremos por $\mathrm{rank}(F) = n$.

Existen módulos que tienen un conjunto generador pero que no tienen base, un ejemplo sencillo que rápidamente se puede generalizar es el siguiente:

Consideremos $M = \mathbb{Z}/6\mathbb{Z}$ como $\mathbb{Z}$-módulo. No es complicado ver que el conjunto $X = \{2 + 6\mathbb{Z}, 3 + 6\mathbb{Z}\}$ genera a M, sin embargo no cumple la propiedad (b) de la definición anterior pues $\{2 + 6\mathbb{Z}\}$ es subconjunto finito de X pero $3 \cdot (2 + 6\mathbb{Z}) = 0$ y $3 \neq 0$. De hecho, si suponemos que existe $X \subseteq M$ que genera a M y consideramos $X' = \{x_1 + 6\mathbb{Z}, \dots, x_n + 6\mathbb{Z}\} \subseteq X$, nuevamente X' tiene la siguiente propiedad $6(x_1 +$

$6\mathbb{Z}) + \ldots + 6(x_n + 6\mathbb{Z}) = 0$ pero $6 \neq 0$, así no se cumple la propiedad (b). De manera similar se puede probar que $Z/n\mathbb{Z}$ $(n \geq 2)$ no es libre como $\mathbb{Z}$-módulo.

Un hecho importante que debemos recalcar es que cada elemento $m \in F$ tiene una única expresión de la forma

$$m = \sum_{m_i \in X'} r_i m_i,$$

donde X' es un subconjunto finito de X.

Proposición 1.61 (Propiedad universal de los módulos libres). *Sea F un R-módulo libre con base $\mathcal{B} = \{m_i : i \in I\}$. Si M es un R-módulo y $\alpha : \mathcal{B} \to M$ una función, entonces existe un único morfismo $\psi : F \to M$ tal que $\psi\,|_{\mathcal{B}} = \alpha$, es decir que el siguiente diagrama conmuta:*

$$\begin{array}{ccc} \mathcal{B} & \xrightarrow{\ i\ } & F \\ & \searrow^{\alpha} & \downarrow{\scriptstyle \psi} \\ & & M \end{array}$$

Demostración:

Sea M un R-módulo y $\alpha : \mathcal{B} \to M$. Tomemos a, $b \in F$, como $\mathcal{B}$ es una base de F entonces

$$a = \sum_{i=1}^{n} r_i m_i \qquad b = \sum_{i=1}^{n} s_i m_i \tag{1.5}$$

(podemos considerar el mismo n y los mismo m_i, solamente debemos tener en cuneta que pondremos $r_i = 0$ y $s_i = 0$ cuando dicho m_i no aparezca en la representación de a y b respectivamente). Definamos

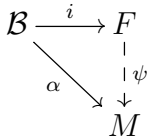
$$\begin{array}{rccc} \psi : & F & \longrightarrow & M \\ & a = \sum_{i=1}^{n} r_i m_i & \longmapsto & \sum_{i=1}^{n} r_i \alpha(m_i) \end{array}$$

por la unicidad de las representaciones de cada elemento la función ψ está bien definida. Ahora, veamos que ψ es morfismo de R-módulos. Sean $r \in R$ y a, $b \in F$, nuevamente podemos escribir a dichos elementos como en la Ecuación (1.5), entonces tenemos que:

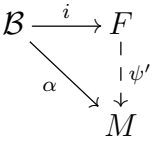
$$\begin{aligned} \psi(ra + b) &= \psi\left(r \sum_{i=1}^{n} r_i m_i + \sum_{i=1}^{n} s_i m_i \right) \\ &= \psi\left(\sum_{i=1}^{n} (rr_i) m_i + \sum_{i=1}^{n} s_i m_i \right) \end{aligned}$$

$$
\begin{aligned}
&= \psi\left(\sum_{i=1}^{n}((rr_i)m_i + s_i m_i)\right)\\
&= \psi\left(\sum_{i=1}^{n}((rr_i) + s_i)m_i\right)\\
&= \sum_{i=1}^{n}((rr_i) + s_i)\alpha(m_i)\\
&= \sum_{i=1}^{n}((rr_i)\alpha(m_i) + s_i\alpha(m_i))\\
&= \sum_{i=1}^{n}(rr_i)\alpha(m_i) + \sum_{i=1}^{n} s_i\alpha(m_i)\\
&= r\sum_{i=1}^{n} r_i\alpha(m_i) + \sum_{i=1}^{n} s_i\alpha(m_i)\\
&= r\psi\left(\sum_{i=1}^{n} r_i m_i\right) + \psi\left(\sum_{i=1}^{n} s_i m_i\right)\\
&= r\psi(a) + \psi(b)
\end{aligned}
$$

Por lo tanto α es morfismo de módulos. Ahora, dado $m_i \in \mathcal{B}$ tenemos que $\psi(i(m_i)) = \psi(m_i) = \psi(1m_i) = 1\alpha(m_i) = \alpha(m_i)$. Por lo tanto, el diagrama siguiente conmuta



Supongamos que existe $\psi' : F \to M$ tal que el diagrama conmuta



entonces para $a = \sum_{i=1}^{n} r_i m_i$ tenemos que

$$\begin{aligned}\psi'(a) &= \psi'\left(\sum_{i=1}^{n} r_i m_i\right)\\ &= \sum_{i=1}^{n} r_i \psi'(i(m_i))\\ &= \sum_{i=1}^{n} r_i \alpha(m_i)\\ &= \sum_{i=1}^{n} r_i \psi(i(m_i))\\ &= \psi\left(\sum_{i=1}^{n} r_i m_i\right)\\ &= \psi(a)\end{aligned}$$

Por lo tanto para ψ es único. ■

Teorema 1.62. *Sea R un anillo y F un R-módulo. Entonces, F es libre si y solo si $F \cong \bigoplus_{i\in I} Rx_i$, donde $x_i \in F$.*

Demostración:
Supongamos que F es libre. Entonces, F tiene una base $X \subseteq F$, tomemos $\bigoplus_{x\in X} Rx$. Afirmamos que $F \cong \bigoplus_{x_i\in X} Rx_i$, en efecto consideremos el siguiente morfismo:

$$\begin{array}{rccc}\alpha: & F & \longrightarrow & \bigoplus_{x_i\in X} Rx_i\\ & \sum_{i=1}^{n} r_i x_i & \longmapsto & (r_i x_i)\end{array}$$

Es claro que el morfismo es una biyección. Por lo tanto, $F \cong \bigoplus_{x_i\in X} Rx_i$.

Supongamos que $F \cong \bigoplus_{i\in I} Rx_i$, donde $x_i \in F$. No es difícil ver que $\{e_i : i \in I\}$ es una base de $\bigoplus_{i\in I} Rx_i$, es decir que este es libre y por tanto F lo es. ■

Lema 1.63. *Dado M un R-módulo. Entonces, existe un epimorfismo $\alpha : F \to M$ donde F es un R-módulo libre.*

Demostración:
Consideremos el conjunto $X = M \setminus \{0\}$ y el módulo $F = \bigoplus_{x^*\in X} Rx^*$. Consideremos el

siguiente morfismo:

$$\begin{array}{rccc} \alpha: & F & \longrightarrow & M \\ & \sum_{j=1}^{n} r_j x_j^* & \longmapsto & \sum_{j=1}^{n} r_j i(x_j^*) \end{array}$$

Definiendo de esta manera a α tenemos que este es un epimorfismo. ■

Teorema 1.64. *Sea* $0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$ *una sucesión exacta de R-módulos. Si* M' *y* M'' *son finitamente generados, entonces* M *también es finitamente generado.*

Demostración:

Como M' y M'' son finitamente generados, digamos $\{x_1', \ldots, x_n'\}$ y $\{x_1'', \ldots, x_m''\}$ son los conjuntos generadores de estos respectivamente. Como β es suprayectiva, entonces para cada $i \in \{1, \ldots, m\}$ existe $y_i \in M$ tal que $\beta(y_i) = x_i''$. Ahora, dado $m \in M$ tenemos que $\beta(m) = \sum_{i=1}^{m} r_i x_i = \beta(\sum_{i=1}^{m} r_i y_i)$, luego $m - \sum_{i=1}^{m} r_i y_i \in \mathrm{Ker}(\beta)$. Como la sucesión es exacta, obtenemos que $m - \sum_{i=1}^{m} r_i y_i = \alpha\left(\sum_{j=1}^{n} s_j x_j'\right) = \sum_{j=1}^{n} s_j \alpha(x_j')$. Así, tenemos que $m = \sum_{j=1}^{n} s_j \alpha(x_j') + \sum_{i=1}^{m} r_i y_i$. Es decir que M está generado por $\{\alpha(x_1'), \ldots, \alpha(x_n'), y_1, \ldots, y_m\}$. ■

Corolario 1.65. *Si* $0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0$ *una sucesión exacta de R-módulos con* M' *y* M'' *finitamente generados, entonces*

$$\mathrm{rank}(M) = \mathrm{rank}(M') + \mathrm{rank}(M'')$$

.

1.3. Producto tensorial

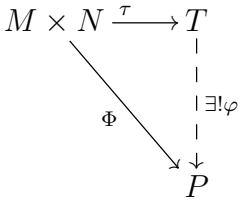
Definición 1.66. *Sean* M, N *y* P *R-módulos. Dada una función* $\Phi : M \times N \to P$, *si*

$$\begin{array}{rccc} \Gamma_{n'}: & M & \longrightarrow & P \\ & m & \longmapsto & \Phi(m, n') \end{array} \qquad \begin{array}{rccc} \Lambda_{m'}: & N & \longrightarrow & P \\ & n & \longmapsto & \Phi(m', n) \end{array}$$

son morfismos de R-módulos para cada $n' \in N$ *y* $m' \in M$, *decimos que* Φ *es* R-bilineal.

Teorema 1.67. *Sean M y N R-módulos. Entonces, existe un R-módulo T y un mapeo $\tau : M \times N \to T$ R-bilineal tal que la siguiente* ***propiedad universal*** *se cumple:*

Dado un mapeo R-bilineal $\Phi : M \times N \to P$ donde P es un R-módulo, entonces existe un único morfismo $\varphi : T \to P$ tal que $\varphi\tau = \Phi$. Es decir que, el siguiente diagrama conmuta:



Además, si existen T' y $\tau' : M \times N \to T'$ que cumplan dicha propiedad universal, entonces existe un único isomorfismo $\psi : T \to T'$ tal que $\psi\tau = \tau'$.

Demostración:

(*Existencia*) Consideremos el R-módulo $F = \bigoplus_{M\times N} R$ (el cual es libre y cuya base es $M \times N$). Los elementos de F son de la forma

$$\sum_{i=1}^{n} a_i(x_i, y_i), \qquad a_i \in R \text{ y } (x_i, y_i) \in M \times N.$$

Ahora, consideremos el submódulo D de F generado por los siguientes elementos:

$$(x + x', y) - (x, y) - (x', y), \qquad (ax, y) - a(x, y),$$

$$(x, y + y') - (x, y) - (x, y'), \qquad (x, ay) - a(x, y),$$

donde x, $x' \in M$, y, $y' \in N$ y $a \in R$.
Denotemos por T al cociente F/D y por $x \otimes y$ la clase de equivalencia en T, es decir $x \otimes y = (x, y) + D$. Entonces, tenemos que T es generado por dichos elementos, así cualquier elemento de T se escribe como

$$\sum_{i=1}^{n} a_i(x_i \otimes y_i) = \sum_{i=1}^{n} a_i((x_i, y_i) + D) = \sum_{i=1}^{n} a_i(x_i, y_i) + D, \quad (x_i, y_i) \in M \times N\,, a_i \in R.$$

Antes de proceder con la demostración, una aclaración importante es que podemos tomar el mismo índice n pues cada elemento $(x, y) \in F$ se puede expresar como com-

binación de los básicos.

Para cualesquiera x, $x' \in M$ y $y \in N$, como $(x+x', y) - (x, y) - (x', y) \in D$ es decir

$$(x + x') \otimes y = (x \otimes y) + (x' \otimes y). \tag{1.6}$$

Usando un argumente similar se muestra que para cualesquiera $x \in M$ y y, $y' \in N$

$$x \otimes (y + y') = (x \otimes y) + (x \otimes y'). \tag{1.7}$$

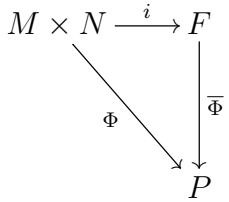
Ahora, para cualesquiera $a \in R$ y $(x, y) \in M \times N$, dado que $(ax, y) - a(x, y) \in D$ es decir

$$ax \otimes y = a(x \otimes y). \tag{1.8}$$

Similarmente se prueba que

$$x \otimes ay = a(x \otimes y). \tag{1.9}$$

Sea $\tau : M \times N \to T$ la función definida por $\tau(x, y) = x \otimes y$, de las Ecuaciones 1.6 – 1.9 tenemos que τ es R-bilineal. Sea P un R-módulo y $\Phi : M \times N \to P$, un morfismo R-bilineal. Como F es un módulo libre con base $M \times N$, por la propiedad universal de los módulos libres la función Φ extiende linealmente a un morfismo de R-módulos $\overline{\Phi} : F \to P$ tal que el siguiente diagrama conmuta:



Definamos $\varphi : T \to P$ por

$$\varphi(x \otimes y) = \overline{\Phi}(x, y) = \Phi(x, y) \qquad (\text{pues } \overline{\Phi} \text{ y } \Phi \text{ coinciden en } M \times N). \tag{1.10}$$

Veamos que $\overline{\Phi}$ anula a los generadores de D. Sean $x,\, x' \in M$ y $y,\, y' \in N$, tenemos

$$\begin{aligned}\overline{\Phi}((x+x',y)-(x,y)-(x',y)) &= \overline{\Phi}((x+x',y))-\overline{\Phi}((x,y))-\overline{\Phi}((x',y))\\ &= \Phi((x+x',y))-\Phi((x,y))-\Phi((x',y))\\ &= \Phi((x,y))+\Phi((x',y))-\Phi((x,y))-\Phi((x',y))\\ &= 0\end{aligned}$$

y similarmente tenemos que $\overline{\Phi}((x,y+y')-(x,y)-(x,y'))=0$. Ahora, dado $a \in R$ tenemos

$$\begin{aligned}\overline{\Phi}((ax,y)-a(x,y)) &= \overline{\Phi}((ax,y))-\overline{\Phi}(a(x,y)) && \text{(porque } \overline{\Phi} \text{ es } R\text{-lineal)}\\ &= \Phi((ax,y))-a\Phi((x,y)) && \text{(por (1.10))}\\ &= a\Phi((x,y))+a\Phi((x,y)) && \text{(ya que } \Phi \text{ es } R\text{-bilineal)}\\ &= 0\end{aligned}$$

de manera análoga se obtiene que $\overline{\Phi}((x,ay)-a(x,y))=0$. Verifiquemos que φ está bien definido; dados $x\otimes y = x'\otimes y'$, entonces

$$(x,y)-(x',y') \in D,$$

es decir, $(x,y)-(x',y')=\sum_i a_i d_i$ para algunos generadores d_i de D y $a_i \in R$. Ahora como $\overline{\Phi}$ anula a los generadores de D tenemos que

$$\overline{\Phi}((x,y)-(x',y')) = \overline{\Phi}\left(\sum_i a_i d_i\right) = \sum_i a_i \overline{\Phi}(d_i) = 0,$$

lo que $\overline{\Phi}((x,y)) = \overline{\Phi}((x',y'))$. Usando (1.10), tenemos que

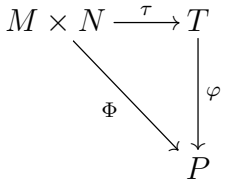
$$\varphi((x\otimes y)) = \varphi((x'\otimes y')),$$

con esto se prueba que φ está bien definida. De hecho, se verifica inmediatamente que φ es morfismo de R-módulos.

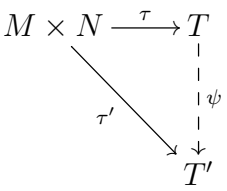
Por definición de τ y φ, para cualquier $(x,y) \in M\times N$

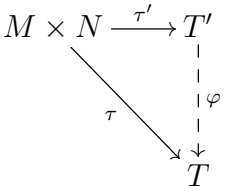
$$\Phi((x,y)) = \varphi((x\otimes y)) = \varphi(\tau((x,y))) = \varphi\tau((x,y)).$$

Es decir que el siguiente diagrama conmuta:

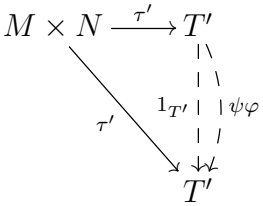


(*Unicidad*) Supongamos que T y $\tau : M \times N \to T$, y T' y $\tau' : M \times N \to T'$ cumplen la propiedad universal para T y T', respectivamente, es decir existen $\psi : T \to T'$ y $\varphi : T' \to T$ tal que $\psi\tau = \tau'$ y $\varphi\tau' = \tau$, respectivamente. Entonces tenemos los siguientes diagramas:

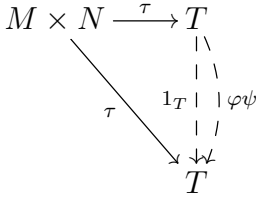




Ahora, notemos que $(\psi\varphi)\tau' = \psi\tau = \tau'$ pero por la propiedad universal, tenemos que $\psi\tau = 1_{T'}$, pues se tiene el siguiente diagrama:



Por otro lado, $(\varphi\psi)\tau = \varphi\tau' = \tau$, nuevamente se obtiene que $\varphi\psi = 1_T$, ya que se tiene el siguiente diagrama:



Por tanto ψ es isomorfismo y tiene la propiedad $\psi\tau = \tau'$. ■

Definición 1.68. *El módulo T de la proposición anterior es llamado producto tensorial de M y N, y lo denotaremos por $M \otimes_R N$ o simplemente $M \otimes N$ cuando no haya ambigüedad del anillo en el que se está trabajando.*

Una observación importante respecto a la notación $m \otimes n$, usada en la demostración de Teorema 1.67 es, en esencia ambigua si no especificamos el producto tensorial al cual pertenece. Por ejemplo, tomemos $R = \mathbb{Z}$, $M = \mathbb{Z}$, $N = N' = \mathbb{Z}_2$ y $M' = 2\mathbb{Z}$. Sea n es un entero no cero y consideremos $2 \otimes n$. Como elemento de $\mathbb{Z} \otimes \mathbb{Z}_2$ tenemos que $2 \otimes n = 1 \otimes 2n = 1 \otimes 0 = 0$, pero como elemento de $2\mathbb{Z} \times \mathbb{Z}_2$ no es cero, pues $1 \notin 2\mathbb{Z}$.

Una observación importante que debemos hacer es que la construcción hecha en la demostración del Teorema 1.67 en general no se utilizará, lo único que debemos tener en cuenta son las igualdades de Ecuaciones 1.6 – 1.9 y que $0 \otimes n = m \otimes 0 = 0$ en $M \otimes N$. Por ejemplo, se puede verificar que si m y n son coprimos, entonces $\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n = 0$. En efecto, como m y n son coprimos por el Lema de Bezout existen a y b tales que $am + bn = 1$. Entonces tenemos para $x \otimes y \in \mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n$

$$x \otimes y = 1(x \otimes y) = (am+bn)(x \otimes y) = (amx \otimes y) + (x \otimes bny) = (0 \otimes y) + (x \otimes 0) = 0 + 0 = 0.$$

Así, se prueba lo deseado, y como podemos observar en ningún momento se utilizó la construcción antes mencionada.

Proposición 1.69. *Sean M y N R-módulos. Entonces $M \otimes N$ es isomorfo a $N \otimes M$.*

Demostración:

Definamos $h : M \times N \to N \otimes M$ como $h(m, n) = n \otimes m$. Veamos que h es R-bilineal:

(a) Sean $n' \in N$ arbitraria pero fija, m_1, $m_2 \in M$ y $r \in R$. Entonces

$$\begin{aligned}
\Gamma_{n'}(m_1 + rm_2) &= h(m_1 + rm_2, n') \\
&= n' \otimes (m_1 + rm_2) \\
&= (n' \otimes m_1) + (n' \otimes rm_2) \\
&= (n' \otimes m_1) + r(n' \otimes m_2) \\
&= h(m_1, n') + rh(m_2, n') \\
&= \Gamma_{n'}(m_1) + r\Gamma_{n'}(m_2)
\end{aligned}$$

Por tanto $\Gamma_{n'}$ es morfismo de R-módulos para toda $n' \in N$.

(b) Por otro lado, sean $m' \in N$ arbitraria pero fija, $n_1, n_2 \in N$ y $r \in R$. Entonces

$$\begin{aligned}\Lambda_{m'}(n_1 + rn_2) &= h(m', n_1 + rn_2)\\ &= (n_1 + rn_2) \otimes m'\\ &= (n_1 \otimes m') + (rn_2 \otimes m')\\ &= (n_1 \otimes m') + r(n_2 \otimes m')\\ &= h(m', n_1) + rh(m', n_2)\\ &= \Lambda_{m'}(n_1) + r\Lambda_{m'}(n_2)\end{aligned}$$

Por tanto $\Lambda_{m'}$ es morfismo para toda $m' \in M$.

Así, h es R-bilineal, y por el Teorema 1.67 existe un morfismo $\varphi : M \otimes N \to N \otimes M$ tal que $\varphi(m \otimes n) = n \otimes m$. Ahora, consideremos $\psi : N \otimes M \to M \otimes N$ como $\psi(n \otimes m) = m \otimes n$ (por argumentos similares a los anteriores ψ es morfismo). Ahora, para $n \otimes m \in N \otimes M$ tenemos que $\varphi\psi(n \otimes m) = \varphi(\psi(n \otimes m)) = \varphi(m \otimes n) = n \otimes m$ y para $m \otimes n \in M \otimes N$ tenemos que $\psi\varphi(m \otimes n) = \psi(\varphi(m \otimes n)) = \psi(n \otimes m) = m \otimes n$. Por tanto φ es isomorfismo (es decir $M \otimes N \cong N \otimes M$). ■

Proposición 1.70. *Sea M un R-módulo. Entonces,$R \otimes M$ es isomorfo a M.*

Demostración:

Primero, consideremos $h : R \times M \to M$ dada por $h(a, m) = am$. Por la forma en la que está definida h obtenemos que esta es R-bilineal. Por el Teorema 1.67, existe $\varphi : R \otimes M \to M$ tal que $\varphi(r \otimes m) = rm$. Por otro lado, definamos $\psi : M \to R \otimes M$ como $\psi(m) = 1 \otimes m$, es inmediato que es un morfismo de R-módulos. Luego, para un elemento $m \in M$ tenemos que $\varphi\psi(m) = \varphi(\psi(m)) = \varphi(1 \otimes m) = 1m = m$; por otro lado, para $r \otimes m \in R \otimes M$ tenemos que

$$\psi\varphi(r \otimes m) = \psi(\varphi(r \otimes m)) = \psi(rm) = 1 \otimes rm = 1 \cdot r \otimes m = r \otimes m.$$

Por tanto φ es isomorfismo (es decir $R \otimes M \cong M$). ■ Ahora, ahondaremos en un concepto fundamental para entender resultados posteriores. Dados $\varphi : M \to M'$ y $\psi : N \to N'$ morfismos de R-módulos, podemos definir una nueva función $h : M \times N \to M \otimes N$ como $h(x, y) = f(x) \otimes g(y)$, veamos que h es R-bilineal es decir que hay que verificar que las funciones definidas en Definición 1.66 en efecto son morfismos.

