El Teorema de Serre-Auslander-Buchsbaum

(Serre-Auslander-Buchsbaum's Theorem)

Ignacio González Mantecón

Trabajo de Fin de Grado

para acceder al

Grado en Matemáticas

Facultad de Ciencias

Universidad de Cantabria

Director: Luis Miguel Pardo Vasallo

Abril - 2022

Abstract. This manuscript is devoted to present a detailed, self-contained proof of both: one of J.P. Serre's conjectures (1955) about regular local rings and the subsequent answer to E. Artin's question about factoriality in said rings, given by M. Auslander and D.A. Buchsbaum in 1959. The first result states that being a regular local ring is a local property, while the second one claims that every regular local ring is a unique factorization domain. Prior to showing the proof of these statements, we analyze the different notions of dimension in Ring Theory and a particular case in which they all coincide, the so-called Dimension Theorem. Then, we introduce the concept of regular local ring, as well as the necessary tools to tackle the problem; that is, bi-functors Tor and Ext, whose properties will play a crucial role in providing a homological characterization of regular local rings in terms of their global dimension. This result constitutes the fundamental pillar of the manuscript and will be key in proving Serre's and Auslander-Buchsbaum's Theorems. By drawing on projective resolutions of R-modules and derived functors, this text aims to highlight the relevance and power of homological methods when solving problems that arise in other branches of Mathematics such as Commutative Algebra.

Key Words: Serre's conjecture, regular local ring, projective resolutions, derived functors, homological methods.

Resumen. Este manuscrito se dedica a presentar una prueba detallada y autocontenida de una de las conjeturas de J.P. Serre (1955) sobre anillos locales regulares y de la respuesta a la pregunta de E. Artin sobre la factorialidad en dichos anillos, por parte de M. Auslander y D.A. Buchsbaum en 1959. El primero de los resultados dice que ser un anillo local regular es una propiedad local, mientras que el segundo afirma que todo anillo local regular es dominio de factorización única. Antes de mostrar la prueba de estas afirmaciones, se analizan las distintas nociones de dimensión de la Teoría de Anillos y un caso particular en el que todas ellas coinciden, el conocido como Teorema de la Dimensión Local. Seguidamente, se introduce el concepto de anillo local regular, así como las herramientas necesarias para abordar el problema; esto es, los bi-functores Tor y Ext, cuyas propiedades jugarán un papel crucial proporcionando una caracterización de los anillos locales regulares en términos de su dimensión global. Este resultado constituye el pilar fundamental de este manuscrito y será clave en la prueba del los Teoremas de Serre y Auslander-Buchsbaum. A través del uso de resoluciones proyectivas de R-módulos y functores derivados, este texto pretende recalcar la relevancia y el poder de los métodos del Álgebra Homológica a la hora de resolver problemas que surgen en otras áreas de las Matemáticas como el Álgebra Conmutativa.

Palabras Clave: conjetura de Serre, anillo local regular, resoluciones proyectivas, functores derivados, métodos del Álgebra Homológica.

Índice

CAPíTULO 0

Introducción y Resumen de Contenidos de la Memoria

Índice

0.1. Introducción y Resumen de resultados

A mediados del pasado siglo XX, el Álgebra Conmutativa, fundada en su forma moderna por E. Noether, sufre un cambio fundamental: la aparición de Técnicas del Álgebra Homológica para responder a preguntas (naturales en el contexto conmutativo) sobre anillos locales regulares. El propósito de este Trabajo Fin de Grado es exponer, de forma tan auto-contenida como sea posible, las respuestas a estas preguntas, recogidas en el conocido como *Teorema de Serre-Auslander-Buchsbaum* (cf. [**Auslander-Buchsbaum, 1957**], [**Auslander-Buchsbaum, 1959**] y [**Serre, 1955**]).

Para contextualizar el trabajo presentado, recordemos un poco el origen del Álgebra Conmutativa moderna. En el primer tercio del pasado siglo, E. Noether fundamenta lo que daría en llamarse "Álgebra Moderna" y, en particular, el "Álgebra Conmutativa" entendida como la teoría de Anillos Conmutativos. El Álgebra Conmutativa se convertirá, con el tiempo, en el lenguaje básico natural de la Geometría Algebraica, la Teoría de Números Algebraicos o la Geometría Diofántica. En origen, E. Noether está muy influenciada por el pensamiento axiomático de D. Hilbert y E. Artin. Algunas de sus contribuciones originales más destacables son el famoso *Teorema de Lasker-Noether* o su desarollo axiomático de lo que hoy llamamos *anillos noetherianos*. Sin embargo, será en su seminario cotidiano en Göttingen, en el que trabaja junto a E. Artin, en donde compartirá su pensamiento con diversos investigadores. De E. Noether se ha destacado siempre su enorme generosidad como se ve en la forma de compartir con los brillantes colaboradores de la época (W. Krull, B.L. van der Waerden o G. Herman, por ejemplo) su pensamiento y sus ideas. Por eso podemos encontrar trazas de esas ideas y pensamiento en las obras fundamentales de estos autores, en especial en la obra de W. Krull[1] o B.L. van der Waerden[2] y [3].

E. Noether muere joven y exiliada en Suiza por su doble condición de mujer y judía. Pero su obra, ideas y pensamiento no se pierden y se expandirán por todo el mundo, estableciéndose como un conocimiento matemático global y usual en la formación incluso de pre-graduados. En este punto, se debe señalar que no sólo se expande en el contexto de la matemática europea occidental, sino que alcanzó gran profundidad, por ejemplo, en la escuela japonesa del Álgebra Conmutativa (Akizuki, Azumaya, Nagata, Nakayama, Matsumura...).

[1][Krull, 1935] W. Krull, *Idealtheorie.* Ergebnisse der Mathematik **4**, Springer, (1935).

[2][van der Waerden, 1930] B.L. van der Waerden, *Moderne Algebra.* Teil I. Die Grundlehren der mathematischen Wissenschaften **33**, Springer, (1930).

[3][van der Waerden, 1931] B. L. van der Waerden, *Moderne Algebra.* Teil II. Die Grundlehren der mathematischen Wissenschaften **34**, Springer, (1931).

A principios de los años 50, el Álgebra Conmutativa sufrirá varios cambios significativos. De una parte, D.G. Northcott publica un texto sobre *Teoría de Ideales*[4], que compila los resultados fundamentales sobre ideales en anillos noetherianos y que influirá textos posteriores como el popular [**Atiyah, 1969**]. De otra parte, A. Weil[5] introduce el concepto de variedad algebraica abstracta que influirá en la escuela de A. Grothendieck y en la Geometría Algebraica moderna. Por su parte, C. Chevalley [6] fortalecerá la iniciativa de A. Weil con su obra del año 1951.

En 1956, H. Cartan y S. Eilenberg[7] introducen el "Álgebra Homológica". Algunos autores mantienen el estilo y tendencia de la escuela de Noether (como [**Zarinski-Samuel, 1958-60**] o [**Nagata, 1962**]), mientras el Álgebra Homológica va generando preguntas que requieren respuesta.

Según confesiones de D.A. Buchsbaum, el origen del presente Trabajo Fin de Grado se resume del modo siguiente:

"In 1953-54, E. Artin asked me to describe homological algebra to him. In addition to Ext and Tor, I decided to show him the 'homological proof' of the Hilbert Basis Theorem and indicated that the same proof showed that a regular local ring had finite dimension. Artin then mentioned the open localization problem, and I said that if the converse of the Theorem I just showed him were true, the localization result would be trivial. He asked if I could prove the converse, I said no, and we both agreed that it would be be nice to prove it. The question of factoriality in regular local rings also came up in that conversation, and so I set myself the goal of proving those two theorems. I persuaded Auslander to join me in that project..." .

A la sazón, J.P. Serre había llegado también a las mismas preguntas que Artin y Buchsbaum. Así, Serre responde (afirmativamente en el sentido de la pregunta de Artin) probando que un anillo es local regular si y solamente si es de dimensión homológica finita en [**Serre, 1955**] (Auslander y Buchsbaum lo harán en [**Auslander-Buchsbaum, 1957**]). Como consecuencia casi inmediata, la propiedad de ser regular será una propiedad local. Son los primeros resultados significativos en los que se prueba el potencial del Álgebra Homológica en el Álgebra Conmutativa, que se resume en los enunciados siguientes:

Teorema (**Serre-Auslander-Buchsbaum**). *Sea $(R, \mathfrak{m})$ un anillo local noetheriano. Entonces, $(R, \mathfrak{m})$ es local regular si y solamente si es de dimensión homológica finita.*

Teorema (**Serre**). *La propiedad de ser "regular" en anillos locales noetherianos es una propiedad local. Es decir, sea $(R, \mathfrak{m})$ un anillo local noetheriano. $(R, \mathfrak{m})$ es local regular si y solamente si para cada ideal primo $\mathfrak{p} \in Spec(R)$, $(R_\mathfrak{p}, \mathfrak{p}R_\mathfrak{p})$ es un anillo local regular.*

Estos dos resultados son probados en el presente Trabajo Fin de Grado: véase Teorema 2.8.5 y 2.8.6; y se complementan con el conocido como Teorema de Auslander-Buchsbaum: [**Auslander-Buchsbaum, 1959**]

Teorema (**Auslander-Buchsbaum**). *Si $(R, \mathfrak{m})$ es un anillo local regular, entonces es dominio de factorización única.*

Este teorema se expone en este Trabajo Fin de Grado: véase Teorema 2.9.7.

A este respecto, deben señalarse dos resultados que preceden al Teorema de Auslander-Buchsbaum y que, sin embargo, no requieren técnicas de Álgebra Homológica.

i) En [**Nagata, 1962**], M. Nagata ya había demostrado que los anillos locales regulares eran dominios de factorización única para el caso de dimensión mayor o igual que 3.
ii) I.S. Cohen en [**Cohen, 1949**], ha probado ya que todo anillo local noetheriano $(R, \mathfrak{m})$ equicaracterístico es un anillo local regular. Un anillo local noetheriano $(R, \mathfrak{m})$ se

[4][Northcott, 1953] D. G. Northcott, *Ideal Theory.* Cambridge University Press, (1953).
[5]5 [Weil, 1946] A. Weil, *Foundations of Algebraic Geometry.* Amer. Mat. Soc., (1946).
[6][Chevalley, 1951] C. Chevalley, *Introduction to the Theory of algebraic functions in one variable.* Amer. Mat. Soc., (1951).
[7][Cartan-Eil., 1956], H. Cartan, S. Eilenberg, *Homological Algebra.* Princeton University Press, (1956).

dice equicaracterístico si tiene la misma característica que su cuerpo residual $k(\mathfrak{m}) = R/\mathfrak{m}$. Los ejemplos naturales son las $K-$álgebras $K[V]_{\mathfrak{p}}$, localización en un primo $\mathfrak{p} \in Spec(K[V])$ de un anillo $K[V]$ de funciones polinomiales sobre una variedad algebraica $V \subseteq K^n$, donde K es un cuerpo. Cohen prueba que todo anillo local noetheriano equicaracterístico y completo $(R, \mathfrak{m})$ contiene un cuerpo isomorfo a $k(\mathfrak{m})$ (cuerpo de representantes). Así, prueba que todo anillo local regular equicaracterístico y completo es isomorfo a un anillo de series de potencias formales y, por los Teoremas de Preparación y División de Weierstrass, es dominio de factorización única. De ahí conluye su particular versión del resultado de Auslander-Buchsbaum.

Estos Teoremas de Serre-Auslander-Buchsbaum causarán un gran impcato en la comunidad de Álgebra Conmutativa. Parecería que todo el Álgebra Conmutativa se subsume en Técnicas del Álgebra Homológica si no fuera por un resultado también famoso de la segunda mitad del pasado siglo: *El Teorema de Quillen* [8] *y Suslin*[9]. Este Teorema resuelve afirmativamente otra conjetura de Serre usando técnicas más próximas a la filosofía de trabajo original de E. Noether y sus primeros seguidores que al Álgebra Homológica.

En todo caso, el presente TFG se dedicará a presentar una prueba tan completa y autocontenida como sea posible de los citados Teoremas de Serre y Auslander-Buchsbaum.

0.2. Unas Palabras sobre Anillos Locales Regulares

En el apartado precedente hemos discutido el contexto histórico de los problemas tratados en este Trabajo Fin de Grado y de su significado. Sin embargo, un término es repetido sistemáticamente sin definir: los anillos locales regulares. En esta Sección pretendemos mostrar al lector cómo y por qué son relevantes estos anillos.

Comencemos por el ejemplo más clásico: los anillos de series de potencias formales $K[[X_1, \ldots, X_n]]$. La prueba se remonta a los Teoremas de División y Preparación de Weierstrass de 1895, que permiten concluir que $K[[X_1, \ldots, X_n]]$ es un anillo local noetheriano cuyo maximal $\mathfrak{m} = (X_1, \ldots, X_n)$ está generado por tantos elementos como su dimensión de Krull y, además, permiten concluir que $K[[X_1, \ldots, X_n]]$ es un dominio de factorización única. Por supuesto, si $K = \mathbb{R} \vee \mathbb{C}$, los mismos resultados son válidos para los anillos de series convergentes $K\{X_1, \ldots, X_n\}$. Recuérdese que la dimensión de Krull de un anillo es el máximo de las longitudes de cadenas de ideales primos en R, es decir, la longitud máxima de caminos en el grafo orientado $(Spec(R), \subseteq)$, donde las aristas vienen dadas por la relación de inclusión. Un *anillo local regular* es un anillo local noetheriano $(R, \mathfrak{m})$, donde el ideal maximal $\mathfrak{m}$ está generado por un conjunto finito de elementos de $\mathfrak{m}$ de cardinal igual a la dimensión de Krull del anillo R. (cf. Proposición 1.5.3 para caracterizaciones equivalentes).

En el caso $n = 1$, el anillo local regular $K[[X_1]]$ (y las ideas de Weierstrass) entronca con un tipo de anillos que nos retro-trae a los trabajos de R. Dedekind: los *anillos de valoración discreta.* Si $(R, \mathfrak{m})$ es un anillo de valoración discreta, el sistema regular de parámetros $\{x\}$ está formado por un solo elemento, los ideales primos de R son (0) y $\mathfrak{m}$ y todo elemento $a \in R$ se puede escribir como $a = u \cdot x^n$, donde $u \in R^{\times}$ es una unidad. El exponente n es único y se llama orden (o valoración discreta) de a. En el caso analítico o en el caso de series de potencias formales es el orden de 0 como cero de la "función". Dedekind estudió estos anillos al estudiar los anillos de enteros algebraicos de un cuerpo de números. Así, sea $K = \mathbb{C}[\theta]$ una extensión finita de $\mathbb{C}$ y sea $\mathbb{Z}_K$ la clausura entera de $\mathbb{Z}$ en K, esto es, el conjunto de los elementos $\alpha \in \mathbb{C}[\theta]$ que satisfacen una ecuación mónica con coeficientes en $\mathbb{Z}$. Entonces, $\mathbb{Z}_K$ es un dominio de Dedekind, esto es, un dominio de integridad de dimensión 1 que es íntegramente cerrado en su cuerpo de fracciones. Se puede probar que un dominio R de dimensión 1 es dominio de Dedekind si y solamente si todas sus localizaciones $R_{\mathfrak{p}}$ por un primo no nulo son anillos de valoración discreta

[8][Quillen, 1976] D. Quillen, Projective modules over polynomial rings. Inventiones Mathematicae **36** (1976), 167-171.

[9][Suslin, 1976] A.A. Suslin, Projective modules over polynomial rings are free (in russian). Doklady Akademii Nauk SSSR **229** (1976), 1063-1066. Translated in Projective modules over polynomial rings are free, Soviet Mathematics, **17** (1976),1160-1164.

(esto es, si y solamente si $R_{\mathfrak{p}}$ es un anillo local regular de dimensión 1). El lector interesado puede seguir estos detalles en el Capítulo 9 de [**Atiyah, 1969**].

Los anillos locales regulares aparecerán también de manera natural en Geometría Algebraica. El caso de curvas es un caso también de dominios de Dedekind. Así, una curva irreducible $C \subseteq \mathbb{A}^n(\mathbb{K})$, con $\mathbb{K}$ algebraicamente cerrado, verifica que para cada punto $p \in C$ la localización $\mathbb{K}[C]_{\mathfrak{m}_p}$ es local regular si y solamente si $\mathbb{K}[C]$ es dominio de Dedekind. Se trata de curvas lisas o sin puntos singulares. En el caso $\mathbb{K} = \mathbb{C}$, serían las curvas que son subvariedad $\mathscr{C}^\infty$ (y analítica) de $\mathbb{C}^n$. Esto no sólo se restringe a curvas. Veámoslo sucintamente.

Sea $V \subseteq \mathbb{A}^n(\mathbb{K})$ una variedad algebraica irreducible en el espacio afín $n-$dimensional. Sea $p \in V$ un punto y T_pV el espacio tangente a V en p (en [**Shafarevich, 2007**] puede seguirse una definición de T_pV cuando $\mathbb{K}$ no necesariamente es $\mathbb{C}$). Un punto $p \in V$ se dice punto *liso* o regular de V cuando la dimensión de T_pV coincide con la dimensión de V como variedad (dimensión de Krull de $\mathbb{K}[V]$). Al resto de puntos se les denomina *singulares*. Sea $\mathfrak{m}_p \subseteq \mathbb{K}[V]$ el ideal de las funciones polinomiales definidas en V que se anulan en p.

$$\mathfrak{m}_p := \{f \in \mathbb{K}[V] : f(p) = 0\}.$$

Se puede probar que $T_pV = (\mathfrak{m}_p/\mathfrak{m}_p^2)^* = Hom_{\mathbb{K}}(\mathfrak{m}_p/\mathfrak{m}_p^2, \mathbb{K})$ es el dual de este cociente de ideales como $\mathbb{K}$-espacio vectorial. De hecho, $\mathfrak{m}_p/\mathfrak{m}_p^2$ es el $\mathbb{K}$-espacio vectorial de las diferenciales en $p \in V$. Esto conduce a un elegante resultado clásico conocido como el Criterio del Jacobiano:

Teorema (**Criterio del Jacobiano**). *Sea $\mathbb{K}$ un cuepo algebraicamente cerrado, $V \subseteq \mathbb{A}^n(\mathbb{K})$ una variedad algebraica afín, $p \in V$ un punto, $(\mathbb{K}[V_p], \mathfrak{m}_p)$ el anillo de gérmenes de funciones racionales definidas en p, $\mathfrak{m}_p/\mathfrak{m}_p^2$ el módulo de diferenciales de V en p y T_pV el espacio tangente a V en p. Son equivalentes:*

i) p es un punto regular de V.
ii) $dim(T_pV) = dim(\mathbb{K}[V]) = dim(\mathbb{K}[V_p])$.
iii) $dim(\mathfrak{m}_p/\mathfrak{m}_p^2) = dim(K[V_p])$, dimensión como $\mathbb{K}$-espacios vectoriales.
iv) El anillo $K[V_p]$ es un anillo local regular de dimensión igual a $dim(V)$.

Por supuesto, en el caso $\mathbb{K} = \mathbb{C}$, la condición $p \in V$ es regular equivale a que V sea una subvariedad analítica (Riemanniana, de hecho) de $\mathbb{C}^n$ en un entorno de $p \in V$.
Con todos estos comentarios hemos pretendido exhibir la omnipresencia de la noción de anillo local regular fuera del contexto del Álgebra Conmutativa.

0.3. Resumen de los Contenidos de la Memoria

En atención a las dos "escuelas" antes descritas del Álgebra Conmutativa, hemos dividido la memoria en dos partes distinguidas:

i) El Capítulo 1 está dedicado a probar el Teorema de la Dimensión Local y fijar la noción de anillo local regular, así como sus primeras propiedades. Este capítulo no contiene elementos de Álgebra Homológica y sigue la escuela de E. Noether y E. Artin.
ii) El Capítulo 2 está dedicado a probar los Teoremas de Serre y Auslander-Buchsbaum. Para hacerlo, hemos introducido las sucesiones de homología de complejos de R-módulos, hemos probado la existencia de resoluciones proyectivas de R-módulos, hemos introducido los bifunctores *Ext* y *Tor* (como Buchsbaum hiciera con Artin), la noción de dimensión homológica y hemos probado los citados teoremas. Aquí se muestra la fuerza del Álgebra Homológica.

A continuación resumimos los principales hitos de cada capítulo.

0.3.1. Resumen del Contenido del Capítulo 1. El capítulo comienza con la Sección 1.2 dedicada a establecer nociones básicas y los enunciados básicos esenciales relativos a *anillos y módulos graduados y filtrados.* Dedicamos especial atención a las filtraciones $\mathfrak{a}$-ádicas definidas por un ideal $\mathfrak{a}$ en un anillo noetheriano, la metrizabilidad de las topologías asociadas o la construcción del anillo graduado asociado $G_{\mathfrak{a}}(R) = \bigoplus_{n\in\mathbb{N}} \mathfrak{a}^n/\mathfrak{a}^{n+1}$ así como las condiciones de noetherianidad. Dado que el desarrollo completo de estos temas llevaría por encima el límite de 50 páginas establecido para los Trabajos Fin de Grado, hemos optado por presentar estos resultados en forma de "Extended Abstract" ("Resumen Extendido"), remitiendo al lector a

[**Pardo, 21**] o [**Raghavan et al., 1975**] para las demostraciones de los principales resultados enunciados. También la Sección 1.4 de este capítulo se presenta en forma de Resumen Extendido: se trata de la sección dedicada al *Lema de Artin-Rees* y al *Teorema de la Intersección de Krull*. En este caso, dada la relevancia de los resultados, hemos preferido incluir una demostración de los mismos en la Sección A.11 del Apéndice A.

El Lema de Artin-Rees puede resumirse del modo siguiente:
Consideremos R un anillo noetheriano, $\mathfrak{a}$ un ideal de R, M un R-módulo finitamente generado (y, por tanto, noetheriano) y N un submódulo de M (por tanto, finitamente generado). Disponemos de la filtración $\mathfrak{a}-$ádica en M dada mediante la siguiente cadena de submódulos:

$$\Sigma_{\mathfrak{a}}(M) := \{M \supseteq \mathfrak{a}M \supseteq \mathfrak{a}^2 M \supseteq ... \supseteq \mathfrak{a}^n M \supseteq ...\}.$$

Esta filtración induce en N una filtración como submódulo:

$$\Sigma_{\mathfrak{a}}(M,N) := \{N = M \cap N \supseteq \mathfrak{a}M \cap N \supseteq \mathfrak{a}^2 M \cap N \supseteq ... \supseteq \mathfrak{a}^n M \cap N \supseteq ...\}.$$

De otro lado, N posee la filtración natural $\mathfrak{a}$-ádica como R-módulo:

$$\Sigma_{\mathfrak{a}}(N) := \{N \supseteq \mathfrak{a}N \supseteq \mathfrak{a}^2 N \supseteq ... \supseteq \mathfrak{a}^n N \supseteq ...\}.$$

El Lema de Artin-Rees afirma, esencialmente, que las filtraciones inducida $\Sigma_{\mathfrak{a}}(M,N)$ y su filtración $\mathfrak{a}$-ádica $\Sigma_{\mathfrak{a}}(N)$ son equivalentes sobre N:

TEOREMA (**Lema de Artin-Rees**). *Sea R un anillo noetheriano, $\mathfrak{a}$ un ideal de R, M un R-módulo finitamente generado y N un submódulo de M. Entonces, existe $n \in \mathbb{N}$ tal que*

$$\mathfrak{a} \cdot (\mathfrak{a}^m M \cap N) = \mathfrak{a}^{m+1} M \cap N, \ \ \forall m \geq n.$$

En nuestro manuscrito este resultado se presenta como Corolario 1.3.3. Una consecuencia relevante de este resultado es el siguiente Teorema de Krull:

TEOREMA (**Teorema de Intersección de Krull**). *Sean R un anillo noetheriano, $\mathfrak{a}$ un ideal de R y M un R-módulo finitamente generado. Entonces,*

i) Si $N := \bigcap_{n\in\mathbb{N}} \mathfrak{a}^n M$, $\mathfrak{a}N = N$.

ii) Si $\mathfrak{a}$ está contenido en el radical de Jacobson de R,

$$\bigcap_{n\in\mathbb{N}} \mathfrak{a}^n M = (0)$$

y la topología definida por la filtración $\mathfrak{a}$-ádica sobre M es Hausdorff y metrizable.

iii) Si R es dominio noetheriano, para cada ideal propio $\mathfrak{a}$ de R se tiene:

$$\bigcap_{n\in\mathbb{N}} \mathfrak{a}^n = (0)$$

y la topología $\mathfrak{a}$-ádica sobre R es Hausdorff y metrizable.

Este resultado aparece como Teorema 1.3.4. Nótese que significa que si R es noetheriano, $\mathfrak{a}$ es un ideal de R y M es un R-módulo finitamente generado, entonces la topología inducida por la filtración $\Sigma_{\mathfrak{a}}(R)$ también es metrizable. También implica que si $\mathfrak{a} \subseteq R$ es un ideal contenido en el radical de Jacobson de R, el anillo graduado $G_{\mathfrak{a}}(R) = \bigoplus_{n\in\mathbb{N}} \mathfrak{a}^n/\mathfrak{a}^{n+1}$ es un dominio de integridad.
Pasamos así a las secciones principales de este capítulo: las Secciones 1.4 y 1.5.

La Sección 1.4 está dedicada a probar el *Teorema de la Dimensión Local*. La idea es probar la coincidencia de tres nociones de dimensión para anillos locales noetherianos. La primera (grado del polinomio de Hilbert-Samuel) hace referencia a una generalización (por parte de P. Samuel) del polinomio de Hilbert para los anillos graduados $\mathbb{K}[V]$ de funciones polinomiales sobre una variedad proyectiva $V \subseteq \mathbb{P}_n(\mathbb{K})$. El grado del polinomio de Hilbert será la dimensión de V. Para generalizarlo, se considera $(R,\mathfrak{m})$ un anillo local noetheriano, $\mathfrak{q} \subseteq \mathfrak{m}$ un ideal de definición de $(R,\mathfrak{m})$ (i.e. un ideal $\mathfrak{q}$ tal que $\exists m \in \mathbb{N}$ con $\mathfrak{m}^m \subseteq \mathfrak{q} \subseteq \mathfrak{m}$) y el anillo graduado asociado a la filtración $\mathfrak{q}$-ádica:

$$G_{\mathfrak{q}}(R) = \bigoplus_{n\in\mathbb{N}} \mathfrak{q}^n/\mathfrak{q}^{n+1}.$$

La función de Hilbert de este anillo graduado coincide con un polinomio (ver Proposición 1.4.4) y, por tanto, se puede extender a la función de Hilbert-Samuel (que resultará ser polinomial):

$$\begin{array}{rccc} P_{\mathfrak{q}}: & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & n & \longmapsto & \ell_{R/\mathfrak{q}}(R/\mathfrak{q}^n), \end{array}$$

donde $R/\mathfrak{q}$ es un anillo artiniano de dimensión 0 y $\ell_{R/\mathfrak{q}}$ significa longitud en el sentido del Teorema de Jordan-Hölder (cf. Teorema A.9.6). Se prueba que el grado de $P_{\mathfrak{q}}$ es independiente del ideal de definición $\mathfrak{q}$ elegido (ver Proposición 1.4.7) y se define la *dimensión de Hilbert-Samuel* de $(R, \mathfrak{m})$ como el grado de $P_{\mathfrak{q}}$.
Por una parte, C. Chevalley está interesado en el número mínimo de generadores de un ideal de definición. Así, la *dimensión de Chevalley* de un anillo local noetheriano $(R, \mathfrak{m})$ es el mínimo de los números naturales $r \in \mathbb{N}$ tales que existen $\{a_1, \ldots, a_r\}$ generando un ideal de definición de $(R, \mathfrak{m})$.
Por último, aunque es la primera históricamente y la más natural, tenemos la *dimensión de Krull* de un anillo local noetheriano $(R, \mathfrak{m})$ como el máximo de las longitudes de caminos en el grafo orientado (con un número infinito de vértices) $(Spec(R), \subseteq)$, donde $\subseteq$ es la inclusión. Es decir, el máximo de las longitudes r de cadenas de primos

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r \subsetneq \mathfrak{m},$$

en $Spec(R)$.
El Teorema de la Dimensión Local afirma que las tres nociones anteriores coinciden (cf. Teorema 1.4.13). Esto es,

TEOREMA. *Sea $(R, \mathfrak{m})$ un anillo local noetheriano. Las tres cantidades siguientes son iguales y finitas:*

i) La dimensión de Krull de $(R, \mathfrak{m})$.
ii) La dimensión de Hilbert-Samuel de $(R, \mathfrak{m})$.
iii) La dimensión de Chevalley de $(R, \mathfrak{m})$.

En particular, el resultado prueba que la dimensión de Krull de los anillos locales noetheriano es finita (a pesar de ser $Spec(R)$ potencialmente infinito, los caminos más largos de $(Spec(R), \subseteq)$ tienen longitud acotada e igual entre todos ellos). Y, por tanto, las alturas de todo primo en un anillo local noetheriano son finitas (i.e. el subgrafo de $(Spec(R), \subseteq)$ de los primos contenidos en un ideal $\mathfrak{p} \in Spec(R)$ tiene altura finita). En cambio, como probó M. Nagata, no todo anillo noetheriano posee dimensión de Krull finita.

El Teorema de la Dimensión Local conduce naturalmente a la noción de anillo local regular, que se discute en la Sección 1.5. El resultado fundamental es la siguiente proposición (que se demuestra como Proposición 1.5.3 en la memoria):

PROPOSICIÓN 0.3.1. *Sea $(R, \mathfrak{m})$ un anillo local noetheriano, $k(\mathfrak{m}) = R/\mathfrak{m}$ su cuerpo residual y sea $r = dim(R)$. Son equivalentes:*

i) El ideal maximal $\mathfrak{m}$ está generado por r elementos. Tales sistemas de generadores de $\mathfrak{m}$ con R elementos se denominan sistemas regulares de parámetros.
ii) El $k(\mathfrak{m})$-espacio vectorial $\mathfrak{m}/\mathfrak{m}^2$ es de dimensión r.
iii) El anillo $G_{\mathfrak{m}}(R)$ es un anillo de polinomios en r variables sobre el cuerpo $k(\mathfrak{m})$, con la graduación natural de $k(\mathfrak{m})[T_1, \ldots, T_r]$.

Cualquier anillo local noetheriano $(R, \mathfrak{m})$ que satisfaga una (y, por tanto, todas) de las propiedades precedentes se denomina *anillo local regular*.

A partir de esta noción, podemos probar algunas propiedades elementales de los anillos locales regulares: son dominios de integridad (Corolario 1.5.4), los sistemas regulares de parámetros forman una sucesión regular y los cocientes $R_j = R/(a_1, \ldots, a_j)$ también son anillos locales regulares (Proposición 1.5.5). Como último resultado elemental probamos que un anillo local noetheriano es regular si y solamente si el ideal maximal está generado por una sucesión regular de longitud igual a la dimensión de Krull (cf. Proposición 1.5.7).

0.3.2. Resumen del Contenido del Capítulo 2. El Capítulo 2 se dedica a establecer los elementos de Álgebra Homológica que conducen a probar los Teoremas de Serre y Auslander-Buchsbaum citados al comienzo de esta Introducción. De nuevo, por no sobrepasar los límites previstos en la normativa de la Facultad de Ciencias, comenzamos con una Sección 2.2 en formato de "Resumen Extendido". Trabajaremos en la categoría de $R - \mathcal{M}od$, cuyos objetos son los módulos sobre un anillo R fijado, y cuyos morfismos son los elementos del R-módulo $Hom_R(M, N)$ con la operación usual de composición de morfismos. Usaremos el lenguaje de Teoría de Categorías para referirnos a functores (covariantes y contravariantes), equivalencia natural, etc. Pero serán usados meramente como lenguaje y no se necesitarán más allá de los elementos mínimos que pueden verse en los primeros capítulos de [**Pardo, 21**]. En esta Sección 2.2 recordamos las nociones de complejos de cadena y co-cadena de R-módulos, las sucesiones de homología (para complejos de cadena) y co-homología (para complejos de co-cadena) y enunciamos algunas de sus propiedades más elementales. Asimismo, definimos los morfismos de cadena y co-cadena, los morfismos conectores entre módulos de homología y la sucesión exacta larga de homología asociada a una sucesión exacta corta de complejos de cadena. También definimos la noción de homotopía entre morfismos de complejos de cadena y recordamos que la existencia de una homotopía genera módulos de homología isomorfos. El material se ha tomado de [**Raghavan et al., 1975**].

La Sección 2.3 está dedicada a probar la existencia de resoluciones proyectivas de R-módulos. Dado un R-módulo M, una resolución proyectiva de M es una sucesión exacta de R-módulos (potencialmente infinita):

$$\cdots \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \xrightarrow{\epsilon} M \longrightarrow 0,$$

donde cada R-módulo P_i es un R-módulo proyectivo. En la Proposición 2.3.1 probamos que todo R-módulo admite una resolución proyectiva y que, si R y M son noetherianos, los R-módulos proyectivos P_i pueden elegirse libres de rango finito. Seguidamente, probaremos algunos resultados elementales de resoluciones proyectivas: El *Lifting Theorem* (Proposición 2.3.2), que afirma que los morfismos entre R-módulos pueden "levantarse" a morfismos entre resoluciones proyectivas; el *Horseshoe Lemma* (Proposición 2.3.3), que muestra cómo una sucesión exacta de R-módulos permite "levantamiento" a una resolución proyectiva de sucesiones exactas cortas; o la Proposición 2.3.4, que muestra cómo un diagrama conmutativo de sucesiones exactas cortas de R-módulos puede "levantarse" a un diagrama conmutativo de resoluciones proyectivas de sucesiones exactas cortas. Las demostraciones son tomadas de [**Raghavan et al., 1975**].

Así llegamos a la Sección 2.4, en la que introducimos los bifunctores $Tor_n^R(M, N)$. Dados M y N dos R-módulos y una resolución proyectiva de M:

$$\underline{P}: \ \cdots \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \xrightarrow{\epsilon} M \longrightarrow 0,$$

se considera el complejo de cadena inducido por $- \otimes_R N$, donde $\otimes_R$ es el producto tensorial:

$$\underline{P} \otimes_R N: \ \cdots \longrightarrow P_n \otimes_R N \longrightarrow P_{n-1} \otimes_R N \longrightarrow \cdots \longrightarrow P_1 \otimes_R N \longrightarrow P_0 \otimes_R N \longrightarrow 0.$$

Los n-ésimos módulos de torsión $Tor_R^n(M, N)$ son los $n-$ésimos módulos de homología de $\underline{P} \otimes_R N$, entonces:

$$Tor_n^R(M, N) := H_n(\underline{P} \otimes_R N).$$

Obviamente, esta definición depende (aparentemente) de la resolución $\underline{P}$ elegida. Por eso hay que hacer un esfuerzo en probar la buena definición de esta noción (ver la Proposición 2.4.2); también establecer su functorialidad y su independencia de las resoluciones proyectivas elegidas (ver la Proposición 2.4.2) así como su carácter de bifunctor (i.e. los functores $Tor_n^R(N, -)$ y los functores $Tor_n^R(-, N)$).
Consolidada la noción, estudiamos su comportamiento sobre diagramas conmutativos de sucesiones exactas cortas de R-módulos (Teorema 2.4.3) y que $Tor_0^R(M, N) \cong M \otimes_R N$. Probamos también la "conmutatividad" ($Tor_n^R(M, N) \cong Tor_n^R(N, M)$) en la Proposición 2.4.5 y su comportamiento con los R-módulos proyectivos.