(a) Sean $n' \in N$ arbitraria pero fija, m_1, $m_2 \in M$ y $r \in R$. Entonces

$$\begin{aligned}
\Gamma_{n'}(m_1 + rm_2) &= h(m_1 + rm_2, n') \\
&= f(m_1 + rm_2) \otimes g(n') \\
&= (f(m_1) + rf(m_2)) \otimes g(n') \\
&= (f(m_1) \otimes g(n')) + (rf(m_2) \otimes g(n')) \\
&= (f(m_1) \otimes g(n')) + r(f(m_2) \otimes g(n')) \\
&= h(m_1, n') + rh(m_2, n') \\
&= \Gamma_{n'}(m_1) + r\Gamma_{n'}(m_2)
\end{aligned}$$

Por tanto $\Gamma_{n'}$ es morfismo para toda $n' \in N$.

(b) Por otro lado, sean $m' \in M$ arbitraria pero fija, n_1, $n_2 \in N$ y $r \in R$. Entonces

$$\begin{aligned}
\Lambda_{m'}(n_1 + rn_2) &= h(m', n_1 + rn_2) \\
&= f(m') \otimes g(n_1 + rn_2) \\
&= f(m') \otimes (g(n_1) + rg(n_2)) \\
&= (f(m') \otimes g(n_1)) + (f(m') \otimes rg(n_2)) \\
&= (f(m') \otimes g(n_1)) + r(f(m') \otimes g(n_2)) \\
&= h(m', n_1) + rh(m', n_2) \\
&= \Lambda_{m'}(n_1) + r\Lambda_{m'}(n_2)
\end{aligned}$$

Por tanto $\Lambda_{m'}$ es morfismo para toda $m' \in M$.

Así, tenemos que h es R-bilineal. Entonces, la Propiedad universal del Teorema 1.67 nos asegura la existencia de un morfismo de R-módulos, al cual denotaremos como:

$$f \otimes g : M \otimes N \to M' \otimes N',$$

tal que $(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$ para todo $x \in M$ y $y \in N$. Ahora, dados $f' : M' \to M''$ y $g' : N' \to N''$ morfismos de R-módulos tenemos que $(f'f) \otimes (g'g)$ y $(f' \otimes g')(f \otimes g)$ coinciden en todos los elementos de $M \otimes N$. En efecto, dado $x \otimes y \in M \otimes N$ tenemos que

$$\begin{aligned}((f'f)\otimes(g'g))(x\otimes y) &= (f'f)(x)\otimes(g'\otimes g)(y)\\ &= f'(f(x))\otimes g'(g(y))\\ &= (f'\otimes g')(f(x)\otimes g(y))\\ &= (f'\otimes g')((f\otimes g)(x\otimes y))\\ &= ((f'\otimes g')(f\otimes g))(x\otimes y)\end{aligned}$$

Así, podemos concluir que $(f'f)\otimes(g'g) = (f'\otimes g')(f\otimes g)$.

Ahora, veamos algunas propiedades del producto tensorial y las sucesiones exactas. Recordemos que dado $\Phi : M\times N\to P$ mapeo R-bilineal, para cada $x\in M$ la función $\Lambda_x : N\to P$ definida por $\Lambda_x(y) = \Phi(x,y)$ es R-lineal, entonces tenemos que Φ induce la siguiente función R-lineal

$$\begin{array}{ccc} M & \longrightarrow & \mathrm{Hom}(N,P)\\ x & \longmapsto & \Lambda_x\end{array}$$

Inversamente, cualquier mapeo $\rho : M\to \mathrm{Hom}_R(N,P)$ de R-módulos induce la función R-bilineal siguiente

$$\begin{array}{ccc} M\times N & \longrightarrow & P\\ (x,y) & \longmapsto & \rho(x)(y)\end{array}$$

Entonces tenemos que el conjunto S de todas las funciones R-bilineales de $M\times N$ a P está en una correspondencia natural uno-a-uno con $\mathrm{Hom}(M,\mathrm{Hom}(N,P))$. Por otro lado S está en correspondencia uno-a-uno con $\mathrm{Hom}(M\otimes N,P)$. Por lo tanto, tenemos el siguiente isomorfismo natural

$$\mathrm{Hom}(M\otimes N,P)\cong\mathrm{Hom}(M,\mathrm{Hom}(N,P)). \tag{1.11}$$

Proposición 1.71. *Dada*

$$M'\xrightarrow{\varphi}M\xrightarrow{\psi}M''\longrightarrow 0 \tag{1.12}$$

una sucesión exacta de R-módulos y morfismos, y dado N un R-módulo. Entonces, la

sucesión

$$M' \otimes N \xrightarrow{\varphi\otimes 1} M \otimes N \xrightarrow{\psi\otimes 1} M'' \otimes N \longrightarrow 0 \tag{1.13}$$

donde 1 *representa la función identidad en* N*, es exacta.*

De manera similar a Proposición 1.56, pasar de (1.12) a (1.13) se le conoce como aplicar el funtor $- \otimes N$.

Demostración:

Sea P un R-módulo. Recordemos que $\mathrm{Hom}(N, P)$ es un R-módulo, entonces, dado que

$$0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$$

es exacta, por Proposición 1.56

$$0 \longrightarrow \mathrm{Hom}(M'', \mathrm{Hom}(N, P)) \longrightarrow \mathrm{Hom}(M, \mathrm{Hom}(N, P)) \longrightarrow \mathrm{Hom}(M', \mathrm{Hom}(N, P))$$

es exacta, por el isomorfismo antes mencionado tenemos que

$$0 \longrightarrow \mathrm{Hom}(M'' \otimes N, P) \longrightarrow \mathrm{Hom}(M \otimes N, P) \longrightarrow \mathrm{Hom}(M' \otimes N, P)$$

nuevamente es exacta, con P arbitrario. Usando la Proposición 1.56, obtenemos que

$$M' \otimes N \xrightarrow{\varphi\otimes 1} M \otimes N \xrightarrow{\psi\otimes 1} M'' \otimes N \longrightarrow 0$$

es exacta. ■

Corolario 1.72. *Dada*

$$0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0 \tag{1.14}$$

una sucesión exacta de R*-módulos y morfismos, y dado* N *un* R*-módulo. Entonces, la sucesión*

$$N \otimes M' \xrightarrow{1\otimes\varphi} N \otimes M \xrightarrow{1\otimes\psi} N \otimes M'' \longrightarrow 0 \tag{1.15}$$

es exacta.

Demostración:

Tenemos por la Proposición 1.71 que

$$M' \otimes N \xrightarrow{\varphi\otimes 1} M \otimes N \xrightarrow{\psi\otimes 1} M'' \otimes N \longrightarrow 0$$

es exacta. Luego usando la Proposición 1.69 tenemos que

$$N \otimes M' \xrightarrow{1\otimes\varphi} N \otimes M \xrightarrow{1\otimes\psi} N \otimes M'' \longrightarrow 0$$

es exacta. ■

De manera similar pasar de (1.14) a (1.15) se le conoce como aplicar el funtor $N\otimes -$.

Corolario 1.73. *Dada una sucesión de R-módulos exacta*

$$\ldots \xrightarrow{\varphi_3} M_3 \xrightarrow{\varphi_2} M_2 \xrightarrow{\varphi_1} M_1 \longrightarrow 0\,.$$

Entonces, para todo R-módulo N, las siguientes sucesiones

$$\ldots \xrightarrow{\varphi_3\otimes 1} M_3 \otimes N \xrightarrow{\varphi_2\otimes 1} M_2 \otimes N \xrightarrow{\varphi_1\otimes 1} M_1 \otimes N \longrightarrow 0$$

$$\ldots \xrightarrow{1\otimes\varphi_3} N \otimes M_3 \xrightarrow{1\otimes\varphi_2} N \otimes M_2 \xrightarrow{1\otimes\varphi_1} N \otimes M_1 \longrightarrow 0$$

son complejos.

Demostración:

Basta probar que alguna de ellas lo es, pues por la Proposición 1.69 automáticamente la otra lo será, entonces probaremos que la primera sucesión es un complejo. Sea $m\otimes n \in \mathrm{Im}(\varphi_i \otimes 1)$. Entonces, existe $m' \otimes n \in M_{i+1} \otimes N$ tal que $(\varphi_i \otimes 1)(m' \otimes n) = m \otimes n$. Luego

$$\begin{aligned}(\varphi_{i+1} \otimes 1)(m \otimes n) &= (\varphi_{i+1} \otimes 1)((\varphi_i \otimes 1)(m' \otimes n)) \\ &= \varphi_{i+1}(\varphi_i(m')) \otimes n \\ &= 0 \otimes n \\ &= 0\end{aligned}$$

Es decir que $m \otimes n \in \mathrm{Ker}(\varphi_{i+1} \otimes 1)$, así hemos probado lo deseado. ■

Proposición 1.74. *Sean R un anillo, I un ideal de R y M un R-módulo. Entonces $(R/I) \otimes_R M$ es isomorfo a M/IM.*

Demostración:
Primero, notemos que $0 \longrightarrow I \xrightarrow{i} R \xrightarrow{\pi} R/I \longrightarrow 0$ es exacta, entonces, por la Proposición 1.71, $I \otimes M \xrightarrow{i\otimes 1} R \otimes M \xrightarrow{\pi\otimes 1} R/I \otimes M \longrightarrow 0$ es exacta. En particular, tenemos que $\pi \otimes 1$ es sobreyectiva, así

$$R/I \otimes M \cong (R \otimes M)/\operatorname{Ker}(\pi \otimes 1) \cong M/\operatorname{Ker}(\pi \otimes 1),$$

y dado que la sucesión es exacta tenemos que

$$R/I \otimes M \cong M/\operatorname{Im}(i \otimes 1).$$

Por otro lado, tenemos que el siguiente diagrama conmuta

$$\begin{array}{ccc} I \otimes M & \xrightarrow{i\otimes 1_M} & R \otimes M \\ {\scriptstyle\lambda}\downarrow & & \downarrow{\scriptstyle\wr} \\ IM & \xrightarrow[i_{IM}]{} & M \end{array}$$

donde λ está dado por $\lambda(\sum x \otimes y) = \sum xy$. Así, $\operatorname{Im}(i \otimes 1_M) \cong \operatorname{Im}(i_{IM})$, es decir que $\operatorname{Im}(i \otimes 1_M) \cong IM$. Así, $R/I \otimes M \cong M/\operatorname{Im}(i \otimes 1) \cong M/\operatorname{Im}(i_{IM}) = M/IM$. ■

Lema 1.75. *Sea R un anillo e I un ideal de R. Si F es un R-módulo libre finitamente generado, entonces $F \otimes R/I$ es libre como R/I-módulo.*

Demostración:
Como F es un R-módulo libre, por el Teorema 1.62 tenemos que $F \cong \bigoplus_{i=1}^{n} R$, luego usando el [DF91, Teorema 17, p. 373] tenemos lo siguiente:

$$F \otimes R/I \cong \left(\bigoplus_{i=1}^{n} R\right) \otimes R/I \cong \bigoplus_{i=1}^{n} (R \otimes R/I).$$

De la Proposición 1.74 tenemos $R \otimes R/I \cong R/IR = R/I$, así $F \otimes R/I \cong \bigoplus_{i=1}^{n} R/I$. Es decir que $F \otimes R/I$ es libre como R/I-módulo. ■

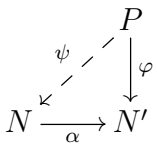
CAPÍTULO 2

FUNTORES EXT Y TOR

Como vimos en resultados del capítulo previo cuando aplicamos los funtores $\mathrm{Hom}(M,-)$, $\mathrm{Hom}(-,M)$, $M\otimes -$, $-\otimes M$ a sucesiones regulares, la exactitud se preserva con ciertas restricciones. Una pregunta natural que nos podríamos hacer es: ¿la exactitud se puede extender más allá de las sucesiones inducidas por esos funtores? La respuesta es sí, y es precisamente en este capítulo donde veremos que existen sucesiones largas que se inducen con los funtores anteriores, esto gracias a los conceptos de Ext y Tor.

2.1. Módulos proyectivos e inyectivos

Definición 2.1. *Dado R un anillo y P un R-módulo. Diremos que P es proyectivo si para todo epimorfismo $\alpha : N \to N'$ y todo morfismo $\varphi : P \to N'$, existe un morfismo $\psi : P \to N'$ tal que el siguiente diagrama conmuta:*



Proposición 2.2. *Dados un anillo R y un R-módulo P. Las siguientes afirmaciones son equivalentes:*

(a) P es proyectivo.

(b) Si $0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$ *es exacta, entonces*
$0 \longrightarrow \mathrm{Hom}(P, M') \xrightarrow{\overline{u}} \mathrm{Hom}(P, M) \xrightarrow{\overline{v}} \mathrm{Hom}(P, M'') \longrightarrow 0$ *es exacta.*

Demostración:

($\Rightarrow$) Supongamos que P es proyectivo. Sea $0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$ una sucesión exacta. Por Proposición 1.57 tenemos que la sucesión

$$0 \longrightarrow \mathrm{Hom}(P, M') \xrightarrow{\overline{u}} \mathrm{Hom}(P, M) \xrightarrow{\overline{v}} \mathrm{Hom}(P, M'')$$

es exacta. Resta verificar que es exacta en $\mathrm{Hom}(P, M'')$, para esto veremos que $\overline{v}$ es suprayectiva. Sea $\varphi \in \mathrm{Hom}(P, M'')$, como P es proyectivo y v es suprayectivo, entonces existe un morfismo $\psi : P \to M$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} & & P \\ & \overset{\psi}{\swarrow} & \downarrow \varphi \\ M & \xrightarrow[v]{} & M'' \end{array}$$

es decir que $\varphi = v\psi = \overline{v}(\psi)$ donde $\psi \in \mathrm{Hom}(P, M)$. Por lo tanto, $\overline{v}$ es suprayectivo.

($\Leftarrow$) Supongamos que toda sucesión exacta $0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$ induce la siguiente sucesión exacta:

$$0 \longrightarrow \mathrm{Hom}(P, M') \xrightarrow{\overline{u}} \mathrm{Hom}(P, M) \xrightarrow{\overline{v}} \mathrm{Hom}(P, M'') \longrightarrow 0\,.$$

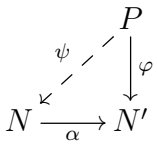
Sea $\alpha : N \to N'$ un epimorfismo y $\varphi : P \to N'$ un morfismo. Así, tenemos que

$$0 \longrightarrow \mathrm{Ker}(\varphi) \xrightarrow{i} N \xrightarrow{\alpha} N' \longrightarrow 0$$

es exacta. Entonces, por hipótesis, la siguiente sucesión es exacta

$$0 \longrightarrow \mathrm{Hom}(P, \mathrm{Ker}(\alpha)) \xrightarrow{\overline{i}} \mathrm{Hom}(P, N) \xrightarrow{\overline{\alpha}} \mathrm{Hom}(P, N') \longrightarrow 0$$

en particular, $\overline{\alpha}$ es suprayectiva. Así, para $\varphi \in \mathrm{Hom}(P, N')$ existe $\psi \in \mathrm{Hom}(P, N)$ tal que $\varphi = \overline{\alpha}(\psi) = \alpha\psi$, es decir que el siguiente diagrama conmuta:



Por lo tanto, P es proyectivo. ■

Proposición 2.3. *Sean P y P' R-módulos. Si P y P' son proyectivos, entonces $P \oplus P'$ es proyectivo.*

Demostración:

Supongamos que P y P' son proyectivos y sea $0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$ exacta. Por la proposición anterior tenemos que las siguientes sucesiones

$$0 \longrightarrow \mathrm{Hom}(P, M') \xrightarrow{\overline{u}} \mathrm{Hom}(P, M) \xrightarrow{\overline{v}} \mathrm{Hom}(P, M'') \longrightarrow 0\,,$$

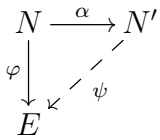
$$0 \longrightarrow \mathrm{Hom}(P', M') \xrightarrow{\overline{u}} \mathrm{Hom}(P', M) \xrightarrow{\overline{v}} \mathrm{Hom}(P', M'') \longrightarrow 0$$

también son exactas. Ahora, dado que $\mathrm{Hom}_R(P \oplus P', N) \cong \mathrm{Hom}_R(P, N) \oplus \mathrm{Hom}_R(P, N)$ para cada R-módulo N ([DF91, Proposición 29, p. 388]), obtenemos que:

$$0 \longrightarrow \mathrm{Hom}(P \oplus P', M') \xrightarrow{\overline{u}} \mathrm{Hom}(P \oplus P', M) \xrightarrow{\overline{v}} \mathrm{Hom}(P \oplus P', M'') \longrightarrow 0$$

es exacta. Nuevamente por la proposición anterior tenemos que $P \oplus P'$ es proyectivo. ■

Definición 2.4. *Dado R un anillo y E un R-módulo. Diremos que E es inyectivo, si para todo monomorfismo $\alpha : N \to N'$ y todo morfismo $\varphi : N \to E$, con N y N' R-módulos, existe un morfismo $\psi : N' \to E$ tal que el siguiente diagrama conmuta:*



Proposición 2.5. *Dados un anillo R y un R-módulo E. Las siguientes afirmaciones son equivalentes:*

(a) E es inyectivo.

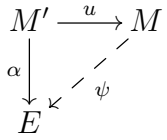
(b) Si $0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$ *es exacta, entonces*
$0 \longrightarrow \mathrm{Hom}(M'', E) \xrightarrow{\overline{v}} \mathrm{Hom}(M, E) \xrightarrow{\overline{u}} \mathrm{Hom}(M', E) \longrightarrow 0$ *es exacta.*

Demostración:

($\Rightarrow$) Supongamos que E es inyectivo. Sea $0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$ una sucesión exacta. Por la Proposición 1.56 tenemos que la sucesión

$$0 \longrightarrow \mathrm{Hom}(M'', E) \xrightarrow{\overline{v}} \mathrm{Hom}(M, E) \xrightarrow{\overline{u}} \mathrm{Hom}(M', E)$$

es exacta. Resta verificar que es exacta en $\mathrm{Hom}(M', E)$, para esto veremos que $\overline{u}$ es suprayectiva. Sea $\alpha \in \mathrm{Hom}(M', E)$, por hipótesis tenemos que u es inyectivo y además E es inyectivo, entonces existe un morfismo $\psi : M \to E$ tal que el siguiente diagrama conmuta:



es decir que $\alpha = \psi u = \overline{u}(\psi)$ donde $\psi \in \mathrm{Hom}(M, E)$. Por tanto $\overline{u}$ es suprayectiva.

($\Leftarrow$) Supongamos que toda sucesión exacta $0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$ induce la siguiente sucesión exacta

$$0 \longrightarrow \mathrm{Hom}(M'', E) \xrightarrow{\overline{v}} \mathrm{Hom}(M, E) \xrightarrow{\overline{u}} \mathrm{Hom}(M', E) \longrightarrow 0\,.$$

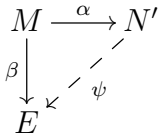
Sean $\alpha : M \to N'$ un monomorfismo y $\beta : M \to E$. Entonces, tenemos que

$$0 \longrightarrow M \xrightarrow{\alpha} N' \xrightarrow{\pi} N'/\operatorname{Im}(\alpha) \longrightarrow 0$$

es exacta. Entonces, por hipótesis, la siguiente sucesión es exacta

$$0 \longrightarrow \mathrm{Hom}(N'/\operatorname{Im}(\alpha), E) \xrightarrow{\overline{\pi}} \mathrm{Hom}(N', E) \xrightarrow{\overline{\alpha}} \mathrm{Hom}(M, E) \longrightarrow 0$$

en particular, $\overline{\alpha}$ es suprayectiva. Así, para $\beta \in \mathrm{Hom}(M, E)$ existe $\psi \in \mathrm{Hom}(N', E)$ tal que $\beta = \overline{\alpha}(\psi) = \psi\alpha$, es decir que el siguiente diagrama conmuta:



Por lo tanto N es inyectivo. ■

Proposición 2.6. *Sean E y E' R-módulos. Si E y E' son inyectivos, entonces $E \oplus E'$ es inyectivo.*

Demostración:
Supongamos que E y E' son inyectivos y sea $0 \longrightarrow M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$ exacta. Por la proposición anterior tenemos que las siguientes sucesiones

$$0 \longrightarrow \mathrm{Hom}(M'', E) \xrightarrow{\overline{u}} \mathrm{Hom}(M, E) \xrightarrow{\overline{v}} \mathrm{Hom}(M', E) \longrightarrow 0\,,$$

$$0 \longrightarrow \mathrm{Hom}(M'', E') \xrightarrow{\overline{u}} \mathrm{Hom}(M, E') \xrightarrow{\overline{v}} \mathrm{Hom}(M', E') \longrightarrow 0$$

también son exactas. Ahora, dado que $\mathrm{Hom}_R(N, E \oplus E') \cong \mathrm{Hom}_R(N, E) \oplus \mathrm{Hom}_R(N, E')$ para cada R-módulo N ([DF91, Proposición 29, p. 388]), obtenemos que:

$$0 \longrightarrow \mathrm{Hom}(M'', E \oplus E') \xrightarrow{\overline{u}} \mathrm{Hom}(M, E \oplus E') \xrightarrow{\overline{v}} \mathrm{Hom}(M', E \oplus E') \longrightarrow 0$$

es exacta. Nuevamente por la proposición anterior tenemos que $E \oplus E'$ es inyectivo. ■

2.2. Resoluciones

Definición 2.7. *Sea M un R-módulo. Definimos una resolución de M como la sucesión exacta de R-módulos:*

$$M_\bullet : \ \ldots \xrightarrow{\varphi_3} M_2 \xrightarrow{\varphi_2} M_1 \xrightarrow{\varphi_1} M_0 \xrightarrow{\alpha} M \longrightarrow 0.$$

Definición 2.8. *Dados un R-módulo M y una resolución de M como la siguiente:*

$$F_\bullet : \ \ldots \xrightarrow{\varphi_3} F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\alpha} M \longrightarrow 0.$$

Si cada F_i es libre, diremos que es una resolución libre de M.

Proposición 2.9. *Dado M un R-módulo, entonces existe una resolución libre.*

Demostración:

Por el Lema 1.63 tenemos que para M existe un epimorfismo $\alpha : F_0 \to M$ donde F_0 es libre , es decir que la sucesión $F \xrightarrow{\alpha} M \longrightarrow 0$ es exacta. Ahora, tomemos $\text{Ker}(\alpha)$ y nuevamente usando el Lema 1.63 existe un epimorfismo $\varphi_1 : F_1 \to \text{Ker}(\alpha)$ entonces tenemos el siguiente diagrama:

$$\begin{array}{ccccccc} F_1 & \xrightarrow{i\varphi_1} & F_0 & \xrightarrow{\alpha} & M & \longrightarrow & 0 \\ & \searrow^{\varphi_1} & \uparrow{\scriptstyle i} & & & & \\ & & \text{Ker}(\alpha) & & & & \end{array}$$

Verifiquemos que la fila es exacta en F_0. Consideremos $x \in \text{Ker}(\alpha)$, como φ_1 es epimorfismo, existe $y \in F_1$ tal que $\varphi_1(y) = x$, luego $i\varphi_1(y) = i(x) = x$. Así, $x \in \text{Im}(i\varphi)$ (i.e. $\text{Ker}(\alpha) \subseteq \text{Im}(i\varphi)$). Ahora, dado $x \in \text{Im}(i\varphi)$, tenemos que existe $y \in F_1$ tal que $i\varphi_1(y) = x$. Luego, $\alpha(x) = \alpha(i\varphi_1(y)) = \alpha(i(\varphi(y))) = \alpha(\varphi_1(y)) = 0$ pues $\varphi_1(y) \in \text{Ker}(\alpha)$ (i.e. $\text{Im}(i\varphi_1) \subseteq \text{Ker}(\alpha)$). Así, la fila es exacta. Continuando de manera similar tenemos el siguiente diagrama:

$$\begin{array}{ccccccccccccccc} \ldots & \xrightarrow{i\varphi_{n+1}} & F_n & \xrightarrow{i\varphi_n} & F_{n-1} & \xrightarrow{i\varphi_{n-1}} & \ldots & \xrightarrow{i\varphi_2} & F_1 & \xrightarrow{i\varphi_1} & F_0 & \xrightarrow{\alpha} & M & \longrightarrow & 0 \\ & & & \searrow^{\varphi_n} & \uparrow{\scriptstyle i} & & & & & \searrow^{\varphi_1} & \uparrow{\scriptstyle i} & & & & \\ & & & & \text{Ker}(i\varphi_{n-1}) & & & & & & \text{Ker}(\alpha) & & & & \end{array}$$

Donde la fila es exacta y cada F_i es libre. Por tanto tenemos que para M existe una resolución por libres. ■

Definición 2.10. *Dados un R-módulo M y una resolución de M como la siguiente:*

$$P_\bullet : \ \ldots \xrightarrow{\varphi_3} P_2 \xrightarrow{\varphi_2} P_1 \xrightarrow{\varphi_1} P_0 \xrightarrow{\alpha} M \longrightarrow 0$$

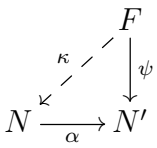
Si cada P_i sea proyectivo, diremos que es una resolución proyectiva de M.

Lema 2.11. *Dado un R-módulo F libre, entonces F es proyectivo.*

Demostración:

Dado F un R-módulo libre. Sean $\alpha : N \to N'$ un epimorfismo y $\psi : F \to N'$ un morfismo. Como F es libre existe $\mathcal{B} = \{b_i : i \in I\}$ una base de este. Entonces $\psi(i(b_i)) \in N'$ para todo $b_i \in \mathcal{B}$, como α es epimorfismo, existe $a_i \in N$ tal que $\alpha(a_i) = \psi(i(b_i))$.

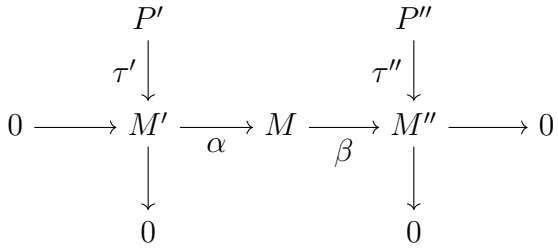
Definamos $\lambda : \mathcal{B} \to N$ como $\lambda(b_i) = a_i$, esta función, por la Proposición 1.61 este induce un morfismo $\kappa : F \to N$ tal que $\kappa(i(b_i)) = a_i$ para toda $b_i \in \mathcal{B}$. Entonces $\alpha(\kappa(i(b_i))) = \alpha(a_i) = \psi(i(b_i))$, por lo tanto $\alpha\kappa i = \psi i$ por la unicidad en Proposición 1.61 $\alpha\kappa = \psi$ es decir que el siguiente diagrama conmuta:



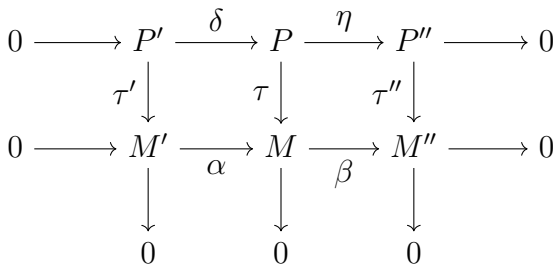
Por lo tanto, F es proyectivo. ■

Corolario 2.12. *Dado M un R-módulo, entonces existe una resolución por proyectivos.*

Lema 2.13. *Consideremos el siguiente diagrama de R-módulos*

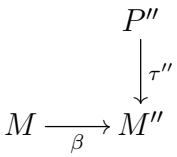


Con P' y P'' proyectivos y la fila es exacta. Entonces existe un R-módulo proyectivo P y un morfismo $\tau : P \to M$ tal que el siguiente diagrama conmuta:



Demostración:

Primero, consideremos el siguiente diagrama



donde β es epimorfismo por hipótesis. Entonces, dado que P'' es proyectivo, existe $\psi : P'' \to M$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccc} & & P'' \\ & \overset{\psi}{\swarrow} & \downarrow{\scriptstyle \tau''} \\ M & \xrightarrow[\beta]{} & M'' \end{array}$$

Ahora, por la Proposición 2.3 definamos $P = P' \oplus P''$ y $\tau : P \to M$ como $\tau(x, y) = \alpha\tau'(x) + \psi(y)$ para cada $(x, y) \in P' \oplus P''$. No es complicado ver que τ en efecto es morfismo y además podemos considerar a δ y η como $\delta(x) = (x, 0)$ y $\eta(x, y) = y$. Sea $m \in M$, entonces como τ'' es suprayectiva tenemos que $\beta(m) = \tau''(y)$ para algún $y \in P''$. Por otro lado $\beta(m - \psi(y)) = \beta(m) - \beta\psi(y) = \beta(m) - \beta(m) = 0$, es decir que $m - \psi(y) \in \mathrm{Ker}(\beta) = \mathrm{Im}(\alpha)$, así que $m - \psi(m) = \alpha(x_1)$ para algún $x_1 \in M'$ y como τ' es suprayectiva tenemos que $x_1 = \tau'(x)$ para algún $x \in P'$. Así, si tomamos $(x, y) \in P$ tenemos que:

$$\tau(x, y) = \alpha\tau'(x) + \psi(y) = \alpha(x_1) + \psi(y) = m - \psi(y) + \psi(y) = m.$$

Por lo tanto τ es suprayectiva.

Verifiquemos que el diagrama conmuta: sea $x \in P$ entonces

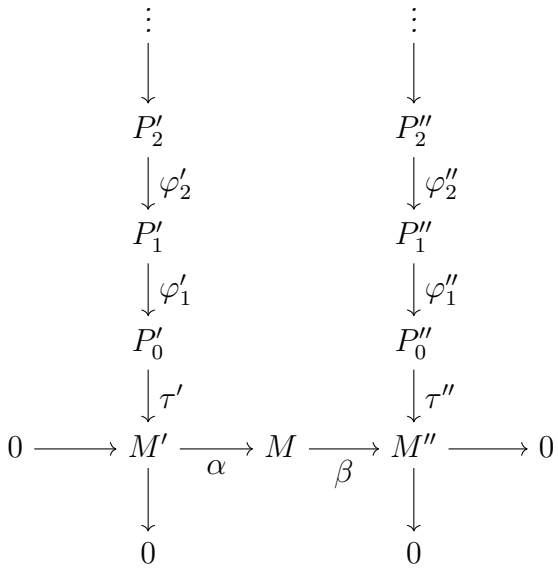
$$\tau\delta(p) = \tau(x, 0) = \alpha\tau'(x) + \psi(0) = \alpha\tau'(x).$$

Por otro lado, dado $(x, y) \in P$ tenemos que

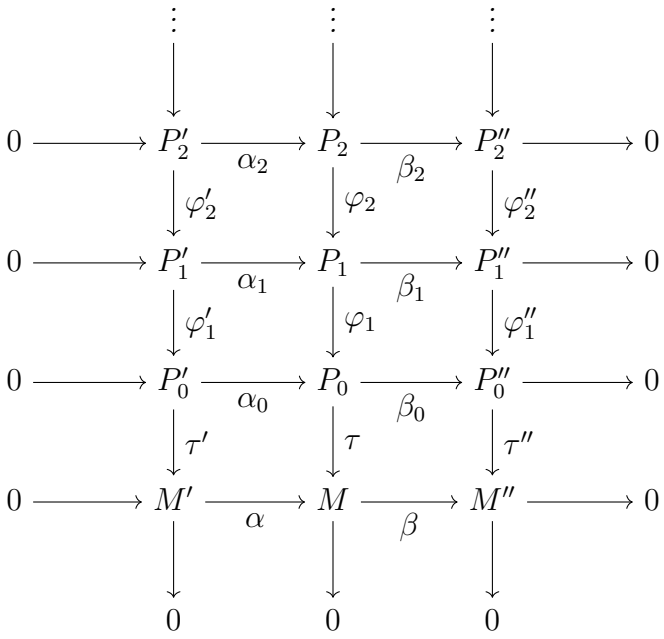
$$\tau''\eta(x, y) = \tau''(y) \quad \text{y} \quad \beta\tau(x, y) = \beta(\alpha\tau'(x) + \psi(y)) = \beta\alpha\tau'(x) + \beta\psi(y) = \tau''(y).$$

■

Lema 2.14 (Lema de la herradura para proyectivos)**.** *Consideremos el siguiente diagrama de R-módulos:*



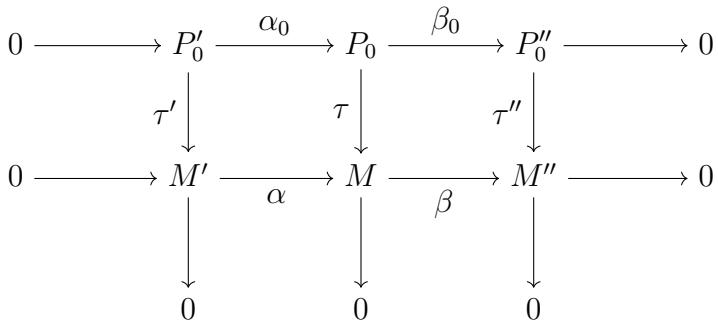
Donde las columnas son resoluciones proyectivas de M' y M'' respectivamente y la fila es exacta. Entonces, existen R-módulos proyectivos P_i $(i \geq 0)$ tales que el siguiente diagrama conmuta, y además cada fila es exacta:



Demostración:

La demostración es constructiva y para el caso de P_0 ya lo tenemos por el lema anterior.

Ahora, para $i \geq 1$ consideremos P_i como la suma directa de P_i' y P_i''. Teniendo en cuenta el diagrama:



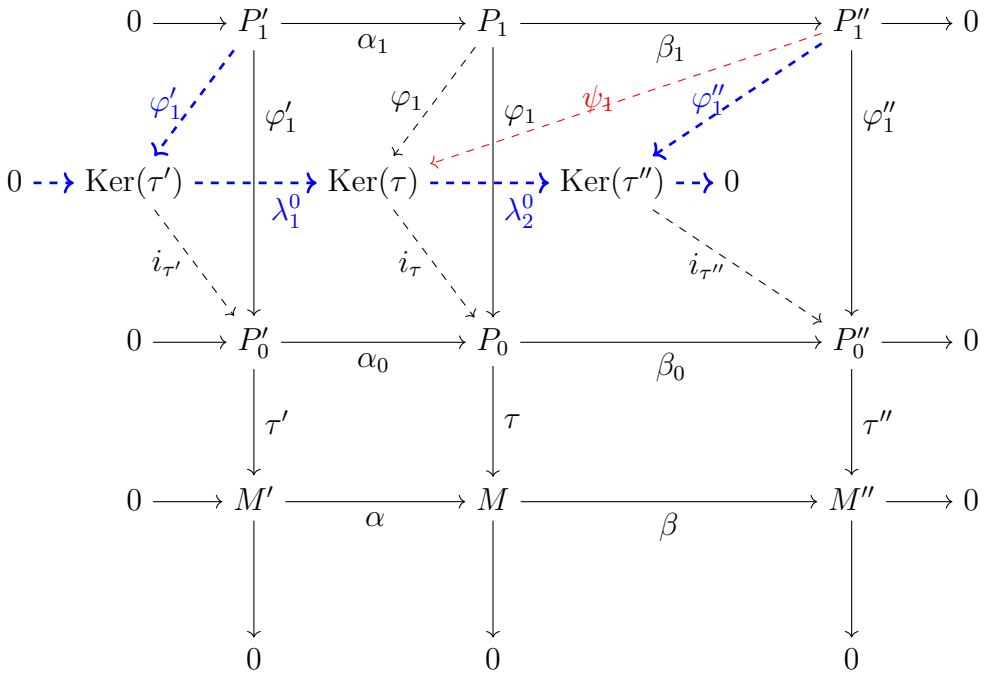
y por el Teorema 1.55 tenemos que la siguiente sucesión es exacta:

$$0 \longrightarrow \mathrm{Ker}(\tau') \xrightarrow{\lambda_1^0} \mathrm{Ker}(\tau) \xrightarrow{\lambda_2^0} \mathrm{Ker}(\tau'') \longrightarrow \mathrm{coker}(\tau') \ .$$

Dado que τ' es suprayectiva, la anterior se reduce a la siguiente:

$$0 \longrightarrow \mathrm{Ker}(\tau') \xrightarrow{\lambda_1^0} \mathrm{Ker}(\tau) \xrightarrow{\lambda_2^0} \mathrm{Ker}(\tau'') \longrightarrow 0 \ .$$

Ahora, dado que las columnas son exactas obtenemos que $\mathrm{Im}(\varphi_i') = \mathrm{Ker}(\varphi_{i-1}')$ y $\mathrm{Im}(\varphi_i'') = \mathrm{Ker}(\varphi_{i-1}'')$, entonces sí podemos correstringir φ_i' y φ_i'' a $\mathrm{Ker}(\varphi_{i-1}')$ y $\mathrm{Ker}(\varphi_{i-1}'')$ respectivamente. Así, tenemos $\lambda_2^0 : \mathrm{Ker}(\tau) \to \mathrm{Ker}(\tau'')$ es suprayectiva y $\varphi_1'' : P_1'' \to \mathrm{Ker}(\tau'')$, entonces existe $\psi_1 : P_1'' \to \mathrm{Ker}(\tau)$ tal que $\lambda_2\psi_1 = \varphi_1''$ pues P_1'' es proyectivo. Entonces, definamos $\varphi_1 : P_1 \to P_0$ como $\varphi_1(x, y) : \lambda_1^0\varphi_1'(x) + \psi_1(y)$, es decir que estamos aplicando el lema anterior al diagrama de flechas azules del siguiente diagrama:



Y dado que $i_{\tau'}$, i_τ, $i_{\tau''}$ son inyectivas, el diagrama en lineas continuas de lo anterior es conmutativo. Continuando de esta manera, construiremos el diagrama que deseamos. ■

Observemos que en la demostración anterior tenemos que la columna central que construimos es una resolución proyectiva de M.

Bajo ciertas condiciones los conceptos de módulo inyectivo y proyectivo coinciden ([Lam99, Teorema 15.9]), sin embargo en nuestro caso no es así. Es decir, existen módulos que son inyectivos y no son proyectivos o viceversa, la pregunta natural que relaciona el lema anterior con lo ya explicado es ¿los módulos libres son también inyectivos? La respuesta es no, hay módulos libres que no son inyectivos. Veamos el siguiente ejemplo:

Ejemplo 2.15. Consideremos a $\mathbb{Z}$ como $\mathbb{Z}$-módulo. Este es libre, pues $\mathbb{Z} = \bigoplus_{i=1}^{1} \mathbb{Z}1$. Sin embargo, este no es inyectivo ya que, por resultados de teoría de grupos "*un grupo abeliano aditivo es inyectivo si y solo si es un grupo divisible*" [Rot02, Corolario 7.73, p. 485], sin embargo 2 no divide a 3 y por tanto $\mathbb{Z}$ no es divisible.

Sin embargo, a pesar de ser conceptos distintos en la teoría que estamos trabajando, resulta que, haciendo las adaptaciones necesarias, tenemos resultados similares a los de módulos proyectivos. Por esta razón, se suele encontrar en la literatura que la teoría de módulos inyectivos es el dual de la teoría de módulos inyectivos.

Definición 2.16. *Dados un R-módulo M y una resolución de M como la siguiente:*

$$0 \longrightarrow M \xrightarrow{\alpha} E_0 \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} E_2 \xrightarrow{\varphi_3} \dots$$

Si cada E_i es inyectivo, diremos que es una resolución inyectiva de M.

El siguiente lema establece una propiedad significativa para el estudio de módulos sobre anillos conmutativos. Sin embargo, su demostración implica el uso de conceptos y resultados de teoría de grupos, que no son el enfoque principal en este contexto. Por lo tanto, no profundizaremos en los detalles de la demostración aquí. No obstante, los interesados pueden consultar la teoría necesaria y los detalles de la demostración en [Alu09, Capítulo VIII].

Lema 2.17. *Sea M un R-módulo. Entonces, existe un morfismo inyectivo $\alpha : M \to N$ donde N es un R-módulo inyectivo.*

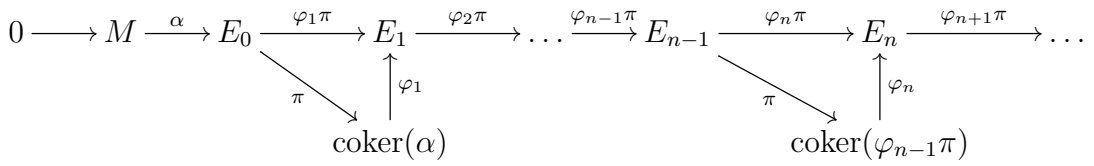
La prueba del hecho anterior puede ser consultada en [Alu09, Capítulo 8, Corolario 6.12, p. 551].

Proposición 2.18. *Sea M un R-módulo. Entonces, M tiene una resolución inyectiva* $0 \longrightarrow M \xrightarrow{\alpha} E_\bullet$.

Demostración:
Por el lema anterior, tenemos que existe un morfismo inyectivo $\alpha : M \to E_0$ donde E_0 es un R-módulo inyectivo. Ahora, consideremos $\operatorname{coker}(\alpha)$, usando nuevamente el lema anterior tenemos que existe $\varphi_1 : \operatorname{coker}(\alpha) \to E_1$ con E_1 inyectivo, entonces tenemos el siguiente diagrama:

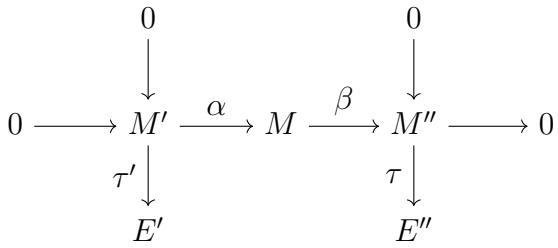
$$\begin{array}{ccccccc} 0 & \longrightarrow & M & \xrightarrow{\alpha} & E_0 & \xrightarrow{\varphi_1 \pi} & E_1 \\ & & & & & \searrow^{\pi} & \uparrow{\scriptstyle \varphi_1} \\ & & & & & & \operatorname{coker}(\alpha) \end{array}$$

La prueba de la exactitud en la fila es similar a la de la proposición 2.9. Continuando de esta manera obtenemos el siguiente diagrama donde la fila es la resolución que buscamos:

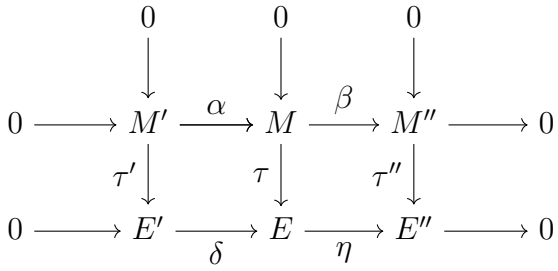


Análogamente a los módulos proyectivos, tenemos los siguientes resultados, cuyas pruebas son si el similares a las de la sección mencionada.

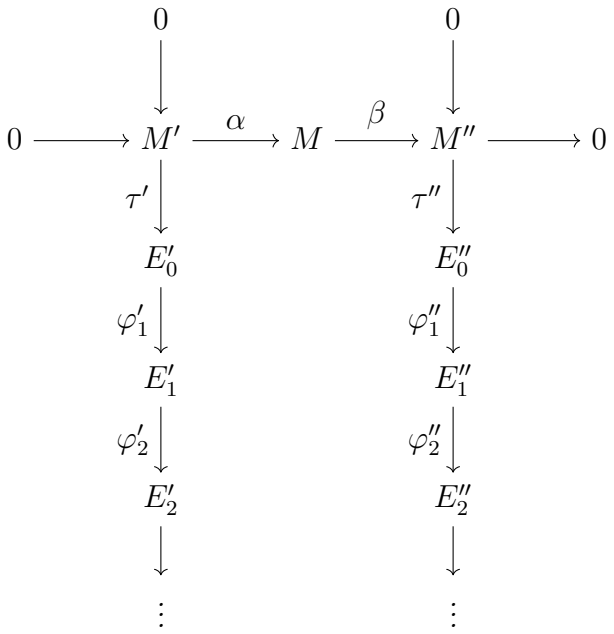
Lema 2.19. *Consideremos el siguiente diagrama*



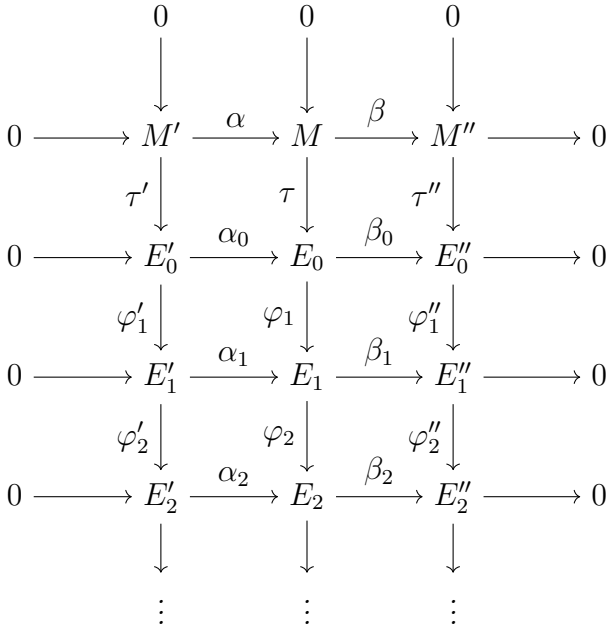
Donde E' y E'' son módulos inyectivos y la fila es exacta. Entonces, existe un R-módulo inyectivo E tal que el siguiente diagrama conmuta:



Lema 2.20 (Lema de la herradura para inyectivos)**.** *Consideremos el siguiente diagrama:*



Donde las columnas son resoluciones inyectivas de M' y M'' respectivamente y la fila es exacta. Entonces, existen R-módulos E_i ($i \geq 0$) tales que el siguiente diagrama conmuta, y además cada fila es exacta:



2.3. Tor y Ext

Definición 2.21. *Dados R-módulos M, N y $P_\bullet$ una resolución por proyectivos de este, digamos*

$$P_\bullet : \ \ldots \xrightarrow{\varphi_2} P_1 \xrightarrow{\varphi_1} P_0 \xrightarrow{\alpha} M \longrightarrow 0. \tag{2.1}$$

Consideremos el complejo

$$\ldots \xrightarrow{\varphi_2} P_1 \xrightarrow{\varphi_1} P_0 \longrightarrow 0\,. \tag{2.2}$$

que resulta de eliminar M. El R-módulo $\mathrm{Tor}_i^R(M,N)$ $(i \geq 0)$ se define como:

$$\mathrm{Tor}_i^R(M,N) = \frac{\mathrm{Ker}(1 \otimes \varphi_i)}{\mathrm{Im}(1 \otimes \varphi_{i+1})}.$$

Donde $1 \otimes \varphi_i$ es el morfismo que se obtiene de aplicar el funtor $N \otimes -$ a la sucesión (2.2), es decir:

$$\ldots \xrightarrow{1\otimes\varphi_2} N \otimes P_1 \xrightarrow{1\otimes\varphi_1} N \otimes P_0 \longrightarrow 0. \tag{2.3}$$

Antes de proceder con resultados relevantes de la definición anterior, debemos hacer una aclaración. En resultados previos aseguramos la existencia de resoluciones por proyectivos, sin embargo no se asegura que dicha resolución por proyectivos sea única. A pesar de esto, el siguiente resultado asegura que no importa la resolución que tomemos, el módulo de la definición anterior está bien definido.