La Sección 2.5 pretende hacer la misma tarea con los bifunctores $Ext_R^n(M, N)$. De nuevo, por las limitaciones de tamaño en la Normativa de la Facultad de Ciencias, hemos optado por dar un formato de "Resumen Extendido" a esta Sección. Pero dada la relevancia de los functores Ext en los Teoremas de Serre y Auslander-Buchsbaum, hemos preferido incluir una construcción detallada de estos bifunctores en la Sección B.2 del Apéndice B.

Los functores Ext toman, en lugar del producto tensorial, el bifunctor $Hom_R(-,-)$ como punto de partida. Así, tomamos dos R-módulos M y N y una resolución proyectiva $\underline{P}$ de M como la precedente y obtenemos un complejo de co-cadena:

$$Hom_R(\underline{P}, N): \ 0 \longrightarrow Hom_R(P_0, N) \longrightarrow Hom_R(P_1, N) \longrightarrow \cdots \longrightarrow Hom_R(P_n, N) \longrightarrow \cdots$$

Los módulos de co-homología serán los módulos Ext:

$$Ext^n_R(M, N) := H^n(Hom_R(\underline{P}, N)).$$

Ciertamente hay que probar la buena definición de esta noción (independencia de $\underline{P}$) y sus propiedades (que se analizan en el Lema B.2.1). Asimismo, el análisis de su carácter bifunctorial ($Ext^n_R(-, N)$ y $Ext^n_R(N, -)$) y la prueba de sus principales propiedades (resumidas en el Teorema 2.5.1) se incluyen en la Sección B.2 del Apéndice B.

La Sección 2.6 está dedicada a introducir la dimensión homológica y a caracterizarla mediante los functores Tor y Ext. Se define la *dimensión homológica* de un R-módulo M como el menor $n \in \mathbb{N}$ tal que existe una resolución proyectiva de longitud n, es decir, al mínimo de los $n \in \mathbb{N}$ tales que existe una sucesión de la forma:

$$\underline{P}: \ 0 \longrightarrow P_n \longrightarrow \cdots \longrightarrow P_0 \longrightarrow M \longrightarrow 0,$$

que es exacta y los P_i's son R-módulos proyectivos.
Por una parte, los R-módulos proyectivos tienen una sencilla caracterización mediante los functores Tor y Ext (véase Proposición 2.6.1 y 2.6.2). Resumiendo, se tiene:

PROPOSICIÓN 0.3.2. *Dado un $(R, \mathfrak{m})$ un anillo local noetheriano y P un R-módulo finitamente generado, las siguientes propiedades son equivalentes:*

i) *P es proyectivo.*
ii) *$Tor^R_n(P, N) = 0$, para todo R-módulo N y para todo $n \in \mathbb{N}$, $n \geq 1$.*
iii) *$Ext^n_R(P, N) = 0$, para todo R-módulo N y para todo $n \in \mathbb{N}$, $n \geq 1$.*

Así se puede caracterizar la dimensión homológica ($hd_R(M)$) de un R-módulo no nulo mediante (cf. Corolario 2.6.4):

$$hd_R(M) = sup\,\{n \in \mathbb{N} : \exists N \in R - \mathcal{M}od |\, Ext^n_R(M, N) \neq 0\}.$$

Técnicamente, podríamos trabajar solamente con los functores Tor^R_n y módulos proyectivos, pero surge una dificultad relevante en caso de $R-$módulos no finitamente generados. Esto se entiende mejor con la noción de *dimensión global.* En la Sección 2.7 se define la dimensión global de un anillo R mediante:

$$gl.dim(R) = sup\,\{hd_R(M) : \ M \in R - \mathcal{M}od\}.$$

Justamente usando los functores Ext^n_R y la noción (que trataremos como auxiliar) de dimensión inyectiva, la Proposición 2.7.4 permite redefinir la dimensión global mediante el uso de R-módulos finitamente generados. Es decir, se prueba que

$$gl.dim(R) = sup\,\{hd_R(M) : \ M \in R - \mathcal{M}od, \ M\ f.g.\}.$$

Así se produce el paso esencial previo a los Teoremas de Serre y Auslander-Buchsbaum, que se resume en el Corolario 2.7.6 y que reproducimos aquí:

COROLARIO 0.3.3. *Si $(R, \mathfrak{m})$ es un anillo local noetheriano y $k(\mathfrak{m}) = R/\mathfrak{m}$ es el cuerpo residual, entonces la dimensión global de R es la dimensión homológica de $k(\mathfrak{m})$ como R-módulo, esto es,*

$$gl.dim(R) = hd_R(k(\mathfrak{m})).$$

Así llegamos a la Sección 2.8 de la memoria, en la que se enuncia y demuestra el resultado clave del Teorema de Serre y Auslander-Buchsbaum y que reproducimos aquí:

TEOREMA. *Sea* $(R, \mathfrak{m})$ *un anillo local noetheriano. Entonces, R es un anillo local regular si y solamente si se da la siguiente igualdad:*

$$gl.dim(R) = hd_R(k(\mathfrak{m})) = dim_{Krull}(R) = dim_{HS}(R) = dim_{Chev}(R).$$

(En vista de la información que nos aporta El Teorema de la Dimensión Local sobre la dimensión de anillos locales noetherianos). Este importante resultado puede resumirse diciendo: *Un anillo local noetheriano* $(R, \mathfrak{m})$ *es local regular si y solamente si tiene dimensión homológica finita, en cuyo caso la dimensión global coincide con las otras nociones de dimensión de R utilizadas en el Teorema de la Dimensión Local.*

Como Buchsbaum explicó a Artin, disponiendo de este resultado es fácil demostrar que la condición de ser local regular es una propiedad local. Fue Serre quien se "adelantó" en [**Serre, 1955**]. Sin embargo, los tres estaban en la misma dirección de pensamiento (ver [**Auslander-Buchsbaum, 1957**]). Por eso lo tenemos asignado a Serre y lo demostramos también en la Sección 2.8:

TEOREMA (**Serre**). *Sea* $(R, \mathfrak{m})$ *un anillo local noetheriano. Son equivalentes:*

i) $(R, \mathfrak{m})$ *es un anillo local regular.*
ii) Para cada $\mathfrak{p} \in Spec(R)$*, el anillo* $(R_{\mathfrak{p}}, \mathfrak{p}R_{\mathfrak{p}})$ *es un anillo local regular.*

Con todos estos resultados, Auslander y Buchsbaum pueden finalmente responder a la cuestión de la factorialidad. Es lo que se hace en la Sección 2.9 y probando el siguiente resultado que reproducimos aquí:

TEOREMA (**Auslander-Buchsbaum**). *Si* $(R, \mathfrak{m})$ *es un anillo local regular, entonces es un dominio de factorización única.*

Para concluir, digamos que lo realmente revolucionario de este trabajo no es tanto los resultados en sí (versiones parciales eran conocidas por Nagata o Cohen, como ya se indicó), sino el tipo de herramientas para demostrarlos, que suponen una entrada poderosa para el Álgebra Homológica en el Álgebra Conmutativa.

0.4. Sobre el estilo y la ortografía usados en este TFG

En algún caso precedente se ha discutido el estilo y la ortografía de las memorias presentadas como Trabajo de Fin de Grado en Matemáticas. En evitación de intervenciones innecesarias, queremos clarificar algunos aspectos relativos al estilo elegido en este texto. Se ha elegido el formato de libro (book) de la American Mathematical Society (AMS). Aunque el idioma utilizado es el español, hemos tratado de seguir lo más fielmente posible las recomendaciones del Libro de Estilo de esta asociación [10] , juntamente con las reglas de estilo recomendadas por D. E. Knuth y co-autores para la Mathematical Association of America (MAA) [11].
Específicamente, hemos tratado de seguir atentamente las siguientes dos reglas:

- *"Numbered theorems, lemmas, etc. are proper nouns and, thus, are capitalized: Theorem 2.3, Lemma 3.1, Figure 4.5"* (p. 79 del AMS Style Guide).
- *"Rule 19. Capitalize names like Theorem 1, Lemma 2, Algorithm 3, Method 4"* (en D. E. Knuth et al.).

[10] M. Letourneau, J. Wright Sharp, AMS Style Guide, Journals, October 2017, AMS, Providence, 2017
[11] D. E. Knuth, T. Larrabee, P. M. Roberts, Mathematical Writing, MAA, 1989

CAPíTULO 1

Teorema de la Dimensión Local

Índice

1.1. Introducción

Este capítulo representa, dentro del cuerpo de la memoria, la componente más "clásica" de nuestra exposición. Como se indica en la Introducción, se trata de exponer una serie de resultados en la estela de la forma en la que E. Noether y E. Artin interpretaban el Álgebra Conmutativa, antes de la aparición de las elegantes técnicas homológicas (objetivo de la segunda parte de esta memoria). Tres son los resultados cuyas demostraciones deseábamos introducir aquí: el Lema de Artin-Rees, el Teorema de la Dimensión Local y el Teorema de la Intersección de Krull. El propósito último es el de dar la definición de anillos locales regulares y exponer algunas de sus propiedades elementales iniciales.

Por razones de limitación de espacio en los Trabajos Fin de Grado de la Facultad de Ciencias (límite de 50 páginas) hemos tenido que decidir qué puntos preservar, trasladando otros a los apéndices finales de la memoria. En este sentido, las Secciones 1.2 y 1.3 quedan redactadas en formato de "Resumen Extendido" (Extended Abstract). La Sección 1.2 se ha tomado de una combinación de [**Pardo, 21**] y [**Raghavan et al., 1975**] y el lector interesado puede acudir a esas fuentes para consultar las demostraciones. También por razones de espacio, hemos decidido usar el mismo formato para la Sección 1.3, pero, en este caso, hemos considerado la relevancia del Lema de Artin-Rees (y del Teorema de la Intersección de Krull) y hemos incluido las demostraciones de los principales resultados en la Sección A.11 del Apéndice A.

Las Secciones 1.4 y 1.5 se han preservado en la forma natural de exposición de textos matemáticos. Así, la Sección 1.4 prueba en detalle el Teorema de la Dimensión Local que, en esencia, demuestra la igualdad entre la diversas nociones de dimensión (concebidas por D. Hilbert-P.Samuel, W. Krull y C. Chevalley) en el caso de anillos locales noetherianos. La Sección 1.5 presenta los anillos locales regulares y describe sus primeras propiedades esenciales.

Para la elaboración de este capítulo se han seguido materiales de [**Pardo, 21**], [**Atiyah, 1969**] y [**Raghavan et al., 1975**].

1.2. Anillos y Módulos Graduados y Filtrados. Anillos y Módulos Topológicos (Resumen Extendido)

Con el propósito de respetar las limitaciones de tamaño de los Trabajos Fin de Grado de la Facultad de Ciencias, hemos optado por introducir esta sección solamente con las definiciones y resultados esenciales relativos a anillos y módulos graduados, filtrados o topológicos.

Definición 1. *Sea R un anillo. Una graduación sobre R es una descomposición de R en grupos abelianos $R = \bigoplus_{n\in\mathbb{N}} R_n$ de forma que $R_n R_m \subseteq R_{m+n}$ para todo $n, m \in \mathbb{N}$. Un anillo con una* *graduación se dice anillo graduado. R_n se denomina n-ésima componente de R y sus elementos no nulos se llaman elementos homogéneos de grado n.*

DEFINICIÓN 2. *Sea $R = \bigoplus_{n\in\mathbb{N}} R_n$ un anillo graduado y M un R-módulo. Una graduación sobre M es una descomposición de M en subgrupos $M = \bigoplus_{n\in\mathbb{N}} M_n$ de forma que $R_m M_n \subseteq M_{m+n}$. Un módulo con una graduación se dice módulo graduado.*

LEMA 1.2.1. *Sean $R = \bigoplus_{n\in\mathbb{N}} R_n$ un anillo graduado y $M = \bigoplus_{n\in\mathbb{N}} M_n$ un R-módulo graduado. Entonces, se tiene:*

i) R_0 es un subanillo de R, R es una R_0-álgebra y R_i es un R_0-módulo.
ii) Para cada $n \in \mathbb{N}$, M_n es un R_0-módulo.

DEFINICIÓN 3. *Sean M, N R-módulos graduados. Un morfismo de módulos graduados de grado r es un morfismo de R-módulos $f : M \longrightarrow N$ que verifica $f(M_n) \subseteq N_{n+r}$ para todo $n \in \mathbb{N}$. Si $r = 0$ se dice simplemente morfismo de módulos graduados.*

DEFINICIÓN 4. *Sea M un R-módulo graduado. Un submódulo N de M se dice graduado si se puede escribir como $N = \bigoplus_{n\in\mathbb{N}}(N \cap M_n)$*

LEMA 1.2.2. *Sea $R = \bigoplus_{n\in\mathbb{N}} R_n$ un anillo graduado y $M = \bigoplus_{n\in\mathbb{N}} M_n$ un R-módulo graduado. Definamos $N_n := \bigoplus_{m\geq n} M_m$. Entonces, N_n es un submódulo graduado de M.*

PROPOSICIÓN 1.2.3. *Sean $R = \bigoplus_{n\in\mathbb{N}} R_n$ y $M = \bigoplus_{n\in\mathbb{N}} M_n$ un anillo y R-módulo graduado respectivamente. Entonces,*

i) Si M es noetheriano, M_n es finitamente generado como R_0-módulo para cada $n \in \mathbb{N}$.
ii) Si R está generado por R_1 como R_0-álgebra, entonces R es noetheriano si y solamente si R_0 es noetheriano y R_n es finitamente generado como R_0-módulo para cada $n \in \mathbb{N}$.

DEFINICIÓN 5. *Sea R un anillo. Una filtración sobre R es una cadena descendente de ideales $\Sigma = \{R = \mathfrak{a}_0 \supseteq \mathfrak{a}_1 \supseteq ... \supseteq \mathfrak{a}_n \supseteq ...\}$ que verifica que $\mathfrak{a}_n\mathfrak{a}_m \subseteq \mathfrak{a}_{m+n}$ para todo $m, n \in \mathbb{N}$. Se dice que el par (R, Σ) es un anillo filtrado.*

DEFINICIÓN 6. *Sea (R, Σ) un anillo filtrado y M un R-módulo. Una filtración sobre M compatible con $\Sigma = \{\mathfrak{a}_n : n \in \mathbb{N}\}$ es una cadena descendente de submódulos de M: $\Sigma' = \{M = M_0 \supseteq M_1 \supseteq ... \supseteq M_n \supseteq ...\}$ tal que $\mathfrak{a}_n M_m \subset M_{n+m}$ para todo $n, m \in \mathbb{N}$. Si M es un R-módulo y Σ' es una filtración compatible con Σ, se dice que el par (M, Σ') es un R-módulo filtrado.*

A partir de este momento cuando se haga mención de un R-módulo filtrado (M, Σ'), se supondrá (R, Σ) filtrado tal que Σ' es compatible con Σ aunque no se especifique explícitamente.

OBSERVACIÓN 1. *Sea (M, Σ') un R-módulo filtrado y N un submódulo de M. Entonces Σ' induce un filtración en N compatible con Σ dada por $\Sigma'' = \{N = N_0 \supseteq N_1 \supseteq N_2 \supseteq ...\}$ donde $N_i = N \cap M_i$ para todo $i \in \mathbb{N}$. Basta notar que si $x \in \mathfrak{a}_n N_m$, $x \in \mathfrak{a}_n M_m \subset M_{n+m}$ y $x \in N$. Por tanto, $x \in N \cap M_{n+m} = N_{n+m}$.*

Dado un anillo R y una filtración $\Sigma = \{\mathfrak{a}_0 \supseteq ... \supseteq \mathfrak{a}_n \supseteq ...\}$ sobre R se puede definir el conjunto $G_\Sigma(R) := \oplus_{n\in\mathbb{N}}(\mathfrak{a}_n/\mathfrak{a}_{n+1})$ al que se le puede dar estructura de anillo graduado con las operaciones inducidas por el producto y la suma en R. Sean $a, b \in G_\Sigma(R)$, entonces existen conjuntos finitos $\{a_i \in \mathfrak{a}_i/\mathfrak{a}_{i+1} : i \in I\}$, $\{b_j \in \mathfrak{a}_j/\mathfrak{a}_{j+1} : j \in J\}$ y conjuntos finitos $I, J \subseteq \mathbb{N}$ de tal forma que

$$a = \sum_{i\in I}(a_i + \mathfrak{a}_{i+1}), \;\; b = \sum_{j\in J}(b_j + \mathfrak{a}_{j+1}).$$

Ahora, consideramos el conjunto $I \cup J$, que es finito por serlo I y J. Tomando $a_k = 0$ si $k \notin I$ y $b_k = 0$ si $k \notin J$ definimos la suma de elementos de la siguiente manera:

$$a + b := \sum_{k\in I\cup J}((a_k + b_k) + \mathfrak{a}_{k+1}),$$

que es una suma finita por ser $I \cup J$ finito y donde el elemento $(a_k + b_k) + \mathfrak{a}_{k+1}$ es claramente homogéneo de grado k. Por otra parte, definimos el producto de la siguiente manera:

$$a \cdot b := \sum_{i\in I, j\in J}(a_i + \mathfrak{a}_{i+1}) \cdot (b_j + \mathfrak{a}_{j+1}),$$

que es una suma finita porque I y J son conjuntos finitos, y donde para cada $n, m \in \mathbb{N}$ el producto de elementos homogéneos viene dado por:

$$\begin{array}{ccc} \mathfrak{a}_n/\mathfrak{a}_{n+1} \times \mathfrak{a}_m/\mathfrak{a}_{m+1} & \longrightarrow & \mathfrak{a}_{n+m}/\mathfrak{a}_{n+m+1} \\ (a_n + \mathfrak{a}_{n+1}, b_m + \mathfrak{a}_{m+1}) & \longmapsto & a_n b_m + \mathfrak{a}_{n+m+1}. \end{array}$$

Veamos que está bien definido comprobando que el resultado de operar dos elementos homogéneos no depende de los representantes elegidos: si $a_n - a'_n \in \mathfrak{a}_{n+1}$ y $b_m - b'_m \in \mathfrak{a}_{m+1}$, entonces $a_n(b_m - b'_m) + b'_m(a_n - a'_n) = a_n b_m - a'_n b'_m \in \mathfrak{a}_{n+m+1}$.

Definición 7 (**Anillo graduado asociado a una filtración**). *Con las notaciones y definiciones precedentes, el anillo $G_\Sigma(R)$ se denomina el anillo graduado asociado a la filtración Σ sobre R.*

Dado R un anillo, $\Sigma = \{R = \mathfrak{a}_0 \supseteq \cdots \supseteq \mathfrak{a}_n \supseteq \dots\}$ una filtración sobre R, $G_\Sigma(R)$ el anillo graduado asociado a la filtración Σ sobre R y (M, Σ') un R-módulo con una filtración $\Sigma' = \{M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n \supseteq \dots\}$ compatible con Σ. Se puede construir el $G_\Sigma(R)$-módulo graduado $G_{\Sigma'}(M) := \oplus_{n\in\mathbb{N}}(M_n/M_{n+1})$. Sean $x, y \in G_{\Sigma'}(M)$, entonces existen conjuntos finitos $\{x_i \in M_i/M_{i+1} : i \in I\}$ y $\{y_j \in M_j/M_{j+1} : j \in J\}$ de tal modo que $I, J \subseteq \mathbb{N}$ son conjuntos finitos y

$$x = \sum_{i\in I}(x_i + M_{i+1}), \;\; y = \sum_{j\in J}(y_j + M_{j+1}).$$

Tomando $x_k = 0$ si $k \notin I$ e $y_j = 0$ si $j \notin J$, definimos la suma de elementos de la siguiente manera:

$$x + y = \sum_{k\in I\cup J}((x_k + y_k) + M_{k+1}),$$

que es una suma finita por ser $I \cup J$ un conjunto finito. Por otra parte, dados $a \in G_\Sigma(R)$ e $y \in G_{\Sigma'}(M)$, existen conjuntos finitos $\{a_i \in \mathfrak{a}_i/\mathfrak{a}_{i+1} : i \in I\}$ $\{y_j \in M_j/M_{j+1} : j \in J\}$ de tal modo que $I, J \subseteq \mathbb{N}$ son conjuntos finitos y

$$a = \sum_{i\in I}(a_i + \mathfrak{a}_{i+1}), \;\; y = \sum_{j\in J}(y_j + M_{j+1}).$$

Definimos el producto de la siguiente manera:

$$a \cdot y = \sum_{i\in I, j\in J}(a_i + \mathfrak{a}_{i+1}) \cdot (y_j + M_{j+1}),$$

que es una suma finita por ser I y J conjuntos finitos y donde para cada $m, n \in \mathbb{N}$ el producto de elementos homogéneos viene dado por

$$\begin{array}{ccc} \mathfrak{a}_n/\mathfrak{a}_{n+1} \times M_m/M_{m+1} & \longrightarrow & M_{n+m}/M_{n+m+1} \\ (a_n + \mathfrak{a}_{n+1}, y_m + M_{m+1}) & \longmapsto & a_n y_m + M_{n+m+1}. \end{array}$$

Por una parte, como Σ' es compatible con Σ se tiene que $\mathfrak{a}_n.M_m \subseteq M_{m+n}$ para todo $n \in N$. Por otra parte, si $a_n - a'_n \in \mathfrak{a}_{n+1}$ e $y_m - y'_m \in \mathbb{M}_{m+1}$, entonces $a_n(y_m - y'_m) + y'_m(a_n - a'_n) = a_n y_m - a'_n y'_m \in \mathbb{M}_{n+m+1}$, con lo que queda probada la buena definición del producto.

Definición 8 (**Módulo graduado asociado a una filtración**). *Con las notaciones y definiciones precedentes, el $G_\Sigma(R)$-módulo $G_{\Sigma'}(M)$ se denomina módulo graduado asociado a la filtración Σ' sobre M.*

Un ejemplo relevante de filtraciones son aquellas definidas por las potencias un ideal $\mathfrak{a}$ de R.

Definición 9. *Sea R un anillo, M un R-módulo y $\mathfrak{a}$ un ideal de R. Se denominan filtraciones $\mathfrak{a}$-ádicas a aquellas definidas por los conjuntos*

$$\Sigma_\mathfrak{a}(R) := \{R = \mathfrak{a}^0 \supseteq \mathfrak{a}^1 \supseteq ...\}, \qquad \Sigma_\mathfrak{a}(M) := \{M = \mathfrak{a}^0 M \supseteq \mathfrak{a}^1 M \supseteq ...\}$$

Definición 10. *Sea R un anillo, M un R-módulo y $\mathfrak{a}$ un ideal de R. Se llama anillo graduado asociado a la filtración $\mathfrak{a}$-ádica en R, $G_\mathfrak{a}(R)$ y $G_\mathfrak{a}(R)$-módulo asociado a la filtración $\mathfrak{a}$-ádica en M, $G_\mathfrak{a}(M)$ a los siguientes módulo y anillo graduados:*

$$G_\mathfrak{a}(R) := \bigoplus_{n\in\mathbb{N}}(\mathfrak{a}^n/\mathfrak{a}^{n+1}), \qquad G_\mathfrak{a}(M) := \bigoplus_{n\in\mathbb{N}}(\mathfrak{a}^n M/\mathfrak{a}^{n+1}M).$$

Definición 11. *Un anillo topológico R es un anillo R dotado de una topología $\mathscr{T}$ de forma que las aplicaciones*

i) $- : R \times R \longrightarrow R,\ -(a, b) = a - b,\ \forall a, b \in R,$
ii) $\cdot : R \times R \longrightarrow R,\ \cdot(a, b) = ab,\ \forall a, b \in R,$

sean continuas considerando la topología producto en $R \times R$.

Definición 12. *Sea* $(R, \mathscr{T})$ *un anillo topológico,* M *un* $(R, \mathscr{T})$*-módulo y* $\mathscr{T}'$ *una topología sobre* M. *Se dice que* $(M, \mathscr{T}')$ *es un* R*-módulo topológico si las aplicaciones*

i) $- : M \times M \longrightarrow M,\ -(x, y) = x - y,\ \forall x, y \in M,$

ii) $\cdot : R \times M \longrightarrow R,\ \cdot(a, x) = a \cdot_R x,\ \forall a \in R,\ \forall x \in M,$

son continuas. Donde en $M \times M$ *consideramos la topología producto inducida por* $\mathscr{T}'$ *y en* $R \times M$ *consideramos la topología producto inducida por* $\mathscr{T}$ *en* R *y* $\mathscr{T}'$ *en* M.

Observación 2. *Cada anillo topológico* $(R, \mathscr{T})$ *puede verse como un* $(R, \mathscr{T})$*-módulo topológico.*

Proposición 1.2.4. *Sean* $(R, \mathscr{T})$ *y* $(M, \mathscr{T}')$ *un anillo y* $(R, \mathscr{T})$*-módulo topológico respectivamente. Para cada* $a \in R$ *y* $x \in M$ *se tiene:*

i) $t_a : R \longrightarrow R,\ t_a(b) = a + b$

ii) $t_x : M \longrightarrow M,\ t_x(y) = x + y$

son homeomorfismos.

Lema 1.2.5. *Sean* $(R, \mathscr{T})$ *un anillo topológico y* $(M, \mathscr{T}')$ *un* $(R, \mathscr{T})$*-módulo topológico,* $x \in M$ *y* V_x *un entorno de* x. *Entonces, si* $f : M \longrightarrow M$ *es una aplicación continua,* $f^{-1}(V_x)$ *es entorno de* $f^{-1}(x)$. *Más aún, si* f *es homeomorfismo se verifica, además, que* $f(V_x)$ *es entorno de* $f(x)$.

Proposición 1.2.6. *Sean* $(R, \mathscr{T})$ *un anillo topológico y* $(M, \mathscr{T}')$ *un* $(R, \mathscr{T})$*-módulo topológico. Sea* Σ' *una base de entornos de* 0 *en* M. *Entonces, para cada* $x \in M$, *la siguiente es una base de entornos de* x: $\Sigma'(x) := t_x(\Sigma') = \{t_x(V) : V \in \Sigma'\} = \{x + V : V \in \Sigma'\}$.

Corolario 1.2.7. *Sea* $(R, \mathscr{T})$ *un anillo topológico y* $(M, \mathscr{T}')$ *un* $(R, \mathscr{T})-$*módulo topológico. La topología* $\mathscr{T}'$ *sobre* M *está unívocamente determinada por una base de entornos del* $0 \in M$.

Observación 3. *En vista de la Observación 2, la propiedad descrita en el Corolario 1.2.7 también se cumple para cualquier anillo topológico* $(R, \mathscr{T})$.

Lema 1.2.8. *Sea* $(R, \mathscr{T})$ *un anillo topológico y* $(M, \mathscr{T}')$ *un* $(R, \mathscr{T})$*-módulo topológico con respecto a la topología* $\mathscr{T}$ *de* R *y* Σ' *una base de entornos de* 0. *Entonces, la clausura de un átomo coincide con la intersección de todos los entornos del punto que define dicho conjunto. Es decir, para todo* $x \in M$ *se tiene:* $\bigcap_{t_x(V) \in \Sigma'(x)} t_x(V) = \overline{\{x\}}$.

Proposición 1.2.9. *Sea* $R, \mathscr{T}$ *un anillo topológico y* $(M, \mathscr{T}')$ *un* $(R, \mathscr{T})$*-módulo topológico con respecto a la topología* $\mathscr{T}$ *de* R. *Las siguientes afirmaciones son equivalentes:*

i) $(M, \mathscr{T}')$ *es Hausdorff*

ii) El conjunto $\{0\}$ *es cerrado*

iii) Si Σ' *es una base de entornos de* 0, *se verifica:* $\bigcap_{V \in \Sigma'} V = \{0\}$.

Sea R un anillo y sea $\Sigma = \{R = \mathfrak{a}_0 \supseteq \mathfrak{a}_1 \supseteq \cdots \supseteq \mathfrak{a}_n \supseteq \dots\}$ una filtración. Definamos el conjunto $\mathscr{T}$ de subconjuntos de R mediante la siguiente propiedad: Para cada $A \subseteq R, A \in \mathscr{T}$ si y solamente si se verifica la siguiente propiedad: $\forall a \in A,\ \exists n \in \mathbb{N} :\ a + \mathfrak{a}_n \subseteq A$.

Proposición 1.2.10. *Con las notaciones precedentes, si* R *es un anillo y* Σ *es una filtración sobre* R, $\mathscr{T}$ *es una topología sobre* R *que hace que* $(R, \mathscr{T})$ *sea un anillo topológico. Además,* $\mathscr{T}$ *es la única topología sobre* R *que tiene a* Σ *como base de entornos de* $0 \in R$ *y tal que* $(R, \mathscr{T})$ *es anillo topológico.*

Supongamos ahora R un anillo con una filtración $\Sigma = \{\mathfrak{a}_0 \supseteq \mathfrak{a}_1 \supseteq \dots\}$ y sea $\mathscr{T}$ la única topología sobre R, existente conforme a la Proposición 1.2.10 precedente. Sea M un R-módulo y $\Sigma' = \{M_0 \supseteq M_1 \supseteq \dots\}$ una filtración sobre M compatible con Σ.
Definimos un conjunto $\mathscr{T}'$ de subconjuntos de M dados por la siguiente propiedad: Para cada $A \subseteq M$, $A \in \mathscr{T}'$ si y solamente si

$$\forall x \in A,\ \exists n \in \mathbb{N} :\ x + M_n \subseteq A.$$

Proposición 1.2.11. *Con las notaciones precedentes,* $(M, \mathscr{T}')$ *es un* $(R\mathscr{T})-$*módulo topológico donde* σ' *es una base de entornos del* $0 \in M$.

PROPOSICIÓN 1.2.12. *Sea R un anillo, M un R-módulo y $\mathfrak{a} \subseteq R$ un ideal de R. Sean $\Sigma_{\mathfrak{a}}(R)$ y $\Sigma_{\mathfrak{a}}(M)$ respectivamente las filtraciones $\mathfrak{a}$-ádicas en R y M. Sean $\mathscr{T}$ y $\mathscr{T}'$ respectivamente las topologías inducidas por $\Sigma_{\mathfrak{a}}(R)$ en R y $\Sigma_{\mathfrak{a}}(M)$ en M. Se verifica:*

i) La topología $\mathscr{T}$ en R es metrizable si y solamente si se verifica $\bigcap_{n\in N} \mathfrak{a}^n = \{0\}$.
ii) La topología $\mathscr{T}'$ en M es metrizable si y solamente si se verifica $\bigcap_{n\in \mathbb{N}} \mathfrak{a}^n M = \{0\}$.

Obsérvese que, en virtud de la Proposición 1.2.9, esto significa que las topologías inducidas por las filtraciones $\mathfrak{a}$-ádicas son metrizables si y solamente si los anillos o módulos topológicos correspondientes son espacios de Hausdorff.

1.3. Lema de Artin-Rees. Teorema de la intersección de Krull (Resumen Extendido)

Como ya indicamos en la Introducción, esta Sección presenta el Lema de Artin-Rees y el Teorema de la Intersección de Krull en formato "Resumen Extendido". Las demostraciones de todos los enunciados que se exponen se encuentran en la Sección A.11 del Apéndice A.

DEFINICIÓN 13. *Sean (R, Σ) y (M, Σ') anillo y R-módulo filtrado respectivamente. Dado un ideal $\mathfrak{a} \in R$ se dice que una filtración Σ' es compatible con $\mathfrak{a}$ si $\mathfrak{a}M^n \subseteq M^{n+1}$ para todo $n \in \mathbb{N}$. Se dice que la filtración Σ' es $\mathfrak{a}$-estable si existe $n_0 \in \mathbb{N}$ tal que $\mathfrak{a}M^m = M^{m+1}$ para todo $m \geq n_0$.*

OBSERVACIÓN 4. *Sea R es un anillo, $\mathfrak{a} \subset R$ un ideal, M un R-módulo y N un submódulo de M. Entonces,*

i) Si una filtración Σ' sobre M es compatible con $\mathfrak{a}$ se tiene, en virtud de la Observación 1, que la filtración Σ'' inducida en N por Σ' es también compatible con $\mathfrak{a}$.
ii) La filtración $\mathfrak{a}$-ádica sobre M es un claro ejemplo de filtración $\mathfrak{a}$-estable.

Dados un anillo R y un ideal $\mathfrak{a} \subset R$, se puede definir el conjunto $\overline{R} := R \oplus \mathfrak{a} \oplus \mathfrak{a}^2 \oplus \ldots$ al que se puede dotar de estructura de anillo graduado mediante las operaciones que inducen la suma y el producto de R. Dados $a, b \in \overline{R}$, existen conjuntos finitos $I, J \subseteq \mathbb{N}$ y conjuntos finitos de elementos homogéneos $\{a_i \in \mathfrak{a}^i : i \in I\}$, $\{b_j \in \mathfrak{a}^j : j \in J\}$ tales que:

$$a = \sum_{i\in I} a_i, \quad b = \sum_{j \in J} b_j.$$

Ahora, consideramos el conjunto $I \cup J$. Añadiendo $a_k = 0$ para $k \in I \cup J \setminus I$ y $b_k = 0$ para $k \in I \cup J \setminus J$, dado que $I \cup J$ es finito, podemos definir la suma de a y b mediante la siguiente identidad:

$$a + b := \sum_{k \in I \cup J} (a_k + b_k),$$

Dado que $\overline{R}$ es suma directa de subgrupos $\{\mathfrak{a}^i : i \in \mathbb{N}\}$, esta definición es única y $a_k + b_k \in \mathfrak{a}^k$ es claramente un elemento homogéneo de grado k en $\overline{R}$. De modo similar, usando las mismas presentaciones de a y b podemos definir el producto:

$$a \cdot b := \sum_{i \in I, j \in J} a_i \cdot b_j.$$

De nuevo, la naturaleza de $\overline{R}$ como suma directa de sus subgrupos nos garantiza la buena definición del producto, donde el producto natural $\mathfrak{a}^n \times \mathfrak{a}^m \longrightarrow \mathfrak{a}^{m+n}$, nos indica que $a_i \cdot b_j$ es un elemento homogéneo de grado $i + j$ de $\overline{R}$.
De manera similar, consideremos un anillo R un ideal $\mathfrak{a} \subseteq R$ y un R-módulo M. Como en la definición, consideremos el anillo $\overline{R} = R \oplus \mathfrak{a} \oplus \cdots$ y el grupo abeliano $\overline{M} := M \oplus \mathfrak{a}M \oplus \mathfrak{a}^2 M \cdots$ Sobre M podemos, de manera natural, inducir una estructura de $\overline{R}$-módulo, mediante la siguiente operación:

$$(\sum_{i\in I} a_i) \cdot (\sum_{j \in J} m_j) := \sum_{i,j} a_i \cdot m_j, \qquad a_i \in \mathfrak{a}^i,\ m_j \in \mathfrak{a}^i M,$$

siendo los argumentos elementales los esperados.