Teorema 2.22. *Supongamos que M es un R módulo con dos resoluciones por proyectivos digamos:*

$$P_\bullet : \ \ldots \longrightarrow P_2 \xrightarrow{\varphi_2} P_1 \xrightarrow{\varphi_1} P_0 \xrightarrow{\alpha} M \longrightarrow 0\,,$$

$$P'_\bullet : \ \ldots \longrightarrow P'_2 \xrightarrow{\varphi'_2} P'_1 \xrightarrow{\varphi'_1} P'_0 \xrightarrow{\alpha'} M \longrightarrow 0\,.$$

Entonces, existen $\lambda_i : P_i \to P'_i$ *tales que el siguiente diagrama conmuta*

$$\begin{array}{ccccccccccc}
\ldots & \longrightarrow & P_2 & \xrightarrow{\varphi_2} & P_1 & \xrightarrow{\varphi_1} & P_0 & \xrightarrow{\alpha} & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \lambda_2} & & \downarrow{\scriptstyle \lambda_1} & & \downarrow{\scriptstyle \lambda_0} & & \downarrow{\scriptstyle 1_M} & & \\
\ldots & \longrightarrow & P'_2 & \xrightarrow[\varphi'_2]{} & P'_1 & \xrightarrow[\varphi'_1]{} & P'_0 & \xrightarrow[\alpha']{} & M & \longrightarrow & 0
\end{array}$$

Además, si existen $\lambda'_i : P_i \to P'_i$ *con la misma condición de antes, entonces existe* $D_i : P_i \to P'_{i+1}$ *tal que* $\lambda_i - \lambda'_i = \varphi'_{i+1}D_i + D_{i+1}\varphi_i$.

Demostración:

El resultado se aleja de los fines del trabajo, pero la demostración puede ser consultada en [Osb00, Proposición 3.1, p. 41]. ■

Corolario 2.23. *Dados* R*-módulos* M *y* N*, el módulo* $\mathrm{Tor}_i^R(M,N)$ *está bien definido para toda* $i \geq 0$.

La prueba del hecho anterior puede ser consultada en [Wei95, Teorema 2.7.2, p. 58].

Proposición 2.24. *Dado un* R*-módulo* M*, tenemos que* $\mathrm{Tor}_0^R(M,N) \cong N \otimes_R M$.

Demostración:

Sea una resolución por proyectivos $\ldots \xrightarrow{\varphi_1} P_0 \xrightarrow{\alpha} M \longrightarrow 0$ de M, en particular tenemos que $P_1 \xrightarrow{\varphi_1} P_0 \xrightarrow{\alpha} M \longrightarrow 0$ es exacta. Entonces, de la Proposición 1.71 se sigue que

$$N \otimes P_1 \xrightarrow{1\otimes\varphi_1} N \otimes P_0 \xrightarrow{1\otimes\varphi_0} N \otimes M \longrightarrow 0 \tag{2.4}$$

es exacta.

Por otro lado, tenemos $N \otimes P_2 \xrightarrow{1\otimes\varphi_2} N \otimes P_1 \xrightarrow{1\otimes\varphi_1} N \otimes P_0 \longrightarrow 0$. Luego de la exactitud de (2.4) tenemos que:

$$\begin{aligned}
N \otimes M &\cong \frac{N \otimes P_0}{\mathrm{Ker}(1 \otimes \varphi_0)} \\
&= \frac{N \otimes P_0}{\mathrm{Im}(1 \otimes \varphi_1)} \\
&= \mathrm{Tor}_0^R(M,N)
\end{aligned}$$

■

Proposición 2.25. *Sea R un anillo y $0 \longrightarrow M \longrightarrow M' \longrightarrow M'' \longrightarrow 0$ una sucesión exacta corta de R-módulos. Entonces, para cualquier R-módulo N existe una sucesión exacta:*

$$\begin{array}{l}
\ldots \longrightarrow \mathrm{Tor}_{i+1}^R(M,N) \longrightarrow \mathrm{Tor}_{i+1}^R(M',N) \longrightarrow \mathrm{Tor}_{i+1}^R(M'',N) \\
\quad \longrightarrow \mathrm{Tor}_{i}^R(M,N) \longrightarrow \mathrm{Tor}_{i}^R(M',N) \longrightarrow \mathrm{Tor}_{i}^R(M'',N) \\
\quad \longrightarrow \mathrm{Tor}_{1}^R(M,N) \longrightarrow \mathrm{Tor}_{1}^R(M',N) \longrightarrow \mathrm{Tor}_{1}^R(M'',N) \\
\quad \longrightarrow M \otimes N \longrightarrow M' \otimes N \longrightarrow M'' \otimes N \longrightarrow 0
\end{array}$$

Demostración:

En esencia, la demostración es inmediata del Lema de la serpiente y Lema de la herradura. ■

Proposición 2.26. *Si R es un anillo y M es un R-módulo. Entonces, para todo R-módulo libre P se tiene que $\mathrm{Tor}_i^R(M,P) = 0$ para $i \geq 1$.*

Demostración:

Como P es libre, tenemos que $\ldots \longrightarrow 0 \longrightarrow P \longrightarrow P \longrightarrow 0$ es una resolución por proyectivos de P. Luego, considerando

$$\ldots \longrightarrow 0 \longrightarrow P \otimes M \longrightarrow 0$$

obtenemos lo que se desea. ■

Corolario 2.27. *Sea R un anillo y $\alpha : N \to S$ un monomorfismo de R-módulos. Si F es un R-módulo libre, entonces $1_F \otimes \alpha : F \otimes N \to F \otimes S$ es inyectivo.*

Demostración:

Consideremos la siguiente sucesión exacta

$$0 \longrightarrow N \xrightarrow{\alpha} S \longrightarrow S/\operatorname{Im}(\alpha) \longrightarrow 0\,.$$

Entonces, por Proposición 2.25 tenemos que

$$\mathrm{Tor}_1^R(F, S/\operatorname{Im}(\alpha)) \longrightarrow F \otimes N \xrightarrow{1_F \otimes \alpha} F \otimes S \longrightarrow F \otimes S/\operatorname{Im}(\alpha) \longrightarrow 0\,.$$

Por la proposición anterior $\mathrm{Tor}_1^R(F, S/\operatorname{Im}(\alpha)) = 0$, y por tanto $1_F \otimes \alpha$ es inyectiva. ■

Definición 2.28. *Dado un R-módulo M y $E_\bullet$ una resolución inyectiva digamos:*

$$E_\bullet : \; 0 \longrightarrow M \xrightarrow{\alpha} E_0 \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} \dots\,. \tag{2.5}$$

Consideremos el complejo

$$0 \longrightarrow E_0 \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} \dots\,. \tag{2.6}$$

que resulta de eliminar M.
El R-módulo $\mathrm{Ext}_R^i(N, M)$ $(i \geq 0)$ se define como:

$$\mathrm{Ext}_R^i(N, M) = \frac{\operatorname{Ker}(\overline{\varphi_{i+1}})}{\operatorname{Im}(\overline{\varphi_i})}.$$

Donde $\overline{\varphi_i}$ es el morfismo que se obtiene de aplicar el funtor $\mathrm{Hom}(N, -)$ a la sucesión (2.6), es decir:

$$0 \longrightarrow \mathrm{Hom}(N, E_0) \xrightarrow{\overline{\varphi_1}} \mathrm{Hom}(N, E_1) \xrightarrow{\overline{\varphi_2}} \dots \tag{2.7}$$

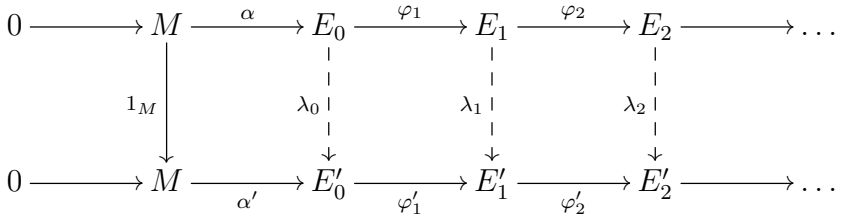
Similarmente a la aclaración en proyectivos, hemos demostrado que todo R-módulo admite una resolución inyectiva sin embargo tampoco hemos probado que esta sea única. A pesar de esto, el resultado siguiente nos ayudará a probar que la definición anterior no depende de la resolución que consideremos.

Teorema 2.29. *Supongamos que M es un R-módulo con dos resoluciones inyectivas, digamos:*

$$E_\bullet : \; 0 \longrightarrow M \xrightarrow{\alpha} E_0 \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} E_2 \longrightarrow \dots\,,$$

$$E'_\bullet : \; 0 \longrightarrow M \xrightarrow[\alpha']{} E'_0 \xrightarrow[\varphi'_1]{} E'_1 \xrightarrow[\varphi'_2]{} E'_2 \longrightarrow \dots\,.$$

Entonces. existen $\lambda_i : E_i \to E'_i$ tales que el siguiente diagrama conmuta:



Además, si existen $\lambda_i' : E_i \to E_i'$ *que cumplan la misma propiedad, entonces existen* $D_i : E_i \to E_{i-1}'$ *tales* $\lambda_i - \lambda_i' = \varphi_i' D_i + D_{i+1}\varphi_{i+1}$.

Corolario 2.30. *Dados* R*-módulos* M *y* N *el módulo* $\mathrm{Ext}_R^i(N, M)$ *está bien definido para toda* $i \geq 0$.

La demostración de este hecho puede ser consultada en [Wei95, Teorema 2.7.6, p. 63].

Proposición 2.31. *Dado* M *un* R*-módulo, tenemos que* $\mathrm{Ext}_R^0(N, M) \cong \mathrm{Hom}_R(N, M)$.

Demostración:
Consideremos una resolución inyectiva $0 \longrightarrow M \xrightarrow{\alpha} E_0 \xrightarrow{\varphi_1} \dots$ de M, en particular la sucesión $0 \longrightarrow M \xrightarrow{\alpha} E_0 \xrightarrow{\varphi_1} E_1$ es exacta. Entonces, del Proposición 1.57 se sigue que:

$$0 \longrightarrow \mathrm{Hom}_R(N, M) \xrightarrow{\overline{\alpha}} \mathrm{Hom}_R(N, E_0) \xrightarrow{\overline{\varphi_1}} \mathrm{Hom}_R(N, E_1) \tag{2.8}$$

es exacta.

Por otro lado, tenemos $0 \longrightarrow \mathrm{Hom}(N, E_0) \xrightarrow{\overline{\varphi_1}} \mathrm{Hom}(N, E_1) \xrightarrow{\overline{\varphi_2}} \mathrm{Hom}(N, E_2)$. Así, tenemos que:

$$\begin{aligned}
\mathrm{Ext}_R^0(N, M) &= \frac{\mathrm{Ker}(\overline{\varphi_1})}{0} \\
&= \mathrm{Ker}(\overline{\varphi_1}) \\
&= \mathrm{Im}(\overline{\alpha}) \\
&\cong \mathrm{Hom}_R(N, M) && \text{(pues } \overline{\alpha} \text{ es inyectiva.)}
\end{aligned}$$

■

Proposición 2.32. *Sea R un anillo y $0 \longrightarrow M \longrightarrow M' \longrightarrow M'' \longrightarrow 0$ una sucesión exacta corta de R-módulos. Entonces, para cualquier R-módulo N existe una sucesión exacta:*

$$
\begin{array}{l}
0 \longrightarrow \mathrm{Hom}_R(N,M) \longrightarrow \mathrm{Hom}_R(N,M') \longrightarrow \mathrm{Hom}_R(N,M'') \\
\longrightarrow \mathrm{Ext}^1_R(N,M) \longrightarrow \mathrm{Ext}^1_R(N,M') \longrightarrow \mathrm{Ext}^1_R(N,M'') \\
\longrightarrow \mathrm{Ext}^i_R(N,M) \longrightarrow \mathrm{Ext}^i_R(N,M') \longrightarrow \mathrm{Ext}^i_R(N,M'') \\
\longrightarrow \mathrm{Ext}^{i+1}_R(N,M) \longrightarrow \mathrm{Ext}^{i+1}_R(N,M') \longrightarrow \mathrm{Ext}^{i+1}_R(N,M'') \longrightarrow \dots
\end{array}
$$

Demostración:

En esencia, la demostración es inmediata del Lema de la serpiente y Lema de la herradura. ■

Proposición 2.33. *Sean R un anillo y M un R-módulo. Si $r_- : M \to M$ denota el morfismo multiplicar por r en M, entonces el morfismo $\overline{r_-} : \mathrm{Ext}^i_R(N,M) \to \mathrm{Ext}^i_R(N,M)$ es mismo el morfismo sobre $\mathrm{Ext}^i_R(N,M)$ para todo R-módulo N y toda $i \geq 0$.*

Demostración:

Consideremos $0 \longrightarrow M \xrightarrow{\alpha} E_0 \xrightarrow{\varphi_1} \dots$ una resolución inyectiva de M. Entonces, definamos $\lambda_i : E_i \to E_i$ como el morfismo multiplicar por r, entonces obtenemos el siguiente diagrama conmutativo:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & M & \xrightarrow{\alpha} & E_0 & \xrightarrow{\varphi_1} & E_1 & \xrightarrow{\varphi_2} & \dots \\
 & & \downarrow{\scriptstyle r_-} & & \downarrow{\scriptstyle \lambda_0} & & \downarrow{\scriptstyle \lambda_1} & & \\
0 & \longrightarrow & M & \xrightarrow[\alpha]{} & E_1 & \xrightarrow[\varphi_1]{} & E_2 & \xrightarrow[\varphi_2]{} & \dots
\end{array}
$$

Entonces, aplicando el funtor $\mathrm{Hom}_R(N,-)$ tenemos el siguiente diagrama que también resulta ser conmutativo:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}(N,M) & \xrightarrow{\overline{\alpha}} & \mathrm{Hom}(N,E_0) & \xrightarrow{\overline{\varphi_1}} & \mathrm{Hom}(N,E_1) & \xrightarrow{\overline{\varphi_2}} & \cdots \\ & & \downarrow{\scriptstyle \overline{r_-}} & & \downarrow{\scriptstyle \overline{\lambda_0}} & & \downarrow{\scriptstyle \overline{\lambda_1}} & & \\ 0 & \longrightarrow & \mathrm{Hom}(N,M) & \xrightarrow[\overline{\alpha}]{} & \mathrm{Hom}(N,E_1) & \xrightarrow[\overline{\varphi_1}]{} & \mathrm{Hom}(N,E_2) & \xrightarrow[\overline{\varphi_2}]{} & \cdots \end{array}$$

Ahora, podemos definir $\overline{r_-} : \mathrm{Ext}^n_R(N,M) \to \mathrm{Ext}^n_R(N,M)$ como $\overline{r_-}(\beta + \mathrm{Im}(\varphi_n)) = (\lambda_n\beta) + \mathrm{Im}(\varphi_n)$.

Pero, para toda $x \in N$ tenemos que $\lambda_n\beta(x) = \lambda_n(\beta(x)) = r(\beta(x))$, por lo tanto $\overline{r_-}(\beta + \mathrm{Im}(\varphi_n)) = r(\beta) + \mathrm{Im}(\varphi_n) = r(\beta + \mathrm{Im}(\varphi_n))$. ■

Lema 2.34. *Sea R un anillo, M, N R-módulos y $r \in \mathrm{Ann}(N)$, entonces r anula a $\mathrm{Ext}^n_R(N,M)$ para toda $n \geq 0$.*

Demostración:

Consideremos $\beta + \mathrm{Im}(\varphi_n) \in \mathrm{Ext}^n_R(N,M)$. Ahora, para cada $x \in N$ tenemos que $r\beta(x) = \beta(rx) = \beta(0) = 0$, luego $r(\beta + \mathrm{Im}(\varphi_n)) = 0$. ■

A pesar de la siguiente teoría no es indispensable en el desarrollo del trabajo, es importante tenerla en cuenta, pues con los ajustes pertinentes se obtienen los mismos resultados.

La siguiente definición es una manera "alternativa" de calcular el módulo Ext, y el resultado inmediato a esta (el cual no se demostrará) indica que es indiferente el enfoque con el que se quiera trabajar.

Definición 2.35. *Dado un R-módulo M y $P_\bullet$ una resolución proyectiva de M digamos:*

$$P_\bullet : \ \ldots \xrightarrow{\varphi_2} P_1 \xrightarrow{\varphi_1} P_0 \xrightarrow{\alpha} M \longrightarrow 0 \, . \tag{2.9}$$

Consideremos el complejo

$$\ldots \xrightarrow{\varphi_2} P_1 \xrightarrow{\varphi_1} P_0 \longrightarrow 0 \, . \tag{2.10}$$

que resulta de eliminar M.

El R-módulo $\mathrm{Ext}^i_R(M,N)$ $(i \geq 0)$ se define como:

$$\mathrm{Ext}^i_R(M,N) = \frac{\mathrm{Ker}(\overline{\varphi_i})}{\mathrm{Im}(\overline{\varphi_{i+1}})}.$$

Donde $\overline{\varphi_i}$ *es el morfismo que se obtiene de aplicar el funtor* $\mathrm{Hom}(-,N)$ *a la sucesión* (2.10)*, es decir:*

$$0 \longrightarrow \mathrm{Hom}(P_0,N) \xrightarrow{\overline{\varphi_1}} \mathrm{Hom}(P_1,N) \xrightarrow{\overline{\varphi_2}} \dots \tag{2.11}$$

Teorema 2.36. *Dados* M *un* R*-módulo,* $P_\bullet$ *una resolución proyectiva de* M *y* $E_\bullet$ *una resolución inyectiva de* M*. Entonces, para toda* $n \geq 0$ *y para todo* R*-módulo* N*, se tiene que* $\mathrm{Ext}^n_R(M,N) \cong \mathrm{Ext}^n_R(N,M)$ *.*

La prueba de este teorema puede ser consultada en [Rot79, Teorema 7.8, p. 196]. Además, similarmente a la teoría desarrollada por inyectivos se tienen los siguientes resultados:

Proposición 2.37. *Dado* M *un* R*-módulo, tenemos que* $\mathrm{Ext}^0_R(M,N) \cong \mathrm{Hom}_R(M,N)$*.*

Proposición 2.38. *Sea* R *un anillo y* $0 \longrightarrow M \longrightarrow M' \longrightarrow M'' \longrightarrow 0$ *una sucesión exacta corta de* R*-módulos. Entonces, para cualquier* R*-módulo* N *existe una sucesión exacta:*

$$\begin{aligned}
&0 \longrightarrow \mathrm{Hom}_R(M'',N) \longrightarrow \mathrm{Hom}_R(M',N) \longrightarrow \mathrm{Hom}_R(M,N) \\
&\hookrightarrow \mathrm{Ext}^1_R(M'',N) \longrightarrow \mathrm{Ext}^1_R(M',N) \longrightarrow \mathrm{Ext}^1_R(M,N) \\
&\hookrightarrow \mathrm{Ext}^i_R(M'',N) \longrightarrow \mathrm{Ext}^i_R(M',N) \longrightarrow \mathrm{Ext}^i_R(M,N) \\
&\hookrightarrow \mathrm{Ext}^{i+1}_R(M'',N) \longrightarrow \mathrm{Ext}^{i+1}_R(M',N) \longrightarrow \mathrm{Ext}^{i+1}_R(M,N) \longrightarrow \dots
\end{aligned}$$

Nos podríamos preguntar porqué si ambas construcciones son, de cierta manera, iguales se desarrollan de manera independiente. La respuesta es sencilla, resulta que el Teorema 2.36 solo es valido cuando R es conmutativo, también, es por esta razón que siempre existe una resolución por inyectivos.

Para Tor tenemos resultados análogos, pero su prueba pasa por bicomplejos de canea lo cual queda fuera del alcance de este trabajo, sin embargo el lector puede consultar estos resultados en [Wei95, Sección 2.6].

CAPÍTULO 3

TEOREMA DE AUSLANDER-BUCHSBAUM

pleta para comprender estos conceptos clave y, al final, nos lleve a apreciar la importancia y el alcance del teorema de Auslander-Buchsbaum en la matemática contemporánea.

En el vasto mundo del álgebra y la teoría de módulos, conceptos como sucesiones regulares, profundidad y dimensión proyectiva son cruciales. Exploraremos estos temas, centrándonos en el poderoso teorema de Auslander-Buchsbaum, vital en geometría algebraica y más. A lo largo, veremos cómo estos conceptos se entrelazan, ofreciendo una visión profunda en matemáticas contemporáneas.

3.1. Sucesiones regulares

Definición 3.1. *Dado un R-módulo M. Diremos que $x \in R$ es un elemento M-regular si cada que $xm = 0$ con $m \in M$ implique que $m = 0$. En caso contrario, diremos que x es un divisor de cero en M.*

Por ejemplo, en $\mathbb{Z}$, como $\mathbb{Z}$-módulo, todos los elementos no cero son $\mathbb{Z}$-regulares, pues $\mathbb{Z}$ es un dominio entero. Otro ejemplo inmediato es un campo $\mathbb{F}$, en este como $\mathbb{F}$-espacio vectorial todos sus elementos no cero son $\mathbb{F}$-regulares.

Proposición 3.2. *Dados R un anillo Noetheriano y M un R-módulo. Entonces, el conjunto de los divisores de cero en M es igual a la unión de todos los primos asociados de M.*

Demostración:
Sea $r \in R$ es un divisor de cero en M, entonces para algún $m \neq 0$ tenemos que $rm = 0$. Por el Corolario 1.39 existe un $s \in R$ tal que $P = \mathrm{Ass}_R(sm)$ es un primo asociado, y claramente $r \in P$. Por lo tanto, $x \in \bigcup_{P_i \in \mathrm{Ass}_R(M)} P_i$.

Si $p \in \bigcup_{P_i \in \mathrm{Ass}_R(M)} P_i$, entonces $p \in P_i$ para algún P_i. Como P_i es un primo asociado $P_i = \mathrm{Ann}_R(m)$ para algún $m \in M$. Así $pm = 0$, es decir que p es un divisor de cero. ■

Definición 3.3. *Dados un anillo R y M un R-módulo. Una sucesión $\mathbf{x} := x_1, x_2, \ldots, x_n$ de elementos de R es llamada sucesión M-regular o simplemente M-regular si se cumple lo siguiente:*

(a) x_1 es un elemento M-regular.