LEMA 1.3.1. *Sea $\mathfrak{a}$ un ideal de R, M un R-módulo con una filtración $\Sigma' = \{M_0 \supseteq M_1 \supseteq ...\}$ compatible con $\mathfrak{a}$. Entonces, $\overline{M}$ es finitamente generado como $\overline{R}$-módulo si y solamente sí Σ' es $\mathfrak{a}$-estable.*

Seguidamente enunciamos un resultado técnico de gran utilidad, encontrado, al menos por E. Artin y D. Rees.

TEOREMA 1.3.2 (**Lema de Artin-Rees**). *Sea R un anillo noetheriano, $\mathfrak{a}$ un ideal de R, M un R-módulo finitamente generado y N un submódulo de M. Entonces, dada una filtración $\mathfrak{a}$-estable Σ' sobre M, la filtración $\Sigma'' = \{N \cap M_n : n \in \mathbb{N}\}$ inducida sobre N es $\mathfrak{a}$-estable.*

COROLARIO 1.3.3. *Sean R un anillo noetheriano, $\mathfrak{a}$ ideal de R, M un R-módulo finitamente generado y N un submódulo de M. Entonces existe $n \in \mathbb{N}$ tal que $\mathfrak{a}(\mathfrak{a}^m M \cap N) = \mathfrak{a}^{m+1} M \cap N$ para todo $m \geq n$.*

A continuación presentamos un enunciado del clásico Teorema de la Intersección de Krull de W. Krull que, entre otras cosas, establece que la topología $\mathfrak{a}$-ádica es metrizable en el caso de los módulos finitamente generados sobre anillos noetherianos.

TEOREMA 1.3.4 (**Teorema de la Intersección de Krull**). *Sean R un anillo noetheriano, $\mathfrak{a}$ un ideal de R y M un R-módulo finitamente generado. Entonces,*

i) Si $N := \bigcap_{n \in \mathbb{N}} \mathfrak{a}^n M$, $\mathfrak{a}N = N$.

ii) Si $\mathfrak{a}$ está contenido en el radical de Jacobson de R,

$$\bigcap_{n \in \mathbb{N}} \mathfrak{a}^n M = (0)$$

y la topología definida por la filtración $\mathfrak{a}$-ádica sobre M es Hausdorff y metrizable.

iii) Si R es dominio noetheriano, para cada ideal propio $\mathfrak{a}$ de R se tiene:

$$\bigcap_{n \in \mathbb{N}} \mathfrak{a}^n = (0)$$

y la topología $\mathfrak{a}$-ádica sobre R es Hausdorff y metrizable.

COROLARIO 1.3.5. *Sea R es un anillo noetheriano y $\mathfrak{a}$ es un ideal de R contenido en el radical de Jacobson. Entonces, si el anillo graduado $G_{\mathfrak{a}}(R)$ asociado a la filtración $\mathfrak{a}$-ádica sobre R es dominio, también lo es R.*

1.4. Teorema de la Dimensión Local

DEFINICIÓN 14. *Sea $f : \mathbb{N} \longrightarrow \mathbb{Q}$ una aplicación. Se dice que f es polinomial si existe $n_0 \in \mathbb{N}$ y $q \in \mathbb{Q}[X]$ tal que $f(n) = q(n)$ para todo $n \geq n_0$.*

OBSERVACIÓN 5. *Para cada aplicación polinomial f existe un único polinomio coincidente con ella (salvo un número finito de puntos). La razón es que dos polinomios en $\mathbb{Q}[X]$ que coincidan en un número infinito de puntos tienen que ser el mismo polinomio. Por eso, se denomina grado de una función polinomial al grado de su único polinomio asociado. Del mismo modo, se habla del coeficiente director de una función polinomial como el coeficiente director de su polinomio asociado.*

Ahora, para una aplicación $f : \mathbb{N} \longrightarrow \mathbb{Q}$ se definen las aplicaciones incremento como:

$$\Delta^0(f)(n) := f(n)$$
$$\Delta^r(f)(n) := \Delta^{r-1}(n+1) - \Delta^{r-1}(n)$$

LEMA 1.4.1. *Sea $r \in \mathbb{N}$. Una aplicación $f : \mathbb{N} \longrightarrow \mathbb{Q}$ es polinomial de grado r si y solamente si Δf es una aplicación polinomial de grado $r - 1$.*

DEMOSTRACIÓN. Por una parte, sea $g = \sum_{0 \leq i \leq r} a_i X^i$ el polinomio asociado a f. Entonces, el polinomio asociado a Δf viene dado por $q'[X] = q[X+1] - q[X]$. Esto es, $q'[X] = \sum_{0 \leq i \leq r} a_i((X+1)^i - X^i)$. En virtud del binomio de Newton, $q'[X] = ra_r X^{r-1} + h(X)$ con $deg(h) \leq r - 2$. Y el grado de $q[X]$ es $r - 1$.
Por otra parte, sea Δf es una aplicación polinomial de grado $r-1$ y sea h su polinomio asociado. Veamos que f es polinomial de grado r por inducción en el grado de h:

- Si $deg(h) = 0$, $\Delta f(n) = f(n+1) - f(n) = c$ para $n \geq n_0$, $c \in \mathbb{Q}$. Esto es, $f(n) = c(n - n_0) + f(n_0)$ para $n \geq n_0$. Por tanto f es polinomial de grado 1.
- Supongamos cierto para $deg(h) = r-1$. Sea $h = \sum_{0 \leq i \leq r} a_i X^i$. En virtud del binomio de Newton, $\Delta f = \frac{a_r}{r+1}\{(n+1)^{r+1} - n^{r+1} + g(n)\}$ con $deg(g) \leq r-1$. Ahora se define la aplicación
$$f^*(n) := f(n) - \frac{a_r}{r+1} n^{r+1}$$
y se tiene, por construcción, que $\Delta f^* = g(n)$. Aplicando hipótesis inductiva, f^* es una función polinomial de grado menor o igual a r. Ahora, $f(n) = f^*(n) + \frac{a_r}{r+1} n^{r+1}$ y se tiene que f es polinomial de grado $r+1$.

□

LEMA 1.4.2. *La aplicación $f : \mathbb{N} \longrightarrow \mathbb{N}$ definida por $f(n) := \binom{n+r}{r}$ es una aplicación polinomial de grado r.*

DEMOSTRACIÓN. Obvia por inducción en r. □

Observemos que $\binom{n+r-1}{r-1}$ es la dimensión del espacio vectorial H_n formado por los polinomios homogéneos de grado n en r variables. Por esta razón, el Lema 1.4.2 será de gran utilidad en la prueba de la Proposición 1.4.10 y, posteriormente, en la Proposición 1.5.3.
Ahora, fijemos unas condiciones que aparecerán reiteradamente a lo largo del resto del capítulo:

- Sea $R = \oplus_{n \in \mathbb{N}} R_n$ un anillo graduado con R_0 artiniano de forma que R esté generado como R_0-álgebra por $\{x_1, \ldots, x_r\} \subset R_1$. Entonces, por el Teorema de la Base de Hilbert (ver Teorema A.8.6), se tiene que R es noetheriano.
- Sea $M = \oplus_{n \in \mathbb{N}} M_n$ un R-módulo graduado finitamente generado. Por el Corolario A.8.5 se tiene que M es noetheriano. Y, en virtud de la Proposición 1.2.3, M_n es finitamente generado como R_0-módulo para todo $n \in \mathbb{N}$. Ahora, por el Corolario A.9.2, se tiene que M_n es artiniano para todo $n \in \mathbb{N}$. Finalmente, en vista del Corolario A.10.16, M_n es de longitud finita y tiene sentido considerar $\ell_{R_0}(M_n)$.

PROPOSICIÓN 1.4.3. *Con las notaciones precedentes, supongamos $\{x_1, \ldots, x_r\}$ un conjunto de elementos que generan R_1 como R_0-módulo. Entonces, la siguiente función $\chi(M, -)$ es una función polinomial de grado menor o igual que $r-1$:*
$$\begin{array}{rccc} \chi(M,-): & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & n & \longmapsto & \chi(M,n) := \ell_{R_0}(M_n). \end{array}$$
A esta función polinomial se la denomina función de Hilbert del R-módulo graduado M.

DEMOSTRACIÓN. La Proposición se prueba por inducción en r:
Para $r = 0$ se tiene que $R = R_0$. Sea S el conjunto finito de generadores homogéneos de M y sea $n_0 = max_{s \in S}\{deg(s)\}$. Entonces cualquier elemento de M tiene como máximo grado n_0 y $M_n = 0$ para todo $n \geq n_0$ y $\chi(M,n) = \ell_{R_0}(M_n) = 0$ para todo $n \geq n_0$, que es de grado -1.
Supuesto cierto para $r-1$, se considera la aplicación:
$$\begin{array}{rccc} \eta_{x_r}: & M & \longrightarrow & M \\ & m & \longmapsto & x_r m. \end{array}$$
Como $x_r \in R_1$ y $x_r M_n \subseteq M_{n+1}$, puede considerarse la restricción $\varphi_n := \eta_{x_r}|_{M_n}$. Estas aplicaciones ayudan a definir para cada $n \in \mathbb{N}$ una sucesión exacta
$$0 \longrightarrow K_n \xrightarrow{i} M_n \xrightarrow{\varphi_n} M_{n+1} \longrightarrow C_{n+1},$$
donde $K_n := ker(\varphi_n)$ y $C_n := M_{n+1}/im\varphi_n$. Ahora consideramos los submódulos graduados de M:
$$K = \bigoplus_{n \in \mathbb{N}} K_n = \bigoplus_{n \in \mathbb{N}} (M_n \cap K); \;\; C = \bigoplus_{n \geq -1} C_n = \bigoplus_{n \geq -1} (M_n \cap C),$$
que son noetherianos porque M lo es, y que tienen estructura de R'-módulo donde $R' = R/(x_r) = R[x_1, \ldots x_r]/(x_r) = R[x_1, \ldots, x_{r-1}]$. Además, como $x_r \in Ann_R(K); x_r \in Ann_R(C)$, sus estructuras como R-módulos y R'-módulos coinciden. En consecuencia, las aplicaciones $\chi(C,-)$ y $\chi(K,-)$ verifican las hipótesis anteriores a la Proposición y, por hipótesis inductiva, son aplicaciones polinomiales de grado menor o igual a $r-2$. Ahora, en virtud del Corolario A.9.9, se tiene que $\ell_{R_0}(K_n) - \ell_{R_0}(M_n) + \ell_{R_0}(M_{n+1}) - \ell_{R_0}(C_{n+1}) = 0$. Esto es, $\Delta\chi(M,n) =$

$\chi(C, n+1) - \chi(K, n)$ y en consecuencia $\Delta\chi(M, -)$ es una aplicación polinomial de grado a lo sumo $r-2$. Finalmente, por el Lema 1.4.1, $\chi(M, -)$ es una aplicación polinomial de grado a lo sumo $r-1$. □

Definición 15. *Con las notaciones precedentes, al polinomio en $\mathbb{Q}[T]$ asociado a la función polinomial $\chi(M, -)$ se se le denomina polinomio de Hilbert de M y se denota también mediante $\chi(M, -)$ cuando no lleve a confusión.*

Definición 16. *Sea $(R, \mathfrak{m})$ un anillo local noetheriano, un ideal $\mathfrak{q}$ de R se denomina ideal de definición de R si existe $n \in \mathbb{N}$ tal que $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$.*

Proposición 1.4.4. *Sea $(R, \mathfrak{m})$ un anillo local noetheriano, $\mathfrak{q}$ un ideal de definición de R y M un R-módulo finitamente generado. Las funciones $\chi(G_{\mathfrak{q}}(R), -)$ y $\chi(G_{\mathfrak{q}}(M), -)$ son polinomiales de grado a lo sumo $r-1$ donde r es el mínimo de los cardinales de los subconjuntos que generan $\mathfrak{q}$ como ideal de R.*

Demostración. $(G_{\mathfrak{q}}(R), -)$ es un anillo graduado con $R_0 = R/\mathfrak{q}$. Además, como R es anillo local de maximal $\mathfrak{m}$, $R/\mathfrak{q}$ es local de maximal $\mathfrak{m}/\mathfrak{q}$. Por otra parte si $\mathfrak{a}$ es un ideal primo de $R/\mathfrak{q}$, entonces existe $\mathfrak{p} \in Spec(R)$ tal que $\mathfrak{a} = R/\mathfrak{p}$ y $\mathfrak{p} \supseteq \mathfrak{q}$. Ahora como $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{p} \subseteq \mathfrak{m}$ tenemos que $\mathfrak{p}$ es un ideal primo que contiene a $\mathfrak{m}^n$. Luego, por ser $\mathfrak{m}$ maximal, se tiene: $\mathfrak{m} = \sqrt{\mathfrak{m}^n} \subseteq \sqrt{\mathfrak{p}} = \mathfrak{p} \subseteq \mathfrak{m}$, Es decir, $\mathfrak{m} = \mathfrak{p}$, y el único ideal primo de $R/\mathfrak{q}$ es $\mathfrak{m}/\mathfrak{q}$, con lo que $Spec(R/\mathfrak{q}) = MaxSpec(R/\mathfrak{q}) = \{\mathfrak{m}/\mathfrak{q}\}$. En particular, $R/\mathfrak{q}$ es un anillo artiniano (ver el Teorema de Akizuki en el Teorema A.10.14). De otro lado, como R es noetheriano, $\mathfrak{q}$ es un ideal finitamente generado. Más aún, si $\{x_1, \ldots, x_r\}$ generan $\mathfrak{q}$ como ideal de R, sus clases módulo $\mathfrak{q}^2$ generan $\mathfrak{q}/\mathfrak{q}^2$ como $R/\mathfrak{q}$-módulo. Es decir,

$$\mathfrak{q}/\mathfrak{q}^2 = R/\mathfrak{q} < \{x_1, \ldots x_r\} >,$$

como $R/\mathfrak{q}$-módulo. Finalmente, $G_{\mathfrak{q}}(R)$ es una $\mathfrak{q}$-álgebra generada por los elementos homogéneos de grado 1, es decir por los elementos de $\mathfrak{q}/\mathfrak{q}^2$. Ahora, observamos que tenemos un epimorfismo natural de $R/\mathfrak{q}$-módulos:

$$\begin{array}{ccc} \mathfrak{q}^n/\mathfrak{q}^{n+1} \times M/\mathfrak{q}M & \longrightarrow & \mathfrak{q}^n M/\mathfrak{q}^{n+1}M \\ (\lambda + \mathfrak{q}^{n+1}, x + \mathfrak{q}M) & \longmapsto & \lambda.x + \mathfrak{q}^{n+1}M. \end{array}$$

Por tanto, $M/\mathfrak{q}M = R/\mathfrak{q} \otimes_R M$ genera $G_{\mathfrak{q}}(R)$ como $G_{\mathfrak{q}}(R)$-módulo. Además, $M/\mathfrak{q}M$ es finitamente generado como $R/\mathfrak{q}$-módulo. Como $R/\mathfrak{q}$ es un anillo artiniano, $\mathfrak{q}^n M/\mathfrak{q}^{n+1}M$ es un $R/\mathfrak{q}$-módulo artiniano (ver Corolario A.9.2).
En suma, tenemos las hipótesis de la Proposición 1.4.3 y podemos concluir que

- El polinomio de Hilbert de $G_{\mathfrak{q}}(R)$ tiene grado a lo sumo $r-1$.
- El polinomio de Hilbert de $G_{\mathfrak{q}}(M)$ tiene grado a lo sumo $r-1$.

□

Observación 6. *En las condiciones de la Proposición anterior, el soporte verifica $Supp(M/\mathfrak{q}^n M) = \{\mathfrak{m}\}$. La prueba es idéntica al argumento seguido en la Proposición 1.4.4. Además, en virtud de la Proposición A.10.13, se tiene que $M/\mathfrak{q}^n M$ es de longitud finita.*

Teorema 1.4.5. *Sea $(R, \mathfrak{m})$ un anillo local noetheriano, M un R-módulo finitamente generado y $\mathfrak{q}$ un ideal de definición de R. Definamos la siguiente función:*

$$\begin{array}{cccc} P_{\mathfrak{q}}(M, -): & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & n & \longmapsto & P_{\mathfrak{q}}(M, n) := \ell_R(M/\mathfrak{q}^n M). \end{array}$$

Entonces, $\Delta P_{\mathfrak{q}}(M, -) = \chi(G_{\mathfrak{q}}(M), -)$. En particular, $P_{\mathfrak{q}}(M, -)$ es una función polinomial llamada función de Samuel (o de Hilbert-Samuel). Se tiene que el grado de $P_{\mathfrak{q}}(M, -)$ está acotado por el número mínimo de generadores de $\mathfrak{q}$.

Demostración. Sea $r := min\{\#(S) : S \text{ genera } \mathfrak{q}\} \in \mathbb{N}$. Se considera la sucesión de R-módulos:

$$0 \longrightarrow \mathfrak{q}^n M/\mathfrak{q}^{n+1}M \xrightarrow{f} M/\mathfrak{q}^{n+1}M \xrightarrow{g} M/\mathfrak{q}^n M \longrightarrow 0,$$

que es exacta, lo que se prueba de modo inmediato. En vista de la Observación 6 precedente, $\mathfrak{q}^n M/\mathfrak{q}^{n+1}M$, $M/\mathfrak{q}^{n+1}M$ y $M/\mathfrak{q}^n M$ son R-módulos de longitud finita que, en virtud de la Proposición A.9.8, verifican:

$$\ell_R(\mathfrak{q}^n M/\mathfrak{q}^{n+1}M) = \ell_R(M/\mathfrak{q}^{n+1}M) - \ell_R(M/\mathfrak{q}^n M).$$

Como $\mathfrak{q} \subseteq Ann_R(\mathfrak{q}^n M/\mathfrak{q}^{n+1}M)$, se tiene que las estructuras de $\mathfrak{q}^n M/\mathfrak{q}^{n+1}M$ como R-módulo y como $R/\mathfrak{q}$-módulo coinciden y, dado que la longitud de $\mathfrak{q}^n M/\mathfrak{q}^{n+1}M$ solo depende de sus submódulos, se sigue que $\ell_R(\mathfrak{q}^n M/\mathfrak{q}^{n+1}M) = \ell_{R/\mathfrak{q}}(\mathfrak{q}^n M/\mathfrak{q}^{n+1}M) = \chi(G_\mathfrak{q}(M), n)$. Finalmente, se induce que

$$\begin{aligned}\chi(G_\mathfrak{q}(M), n) = \ell_R(\mathfrak{q}^n M/\mathfrak{q}^{n+1}M) &= \ell_R(M/\mathfrak{q}^{n+1}M) - \ell_R(M/\mathfrak{q}^n M)\\ &= P_\mathfrak{q}(M, n+1) - P_\mathfrak{q}(M, n) = \Delta P_\mathfrak{q}(M, n).\end{aligned}$$

Ahora, por la Proposición 1.4.4, $\chi(G_\mathfrak{q}(M), -)$ es una aplicación de grado a lo sumo $r - 1$. En virtud del Lema 1.4.1, $P_\mathfrak{q}(M, -)$ es una aplicación polinomial de grado a lo sumo r. □

Veamos, seguidamente, que el grado de la función polinomial de Samuel es independiente del ideal de definición $\mathfrak{q}$ elegido.

LEMA 1.4.6. *Sean $f, g : \mathbb{N} \longrightarrow \mathbb{N}$ dos funciones polinomiales. Supongamos que existen $m, m_0 \in N$ tal que*

$$f(n) \leq g(n) \leq f(mn + m_0).$$

Entonces, $deg(f) = deg(g)$. Más aún, si a_d es el coeficiente director de f y b_d es el coeficiente director de g, se tiene que

$$a_d \leq b_d \leq a_d m^d.$$

DEMOSTRACIÓN. Definamos $h(n) := f(mn+m_0)$. Veamos que h es una función polinomial de grado $deg(h) = deg(f)$. Sea $f' := \sum_{i=0}^{d} a_i X^i$ el polinomio asociado a la aplicación polinomial f, entonces, en virtud del Binomio de Newton:

$$f'(mn + m_0) = \sum_{i=0}^{d} a_i(mn + m_0)^i = a_d((mn)^d + d(mn)^{d-1}m_0 + \cdots + m_0^d) + f''(mn + m_0),$$

donde f'' es un polinomio de grado estrictamente menor que d. Por tanto, el polinomio asociado a la aplicación polinomial h será $h' = a_d m^d X^d + h''(X)$ con $h''(X)$ polinomio de grado estrictamente menor que d o, equivalentemente $h' = \sum_{i=0}^{d} c_i X^i$ donde $c_d = a_d m^d$. Y, en consecuencia, se tiene que f y h son aplicaciones polinomiales de grado d (tienen el mismo grado). Probemos que $deg(f) = deg(g)$ por inducción en $deg(f)$. Si $deg(f) = -1$, existe $n_0 \in \mathbb{N}$ tal que $f(n) = 0$ para todo $n \geq n_0$. Como $deg(f) = deg(h) = 0$, existe $n_1 \in \mathbb{N}$ tal que $h(n) = 0$ para todo $n \geq n_1$. Esta condición implica que $g(n) = 0$ para todo $n \geq max\{n_0, n_1\}$ y, por tanto, $deg(g) = -1$. Supongamos, ahora, $deg(f) \geq 0$. Consideremos las aplicaciones incremento Δf, Δg y Δh. Por el Lema 1.4.1, $deg(\Delta f) = deg(f) - 1$ y $deg(\Delta h) = deg(h) - 1 = deg(f) - 1$. Además se tiene que

$$\Delta f(n) \leq \Delta g(n) \leq \Delta h(n). \tag{1.4.1}$$

Por una parte $\Delta f(n) \leq \Delta g(n)$ si y solamente si $f(n+1) - g(n+1) \leq f(n) - g(n)$. Si esto no fuese así, existiría $l_1 \in \mathbb{N}$ tal que $0 \geq f(l_1 + 1) - g(l_1 + 1 > f(l_1) - g(l_1)$, lo que implicaría $f(l) > g(l)$, entrando en contradicción con la hipótesis $f(n) \leq g(n)$. De la misma manera, $\Delta g(n) \leq \Delta h(n)$ si y solamente si $g(n+1) - h(n+1) \leq g(n) - h(n)$. Si esto no fuese así, existiría $l_2 \in \mathbb{N}$ tal que $0 \geq g(l_2+1) - h(l_2+1) > g(l_2) - h(l_2)$, lo que implicaría $g(l_2) > h(l_2)$, entrando en contradicción con la hipótesis $g(n) \leq f(mn+m_0) = h(n)$. En suma, se tiene que las aplicaciones Δf y Δh son aplicaciones polinomiales de grado $deg(f) - 1$ y verifican la Igualdad (1.4.1). Entonces, por hipótesis inductiva se tiene que Δg es una aplicación polinomial de grado $deg(f) - 1$. En virtud del Lema 1.4.1, se tiene que g es una aplicación polinomial de grado $deg(g) = deg(f)$.
Sea $d := deg(f) = deg(g)$. Veamos que $a_d \leq b_d \leq a_d m^d$ por inducción en d. Si $d = -1$, entonces $a_d = b_d = a_d.m^d = 0$. Si $d = 0$, entonces existen $n_0, n_1, n_2 \in \mathbb{N}$ tales que $f(n) = a_d$ para todo $n \geq n_0$; $g(n) = b_d$ para todo $n \geq n_1$ y $h(n) = a_d m^d = a_d.m^0 = a_d$ para todo $n \geq n_2$. Por tanto, la desigualdad $f(n) \leq g(n) \leq h(n)$ se escribe $a_d \leq b_d \leq a_d$ para todo $n \geq max\{n_0, n_1, n_2\}$, con lo que queda probado este caso. Supongamos $d > 0$. Consideremos nuevamente las aplicaciones incremento Δf, Δg y Δh. Sean f', g', h' sus polinomios asociados respectivamente. En virtud del Lema 1.4.1, se tiene que

$$f'(X) = da_d X^{d-1} + f_2(X), \quad g'(X) = db_d X^{d-1} + g_2(X) \quad h'(T) = da_d m^d T^{d-1} + h_2(T),$$

donde f_2, g_2, $h_2 \in \mathbb{Q}[X]$ son polinomios de grado a lo sumo $d-2$. Por hipótesis de inducción:

$$da_d \leq db_d \leq da_d m^d.$$

Como $d > 0$, se tiene que

$$a_d \leq b_d \leq a_d m^d.$$

□

Proposición 1.4.7. *Sea $(R, \mathfrak{m})$ un anillo local noetheriano, $\mathfrak{q}$ un ideal de definición de R y M un módulo finitamente generado, entonces $P_\mathfrak{q}(M,-)$ y $P_\mathfrak{m}(M,-)$ tienen el mismo grado. En particular, el grado del polinomio de Samuel no depende del ideal de definición elegido.*

Demostración. Como $\mathfrak{q}$ es ideal de definición de R, existe $m \in \mathbb{N}$ con $\mathfrak{m}^m \subseteq \mathfrak{q} \subseteq \mathfrak{m}$. Por consiguiente, $\mathfrak{m}^{mn} \subseteq \mathfrak{q}^n \subseteq \mathfrak{m}^n$ para todo $n \in \mathbb{N}$. Ahora consideramos los siguiente morfismos suprayectivos, que no son más que las proyecciones canónicas: $M/\mathfrak{q}^n \longrightarrow M/\mathfrak{m}^n$ y $M/\mathfrak{q}^{mn} \longrightarrow M/\mathfrak{q}^n$. Entonces se tiene que $\ell_R(M/\mathfrak{m}^n) \leq \ell_R(M/\mathfrak{q}^n) \leq \ell_R(M/\mathfrak{m}^{nm})$. O lo que es lo mismo,

$$P_\mathfrak{m}(M,n) \leq P_\mathfrak{q}(M,n) \leq P_\mathfrak{m}(M,mn).$$

En virtud del Lema 1.4.6 precedente, $deg(P_\mathfrak{q}(M,-)) = deg(P_\mathfrak{m}(M,-))$. □

Definición 17. *En las condiciones de la Proposición 1.4.5, se define la dimensión de Hilbert-Samuel de M, y se denota $dim_{HS}(M)$, al grado del polinomio de Samuel respecto de cualquier ideal de definición $\mathfrak{q}$ de R.*

Observación 7. *En las condiciones de la Proposición 1.4.5, los coeficientes directores a_d de los polinomios de Samuel verifican siempre $a_d \geq 0$: basta notar que $P_\mathfrak{q}(M,n) = \ell_R(M/\mathfrak{q}^n M) \geq 0$ para todo $n \in \mathbb{N}$ y aplicar el Lema 1.4.6 a las aplicaciones polinomiales $P_\mathfrak{q}(M,n)$ y $f := 0$. Además, si $a_d = 0$, existe $n_0 \in \mathbb{N}$ tal que $P_\mathfrak{q}(M,n) = 0$ para todo $n \geq n_0$, entonces $\ell_R(M/\mathfrak{q}^{n_0}M) = 0$ y $M/\mathfrak{q}^{n_0}M = 0$. O, equivalentemente, $M = \mathfrak{q}^{n_0}M$. Como R es local, $\mathfrak{R} = \{\mathfrak{m}\}$ y $\mathfrak{q}^{n_0} \subseteq \mathfrak{m}$ es un ideal contenido en el ideal de Jacobson de R. En consecuencia, por el Lema de Nakayama (ver Proposición A.8.12), se tiene que $M = 0$.*

Proposición 1.4.8. *Sea $(R, \mathfrak{m})$ un anillo local noetheriano. $\mathfrak{q}$ un ideal de definición de R y*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

una sucesión exacta corta de R-módulos finitamente generados. Entonces, existe una aplicación polinomial $R : \mathbb{N} \longrightarrow \mathbb{N}$ de coeficiente director no negativo cuyo grado es estrictamente menor que el grado de $P_\mathfrak{q}(M,-)$ y verificándose:

$$P_\mathfrak{q}(M',n) + P_\mathfrak{q}(M'',n) = P_\mathfrak{q}(M,n) + R(n)$$

para todo $n \in \mathbb{N}$.

Demostración. Primero notamos que como f es inyectiva, puede entenderse M' como submódulo de M y tiene sentido considerar $M' \cap \mathfrak{q}^n M$. Entonces, construimos la sucesión de R-módulos

$$0 \longrightarrow M'/(M' \cap \mathfrak{q}^n M) \xrightarrow{\tilde{f}} M/\mathfrak{q}^n M \xrightarrow{\tilde{g}} M''/\mathfrak{q}^n M'' \longrightarrow 0\ ,$$

que es exacta corta. Para verlo basta notar que $\tilde{f}$ es inyectiva por serlo f y $\tilde{g}$ es suprayectiva y está bien definida por ser g suprayectiva. De otro lado, $ker(\tilde{g}) = ker(g)/\mathfrak{q}^n M = im(f)/\mathfrak{q}^n M = Im(\tilde{f})$. Además, por la Observación 6, $M/\mathfrak{q}^n M$ es de longitud finita. En virtud de la Proposición A.9.8, $M'/(M' \cap \mathfrak{q}^n M)$ y $M''/\mathfrak{q}^n M''$ son de longitud finita y se tiene la relación:

$$\ell_R(M/\mathfrak{q}^n M) = \ell_R(M'/(M' \cap \mathfrak{q}^n M)) + \ell_R(M''/\mathfrak{q}^n M''). \tag{1.4.2}$$

Observamos, entonces, que $\ell_R(M'/(M' \cap \mathfrak{q}^n M)) = P_\mathfrak{q}(M,n) - P_\mathfrak{q}(M'',n)$ es una aplicación polinomial. Definimos $M'_n := M' \cap q^n M$ y obtenemos una filtración en M' a partir de la filtración $\mathfrak{q}$-ádica en M. Ahora, por el Corolario 1.3.3 del Teorema de Artin-Rees (ver Teorema 1.3.2), se tiene que existe $n_0 \in N$ tal que $\mathfrak{q}M'_n = \mathfrak{q}(\mathfrak{q}^n M \cap M') = \mathfrak{q}^{n+1}M \cap M' = M'_{n+1}$ para todo $n \geq n_0$. En particular, para cada $n \in \mathbb{N}$, $\mathfrak{q}^{n+n_0}M' \subseteq M'_{n+n_0} = \mathfrak{q}^n M'_{n_0} \subseteq \mathfrak{q}^n M'$. Esto implica:

$$P_\mathfrak{q}(M',n) = \ell_R(M'/\mathfrak{q}^n M') \leq \ell_R(M'/M'_{n+n_0}) \leq \ell_R(M'/\mathfrak{q}^{n+n_0}M') = P_\mathfrak{q}(M',n+n_0).$$

A partir de la relación anterior, en virtud del Lema 1.4.6, se sigue que $\ell_R(M'/M'_{n+n_0})$ y $P_{\mathfrak{q}}(M', n)$ tienen el mismo grado y mismo coeficiente director. Ahora, se construye la aplicación polinomial $R : \mathbb{N} \longrightarrow \mathbb{N}$ dada por

$$R(n) := P_{\mathfrak{q}}(M', n) - \ell_R(M'/M'_n) \ ,$$

que, en virtud de la Igualdad (1.4.2), verifica $P_{\mathfrak{q}}(M', n) + P_{\mathfrak{q}}(M'', n) = P_{\mathfrak{q}}(M, n) + R(n)$. Notemos que tiene coeficiente director no negativo porque $R(n) \geq 0$ para $n \geq n_0$. Además, como $R(T)$ está definida como la diferencia de dos aplicaciones polinomiales con mismo grado y coeficiente director, se tiene que $deg(R(T)) < deg(\ell_R(M'/M'_n))$. Finalmente, como $\ell_R(M'/M'_n) = P_{\mathfrak{q}}(M, n) - P_{\mathfrak{q}}(M'', n)$, se tiene que $deg(\ell_R(M'/M'_n) \leq max\{deg(P_{\mathfrak{q}}(M, n)), deg(P_{\mathfrak{q}}(M'', n))\} = deg(P_{\mathfrak{q}}(M, n)$ dada la Igualdad (1.4.2), y en consecuencia, $deg(R(T)) < deg(P_{\mathfrak{q}}(M, n))$. □

COROLARIO 1.4.9. *Sea $(R, \mathfrak{m})$ un anillo local noetheriano, $\mathfrak{q}$ un ideal de definición de R, M un R-módulo finitamente generado y N un submódulo de M. Entonces,*

$$dim_{HS}(N) \leq dim_{HS}(M)$$

$$dim_{HS}(M/N) \leq dim_{HS}(M)$$

DEMOSTRACIÓN. Consideramos la sucesión exacta corta $0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$. Por 1.4.8, $P_{\mathfrak{q}}(N, n) + P_{\mathfrak{q}}(M/N, n) = P_{\mathfrak{q}}(M, n) + R(n)$. Como los coeficientes de $P_{\mathfrak{q}}(N, n)$ y $P_{\mathfrak{q}}(N, n)$ son no negativos y $deg(R(T)) < deg(P_{\mathfrak{q}}(M, -))$ se tiene que los grados de $P_{\mathfrak{q}}(N, -)$ y $P_{\mathfrak{q}}(M/N, -)$ no pueden ser superiores al grado de $P_{\mathfrak{q}}(M, -)$. □

PROPOSICIÓN 1.4.10. *Sea $(R, \mathfrak{m})$ un anillo local noetheriano, $k = R/\mathfrak{m}$ y r el mínimo de los cardinales de los conjuntos que generan $\mathfrak{m}$ como ideal de R. Se tiene que $deg(\chi(G_{\mathfrak{m}}(R), -)) = r - 1$ si y solamente si $\varphi : k[X_1 \ldots, X_r] \longrightarrow G_{\mathfrak{m}}(R)$ es isomorfismo.*

DEMOSTRACIÓN. Notemos que, en general, se puede definir el epimorfismo de grado 0 de k-álgebras graduadas $\varphi : k[X_1 \ldots, X_r] \longrightarrow G_{\mathfrak{m}}(R)$ tomando $\varphi(X_i) := x_i + \mathfrak{m}^2$ para $1 \leq i \leq r$, donde $\{x_1 \ldots x_r\}$ es el conjunto generador minimal de $\mathfrak{m}$ como ideal de R (esto se debe a que, como se vio en la Proposición 1.4.4, el conjunto $\{x_i + \mathfrak{m}^2 \ : \ 1 \leq i \leq r\}$ genera $\mathfrak{m}/\mathfrak{m}^2$ como k-módulo y $G_{\mathfrak{m}}(R)$ es una $k-$álgebra generada por los elementos de $\mathfrak{m}/\mathfrak{m}^2$); $k[X_1 \ldots, X_r] = H$, donde $H := \bigoplus_{n \in \mathbb{N}} H_n$ y H_n es el espacio vectorial de polinomios homogéneos de grado n con coeficientes en k. Más aún, se puede definir el epimorfismo de k-módulos:

$$\varphi_n := \varphi|_{H_n} : H_n \longrightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1}.$$

Por una parte, $\varphi : k[X_1 \ldots, X_r] \longrightarrow G_{\mathfrak{m}}(R)$ es claramente un morfismo de k-álgebras, pues se han definido la imagen de un conjunto generador $\{X_1 \ldots, X_r\}$ y se ha extendido por linealidad. Por otra parte, es un morfismo graduado de grado 0, pues si $h \in H_n$, entonces h es de la forma

$$h = \sum_{i=0}^{s} (a_i \prod_{j=0}^{n} X_{i,j}), \qquad X_{i,j} \in \{X_1, \ldots, X_r\}.$$

En consecuencia, tenemos:

$$\varphi(h) = \sum_{i=0}^{s} (a_i \prod_{j=1}^{n} \varphi(X_{i,j})) = \sum_{i=0}^{s} a_i \prod_{j=1}^{n} \bar{x}_{i,j},$$

con $\bar{x}_{i,j} \in \{\bar{x}_1, \ldots, \bar{x}_r\}$, siendo $\bar{x}_k = x_k + \mathfrak{m}^2 \in \mathfrak{m}/\mathfrak{m}^2$. Por tanto, $f(h) \in \mathfrak{m}^n/\mathfrak{m}^{n+1}$. Retomemos el morfismo $\varphi_n : H_n \longrightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1}$. Está bien definido porque φ es morfismo graduado de grado 0 y $\varphi_n(H_n) \subseteq \mathfrak{m}^n/\mathfrak{m}^{n+1}$. Además, es suprayectivo porque $\mathfrak{m}^n$ es el ideal generado por los productos $\{\prod_{j=1}^{n} x_{i,j} : x_{i,j} \in \{x_1, \ldots, x_r\}\}$. Finalmente, como φ_n es suprayectivo para cada $n \in \mathbb{N}$, entonces, dado

$$x = \sum_{i=0}^{t} x_i \in G_{\mathfrak{m}}(R),$$

donde $x_i \in \mathfrak{m}^i/\mathfrak{m}^{i+1}$ y dado $h_i \in H_i$ tal que $\varphi_i(h_i) = x_i$, concluimos

$$\varphi(\sum_{i=0}^{t} h_i) = \sum_{i=0}^{t} \varphi(h_i) = \sum_{i=0}^{t} \varphi_i(h_i) = \sum_{i=0}^{t} x_i = x,$$

y φ es un epimorfismo de anillos.
Supongamos que φ es un isomorfismo. Entonces, para cada $n \in \mathbb{N}$ se tiene que

$$\varphi_n : H_n \longrightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1}$$

es un isomorfismo. Ya se ha visto que φ_n es morfismo suprayectivo. Además, como $\varphi_n = \varphi|_{H_n}$, si φ_n no fuese inyectiva, φ tampoco sería inyectiva. Esto entra en contradicción con la hipótesis de que φ es isomorfismo.
Ahora, como φ_n es isomorfismo, $\chi(G_\mathfrak{m}(A), n) = \ell_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = \ell_k(H_n) = dim_k(H_n) = \binom{n+r-1}{r-1}$. En virtud del Lema 1.4.2, $\chi(G_\mathfrak{m}(R), n)$ es una aplicación polinomial de grado $r-1$.
Por otra parte, si φ no es isomorfismo, definamos $N := ker(\varphi) \neq 0$. Nótese que N es un ideal homogéneo de H. Es decir, N está generado por elementos homogéneos de H. Como k es cuerpo, k es noetheriano y, en virtud del Teorema de la Base de Hilbert (cf. Teorema A.8.6), $k[X_1, \ldots, X_r] = H$ es noetheriano. Con lo que se tiene que N es un ideal finitamente generado. Sea F un conjunto generador finito de N como ideal de H. Supongamos f un elemento no homogéneo de F. Entonces, existe un conjunto $I \subseteq \mathbb{N}$ finito tal que $f = \sum_{i\in I} f_i$, donde $f_i \in H_i$ es un elemento homogéneo de grado i de H. Como F genera $N = ker\varphi$ y $f \in F$, $\varphi(f) = 0$. Y dado $i_0 \in I$ se tendría $f_{i_0} = -\sum_{i\in I,\ i\neq i_0} f_i$ que son dos fomas distintas de expresar un mismo elemento en H, lo que entra en contradicción con que $H = \oplus_{n\in\mathbb{N}} H_n$ sea una suma directa. Por tanto, visto que N es un ideal homogéneo de H, podemos escribir

$$N = \bigoplus_{n\in N} N_n, \qquad N_n = H_n \cap ker(\varphi) = ker(\varphi_n).$$

Ahora, se tiene que N es un ideal de H, en particular es un subespacio vectorial del k-espacio vectorial H. Luego $N_n = N \cap H_n$ es la intersección de dos subespacios vectoriales de H y es, a su vez, subespacio vectorial de H. Más aún, como $N_n \subseteq H_n$. N_n puede verse como un subespacio vectorial del k-espacio vectorial H_n. En virtud de la Proposición A.9.10, $\ell_k(N_n) = dim_k(N_n) \leq dim_k(H_n) = \ell_k(H_n)$ y N_n es de longitud finita como k-módulo. Más aún, para cada $n \in \mathbb{N}$ se tiene la sucesión exacta corta de k-espacios vectoriales de dimensión finita:

$$0 \longrightarrow N_n \xrightarrow{i_n} H_n \xrightarrow{\varphi_n} \mathfrak{m}^n/\mathfrak{m}^{n+1} \longrightarrow 0.$$

En virtud de la Proposición A.9.8, se tiene la relación:

$$\chi(G_\mathfrak{m}(A), -) = \binom{n+r-1}{r-1} - \ell_k(N_n) \tag{1.4.3}$$

Tómese $f \in N$ homogéneo. Sea $d = deg(f)$. Se tiene que $f.H_n \subseteq N_{n+d}$ para todo $n \in \mathbb{N}$. Por una parte, por la estructura de anillo graduado en H, se tiene el contenido $f.H_n \subseteq H_{n+d}$. De otro lado, como N es ideal de H, $f.H_n \subseteq N$. Ahora, como $N_n \subseteq H_n$, $\ell_k(N_n) \leq \ell_k(H_n)$. Además, como H_n es dominio de integridad y $f \neq 0$ se tiene que la aplicación $H_n \longrightarrow fH_n$ dada por $g \longmapsto fg$ es isomorfismo de k-espacios vectoriales y por tanto, $dim_k(H_n) = \ell_k(H_n) = \ell_k(fH_n) = dim_k(fH_n)$. En consecuencia, se tiene:

$$\ell_k(N_n) \leq \ell_k(H_n) = \ell_k(fH_n) \leq \ell_k(N_{n+d})$$

Finalmente, en virtud del Lema 1.4.6, $\ell_k(H_n) = \binom{n+r-1}{r-1}$ y $\ell_k(N_n)$ son aplicaciones polinomiales con el mismo grado y coeficiente director. Como $deg(\ell_k(H_n)) = r-1$, la Igualdad (1.4.3) implica que $deg(\chi(G_\mathfrak{m}(A), -)) < r-1$. □

Corolario 1.4.11. *Con las notaciones de la Proposición precedente, si* $\mathfrak{q}$ *es un ideal de definición de* R*, se tiene que* $deg(P_\mathfrak{q}(R, -)) = r$ *si y solamente si*

$$\varphi : k[X_1 \ldots, X_r] \longrightarrow G_\mathfrak{m}(R)$$

es un isomorfismo.

Demostración. Por una parte, supongamos que $deg(P_\mathfrak{q}(R, -)) = r$. Entonces, en virtud de la Proposición 1.4.7, $deg(P_\mathfrak{q}(R, -)) = deg(P_\mathfrak{m}(R, -))$. Ahora, por el Teorema 1.4.5 se tiene que $\chi(G_\mathfrak{m}(R), -) = \Delta P_\mathfrak{m}(R, -)$ y, por el Lema 1.4.1, se infiere que $deg(\chi(G_\mathfrak{m}(R), -)) = deg(\Delta P_\mathfrak{m}(R, -)) = r-1$. Aplicando la Proposición 1.4.10 precedente, φ es un isomorfismo.
De otro lado, supongamos que φ es un isomorfismo. Por la Proposición anterior 1.4.10, $deg(\chi(G_\mathfrak{m}(R), -)) = r-1$. En virtud del Teorema 1.4.5, $\chi(G_\mathfrak{m}(R), -) = \Delta P_\mathfrak{m}(R, -)$ Aplicando

nuevamente el Lema 1.4.1, $deg(P_{\mathfrak{m}}(R,-)) = r$. Finalmente, la Proposición 1.4.7 garantiza que $deg(P_{\mathfrak{m}}(R,-)) = deg(P_{\mathfrak{q}}(R,-)) = r$. □

En la definición siguiente usaremos el soporte de un R-módulo $Supp(M)$ y los primos asociados de un R-módulo $Ass(M)$, que se describen en la Sección A.10 del Apéndice A. Como no tenemos especial interés en casos más sofisticados en este Trabajo Fin de Grado, nos restringimos al caso noetheriano.

DEFINICIÓN 18. *Sean R un anillo noetheriano y M un R-módulo finitamente generado. Se consideran las siguientes nociones:*
i) Una cadena en R es una sucesión de ideales primos $\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_r$ tal que $\mathfrak{p}_i \neq \mathfrak{p}_{i+1}$ para $0 \leq i \leq r-1$. Se dice, además, que esta cadena es de longitud r.
ii) La altura de un ideal $\mathfrak{p}$ se define como:

$$ht(\mathfrak{p}) := sup\ \{r :\ \exists\{\mathfrak{p}_0, \ldots, \mathfrak{p}_r\} \subseteq Spec(R) :\ \mathfrak{p}_0 \subseteq \cdots \subseteq \mathfrak{p}_r = \mathfrak{p}\}.$$

Es decir, el supremo de las longitudes de las cadenas en R de la forma $\mathfrak{p}_0 \subseteq \cdots \subseteq \mathfrak{p}_r = \mathfrak{p}$.
iii) La co-altura de un ideal $\mathfrak{p}$ se define como:

$$coht\mathfrak{p} := sup\ \{r :\ \exists\{\mathfrak{p}_0, \ldots, \mathfrak{p}_r\} \subseteq Spec(R) :\ \mathfrak{p} = \mathfrak{p}_0 \subseteq \cdots \subseteq \mathfrak{p}_r\}.$$

Es decir, el supremo de las longitudes de las cadenas en R de la forma $\mathfrak{p} = \mathfrak{p}_0 \subseteq \cdots \subseteq \mathfrak{p}_r$.
iv) La dimensión de Krull de M, denotada $dim_{Kr}(M)$, se define de la siguiente manera:

$$dim_{Kr}(M) := sup\ \{coht(\mathfrak{p}) :\ \mathfrak{p} \in Supp(M)\}.$$

Si $M = 0$ se define $dim_{Kr}(M) := -1$.
v) La dimensión de Krull del anillo R se define como la dimensión de R visto como R-módulo.

Como estamos en el caso noetheriano y como la dimensión de Krull es el supremo de las co-alturas de los ideales del soporte, dicho supremo, de alcanzarse, será en los primos minimales de $Supp(M)$. En virtud del Corolario A.10.12, se tiene que

$$dim_{Kr}(M) = sup\ \{coht(\mathfrak{p}) :\ \mathfrak{p} \in Ass(M)\}.$$

PROPOSICIÓN 1.4.12. *Sea R un anillo y $\mathfrak{p}$ un ideal primo de R. Entonces,*

i) $dim_{Kr}(R/\mathfrak{p}) = coht(\mathfrak{p})$
ii) $dim_{Kr}(R_{\mathfrak{p}}) = ht(\mathfrak{p})$

DEMOSTRACIÓN. Ambas afirmaciones se siguen de modo inmediato dado que

$$Supp(R/\mathfrak{p}) = Spec(R/\mathfrak{p}) = \{\mathfrak{q}/\mathfrak{p} : \mathfrak{q} \in Spec(R),\ \mathfrak{q} \supseteq \mathfrak{p}\},$$
$$Supp(R_{\mathfrak{p}}) = Spec(R_{\mathfrak{p}}) \cong \{\mathfrak{q} \in Spec(R) :\ \mathfrak{q} \subseteq \mathfrak{p}\}.$$

Ver la Proposición A.10.11. □

DEFINICIÓN 19. *Sea $(R, \mathfrak{m})$ un anillo local noetheriano y M un R-módulo finitamente generado. Se llamará dimensión de Chevalley de M y se denotará $dim_{Chev}(M)$ a*

$$dim_{Chev}(M) := min\ \{n \in \mathbb{N} :\ \exists\, a_1, \ldots, a_n \in \mathfrak{m},\ \ell_R(M/(a_1, \ldots, a_n)M < +\infty\}.$$

Si $M = 0$, se define $dim_{Chev}(M) := -1$.

OBSERVACIÓN 8. *Notemos que como R es local $M/\mathfrak{m}M$ es un $R/\mathfrak{m}$-espacio vectorial de dimensión finita. Y en virtud de la Proposición A.9.10, $\ell_{R/\mathfrak{m}}(M/\mathfrak{m}M) < +\infty$. Además, su estructura como R-módulo coincide con la de $R/\mathfrak{m}$-módulo porque $\mathfrak{m} \subseteq Ann_R(M/\mathfrak{m}M)$. En consecuencia, $\ell_R(M/\mathfrak{m}M) = \ell_{R/\mathfrak{m}}(M/\mathfrak{m}M) < \infty$. Además, como R es noetheriano, $\mathfrak{m}$ es finitamente generado y se tiene que $dim_{Chev}(M)$ está acotado por el cardinal de cualquier conjunto que genere a $\mathfrak{m}$ como ideal de R.*

El siguiente Teorema unifica los conceptos de dimensión de Krull, dimensión de Samuel y dimensión de Chevalley para módulos finitamente generados sobre anillos locales noetherianos. Una consideración a tener en cuenta previa a la demostración es que, la Observación 8 y el Teorema 1.4.5 garantizan que, en este caso particular, $dim_{Chev}(M) < +\infty$ y $dim_{HS}(M) < +\infty$.

TEOREMA 1.4.13 (**Teorema de la Dimensión Local**). *Sea $(R, \mathfrak{m})$ un anillo local noetheriano y M un R-módulo finitamente generado, entonces*

$$dim_{Kr}(M) = dim_{HS}(M) = dim_{Chev}(M) < +\infty.$$

Demostración. Dividamos la prueba en 3 partes:

$$dim_{Kr}(M) \leq dim_{HS}(M) \tag{1.4.4}$$

$$dim_{HS}(M) \leq dim_{Chev}(M) \tag{1.4.5}$$

$$dim_{Chev}(M) \leq dim_{Kr}(M) \tag{1.4.6}$$

i) Como $dim_{HS}(M) < +\infty$, probémoslo por inducción en $dim_{HS}(M)$: Si $dim_{HS}(M) = -1$, entonces existe $n_0 \in \mathbb{N}$ tal que $P_{\mathfrak{m}}(M, n) = 0$ para todo $n \geq n_0$. Es decir, $M = \mathfrak{m}^n M$. Por el Lema de Nakayama (cf. Proposición A.8.12), $M = 0$ y $dim_{Kr}(M) = -1$.
Sea $dim_{HS}(M) \geq 0$. Por el Teorema A.10.3, $Ass_R(M)$ es un conjunto finito y, en consecuencia, existe $\mathfrak{p} \in Ass_R(M)$ verificando

$$sup\,\{coht(\mathfrak{q}) : \ \mathfrak{q} \in Ass_R(M)\} = coht(\mathfrak{p}).$$

En virtud de la Proposición 1.4.12, $coht(\mathfrak{p}) = dim_{Kr}(R/\mathfrak{p})$. Por otra parte, como $\mathfrak{p} \in Ass_R(M)$, en vista de la Observación 17, $R/\mathfrak{p} \longrightarrow M$ es un monomorfismo de R-módulos. En consecuencia, $R/\mathfrak{p}$ puede verse como un submódulo de M. Entonces, por el Corolario 1.4.9, se tiene que $dim_{HS}(R/\mathfrak{p}) \leq dim_{HS}(M)$.
Por tanto, para probar la Desigualdad (1.4.4) es suficiente probar que $dim_{Kr}(R/\mathfrak{p}) \leq dim_{HS}(R/\mathfrak{p})$. Como hay una correspondencia biyectiva entre los primos de $R/\mathfrak{p}$ y los primos de R que contienen a $\mathfrak{p}$, debemos comprobar que si $\mathfrak{p} = \mathfrak{p}_0 \subseteq \cdots \subseteq \mathfrak{p}_r$ es una cadena de ideales en R, entonces $r \leq dim_{HS}(R/\mathfrak{p})$. Probémoslo por inducción en r: Supongamos $r = 0$. Si fuese $dim_{HS}(R/\mathfrak{p}) = -1$, existiría $n_0 \in \mathbb{N}$ de modo que $P_{\mathfrak{m}}(R/\mathfrak{p}, n) = 0$ para todo $n \geq n_0$, esto es, $(R/\mathfrak{p})/\mathfrak{m}^n \cong R/\mathfrak{p}\mathfrak{m}^n = 0$. Por el Lema de Nakayama (Proposición A.8.12), $R = \mathfrak{p}\mathfrak{m}^n \subseteq \mathfrak{m}$ contradiciendo la maximalidad de $\mathfrak{m}$. Por tanto, debe ser $r = 0 \leq dim_{HS}(R/\mathfrak{p})$.
Sea $r \geq 1$. Sean $\mathfrak{p} = \mathfrak{p}_0 \subseteq \cdots \subseteq \mathfrak{p}_r$ una cadena de ideales de R, $a \in \mathfrak{p}_1 \backslash \mathfrak{p}_0$ y $\mathfrak{p}'$ el ideal primo minimal que contiene al ideal suma $\mathfrak{p} + (a)$ a su vez contenido en $\mathfrak{p}_1$. Se construye la cadena de ideales $\mathfrak{p}' \subseteq \mathfrak{p}_2 \subseteq \cdots \subseteq \mathfrak{p}_r$, que tiene longitud $r - 1$. Por hipótesis inductiva, $r - 1 \leq dim_{HS}(R/\mathfrak{p}')$. Además, si $x \in Ann_R({}^{R}/_{((a)\,+\,\mathfrak{p})})$, entonces $xy \in R/(a) + \mathfrak{p} \subseteq \mathfrak{p}'$ para todo $y \in R$. En particular, para todo $y \in R \backslash \mathfrak{p}'$. Por primalidad de $\mathfrak{p}'$ se tiene que $x \in \mathfrak{p}'$ y, por tanto, $\mathfrak{p}' \supseteq Ann_R({}^{R}/_{((a)\,+\,\mathfrak{p})})$. En virtud del apartado *iii)* de la Proposición A.10.11, $\mathfrak{p}' \in Supp({}^{R}/_{((a)\,+\,\mathfrak{p})})$. Es más, como $\mathfrak{p}'$ es primo minimal que contiene a $(a) + \mathfrak{p}$, $\mathfrak{p}'$ es primo minimal de $Supp({}^{R}/_{((a)\,+\,\mathfrak{p})})$. Por el Corolario A.10.12, $\mathfrak{p}' \in Ass_R({}^{R}/_{((a)\,+\,\mathfrak{p})})$. Ahora, de acuerdo a la Observación 17, $R/\mathfrak{p}' \longrightarrow {}^{R}/_{((a)\,+\,\mathfrak{p})}$ es monomorfismo. En consecuencia, $R/\mathfrak{p}'$ puede verse como un submódulo de ${}^{R}/_{((a)\,+\,\mathfrak{p})}$. Por el Corolario 1.4.9, se tiene que $dim_{HS}(\mathfrak{p}') \leq dim_{HS}\left({}^{R}/_{((a)\,+\,\mathfrak{p})}\right)$. Consideremos la sucesión exacta de R-módulos:

$$0 \longrightarrow R/\mathfrak{p} \xrightarrow{\varphi} R/\mathfrak{p} \xrightarrow{\pi} {}^{R}/_{((a)\,+\,\mathfrak{p})},$$

donde φ es la homotecia por a en $R/\mathfrak{p}$ y π es la proyección canónica. Por una parte π es suprayectiva por ser proyección y está bien definida porque $\mathfrak{p} \subseteq (a) + \mathfrak{p}$. Por otra parte, la inyectividad de φ queda garantizada por la primalidad de $\mathfrak{p}$. Además, $(a) + \mathfrak{p} = ker(\pi) = Im(\varphi)$. En virtud de la Proposición 1.4.8,

$$P_{\mathfrak{m}}(R/\mathfrak{p}, n) + P_{\mathfrak{m}}({}^{R}/_{((a)\,+\,\mathfrak{p})}, n) = P_{\mathfrak{m}}(R/\mathfrak{p}, n) + R(n),$$

donde $deg(R) < deg(P_{\mathfrak{m}}(R/\mathfrak{p}, -))$. Entonces, $R(n) = P_{\mathfrak{m}}({}^{R}/_{((a)\,+\,\mathfrak{p})}), n)$ y se tiene:

$$r - 1 \leq dim(R/\mathfrak{p}') \leq dim_{HS}({}^{R}/_{((a)\,+\,\mathfrak{p})}) < dim_{HS}(R/\mathfrak{p}).$$

Por tanto, $r \leq dim_{HS}(R/\mathfrak{p})$.

ii) Probemos la Desigualdad (1.4.5). Por una parte, si $dim_{HS}(M) = -1$, entonces $M = 0$ y $dim_{Chev}(M) = -1$.
Sea $s := dim_{HS}(M) \geq 0$; $a_1, \ldots, a_s \in \mathfrak{m}$ tales que $M/(a_1, \ldots, a_s)M$ es de longitud finita; $\mathfrak{a} := Ann_R(M)$; y $\mathfrak{b} := (a_1, \ldots, a_s) + \mathfrak{a}$.

Afirmación. $Supp(R/\mathfrak{b}) = \{\mathfrak{m}\}$.

Demostración. Veamos primero que $Supp(M/(a_1 \ldots, a_s)M) = \{\mathfrak{m}\}$. Por una parte, la Proposición A.6.6 garantiza que $M/(a_1, \ldots, a_s)M \cong R/(a_1, \ldots, a_s) \otimes_R M$. Por otra parte, la

Proposición A.8.15 establece que $Supp(R/(a_1,\dots,a_s)\otimes_R M) = Supp(M)\cap Supp(R/(a_1,\dots,a_s))$. Combinando ambos resultados, se tiene:

$$Supp(M/(a_1,\dots,a_s)M) = Supp(M)\cap Supp(R/(a_1,\dots,a_s)).$$

Como $M/(a_1,\dots,a_s)M$ es de longitud finita, en virtud de la Proposición A.10.13 se tiene que todo ideal de $Supp(M/(a_1,\dots,a_s)M)$ es maximal. Pero como $(R,\mathfrak{m})$ es local, debe ser $Supp(M/(a_1,\dots,a_s)M)=\{\mathfrak{m}\}$.
Ahora, si $x\in Ann_R(R/\mathfrak{b})$ entonces $xa\in\mathfrak{b}\subseteq\mathfrak{m}$ para todo $a\in R\setminus\mathfrak{m}$. Por la primalidad de $\mathfrak{m}$ se tiene que $x\in\mathfrak{m}$ y, en consecuencia, $\mathfrak{m}\supseteq Ann_R(R/\mathfrak{b})$. En vista del apartado *iii)* de la Proposición A.10.11, $\mathfrak{m}\in Supp(R/\mathfrak{b})$. Por otra parte, si $\mathfrak{p}\in Supp(R/\mathfrak{b})$, por el apartado *iii)* de la Proposición A.10.11 se tiene que $\mathfrak{p}\supseteq Ann_R(R/\mathfrak{b})$. En particular, $\mathfrak{p}\supseteq Ann_R(R/\mathfrak{b})\supseteq \mathfrak{a}=Ann_R(M)$. Por el apartado *iii)* de la Proposición A.10.11, $\mathfrak{p}\in Supp(M)$. Además, $\mathfrak{p}\supseteq Ann_R(R/\mathfrak{b})\supseteq\mathfrak{b}\supseteq(a_1,\dots,a_s)\supseteq Ann_R(R/(a_1,\dots,a_s))$. Por tanto, $\mathfrak{p}\in Supp(R/(a_1,\dots,a_s))$. Entonces $\mathfrak{p}\in Supp(M)\cap Supp(R/(a_1,\dots,a_s)) = Supp(M/(a_1,\dots,a_s)M)$. Por consiguiente, $\mathfrak{p}$ debe ser maximal, con lo que se tiene $\mathfrak{p}=\mathfrak{m}$. □

Ahora, en virtud del Corolario A.10.12, los elementos minimales de $Supp(R/\mathfrak{b})$ y $Ass(R/\mathfrak{b})$ coinciden y se tiene $Ass(R/\mathfrak{b})=\{\mathfrak{m}\}$. Por el Teorema de Unicidad (cf. Teorema A.10.3), $Ass(R/\mathfrak{b})$ es independiente de la descomposición primaria escogida y se tiene que $\mathfrak{b}$ es un ideal $\mathfrak{m}$-primario. Esto es, $m_i^{n_i}\in\mathfrak{b}$ para todo $m_i\in\mathfrak{m}$. Como R un anillo noetheriano, $\mathfrak{m}$ es un ideal finitamente generado. Sea T conjunto finito generador de $\mathfrak{m}$. Para cada $t_i\in T$ definimos $n_i := min\,\{n\in\mathbb{N}:\ t_i^{n_i}\in\mathfrak{b}\}$ y $l := max\,\{n_i:\ t_i\in T\}$. Entonces, $\mathfrak{m}^l\subseteq\mathfrak{b}\subseteq\mathfrak{m}$ y $\mathfrak{b}$ es un ideal de definición de A.
Definimos $\bar R := R/\mathfrak{a}$ y $\bar{\mathfrak{b}} := \mathfrak{b}/\mathfrak{a}$. Como existe una biyección entre los ideales de R que contienen a $\mathfrak{a}$ y los ideales de $R/\mathfrak{a}$ que preserva la inclusión, el anillo noetheriano $(\bar R,\mathfrak{m}/\mathfrak{a})$ es local y $\bar{\mathfrak{b}}$ es un ideal de definición de $\bar R$. Además, como $\mathfrak{b}=(a_1,\dots,a_s)+\mathfrak{a}$, $\bar{\mathfrak{b}}=(\bar{a_1},\dots,\bar{a_s})$ donde $\bar{a_i}$ es la imagen de a_i por la proyección canónica $R\longrightarrow R/\mathfrak{a}$.
Finalmente, como M es finitamente generado, $(\bar R,\mathfrak{m}/\mathfrak{a})$ es un anillo local noetheriano y $\bar{\mathfrak{b}}$ es un ideal de definición de $\bar R$ generado por s elementos, el Teorema 1.4.5 garantiza que $deg(P_{\bar{\mathfrak{b}}}(M,-))\le s$. Pero la estructura de M como R-módulo y como $\bar R$-módulo coinciden por ser $\mathfrak{a}=Ann_R(M)$. Como la longitud solo depende de los submódulos de M, se tiene que $\ell_R(M/\mathfrak{b}^nM)=\ell_{\bar R}(M/\bar{\mathfrak{b}}^nM)$. Por consiguiente, $P_{\bar{\mathfrak{b}}}(M,-)=P_{\mathfrak{b}}(M,-)$ y

$$dim_{HS}(M) = deg(P_{\mathfrak{b}}(M,-))\le s = dim_{Chev}(M).$$

iii) Probemos la Desigualdad (1.4.6) por inducción en $dim_{Kr}(M)$. Si $dim_{Kr}(M)=-1$, $M=0$ y $dim_{Chev}(M)=-1$.
Si $dim_{Kr}(M)=0$ se tiene que $Supp(M)=\{\mathfrak{m}\}$. Como $(R,\mathfrak{m})$ es local y $Ann_R(M)$ es un ideal de R se sigue que $\mathfrak{m}\supseteq Ann_R(M)$ y en virtud del apartado *iii)* de la Proposición A.10.11, $\mathfrak{m}\in Supp(M)$. De otro lado, si $\mathfrak{p}$ es un primo de $Supp(M)$, $\mathfrak{p}\subseteq\mathfrak{m}$. Como $dim_{Kr}(M)=0$ debe ser $\mathfrak{p}=\mathfrak{m}$. Ahora, como $Supp(M)=\{\mathfrak{m}\}$, todo elemento del soporte de M es maximal y, en virtud de la Proposición A.10.13, M es de longitud finita. Por tanto, $dim_{Chev}(M)=0$.
Sea $dim_{Kr}(M)>0$. Como M es finitamente generado y R es noetheriano, el Teorema A.10.3 garantiza que $Ass_R(M)$ es finito. Sea $\{\mathfrak{p}_i\}_{1\le i\le g}\subseteq Ass_R(M)$ el conjunto de primos asociados de M con $dim_{Kr}(M)=coht(\mathfrak{p}_i)$, es decir, el conjunto de primos minimales de $Ass_R(M)$. Como $dim_{Kr}(M)>0$, $\mathfrak{m}$ no puede ser un ideal minimal de $Supp(M)$ y, en consecuencia, $\mathfrak{p}_i\subsetneq\mathfrak{m}$ para cada i, $1\le i\le g$. Por el Lema A.2.1, no es, por tanto, posible que $\mathfrak{m}\subseteq\cup_{0\le i\le g}\mathfrak{p}_i$. En particular, existirá $a\in\mathfrak{m}\setminus(\cup_{0\le i\le g}\mathfrak{p}_i)$. Defínase $M' := M/aM$.

Afirmación. $Supp(M')\subseteq Supp(M)\setminus\{\mathfrak{p}_1,\dots,\mathfrak{p}_g\}$

Demostración. Por una parte, como $Ann_R(M)\subseteq Ann_R(M/aM)$, se tiene que si $\mathfrak{q}\subseteq Ann_R(M)$, entonces $\mathfrak{q}\subseteq Ann_R(M/aM)$. En virtud del apartado *iii)* de la Proposición A.10.11, $Supp(M')\subseteq Supp(M)$. Por otra parte, si $\mathfrak{p}_i\in Supp(M')$ con $0\le i\le g$, $\mathfrak{p}_i\supseteq Ann_R(M')$. Pero $a\in Ann_R(M')$, por tanto $a\in\mathfrak{p}_i$ y se llega a una contradicción. □

Por tanto, como el soporte de M' está contenido en el soporte de M pero no contiene a los primos minimales de R, se tiene que $dim_{Kr}(M')<dim_{Kr}(M)$.

Sea $t := dim_{Chev}(M')$ y $\{a_1, \ldots, a_t\} \subseteq \mathfrak{m}$ tales que $M'/(a_1, \ldots, a_t)M'$ es de longitud finita. Se tiene, además

$$M'/(a_1, \ldots, a_t)M' \cong M/(a, a_1, \ldots, a_t)M'.$$

Pero como $(a, a_1, \ldots, a_t)M' \subseteq (a, a_1, \ldots, a_t)M$,

$$M/(a, a_1, \ldots, a_t)M \subseteq M'/(a_1, \ldots, a_t)M'.$$

Por consiguiente, $M/(a, a_1, \ldots, a_t)M$ puede verse como un submódulo de un R-módulo de longitud finita. En virtud del Corolario A.9.7, $M/(a, a_1, \ldots, a_t)M$ es de longitud finita y, por tanto,

$$dim_{Chev}(M) \leq t + 1.$$

Finalmente, por hipótesis de inducción, $t = dim_{Chev}(M') \leq dim_{Kr}(M')$, pero se había visto que $dim_{Kr}(M') < dim_{Kr}(M)$. Por lo tanto debe ser $t + 1 \leq dim_{Kr}(M)$ y se tiene

$$dim_{Chev}(M) \leq t + 1 \leq dim_{Kr}(M).$$

□

Dentro de la prueba del anterior teorema ya hemos probado la finidad de la dimensión de Krull de anillo locales noetherianos (las otras dos nociones de dimensión eran ya finitas por definición). En particular, hemos probado el siguiente:

Corolario 1.4.14. *Si $(R, \mathfrak{m})$ es un anillo local noetheriano se tiene:*

$$dim_{Kr}(R) = ht(\mathfrak{m}) < +\infty. \tag{1.4.7}$$

Del mismo modo, si M es un R-módulo finitamente generado tenemos:

i) $dim_{Kr}(M) \leq dim_{Kr}(R) < +\infty$.

ii) $coht(\mathfrak{p}) < +\infty$, para todo $\mathfrak{p} \in Supp(M)$.

Si R' es un anillo noetheriano cualquiera, tenemos:

$$ht(\mathfrak{q}) < +\infty, \ \ \forall \mathfrak{q} \in Spec(R'). \tag{1.4.8}$$

Demostración. Por una parte, notemos que $Ann_R(R) = (0)$, luego $Supp(R) = Spec(R)$. Además, como $(R, \mathfrak{m})$ es un anillo local, $\mathfrak{p} \subseteq \mathfrak{m}$ para todo $\mathfrak{p} \in Spec(R)$. Por tanto,

$$\begin{aligned} dim_{Kr}(R) &= sup\,\{coht(\mathfrak{p}) : \ \mathfrak{p} \in Spec(R)\} \\ &= sup\,\{r : \ \exists \{\mathfrak{p}_0, \ldots, \mathfrak{p}_r\} \subseteq Spec(R) : \ \mathfrak{p} = \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_r = \mathfrak{m}\} = ht(\mathfrak{m}). \end{aligned}$$

Para un $(R, \mathfrak{m})$-módulo M, es claro que

$$Supp(M) \subseteq Spec(R) = Supp(R).$$

Por el apartado $i)$ de la Proposición 1.4.12,

$$dim_{Kr}(R/\mathfrak{p}) = coht(\mathfrak{p}) \leq sup\,\{coht(\mathfrak{q}) : \ \mathfrak{q} \in Spec(R)\} = dim_{Kr}(R), \quad \forall \mathfrak{p} \in Spec(R),$$

con lo que se siguen las propiedades $i)$ y $ii)$.

Finalmente, como R' es un anillo noetheriano, en virtud de la Proposición A.8.1, $R'_{\mathfrak{q}}$ es un anillo local noetheriano para cada $\mathfrak{q} \in Spec(R')$. Por la Desigualdad (1.4.7) se tiene que $dim(R'_{\mathfrak{q}}) < +\infty$. En virtud del apartado $ii)$ de la Proposición 1.4.12,

$$ht(\mathfrak{q}) = dim_{Kr}(R'_{\mathfrak{q}}) < +\infty,$$

y queda probada la Desigualdad (1.4.8). □

Observación 9. *Aunque todo anillo local noetheriano tiene dimensión de Krull finita, esto no es cierto para cualquier anillo noetheriano ni, menos aún, para anillos no noetherianos. Ver ejemplos en* [**Nagata, 1962**] *y* [**Gordon-Jobson, 1973**].