(b) x_i es un elemento $M/(x_1, \ldots, x_{i-1})M$-regular para todo $i = 2, \ldots, n$, donde $(x_1, \ldots, x_{i-1})$ es el ideal generado por $\{x_1, \ldots, x_{i-1}\}$.

(c) $M/(x_1, \ldots, x_n)M = M/\mathbf{x}M \neq 0$.

En caso de que $M = R$ simplemente diremos que $\mathbf{x}$ es un sucesión regular. Y de cumplirse unicamente (a) y (b) diremos que $\mathbf{x}$ es un M-sucesión débil.

Ejemplo 3.4. El ejemplo clásico de sucesión regular es $\mathbf{x} := X_1, X_2 \ldots, X_n$ de indeterminadas en el anillo de polinomios $R[X_1, X_2, \ldots, X_n]$.

Ejemplo 3.5. Otro ejemplo, que no resulta tan evidente es el siguiente, dado K un campo entonces, en $R = K[x, y, z]$ la sucesión x, $y(1-x)$, $z(1-x)$ es regular. Tenemos lo siguiente:

(a) x es regular, pues R es un dominio entero.

(b) Sea $f \in R/(x)R$ tal que $f \cdot (y(1-x)) = 0$ en el cociente $R/(x)$, entonces tenemos que

$$\begin{aligned} f \cdot (y(1-x)) = 0 &\Rightarrow f \cdot (y - yx) = 0 \\ &\Rightarrow fy - fyx = 0 && (fyx \in (x)R) \\ &\Rightarrow fy = 0 && (\text{como } R/(x)R \cong K[y,z]) \\ &\Rightarrow f = 0 \end{aligned}$$

por lo tanto $y(1-x)$ es $R/(x)R$-regular.

(c) Análogamente se prueba que $z(1-x)$ es $R/(x, y(1-x))R$-regular, pues tenemos que $R/(x, y(1-x))R \cong K[z]$.

(d) Ahora, tenemos que $R/(x, y(1-x), z(1-x))R \cong F$ y por tanto no es cero. Así tenemos que x, $y(1-x)$, $z(1-x)$ es regular en $R = K[x, y, z]$.

Es lógico asumir que si una sucesión regular puede ser permutada de varias formas, esas permutaciones también mantendrían su regularidad inherente. Sin embargo, esto no siempre es el caso. Por ejemplo, la sucesión $y(1-x)$, $z(1-x)$, x no es regular, a pesar de que los elementos son los mismos del ejemplo anterior. No es regular pues $y \in R/(y(1-x))R$ y $y \neq 0$ pero $y(z(1-x)) = z(y(1-x)) = z \cdot 0 = 0$, es decir que $z(1-x)$ no es $R/(y(1-x))R$-regular.

El siguiente resultado establece las condiciones bajo las cuales una sucesión regular puede ser permutada y aún mantener su regularidad.

Proposición 3.6. *Sea R un anillo local Noetheriano, M un R-módulo finito regular y $\mathbf{x} = x_1, x_2, \ldots, x_n$ una M-sucesión. Entonces cada permutación de $\mathbf{x}$ es una M-sucesión.*

Demostración:

Recordemos que toda permutación de elementos es producto de transposiciones, entonces basta verificar para $x_1, \ldots, x_{i+1}, x_i, \ldots, x_n$. Como $x_1, \ldots, x_{i-1}$ cumple *(a)* y *(b)* de la Definición 3.3, entonces basta tomar $i = 1$ y sin pérdida de generalidad podemos suponer que $\mathbf{x} = x_1, x_2$. Es decir, debemos verificar que x_2, x_1 es una M-sucesión. Primero, consideremos el siguiente morfismo

$$\begin{array}{rccc} \lambda_{x_2}: & M & \longrightarrow & M \\ & m & \longmapsto & x_2 m \end{array}$$

Sea $m \in \operatorname{Ker}(\lambda_{x_2})$, es decir que $\lambda_{x_2}(m) = x_2 m = 0$. Afirmamos que $m \in x_1 M$. De lo contrario $m + x_1 M \neq 0 \in M/x_1 M$ luego $x_2 m + x_1 M \neq 0$, al ser x_2 un elemento $M/x_1 M$-regular lo cual es absurdo pues $x_2 m = 0$ y así $x_2 m + x_1 M = 0$. Por tanto $m \in x_1 M$, es decir que $m = x_1 m'$ con $m' \in M$. Entonces $\lambda_{x_2}(m) = x_2(x_1 m') = 0$, pero $x_2(x_1 m') = x_1(x_2 m') = 0$ y por hipótesis x_1 es M regular tenemos que $x_2 m' = 0$, en consecuencia $m' \in \operatorname{Ker}(\lambda_{x_2})$, es decir que $\operatorname{Ker}(\lambda_{x_2}) = x_1 \operatorname{Ker}(\lambda_{x_2})$. Como el anillo

es Noetheriano y M es finito, tenemos que $\mathrm{Ker}(\lambda_{x_2})$ es finitamente generado, y dado que el anillo es local (x_1) está contenido en el radical de Jacobson. Así, por el lema de Nakayama $\mathrm{Ker}(\lambda_{x_2}) = 0$. Es decir, que x_2 es un elemento M-regular.

Ahora, sea $m + x_2M \in M/x_2M$ tal que $x_1m + x_2M = 0$. Entonces, $x_1m \in x_2M$, es decir que $x_1m = x_2m'$ para algún $m' \in M$. Luego, por hipótesis, x_2 es un elemento M/x_1M regular y usando que $x_1m+x_1M = 0 = x_2m'+x_1M = x_2(m'+x_1M)$, entonces $m' + x_1M = 0$, es decir que $m' = x_1m''$ con $m'' \in M$. Luego, $x_1m = x_2x_1m''$ luego $x_1(m - x_2m'') = 0$, como x_1 es M-regular, entonces $m = x_2m''$. Por último, tenemos que $m + x_2M = x_2m'' + x_2M = 0$ por tanto x_1 es M/x_2M-regular. Así, x_2, x_1 es una M-sucesión. ■

Proposición 3.7. *Sea M un R-módulo, y $\mathbf{x}$ una M-sucesión débil. Entonces, una sucesión exacta de R-módulos*

$$M' \longrightarrow M \longrightarrow M'' \longrightarrow 0\ ,$$

induce la siguiente sucesión exacta

$$M'/\mathbf{x}M' \longrightarrow M/\mathbf{x}M \longrightarrow M''/\mathbf{x}M'' \longrightarrow 0\ .$$

Demostración:
Como $M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ es exacta, usando el Corolario 1.72, tenemos que

$$R/\mathbf{x} \otimes M' \longrightarrow R/\mathbf{x} \otimes M \longrightarrow R/\mathbf{x} \otimes M'' \longrightarrow 0$$

es exacta. Luego, usando la Proposición 1.74, se obtiene que

$$M'/\mathbf{x}M' \longrightarrow M/\mathbf{x}M \longrightarrow M''/\mathbf{x}M'' \longrightarrow 0$$

es exacta. ■

Corolario 3.8. *Sea R un anillo y*

$$N_\bullet : \ \ldots \longrightarrow N_2 \xrightarrow{\varphi_2} N_1 \xrightarrow{\varphi_1} N_0 \longrightarrow 0$$

una sucesión exacta. Si $\mathbf{x}$ es una N_i-secesión débil para toda $i \geq 1$, entonces la siguiente

sucesión

$$\ldots \longrightarrow R/(\mathbf{x}) \otimes N_2 \xrightarrow{1_{R/\mathbf{x}} \otimes \varphi_2} R/(\mathbf{x}) \otimes N_1 \xrightarrow{1_{R/\mathbf{x}} \otimes \varphi_1} R/(\mathbf{x}) \otimes N_0 \longrightarrow 0$$

es exacta.

Demostración:

Por argumentos similares a los de la proposición anterior, es suficiente probarlo para el caso en el que $\mathbf{x} = x$. Además, si x es un elemento N_i-regular, entonces también es un elemento $\mathrm{Im}(\varphi_{i+1})$-regular. Pues si $m \in \mathrm{Im}(\varphi_{i+1})$ es tal que $xm = 0$ como $\mathrm{Im}(\varphi_{i+1}) \subseteq N_i$ entonces $m = 0$. Así, solo basta aplicar la proposición anterior a las sucesiones

$$N_{i+2} \longrightarrow N_{i+1} \longrightarrow \mathrm{Im}(\varphi_{i+1}) \longrightarrow 0\ .$$

■

Definición 3.9. *Sean R un anillo Noetheriano (I un ideal) y M un R-módulo. Si $\mathbf{x} = x_1, \ldots, x_n$ es M-regular contenida en R (contenida en I). Diremos que $\mathbf{x}$ es maximal (en I) si para cualquier elemento $x_{n+1} \in R$ ($x_{n+1} \in I$), la siguiente sucesión $\mathbf{x}' = x_1, \ldots, x_n, x_{n+1}$ no es M-regular.*

Mas adelante probaremos que toda M-sucesión maximal en un ideal I que cumpla que $IM \neq M$ tiene la misma longitud si M es finito. Esto nos permitirá introducir nociones básicas de grado y profundidad.

3.2. Grado, profundidad y dimensión proyectiva

Relacionado con las las sucesiones regulares, los módulos finitos sobre anillos Noetherianos se distinguen por dos razones: primero, cada divisor de cero de M esta contenido en un ideal primo asociado, y, la segunda el número de dichos primos es finito. Dichos hechos implican la siguiente proposición la cual es considerada como una de las más útiles en la teoría de anillos conmutativos.

Proposición 3.10. *Sean R un anillo Noetheriano y M un R-módulo finito. Si un ideal $I \subseteq R$ consiste de los divisores de cero de M, entonces $I \subseteq P$ para algún $P \in \mathrm{Ass}(M)$.*

Demostración:
Si I consiste de divisores de cero, entonces $I \subseteq \bigcup_{P_i \in \mathrm{Ass}_R(M)} P_i$ y $\mathrm{Ass}_R(M)$ es finito. Así, por la Proposición 1.6 tenemos que existe P_i tal que $I \subseteq P_i$. ■

Proposición 3.11. *Sean M y N R-módulos. Consideremos $I = \mathrm{Ann}(N)$, entonces:*

(a) Si I contiene un elemento M-regular, entonces $\mathrm{Hom}_R(N, M) = 0$.

(b) Si R es Noetheriano, M, N finitamente generados y $\mathrm{Hom}_R(N, M) = 0$, entonces I contiene un elemento M-regular.

Demostración:

(a) Supongamos que $a \in I$ es un elemento M-regular. Dado $\varphi \in \mathrm{Hom}_R(N, M)$ y $n \in N$. Entonces tenemos que $an = 0$ pues $I = \mathrm{Ann}(N)$, luego $\varphi(an) = 0$, como φ es morfismo y a es M-regular tenemos que $\varphi(n) = 0$. Así $\varphi = 0$ (i.e. $\mathrm{Hom}_R(N, M) = 0$).

(b) Ver [BH98, p. 9].

■

Lema 3.12. *Sean M y N R-módulos y $\mathbf{x} = x_1, \ldots, x_n$ una M-sucesión débil en $\mathrm{Ann}(N)$. Entonces:*

$$\mathrm{Hom}_R(N, M/\mathbf{x}M) \cong \mathrm{Ext}^n_R(N, M).$$

Demostración:
Procedamos por inducción sobre n. El paso inductivo, cuando $n = 0$ es inmediato de la Proposición 2.31. Supongamos que para toda $\mathbf{x}' = x_1, \ldots, x_{n-1}$ una sucesión M-regular contenida en $\mathrm{Ann}_R(N)$ y todo x_n un elemento $M/\mathbf{x}'M$-regular contenida en $\mathrm{Ann}_R(N)$ se tiene que $\mathrm{Hom}_R(N, M/\mathbf{x}'M) \cong \mathrm{Ext}^{n-1}_R(N, M)$. Ahora, consideremos la siguiente sucesión exacta

$$0 \longrightarrow M \xrightarrow{x_1\text{-}} M \longrightarrow M/x_1M \longrightarrow 0\,.$$

Por la Proposición 2.32, tenemos la siguiente sucesión exacta:

$$\mathrm{Ext}^{n-1}_R(N, M) \longrightarrow \mathrm{Ext}^{n-1}_R(N, M/x_1M) \xrightarrow{\psi} \mathrm{Ext}^n_R(N, M) \xrightarrow{\overline{x_1\text{-}}} \mathrm{Ext}^n_R(N, M)\,.$$

Por otro lado, como x_n es $M/\mathbf{x}'M$-regular, entonces $\mathrm{Hom}_R(N, M/\mathbf{x}'M) = 0$, pues $x_n \in \mathrm{Ann}_R(N)$ y por hipótesis de inducción tenemos que $\mathrm{Ext}_R^{n-1}(N, M) = 0$. Ahora, el morfismo $\overline{x_1\text{-}} : \mathrm{Ext}_R^n(N, M) \to \mathrm{Ext}_R^n(N, M)$ es el morfismo multiplicar por x_1 y como este es un anulador de N, tenemos que $\overline{x_1\text{-}} : \mathrm{Ext}_R^n(N, M) \to 0$ es epimorfismo. Con esto, obtenemos la siguiente sucesión:

$$0 \longrightarrow \mathrm{Ext}_R^{n-1}(N, M/x_1M) \xrightarrow{\psi} \mathrm{Ext}_R^n(N, M) \xrightarrow{\overline{x_1\text{-}}} 0 \, .$$

Es decir que $\mathrm{Ext}_R^{n-1}(N, M/x_1M) \cong \mathrm{Ext}_R^n(N, M)$.

Ahora, tenemos que $x_2, \ldots, x_n$ es una M/x_1M-sucesión débil contenida en $\mathrm{Ann}(N)$ de longitud $n-1$, entonces por hipótesis de inducción, tenemos que

$$\mathrm{Hom}_R(N, (M/x_1M)/(x_2, \ldots, x_n)(M/x_1M)) \cong \mathrm{Ext}_R^{n-1}(N, M/x_1M)$$

Afirmamos que $(M/x_1M)/(x_2, \ldots, x_n)(M/x_1M) \cong M/(x_1, \ldots, x_n)M$. Para probar esta afirmación, consideremos los epimorfismos canónicos

$$\pi_1 : M \to M/x_1M \qquad \pi_2 : M/x_1M \to (M/x_1M)/(x_2, \ldots, x_n)(M/x_1M).$$

Entonces $\pi_2\pi_1 : M \to (M/x_1M)/(x_2, \ldots, x_n)(M/x_1M)$ también es epimorfismo, luego

$$M/\operatorname{Ker}(\pi_2\pi_1) \cong (M/x_1M)/(x_2, \ldots, x_n)(M/x_1M).$$

Ahora, probaremos que $\mathrm{Ker}(\pi_2\pi_1) = (x_1, \ldots, x_n)M$. Tenemos que $x \in \mathrm{Ker}(\pi_2\pi_1)$ ocurre unicamente cuando

$$\pi_2(\pi_1(x)) = \pi_2(x + M/x_1M) = (x + M/x_1M) + (M/x_1M)/(x_2, \ldots, x_n)(M/x_1M) = 0.$$

Lo anterior pasa unicamente si $x + M/x_1M \in (x_2, \ldots, x_n)(M/x_1M)$ esto pasa si y solo

si

$$\begin{aligned} x + M/x_1M &= \sum a_i(m_i + x_1M), \quad a_i \in (x_2, \ldots, x_n),\ m_i \in M \\ &= \sum \left(\sum_{i=2}^{n} r_i x_i \right) (m_i + x_1M) \\ &= \sum \left(\left(\sum_{i=2}^{n} r_i x_i \right) m_i + x_1M \right) \\ &= \sum \left(\left(\sum_{i=2}^{n} r_i x_i \right) m_i \right) + x_1M \end{aligned}$$

si y solo si $x - \sum \left(\left(\sum_{i=2}^{n} r_i x_i \right) m_i \right) = \sum (r_1 x_1) m_i$ si y solo si $x = \sum \left(\left(\sum_{i=1}^{n} r_i x_i \right) m_i \right)$. Así, $\mathrm{Ker}(\pi_2 \pi_1) = (x_1, \ldots, x_n)M$. Es decir que

$$M/(x_1, \ldots, x_n)M \cong (M/x_1M)/(x_2, \ldots, x_n)(M/x_1M).$$

Finalmente, tenemos que

$$\begin{aligned} \mathrm{Hom}_R(N, M/(x_1, \ldots, x_n)M) \cong \mathrm{Hom}_R(N, (M/x_1M)/(x_2, \ldots, x_n)(M/x_1M)) \cong \\ \mathrm{Ext}_R^{n-1}(N, M/x_1M) \cong \mathrm{Ext}_R^n(N, M). \end{aligned}$$

■

Teorema 3.13 (Rees). *Sea R un anillo Noetheriano, M un R-módulo finito e I un ideal tal que $IM \neq M$. Entonces todas las M-sucesiones regulares maximales tienen la misma longitud n dada por*

$$n = \mín\{i : \mathrm{Ext}_R^i(R/I, M) \neq 0\}.$$

Demostración:

Consideremos $\mathbf{x} = x_1, \ldots, x_n$ una M-sucesión en I. Ahora, para $i = 1, 2, \ldots, n$ definamos $I_i = (x_1, \ldots, x_{i-1})$. Así, como $\mathbf{x}$ es una M-sucesión tenemos que x_i es un elemento M/I_iM-regular, y por el lema anterior y la Proposición 3.11(a) tenemos que

$$\mathrm{Ext}_R^{i-1}(R/I, M) \cong \mathrm{Hom}_R(R/I, M/I_iM) = 0.$$

Por otro lado, como $\mathbf{x}$ es una M-sucesión maximal contenida en I, tenemos que $M/\mathbf{x}M$ no contiene elementos regulares, entonces por la Proposición 3.11(b) tenemos que $\mathrm{Hom}_R(R/I, M/IM) \neq 0$, es decir que $\mathrm{Ext}^n_R(R/I, M) \neq 0$. ■

Definición 3.14. *Sean R un anillo Noetheriano, M un R-módulo finito e I un ideal tal que $IM \neq M$. Entonces, a la longitud común de las M-sucesiones maximales en I la llamaremos grado de I en M y lo denotaremos por* $\mathrm{grade}(I, M)$.

Cuando R sea un anillo local Noetheriano con ideal máximo $\mathfrak{m}$ y entonces al grado de $\mathfrak{m}$ en M lo llamaremos profundidad de M y lo denotaremos por $\mathrm{depth}(M)$.

Una convención que debemos tomar en cuenta es que en el caso en el que $IM = M$, diremos que $\mathrm{grade}(I, M) = \infty$. Además, es inmediato del Teorema 3.13 que podemos calcular la profundidad de M como sigue:

Teorema 3.15. *Si R es un anillo local Noetheriano con ideal máximo $\mathfrak{m}$ y M es un R-módulo finito no cero. Entonces,* $\mathrm{depth}(M) = \mín\{i : \mathrm{Ext}^i_R(R/\mathfrak{m}, M) \neq 0\}$.

Proposición 3.16. *Sean R un anillo Noetheriano (I un ideal) y M un R-módulo. Entonces, toda M-sucesión $\mathbf{x}$ puede ser extendida a una sucesión maximal contenida en R (contenida I).*

Demostración:
Supongamos que todas la M-sucesiones maximales contenidas en R tienen longitud n. Sea $x_1, \ldots, x_p$ una M sucesión tal que $p < n$, como no es maximal existe y_1 tal que $x_1, \ldots, x_p, y_1$ es una M-sucesión. Continuando de esta manera, obtenemos la una sucesión $x_1, \ldots, x_p, y_1, \ldots, y_{n-p}$ de longitud n y que por consecuente es maximal. ■

Proposición 3.17. *Sea R un anillo Noetheriano, I un ideal de R y*

$$0 \longrightarrow U \longrightarrow M \longrightarrow N \longrightarrow 0$$

una sucesión exacta de R-módulos finitos. Entonces tenemos lo siguiente:

(a) $\mathrm{grade}(I, M) \geq \mín\{\mathrm{grade}(I, U), \mathrm{grade}(I, N)\}$.

(b) $\mathrm{grade}(I, U) \geq \mín\{\mathrm{grade}(I, M), \mathrm{grade}(I, N) + 1\}$.

(c) $\mathrm{grade}(I, N) \geq \mín\{\mathrm{grade}(I, U) - 1, \mathrm{grade}(I, M)\}$.

Demostración:

Primero, supongamos que $\operatorname{grade}(I,M) = m$, $\operatorname{grade}(I,U) = u$ y $\operatorname{grade}(I,N) = n$, donde I, U y N son R-módulos no cero. Por definición tenemos que:

$$\begin{aligned} \operatorname{Ext}^i_R(R/I,M) &= 0, \qquad \forall i < \operatorname{grade}(I,M) = m \\ \operatorname{Ext}^i_R(R/I,U) &= 0, \qquad \forall i < \operatorname{grade}(I,U) = u \\ \operatorname{Ext}^i_R(R/I,N) &= 0, \qquad \forall i < \operatorname{grade}(I,N) = n. \end{aligned}$$

Finalmente, como la sucesión dada es exacta, la siguiente también lo es

$$0 \to \ldots \to \operatorname{Ext}^i_R(R/I,U) \to \operatorname{Ext}^i_R(R/I,M) \to \operatorname{Ext}^i_R(R/I,N) \to \operatorname{Ext}^{i+1}_R(R/I,U) \to \ldots$$

(a) Supongamos que $\operatorname{grade}(I,M) < \text{mín}\{\operatorname{grade}(I,U), \operatorname{grade}(I,N)\}$.
Ahora, si $\operatorname{grade}(I,U) \leq \operatorname{grade}(I,N)$, entonces $m < u \leq n$ tenemos lo siguiente

$$\ldots \to \operatorname{Ext}^m_R(R/I,U) \to \operatorname{Ext}^m_R(R/I,M) \to \operatorname{Ext}^m_R(R/I,N) \to \ldots$$

pero lo anterior se reduce a lo siguiente

$$\ldots \to 0 \to \operatorname{Ext}^m_R(R/I,M) \to 0 \to \ldots$$

lo cual implica que $\operatorname{Ext}^m_R(R/I,M) = 0$, lo cual es absurdo, pues $m = \operatorname{grade}(I,M)$.

Para el caso en el que $\operatorname{grade}(I,N) < \operatorname{grade}(I,U)$, análogamente, se obtiene que $\operatorname{Ext}^m_R(R/I,M) = 0$.

Por lo tanto, se debe dar que $\operatorname{grade}(I,M) \geq \text{mín}\{\operatorname{grade}(I,U), \operatorname{grade}(I,N)\}$.

(b) Supongamos que $\operatorname{grade}(I,U) < \text{mín}\{\operatorname{grade}(I,M), \operatorname{grade}(I,N)+1\}$.
Si $\operatorname{grade}(I,M) \leq \operatorname{grade}(I,N)+1$, entonces $u < m \leq n+1$ (en particular $u-1 < n$).
Así, tenemos que

$$\ldots \to \operatorname{Ext}^{u-1}_R(R/I,N) \to \operatorname{Ext}^u_R(R/I,U) \to \operatorname{Ext}^u_R(R/I,M) \to \ldots$$

por argumentos similares a los anteriores se tiene que $\mathrm{Ext}^u_R(R/I, U) = 0$, lo que es absurdo.