Un resultado importante para el que el Teorema de la Dimensión es una herramienta especialmente útil de la que nos serviremos más adelante es el Teorema del Ideal Principal de Krull:

Lema 1.4.15. *Sea R un anillo noetheriano y $\mathfrak{a}$ un ideal de R generado por r elementos. Entonces, todo ideal primo minimal $\mathfrak{p}$ de R que contiene a $\mathfrak{a}$ verifica $ht(\mathfrak{p}) \leq r$.*

Demostración. Considérese el anillo local $(R_{\mathfrak{p}}, \mathfrak{p}R_{\mathfrak{p}})$.

Afirmación. $Supp(R_{\mathfrak{p}}/\mathfrak{a}R_{\mathfrak{p}}) = \{\mathfrak{p}R_{\mathfrak{p}}\}$.

DEMOSTRACIÓN. Por una parte, si $x \in Ann_{R_\mathfrak{p}}(R_\mathfrak{p}/\mathfrak{a}R_\mathfrak{p})$, $xy \in \mathfrak{a}R_\mathfrak{p} \subseteq \mathfrak{p}R_\mathfrak{p}$ para todo $y \in (R_\mathfrak{p} \setminus \mathfrak{p}R_\mathfrak{p})/(\mathfrak{a}R_\mathfrak{p})$. Entonces $xy \in \mathfrak{p}R_\mathfrak{p}$, $y \notin \mathfrak{p}R_\mathfrak{p}$, por la primalidad de $\mathfrak{p}R_\mathfrak{p}$ se tiene $x \in \mathfrak{p}R_\mathfrak{p}$. En virtud del apartado *iii*) de la Proposición A.10.11, $\mathfrak{p}R_\mathfrak{p} \in Supp(R_\mathfrak{p}/\mathfrak{a}R_\mathfrak{p})$. Por otra parte, en virtud del Corolario A.2.5, cualquier ideal primo de $R_\mathfrak{p}$ es de la forma $\mathfrak{q}R_\mathfrak{p}$ donde $\mathfrak{q}$ es un ideal primo de R contenido en $\mathfrak{p}$. Más aún, si $\mathfrak{q}R_\mathfrak{p} \subsetneq \mathfrak{p}R_\mathfrak{p}$, entonces $\mathfrak{q} \subseteq \mathfrak{p}$. De ser este el caso, por minimalidad de $\mathfrak{p}$ se tiene que $\mathfrak{q} \subsetneq \mathfrak{a} \subseteq \mathfrak{p}$. Sea $a \in \mathfrak{a}$, $a \notin \mathfrak{q}$. Entonces $\frac{a}{1} \notin \mathfrak{q}R_\mathfrak{p}$. Pero $\frac{a}{1} \in Ann_{R_\mathfrak{p}}(R_\mathfrak{p}/\mathfrak{a}R_\mathfrak{p})$. Luego $Ann_{R_\mathfrak{p}}(R_\mathfrak{p}/\mathfrak{a}R_\mathfrak{p}) \nsubseteq \mathfrak{q}R_\mathfrak{p}$ y por el apartado *iii*) de la Proposición A.10.11, $\mathfrak{q}R_\mathfrak{p} \notin Supp(R_\mathfrak{p}/\mathfrak{a}R_\mathfrak{p})$. □

Ahora bien, como $Supp(R_\mathfrak{p}/\mathfrak{a}R_\mathfrak{p}) = \{\mathfrak{p}R_\mathfrak{p}\}$ y $\mathfrak{p}R_\mathfrak{p}$ es maximal, en virtud de la Proposición A.10.13, $R_\mathfrak{p}/\mathfrak{a}R_\mathfrak{p}$ es de longitud finita como $R_\mathfrak{p}$-módulo, y también lo será $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ viéndolo como un submódulo del anterior mediante la proyección natural $R_\mathfrak{p}/\mathfrak{a}R_\mathfrak{p} \longrightarrow R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ (cf. Corolario A.9.7). Ahora, como $\mathfrak{p}$ (y, en consecuencia, $\mathfrak{p}R_\mathfrak{p}$) está generado por r elementos, se tiene que $dim_{Chev}(R_\mathfrak{p}) \leq r$. Finalmente, en virtud del Teorema de la Dimensión Local (ver Teorema 1.4.13) y el apartado *ii*) de la Proposición 1.4.12, se tiene:

$$ht(\mathfrak{p}) = dim_{Kr}(R_\mathfrak{p}) = dim_{Chev}(R_\mathfrak{p}) \leq r.$$

□

DEFINICIÓN 20. *Sea R un anillo, una sucesión regular de longitud r es una cadena de elementos $a_1, \ldots, a_r \in R$ tales que se verifican las propiedades siguientes:*

i) *$\mathfrak{a} = (a_1, \ldots, a_r)$ es un ideal propio de R (i.e. $\mathfrak{a} \subsetneq R$)*

ii) *Para cada i, $1 \leq i \leq r$ el elemento a_i no es un divisor de cero en $R/(a_1, \ldots, a_{i-1})$*

TEOREMA 1.4.16 (**Teorema del Ideal Principal de Krull**). *Sea R un anillo noetheriano y $\mathfrak{a} = (a_1, \ldots, a_r)$ un ideal propio de R. Entonces*

i) *Para cada ideal primo $\mathfrak{p} \in Spec(R)$, minimal sobre $\mathfrak{a}$ se tiene*

$$ht(\mathfrak{p}) \leq r.$$

ii) *Si la sucesión $a_1, \ldots, a_r \in R$ es una sucesión regular en R, entonces para cada ideal primo $\mathfrak{p} \in Spec(R)$, minimal sobre el ideal $\mathfrak{a}$, se tiene*

$$ht(\mathfrak{p}) = r.$$

DEMOSTRACIÓN. La primera parte del Teorema está demostrada en el Lema 1.4.15.
Probemos *ii*) por inducción en r. Supongamos $r = 1$, como a_1 es una sucesión regular, a_1 no es divisor de cero en R. En virtud de la Proposición A.10.5, se tiene que

$$a_1 \notin \bigcup_{\mathfrak{q} \in Ass_R(R)} \mathfrak{q}.$$

Por tanto, se verifica $a_1 \notin \mathfrak{q}$ para todo $\mathfrak{q} \in Ass_R(R)$. Ahora, si $x \in Ann_R({}^{R}/_{(a_1)})$, $xy \in (a_1) \subseteq \mathfrak{p}$ para todo $y \in R \backslash \mathfrak{p}$. Por primalidad de $\mathfrak{p}$ se tiene que $x \in \mathfrak{p}$ y, en consecuencia, $\mathfrak{p} \supseteq Ann_R({}^{R}/_{(a_1)})$. En virtud del apartado *iii*) de la Proposición A.10.11, $\mathfrak{p} \in Supp({}^{R}/_{(a_1)})$. De otro lado, como $\mathfrak{p} \supseteq Ann_R({}^{R}/_{(a_1)}) \supseteq Ann_R(R)$, por el apartado *ii*) de la Proposición A.10.11, existe $q \in Ass_R(R)$ con $\mathfrak{q} \subseteq \mathfrak{p}$. Pero como $a_1 \notin \mathfrak{q}$ se tiene la cadena $\mathfrak{q} \subsetneq \mathfrak{p}$ y $ht(\mathfrak{p}) \geq 1$. Por *i*), debe ser $ht(\mathfrak{p}) = 1$.
Sea $r > 1$. Como $a_1, \ldots, a_r \in R$ es una sucesión regular, a_r no es divisor de cero de $R/(a_1, \ldots, a_{r-1})$. En virtud de la Proposición A.10.5,

$$a_r \notin \bigcup_{\mathfrak{q} \in Ass_R({}^{R}/_{(a_1, \ldots, a_{r-1})})} \mathfrak{q}.$$

Por tanto, se verifica $a_r \notin \mathfrak{q}$ para todo $\mathfrak{q} \in Ass_R({}^{R}/_{(a_1, \ldots, a_{r-1})})$. Ahora bien, si se tiene $x \in Ann_R({}^{R}/_{(a_1, \ldots, a_{r-1})})$, entonces $xy \in (a_1, \ldots, a_{r-1}) \subseteq (a_1, \ldots, a_r) \subseteq \mathfrak{p}$ para todo $y \in R \setminus \mathfrak{p}$. En consecuencia, $x \in \mathfrak{p}$. Por tanto $\mathfrak{p} \supseteq Ann_R({}^{R}/_{(a_1, \ldots, a_{r-1})})$. En virtud del apartado *ii*) de la Proposición A.10.11, existe $\mathfrak{q} \in Ass_R({}^{R}/_{(a_1, \ldots, a_{r-1})})$ minimal sobre $(a_1, \ldots, a_{r-1})$ tal que $\mathfrak{q} \subseteq \mathfrak{p}$. Pero como $a_r \in \mathfrak{p}$ y $a_r \notin \mathfrak{q}$ para todo $\mathfrak{q} \in Ass_R({}^{R}/_{(a_1, \ldots, a_{r-1})})$, se tiene que $\mathfrak{q} \subsetneq \mathfrak{p}$. Ahora, por hipótesis inductiva se sigue que $ht(\mathfrak{q}) = r - 1$. En consecuencia, $ht(\mathfrak{p}) \geq r$. Finalmente, en virtud del apartado *i*), $ht(\mathfrak{p}) = r$. □

1.5. Anillos Locales Regulares

Sea $(R, \mathfrak{m})$ un anillo local noetheriano. En virtud del Corolario 1.4.14, R es de dimensión finita. Sea $r = dim_{Kr}(R)$. El Teorema de la Dimensión Local (ver Teorema 1.4.13) garantiza que $dim_{Chev}(R) = r$ y, en consecuencia, $\mathfrak{m}$ no puede estar generado por menos de r elementos. Como usualmente, escribiremos $k = k(\mathfrak{m}) = R/\mathfrak{m}$ para denotar el cuepo de restos módulo $\mathfrak{m}$ del anillo local $(R, \mathfrak{m})$.

DEFINICIÓN 21. *Con las notaciones precedentes, un anillo local notheriano $(R, \mathfrak{m})$ se dice regular si $\mathfrak{m}$ posee un conjunto generador de cardinal igual a $r = dim_{Kr}(R)$.*

El siguiente Lema expone un resultado clásico, adaptado al caso de anillos locales, consecuencia del Lema de Nakayama. El lector puede acudir a [**Pardo, 21**] para una prueba.

LEMA 1.5.1. *Sea $(R, \mathfrak{m})$ un anillo local de cuerpo residual $k := R/\mathfrak{m}$ y M un R-módulo finitamente generado. Entonces, son equivalentes:*

i) $\{x_1, \ldots, x_n\}$ generan M como R-módulo;
ii) $\{\bar{x}_1, \ldots, \bar{x}_n\}$ generan $M/\mathfrak{m}M$ como k-espacio vectorial,

donde, para cada i, $1 \leq 1 \leq n$, $\bar{x}_i$ es la clase de x_i módulo $\mathfrak{m}M$.

PROPOSICIÓN 1.5.2. *Sea $(R, \mathfrak{m})$ un anillo local, $k := R/\mathfrak{m}$ su cuerpo residual, M un R-módulo finitamente generado y $M/\mathfrak{m}M$ el k-espacio vectorial correspondiente. Sea $\{x_1, \ldots, x_n\} \subseteq M$ un conjunto generador M y sean $\{\bar{x}_1, \ldots, \bar{x}_n\} \subseteq M/\mathfrak{m}M$ sus clases residuales módulo $\mathfrak{m}M$. Son equivalentes:*

i) $\{x_1, \ldots, x_n\}$ es un conjunto de generadores de M de cardinal minimal;
ii) $\{\bar{x}_1, \ldots, \bar{x}_n\}$ forman una base de $M/\mathfrak{m}M$ como k-espacio vectorial.

DEMOSTRACIÓN. Si $\bar{S} = \{\bar{x_1}, \ldots, \bar{x_n}\}$ genera $M/\mathfrak{m}M$ como k-espacio vectorial y no es base, entonces S no es minimal. Por consiguiente, existe un conjunto de cardinal $s < n$ que genera $M/\mathfrak{m}M$ como k-espacio vectorial y, por el Lema 1.5.1 precedente, existirá un conjunto de cardinal $s < n$ que genere M como R-módulo. En consecuencia, $S = \{x_1, \ldots, x_n\}$ no es un conjunto generador minimal de M.
Recíprocamente, si S no es un conjunto generador minimal de $\mathfrak{m}$, existirá un conjunto generador de cardinal $s < n$ que genere $\mathfrak{m}$ como ideal de R y, por el Lema 1.5.1, habrá un conjunto de cardinal $s < n$ que genere $M/\mathfrak{m}M$ como k-espacio vectorial. En consecuencia, $\bar{S}$ no puede ser base. □

PROPOSICIÓN 1.5.3. *Sea $(R, \mathfrak{m})$ un anillo local noetheriano de cuerpo residual $k := R/\mathfrak{m}$ y sea $r = dim_{Kr}(R)$. Entonces, las siguientes condiciones son equivalentes:*

i) R es regular;
ii) la dimensión del k-espacio vectorial $\mathfrak{m}/\mathfrak{m}^2$ es igual a r;
iii) La aplicación:

$$\varphi : k[X_1, \ldots, X_r] = \bigoplus_{n \in N} H_n(X_1, \ldots, X_r) \longrightarrow \bigoplus_{n \in \mathbb{N}} \mathfrak{m}^n/\mathfrak{m}^{n+1} = G_{\mathfrak{m}}(R)$$

es un isomorfismo de $k-$álgebras graduadas.

DEMOSTRACIÓN. $ii) \Rightarrow i)$ Como $(R, \mathfrak{m})$ es un anillo local noetheriano, el ideal $\mathfrak{m}$ es un R-módulo finitamente generado. Aplicando la Proposición 1.5.2 precedente a $M = \mathfrak{m}$, $\mathfrak{m}$ admite un conjunto generador de r elementos y, en consecuencia, R es regular.
$iii) \Rightarrow ii)$ Sea $\varphi : k[X_1, \ldots, X_r] \longrightarrow G_{\mathfrak{m}}(R)$ un isomorfismo de k-álgebras graduadas. Entonces, la aplicación:

$$\varphi_n : H_1(X_1, \ldots, X_r) \longrightarrow \mathfrak{m}/\mathfrak{m}^2$$

es un isomorfismo de k-espacios vectoriales (ver la demostración de la Proposición 1.4.10) y, por consiguiente, $dim_k(\mathfrak{m}/\mathfrak{m}^2) = dim_k(H_1(X_1, \ldots, X_r)$. Pero

$$dim_k(H_1(X_1, \ldots, X_r)) = \binom{r}{r-1} = r.$$

En consecuencia, $dim_k(\mathfrak{m}/\mathfrak{m}^2) = r$.
$i) \Rightarrow iii)$ Sea $\{x_1, \ldots, x_r\}$ un conjunto generador de $\mathfrak{m}$. Como $dim_{Kr}(R) = r$, r es el mínimo

de los cardinales de los posibles conjuntos que generan $\mathfrak{m}$ como ideal de R. Ahora bien, como $dim_{Kr}(R) = dim_C hev(R) = deg(P_{\mathfrak{m}}(R, -)) = r$, en virtud del Corolario 1.4.11,

$$\varphi : k[X_1, \ldots, X_r] \longrightarrow G_{\mathfrak{m}}(R)$$

es isomorfismo. □

COROLARIO 1.5.4. *Todo anillo local regular $(R, \mathfrak{m})$ de cuerpo residual $k := R/\mathfrak{m}$ es dominio de integridad.*

DEMOSTRACIÓN. En virtud de la Proposición anterior, $G_{\mathfrak{m}}(R) \cong k[X_1, \ldots, X_r]$. Ahora bien, como $k[X_1, \ldots, X_r]$ es dominio de integridad, $G_{\mathfrak{m}}(R)$ también lo es. Finalmente, como $G_{\mathfrak{m}}(R)$ es dominio de integridad, por el Corolario 1.3.5, se sigue que R es dominio de integridad. □

DEFINICIÓN 22. *Sea $(R, \mathfrak{m})$ un anillo local regular tal que $dim_{Kr}(R) = r$. Se llama sistema regular de parámetros de R a cualquier conjunto generador de $\mathfrak{m}$ de cardinal r.*

OBSERVACIÓN 10. *Notemos que, dado $(R, \mathfrak{m})$ anillo local regular de dimensión, cualquier sistema regular de parámetros es un conjunto generador minimal de $\mathfrak{m}$.*

PROPOSICIÓN 1.5.5. *Sean $(R, \mathfrak{m})$ un anillo local de cuerpo residual $k := R/\mathfrak{m}$ con $dim_{Kr}(R) = r$, y sea $\{a_1, \ldots, a_j\}$, $0 \leq j \leq r$ un subconjunto de $\mathfrak{m}$. Entonces, las siguientes afirmaciones son equivalentes:*

i) *$\{a_1, \ldots, a_j\}$ es subconjunto de un sistema regular de parámetros de R;*
ii) *las imágenes $\bar{a}_1, \ldots, \bar{a}_j$ de $a_1, \ldots, a_j$ respectivamente por la proyección canónica: $\pi : \mathfrak{m} \longrightarrow \mathfrak{m}/\mathfrak{m}^2$, son linealmente independientes sobre k;*
iii) *$R/(a_1, \ldots, a_j)$ es un anillo local regular de dimensión $r - j$.*

DEMOSTRACIÓN. *i)* $\Leftrightarrow$ *ii)* Sea $\{a_1, \ldots, a_j\}$ un subconjunto de un sistema regular de parámetros $S = \{a_1, \ldots, a_j, a_{j+1}, \ldots, a_r\}$. Como S es un conjunto generador minimal de $\mathfrak{m}$, en virtud de la Proposición 1.5.2, el conjunto $\bar{S} = \{\bar{a}_1, \ldots, \bar{a}_j, \bar{a}_{j+1}, \ldots, \bar{a}_r\}$ es una base para el $k-$espacio vectorial $\mathfrak{m}/\mathfrak{m}^2$. En particular, $\bar{a}_1, \ldots, \bar{a}_j$ son linealmente independientes.
Recíprocamente, si $\bar{a}_1, \ldots, \bar{a}_j$ son linealmente independientes sobre k, se puede construir una base para el k-espacio vectorial $\mathfrak{m}/\mathfrak{m}^2$ $B = \{\bar{a}_1, \ldots, \bar{a}_j, b_1, \ldots, b_{r-j}\}$. Notemos que, en virtud de la Proposición 1.5.3, debe ser $dim_k(\mathfrak{m}/\mathfrak{m}^2) = r$. Además, como $\pi : \mathfrak{m} \longrightarrow \mathfrak{m}/\mathfrak{m}^2$ es suprayectiva, para cada i, $1 \leq i \leq r - j$ podemos tomar $b_i = \pi(a_{i+j}) = \bar{a}_{i+j}$ para algún $a_{i+j} \in \mathfrak{m}$. De esta forma, como $B = \{\bar{a}_1, \ldots, \bar{a}_j, \bar{a}_{j+1}, \ldots, \bar{a}_r\}$ es base para el k-espacio vectorial $\mathfrak{m}/\mathfrak{m}^2$, $S = \{a_1, \ldots, a_j, a_{j+1}, \ldots, a_r\}$ es un conjuto generador de $\mathfrak{m}$ de cardinal r. En consecuencia, S es un sistema regular de parámetros de R con $\{a_1, \ldots, a_j\} \subseteq S$.
i) $\Rightarrow$ *iii)* Sean $\bar{R} = {}^{R}/_{(a_1, \ldots a_j)}$, $\bar{\mathfrak{m}} = {}^{\mathfrak{m}}/_{(a_1, \ldots, a_j)}$, $\{a_1, \ldots, a_j, a_{j+1}, \ldots, a_r\}$ un sistema regular de parámetros de R. Como existe una correspondencia biyectiva que preserva el orden entre los ideales de $\bar{R}$ y los ideales de R que contienen a $(a_1, \ldots a_j)$, el anillo $(\bar{R}, \bar{m})$ es local. Además, como $a_1, \ldots, a_r$ generan $\mathfrak{m}$, $a_{j+1}, \ldots, a_r$ generan $\bar{\mathfrak{m}}$. En virtud del Teorema 1.4.5, $dim_{Kr}(\bar{R}) = deg(P_{\bar{\mathfrak{m}}}(\bar{R}, -)) \leq r - j$. Sea $s = dim_{Kr}(\bar{R}) = dim_{Chev}(\bar{R})$ y sean $\bar{b}_1, \ldots, \bar{b}_s \in \bar{\mathfrak{m}}$ tales que ${}^{\bar{R}}/_{(\bar{b}_1, \ldots, \bar{b}_s)}$ es de longitud finita, donde para cada i, $1 \leq i \leq s$, $\bar{b}_i$ es la imagen de algún $b_i \in \mathfrak{m}$ mediante la proyección canónica $\mathfrak{m} \longrightarrow {}^{\mathfrak{m}}/_{(a_1, \ldots, a_j)} = \bar{\mathfrak{m}}$. Entonces, como

$${}^{R}/_{(a_1, \ldots, a_j, b_1, \ldots, b_s)} \cong {}^{R/(a_1, \ldots, a_j)}/_{(\bar{b}_1, \ldots, \bar{b}_s)} = {}^{\bar{R}}/_{(\bar{b}_1, \ldots, \bar{b}_s)},$$

se sigue que ${}^{R}/_{(a_1, \ldots, a_j, b_1, \ldots, b_s)}$ es de longitud finita y, por tanto, $r = dim_{Kr}(R) = dim_{Chev}(R) \leq j + s$, es decir, $r - j \leq s$. Pero se tenía que $s \leq r - j$. Por tanto, debe ser $dim_{Kr}(\bar{R}) = s = r - j$.
iii) $\Rightarrow$ *i)* Sea $\{\bar{a}_{j+1}, \ldots, \bar{a}_r\}$ un sistema regular de parámetros de $\bar{R}$, donde para cada i, $j + 1 \leq i \leq r$, $\bar{a}_i$ es la imagen de $a_i \in \mathfrak{m}$ por la proyección canónica $\mathfrak{m} \longrightarrow \bar{\mathfrak{m}} = {}^{\mathfrak{m}}/_{(a_1, \ldots a_j)}$. Como $\bar{\mathfrak{m}} \cap (a_1, \ldots, a_j) = \{0\}$, en virtud del Segundo Teorema de Isomorfía,${}^{\mathfrak{m}}/_{(a_1, \ldots, a_j)} = \bar{\mathfrak{m}} \cong {}^{(\mathfrak{m} + (a_1, \ldots, a_j))}/_{(a_1, \ldots, a_j)}$. Ahora, en virtud del Tercer Teorema de Isomorfía, $\mathfrak{m} \cong \bar{\mathfrak{m}} + (a_1, \ldots, a_j)$. Como $\{\bar{a}_{j+1}, \ldots, \bar{a}_r, a_1, \ldots, a_r\}$ generan $\bar{\mathfrak{m}} + (a_1, \ldots, a_j)$, el isomorfismo $\varphi : \bar{\mathfrak{m}} + (a_1, \ldots, a_j) \longrightarrow \mathfrak{m}$ estará determinado por las imágenes de dicho conjunto generador. Tomando $\varphi(a_i) := a_i$ para $1 \leq i \leq j$ y $\varphi(\bar{a}_i) := a_i$ para $j + 1 \leq i \leq r$, se tiene que $\{a_1, \ldots, a_j, a_{j+1}, \ldots, a_r\}$ es un sistema generador de $\mathfrak{m}$ de cardinal r y, por tanto, un sistema regular de parámentros de R con $\{a_1, \ldots, a_j\} \subseteq S$. □

PROPOSICIÓN 1.5.6. *Sea* $(R, \mathfrak{m})$ *un anillo local regular de cuerpo residual* $k := R/\mathfrak{m}$ *y de dimensión* r*; sea* $\{a_1, \ldots, a_j\}$ *un subconjunto de un sistema regular de parámetros de* R*. Entonces, el ideal* $\mathfrak{p} = (a_1, \ldots, a_j)$ *es un ideal primo de altura* j*.*

DEMOSTRACIÓN. En virtud de la Proposición 1.5.5 precedente, $R/\mathfrak{p}$ es un anillo local regular y, por el Corolario 1.5.4, $R/\mathfrak{p}$ es dominio de integridad. En consecuencia, $\mathfrak{p}$ es un ideal primo. Probemos que $ht(\mathfrak{p}) = j$ por inducción en j. Si $j = 0$, $\mathfrak{p} = 0$ y $ht(\mathfrak{p}) = 0$.
Sea $j \geq 1$. Se tiene, por hipótesis inductiva que el ideal $(a_1, \ldots, a_{j-1})$ es un ideal primo de altura $j - 1$.

AFIRMACIÓN. $\{a_1, \ldots, a_j\}$ *es un conjunto generador minimal de* $\mathfrak{p}$*.*

DEMOSTRACIÓN. Por una parte, como $\{a_1, \ldots, a_j\}$ es conjunto generador de $\mathfrak{p}$, la proyección $\mathfrak{p} \longrightarrow \mathfrak{p}/(\mathfrak{m}\mathfrak{p})$ garantiza que $\{a_1 \bmod (\mathfrak{m}\mathfrak{p}), \ldots, a_j \bmod (\mathfrak{m}\mathfrak{p})\}$ es un conjunto generador de $\mathfrak{p}/(\mathfrak{m}\mathfrak{p})$. Por otra parte, en virtud del apartado *ii*) de la Proposición 1.5.5, las imágenes $\bar{a_1}, \ldots, \bar{a_j}$ de $a_1, \ldots, a_j$ respectivamente mediante la proyección $\pi : \mathfrak{m} \longrightarrow \mathfrak{m}/\mathfrak{m}^2$ son linealmente independientes sobre k. Ahora, como $\mathfrak{p}\mathfrak{m} \subseteq \mathfrak{m}^2$ se tiene que, para cada i, $1 \leq i \leq j$, $a_i \bmod (\mathfrak{p}\mathfrak{m}) = a_i \bmod \mathfrak{m}^2 = \bar{a_i}$. Por consiguiente, $\bar{a_1}, \ldots, \bar{a_j} \in \mathfrak{p}/\mathfrak{m}\mathfrak{p}$ son linealmente independientes sobre k. En virtud de la Proposición 1.5.2, $\{a_1, \ldots, a_j\}$ es un conjunto generador minimal de $\mathfrak{p}$. □

La Afirmación precedente garantiza la contención estricta $(a_1, \ldots, a_{j-1}) \subsetneq \mathfrak{p}$. En consecuencia, $ht(\mathfrak{p}) \geq j$. De otro lado, aplicando el Lema 1.4.15 al ideal $\mathfrak{p}$, se sigue que $ht(\mathfrak{p}) \leq j$. Por consiguiente, $ht(\mathfrak{p}) = j$. □

PROPOSICIÓN 1.5.7. *Sea* $(R, \mathfrak{m})$ *un anillo local noetheriano de cuerpo residual* $k := R/\mathfrak{m}$*. Entonces,* R *es regular si y solamente si* $\mathfrak{m}$ *está generado por una sucesión regular en* R*.*

DEMOSTRACIÓN. Supongamos que R es regular y $\{a_1 \ldots, a_r\}$ un sistema regular de parámetros de R. Probemos que $a_1, \ldots a_r$ es una sucesión regular por inducción en r. Si $r = 1$, entonces $\mathfrak{m} = (a_1)$ y $dim_{Kr}(R) = r = 1$. Por reducción al absurdo, si a_1 fuese divisor de cero de R, por la Proposición A.10.5, $a_1 \in \bigcup_{\mathfrak{q} \in Ass(R)} \mathfrak{q}$. En consecuencia, $\mathfrak{m} = (a_1) \subseteq \bigcup_{\mathfrak{q} \in Ass(R)} \mathfrak{q}$. Ahora, por el Lema A.2.1, existe $\mathfrak{q} \in Ass(R)$ tal que $\mathfrak{m} \subseteq \mathfrak{q}$. Por maximalidad de $\mathfrak{m}$, debe ser $\mathfrak{q} = \mathfrak{m}$. Con lo que se sigue que $dim_{Kr}(R) = r = 0$, lo cual contradice la hipótesis $r = 1$.
Supongamos $r > 1$, por hipótesis inductiva, $\{a_1, \ldots, a_{r-1}\}$ es una sucesión regular. Por tanto, solo queda probar que a_r no es divisor de cero de $R/(a_1, \ldots a_{r-1})$. Como $\{a_1, \ldots, a_{r-1}\}$ es un subconjunto del sistema regular de parámetros $\{a_1, \ldots, a_r\}$, en virtud de la Proposición 1.5.5 y con las notaciones utilizadas en la misma, tomando $j = r - 1$ se sigue que $(\bar{R}, \bar{\mathfrak{m}})$ es un anillo local regular de dimensión $r - (r - 1) = 1$, donde $\bar{R} = R/(a_1, \ldots a_{r-1})$ y $\bar{\mathfrak{m}} = \mathfrak{m}/(a_1, \ldots, a_{r-1})$. Además, como $a_1 \ldots, a_r$ generan $\mathfrak{m}$, la imagen de a_r por la proyección $R \longrightarrow \bar{R}$ genera $\bar{\mathfrak{m}}$. Ahora bien, si a_r fuese divisor de cero de $\bar{R}$, entonces, siguiendo el mismo razonamiento que en el caso $r = 1$, se tendría que $\bar{\mathfrak{m}} \in Ass(\bar{R})$. En consecuencia, se concluiría que $dim_{Kr}(\bar{R}) = 0$, lo cual es una contradicción.
De otro lado, supongamos que $a_1 \ldots, a_r$ es una sucesión regular. Notemos que, como $(R, \mathfrak{m})$ es un anillo local noetheriano, por el Corolario 1.4.14, $dim_{Kr}(R) = ht(\mathfrak{m})$. Ahora, tomando $\mathfrak{p} = \mathfrak{m} = (a_1 \ldots, a_r)$ en el apartado *ii*) del Teorema 1.4.16, se sigue que $dim_{Kr}(R) = ht(\mathfrak{m}) = r$. En consecuencia, $(R, \mathfrak{m})$ es un anillo local regular de dimensión r. □

CAPíTULO 2

Dimensión Homológica. Teorema de Serre-Auslander-Buchsbaum

Índice

2.1. Introducción

Este capítulo está dedicado a culminar el Trabajo Fin de Grado. Dos son los propósitos esenciales de su contenido. De una parte, como se indicaba en la Introducción, nos ocupamos de introducir los elementos esenciales del Álgebra Homológica que fueron usados por J.P. Serre, M. Auslander y D.A. Buchsbaum para desembarcar con nuevas herramientas en el contexto del Álgebra Conmutativa a la manera de E. Noether, E. Artin o B.L. van der Waerden. De otro lado, se muestra cómo esos elementos son utilizados para responder a las preguntas sobre anillos locales regulares en la forma de los Teoremas de Serre y Auslander-Buchsbaum.

Más concretamente, los instrumentos de Álgebra Homológica que se introducen son los siguientes:
En primer lugar trabajaremos en la categoría de $R - \mathcal{M}od$, cuyos objetos son los R-módulos sobre un anillo fijado y cuyos morfismos son los elementos de $Hom_R(M, N)$. En la Sección 2.2 introduciremos el lenguaje de complejos de cadena y co-cadena, los módulos de homología y co-homología y la relación de homotopía. Dada la restricción de páginas en la normativa de Trabajo Fin de Grado, hemos optado por introducir en esta Sección solamente las nociones, comentarios y enunciados de los resultados principales. En la Sección B.1 del Apéndice B hemos incluido los mismos resultados con demostración completa de todos ellos. Seguidamente nos ocupamos de demostrar la existencia de resolución proyectiva de R-módulos, así como algunas propiedades esenciales (con demostraciones). Con estas herramientas, introducimos los bi-functores Tor en la Seccion 2.4. Hacemos una introducción completa (con demostraciones detalladas) de las nociones y sus principales propiedades. La Sección 2.5 siguiente se dedica a los bi-functores Ext. Esta vez, por causa de las limitaciones de páginas, nos limitamos a presentar las nociones y sus propiedades (enunciados) esenciales. Hemos dispuesto la Sección B.2 del Apéndice B para exponer las demostraciones completas de esta construcción del bi-functor Ext y sus propiedades.

En segundo lugar, nos ocupamos del uso de esas herramientas en relación con los anillos locales regulares, objeto de esta memoria. Además de las nociones de dimensión usadas en el Teorema de la Dimensión Local, introduciremos la dimensión homológica, la dimensión inyectiva y la dimensión global de anillos en las Secciones 2.6 y 2.7 (completas). Con ellas llegamos al primer resultado esencial de esta memoria: el Teorema 2.8.5, que afirma que un anillo local noetheriano es local regular si y solamente si su dimensión homológica es finita, en cuyo caso la dimensión global coincide con su dimensión de Krull. Armado con esta caracterización, J.P. Serre pudo resolver la primera de las conjeturas (Teorema 2.8.6): Ser local regular es una propiedad local, esto es, un anillo local noetheriano $(R, \mathfrak{m})$ es regular si y solamente si todas sus localizaciones $R_\mathfrak{p}$, por un primo $\mathfrak{p} \in Spec(R)$, son anillos locales regulares. Finalmente, la Sección 2.9 es dedicada a probar el Teorema de Auslander-Buchsbaum (Teorema 2.9.7): todo anillo local regular es dominio de factorización única.

2.2. Complejos de Cadena y Co-cadena, Homología y Co-homología.

Como ya se indicó en la Introducción precedente, las demostraciones de los resultados descritos en esta Sección pueden seguirse en la Sección B.1 del Apéndice B. Asimismo, recordamos que nuestra categoría es la categoría $R - \mathcal{M}od$ antes descrita.

Definición 23. *Sea R un anillo y $\mathcal{M} := \{M_n : n \in \mathbb{Z}\}$ una familia numerable de R-módulos.*

- *i) Un complejo de cadena con soporte $\mathcal{M}$ es un par $\{\mathcal{M}, \mathcal{D}\}$ donde $\mathcal{D} = \{d_n : n \in Z\}$ es una familia numerable de morfismos $d_n \in Hom_R(M_n, M_{n-1})$ de tal modo que $d_{n-1} \circ d_n = 0$.*
- *ii) Un complejo de co-cadena con soporte $\mathcal{M}$ es un par $(\mathcal{M}, \mathcal{C})$ donde $\mathcal{C} = \{c^n : n \in \mathbb{Z}\}$ es una familia numerable de morfismos $c^n \in Hom_R(M_n, M_{n+1})$ de tal forma que $c^{n+1} \circ c_n = 0$*

Los complejos de cadena y co-cadena se representan usualmente mediante:

(2.2.1) C. cadena $\underline{M}$ $$\ldots \xrightarrow{d_{n+1}} M_n \xrightarrow{d_n} M_{n-1} \xrightarrow{d_{n-1}} M_{n-2} \xrightarrow{d_{n-2}} \ldots$$

(2.2.2) C. co-cadena $\overline{M}$ $$\ldots \xrightarrow{c^{n-1}} M^n \xrightarrow{c_n} M^{n+1} \xrightarrow{c^{n+1}} M^{n+2} \xrightarrow{c^{n+2}} \ldots$$

El paso de complejos de cadena a complejos de co-cadena puede hacerse mediante *dualización*. Tomemos el functor contravariante $Hom_R(-, R)$ (cf. Sección A.3 del Apéndice A). Así, dado un comlejo de cadena como (2.2.1), podemos definir $N^n := Hom_(M_n, R)$ y $c^{n-1} := Hom_R(d_n, R)$ y tendremos un complejo de co-cadena $(N^n, \{c^n\}_{n\in\mathbb{Z}})$.

- i) Dado un complejo de cadena como (2.2.1), al índice del R-módulo M_n se le llama *grado*. Los elementos de $ker(d_n)$ denominan *ciclos de grado n*, mientras que a los elementos de $Im(d_{n+1})$ se les denomina *bordes de grado n* del complejo. El *n-ésimo módulo de homología* se define como el R-módulo cociente:
$$H_n(\underline{M}) = {}^{ker(d_n)}/_{Im(d_{n+1})}.$$
- ii) Igualmente, para un complejo de co-cadena como (2.2.2), los elementos de $ker(c^n)$ se denominan *co-ciclos de grado n*; los elementos de $= Im(c^{n-1})$ se denominan *co-bordes de grado n* y al R-módulo cociente siguiente se le denomina *n-ésimo módulo de co-homología*:
$$H^n(\overline{M} = {}^{ker(c^n)}/_{Im(c^{n-1})}.$$

Un complejo de cadena (respectivamente co-cadena) de R-módulos $\underline{M}$ (resp. $\overline{M}$) es una sucesión exacta de R-módulos si y solamente si todos sus módulos de homología (resp. co-homología) son nulos.

Definición 24. *Sean $\underline{M}, \underline{N}$ dos complejos de cadena de R-módulos, un morfismo de complejos de R-módulos o aplicación de cadena $f : \underline{M} \longrightarrow \underline{N}$ es una familia de morfismos de R-módulos $\{f_n : M_n \longrightarrow N_n\}_{n\in\mathbb{Z}}$ de forma que $f_{n-1} \circ d_n = d'_n \circ f_n$ para cada $n \in \mathbb{Z}$. Es decir, de forma que los siguiente diagramas conmuten para todo $n \in \mathbb{Z}$:*

$$\begin{tikzcd} M_n \arrow[r, "f_n"] \arrow[d, "d_n"] & N_n \arrow[d, "d'_n"] \\ M_{n-1} \arrow[r, "f_{n-1}"] & N_{n-1} \end{tikzcd}$$

Proposición 2.2.1. *Si $\underline{M}$ y $\underline{N}$ son dos complejos de cadena de R-módulos y $f : \underline{M} \longrightarrow \underline{N}$ una aplicación de cadena, para cada $n \in \mathbb{N}$, $f_n : M_n \longrightarrow N_n$ induce un morfismo de R-módulos:*
$$\begin{array}{cccc} H_n(f): & H_n(\underline{M}) & \longrightarrow & H_n(\underline{N}) \\ & x + Im(d_{n+1}) & \mapsto & f_n(x) + Im(d'_{n+1}). \end{array}$$

Definición 25. *Sean* $\overline{M}$, $\overline{N}$ *dos complejos de co-cadena. Una aplicación de co-cadena* $f : \overline{M} \longrightarrow \overline{N}$ *es una una familia de morfismos de* R*-módulos* $\{f^n : M^n \longrightarrow N^n\}_{n\in\mathbb{Z}}$ *tales que los diagramas siguientes conmuten para todo* $n \in \mathbb{Z}$*:*

$$\begin{array}{ccc} M^n & \xrightarrow{f^n} & N^n \\ \big\downarrow{\scriptstyle c^n} & & \big\downarrow{\scriptstyle c'^n} \\ M^{n+1} & \xrightarrow{f^{n+1}} & N^{n+1} \end{array}$$

Observación 11. *Los módulos de homología y co-homología tienen un caracter functorial sobre los morfismos de cadena y co-cadena. Es claro que* $H_n(Id_{M_n}) = Id_{H_n}$ *(resp.* $H^n(Id) = Id_{H^n}$*) y dados* $f : \underline{M} \longrightarrow \underline{N}$, $g : \underline{N} \longrightarrow \underline{P}$ *dos morfismos de cadena,* $H_n(g \circ f) = H_n(g) \circ H_n(f)$ *y similarmente pasa con los morfismos de co-cadena.*

Definición 26 (**Functor exacto**). *Sea* F *es un functor de la categoría de* R*-módulos en sí misma.*

i) *Si* F *es covariante, se dice exacto a izquierda (resp. a derecha) si para cada s.e.c.* $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$*, la siguiente es una sucesión exacta:*
$$0 \longrightarrow F(M') \longrightarrow F(M) \longrightarrow F(M'').$$
(Resp. si la sucesión $F(M') \longrightarrow F(M) \longrightarrow F(M'') \longrightarrow 0$ *es exacta).*

ii) *Si* F *es contravariante, se dice que* F *es exacto a izquierda (resp. a derecha) si para cada s.e.c.* $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$*, la siguiente es una sucesión exacta:*
$$0 \longrightarrow F(M'') \longrightarrow F(M) \longrightarrow F(M').$$
(Resp. si la sucesión $F(M'') \longrightarrow F(M) \longrightarrow F(M') \longrightarrow 0$ *es exacta).*

Un functor se dice exacto si es exacto a izquierda y a derecha.

Definición 27. *Sean* $\underline{M}$, $\underline{N}$, $\underline{P}$ *complejos de cadena de* R*-módulos y* $f : \underline{M} \longrightarrow \underline{N}$, $g : \underline{N} \longrightarrow \underline{P}$ *aplicaciones de cadena. Se dice que la sucesión de complejos de cadena*

$$0 \longrightarrow \underline{M} \xrightarrow{f} \underline{N} \xrightarrow{g} \underline{P} \longrightarrow 0$$

es exacta si, para cada $n \in \mathbb{Z}$*, las siguientes son sucesiones exactas de* R*-módulos:*

$$0 \longrightarrow M_n \xrightarrow{f_n} N_n \xrightarrow{g_n} P_n \longrightarrow 0$$

Proposición 2.2.2. *Sea* $0 \longrightarrow \underline{M} \xrightarrow{f} \underline{N} \xrightarrow{g} \underline{P} \longrightarrow 0$ *una sucesión exacta de complejos de cadena de* R*-módulos. Entonces, existe un morfismo de* R*-módulos*

$$\partial_n : H_n(\underline{P}) \longrightarrow H_{n-1}(\underline{M}).$$

A esta familia de morfismos de R*-modulos* $\{\partial_n\}_{n\in\mathbb{Z}}$ *se la denomina morfismos conectores.*

Proposición 2.2.3. *Sea* $0 \longrightarrow \underline{M} \xrightarrow{f} \underline{N} \xrightarrow{g} \underline{P} \longrightarrow 0$ *una sucesión exacta de complejos de cadena de* R*-módulos. Entonces, la sucesión de* R*-módulos*

$$\cdots \longrightarrow H_n(\underline{M}) \xrightarrow{H_n(f)} H_n(\underline{N}) \xrightarrow{H_n(g)} H_n(\underline{P}) \xrightarrow{\partial_n} H_{n-1}(\underline{M}) \xrightarrow{H_{n-1}(f)} H_{n-1}(\underline{N})$$

es exacta.

Proposición 2.2.4. *Sean* $\underline{M}$, $\underline{N}$ *y* $\underline{P}$ *complejos de cadena de* R*-módulos; sea*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \underline{M} & \xrightarrow{f} & \underline{N} & \xrightarrow{g} & \underline{P} & \longrightarrow & 0 \\ & & \big\downarrow{\scriptstyle\alpha} & & \big\downarrow{\scriptstyle\beta} & & \big\downarrow{\scriptstyle\gamma} & & \\ 0 & \longrightarrow & \underline{M'} & \xrightarrow{f'} & \underline{N'} & \xrightarrow{g'} & \underline{P'} & \longrightarrow & 0 \end{array}$$

un diagrama conmutativo cuyas filas son sucesiones exactas. Entonces, el diagrama

$$\begin{array}{ccccccccccccc} \dots & \longrightarrow & H_n(\underline{M}) & \xrightarrow{H_n(f)} & H_n(\underline{N}) & \xrightarrow{H_n(g)} & H_n(\underline{P}) & \xrightarrow{\partial_n} & H_{n-1}(\underline{M}) & \xrightarrow{H_{n-1}(f)} & H_{n-1}(\underline{N}) & \longrightarrow & \dots \\ & & \big\downarrow{\scriptstyle H_n(\alpha)} & & \big\downarrow{\scriptstyle H_n(\beta)} & & \big\downarrow{\scriptstyle H_n(\gamma)} & & \big\downarrow{\scriptstyle H_{n-1}(\alpha)} & & \big\downarrow{\scriptstyle H_{n-1}(\beta)} & & \\ \dots & \longrightarrow & H_n(\underline{M'}) & \xrightarrow{H_n(f')} & H_n(\underline{N'}) & \xrightarrow{H_n(g')} & H_n(\underline{P'}) & \xrightarrow{\partial'_n} & H_{n-1}(\underline{M'}) & \xrightarrow{H_{n-1}(f')} & H_{n-1}(\underline{N'}) & \longrightarrow & \dots \end{array}$$

es conmutativo.

Definición 28. *Sean $\underline{M}$, $\underline{N}$ complejos de cadena de R-módulos. Sean $f, g : \underline{M} \longrightarrow \underline{N}$ dos morfismos de cadena. Una homotopía entre f y g es una familia de morfismos de R-módulos $\{h_n : M_n \longrightarrow N_{n+1}\}_{n\in\mathbb{Z}}$ que verifican la siguiente propiedad:*

$$(h_{n-1} \circ d_n)(x) + (d'_{n+1} \circ h_n)(x) = f_n(x) - g_n(x) \qquad \forall x \in M_n,\ \forall n \in \mathbb{Z}. \tag{2.2.3}$$

Cuando existe una homotopía entre f y g se dice que f y g son homótopos.

La homotopía define una relación de equivalencia $\sim$ en el conjunto de morfismos de cadena de $\underline{M}$ en $\underline{N}$, donde dos morfismos de cadena $f, g : \underline{M} \longrightarrow \underline{N}$ están relacionados si existe una homotopía entre ellos, es decir, si son homótopos. Para ver que $f \sim f$ basta tomar $h_n = d_n$. Ahora, si $f \sim g$, entonces existen $\{h_n\}_{n\in\mathbb{Z}}$ verificando la Igualdad (2.2.3). Por tanto, se tiene que

$$-(h_{n-1} \circ d_n)(x) - (d'_{n+1} \circ h_n)(x) = g_n(x) - f_n(x) \qquad \forall x \in M_n,\ \forall n \in \mathbb{Z}.$$

Como d_n, d'_n y h_n son morfismos de R-módulos, se sigue que

$$(-h_{n-1} \circ d_n)(x) + (d'_{n+1} \circ -h_n)(x) = g_n(x) - f_n(x) \qquad \forall x \in M_n,\ \forall n \in \mathbb{Z}.$$

Por tanto se tiene que $\{h'_n\}_{n\in\mathbb{Z}}$ donde $h'_n = -h_n$ es una homotopía entre g y f, concluyendo que $g \sim f$. Finalmente, sean $f^1, f^2, f^3 : \underline{M} \longrightarrow \underline{N}$ verificando $f^1 \sim f^2$ y $f^2 \sim f^3$ con homotopías $\{h^1_n\}_{n\in\mathbb{Z}}$ y $\{h^2_n\}_{n\in\mathbb{Z}}$ respectivamente. Tomando $h_n = h^1_n + h^2_n$ se tiene que

$$\begin{aligned}&(h_{n-1} \circ d_n)(x) + (d'_{n+1} \circ h_n)(x) = (h^1_{n-1} \circ d_n)(x) + (h^2_{n-1} \circ d_n)(x)\\ &+(d'_{n+1} \circ h^1_n)(x) + (d'_{n+1} \circ h^2_n)(x) = f^1_n(x) - f^2_n(x) + f^2_n(x) - f^3_n(x) = f^1_n(x) - f^3_n(x)\end{aligned}$$

para cada $x \in M_n$ y cada $n \in \mathbb{Z}$. Por tanto, $\{h_n\}_{n\in\mathbb{Z}}$ es una homotopía entre f^1_n y f^3_n. Concluimos así que $f^1_n \sim f^3_n$.

Proposición 2.2.5. *Sean $\underline{M}$, $\underline{N}$ complejos de cadena de R-módulos; $f, g : \underline{M} \longrightarrow \underline{N}$ morfismos de cadena homótopos. Entonces, $H_n(f) = H_n(g)$ para todo $n \in \mathbb{Z}$.*

2.3. Existencia de Resolución Proyectiva de R-módulos

Recordamos sucintamente la noción de R-módulo proyectivo. El lector puede seguir estas nociones en [**Pardo, 21**], [**Raghavan et al., 1975**] o el TFG [**López, 21**].

Definición 29 (**Módulo Libre**). *Un R-módulo M se dice libre si existe un conjunto X de tal modo que M es isomorfo al R-módulo siguiente:*

$$\bigoplus_X R := \{f : X \longrightarrow R : f \text{ es aplicación y } \exists Y \subseteq X \text{ finito con } f(x) = 0,\ \forall x \in X \setminus Y\}$$

Si podemos elegir X de cardinal finito diremos que M es un R-módulo libre de rango finito.

Denotaremos por $rank_R(M)$ el rango de un R-módulo de rango finito.

Definición 30 (**Módulo Proyectivo**). *Un R-módulo P se dice proyectivo si el functor covariante $Hom_R(P, -)$ es exacto.*

Por la Proposición A.3.1, $Hom_R(P, -)$ es un functor exacto a izquierda si y solamente si transforma epimorfismos en epimorfismos. Esto es equivalente a la siguiente propiedad: Dado $g : N \longrightarrow M$ un epimorfismo de R-módulos y dado $f : P \longrightarrow M$ un morfismo, existe $h : P \longrightarrow N$ tal que $f = g \circ h$. Esto se resume con el diagrama siguiente:

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

Otras caracterizaciones son descritas en la Sección A.4 del Apéndice A.

Definición 31 (**Resolución Proyectiva**). *Sea M un R-módulo. Una resolución proyectiva de M es un par $(\underline{P}, \epsilon)$, donde $\underline{P} = \{P_n\}_{n\in\mathbb{N}}$ es un complejo de cadena de R-módulos proyectivos, $\epsilon : P_0 :\longrightarrow M$ es un morfismo de R-módulos y la siguiente es una sucesión exacta de R-módulos:*

$$\cdots \longrightarrow P_n \xrightarrow{d_n} P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \xrightarrow{\epsilon} M \longrightarrow 0,$$

A los morfismo d_n se denominan morfismos borde. La resolución proyectiva se dice libre si los módulos proyectivos P_n son libres y se dice resolución finita si $\exists k \in \mathbb{N}$ tal que $P_n = 0, \forall n \geq k$.

PROPOSICIÓN 2.3.1 (**Existencia de Resolución Proyectiva**). *Sean R un anillo. Todo R-módulo M admite una resolución libre (y, por tanto, una resolución proyectiva). Además, si M y R son noetherianos, se puede suponer que los R-módulos libres P_n de la resolución son todos de rango finito.*

DEMOSTRACIÓN. Nótese que si M es un R-módulo y $\mathcal{B}$ es un sistema generador de M como R-módulo, existe el epimorfismo natural $\pi : F := \bigoplus_{\mathcal{B}} R \longrightarrow M$, donde $F = \bigoplus_{\mathcal{B}} R$ es el R-módulo libre que tiene a $\mathcal{B}$ como base. De este modo, comenzamos con una base $\mathcal{B}_0$ de M y $F_0 = \bigoplus_{\mathcal{B}_0} R$ genera un primer epimorfismo $F_0 \xrightarrow{\epsilon_0} M$. Ahora, construimos la resolución libre de M inductivamente. Supongamos que tenemos ya construida una sucesión exacta:

$$F_n \xrightarrow{\epsilon_n} F_{n-1} \longrightarrow \cdots \longrightarrow F_0 \xrightarrow{\epsilon_0} M \longrightarrow 0.$$

Sea $K_n = ker(\epsilon_n)$ el núcleo de ϵ_n y consideramos $\mathcal{B}_{n+1}$ un sistema generador de K_n. Definamos F_{n+1} como el R-módulo libre con base $\mathcal{B}_{n+1}$. Esto es, $F_{n+1} = \bigoplus_{\mathcal{B}_{n+1}} R$. Definamos $\epsilon_{n+1} : F_{n+1} \longrightarrow K_n$ la proyección natutal. Entonces, tenemos un nuevo término en nuestra cadena:

$$F_{n+1} \xrightarrow{\epsilon_{n+1}} F_n \xrightarrow{\epsilon_n} F_{n-1} \longrightarrow \cdots \longrightarrow F_0 \xrightarrow{\epsilon_0} M \longrightarrow 0,$$

donde usamos que $K_n \subseteq F_n$. Además, como $Im(\epsilon_{n+1}) = k_n = ker(\epsilon_n)$, la sucesión es exacta. Como R es noetheriano y M es finitamente generado, se prueba fácilmente por inducción que cada F_n es un R-módulo libre finitamente generado (y, por tanto, noetheriano) y cada $K_{n+1} \subseteq F_n$ es un R-módulo noetheriano, lo que implicará que F_{n+1} sea también noetheriano y finitamente generado. □

DEFINICIÓN 32. *Sea $f : M \longrightarrow M'$ un morfismo de R-módulos. Sean $(\underline{P}, \epsilon)$ y $(\underline{P}', \epsilon')$ resoluciones proyectivas de M y M' respectivamente. Una aplicación de cadena $F : \underline{P} \longrightarrow \underline{P}'$, $F = \{F_n : n \in \mathbb{N}\}$ se dice que es una aplicación de cadena sobre f si se verifica que $f \circ \epsilon = \epsilon' \circ F_0$.*

PROPOSICIÓN 2.3.2 (**Lifting Theorem**). *Sea $f : M \longrightarrow M'$ un morfismo de R-módulos, $(\underline{P}, \epsilon)$ y $(\underline{P}', \epsilon')$ resoluciones proyectivas de M y M' respectivamente. Entonces, existe una aplicación de cadena $F : \underline{P} \longrightarrow \underline{P}'$ sobre f. Más aún, si $F, G : \underline{P} \longrightarrow \underline{P}'$ son aplicaciones de cadena sobre f, entonces F y G son homótopas.*

DEMOSTRACIÓN. Consideremos el siguiente diagrama cuyas filas son sucesiones exactas. Por la Proposición A.4.2, siendo P_0 proyectivo, existirá $F_0 : P_0 \longrightarrow P_0'$ que hace conmutativo el diagrama:

$$\begin{tikzcd} P_0 \arrow[r, "\epsilon"] \arrow[d, dotted, "\exists F_0"'] & M \arrow[r] \arrow[d, "f"] & 0 \\ P_0' \arrow[r, "\epsilon'"] & M' \arrow[r] & 0. \end{tikzcd}$$

Definamos F_n inductivamente. Sea $n \geq 1$. Tomando $F_{-1} = f$, $d_0 = \epsilon$ y $d_0' = \epsilon'$, se tiene el siguiente diagrama conmutativo:

$$\begin{tikzcd} P_n \arrow[r, "d_n"] & P_{n-1} \arrow[r, "d_{n-1}"] \arrow[d, "F_{n-1}"] & P_{n-2} \arrow[d, "F_{n-2}"] \\ P_n' \arrow[r, "d_n'"] & P_{n-1} \arrow[r, "d_{n-1}'"] & P_{n-2}' \end{tikzcd}$$

Por tanto, $d_{n-1}' \circ F_{n-1} \circ d_n = F_{n-2} \circ d_{n-1} \circ d_n$. Pero como $d_{n-1} \circ d_n = 0$, se sigue que $d_{n-1}' \circ F_{n-1} \circ d_n = 0$. Por consiguiente, $Im(F_{n-1} \circ d_n) \subseteq ker(d_{n-1}')$. De nuevo, por la Proposición A.4.2, como P_n es proyectivo, existirá un morfismo $F_n : P_n \longrightarrow P_n'$ tal que $d_n' \circ F_n = F_{n-1} \circ d_n$. Esto se resume en el siguiente diagrama conmutativo:

$$\begin{tikzcd} P_n \arrow[r, "d_n"] \arrow[d, dotted, "\exists F_n"'] & P_{n-1} \arrow[d, "F_{n-1}"] & \\ P_n' \arrow[r, "d_n'"] & Im(d_n') \arrow[r] & 0. \end{tikzcd}$$

Por tanto, se tiene que $F = \{F_n : n \in \mathbb{N}\}$ es una aplicación de cadena sobre f. Supongamos que $F, G : \underline{P} \longrightarrow \underline{P}'$, donde $F = \{F_n : n \in \mathbb{N}\}$ y $G = \{G_n : n \in \mathbb{N}\}$ son aplicaciones de cadena sobre f. Esto significa que $\epsilon' \circ G_0 = f \circ \epsilon = \epsilon' \circ F_0$. En consecuencia $\epsilon'(F_0 - G_0) = 0$

e $Im(F_0 - G_0) \subseteq ker(\epsilon')$. Como $(\underline{P}', \epsilon')$ es una resolución proyectiva de M', $ker(\epsilon') = Im(d'_1)$. Por tanto, podemos considerar el diagrama:

$$\begin{tikzcd} & P_0 \arrow[dl, dotted, "\exists h_0"'] \arrow[d, "F_{n-1}"] & \\ P'_1 \arrow[r, "d'_1"] & Im(d'_1) \arrow[r] & 0. \end{tikzcd}$$

Por la Proposición A.4.2, como P_0 es proyectivo, existe $h_0 : P_0 \longrightarrow P'_1$ verificando $d'_1 \circ h_0 = F_0 - G_0$. Ahora, procedamos inductivamente. Supongamos $n \geq 1$. Como F y G son aplicaciones de cadena, se verifica $d'_n \circ F_n = F_{n-1} \circ d_n$ y $d'_n \circ G_n = G_{n-1} \circ d_n$. Por consiguiente, $d'_n \circ (F_n - G_n) = (F_{n-1} - G_{n-1}) \circ d_n$. Ahora, por hipótesis inductiva,

$$(F_{n-1} - G_{n-1}) \circ d_n = d'_n \circ h_{n-1} \circ d_n + h_{n-2} \circ d_{n-1} \circ d_n.$$

Como $d_{n-1} \circ d_n = 0$, se tiene finalmente $d'_n \circ (F_n - G_n) = (F_{n-1} - G_{n-1}) \circ d_n = d'_n \circ h_{n-1} \circ d_n$. Entonces, se sigue que $d'_n \circ (F_n - G_n - h_{n-1} \circ d_n) = 0$ e $Im(F_n - G_n - h_{n-1} \circ d_n) \subseteq ker(d'_n) = Im(d'_{n+1})$. En consecuencia, podemos considerar el siguiente diagrama:

$$\begin{tikzcd} & P_n \arrow[dl, dotted, "\exists h_n"'] \arrow[d, "F_n - G_n - h_{n-1} \circ d_n"] & \\ P'_{n+1} \arrow[r, "d'_{n+1}"] & Im(d'_{n+1}) \arrow[r] & 0. \end{tikzcd}$$

Por la Proposición A.4.2, como P_n es un R-módulo proyectivo, existe $h_n : P_n \longrightarrow P_{n+1}$ verificando $h_n \circ d'_{n+1} = F_n - G_n - h_{n-1} \circ d_n$. Es decir, $h_n \circ d'_{n+1} + h_{n-1} \circ d_n = F_n - G_n$. Por tanto, $h = \{h_n : \ n \in \mathbb{N}\}$ es una homotopía entre F y G. Es decir, F y G son homótopas. $\square$

Proposición 2.3.3 (**Horseshoe Lemma**). *Sea* $0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{j} M'' \longrightarrow 0$ *una sucesión exacta de R-módulos. Sean* $(\underline{P}', \epsilon')$ *y* $(\underline{P}'', \epsilon'')$ *resoluciones proyectivas de M' y M'' respectivamente. Entonces, existe una resolución proyectiva* $(\underline{P}, \epsilon)$ *de M de modo que la sucesión de complejos de cadena:*

$$0 \longrightarrow \underline{P}' \xrightarrow{f} \underline{P} \xrightarrow{g} \underline{P}'' \longrightarrow 0,$$

con $f = \{f_n\}_{n \in \mathbb{Z}}$ *y* $g = \{g_n\}_{n \in Z}$*, sea exacta. Y tal que el diagrama:*

$$\begin{tikzcd} 0 \arrow[r] & P'_0 \arrow[r, "f_0"] \arrow[d, "\epsilon'"] & P_0 \arrow[r, "g_0"] \arrow[d, "\epsilon"] & P''_0 \arrow[r] \arrow[d, "\epsilon''"] & 0 \\ 0 \arrow[r] & M' \arrow[r, "i"] & M \arrow[r, "j"] & M'' \arrow[r] & 0 \end{tikzcd} \tag{2.3.1}$$

conmute.

Demostración. Para cada $n \in N$ definimos $P_n := P'_n \oplus P''_n$ y tomamos $f_n : P'_n \longrightarrow P_n$ con $f_n(x') = x'$; $g_n : P_n \longrightarrow P''_n$ con $g_n(x' \oplus x'') = x''$, que no son más que la inclusión y la proyección natural en la suma directa.

Afirmación. *Existen morfismos de R-módulos* $l : P''_0 \longrightarrow M$ *y, para cada* $n \in \mathbb{N}$ *con* $n > 0$, $k_n : P''_n \longrightarrow P'_{n-1}$ *verificando:*

i) $\epsilon'' = j \circ l, \qquad i \circ \epsilon' \circ k_1 + l \circ d''_1 = 0;$
ii) $d'_{n-1} \circ k_n + k_{n-1} \circ d''_n = 0, \ \forall n \in \mathbb{N}, \ n > 1.$

Demostración. Por una parte, consideremos el diagrama:

$$\begin{tikzcd} & P''_0 \arrow[dl, dotted, "\exists l"'] \arrow[d, "\epsilon''"] & \\ M \arrow[r, "j"] & M'' \arrow[r] & 0, \end{tikzcd}$$

cuya fila inferior es una sucesión exacta de R-módulos. Como P''_0 es un R-módulo proyectivo, por la Proposición A.4.2, existe un morfismo $l : P_0 \longrightarrow M$ verificando $\epsilon'' = j \circ l$. Construimos k_n inductivamente. Consideremos la composición $j \circ (-l) \circ d''_1$. Por $i)$, se tiene $j \circ (-l) \circ d''_1 = -\epsilon'' \circ d''_1$. Como $(\underline{P}'', \epsilon'')$ es una resolución proyectiva de M'', $\epsilon'' \circ d''_1 = 0$. Por tanto, se sigue que $j \circ (-l) \circ d''_1 = 0$ e $Im(-l \circ d''_1) \subseteq ker(j) = Im(i)$. Ahora, como $(\underline{P}', \epsilon')$ es una resolución proyectiva de M', ϵ' es epimorfismo e $Im(i) = Im(i \circ \epsilon')$. En consecuencia, $Im(-l \circ d_1'') \subseteq Im(i \circ \epsilon')$, y podemos considerar el diagrama:

$$\begin{tikzcd} & P_1'' \arrow[dl, dotted, "\exists k_1"'] \arrow[d, "-l\circ d_1''"] & \\ P_0'' \arrow[r, "i\circ\epsilon'"] & Im(i\circ\epsilon') \arrow[r] & 0, \end{tikzcd}$$

Como P_1'' es proyectivo, existe $k_1 : P_1'' \longrightarrow P_0'$ verificando la segunda igualdad de i). Sea $n > 1$, definiendo $d_0' := i \circ \epsilon'$; $k_0 := l$ se tiene, por hipótesis inductiva, $d_{n-2}' \circ (-k_{n-1}) \circ d_n'' = -k_{n-1} \circ d_{n-1}'' \circ d_n''$. Como $d_{n-1}'' \circ d_n'' = 0$, $d_{n-2}'(-k_{n-1} \circ d_n'') = 0$ e $Im(-k_{n-1} \circ d_n'') \subseteq ker(d_{n-2}') = Im(d_{n-1}')$. Por tanto, como P_n'' es proyectivo, existirá $k_n : P_n'' \longrightarrow P_{n-1}'$ tal que el siguiente diagrama es conmutativo:

$$\begin{tikzcd} & P_n'' \arrow[dl, dotted, "\exists k_n"'] \arrow[d, "-k_{n-1}\circ d_n''"] & \\ P_{n-1}'' \arrow[r, "d_{n-1}'"] & Im(d_{n-1}') \arrow[r] & 0, \end{tikzcd}$$

□

Definimos ahora los morfimos $\{d_n : \ n \in \mathbb{N}, \ n > 0\}$ y ϵ del modo siguiente:

$$\begin{array}{rccl} \epsilon : & P_0 & \longrightarrow & M \\ & x' \oplus x'' & \mapsto & (i \circ \epsilon')(x') + l(x''), \end{array} \qquad \begin{array}{rccl} d_n : & P_n & \longrightarrow & P_{n-1} \\ & x' \oplus x'' & \mapsto & (d_n'(x') + k_n(x'')) \oplus d_n''(x''). \end{array}$$

Comprobemos que $(\underline{P}, \epsilon)$ es una resolución proyeciva de M, i.e. que la sucesión:

$$\cdots \longrightarrow P_n \xrightarrow{d_n} P_{n-1} \xrightarrow{d_{n-1}} \cdots \longrightarrow P_0 \xrightarrow{\epsilon} M \longrightarrow 0 \tag{2.3.2}$$

es exacta. Sea $m \in M$. Consideremos $j(m) \in M''$. Como $(\underline{P}'', \epsilon'')$ es una resolución proyectiva de M'', ϵ'' es epimorfismo. Sea $x'' \in P_0''$ tal que $\epsilon''(x'') = j(m)$. Tomamos $l(x'') \in M$. Como $j \circ l = \epsilon''$, $m - l(x'') \in ker(j) = Im(i)$. Entonces, existe $m' \in M'$ verificando $i(m') = m - l(x'')$. Ahora, como $(\underline{P}', \epsilon')$ es una resolución proyectiva de M', ϵ' es epimorfismo y, por tanto, existe $x' \in P_0'$ de modo que $\epsilon'(x') = m'$. Por consiguiente, $i \circ \epsilon(x') = m - l(x'')$. Es decir, $\epsilon(x', x'') = m$. Por tanto, ϵ es epimorfismo y la Sucesión (2.3.2) es exacta en M. Además, se tiene que, por una parte:

$$(d_1 \circ \epsilon)(x' \oplus x'') = (i \circ \epsilon' \circ d_1')(x') + (i \circ \epsilon' \circ k_1)(x'') + (l \circ d_1'')(x'') = 0,$$

pues $d_1' \circ \epsilon' = 0$ por ser $(\underline{P}', \epsilon')$ resolución proyectiva de M' e $(i \circ \epsilon' \circ k_1)(x') + (l \circ d_1'')(x'') = 0$ por la propiedad i). Por tanto, $Im(d_1) \subseteq ker(\epsilon)$. De otro lado, si $x' \oplus x'' \in ker(\epsilon)$, $(i \circ \epsilon')(x') + l(x'') = 0$. Entonces, se sigue que $-(j \circ i \circ \epsilon')(x') = (j \circ l)(x'') = \epsilon''(x'') = 0$, pues $j \circ i = 0$. En consecuencia, $x'' \in ker(\epsilon'') = Im(d_1'')$, y existe $x_1'' \in P_1''$ verificando $d_1''(x_1'') = x''$. Además,

$$(i \circ \epsilon')(x') - (i \circ \epsilon' \circ k_1)(x_1'') = 0. \tag{2.3.3}$$

Para verlo, basta aplicar la propiedad i) a la parte izquierda de la igualdad anterior teniendo en cuenta que, por hipótesis, $(i \circ \epsilon')(x') = l(x'') = (l \circ d_1'')(x_1'')$. Ahora bien, como i es monomorfismo, la Igualdad (2.3.3) implica que $\epsilon'(x') - \epsilon'(k_1(x_1'')) = \epsilon'(x' - k_1(x_1'')) = 0$. Por consiguiente, $x - k_1(x_1'') \in ker(\epsilon') = Im(d_1')$, y existe $x_1' \in P_1'$ verificando $d_1'(x_1') = x' - k_1(x_1'')$. Se sigue que $d_1(x_1' \oplus x_1'') = (d_1'(x_1') + k_1(x_1'')) \oplus d_1''(x_1'') = x' \oplus x''$ y, por tanto, $ker(\epsilon) \subseteq Im(d_1)$. Con esto queda probada la exactitud en P_0. Sea $n > 0$. De un lado, se tiene que:

$$d_n \circ d_{n-1} = (d_{n-1}'(d_n' + k_n) + k_{n-1} \circ d_n'') \oplus (d_{n-1}'' \circ d_n'') = 0,$$

pues $d_{n-1}'' \circ d_n'' = 0$; $d_{n-1}' \circ d_n' = 0$; y, por la propiedad ii), $d_{n-1}' \circ k_n + k_{n-1} \circ d_n'' = 0$. Por tanto, se sigue que $Im(d_n) \subseteq ker(d_{n-1})$. Por otra parte, si $x' \oplus x'' \in ker(d_{n-1})$, $d_{n-1}'(x') + k_{n-1}(x'')$ y $d_{n-1}''(x'') = 0$. Es decir, $x'' \in ker(d_{n-1}'') = Im(d_n'')$, y existe $x_1'' \in P_n''$ verificando $d_n''(x_1'') = x''$. Además, como $k_{n-1}(x'') = (k_{n-1} \circ d_n'')(x_1'') = (d_{n-1}' \circ k_n)(x_1'')$, se tiene:

$$0 = d_{n-1}'(x') + k_{n-1}(x'') = d_{n-1}'(x') + (d_{n-1}' \circ k_n)(x_1'') = d_{n-1}'(x' - k_n(x_1'')).$$

Luego $x' - k_n(x_1'') \in ker(d_{n-1}') = Im(d_n')$, y existe $x_1' \in P_n'$ verificando $d_n'(x_1') = x' - k_n(x_1'')$. Entonces, se sigue que $d_n(x_1' \oplus x_1'') = x' \oplus x''$, y $ker(d_{n-1}) \subseteq Im(d_n)$. Con esto queda probada la exactitud en P_n. Finalmente, es claro que $(\epsilon \circ f_0)(x') = \epsilon(x') = (i \circ \epsilon)(x')$ por definición de

ϵ. Ahora, usando la definición de g_0 y la propiedad i), $(\epsilon'' \circ g_0)(x' \oplus x'') = \epsilon''(x'') = (j \circ l)(x'')$. De otro lado, $\epsilon(x' \oplus x'') = (i \circ \epsilon')(x') + l(x'')$. Componiendo con j, se tiene

$$(j \circ \epsilon)(x' \oplus x'') = j \circ ((i \circ \epsilon')(x') + l(x'')) = (j \circ i \circ \epsilon')(x') + (j \circ l)(x'') = (j \circ l)(x''),$$

pues $i \circ j = 0$. Con esto queda probada la conmutatividad del Diagrama (2.3.1). $\square$

DEFINICIÓN 33. *Sea C : $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ una sucesión exacta de R-módulos. Una resolución proyectiva de C es una sucesión exacta de complejos de cadena de R-módulos $0 \longrightarrow \underline{P}' \longrightarrow \underline{P} \longrightarrow \underline{P}'' \longrightarrow 0$, donde $(\underline{P}', \epsilon')$, $(\underline{P}, \epsilon)$ y $(\underline{P}'', \epsilon'')$ son resoluciones proyectivas de M', M y M'' respectivamente, de forma que el Diagrama (2.3.1) sea conmutativo.*

La Proposición 2.3.3 precedente prueba que las sucesiones exactas cortas poseen resolución proyectiva.