Para el caso en el que $\mathrm{grade}(I, N)+1 < \mathrm{grade}(I, M)$ se prueba, de manera similar que $\mathrm{Ext}^u_R(R/I, U) = 0$.

Por lo tanto, $\mathrm{grade}(I, U) \geq \mathrm{mín}\{\mathrm{grade}(I, M), \mathrm{grade}(I, N) + 1\}$.

(c) Supongamos que $\mathrm{grade}(I, N) < \mathrm{mín}\{\mathrm{grade}(I, U) - 1, \mathrm{grade}(I, M)\}$.
Si $\mathrm{grade}(I, U) - 1 \leq \mathrm{grade}(I, M)$ se tiene que $n < u - 1 \leq m$ (en particular $n + 1 < u$). Así, obtenemos

$$\ldots \to \mathrm{Ext}^n_R(R/I, M) \to \mathrm{Ext}^n_R(R/I, N) \to \mathrm{Ext}^{n+1}_R(R/I, U) \to \ldots$$

nuevamente obtenemos que $\mathrm{Ext}^n_R(R/I, N) = 0$, lo que es absurdo.

Como antes, el caso $\mathrm{grade}(I, M) < \mathrm{grade}(I, U) - 1$ es análogo.

Así, se debe cumplir $\mathrm{grade}(I, N) \geq \mathrm{mín}\{\mathrm{grade}(I, U) - 1, \mathrm{grade}(I, M)\}$.

Para el caso en el que alguno sea cero la proposición es inmediata pues $IM = M$ (respectivamente, $IU = U$ y $IN = N$) y por tanto $\mathrm{grade}(I, M) = \infty$ (respectivamente, $\mathrm{grade}(I, U) = \infty$ y $\mathrm{grade}(I, N) = \infty$). ■

Proposición 3.18. *Sea R un anillo local Noetheriano y M un R-módulo finitamente generado. Entonces,* $\mathrm{depth}(M) = 0$ *si y solo si* $\mathfrak{m} \in \mathrm{Ass}(M)$ *donde* $\mathfrak{m}$ *es el ideal máximo de R.*

Demostración:

Supongamos que $\mathrm{depth}(M) = 0$. Entonces $\mathfrak{m}$ consiste de los divisores de cero de M, luego $\mathfrak{m} \subseteq P$ para algún $P \in \mathrm{Ass}_R(M)$. Dado que $\mathfrak{m}$ es maximal, tenemos que $\mathfrak{m} = P$. Por lo tanto, $\mathfrak{m} \in \mathrm{Ass}_R(M)$. El recíproco es inmediato. ■

El siguiente resultado enuncia una serie de fórmulas que serán de utilidad a la hora de calcular grados. Sin embargo simplemente lo enunciaremos, para ver la demostración se puede consultar [BH98, p. 11].

Proposición 3.19. *Sean R un anillo Noetheriano, I, J ideales de R y M un R-módulo finito. Entonces:*

(a) $\operatorname{grade}(I, M) = \operatorname{ínf}\{\operatorname{depth}(M_P) : P \in V(I)\}$ *donde* $V(I)$ *denota el conjunto de ideales primos que contienen a* I.

(b) $\operatorname{grade}(I, M) = \operatorname{grade}(\sqrt{I}, M)$.

(c) $\operatorname{grade}(I \cap J) = \operatorname{mín}\{\operatorname{grade}(I, M), \operatorname{grade}(J, M)\}$.

(d) Si $\mathbf{x} = x_1, \ldots, x_n$ *es una* M*-sucesión contenida en* I*, entonces*

$$\operatorname{grade}(I/(\mathbf{x}), M/\mathbf{x}M) = \operatorname{grade}(I, M/\mathbf{x}M) = \operatorname{grade}(I, M) - n.$$

Definición 3.20. *Dado un* R*-módulo* M *y una resolución por proyectivos*

$$P_\bullet : \ \ldots \xrightarrow{\varphi_{n+1}} P_n \xrightarrow{\varphi_n} \ldots \xrightarrow{\varphi_3} P_2 \xrightarrow{\varphi_2} P_1 \xrightarrow{\varphi_1} P_0 \xrightarrow{\alpha} M \longrightarrow 0 \ .$$

Entonces, para $i = 1, 2, \ldots$ *definimos* i*-ésima sizigia de* M *como* $M_i = \operatorname{Ker}(\varphi_{i-1})$.

Otro concepto crucial para poder cumplir el objetivo de este capítulo es el siguiente:

Definición 3.21. *Dado un* R*-módulo* M*. Diremos que* M *tiene dimensión proyectiva igual a infinito si no existe una* n*-sizigia proyectiva. En caso contrario, definimos la dimensión proyectiva de* M *como:*

$$\operatorname{proj\,dim}(M) = \operatorname{mín}\{n : n\text{-ésima sizigia es proyectiva}\}.$$

Si la dimensión proyectiva de M *es* n*, entonces diremos que la siguiente sucesión es una resolución libre de longitud* n *de* M*:*

$$0 \longrightarrow M_n = \operatorname{Ker}(\varphi_{n-1}) \xrightarrow{\varphi_n} \ldots \xrightarrow{\varphi_3} P_2 \xrightarrow{\varphi_2} P_1 \xrightarrow{\varphi_1} P_0 \xrightarrow{\alpha} M \longrightarrow 0 \ ,$$

es decir, remplazamos el n*-ésimo módulo proyectivo de la resolución por proyectivos por la* n*-ésima sizigia.*

Definición 3.22. *Dados* R *un anillo local Noetheriano con ideal máximo* $\mathfrak{m}$*,* M R*-módulo y una resolución por libres de* M

$$F_\bullet : \ \ldots \xrightarrow{\varphi_{n+1}} F_n \xrightarrow{\varphi_n} \ldots \xrightarrow{\varphi_3} F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\alpha} M \longrightarrow 0 \ .$$

Diremos que $F_\bullet$ *es minimal si* $\varphi_i(F_i) \subseteq \mathfrak{m}F_{i-1}$ *para toda* $i \geq 1$.

Proposición 3.23. *Sea R un anillo local Noetheriano con ideal máximo $\mathfrak{m}$ y M un R-módulo finitamente generado. Entonces, existe una resolución libre minimal de M.*

Demostración:

Sea $\beta_0 = \mu(M)$, elijamos un sistema minimal de generadores de M, digamos $x_1, \ldots, x_{n_0}$. Consideremos el R-módulo libre $F_0 = \bigoplus_{i=1}^{\beta_0} R$, definamos

$$\begin{array}{cccc} \varphi_0 & F_0 & \longrightarrow & M \\ & e_i & \longmapsto & x_i \end{array}$$

Donde $e_1, \ldots, e_{n_0}$ es la base canónica de F_0. Es inmediato que el morfismo anterior es suprayectivo.

Ahora, sea $\beta_1 = \mu(\mathrm{Ker}(\varphi_0))$, tomando $F_1 = \bigoplus_{i=1}^{\beta_1} R$ definimos $\varphi_1 : F_0 \to \mathrm{Ker}(\varphi_0)$ definido de manera similar a la anterior. Continuando de esta manera obtenemos el siguiente diagrama:

$$\begin{array}{ccccccccccc} \ldots & \xrightarrow{i\varphi_3} & F_2 & \xrightarrow{i\varphi_2} & F_1 & \xrightarrow{i\varphi_1} & F_0 & \xrightarrow{\varphi_0} & M & \longrightarrow & 0\,. \\ & \searrow^{\varphi_3} & \uparrow & \searrow^{\varphi_2} & \uparrow & \searrow^{\varphi_1} & \uparrow & & & & \\ & & \mathrm{Ker}(\varphi_2) & & \mathrm{Ker}(\varphi_1) & & \mathrm{Ker}(\varphi_0) & & & & \end{array}$$

Donde la fila es exacta por construcción y además, afirmamos que es minimal. En efecto, consideremos la siguiente sucesión exacta.

$$\varphi(F_i) \longrightarrow F_{i-1} \longrightarrow \mathrm{Ker}(\varphi_{i-2}) \longrightarrow 0$$

Entonces, usando la Proposición 1.71 y la Proposición 1.74 tenemos que la siguiente sucesión es exacta:

$$\varphi_i(F_i)/\mathfrak{m}\varphi_i(F_i) \longrightarrow F_{i-1}/\mathfrak{m}F_{i-1} \xrightarrow{\alpha} \mathrm{Ker}(\varphi_{i-2})/\mathfrak{m}\,\mathrm{Ker}(\varphi_{i-2}) \longrightarrow 0\,.$$

Como α es un epimorfismo entre dos $R/\mathfrak{m}$-espacios vectoriales de la misma dimensión (así los tomamos por construcción), tenemos que α es un isomorfismo. Por lo tanto, $\varphi_i(F_i) \subseteq \mathfrak{m}(F_{i-1})$. ■

Definición 3.24. *Dado un anillo local Noetheriano R, M un R-módulo finitamente*

generado y

$$F_\bullet : \ \ldots \longrightarrow F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \longrightarrow 0$$

una resolución libre minimal de M. Al rango de F_i denotado por β_i lo llamaremos i-ésimo número de Betti.

Lema 3.25. *Sea R un anillo Noetheriano local con ideal máximo $\mathfrak{m}$, M un R-módulo finitamente generado y*

$$F_\bullet : \ \ldots \longrightarrow F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \longrightarrow 0$$

es una resolución libre. Entonces $F_\bullet$ es minimal si y solo si $1_{R/\mathfrak{m}} \otimes \varphi_i = 0$ para toda $i \geq 1$.

Demostración:

Supongamos que $F_\bullet$ es minimal. Tenemos lo siguiente

$$F_i/\mathfrak{m}F_i \cong F_i \otimes R/\mathfrak{m} \xrightarrow{\varphi_i \otimes 1_{R/\mathfrak{m}}} F_{i-1} \otimes R/\mathfrak{m} \cong F_{i-1}/\mathfrak{m}F_{i-1}$$

Abusando de la notación, tenemos que $(\varphi_i \otimes 1_{R/\mathfrak{m}})(x + \mathfrak{m}F_i) = \varphi_i(x) + \mathfrak{m}F_{i-1} = 0$, pues la resolución es minimal.

El recíproco es inmediato. ■

Lema 3.26. *Sea R un anillo local Noetheriano con ideal máximo $\mathfrak{m}$ y M un R-módulo finitamente generado. Entonces, $M \otimes R/\mathfrak{m} = 0$ si y solo si $M = 0$.*

Demostración:

Recordemos que $M \otimes R/\mathfrak{m} \cong M/\mathfrak{m}M$ por Proposición 1.74. Es decir que $M/\mathfrak{m}M = 0$, es decir que $M = \mathfrak{m}M$ y como $\mathfrak{m}$ está contenido en el radical de Jacobson, por la Proposición 1.47 tenemos $M = 0$. El recíproco es inmediato. ■

Teorema 3.27. *Sea R un anillo Noetheriano local con ideal máximo $\mathfrak{m}$ y M un R-módulo finitamente generado. Entonces*

$$\operatorname{proj\,dim}(M) = \sup\{i : \operatorname{Tor}_i^R(M, R/\mathfrak{m}) \neq 0\},$$

Demostración:

Supongamos que $\operatorname{proj\,dim}(M) = n$, es decir que existe una resolución por libres de

longitud n, digamos

$$0 \longrightarrow F_n \xrightarrow{\varphi_n} F_{n-1} \xrightarrow{\varphi_{n-1}} \ldots \longrightarrow F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} M \longrightarrow 0\ ,$$

la cual podemos asumir minimal. Luego por Corolario 1.73 tenemos

$$0 \longrightarrow \frac{R}{\mathfrak{m}} \otimes F_n \xrightarrow{1_{R/\mathfrak{m}}\otimes\varphi_n} \frac{R}{\mathfrak{m}} \otimes F_{n-1} \xrightarrow{1_{R/\mathfrak{m}}\otimes\varphi_{n-1}} \ldots \longrightarrow \frac{R}{\mathfrak{m}} \otimes F_2 \xrightarrow{1_{R/\mathfrak{m}}\otimes\varphi_2} \frac{R}{\mathfrak{m}} \otimes F_1 \xrightarrow{1_{R/\mathfrak{m}}\otimes\varphi_1} \frac{R}{\mathfrak{m}} \otimes M \longrightarrow 0\ ,$$

es un complejo, además $\operatorname{Tor}_i^R(M, R/\mathfrak{m}) = 0$ para todo $i > n$. Por tanto,

$$\sup\{i : \operatorname{Tor}_i^R(M, R/\mathfrak{m}) \neq 0\} \leq n.$$

Por otro lado, tenemos que $\operatorname{Tor}_n^R(M, R/\mathfrak{m}) \neq 0$, pues del Lema 3.25 obtenemos que $1_{R/\mathfrak{m}} \otimes \varphi_n = 0$. Entonces, $\operatorname{Ker}(1_{R/\mathfrak{m}} \otimes \varphi_n) = R/\mathfrak{m} \otimes F_i$ y $\operatorname{Im}(1_{R/\mathfrak{m}} \otimes \varphi_{n+1}) = 0$. Así,

$$\operatorname{Tor}_n^R(M, R/\mathfrak{m}) = \frac{\operatorname{Ker}(1_{R/\mathfrak{m}} \otimes \varphi_n)}{\operatorname{Im}(1_{R\mathfrak{m}} \otimes \varphi_{n+1})} = F_n \otimes R/\mathfrak{m} \neq 0,$$

del Lema 3.26. Por lo tanto, $\operatorname{proj\,dim}(M) = \sup\{i : \operatorname{Tor}_i^R(M, R/\mathfrak{m}) \neq 0\}$. ■

Proposición 3.28. *Sea R un anillo local Noetheriano con ideal máximo $\mathfrak{m}$ y M un R-módulo finitamente generado. Si $x \in \mathfrak{m}$ es un elemento M-regular y R-regular (M-R-regular), entonces*

$$\operatorname{proj\,dim}_R(M) = \operatorname{proj\,dim}_{R/(x)}(M/xM).$$

Demostración:

Sea

$$F_\bullet : \ \ldots \longrightarrow F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} M \longrightarrow 0\ ,$$

una resolución por libres minimal de M. Como x es un elemento M-R-regular entonces por el Corolario 3.8 tenemos el complejo

$$F'_\bullet : \ \ldots \longrightarrow R/(x) \otimes F_2 \xrightarrow{1_{R/(x)}\otimes\varphi_2} R/(x) \otimes F_1 \xrightarrow{1_{R/(x)}\otimes\varphi_1} M/xM \longrightarrow 0\ .$$

Luego, se tiene que $F'_\bullet$ es una resolución minimal de M/xM sobre $R/(x)$. Entonces,

con lo anterior y usando el Lema 1.75 tenemos que:

$$\begin{aligned}\operatorname{proj\,dim}_{R/(x)}(M/xM) &= \sup\{i : \operatorname{Tor}_i^{R/(x)}(M/xM, R/\mathfrak{m}) \neq 0\} \\ &= \sup\{i : \operatorname{Tor}_i^{R}(M, R/\mathfrak{m}) \neq 0\} \\ &= \operatorname{proj\,dim}_R(M, R/(x)).\end{aligned}$$

■

Proposición 3.29. *Sea R un anillo Noetheriano, I un ideal de R, M un R-módulo finitamente generado y $\mathbf{x} = x_1, \ldots, x_n$ un M-sucesión contenida en I. Entonces, son equivalentes:*

(a) $IM = M$.

(b) $I(M/\mathbf{x}M) = M/\mathbf{x}M$.

(c) $(I/\mathbf{x})/(M/\mathbf{x}M) = M/\mathbf{x}M$.

Demostración:

Primero, denotaremos por $\overline{R} = R/\mathbf{x}$, $\overline{I} = I/\mathbf{x}$ y $\overline{M} = M/\mathbf{x}M$.

Demostraremos (a) implica (b): tenemos que $I\overline{M} \subseteq \overline{M}$, a continuación demostraremos que $\overline{M} \subseteq I\overline{M}$. Sea $m + \mathbf{x}M \in \overline{M}$, como $m \in M = IM$, $m = \sum_{i=1}^n (r_i m_i)$ donde $r_i \in I$ y $m_i \in M$. Luego, $m + \mathbf{x}M = (\sum_{i=1}^n (r_i m_i)) + \mathbf{x}M = \sum_{i=1}^n r_i(m_i + \mathbf{x}M) \in I\overline{M}$.

Ahora, probemos (b) implica (c) no sin antes recalcar que indirectamente en (c) nos dice que $\overline{M}$ tiene estructura de $\overline{R}$-módulo, con la ley de composición externa $(r + \mathbf{x})(m + \mathbf{x}M) = r(m + \mathbf{x})$. Nuevamente, tenemos la contención $\overline{IM} \subseteq \overline{M}$, falta probar que $\overline{M} \subseteq \overline{IM}$. Sea $m + \mathbf{x}M \in \overline{M}$, como $\overline{M} = I\overline{M}$ tenemos que $m + \mathbf{x}M = \sum_{i=1}^n (r_i(m_i + \mathbf{x}M)) = \sum_{i=1}^n ((r_i + \mathbf{x})(m_i + \mathbf{x}M)) \in \overline{IM}$.

Por último, probaremos que (c) implica (a):similarmente a las implicaciones anteriores solo resta probar que $M \subseteq IM$. Sea $m \in M$, entonces $m + \mathbf{x}M \in \overline{M} = \overline{IM}$, así $m + \mathbf{x}M = \sum_{i=1}^n ((r_i + \mathbf{x})(m_i + \mathbf{x}M)) = (\sum_{i=1}^n r_i m_i) + \mathbf{x}M$. Luego, $m - \sum_{i=1}^n r_i m_i \in \mathbf{x}M$, es decir que $m - \sum_{i=1}^n r_i m_i = \sum_{k=1}^s (\sum_{i=1}^n s_i x_i)\, m_k$ con tenemos que $m \in IM$. ■

Proposición 3.30. *Sea M un R-módulo finitamente generado sobre un anillo local Noetheriano con ideal máximo $\mathfrak{m}$ y $\mathbf{x} = x_1, \ldots, x_n$ una M-sucesión contenida en $\mathfrak{m}$.*

Con la notación de la proposición anterior tenemos que:

$$\operatorname{depth}^{\overline{R}}(\overline{M}) = \operatorname{depth}^{R}(\overline{M}) = \operatorname{depth}^{R}(M) - n.$$

Demostración:
Sea $\mathbf{x}' = x'_1, \ldots, x'_m$ una $\overline{M}$-sucesión maximal contenida en $\mathfrak{m}$. Tenemos que cada x'_i es un elemento $\overline{M}/(x'_1, \ldots, x'_{i-1})\overline{M}$-regular y por cálculos similares a los de la proposición anterior tenemos que x'_i es $\overline{M}/(x'_1 + \mathbf{x}, \ldots, x'_{i-1} + \mathbf{x})\overline{M}$-regular.

Por otro lado, dado que $\mathbf{x}'$ es una $\overline{M}$-sucesión contenida en $\mathfrak{m}$, entonces $\mathbf{x}'M \neq M$, y por la proposición anterior tenemos que $(x'_1 + \mathbf{x}, \ldots, x'_m + \mathbf{x})\overline{M} \neq \overline{M}$. Por lo tanto $x'_1 + \mathbf{x}, \ldots, x'_m + \mathbf{x}$ es una $\overline{M}$-sucesión contenida en $\overline{\mathfrak{m}}$. Es claro que $x'_1 + \mathbf{x}, \ldots, x'_m + \mathbf{x}$ es una $\overline{M}$-sucesión maximal contenida en $\overline{\mathfrak{m}}$, ya que de lo contrario, existe $x' + \mathbf{x} \in \overline{\mathfrak{m}}$ tal que $x'_1 + \mathbf{x}, \ldots, x'_m + \mathbf{x}, x' + \mathbf{x}$ es una $\overline{M}$-sucesión maximal (esto es sin pérdida de generalidad pero podría extenderse a más elementos) contenida en $\overline{\mathfrak{m}}$, nuevamente haciendo cálculos como los de antes tenemos que $x'_1, \ldots, x'_m, x'$ es una $\overline{M}$-sucesión contenida en $\mathfrak{m}$ lo que contradice la maximalidad de $\mathbf{x}'$. Por lo tanto, $x'_1 + \mathbf{x}, \ldots, x'_m + \mathbf{x}$ es una $\overline{M}$-sucesión maximal contenida en $\overline{\mathfrak{m}}$, en consecuencia $\operatorname{depth}^{\overline{R}}(\overline{M}) = \operatorname{depth}^{R}(\overline{M})$.

Por otro lado, dada una M-sucesión contenida en $\mathfrak{m}$, $x_1, \ldots, x_n$ puede ser extendida a una M sucesión maximal en $\mathfrak{m}$, digamos $x_1, \ldots, x_n, \ldots, x_m$. Entonces, tenemos que $x_1, \ldots, x_n$ es un M-sucesión e inmediatamente de la definición que $x_{n+1}, \ldots, x_m$ una $\overline{M}$-sucesión. Afirmamos 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 existe $x \in R$ tal que $x_{n+1}, \ldots, x_m, x$ es una $\overline{M}$ entonces $x_1, \ldots, x_n, \ldots x_m, x$ es una M sucesión, lo que es un absurdo. Por tanto, $\operatorname{depth}^{R}(\overleftarrow{M}) = \operatorname{depth}^{R}(M) - n$. ■

Observación. Dado un anillo local Noetheriano R con ideal máximo $\mathfrak{m}$, entonce para cada R-módulo libre finitamente generado F, tenemos que $\operatorname{depth}(R) = \operatorname{depth}(F)$.

Demostración:
Es una observación importante que utiliza un poco de teoría de categorías, pero en esencia se prueba como sigue: como F es libre y finitamente generado, $F \cong \bigoplus_{i=1}^{n} R$. Luego, tenemos que

$$\operatorname{Ext}^s_R(R/\mathfrak{m}, F) \cong \operatorname{Ext}^s_R(R/\mathfrak{m}, \bigoplus_{s=1}^{n} R) \cong \bigoplus_{i=1}^{n} \operatorname{Ext}^i_R(R/\mathfrak{m}, R) = \prod_{i=1}^{s} \operatorname{Ext}^s_R(R/\mathfrak{m}, R),$$

(es en esta parte donde se usaría la teoría categórica para justificar la segunda congruencia). Entonces, $\operatorname{Ext}^s_R(R/\mathfrak{m}, F) = 0$ si y solo si $\operatorname{Ext}^s_R(R/\mathfrak{m}, R) = 0$. Entonces, $\text{mín}\{\operatorname{Ext}^i_R(R/\mathfrak{m}, F)\} = \text{mín}\{\operatorname{Ext}^i_R(R/\mathfrak{m}, R)\}$ lo cual implica que $\operatorname{depth}(R) = \operatorname{depth}(F)$. ■

Lema 3.31. *Sea R un anillo local con ideal máximo $\mathfrak{m}$, y $\varphi : F \to G$ un morfismo de R-módulos finitos. Supongamos que F es libre y sea M un R-módulo tal que $\mathfrak{m} \in \operatorname{Ass}(M)$. Si $\varphi \otimes M$ es inyectivo, entonces, el morfismo $\varphi \otimes 1_{R/\mathfrak{m}}$ es inyectivo.*

Demostración:
Como $\mathfrak{m} \in \operatorname{Ass}(M)$, entonces, de Proposición 1.42 existe un morfismo $\lambda : R/\mathfrak{m} \to M$ inyectivo. Como F es un R-módulo libre $\lambda \otimes 1_F : F \otimes R/\mathfrak{m} \to F \otimes M$ es inyectiva. Consideremos el siguiente diagrama

$$\begin{array}{ccc} F \otimes R/\mathfrak{m} & \xrightarrow{1_F \otimes \lambda} & F \otimes M \\ \downarrow{\scriptstyle \varphi \otimes 1_{R/\mathfrak{m}}} & & \downarrow{\scriptstyle \varphi \otimes 1_M} \\ G \otimes R/\mathfrak{m} & \xrightarrow[1_G \otimes \lambda]{} & G \otimes M \end{array}$$

Tenemos que $(\varphi \otimes 1_M)(1_F \otimes \lambda) = (1_G \otimes \lambda)(\varphi \otimes 1_{R/\mathfrak{m}})$, pues el diagrama conmuta. Ahora, como $(\varphi \otimes 1_M)(1_F \otimes \lambda)$ es inyectiva, entonces $\varphi \otimes 1_{R/\mathfrak{m}}$ también es inyectiva. ■

Teorema 3.32 (Auslander-Buchsbaum). *Sean R un anillo local Noetheriano con ideal máximo $\mathfrak{m}$, M un R-módulo finitamente generado no cero. Si $\operatorname{proj\,dim}(M) < \infty$, entonces*

$$\operatorname{proj\,dim}(M) + \operatorname{depth}(M) = \operatorname{depth}(R).$$

Demostración:
Procedamos por inducción en $\operatorname{depth}(R)$. Primero, como $\operatorname{proj\,dim}(M)$ es finita, entonces M admite una resolución minimal por libres, digamos

$$F_\bullet : \; 0 \longrightarrow F_n \xrightarrow{\varphi_n} F_{n-1} \longrightarrow \ldots \longrightarrow F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\alpha} M \longrightarrow 0 \,,$$

donde $n = \operatorname{proj\,dim}(M)$. Ahora, si $\operatorname{depth}(R) = 0$, tenemos que $\mathfrak{m} \in \operatorname{Ass}_R(R)$ pues $\mathfrak{m}$ no contiene elementos regulares. Supongamos que $n \geq 1$, entonces por el Lema 3.31 tenemos que $\varphi_n \otimes 1_{R/\mathfrak{m}}$ es inyectivo, es decir que $\operatorname{Ker}(\varphi_n \otimes 1_{R/\mathfrak{m}}) = 0$, por otro lado $\operatorname{Tor}_n^R(M, R/\mathfrak{m}) \neq 0$ pues de lo contrario $F_\bullet$ no sería minimal, pero $\operatorname{Tor}_n^R(M, R/\mathfrak{m}) = \operatorname{Ker}(\varphi_n \otimes 1_{R/\mathfrak{m}})$ lo cual es absurdo. Por lo tanto $n = 0$. Así que M es libre, y de la observación anterior tenemos que $\operatorname{depth} M = \operatorname{depth}(R)$.

Ahora, supongamos que $\operatorname{depth}(R) > 0$. Si $\operatorname{depth}(M) > 0$, entonces por la Proposición 3.18 tenemos que $\mathfrak{m} \notin \operatorname{Ass}(R)$ y $\mathfrak{m} \notin \operatorname{Ass}(M)$. Ahora, afirmamos que existe $x \in \mathfrak{m}$ tal que este es un elemento R-regular y M-regular. De lo contrario, tendríamos que todos los elementos de $\mathfrak{m}$ son divisores de cero de R y M, es decir que $\mathfrak{m} \subseteq \left(\bigcup_{P_i \in \operatorname{Ass}_R(R)} P_i\right) \cup \left(\bigcup_{P_i' \in \operatorname{Ass}_R(M)} P_i'\right)$ y dado que $\operatorname{Ass}(R)$ y $\operatorname{Ass}(M)$ son finitos tenemos que $\mathfrak{m} \in \operatorname{Ass}(R)$ y $\mathfrak{m} \in \operatorname{Ass}(M)$ lo que es absurdo. Ahora, aplicaremos la hipótesis de inducción al anillo local Noetheriano $R/(x)$ y al $R/(x)$-módulo finitamente generado no cero pues $\operatorname{depth}^{R/(x)}(R/(x)) = \operatorname{depth}^R(R) - 1$. Entonces:

$$\operatorname{depth}^{R/(x)}(M/(x)M) = \operatorname{depth}^R(M) - 1 \quad \text{y} \quad \operatorname{proj\,dim}_{R/(x)}(M/(x)M) = \operatorname{proj\,dim}_R(M).$$

Luego,

$$\begin{aligned} \operatorname{proj\,dim}_{R/(x)}(M/(x)M) + \operatorname{depth}^{R/(x)}(M/(x)M) &= \operatorname{depth}^{R/(x)}(R/(x)) \\ \Rightarrow \operatorname{proj\,dim}_R(M) - 1 + \operatorname{depth}^R(M) &= \operatorname{depth}^R(R) - 1 \\ \Rightarrow \operatorname{proj\,dim}_R(M) + \operatorname{depth}^R(M) &= \operatorname{depth}^R(R). \end{aligned}$$

Finalmente, para el caso cuando $\operatorname{depth}(M) = 0$, consideremos la siguiente sucesión exacta

$$0 \longrightarrow \operatorname{Ker}(\alpha) \longrightarrow F_0 \xrightarrow{\alpha} M \longrightarrow 0\,.$$

De la Proposición 3.17, tenemos que

$$0 = \operatorname{depth}(M) \geq \min\{\operatorname{depth}(\operatorname{Ker}(\alpha)) - 1, \operatorname{depth}(F_0)\} = \operatorname{depth}(\operatorname{Ker}(\alpha)) - 1.$$

Por la misma proposición tenemos que

$$\operatorname{depth}(\operatorname{Ker}(\alpha)) \geq \min\{\operatorname{depth}(F_0), \operatorname{depth}(M) + 1\} = 1.$$

Por lo tanto $\operatorname{depth}(\operatorname{Ker}(\alpha)) = 1$. Ahora, observemos el complejo

$$F_\bullet : \ 0 \longrightarrow F_n \xrightarrow{\varphi_n} F_{n-1} \longrightarrow \ldots \longrightarrow F_1 \xrightarrow{i\varphi_1} \operatorname{Ker}(\alpha) \longrightarrow 0 \, ,$$

el cual es una resolución libre de $\operatorname{Ker}(\alpha)$, entonces $\operatorname{proj\,dim}(\operatorname{Ker}(\alpha)) \leq n-1$. Ahora, supongamos que existe una resolución libre de $\operatorname{Ker}(\alpha)$ de longitud j, estrictamente menor a $n-1$, digamos:

$$F'_\bullet : \ 0 \longrightarrow F'_j \xrightarrow{\varphi'_j} F'_{j-1} \longrightarrow \ldots \longrightarrow F'_1 \xrightarrow{\varphi'_1} F'_0 \xrightarrow{\alpha'} \operatorname{Ker}(\alpha) \longrightarrow 0 \, ,$$

entonces, el siguiente complejo es una resolución libre de M:

$$0 \longrightarrow F'_j \xrightarrow{\varphi'_n} F'_{j-1} \longrightarrow \ldots \longrightarrow F'_1 \xrightarrow{\varphi'_1} F'_0 \xrightarrow{i\alpha'} F_0 \xrightarrow{\alpha} M \longrightarrow 0$$

$$\alpha' \searrow \quad \uparrow i$$

$$\operatorname{Ker}(\alpha)$$

La longitud de la resolución anterior es $j+1 < n$, pro $n = \operatorname{proj\,dim}(M)$, lo cual es absurdo. Por lo tanto, $\operatorname{proj\,dim}_R(\operatorname{Ker}(\alpha)) = \operatorname{proj\,dim}_R(M) - 1$. Similarmente, al caso anterior, dado que $\operatorname{depth}(\operatorname{Ker}(\alpha)) > 0$ obtenemos que

$$\begin{aligned} &\operatorname{proj\,dim}_R(\operatorname{Ker}(\alpha)) + \operatorname{depth}^R(\operatorname{Ker}(\alpha)) = \operatorname{depth}^R(R) \\ &\qquad \Rightarrow \operatorname{proj\,dim}_R(M) - 1 + \operatorname{depth}^R(M) + 1 = \operatorname{depth}^R(R) \\ &\qquad\qquad \Rightarrow \operatorname{proj\,dim}_R(M) + \operatorname{depth}^R(M) = \operatorname{depth}^R(R). \end{aligned}$$

■

Corolario 3.33 (Teorema de las sizigias de Hilbert). *Sean $R = \mathbb{F}[x_1, \ldots, x_n]$ el anillo de polinomios con coeficientes en el campo $\mathbb{F}$ y M un R-módulo finitamente generado, entonces* $\operatorname{proj\,dim}_R(M) \leq n$.

Demostración:

Se cumplen inmediatamente las hipótesis del teorema anterior, y del [Eis95, Teorema 2.2.7, p. 66] tenemos que $\operatorname{proj\,dim}_R(M)$ es finita. Entonces, por el teorema anterior tenemos que $\operatorname{depth}(M) + \operatorname{proj\,dim}(M) = \operatorname{depth}(R)$, pero $\operatorname{depth}(R) = n$, entonces $\operatorname{proj\,dim}(M) = n - \operatorname{depth}(M) \leq n$. ■

CAPÍTULO 4

FACTORIZACIÓN POR MATRICES

En este capítulo desarrollaremos la teoría necesaria para entender y demostrar nuestro objetivo del trabajo. En la última sección de este capítulo daremos ejemplos y mostraremos razones por las cuales el concepto de factorización por matrices ha tenido un gran impacto y algunas conjeturas o resultados que giran entorno a dicha proposición.

4.1. Factorización por matrices

En capítulos previos definimos la dimensión de un anillo R (local) Noetheriano y la profundidad de un R-módulo M. La siguiente definición relaciona estos dos conceptos.

Definición 4.1. *Dados R un anillo local Noetheriano y M un R-módulo finitamente generado no cero. Diremos que M es un módulo Cohen-Macaulay Maximal (o simplemente MCM) si* $\operatorname{depth}(M) = \dim(R)$.

Ejemplo 4.2. Dados un anillo R regular local y $f \in R[x_1, \ldots, x_n]$ no cero, entonces todo módulo M sobre el anillo $S = R/(f)$ es Cohen-Macaulay Maximal [BGS87, Sección 2].

Definición 4.3. *Dados un R-módulo y $F_\bullet$ una resolución libre de M. Diremos que $F_\bullet$ es periódica de periodo 2 (o simplemente periódica) si $\varphi_{2n+1} : F_{2n+1} \to F_{2n}$ es igual para toda $n \in \{0, 1, 2, \ldots\}$ y $\varphi_{2n} : F_{2n} \to F_{2n-1}$ es el mismo para toda $n \in \{1, 2, \ldots\}$. Es decir que $F_\bullet$ se ve de la siguiente manera:*

$$F_\bullet : \ \ldots \longrightarrow F_5 \xrightarrow{\lambda} F_4 \xrightarrow{\mu} F_3 \xrightarrow{\lambda} F_2 \xrightarrow{\mu} F_1 \xrightarrow{\lambda} F_0 \xrightarrow{\alpha} M \longrightarrow 0 \ .$$

Ahora, enunciaremos el último concepto y un par de resultados que nos serán de utilidad para demostrar el resultado que nos propusimos como objetivo.

Definición 4.4. *Sea un R un anillo y $x \in R$, definimos la factorización por matrices de x como un par ordenado de funciones entre R-módulos libres*

$$(\varphi : F \to G, \psi : G \to F)$$

tal que $\varphi\psi = x1_G$ y $\psi\varphi = x1_F$ (para simplificar la notación, lo denotaremos simplemente por (φ, ψ)).

Esta definición, es la propuesta en el articulo de Eisenbud [Eis80b], sin embargo más adelante daremos una definición que se ajusta a los fines de nuestro trabajo.

Lema 4.5. *Sea R un anillo regular local Noetheriano de dimensión finita. Entonces todo R-módulo tiene dimensión proyectiva finita.*

Demostración:
La demostración requiere el desarrollo de más teoría es por ello que el lector la puede consultar en [Eis95, Teorema 2.2.7, p. 66]. ■

De igual manera, lo resultados siguientes requieren del desarrollo de la teoría de descomposición y por ello referiremos al autor a la bibliografía adecuada para la consulta de la demostración.

Proposición 4.6. *Sea R un anillo local Noetheriano, $x \in R$ que no es un divisor de cero. Entonces,* $\dim(R/(x)) = \dim(R) - 1$ *[AM16, Corolario 11.18].*

Proposición 4.7. *Si R es un anillo regular local, R es un dominio entero [Kap73, Teorema 164].*

El resultado estelar del trabajo es el siguiente:

Teorema 4.8. *Dados un anillo regular local Noetheriano R de dimensión d, $x \in R$ y el anillo $S = R/(x)$. Si M es un S-módulo MCM, entonces M tiene una resolución libre periódica.*

Demostración:

Primero, por el Lema 4.5 y Teorema 3.32 tenemos que:

$$\operatorname{proj\,dim}(M) + \operatorname{depth}(M) = \operatorname{depth}(R).$$

Luego, de la Proposición 4.7 tenemos que x no es un divisor de cero y como M es un S-módulo MCM tenemos que $\operatorname{depth}(M) = \dim(S)$, por lo tanto:

$$\begin{aligned}\operatorname{proj\,dim}(M) + \operatorname{depth}(M) &= \operatorname{depth}(S)\\ \Rightarrow \operatorname{proj\,dim}(M) &= \operatorname{depth}(R) - \operatorname{depth}(M)\\ &= \dim(R) - \dim(S) = \dim(R) - \dim(R) - 1 = 1.\end{aligned}$$

Es decir que M tiene una resolución libre minimal de longitud 1, digamos:

$$0 \longrightarrow F_1 \xrightarrow{\varphi} F_0 \xrightarrow{\alpha} M \longrightarrow 0\,.$$

Como M es un S-módulo tenemos que $xM = 0$, ya que dado un elemento $m \in M$, entonces $xm = xm + (x) = 0$. Luego, tenemos que $xF_0 \subseteq \operatorname{Ker}(\alpha)$, como la sucesión es exacta tenemos el siguiente diagrama:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & F_1 & \xrightarrow{\varphi} & F_0 & \xrightarrow{\alpha} & M & \longrightarrow & 0\\ & & & & \downarrow{\scriptstyle x\cdot} & & & & \\ & & F_1 & \xrightarrow[\varphi]{} & \operatorname{Im}(\varphi) & \longrightarrow & 0 & & \end{array}$$

Como los módulos F_0 y F_1 son libres, en particular son proyectivos, entonces existe $\psi : F_0 \to F_1$ tal que el siguiente diagrama conmuta:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & F_1 & \xrightarrow{\varphi} & F_0 & \xrightarrow{\alpha} & M & \longrightarrow & 0\\ & & & \swarrow{\scriptstyle \psi} & \downarrow{\scriptstyle x\cdot} & & & & \\ & & F_1 & \xrightarrow[\varphi]{} & \operatorname{Im}(\varphi) & \longrightarrow & 0 & & \end{array}$$

Ahora, como F_0 y F_1 son libres, entonces son isomorfos a una suma directa de R además de ser finita por la minimalidad de la resolución. Así, por resultados previos tenemos que $F_0 \cong F_1 \cong \bigoplus_{i=1}^{n} S$. Entonces $x \cdot (r_1, \ldots, r_n) = (xr_1, \ldots, xr_n) =$

$x\,\mathrm{Id}_{S^n}(r_1,\ldots,r_n)$, es decir que $\varphi\psi = x\,\mathrm{Id}_{S^n}$.

Ahora, tenemos que la siguiente sucesión es exacta:

$$\ldots \longrightarrow F_1 \xrightarrow{\varphi} F_0 \xrightarrow{\psi} F_1 \xrightarrow{\varphi} F_0 \xrightarrow{\psi} F_1 \xrightarrow{\varphi} F_0 \xrightarrow{\alpha} M \longrightarrow 0\,.$$

El resultado anterior, muestra que para cualquier S-módulo MCM existe una factorización por matrices que "genera" una resolución libre periódica de M, pues la composición restante resulta de la exactitud de la última sucesión. Y de la demostración anterior, podemos ver porque se les atribuye el nombre de factorización por matrices. Pues dado que F_0 y F_1 son isomorfos a $\bigoplus_{i=1}^{S} := S^n$, entonces abusando de la notación tomemos $s \in S^n$, dado que $\{e_1,\ldots,e_n\}$ es una base de S^n, es decir que $s = s_1e_1+\ldots+s_ne_n$ y recordando la manera en la que multiplicamos matrices, tenemos lo siguiente:

$$s = \begin{pmatrix} s_1 & \ldots & s_n \end{pmatrix} \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} s_1 & \ldots & s_n \end{pmatrix} \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix}.$$

Entonces, un morfismo $\alpha : S^n \to S^n$ al aplicarlo a un $s \in S^n$ se ve de la siguiente manera:

$$\alpha(s) = \begin{pmatrix} \alpha(s_1) & 0 & \ldots & 0 \\ 0 & \alpha(s_2) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \alpha(s_n) \end{pmatrix} = \begin{pmatrix} \alpha(e_1) & 0 & \ldots & 0 \\ 0 & \alpha(e_2) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \alpha(e_n) \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix}.$$

Aunque los siguientes resultados no serán probados muestran el potencial que el concepto de factorización por matrices puede tener. Este primer resultado se podría considerar como el recíproco del Teorema 4.8:

Teorema 4.9. *Dada un S-módulo M, donde $S = R/(x)$ y R es como en el Teorema 4.8. Si M admite una resolución libre periódica, entonces M es un módulo Cohen-Macaulay Maximal.*

Demostración:

La demostración puede ser consultada en [Eis80a, Corolario 6.3]. ■

Ahora, si denotamos al conjunto de factorización por matrices de $x \in R$ como $\mathbf{MF}_S(x)$, podemos dotar al conjunto con la estructura de categoría aditiva, donde los morfismos están dados como sigue:

Definición 4.10. *Dados $(\varphi_1, \psi_1), (\varphi_2, \psi_2) \in \mathbf{MF}_S(x)$, un morfismo entre estos dos elementos es un par de morfismos (α, β) tales que el siguiente diagrama conmuta:*

$$\begin{array}{ccccc} F_1 & \xrightarrow{\varphi_1} & G_1 & \xrightarrow{\psi_1} & F_1 \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \alpha} \\ F_2 & \xrightarrow{\varphi_2} & G_2 & \xrightarrow{\psi_2} & F_2 \end{array} .$$

Y "sumar" (categóricamente hablando) dos factorizaciones por matrices se define como sigue:

Definición 4.11. *Dados $(\varphi_1, \psi_1), (\varphi_2, \psi_2) \in \mathbf{MF}_S(x)$, definimos la suma como:*

$$(\varphi_1, \psi_1) \oplus (\varphi_2, \psi_2) = \left(\begin{pmatrix} \varphi_1 & 0 \\ 0 & \varphi_2 \end{pmatrix}, \begin{pmatrix} \psi_1 & 0 \\ 0 & \psi_2 \end{pmatrix} \right)$$

En el contexto del lenguaje categórico, gracias a las definiciones anteriores y a los Teoremas 4.8 y 4.9 diríamos que existe una correspondencia uno a uno entre la categoría de S-módulos Cohen-Macaulay Maximales (sin sumandos directos libres) y las factorizaciones por matrices de x. Esta equivalencia categórica es de gran utilidad en distintas ramas de las matemáticas, por ejemplo en geometría algebraica, teoría de singularidades.

4.2. Ejemplos de factorizaciones por matrices

Para concluir con este trabajo, presentaremos algunos ejemplos de factorizaciones por matrices, estos son ejemplos explícitos que podemos encontrar en la literatura que son hasta cierto punto limitados, pues aunque veremos un método para calcularlas, las matrices resultantes son extremadamente grandes. Por ejemplo, Buchweitz, Eisenbud y Herzog [BEH87] probaron que el tamaño mínimo de la factorización por matrices

de $F_n(x_1,\ldots,x_n) = x_1^2 + \ldots + x_n^n$ está acotada inferiormente por $2^{\frac{n-2}{2}}$, para $n \geq 8$. En particular, probaron que la factorización por matrices de F_{16} es de tamaño 128×128.

Como mencionamos anteriormente, la Definición 4.4 está pensada en el contexto general, sin embargo utilizaremos un caso particular de dicha definición. Dado un polinomio f en el anillo $R = \mathbb{C}[x_1,\ldots,x_n]$ (o en general en cualquier campo algebraicamente cerrado) una factorización de matrices de f es un par (ordenado) (φ,ψ) de matrices cuadradas de la misma dimensión con entradas en R tales que $\varphi\psi = f\,\mathrm{Id} = \psi\varphi$, donde Id representa la matriz identidad de la dimensión de φ y ψ. Esta definición fue utilizada por Yoshino en 1998 [Yos98].

Además, contrario a resultados usuales, esta factorización no necesariamente es única, de hecho veremos ejemplos en los que existen infinitas factorizaciones por matrices, también Eisenbud probó que cualquier polinomio acepta una factorización por matrices. Por ejemplo, consideremos el polinomio y^2+x^n con $n \geq 3$ impar, este es irreducible en $\mathbb{C}[x,y]$ (Criterio de Eisenstein), sin embargo considerando

$$\varphi = \psi = \begin{pmatrix} y & x \\ x^{n-1} & -y \end{pmatrix},$$

tenemos que:

$$\varphi\psi = \begin{pmatrix} y & x \\ x^{n-1} & -y \end{pmatrix}^2 = \begin{pmatrix} y^2+x^n & yx-xy \\ x^{n-1}y - yx^{n-1} & x^n+y^2 \end{pmatrix}$$
$$= \begin{pmatrix} y^2+x^n & 0 \\ 0 & y^2+x^n \end{pmatrix} = (y^2+x^n)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Y de hecho, las siguientes matrices también cumplen dicha propiedad

$$\varphi^k = \psi^k = \begin{pmatrix} y & x^k \\ x^{n-k} & -y \end{pmatrix},$$

donde $1 \leq k \leq \dfrac{n-1}{2}$. Con esto, tenemos un ejemplo de que, sin importar la naturalidad del polinomio existe al menos un par de matrices que cumplen con la definición que ajustamos.

Veamos un ejemplos más complejos, para los cuales consideraremos que los polinomios son elementos del anillo $\mathbb{C}[x, y, z]$.

Ejemplo 4.12. El polinomio $x^{l+1} + yz$ admite las siguientes factorizaciones por matrices, una para cada $k \leq l$, las cuales están dadas de la siguiente manera:

$$\varphi_k = \begin{pmatrix} y & x^{l+1-k} \\ x^k & -z \end{pmatrix}, \qquad \psi_k = \begin{pmatrix} z & x^{l+1-k} \\ x^k & -y \end{pmatrix}.$$

Ejemplo 4.13. El polinomio $x^2y+y^{s-1}+z^2$, al igual que en el ejemplo anterior admite las siguientes factorizaciones por matrices, solo que en este tenemos varios casos.