PROPOSICIÓN 2.3.4. *Sea dado un diagrama conmutativo cuyas fila son sucesiones exactas de la forma siguiente:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{i_1} & M & \xrightarrow{p_1} & M'' & \longrightarrow & 0 \\ & & \Big\downarrow f' & & \Big\downarrow f & & \Big\downarrow f'' & & \\ 0 & \longrightarrow & N' & \xrightarrow{i_2} & N & \xrightarrow{p_2} & N'' & \longrightarrow & 0. \end{array} \tag{2.3.4}$$

Supongamos dadas las resoluciones proyectivas de ambas filas que se siguen del Horseshoe Lemma (Proposición 2.3.3 anterior):

$$0 \longrightarrow \underline{P}' \longrightarrow \underline{P} \longrightarrow \underline{P}'' \longrightarrow 0, \qquad 0 \longrightarrow \underline{Q}' \longrightarrow \underline{Q} \longrightarrow \underline{Q}'' \longrightarrow 0$$

respectivamente resoluciones proyectivas de:

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0, \qquad 0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0.$$

Y sean $F' : \underline{P}' \longrightarrow \underline{Q}'$, $F'' : \underline{P}'' \longrightarrow \underline{Q}''$ morfismos entre resoluciones proyectivas que levantan respectivamente a los morfismos f' y f'' conforme a la Proposición 2.3.3 anterior. Entonces, existe un morfismo $F : \underline{P} \longrightarrow \underline{Q}$ sobre f de manera que el diagrama siguiente conmuta:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \underline{P}' & \longrightarrow & \underline{P} & \longrightarrow & \underline{P}'' & \longrightarrow & 0 \\ & & \Big\downarrow F' & & \Big\downarrow F & & \Big\downarrow F'' & & \\ 0 & \longrightarrow & \underline{Q}' & \longrightarrow & \underline{Q} & \longrightarrow & \underline{Q}'' & \longrightarrow & 0. \end{array} \tag{2.3.5}$$

DEMOSTRACIÓN. En vista de la demostración de la Proposición 2.3.3 podemos suponer que: $P_n = P'_n \oplus P''_n$, $Q_n = Q'_n \oplus Q''_n$; existen morfismos $l : P_0 \longrightarrow M$, $k_n : P''_n \longrightarrow P'_{n-1}$ verificando las propiedades i) y ii) de la Proposición 2.3.3 precedente; existen morfismos $l' : Q''_0 \longrightarrow Q$, $k'_n : Q''_n \longrightarrow Q'_{n-1}$ verificando las propiedades análogas a i) y ii) de la Proposición 2.3.3 anterior para los Q's. Notemos que los morfismos borde $d_n : P_n \longrightarrow P_{n-1}$ y el morfismo $\epsilon_P : P_0 \longrightarrow M$ son los definidos en la Proposición 2.3.3 precedente. Se verifica la afirmación análoga para los morfismos borde $c_n : Q_n \longrightarrow Q_{n-1}$ y el morfismo $\epsilon_Q : Q_o \longrightarrow N$.

AFIRMACIÓN. *Existen morfismos $\phi_0 : P''_0 \longrightarrow Q'_0$ y $\phi_n : P''_n \longrightarrow Q'_n$, $n > 0$ verificando:*

(1) $i_2 \circ \epsilon' \circ \phi_0 + l' \circ F''_0 = f \circ l$;
(2) $c'_n \circ \phi_n - \phi_{n-1} \circ d''_n = F'_{n-1} \circ k_n - k'_n \circ F''_n$.

DEMOSTRACIÓN. Consideremos, ahora, el morfismo $(f \circ l - l' \circ F''_0) : P_0 \longrightarrow N$ y su composición con $p_2 : N \longrightarrow N''$. Se tiene que $p_2(f \circ l - l' \circ F''_0) = p_2 \circ f \circ l - p_2 \circ l' \circ F''_0$. Como el Diagrama (2.3.4) conmuta, se tiene que $p_2 \circ f = f'' \circ p_1$, y por la propiedad i) de la Proposición 2.3.3, $p_1 \circ l = \epsilon''_P$. Ahora, utilizando la propiedad i) análoga para los Q's, $p_2 \circ l' = \epsilon''_Q$. Ahora bien, por ser F'' un morfismo sobre f'', se sigue que $p_2(f \circ l - l' \circ F''_0) = f'' \circ \epsilon''_P - \epsilon''_Q \circ F_0 = 0$. En consecuencia, $Im(f \circ l - l' \circ F''_0) \subseteq ker(p_2) = Im(i_2) = Im(i_2 \circ \epsilon'_Q)$, por ser ϵ'_Q epimorfismo. Por tanto, Como P''_0 es un R-módulo proyectivo, existe $\phi_0 : P''_0 \longrightarrow Q'_0$ tal que el diagrama siguiente es conmutativo y verificando (1):

$$\begin{tikzcd} & P_0'' \arrow[dl, dotted, "\exists \phi_0"'] \arrow[d, "f\circ l - l'\circ F_0''"] & \\ Q_0' \arrow[r, "i_2\circ\epsilon_Q'"] & Im(i_2\circ\epsilon_Q') \arrow[r] & 0. \end{tikzcd}$$

Supongamos, por inducción, que existe $\phi_{n-1} : P'_{n-1} \longrightarrow Q'_{n-1}$ verificando (2), tomando $d'_0 = i_2 \circ \epsilon_Q$, $F'_{-1} = f$, $\phi_{-1} = 0$, $k_0 = l$, $k'_0 = l'$ para el caso $n = 1$. Consideremos el morfismo $F_{n-1} \circ K_n - K'_n \circ F''_n + \phi_{n-1} \circ d''_n : P''_n \longrightarrow Q_{n-1}$ y su composición con c'_{n-1}:

$$\begin{aligned} &c'_{n-1}(F_{n-1} \circ K_n - K'_n \circ F''_n + \phi_{n-1} \circ d''_n) \\ &= c_{n-1} \circ F_{n-1} \circ K_n - c_{n-1} \circ K'_n \circ F''_n + c_{n-1} \circ \phi_{n-1} \circ d''_n. \end{aligned} \tag{2.3.6}$$

Ahora bien,

$$c'_{n-1} \circ F_{n-1} \circ k_n = F'_{n-2} \circ d'_{n-1} \circ k_n = -F_{n-2} \circ k_{n-1} \circ d''_n, \tag{2.3.7}$$

donde la primera igualdad se debe a que F' es aplicación de cadena, y la segunda se tiene por la propiedad *ii*) (ver demostración de la Proposición 2.3.3). De otro lado,

$$- c'_{n-1} \circ k'_n \circ F''_n = k'_{n-1} \circ c''_n \circ F''_n = k'_{n-1} \circ F''_{n-1} \circ d''_n, \tag{2.3.8}$$

donde la primera igualdad se debe a la propiedad análoga a *ii*) para los Q's (ver demostración de la Proposición 2.3.3), y la segunda se sigue de que F'' es una aplicación de cadena. Además, se verifica:

$$\begin{aligned} c'_{n-1} \circ \phi_{n-1} \circ d''_n &= \phi_{n-2} \circ d''_{n-1} \circ d''_n + F'_{n-2} \circ k_{n-1} \circ d''_n - k'_{n-1} \circ F''_{n-1} \circ d''_n \\ &= F'_{n-2} \circ k_{n-1} d''_n - k'_{n-1} \circ F''_{n-1} \circ d_n, \end{aligned} \tag{2.3.9}$$

donde la primera igualdad se tiene por hipótesis inductiva, y la segunda se sigue de que $d''_{n-1} \circ d''_n = 0$. Utilizando las Igualdades (2.3.7), (2.3.8) y (2.3.9) en la Igualdad (2.3.6) se concluye que $c'_{n-1}(F_{n-1} \circ K_n - K'_n \circ F''_n + \phi_{n-1} \circ d''_n) = 0$. Por tanto,

$$Im(F_{n-1} \circ K_n - K'_n \circ F''_n + \phi_{n-1} \circ d''_n) \subseteq ker(c'_{n-1}) = Im(c'_n).$$

Como P''_n es proyectivo, existe $\phi_n : P''_n \longrightarrow Q'_n$ haciendo conmutativo el siguiente diagrama y verificando (2):

$$\begin{tikzcd} & P_n'' \arrow[dl, dotted, "\exists \phi_n"'] \arrow[d, "F_{n-1}\circ K_n - K_n'\circ F_n'' + \phi_{n-1}\circ d_n''"] & \\ Q_n' \arrow[r, "c_n'"] & Im(c_n') \arrow[r] & 0, \end{tikzcd}$$

□

Definimos $\{F_n\}_{n\in\mathbb{N}} = F : \underline{P} \longrightarrow \underline{Q}$ como sigue:

$$\begin{array}{rccl} F_n : & P_n & \longrightarrow & Q_n \\ & (x' \oplus x'') & \mapsto & F_n(x' \oplus x'') = (F'_n(x') + \phi_n(x'')) \oplus F''_n(x''). \end{array}$$

Ahora bien, para cada $n \in \mathbb{N}$, $n > 0$ se tiene:

$$\begin{aligned} F_{n-1} \circ d_n &= F_{n-1}((d'_n + k_n) \oplus d''_n) = (F'_{n-1} \circ d'_n + F'_{n-1} \circ k_n + \phi_{n-1} \circ d''_n) \oplus (F''_{n-1} \circ d''_n) \\ &= (c'_n \circ F'_n + c'_n \circ \phi_n + k'_n \circ F''_n) \oplus (c''_n \circ F''_n) = c_n((F'_n + \phi_n) \oplus F''_n) = c_n \circ F_n, \end{aligned}$$

donde la tercera igualdad se sigue de que $F'_{n-1} \circ d'_n = c'_n \circ F'_n$ por ser F' aplicación de cadena; $F''_{n-1} \circ d''_n = c''_n \circ F''_n$ por ser F'' aplicación de cadena; y $F'_{n-1} \circ k_n + \phi_{n-1} \circ d''_n = c'_n \circ \phi_n + k'_n \circ F''_n$ por la propiedad (2). Por tanto, concluimos que $F : \underline{P} \longrightarrow \underline{Q}$ es una aplicación de cadena. Más aún,

$$\begin{aligned} \epsilon_Q \circ F_0 &= \epsilon_Q((F'_0 + \phi_0) \oplus F''_0) = i_2 \circ \epsilon'_Q \circ F'_0 + i_2 \circ \epsilon'_Q \circ \phi_0 + l \circ F''_0 = i_2 \circ \epsilon'_Q \circ F'_0 + f \circ l \\ &= i_2 \circ f' \circ \epsilon'_P + f \circ l = f \circ i_1 \circ \epsilon'_P + f \circ l = f(i_1 \circ \epsilon'_P + l) = f \circ \epsilon_P, \end{aligned}$$

donde la tercera igualdad se sigue de que, por la propiedad (1), $i_2 \circ \epsilon'_Q \circ \phi_0 + l \circ F_0 = f \circ l$; la cuarta igualdad se debe a que $\epsilon'_Q \circ F'_0 = f' \circ \epsilon'_P$, por ser F' una aplicación de cadena sobre f'; y en la quinta igualdad se tiene que $i_2 \circ f' = f \circ i_1$ por la conmutatividad del Diagrama (2.3.4).

Por tanto, se infiere que F es una aplicación de cadena sobre f. Finalmente, para cada $n \in \mathbb{N}$ se tiene que, si $\varphi_{n,i}$ y $\pi_{n,i}$, $i = 1, 2$ son las inclusiones y proyecciones canónicas respectivamente,

$$F_n(\varphi_{n,1}(x')) = F_n(x' \oplus 0) = F'_n(x') \oplus 0 = \varphi_{n,2}(F'_n(x'));$$

$$\pi_{n,2}(F_n(x' \oplus x'')) = \pi_{n,2}((F'_n(x') + \phi_n(x'')) \oplus F''_n(x'')) = F''_n(x') = F''_n(\pi_{n,1}(x' \oplus x'')).$$

En consecuencia, el diagrama:

$$\begin{array}{ccccc} P'_n & \xrightarrow{\varphi_{n,1}} & P_n & \xrightarrow{\pi_{n,1}} & P''_n \\ \big\downarrow{\scriptstyle F'_n} & & \big\downarrow{\scriptstyle F_n} & & \big\downarrow{\scriptstyle F''_n} \\ Q'_n & \xrightarrow{\varphi_{n,2}} & Q_n & \xrightarrow{\pi_{n,2}} & Q''_n \end{array}$$

es conmutativo. Lo que equivale a decir que el Diagrama (2.3.5) es conmutativo. □

2.4. Functores Tor

Sea M un R-módulo y $(\underline{P}, \epsilon)$ una resolución proyectiva de M. Entonces, dado un R-módulo N, podemos considerar el complejo de cadena de R-módulos:

$$\underline{P} \otimes_R N : \qquad \cdots \longrightarrow P_n \otimes_R N \xrightarrow{d_n \otimes Id_N} P_{n-1} \otimes_R N \longrightarrow \cdots \longrightarrow P_0 \otimes_R N \longrightarrow 0.$$

Basta notar que $(d_{n-1} \otimes Id_N) \circ (d_n \otimes Id_N) = (d_{n-1} \circ d_n) \otimes Id_N = 0 \otimes Id_N = 0$. Los módulos de homología $H_n(\underline{P} \otimes_R N)$ del complejo de cadena $\underline{P} \otimes_R N$ se denotan por $H_n(M, N; \underline{P})$.
Sea, ahora, $f : M \longrightarrow M'$ un morfismo de R-módulos; $(\underline{P}, \epsilon)$, $(\underline{P}', \epsilon')$ resoluciones proyectivas de M y M' respectivamente. Notemos que, en virtud de la Proposición 2.3.2, existe una aplicación de cadena $\{F_n\}_{n \in \mathbb{N}} = F : \underline{P} \longrightarrow \underline{P}'$ sobre f. Además, se tiene que:

$$(d'_n \otimes Id_N) \circ (F_n \otimes Id_N) = (d'_n \circ F_n) \otimes Id_N = (F_{n-1} \circ d_n) \otimes Id_N = (F_{n-1} \otimes Id_N) \circ (d_n \otimes Id_N).$$

En consecuencia, el diagrama:

$$\begin{array}{ccc} P_n \otimes_R N & \xrightarrow{F_n \otimes Id_N} & P'_n \otimes_R N \\ \big\downarrow{\scriptstyle d_n \otimes Id_N} & & \big\downarrow{\scriptstyle d'_n \otimes Id_N} \\ P_{n-1} \otimes_R N & \xrightarrow{F_{n-1} \otimes Id_N} & P'_{n-1} \otimes_R N \end{array}$$

conmuta para todo $n \in \mathbb{N}$, $n \geq 1$, y $\{F_n \otimes Id_N\}_{n \in \mathbb{N}} = F \otimes Id_N : \underline{P} \otimes_R N \longrightarrow \underline{P}' \otimes_R N$ es una aplicación de cadena. En virtud de la Proposición 2.2.1, $F \otimes Id_N$ induce un morfismo de R-módulos:

$$H_n(f, N; \underline{P}, \underline{P}') := H_n(F \otimes Id_N) : H_n(M, N; \underline{P}) \longrightarrow H_n(M', N; \underline{P}').$$

Veamos que $H_n(f, N; \underline{P}, \underline{P}')$ está bien definido al no depender de la elección de F. Si $F, G : \underline{P} \longrightarrow \underline{P}'$ son aplicaciones de cadena sobre f, entonces, por la Proposición 2.3.2, F y G son homótopas, i.e. existe una homotopía $h = \{h_n : P_n \longrightarrow P'_{n+1}\}$ entre dichas aplicaciones. Entonces, para cada $n \in \mathbb{N}$ se tiene:

$$\begin{aligned} &(h_{n-1} \otimes Id_N) \circ (d_n \otimes Id_N) + (d'_{n+1} \otimes Id_N) \circ (h_n \otimes Id_N) \\ = &(h_{n-1} \circ d_n) \otimes Id_N + (d'_{n+1} \circ h_n) \otimes Id_N = (h_{n-1} \circ d_n + d'_{n+1} \circ h_n) \otimes Id_N \\ &= (F_n - G_n) \otimes Id_N = F_n \otimes Id_N - G_n \otimes Id_N. \end{aligned}$$

En consecuencia, $F \otimes Id_N, G \otimes Id_N : \underline{P} \otimes_R N \longrightarrow \underline{P}' \otimes_R N$ son aplicaciones homótopas. En virtud de la Proposición 2.2.5, se sigue que $F \otimes Id_N$ y $G \otimes Id_N$ inducen el mismo morfismo $H_n(f, N; \underline{P}, \underline{P}')$. Dada $0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{j} M'' \longrightarrow 0$ una sucesión exacta de R-módulos consideremos una resolución proyectiva de la misma $\mathcal{P}$: $\quad 0 \longrightarrow \underline{P}' \longrightarrow \underline{P} \longrightarrow \underline{P}'' \longrightarrow 0$. La siguiente es una sucesión exacta (cf. Lema 2.4.1):

$$\mathcal{P} \otimes_R N : 0 \longrightarrow \underline{P}' \otimes_R N \longrightarrow \underline{P} \otimes_R N \longrightarrow \underline{P}'' \otimes_R N \longrightarrow 0.$$

Denotaremos por: $\partial_n(N, \mathcal{P}) : H_n(M'', N; \underline{P}'') \longrightarrow H_{n-1}(M', N; \underline{P}')$ a los morfismos conectores asociados a $\mathcal{P} \otimes_R N$ conforme a la Proposición 2.2.2.

Lema 2.4.1. *i) Sean $f : M \longrightarrow M'$, $g : M' \longrightarrow M''$ morfismos de R-módulos; y sean $\underline{P}$, $\underline{P}'$ y $\underline{P}''$ resoluciones proyectivas de M, M' y M'' respectivamente. Entonces, para cada $n \in \mathbb{N}$ se tiene:*

$$H_n(g \circ f, N; \underline{P}, \underline{P}'') = H_n(g, N; \underline{P}', \underline{P}'') \circ H_n(f, N; \underline{P}, \underline{P}').$$

Más aún, $H_n(1_M, N; \underline{P}, \underline{P}) = Id_{H_n(M,N;\underline{P})}$.
ii) Si $\mathcal{P} : 0 \longrightarrow \underline{P}' \xrightarrow{\varphi} \underline{P} \xrightarrow{\pi} \underline{P}'' \longrightarrow 0$ es una resolución proyectiva de una sucesión exacta de R-módulos $0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{j} M'' \longrightarrow 0$, entonces la siguiente sucesión de R-módulos es exacta:

$$\cdots \longrightarrow H_n(M'', N; \underline{P}'') \xrightarrow{\partial_n(N,\mathcal{P})} H_{n-1}(M', N; \underline{P}') \xrightarrow{H_{n-1}(i,N;\underline{P}',\underline{P})} H_{n-1}(M, N; \underline{P})$$
$$\xrightarrow{H_{n-1}(j,N;\underline{P},\underline{P}'')} H_{n-1}(M'', N; \underline{P}'') \longrightarrow \cdots \longrightarrow H_0(M'', N; \underline{P}'') \longrightarrow 0.$$

iii) Dado un diagrama conmutativo, cuyas filas son sucesiones exactas:

$$\begin{array}{rccccccccc} \mathcal{M}: & 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ \mathcal{L}: & 0 & \longrightarrow & L' & \longrightarrow & L & \longrightarrow & L'' & \longrightarrow & 0, \end{array}$$

y dado el diagrama conmutativo de resoluciones proyectivas siguiente:

$$\begin{array}{rccccccccc} \mathcal{P}: & 0 & \longrightarrow & \underline{P}' & \xrightarrow{\varphi^1} & \underline{P} & \xrightarrow{\pi^1} & \underline{P}'' & \longrightarrow & 0 \\ & & & \downarrow{\scriptstyle F'} & & \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle F''} & & \\ \mathcal{Q}: & 0 & \longrightarrow & \underline{Q}' & \xrightarrow{\varphi^1} & \underline{Q} & \xrightarrow{\pi^2} & \underline{Q}'' & \longrightarrow & 0, \end{array} \tag{2.4.1}$$

donde $\mathcal{P}$ y $\mathcal{Q}$ son resoluciones proyectivas de $\mathcal{M}$ y $\mathcal{L}$ respectivamente; F, F' y F'' son aplicaciones de cadena sobre f, f' y f'' respectivamente. Entonces, el siguiente diagrama es conmutativo para cada $n \in \mathbb{N}$, $n \geq 1$:

$$\begin{array}{ccc} H_n(M'', N; \underline{P}'') & \xrightarrow{H_n(f'',N;\underline{P}'',\underline{Q}'')} & H_n(L'', N; \underline{Q}'') \\ \downarrow{\scriptstyle \partial_n(N,\mathcal{P})} & & \downarrow{\scriptstyle \partial_n(N,\mathcal{Q})} \\ H_{n-1}(M', N; \underline{P}') & \xrightarrow{H_{n-1}(f',N;\underline{P}',\underline{Q}')} & H_{n-1}(L', N; \underline{Q}'). \end{array} \tag{2.4.2}$$

Demostración. *i)* Sean F y G aplicaciones de cadena sobre f y g respectivamente. Entonces, el diagrama

$$\begin{array}{ccccc} P_0' & \xrightarrow{F_0} & P_0 & \xrightarrow{G_0} & P_0'' \\ \downarrow{\scriptstyle \epsilon'} & & \downarrow{\scriptstyle \epsilon} & & \downarrow{\scriptstyle \epsilon''} \\ M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' \end{array}$$

conmuta y, en consecuencia, $\epsilon'' \circ G_0 \circ F_0 = g \circ f \circ \epsilon$, i.e. $G \circ F$ es una aplicación de cadena sobre $g \circ f$. Por tanto, en vista de la Observación 11,

$$\begin{aligned} H_n(g \circ f, N; \underline{P}', \underline{P}'') = H_n((G \otimes Id_N) \circ (F \otimes Id_N) &= H_n(G \otimes Id_N) \circ H_n(F \otimes Id_N) \\ &= H_n(g, N; \underline{P}', \underline{P}) \circ H_n(f, N; \underline{P}, \underline{P}''). \end{aligned}$$

Más aún, $\{Id_{P_n} : P_n \longrightarrow P_n\}_{n \in \mathbb{N}} = Id_{\underline{P}} : \underline{P} \longrightarrow \underline{P}$ es una aplicación de cadena sobre Id_M. En consecuencia, $H_n(Id_M, N; \underline{P}, \underline{P}) = H_n(Id_{\underline{P}} \otimes Id_N) = Id_{H_n(\underline{P} \otimes_R N)} = Id_{H_n(M,N;P)}$.
ii) Como la Sucesión $\mathcal{P}$ es exacta, se tiene que, para cada $n \in \mathbb{N}$, la sucesión:

$$\mathcal{P}_n : 0 \longrightarrow P_n' \xrightarrow{\varphi_n} P_n \xrightarrow{\pi_n} P_n'' \longrightarrow 0$$

es exacta. Además, como en virtud de la Proposición A.6.5, el functor $(- \otimes_R N)$ es exacto a derecha, se tiene que la sucesión:

$$P_n' \otimes_R N \xrightarrow{\varphi_n \otimes Id_N} P_n \otimes_R N \xrightarrow{\pi_n \otimes Id_N} P_n'' \otimes_R N \longrightarrow 0$$

es exacta. Ahora bien, sea $m \otimes n \in P'_n \otimes_R N$ tal que $(\varphi_n \otimes Id_N)(m \otimes n) = 0$. Como P''_n es proyectivo, en virtud de la Proposición A.4.2, la sucesión $\mathcal{P}_n$ se escinde. Esto es, existe $h_n : P_n \longrightarrow P'_n$ tal que $h_n \circ \varphi_n = Id_{P'_n}$. Entonces,

$$0 = (h_n \otimes Id_N)(0) = ((h_n \otimes Id_N) \circ (\varphi_n \otimes Id_N))(m \otimes n) = (Id_{P'_n} \otimes Id_N)(m \otimes n) = m \otimes n.$$

Por tanto, $\varphi \otimes Id_N$ es monomorfismo de R-módulos y, en consecuencia, la sucesión:

$$0 \longrightarrow P'_n \otimes_R N \overset{\varphi_n \otimes Id_N}{\longrightarrow} P_n \otimes_R N \overset{\pi_n \otimes Id_N}{\longrightarrow} P''_n \otimes_R N \longrightarrow 0$$

es exacta para cada $n \in \mathbb{N}$. Es decir, la sucesión de complejos de cadena:

$$0 \longrightarrow \underline{P}' \otimes_R N \overset{\varphi \otimes Id_N}{\longrightarrow} \underline{P} \otimes_R N \overset{\pi \otimes Id_N}{\longrightarrow} \underline{P}'' \otimes_R N \longrightarrow 0 \tag{2.4.3}$$

es exacta, donde $\varphi = \{\varphi_n\}_{n \in \mathbb{N}}$ y $\pi = \{\pi_n\}_{n \in \mathbb{N}}$. Ahora, aplicando la Proposición 2.2.3 a la Sucesión (2.4.3) precedente, se sigue que la sucesión:

$$\begin{gathered}\cdots \longrightarrow H_n(\underline{P}'' \otimes_R N) \overset{\partial_n(N,\mathcal{P})}{\longrightarrow} H_{n-1}(\underline{P}' \otimes_R N) \overset{H_{n-1}(\phi \otimes Id_N)}{\longrightarrow} H_{n-1}(\underline{P} \otimes_R N) \\ \overset{H_{n-1}(\pi \otimes Id_N)}{\longrightarrow} H_{n-1}(\underline{P}'' \otimes_R N) \longrightarrow \cdots \longrightarrow H_0(\underline{P}'' \otimes_R N) \longrightarrow 0\end{gathered}$$

es exacta. Pero como $\mathcal{P}$ es una resolución proyectiva de $0 \longrightarrow M' \overset{i}{\longrightarrow} M \overset{j}{\longrightarrow} M'' \longrightarrow 0$, $\varphi : \underline{P}' \longrightarrow \underline{P}$ es una aplicación de cadena sobre i; y $\pi : \underline{P} \longrightarrow \underline{P}''$ es una aplicación de cadena sobre j. En consecuencia, $H_n(\varphi \otimes Id_N) = H_n(i, N; \underline{P}', \underline{P})$ y $H_n(\pi \otimes Id_N) = H_n(j, N; \underline{P}, \underline{P}'')$ para cada $n \in \mathbb{N}$. Además, $H_n(\underline{P}' \otimes_R N) = H_n(M', N; \underline{P}')$; $H_n(\underline{P} \otimes_R N) = H_n(M, N; \underline{P})$; y $H_n(\underline{P}'' \otimes_R N) = H_n(M'', N; \underline{P}'')$, con lo que se tiene *ii*).
iii) Siguiendo el mismo argumento que en el apartado *ii*), se tiene que las sucesiones de complejos de cadena:

$$0 \longrightarrow \underline{P}' \otimes_R N \longrightarrow \underline{P} \otimes_R N \longrightarrow \underline{P}'' \otimes_R N \longrightarrow 0, \quad 0 \longrightarrow \underline{Q}' \otimes_R N \longrightarrow \underline{Q} \otimes_R N \longrightarrow \underline{Q}'' \otimes_R N \longrightarrow 0$$

son exactas. Además, como el Diagrama (2.4.1) es conmutativo, también lo será el diagrama:

$$\begin{tikzcd} 0 \arrow[r] & \underline{P}' \otimes_R N \arrow[r, "\varphi^1 \otimes Id_N"] \arrow[d, "F' \otimes Id_N"] & \underline{P} \otimes_R N \arrow[r, "\pi^1 \otimes Id_N"] \arrow[d, "F \otimes Id_N"] & \underline{P}'' \otimes_R N \arrow[r] \arrow[d, "F'' \otimes Id_N"] & 0 \\ 0 \arrow[r] & \underline{Q}' \otimes_R N \arrow[r, "\varphi^2 \otimes Id_N"] & \underline{Q} \otimes_R N \arrow[r, "\pi^2 \otimes Id_N"] & \underline{Q}'' \otimes_R N \arrow[r] & 0 \end{tikzcd}$$

Aplicando la Proposición 2.2.4, se sigue que el diagrama:

$$\begin{tikzcd} H_n(\underline{P} \otimes_R N) \arrow[r, "H_n(\pi^1 \otimes Id_N)"] \arrow[d, "H_n(F \otimes Id_N)"] & H_n(\underline{P}'' \otimes_R N) \arrow[r, "\partial_n(N,\mathcal{P})"] \arrow[d, "H_n(F'' \otimes Id_N)"] & H_{n-1}(\underline{P}' \otimes_R N) \arrow[r, "H_{n-1}(\varphi^1 \otimes Id_N)"] \arrow[d, "H_{n-1}(F' \otimes Id_N)"'] & H_{n-1}(\underline{P} \otimes_R N) \arrow[d, "H_{n-1}(F \otimes Id_N)"'] \\ H_n(\underline{Q} \otimes_R N) \arrow[r, "H_n(\pi^2 \otimes Id_N)"] & H_n(\underline{Q}'' \otimes_R N) \arrow[r, "\partial_n(N,\mathcal{Q})"] & H_{n-1}(\underline{Q}' \otimes_R N) \arrow[r, "H_{n-1}(\varphi^2 \otimes Id_N)"] & H_{n-1}(\underline{Q} \otimes_R N) \end{tikzcd}$$

es conmutativo. Ahora bien, como F, F' y F'' son aplicaciones de cadena sobre f, f' y f'' respectivamente, se tiene que $H_n(F \otimes Id_N) = H_n(f, N; \underline{P}, \underline{Q})$; $H_n(F' \otimes Id_N) = H_n(f', N; \underline{P}', \underline{Q}')$; y $H_n(F'' \otimes N) = H_n(f'', N; \underline{P}'', \underline{Q}'')$. Por tanto, en particular, el Diagrama (2.4.2) conmuta. $\square$

PROPOSICIÓN 2.4.2. *Sea M un R-módulo y sean $(\underline{P}, \epsilon_P)$, $(\underline{Q}, \epsilon_Q)$ dos resoluciones proyectivas de M. Entonces,*

$$H_n(Id_M, N; \underline{P}, \underline{Q}) : H_n(M, N; \underline{P}) \longrightarrow H_n(M, N; \underline{Q})$$

es un isomorfismo de R-módulos, para cada $n \in \mathbb{N}$. Además, si $f : M \longrightarrow M'$ es un morfismo de R-módulos y $\underline{P}'$, $\underline{Q}'$ son resoluciones proyectivas de M', entonces el diagrama:

$$\begin{tikzcd} H_n(M, N; \underline{P}) \arrow[r, "H_n(Id_M, N; \underline{P}, \underline{Q})"] \arrow[d, "H_n(f, N; \underline{P}, \underline{P}')"] & H_n(M, N; \underline{Q}) \arrow[d, "H_n(f, N; \underline{Q}, \underline{Q}')"] \\ H_n(M', N\underline{P}') \arrow[r, "H_n(Id_{M'}, N; \underline{P}', \underline{Q}')"] & H_n(M', N; \underline{Q}') \end{tikzcd} \tag{2.4.4}$$

es conmutativo para todo $n \in \mathbb{N}$. Más aún, si $\mathcal{M} : 0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ es una sucesión exacta de R-módulos y

$$\mathcal{P} : \ 0 \longrightarrow \underline{P}' \longrightarrow \underline{P} \longrightarrow \underline{P}'' \longrightarrow 0, \quad \mathcal{Q} : \ 0 \longrightarrow \underline{Q}' \longrightarrow \underline{Q} \longrightarrow \underline{Q}'' \longrightarrow 0$$

son resoluciones proyectivas de $\mathcal{M}$, entonces el diagrama:

$$(2.4.5)\qquad \begin{array}{ccc} H_n(M'', N; \underline{P}'') & \xrightarrow{H_n(Id_{M''}, N; \underline{P}'', \underline{Q}'')} & H_n(M'', N; \underline{Q}'') \\ \Big\downarrow \partial_n(N,\mathcal{P}) & & \Big\downarrow \partial_n(N,\mathcal{Q}) \\ H_{n-1}(M', N; \underline{P}') & \xrightarrow{H_{n-1}(Id_{M'}, N; \underline{P}', \underline{Q}')} & H_{n-1}(M', N; \underline{Q}') \end{array}$$

conmuta para todo $n \in \mathbb{N}$, $n \geq 1$.