- Cuando $k = 1$ la factorización es la siguiente:

$$\varphi_1 = \psi_1 = \begin{pmatrix} z & x^2 + y^{s-2} \\ y & -z \end{pmatrix}.$$

- Cuando k es par tal que $2 \leq k \leq s-2$ la factorización esta dada por:

$$\varphi_k = \psi_k = \begin{pmatrix} -z & 0 & xy & y^{k/2} \\ 0 & -z & y^{s-1-\frac{k}{2}} & -x \\ x & y^{\frac{k}{2}} & z & 0 \\ y^{s-1-\frac{k}{2}} & -xy & 0 & z \end{pmatrix}$$

- Finalmente, cuando k es impar tal que $3 \leq k \leq s-1$ la factorización es la siguiente:

$$\varphi_k = \psi_k = \begin{pmatrix} -z & y^{\frac{k-1}{2}} & xy & 0 \\ y^{s-\frac{k+1}{2}} & z & & -x \\ x & 0 & z & y^{\frac{k-3}{2}} \\ 0 & -xy & y^{s-\frac{k-1}{2}} & z \end{pmatrix}$$

Sin embargo, no necesariamente depende de la elección de algún k. También tenemos los siguientes casos que únicamente depende el valor de s.

- Cuando s es par, tenemos dos posibles factorizaciones:

$$\varphi_{s-1} = \psi_{s-1} = \begin{pmatrix} z & y\left(x + iy^{\frac{s-2}{2}}\right) \\ x - iy^{\frac{s-2}{2}} & -z \end{pmatrix},$$

$$\varphi_s = \psi_s = \begin{pmatrix} z & y\left(x - iy^{\frac{s-2}{2}}\right) \\ x + iy^{\frac{s-2}{2}} & -z \end{pmatrix}.$$

- Cuando s es impar, también tenemos dos posibles factorizaciones:

$$\varphi_{s-1} = \begin{pmatrix} z + iy^{\frac{s-1}{2}} & xy \\ x & -\left(z - iy^{\frac{s-1}{2}}\right) \end{pmatrix},$$

$$\psi_{s-1} = \begin{pmatrix} z - iy^{\frac{s-1}{2}} & xy \\ x & -\left(z + iy^{\frac{s-1}{2}}\right) \end{pmatrix}.$$

$$\varphi_s = \begin{pmatrix} z - iy^{\frac{s-1}{2}} & xy \\ x & -\left(z + iy^{\frac{s-1}{2}}\right) \end{pmatrix},$$

$$\psi_s = \begin{pmatrix} z + iy^{\frac{s-1}{2}} & xy \\ x & -\left(z - iy^{\frac{s-1}{2}}\right) \end{pmatrix}.$$

Ejemplo 4.14. Para el polinomio $x^3 + y^4 + z^2$ se conocen las siguientes factorizaciones por matrices:

- $$\varphi_1 = \psi_1 \begin{pmatrix} -z & 0 & x^2 & y^2 \\ 0 & -z & y & -x \\ x & y^3 & z & 0 \\ y & -x^2 & 0 & z \end{pmatrix}.$$

- $$\varphi_2 = \begin{pmatrix} -iz & -y^2 & xy & 0 & x^2 & 0 \\ -y^2 & -iz & 0 & 0 & 0 & x \\ 0 & 0 & -iz & -x & 0 & y \\ 0 & xy & -x^2 & -iz & y^3 & 0 \\ x & 0 & 0 & y & -iz & 0 \\ 0 & x^2 & y^3 & 0 & xy^2 & -iz \end{pmatrix},$$

$$\psi_2 = \begin{pmatrix} iz & -y^2 & xy & 0 & x^2 & 0 \\ -y^2 & iz & 0 & 0 & 0 & x \\ 0 & 0 & iz & -x & 0 & y \\ 0 & xy & -x^2 & y & iz & 0 \\ 0 & x^2 & y^2 & 0 & xy^2 & iz \end{pmatrix}$$

- $$\varphi_3 = \begin{pmatrix} -y^2+iz & 0 & xy & x \\ -xy & y^2+iz & x^2 & 0 \\ 0 & x & iz & y \\ x^2 & -xy & y^3 & iz \end{pmatrix}, \quad \psi_3 = \begin{pmatrix} -y^2-iz & 0 & xy & x \\ -xy & y^2-iz & x^2 & 0 \\ 0 & x & -iz & y \\ x^2 & -xy & y^3 & -iz \end{pmatrix}.$$

- $$\varphi_4 = \begin{pmatrix} -y^2-iz & 0 & xy & x \\ -xy & y^2-iz & x^2 & 0 \\ 0 & x & -iz & y \\ x^2 & -xy & y^3 & -iz \end{pmatrix}, \quad \psi_4 = \begin{pmatrix} -y^2+iz & 0 & xy & x \\ -xy & y^2+iz & x^2 & 0 \\ 0 & x & iz & y \\ x^2 & -xy & y^3 & iz \end{pmatrix}.$$

- $$\varphi_5 = \begin{pmatrix} -y^2+iz & x \\ x^2 & y^2+iz \end{pmatrix}, \quad \psi^5 = \begin{pmatrix} -y^2-iz & x \\ x^2 & y^2-iz \end{pmatrix}.$$

- $$\varphi_6 = \begin{pmatrix} -y^2-iz & x \\ x^2 & y^2-iz \end{pmatrix}, \quad \psi_6 = \begin{pmatrix} -y^2+iz & x \\ x^2 & y^2+iz \end{pmatrix}.$$

Ejemplo 4.15. Ahora, para el polinomio $x^3+xy^3+z^2$ también se conocen las siguientes:

- $$\varphi^1 = \psi^1 = \begin{pmatrix} z & 0 & -x^2 & y \\ 0 & z & xy^2 & x \\ -x & y & -z & 0 \\ xy^2 & x^2 & 0 & -z \end{pmatrix}.$$

- $$\varphi^2 = \psi^2 = \begin{pmatrix} -z & y^2 & xy & 0 & x^2 & 0 \\ xy & z & 0 & 0 & 0 & -x \\ 0 & 0 & z & -x & 0 & y \\ 0 & -xy & -x^2 & -x & xy^2 & 0 \\ x & 0 & 0 & y & z & 0 \\ 0 & -x^2 & xy^2 & 0 & x^2y & y \end{pmatrix}.$$

- $$\varphi^3 = \psi^3 = \begin{pmatrix} -z & 0 & xy & -y^2 & 0 & 0 & x^2 & 0 \\ 0 & -z & 0 & y^2 & 0 & 0 & 0 & x \\ y^2 & y^2 & z & 0 & 0 & -x & 0 & 0 \\ 0 & xy & 0 & z & -x^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -x & -z & 0 & 0 & y \\ 0 & 0 & -x^2 & 0 & 0 & -z & xy^2 & y^2 \\ x & 0 & 0 & 0 & -y^2 & y^2 & z & 0 \\ 0 & x^2 & 0 & 0 & xy^2 & 0 & 0 & z \end{pmatrix}.$$

- $$\varphi^4 = \psi^4 = \begin{pmatrix} -z & y^2 & 0 & x \\ xy & z & -x^2 & 0 \\ 0 & -x & -z & y \\ x^2 & 0 & xy^2 & z \end{pmatrix}.$$

- $$\varphi^5 = \psi^5 = \begin{pmatrix} -z & 0 & xy & 0 & 0 & x \\ -xy & z & 0 & -y^2 & -x^2 & 0 \\ y^2 & 0 & z & -x & xy & 0 \\ 0 & -xy & -x^2 & -z & 0 & 0 \\ 0 & -x & 0 & 0 & xy & -xy^2 & z \end{pmatrix}.$$

- $$\varphi^6 = \psi^6 = \begin{pmatrix} z & 0 & -xy & x \\ 0 & z & x^2 & y^2 \\ -y^2 & x & -z & 0 \\ x^1 & xy & 0 & -z \end{pmatrix}.$$

- $$\varphi^7 = \psi^7 = \begin{pmatrix} z & x \\ x^2+y^3 & -z \end{pmatrix}.$$

Ejemplo 4.16. Finalmente, para el polinomio $x^3 + y^5 + z^2$ tenemos las siguientes factorizaciones:

- $$\varphi^1 = \psi^1 = \begin{pmatrix} z & 0 & x & y \\ 0 & z & y^4 & -x^2 \\ x^2 & y & -z & 0 \\ y^2 & -x & 0 & -z \end{pmatrix}.$$

- $$\varphi^2 = \psi^2 = \begin{pmatrix} z & -y^2 & xy & 0 & -x^2 & 0 \\ -y^3 & -z & 0 & 0 & 0 & x \\ 0 & 0 & -z & x & 0 & y \\ 0 & -xy & x^2 & z & y^4 & 0 \\ -x & 0 & 0 & y & -z & 0 \\ 0 & x^2 & y^4 & 0 & -xy^3 & z \end{pmatrix}.$$

- $$\varphi^3 = \psi^3 = \begin{pmatrix} -z & 0 & -xy & y^2 & 0 & 0 & x^2 & 0 \\ 0 & -z & y^3 & 0 & 0 & 0 & 0 & x \\ 0 & y^2 & z & 0 & 0 & -x & 0 & 0 \\ y^3 & xy & 0 & z & -x^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -x & -z & 0 & y^3 & y \\ 0 & 0 & -x^2 & 0 & 0-z & 0 & y^2 & \\ x & 0 & 0 & 0 & y^2 & -y & z & 0 \\ 0 & x^2 & 0 & 0 & 0 & y^3 & 0 & z \end{pmatrix}$$

- $$\varphi^4 = \psi^4 = \begin{pmatrix} z & 0 & xy & 0 & 0 & -y^2 & y^3 & 0 & -x^2 & 0 \\ 0 & -z & 0 & 0 & 0 & 0 & 0 & -y^2 & 0 & x \\ 0 & 0 & -z & y^2 & 0 & 0 & 0 & x & 0 & 0 \\ 0 & xy & y^3 & z & 0 & 0 & -x^2 & 0 & 0 & 0 \\ 0 & y^2 & 0 & 0 & z & -x & 0 & 0 & y^3 & 0 \\ -y^3 & 0 & 0 & 0 & -x^2 & -z & 0 & 0 & 0 & y^2 \\ 0 & 0 & 0 & -x & 0 & 0 & -z & 0 & 0 & y \\ 0 & -y^3 & x^2 & 0 & 0 & 0 & xy^2 & z & 0 & 0 \\ -x & 0 & 0 & 0 & y^2 & 0 & 0 & y & -z & 0 \\ 0 & x^2 & xy^2 & 0 & 0 & 0 & y^4 & 0 & 0 & z \end{pmatrix}.$$

- $$\varphi^5 = \psi^5 = \begin{pmatrix} -z & 0 & 0 & 0 & 0 & 0 & 0 & y^2 & 0 & 0 & 0 & x \\ 0 & -z & -xy & 0 & 0 & 0 & y^3 & -y^2 & 0 & 0 & x^2 & 0 \\ 0 & 0 & z & 0 & 0 & -y^2 & 0 & 0 & y^3 & -x & 0 & 0 \\ xy & 0 & 0 & z & -y^3 & 0 & 0 & 0 & -x^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -y^2 & -z & 0 & 0 & x & 0 & 0 & 0 & 0 \\ 0 & 0 & -y^3 & 0 & 0 & -z & -x^2 & 0 & 0 & 0 & xy^2 & y^2 \\ y^2 & y^2 & 0 & 0 & 0 & -x & z & 0 & 0 & 0 & 0 & 0 \\ y^3 & 0 & 0 & 0 & x^2 & 0 & 0 & z & -xy^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -x & 0 & 0 & 0 & 0 & -z & 0 & 0 & y \\ 0 & 0 & -x^2 & -y^3 & 0 & 0 & xy^2 & 0 & 0 & -z & -y^4 & 0 \\ 0 & x & 0 & 0 & y^2 & 0 & 0 & 0 & 0 & -y & z & 0 \\ x^2 & 0 & 0 & 0 & -xy^2 & 0 & 0 & 0 & y^4 & 0 & 0 & z \end{pmatrix}$$

- $$\varphi^6 = \psi^6 = \begin{pmatrix} -z & 0 & 0 & y^2 & 0 & x \\ xy & z & -y^3 & 0 & -x^1 & 0 \\ 0 & -y^2 & -z & x & 0 & 0 \\ y^3 & 0 & x^2 & z & -xy^2 & 0 \\ 0 & -x & 0 & 0 & -z & y \\ x^2 & 0 & -xy^2 & 0 & y^4 & z \end{pmatrix}.$$

- $$\varphi^7 = \psi^7 = \begin{pmatrix} z & 0 & 0 & 0 & -y^3 & 0 & 0 & -x \\ xy & -z & 0 & 0 & 0 & y^2 & x^2 & 0 \\ 0 & 0 & -z & y^2 & 0 & x & -y^3 & 0 \\ 0 & 0 & 0 & z & -x^2 & 0 & 0 & y^2 \\ -y^2 & 0 & 0 & -x & -z & 0 & 0 & 0 \\ 0 & y^3 & x^2 & 0 & xy^2 & z & 0 & 0 \\ 0 & x & -y^2 & 0 & 0 & 0 & z & y \\ -x^2 & 0 & 0 & y^3 & 0 & 0 & 0 & -z \end{pmatrix}$$

- $$\varphi^8 = \psi^8 = \begin{pmatrix} z & 0 & x & y^2 \\ 0 & z & y^3 & -x^2 \\ x^2 & y^2 & -z & 0 \\ y^3 & -x & 0 & -z \end{pmatrix}$$

A los polinomios de los últimos 4 ejemplos se les conoce como *polinomios del tipo ADE (de tres variables)*, de hecho en [KST07] se prueba que estas matrices son todas la posibles factorizaciones por matrices de cada uno de estos polinomios, cuando decimos que son todas estamos haciendo referencia a que en caso de encontrar alguna otra factorización por matrices que no sea alguna de las que se enuncian en cada ejemplo, entonces esa factorización se puede "descomponer" en una suma directa de alguna de las anteriores. También, podemos observar que hay matrices que podrían requerir de métodos avanzados para hallarlas, es por ello que los ejemplos con la propiedad de ser indescomponibles son escasos en la literatura y como mencionamos el tamaño de las matrices puede ser muy grande. Incluso si existieran ejemplos de factorizaciones por matrices, hacer la comprobación vía computadora tomaría una cantidad de tiempo exagerada, pues el algoritmo más eficiente que se conoce para multiplicar matrices de $n \times n$ toma un tiempo del orden de n^3.

4.3. Algoritmos para encontrar factorizaciones por matrices y más ejemplos

4.3.1. Método estándar

Como ya hemos recalcado en la secciones anteriores, dado un polinomio con coeficientes complejos y hallar una factorización por matrices resulta tedioso, además de que es complejo verificar que dicho par de matrices cumpla con la definición. Sin embargo, Crisler en [CD16] describió un método para hallar la factorización de cualquier polinomio, a pesar de ser de gran utilidad, este método resulta ser ineficiente, pues si el polinomio consta de n monomios la matriz resultante al aplicarle esta técnica es de tamaño $2^{n-1} \times 2^{n-1}$.

A la técnica descrita por Crisler se le conoce como **método estándar**. Dado un polinomio $p = f_1 + f_2 + \ldots + f_n \in \mathbb{C}[x, y, z]$ donde f_i representa un monomio, debemos seguir los siguientes pasos para hallar una factorización por matrices:

- A los momios f_1 y f_2 los separaremos en dos factores, digamos que $f_1 = g_{f_1} h_{f_1}$ y $f_2 = g_{f_2} h_{f_2}$, entonces el siguiente par de matrices es una factorización para $f_1 + f_2$:
$$\varphi_1 = \begin{pmatrix} g_{f_1} & -g_{f_2} \\ h_{f_2} & h_{f_1} \end{pmatrix}, \quad \psi_1 = \begin{pmatrix} h_{f_1} & g_{f_2} \\ -h_{f_2} & g_{f_1} \end{pmatrix}.$$

- Para el monomio f_3 de igual manera, lo separamos en dos factores $f_3 = g_{f_3} h_{f_3}$, luego las "matrices" siguientes son una factorización de $f_1 + f_2 + f_2$:
$$\varphi_2 = \begin{pmatrix} \varphi_1 & -g_{f_3} \operatorname{Id}_2 \\ h_{f_3} \operatorname{Id}_2 & \psi_1 \end{pmatrix}, \quad \psi_2 = \begin{pmatrix} \psi_1 & g_{f_3} \operatorname{Id}_2 \\ -h_{f_3} \operatorname{Id}_2 & \varphi_1 \end{pmatrix}.$$

  Hacemos un énfasis en "matrices" ya que, rigurosamente hablando, φ_2 y ψ_2 son matrices pero sus entradas son matrices, sin embargo debemos entender la notación anterior como una "fusión" de las matrices.

- Continuando de esta manera, cuando llegamos al monomio $f_n = g_{f_n} h_{f_n}$ obtenemos las siguientes matrices que resultan ser una factorización de p que lo que

buscamos:

$$\varphi_{n-1} = \begin{pmatrix} \varphi_{n-1} & -g_{f_n}\operatorname{Id}_n \\ h_{f_n}\operatorname{Id}_n & \psi_{n-1} \end{pmatrix}, \quad \psi_{n-1} = \begin{pmatrix} \psi_{n-1} & g_{f_n}\operatorname{Id}_n \\ -h_{f_n}\operatorname{Id}_n & \varphi_{n-1} \end{pmatrix}.$$

Nuevamente, es inmediato ver que podemos obtener al menos $n!$ factorizaciones por matrices del polinomio p, es decir al menos tantas como permutaciones de la cantidad de monomios que tenga el polinomio elegido. Ahora, veamos un par de ejemplos utilizando este método.

Ejemplo 4.17. Consideremos el polinomio $p = x^2y^3 + xz^7$. Entonces, tomando $f_1 = (x^2)(y^3)$ y $f_2 = (x)(z^7)$ tenemos el siguiente par de matrices:

$$\varphi = \begin{pmatrix} x^2 & -x \\ z^7 & y^3 \end{pmatrix}, \quad \psi = \begin{pmatrix} y^3 & x \\ -z^7 & x^2 \end{pmatrix}$$

Ejemplo 4.18. Aplicando el método al polinomio $p = x^2y^3 + xz^7 + xyz$, tenemos, del ejemplo anterior, que las siguientes matrices son una factorización de $x^2y^3 + xz^7$:

$$\varphi_1 = \begin{pmatrix} x^2 & -x \\ z^7 & y^3 \end{pmatrix}, \quad \psi_1 = \begin{pmatrix} y^3 & x \\ -z^7 & x^2 \end{pmatrix}$$

Continuando con el método y considerando a $f_3 = (xy)z$ tenemos que la factorización por matrices de p:

$$\varphi = \begin{pmatrix} x^2 & -x & -xy & 0 \\ z^7 & y^3 & 0 & -xy \\ z & 0 & y^3 & x \\ 0 & z & -z^7 & x^2 \end{pmatrix}, \quad \psi = \begin{pmatrix} y^3 & x & xy & 0 \\ -z^7 & x^2 & 0 & xy \\ -z & 0 & x^2 & -x \\ 0 & -z & z^7 & y^3 \end{pmatrix}$$

El método anterior se puede "simplificar" en la siguiente proposición que técnicamente describe lo que hemos hecho en cada paso y cuya demostración puede ser consultada en [Fom24, Corolario 4.1]:

Proposición 4.19. *Dados tres polinomios f, g, $h \in \mathbb{C}[x, y, z]$ y (α, β) una factorización por matrices de f de tamaño n, entonces las siguientes matrices on una factori-*

zación de $f + gh$*:*

$$\varphi = \begin{pmatrix} \alpha & -g\,\mathrm{Id}_n \\ h\,\mathrm{Id}_n & \beta \end{pmatrix}, \quad \psi = \begin{pmatrix} \beta & g\,\mathrm{Id}_n \\ -h\,\mathrm{Id}_n & \alpha \end{pmatrix}.$$

BIBLIOGRAFÍA

[Alu09] Paolo Aluffi. *Algebra: Chapter 0*, volume 104 of *Grad. Stud. Math.* Providence, RI: American Mathematical Society (AMS), 2009.

[AM16] Michael F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Boulder: Westview Press, student economy edition edition, 2016.

[BEH87] Ragnar-Olaf Buchweitz, David Eisenbud, and Jürgen Herzog. Cohen-Macaulay modules on quadrics. With an appendix by Ragnar-Olaf Buchweitz: The comparison theorem (p. 96- 116). Singularities, representation of algebras, and vector bundles, Proc. Symp., Lambrecht/Pfalz/FRG 1985, Lect. Notes Math. 1273, 58-95; 96-116 (1987)., 1987.

[BGS87] R.-O. Buchweitz, G.-M. Greuel, and F.-O. Schreyer. Cohen-Macaulay modules on hypersurface singularities. II. *Invent. Math.*, 88:165–182, 1987.

[BH98] Winfried Bruns and Jürgen Herzog. *Cohen-Macaulay rings.*, volume 39 of *Camb. Stud. Adv. Math.* Cambridge: Cambridge University Press, rev. ed. edition, 1998.

[CD16] David Crisler and Kosmas Diveris. Matrix factorizations of sums of squares polynomials. *Pi Mu Epsilon J.*, 14(5):301–306, 2016.

[DF91] David S. Dummit and Richard M. Foote. *Abstract algebra*. Englewood Cliffs, NJ: Prentice-Hall International, Inc., 1991.

[Eis80a] David Eisenbud. Homological algebra of a complete intersection, with an application to group representations. *Trans. Am. Math. Soc.*, 260:35–64, 1980.

[Eis80b] David Eisenbud. Homological algebra on a complete intersection, with an application to group representations. *Transactions of the American Mathematical Society*, 260(1):35–64, 1980.

[Eis95] David Eisenbud. *Commutative algebra. With a view toward algebraic geometry*, volume 150 of *Grad. Texts Math.* Berlin: Springer-Verlag, 1995.

[Fom24] Yves Baudelaire Fomatati. Refined multiplicative tensor product of matrix factorizations. *J. Pure Appl. Algebra*, 228(5):20, 2024. Id/No 107556.

[Kap73] Irving Kaplansky. Commutative rings. Conf. commutat. Algebra, Lawrence, Kansas 1972, Lect. Notes Math. 311, 153-166 (1973)., 1973.

[KST07] Hiroshige Kajiura, Kyoji Saito, and Atsushi Takahashi. Matrix factorizations and representations of quivers. II: Type ADE case. *Adv. Math.*, 211(1):327–362, 2007.

[Lam99] Tsit Yuen Lam. *Lectures on modules and rings*, volume 189 of *Grad. Texts Math.* New York, NY: Springer, 1999.

[Mus99] Chitikila Musili. *Introduction to rings and modules.* New Delhi: Narosa Publishing House, 2nd, revised ed. edition, 1999.

[Osb00] Scott Osborne. *Basic homological algebra*, volume 196 of *Grad. Texts Math.* New York, NY: Springer, 2000.

[Rot79] Joseph J. Rotman. *An introduction to homological algebra*, volume 85 of *Pure Appl. Math., Academic Press*. Academic Press, New York, NY, 1979.

[Rot02] Joseph J. Rotman. *Advanced modern algebra*. Upper Saddle River, NJ: Prentice Hall/Pearson Education, 2002.

[Wei95] Charles A. Weibel. *An introduction to homological algebra. 1st pbk-ed*, volume 38 of *Camb. Stud. Adv. Math.* Cambridge: Cambridge Univ. Press, 1st pbk-ed. edition, 1995.

[Yos98] Yuji Yoshino. Tensor products of matrix factorizations. *Nagoya Math. J.*, 152:39–56, 1998.