Demostración. Tomando $M = M' = M''$; $f = g = Id_M$; $\underline{P} = \underline{P}''$; $\underline{P}' = \underline{Q}$ en el apartado $i)$ del Lema 2.4.1 precedente, se tiene que:

$$H_n(Id_M, N; \underline{Q}, \underline{P}) \circ H_n(Id_M, N; \underline{P}, \underline{Q}) = H_n(Id_M, N; \underline{P}, \underline{P}) = Id_{H_n(M,N;\underline{P})}.$$

De la misma manera,

$$H_n(Id_M, N; \underline{P}, \underline{Q}) \circ H_n(Id_M, N; \underline{Q}, \underline{P}) = H_n(Id_M, N; \underline{Q}, \underline{Q}) = Id_{H_n(M,N;\underline{Q})}.$$

En consecuencia, $H_n(Id_M, N; \underline{P}, \underline{Q})$ y $H_n(Id_M, N; \underline{Q}, \underline{P})$ son isomorfismos de R-módulos. Ahora, si $f : M \longrightarrow M'$ es un morfismo de R-módulos, de nuevo, aplicando el apartado $i)$ del Lema 2.4.1 a la composición de f con las aplicaciones identidad correspondientes a izquierda y derecha, se tiene:

$$\begin{aligned} H_n(f, N; \underline{Q}, \underline{Q}') \circ H_n(Id_M, N; \underline{P}, \underline{Q}) &= H_n(f \circ Id_M, N; \underline{P}, \underline{Q}') = H_n(f, N; \underline{P}, \underline{Q}') \\ &= H_n(Id_{M'} \circ f, N; \underline{P}, \underline{Q}') = H_n(Id_{M'}, N; \underline{P}', \underline{Q}') \circ H_n(f, N; \underline{P}, \underline{P}'), \end{aligned}$$

de donde se sigue la conmutatividad del Diagrama (2.4.4).
Finalmente, consideremos el diagrama conmutativo:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \Big\downarrow Id_{M'} & & \Big\downarrow Id_M & & \Big\downarrow Id_{M''} & & \\ 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0, \end{array}$$

cuyas filas son la sucesión exacta $\mathcal{M}$. Entonces, estamos en las condiciones de la Proposición 2.3.4. Por tanto, existen aplicaciones de cadena $F : \underline{P} \longrightarrow \underline{Q}$; $F' : \underline{P}' \longrightarrow \underline{Q}'$; $F'' : \underline{P}'' \longrightarrow \underline{Q}''$ sobre f, f' y f'' respectivamente de forma que el diagrama:

$$(2.4.6)\qquad \begin{array}{ccccccccc} 0 & \longrightarrow & \underline{P}' & \longrightarrow & \underline{P} & \longrightarrow & \underline{P}'' & \longrightarrow & 0 \\ & & \Big\downarrow F' & & \Big\downarrow F & & \Big\downarrow F'' & & \\ 0 & \longrightarrow & \underline{Q}' & \longrightarrow & \underline{Q} & \longrightarrow & \underline{Q}'' & \longrightarrow & 0 \end{array}$$

conmute. Notemos que se trata de un caso particular del enunciado $iii)$ del Lema 2.4.1 precedente, donde se han tomado $L = M$, $L' = M'$, $L'' = M''$; $f = Id_M$, $f' = Id_{M'}$, $f'' = Id_{M''}$. Por tanto, se sigue que el Diagrama (2.4.5) es conmutativo. □

Definición 34 (**Functores Tor**). *Sea N un R-módulo y $n \in \mathbb{N}$. Se define el functor $Tor_n^R(-, N)$, de la categoría de R-módulos en sí misma, de la manera siguiente:*

i) A cada R-módulo M le asigna el R-módulo $Tor_n^R(M, N) := H_n(M, N; \underline{P})$, donde $\underline{P}$ es una resolución proyectiva de M;

ii) a cada morfismo $f : M \longrightarrow M'$ de R-módulos le asigna el morfismo :

$$Tor_n^R(f, N) := H_n(f, N; \underline{P}, \underline{P}') : Tor_n^R(M, N) \longrightarrow Tor_n^R(M', N),$$

donde $\underline{P}$ y $\underline{P}'$ son resoluciones proyectivas de M y M' respectivamente.

Notemos que el enunciado $i)$ del Lema 2.4.1 prueba que $Tor_n^R(-, N)$ es un functor covariante. La Proposición 2.4.2 implica que $H_n(M, N; \underline{P}) = Tor_n^R(M, N)$ no depende de la resolución proyectiva $\underline{P}$ de M elegida (salvo isomorfismo). Además, si $f : M \longrightarrow M'$ es un morfismo de R-módulos y $\underline{P}'$,$\underline{Q}'$ son resoluciones proyectivas de M', se tiene, de nuevo, por la Proposición 2.4.2, $H_n(f, N; \underline{P}, \underline{P}')$ es independiente de las resoluciones $\underline{P}$, $\underline{P}'$ elegidas, por lo que se denotará como $Tor_n^R(f, N)$. Más aún, dado un R-módulo N y una sucesión exacta de R-módulos $\mathcal{M}$:

$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$, el Diagrama (2.4.5) de la Proposición 2.4.2 garantiza que los morfismos conectores:

$$\partial_n(N, \mathcal{P}) : H_n(M'', N; \underline{P}'') \longrightarrow H_{n-1}(M', N; \underline{P}')$$

no dependen de la resolución $0 \longrightarrow \underline{P}' \longrightarrow \underline{P} \longrightarrow \underline{P}'' \longrightarrow 0$ de $\mathcal{M}$ elegida (salvo composición con isomorfismos). Por tanto, se denotarán por:

$$\partial_n(M'', M'; N) : Tor_n^R(M'', N) \longrightarrow Tor_{n-1}^R(M', N) \qquad n \in \mathbb{N},\ n \geq 1.$$

Supongamos ahora que $\underline{P}$ es una resolución proyectiva de M y $f : N \longrightarrow N'$ es un morfismo de R-módulos. Entonces, f induce una aplicación de cadena

$$\{Id_{P_n} \otimes f\}_{n\in\mathbb{N}} = Id_{\underline{P}} \otimes f : \underline{P} \otimes_R N \longrightarrow \underline{P} \otimes_R N',$$

donde:

$$\begin{array}{rccc} Id_{P_n} \otimes f : & \underline{P} \otimes_R N & \longrightarrow & \underline{P} \otimes_R N' \\ & p \otimes n & \mapsto & p \otimes f(n). \end{array}$$

Ahora, en virtud de la Proposición 2.2.1, $Id_{\underline{P}} \otimes f$ induce un morfismo de R-módulos:

$$H_n(\mathrm{Id}_{\underline{P}} \otimes f) : H_n(\underline{P} \otimes_R N) \longrightarrow H_n(\underline{P} \otimes_R N').$$

Ahora bien, se tiene que $H_n(\underline{P} \otimes_R N) = H_n(M, N; \underline{P}) = Tor_n^R(M, N)$ y $H_n(\underline{P} \otimes_R N') = H_n(M, N'; \underline{P}) = Tor_n^R(M, N')$. En vista de estas consideraciones, podemos dar la siguiente definición:

Definición 35 (**Functores Tor**). *Sea M un R-módulo y $n \in \mathbb{N}$. Se define el functor $Tor_n^R(M, -)$, de la categoría de R-módulos en sí misma, como sigue:*

i) A cada R-módulo N le asigna el R-módulo $Tor_n^R(M, N)$;

ii) a cada morfismo de R-módulos $f : N \longrightarrow N'$ le asigna el morfismo:

$$Tor_n^R(N, f) := H_n(Id_{\underline{P}} \otimes f) : Tor_n^R(M, N) \longrightarrow Tor_n^R(M, N'),$$

donde $\underline{P}$ es una resolución proyectiva de M.

Es sencillo verificar, usando la Proposición 2.2.1, que $Tor_n^R(M, -)$ es un functor covariante de la categoría de R-módulos en sí misma. Ahora bien, si $f : N \longrightarrow N'$ es un morfismo de R-módulos y $\underline{P}$, $\underline{Q}$ son resoluciones proyectivas de M y $n \in \mathbb{N}$, consideremos el diagrama:

$$\begin{array}{ccc} H_n(M, N; \underline{P}) & \xrightarrow{H_n(Id_{\underline{P}} \otimes f)} & H_n(M, N'; \underline{P}) \\ {\scriptstyle H_n(Id_M, N; \underline{P}, \underline{Q})}\Big\downarrow & & \Big\downarrow{\scriptstyle H_n(Id_M, N'; \underline{P}, \underline{Q})} \\ H_n(M, N; \underline{Q}) & \xrightarrow{H_n(Id_{\underline{Q}} \otimes f)} & H_n(M, N'; \underline{Q}) \end{array} \tag{2.4.7}$$

Notemos que $H_n(Id_M, N; \underline{P}, \underline{Q}) = H_n(F \otimes Id_N)$ y $H_n(Id_M, N'; \underline{P}, \underline{Q}) = H_n(F \otimes Id_{N'})$ para cualquier $F : \underline{P} \longrightarrow \underline{Q}$ aplicación de cadena sobre Id_M. Entonces, se sigue que:

$$\begin{aligned} H_n(F \otimes Id_{N'}) \circ H_n(Id_{\underline{P}} \otimes f) &= H_n((F \circ Id_{\underline{P}}) \otimes (Id'_N \circ f)) = H_n(F \otimes f) \\ &= H_n((Id_{\underline{Q}} \circ F) \otimes (f \circ Id_N)) = H_n(Id_{\underline{Q}} \otimes f) \circ H_n(F \otimes Id_N), \end{aligned}$$

de donde se sigue la conmutatividad del Diagrama (2.4.7). Además, por la Proposicion 2.4.2, se tiene que $H_n(Id_M, N; \underline{Q}, \underline{P})$ y $H_n(Id_M, N'; \underline{P}, \underline{Q})$ son isomorfismos. Por consiguiente, $H_n(Id_{\underline{P}} \otimes f) = Tor_n^R(M, f)$ es independiente de la resolución proyectiva $\underline{P}$ de M elegida (salvo composición con isomorfismos). Consideremos ahora un R-módulo M, una resolución proyectiva $(\underline{P}, \epsilon)$ de M y una sucesión exacta de R-módulos: $0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$. Como P_n es un R-módulo proyectivo para todo $n \in \mathbb{N}$, en virtud de la Proposición A.4.4, $0 \longrightarrow P_n \otimes_R N' \longrightarrow P_n \otimes_R N \longrightarrow P_n \otimes_R N'' \longrightarrow 0$ es una sucesión exacta de R-módulos para todo $n \in \mathbb{N}$. Por tanto la sucesión de complejos de cadena $\mathcal{P} : 0 \longrightarrow \underline{P} \otimes_R N' \longrightarrow \underline{P} \otimes_R N \longrightarrow \underline{P} \otimes_R N'' \longrightarrow 0$ es exacta. En virtud de la Proposición 2.2.2, existen morfismos conectores:

$$\partial_n : Tor_n^R(M, N'') = H_n(\underline{P} \otimes_R N'') \longrightarrow H_{n-1}(\underline{P} \otimes_R N') = Tor_{n-1}^R(M, N'), \qquad n \in \mathbb{N},\ n \geq 1.$$

Veamos ahora que estos morfismos conectores no dependen de la resolución proyectiva $(\underline{P}, \epsilon)$ de M elegida (salvo composición con isomorfismos). Sean $(\underline{P}, \epsilon_P)$ y $(\underline{Q}, \epsilon_Q)$ dos resoluciones proyectivas de M y $0 \longrightarrow N' \xrightarrow{i} N \xrightarrow{j} N'' \longrightarrow 0$ una sucesión exacta de R-módulos. Por la

Proposición 2.3.2, existe $F : \underline{P} \longrightarrow \underline{Q}$ una aplicación de cadena sobre Id_M. En consecuencia, se tiene el siguiente diagrama conmutativo cuyas filas son sucesiones exactas:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \underline{P} \otimes_R N' & \xrightarrow{Id_{\underline{P}} \otimes i} & \underline{P} \otimes_R N & \xrightarrow{Id_{\underline{P}} \otimes j} & \underline{P} \otimes_R N'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle F\otimes Id_{N'}} & & \downarrow{\scriptstyle F\otimes Id_{N}} & & \downarrow{\scriptstyle F\otimes Id_{N''}} & & \\
0 & \longrightarrow & \underline{Q} \otimes_R N' & \xrightarrow{Id_{\underline{Q}} \otimes i} & \underline{Q} \otimes_R N & \xrightarrow{Id_{\underline{Q}} \otimes j} & \underline{Q} \otimes_R N'' & \longrightarrow & 0
\end{array}$$

Por la Proposición 2.2.4, se sigue que el siguiente diagrama es conmutativo para todo $n \geq 1$:

$$\begin{array}{ccc}
H_n(\underline{P} \otimes_R N'') & \xrightarrow{H_n(F \otimes Id_{N''})} & H_n(\underline{Q} \otimes_R N'') \\
\downarrow{\scriptstyle \partial_n} & & \downarrow{\scriptstyle \partial_n} \\
H_{n-1}(\underline{P} \otimes_R N') & \xrightarrow{H_{n-1}(F \otimes Id_{N'})} & H_{n-1}(\underline{Q} \otimes_R N'),
\end{array}$$

donde $H_{n-1}(F \otimes Id_{N'}) = H_{n-1}(Id_M, N'; \underline{P}, \underline{Q})$ y $H_n(F \otimes Id_{N''}) = H_n(Id_M, N''; \underline{P}; \underline{Q})$ son isomorfismos (cf. Proposición 2.4.2). Por tanto, estos morfismos conectores se denotarán por $\partial_n(M; N'', N') : Tor_n^R(M, N'') \longrightarrow Tor_{n-1}^R(M, N')$.

Teorema 2.4.3. *i) Sean N un R-módulo y $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ es una sucesión exacta de R-módulos. Entonces, se tienen las sucesiones exactas:*

$$\cdots \longrightarrow Tor_n^R(M'', N) \overset{\partial_n(M'',M';N)}{\longrightarrow} Tor_{n-1}^R(M', N) \overset{Tor_{n-1}^R(f,N)}{\longrightarrow} Tor_{n-1}^R(M, N) \overset{Tor_{n-1}^r(g,N)}{\longrightarrow}$$
$$\overset{Tor_{n-1}^r(g,N)}{\longrightarrow} Tor_{n-1}^R(M'', N) \longrightarrow \cdots \longrightarrow Tor_0^R(M'', N) \longrightarrow 0,$$

$$\cdots \longrightarrow Tor_n^R(N, M'') \overset{\partial_n(N,M'';M')}{\longrightarrow} Tor_{n-1}^R(N, M') \overset{Tor_{n-1}^R(N,f)}{\longrightarrow} Tor_{n-1}^R(N, M) \overset{Tor_{n-1}^r(N,g)}{\longrightarrow}$$
$$\overset{Tor_{n-1}^r(N,g)}{\longrightarrow} Tor_{n-1}^R(N, M'') \longrightarrow \cdots \longrightarrow Tor_0^R(N, M'') \longrightarrow 0.$$

ii) Si el diagrama:

$$\begin{array}{cccccccccc}
\mathcal{M}: & 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\
 & & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\
\mathcal{K}: & 0 & \longrightarrow & K' & \longrightarrow & K & \longrightarrow & K'' & \longrightarrow & 0,
\end{array} \tag{2.4.8}$$

cuyas filas son sucesiones exactas de R-módulos, es conmutativo, se tiene que los diagramas siguientes son conmutativos para todo $n \in \mathbb{N}$, $n \geq 1$:

$$\begin{array}{ccc}
Tor_n^R(M'', N) & \xrightarrow{\partial_n(M'',M';N)} & Tor_{n-1}^R(M', N) \\
\downarrow{\scriptstyle Tor_n^R(f'',N)} & & \downarrow{\scriptstyle Tor_{n-1}^R(f',N)} \\
Tor_n^R(K'', N) & \xrightarrow{\partial_n(K'',K';N)} & Tor_{n-1}^R(K', N)
\end{array}
\qquad
\begin{array}{ccc}
Tor_n^R(N, M'') & \xrightarrow{\partial_n(N;M'',M')} & Tor_{n-1}^R(N, M') \\
\downarrow{\scriptstyle Tor_n^R(N,f'')} & & \downarrow{\scriptstyle Tor_{n-1}^R(N,f')} \\
Tor_n^R(N, K'') & \xrightarrow{\partial_n(N;K'',K')} & Tor_{n-1}^R(N, K').
\end{array}$$

iii) El functor $Tor_n^R(M, N)$ es lineal en M y N para todo $n \in \mathbb{N}$.
iv) Existe un isomorfismo $Tor_0^R(M, N) \cong M \otimes_R N$ que es functorial en M y N.

Demostración. *i)* La primera de las sucesiones es exactamente la sucesión del apartado *ii)* del Lema 2.4.1, que es exacta. Para comprobar la exactitud de la segunda se aplica la Proposición 2.2.3 a la sucesión exacta de complejos de cadena: $0 \longrightarrow \underline{Q} \otimes_R M' \longrightarrow \underline{Q} \otimes_R M \longrightarrow \underline{Q} \otimes_R M'' \longrightarrow 0$, donde $\underline{Q}$ es una resolución proyectiva cualquiera de N.
ii) Por una parte, tomemos resoluciones proyectivas $0 \longrightarrow \underline{P'} \longrightarrow \underline{P} \longrightarrow \underline{P''} \longrightarrow 0$ y $0 \longrightarrow \underline{Q'} \longrightarrow \underline{Q} \longrightarrow \underline{Q''} \longrightarrow 0$ de $\mathcal{M}$ y $\mathcal{K}$ respectivamente. Por la Proposición 2.3.2, se tiene que existen aplicaciones de cadena $F' : \underline{P'} \longrightarrow \underline{Q'}$ y $F'' : \underline{P''} \longrightarrow \underline{Q''}$ sobre f' y f'' respectivamente. Ahora, en virtud de la Proposición 2.3.4, existe una aplicación de cadena $F : \underline{P} \longrightarrow \underline{Q}$ sobre f que hace el Diagrama (2.4.1) conmute. Por el apartado *iii)* del Lema 2.4.1, el Diagrama (2.4.2), que es el primer diagrama de *ii)*, conmuta. De otro lado, si $\underline{P}$ es una resolución proyectiva

cualquiera de N, como el Diagrama (2.4.8) es conmutativo, también lo será el diagrama:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \underline{P}\otimes_R M' & \longrightarrow & \underline{P}\otimes_R M & \longrightarrow & \underline{P}\otimes_R M'' & \longrightarrow & 0 \\ & & \big\downarrow{\scriptstyle Id_{\underline{P}}\otimes f'} & & \big\downarrow{\scriptstyle Id_{\underline{P}}\otimes f} & & \big\downarrow{\scriptstyle Id_{\underline{P}}\otimes f''} & & \\ 0 & \longrightarrow & \underline{P}\otimes_R K' & \longrightarrow & \underline{P}\otimes_R K & \longrightarrow & \underline{P}\otimes_R K'' & \longrightarrow & 0 \end{array}$$

Aplicando la Proposición 2.2.4 al diagrama anterior, se sigue que el diagrama:

$$\begin{array}{ccc} H_n(\underline{P}\otimes_R M') & \xrightarrow{\partial_n} & \underline{P}\otimes_R M'' \\ {\scriptstyle H_n(Id_{\underline{P}}\otimes f')}\big\downarrow & & \big\downarrow{\scriptstyle H_n(Id_{\underline{P}}\otimes f'')} \\ \underline{P}\otimes_R K' & \xrightarrow{\partial'_n} & \underline{P}\otimes_R K'' \end{array}$$

donde ∂_n y ∂'_n son los morfismos conectores correspondientes, es conmutativo. Es decir, el segundo diagrama del apartado $ii)$ es conmutativo.
$iii)$ De un lado, sean $k, l : N \longrightarrow N'$ morfismos de R-módulos; $a, b \in R$; $\underline{P}$ una resolución proyectiva de un R-módulo M. Entonces, para cada $n \in \mathbb{N}$, se tiene que:

$$\begin{gathered} aTor_n^R(M,k) + bTor_n^R(M,l) = aH_n((Id_{\underline{P}}\otimes k)) + bH_n((Id_{\underline{P}}\otimes l)) \\ = H_n(Id_{\underline{P}}\otimes ak + Id_{\underline{P}}\otimes bl) = H_n(Id_{\underline{P}}, ak+bl) = Tor_n^R(M, ak+bl). \end{gathered}$$

En consecuencia, se tiene la linealidad en N. De otro lado, sea N un R-módulo; $f, g : M \longrightarrow M'$ morfismos de R-módulos; $a, b \in R$; $(\underline{P}, \epsilon)$ y $(\underline{P}', \epsilon')$ resoluciones proyectivas de M y M' respectivamente; y $n \in \mathbb{N}$. Por la Proposición 2.3.2, existen aplicaciones de cadena $F, G : \underline{P} \longrightarrow \underline{P}'$ sobre f y g respectivamente. Entonces,

$$(af+bg)\circ\epsilon = a(f\circ\epsilon) + b(g\circ\epsilon) = a(\epsilon'\circ F_0) + b(\epsilon'\circ G_0) = \epsilon'\circ(aF_0+bG_0).$$

Por tanto, $aF + bG$ es una aplicación de cadena sobre $af + bg$. En consecuencia,

$$\begin{aligned} Tor_n^R(af+bg, N) &= H_n(af+bg, N; \underline{P}, \underline{P}') = H_n((aF+bG)\otimes Id_N) \\ &= H_n((aF\otimes Id_N) + (bG\otimes Id_N)) = H_n(aF\otimes Id_N) + H_n(bG\otimes Id_N) \\ &= aH_n(F\otimes Id_N) + bH_n(G\otimes Id_N) = aTor_n^R(f,M) + bTor_n^R(g,N), \end{aligned}$$

donde las igualdades se siguen de la linealidad del morfismo inducido por una aplicación de cadena (ver Proposición 2.2.1). Por tanto, $Tor_n^R(M,N)$ es lineal en M.
$iv)$ Sean N y M dos R-módulos, y sea $(\underline{P}, \epsilon)$ una resolución proyectiva de M. Entonces, como la sucesión $P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} M \longrightarrow 0$ es exacta y, por la Proposición A.6.5, el functor $(-\otimes_R N)$ es exacto a derecha, se sigue que la sucesión de R-módulos:

$$P_1\otimes_R N \xrightarrow{d_1\otimes Id_N} P_0\otimes_R N \xrightarrow{\epsilon\otimes Id_N} M\otimes_R N \longrightarrow 0 \tag{2.4.9}$$

es exacta. En particular, $\epsilon\otimes Id_N : P_0\otimes_R N \longrightarrow M\otimes_R N$ es epimorfismo de R-módulos. En virtud del Primer Teorema de Isomorfía, $P_0\otimes_R N/ker(\epsilon\otimes Id_N) \cong M\otimes_R N$. Ahora bien, por exactitud de la Sucesión (2.4.9), $ker(\epsilon\otimes Id_N) = Im(d_1\otimes Id_N)$. Entonces,

$$Tor_0^R(M,N) = P_0\otimes N/Im(d_1\otimes Id_N) \cong M\otimes_R N,$$

Dicho isomorfismo se denotará por:

$$\begin{array}{cccc} \epsilon(M,N): & Tor_0^R(M,N) & \longrightarrow & M\otimes_R N \\ & x + Im(d_1\otimes Id_N) & \mapsto & (\epsilon\otimes Id_N)(x), \end{array}$$

para cada $x \in P_0\otimes_R N$. Veamos que $\epsilon(M,N)$ es functorial en M y N. Sea $f : M \longrightarrow M'$ un morfismo de R-módulos y sean $(\underline{P}, \epsilon)$, $(\underline{P}', \epsilon')$ resoluciones proyectivas de M y M' respectivamente. En virtud de la Proposición 2.3.2, podemos suponer que existe una aplicación de cadena $F : \underline{P} \longrightarrow \underline{P}'$ sobre f. Consideremos el siguiente diagrama:

$$\begin{array}{ccc} Tor_0^R(M,N) & \xrightarrow{\epsilon(M,N)} & M\otimes_R N \\ {\scriptstyle Tor_0^R(f,N)}\big\downarrow & & \big\downarrow{\scriptstyle f\otimes Id_N} \\ Tor_0^R(M',N) & \xrightarrow{\epsilon(M',N)} & M'\otimes_R N \end{array} \tag{2.4.10}$$

Utilizando F para evaluar $Tor^R(f,N)$, se tiene que:

$$\begin{aligned} \epsilon(M',N)\circ Tor_0^R(f,N) &= \epsilon(M',N)\circ H_0(F\otimes Id_N) = \\ = (\epsilon'\circ F_0)\otimes Id_N = (f\circ\epsilon)\otimes Id_N &= f\otimes Id_N\circ\epsilon\otimes Id_N = f\otimes Id_N\circ\epsilon(M,N), \end{aligned}$$

de donde se sigue la conmutatividad del Diagrama (2.4.10). Esto prueba que $\epsilon(M,N)$ es functorial en M. De otro lado, si $g: N \longrightarrow N'$ es un morfismo de R-módulos y $\underline{P}$ es una resolución proyectiva de M, podemos considerar el diagrama:

$$\begin{array}{ccc} Tor_0^R(M,N) & \xrightarrow{\epsilon(M,N)} & M\otimes_R N \\ {\scriptstyle Tor_0^R(M,g)}\downarrow & & \downarrow{\scriptstyle Id_M\otimes g} \\ Tor_0^R(M,N') & \xrightarrow{\epsilon(M,N')} & M\otimes_R N' \end{array} \tag{2.4.11}$$

Se tiene que:

$$\begin{aligned} \epsilon(M,N')\circ Tor_0^R(M,g) = \epsilon(M,N')\circ H_0(Id_{\underline{P}}\otimes g) &= \epsilon\otimes Id_{N'}\circ Id_{P_0}\otimes g = \epsilon\otimes g \\ &= (Id_M\otimes g)\circ(\epsilon\otimes Id_N) = Id_M\otimes g\circ\epsilon(M,N), \end{aligned}$$

de donde se sigue la conmutatividad del Diagrama (2.4.11). Esto prueba que $\epsilon(M,N)$ es functorial en N. □

LEMA 2.4.4. *Sea P un R-módulo proyectivo. Entonces, $Tor_n^R(P,M) = 0$ y $Tor_n^R(M,P) = 0$ para todo R-módulo M y todo $n\in\mathbb{N}$, $n\geq 1$.*

DEMOSTRACIÓN. Como P es un R-módulo proyectivo, se tiene que $\underline{P}: 0\longrightarrow P\xrightarrow{Id_P} P\longrightarrow 0$ es una resolución proyectiva de P. Por tanto, $P_0 = P$ y $P_n = 0$ para todo $n\in\mathbb{N}$, $n\geq 1$. Utilizando $\underline{P}$ para calcular $Tor_n^R(P,M)$, se tiene que $Tor_n^R(P,M) = 0$ para todo $n\in\mathbb{N}$, $n\geq 1$. De otro lado, sea $(\underline{Q},\epsilon)$ una resolución proyectiva de M. Entonces, por la Proposición A.4.4, la sucesión:

$$\mathcal{Q}:\cdots\longrightarrow Q_n\otimes_R P\xrightarrow{d_n\otimes Id_N} Q_{n-1}\otimes_R N\longrightarrow\cdots\longrightarrow Q_0\otimes_R P\xrightarrow{\epsilon\otimes Id_N} M\otimes_R P\longrightarrow 0$$

es exacta. Entonces, $H_n(\mathcal{Q}) = 0$ para todo $n\in\mathbb{N}$. En particular, $0 = H_{n+1}(\mathcal{Q}) = H_n(\underline{Q}\otimes_R P) = Tor_n^R(M,P)$ para todo $n\in\mathbb{N}$, $n\geq 1$. □

PROPOSICIÓN 2.4.5. *Sean M y N R-módulos. Entonces, para cada $n\in\mathbb{N}$ existe un isomorfismo $Tor_n^R(M,N)\cong Tor_n^R(N,M)$ que es functorial en M y N.*

DEMOSTRACIÓN. Probémoslo por inducción en n. Para $n=0$, se tiene $Tor_0^R(M,N)\cong M\otimes_R N\cong N\otimes_R M\cong Tor_0^R(N,M)$ por la Proposición A.6.2. Además, este isomorfismo es functorial en M y N. Sea $n\geq 1$. Tomamos el R-módulo libre $F = \bigoplus_M R$, el epimorfismo canónico $\pi: F\longrightarrow M$ y $K = ker(\pi)$. Consideramos la sucesión exacta de R-módulos: $0\longrightarrow K\xrightarrow{i} F\xrightarrow{\pi} M\longrightarrow 0$, donde i es la inclusión natural. Por el apartado $ii)$ del Teorema 2.4.3, las sucesiones de R-módulos:

$$Tor_n^R(F,N)\xrightarrow{Tor_n^R(\pi,N)} Tor_n^R(M,N)\xrightarrow{\partial_n(M,K;N)} Tor_{n-1}^R(K,N)\xrightarrow{Tor_{n-1}^R(i,N)} Tor_{n-1}^R(F,N)$$

$$Tor_n^R(N,F)\xrightarrow{Tor_n^R(N,\pi)} Tor_n^R(N,M)\xrightarrow{\partial_n(N;M,K)} Tor_{n-1}^R(N,K)\xrightarrow{Tor_{n-1}^R(N,i)} Tor_{n-1}^R(N,F)$$

son exactas. Notemos que, como F es un R-módulo libre, por el Corolario A.4.3, F es proyectivo y, por el Lema 2.4.4, $Tor_n^R(F,N) = 0$, para $n\geq 1$. Además, por hipótesis inductiva, existen isomorfismos $\phi(K,N) = \phi: Tor_{n-1}^R(K,N)\longrightarrow Tor_{n-1}^R(N,K)$, $\psi(F,N) = \psi: Tor_{n-1}^R(F,N)\longrightarrow Tor_{n-1}^R(N,F)$ functoriales en ambas variables. Entonces, se tiene el diagrama:

$$\begin{array}{ccccccc} 0 & \longrightarrow & Tor_n^R(M,N) & \xrightarrow{\partial_n(M,K;N)} & Tor_{n-1}^R(K,N) & \xrightarrow{Tor_{n-1}^R(i,N)} & Tor_{n-1}^R(F,N) \\ & & \vdots{\scriptstyle\varphi} & & \downarrow{\scriptstyle\phi} & & \downarrow{\scriptstyle\psi} \\ 0 & \longrightarrow & Tor_n^R(N,M) & \xrightarrow{\partial_n(N;M,K)} & Tor_{n-1}^R(N,K) & \xrightarrow{Tor_{n-1}^R(N,i)} & Tor_{n-1}^R(N,F), \end{array} \tag{2.4.12}$$

cuya conmutatividad viene garantizada por la functorialidad de los isomorfismos ϕ y ψ, y cuyas filas son sucesiones exactas de R-módulos. Entonces, $\partial_n(M,K;N)$ y $\partial_n(N;M,K)$ son monomorfismos y ϕ induce un morfismo de R-módulos:

$$\begin{array}{rccl} \varphi: & Tor_n^R(M,N) & \longrightarrow & Tor_n^R(N,M) \\ & x & \mapsto & \partial_n(N;M,K)^{-1}(\phi \circ \partial_n(M,K;N)(x)). \end{array}$$

Por una parte, como el Diagrama (2.4.12) conmuta, se tiene que:

$$Tor_{n-1}^R(N,i) \circ \phi \circ \partial_n(M,K;N) = \psi \circ Tor_{n-1}^R(i,N) \circ \partial_n(M,K;N).$$

Pero $Tor_{n-1}^R(i,N) \circ \partial_n(M,K;N) = 0$. Por tanto, $\phi \circ \partial_n(M,K;N) \in ker(Tor_{n-1}^R(N,i)) = Im(\partial_n(N;M,K))$. De otro lado, como $\partial_n(N;M,K)$ es inyectivo, φ queda unívocamente determinado, lo que garantiza su buena definición. Ahora bien, como $\partial_n(M,K;N)$ y ϕ son monomorfismos, también lo será su composición. De ahí se sigue que φ es monomorfismo. Por otro lado, sea $x \in Tor_n^R(N,M)$. Claramente, $(Tor_{n-1}^R(N,i) \circ \partial_n(N;M,K))(x) = 0$. Como ψ es isomorfismo, $(\psi^{-1} \circ Tor_{n-1}^R(N,i) \circ \partial_n(N;M,K))(x) = 0$. Pero

$$(\psi^{-1} \circ (Tor_{n-1}^R(N,i) \circ \partial_n)(N;M,K)(x) = (Tor_{n-1}^R(i,N) \circ \phi^{-1} \circ \partial_n(N;M,K))(x).$$

Por tanto,

$$(\phi^{-1} \circ \partial_n(N;M,K))(x) \in ker(Tor_{n-1}^R(i,N)) = Im(\partial_n(M,K;N)).$$

Entonces, existe $y \in Tor_n^R(M,N)$ verificando $(\phi \circ \partial_n(M,K;N))(y) = \partial_n(N;M,K)(x)$. En consecuencia, $\varphi(y) = x$ y φ es epimorfismo. Por consiguiente, φ es isomorfismo. Veamos que ϕ es functorial en M y N. Sea $f : M \longrightarrow M'$ un morfismo de R-módulos. Podemos tomar $F = \bigoplus_M R$, $F' = \bigoplus_{M'} R$; las proyecciones canónicas $\pi : F \longrightarrow M$, $\pi' : F' \longrightarrow M'$; y $K = ker(\pi)$, $K' = ker(\pi')$. Además, se puede definir $h : F \longrightarrow F'$ mediante $h(\delta_{mn}) := \delta_{f(m)n}$ y extendiéndolo por linealidad, donde δ_{mn} (resp. $\delta_{f(m)n}$) es la Delta de Kronecker, i.e. el elemento natural de la base canónica de F (resp. F'). Con esta definición, es claro que el diagrama:

(2.4.13)
$$\begin{tikzcd} 0 \arrow[r] & K \arrow[r, "i"] \arrow[d, dotted, "g"] & F \arrow[r, "\pi"] \arrow[d, "h"] & M \arrow[r] \arrow[d, "f"] & 0 \\ 0 \arrow[r] & K' \arrow[r, "i'"] & F' \arrow[r, "\pi'"] & M' \arrow[r] & 0, \end{tikzcd}$$

cuyas filas son sucesiones exactas de R-módulos, conmuta. Además, h induce un morfismo $g : K \longrightarrow K'$ dado por $g(x) = i'^{-1}((h \circ i)(x))$. Notemos que está bien definido, pues por exactitud de la fila superior del Diagrama (2.4.13) precedente:

$$\pi' \circ h \circ i = f \circ \pi \circ i = 0.$$

Por tanto, $Im(h \circ i) \subseteq ker(\pi') = Im(i')$, donde el último contenido se sigue de la exactitud de la fila inferior. Además, como i' es monomorfismo, g queda unívocamente determinado. Ahora bien, podemos considerar el diagrama:

(2.4.14)
$$\begin{tikzcd} Tor_n^R(M,N) \arrow[r, "\partial_n(M,K;N)"] \arrow[d, "Tor_n^R(f,N)"] & Tor_{n-1}^R(K,N) \arrow[r, "\phi(K,M)"] \arrow[d, "Tor_{n-1}^R(g,N)"] & Tor_{n-1}^R(N,K) \arrow[d, "Tor_{n-1}^R(N,g)"] \\ Tor_n^R(M',N) \arrow[r, "\partial_n(M',K';N)"] & Tor_{n-1}^R(K',N) \arrow[r, "\phi(K',N)"] & Tor_{n-1}^R(N,K') \end{tikzcd}$$

cuya conmutatividad queda garantizada por la functorialidad de ϕ y por el apartado $ii)$ del Teorema 2.4.3. Pero, como por el Diagrama (2.4.12),

$$\phi(K,M) \circ \partial_n(M,K;N) = \partial_n(N,M,K) \circ \varphi(M,N)$$

y

$$\phi(K',M') \circ \partial_n(M',K';N) = \partial_n(N,M',K') \circ \varphi(M',N),$$

se tiene que el diagrama:

(2.4.15)
$$\begin{tikzcd} Tor_n^R(M,N) \arrow[r, "\varphi(M,N)"] \arrow[d, "Tor_n^R(f,N)"] & Tor_n^R(N,M) \arrow[r, "\partial_n(N;M,K)"] & Tor_{n-1}^R(N,K) \arrow[d, "Tor_{n-1}^R(N,g)"] \\ Tor_n^R(M',N) \arrow[r, "\varphi(M',N)"] & Tor_n^R(N,M') \arrow[r, "\partial_n(N;M',K')"] & Tor_{n-1}^R(N,K') \end{tikzcd}$$

conmuta. Además, de nuevo, por el apartado *ii*) del Teorema 2.4.3, se tiene el diagrama conmutativo:

(2.4.16)
$$\begin{array}{ccc} Tor_n^R(N,M) & \xrightarrow{\partial_n(N;M,K)} & Tor_{n-1}^R(N,K) \\ \downarrow{\scriptstyle Tor_n^R(N,f)} & & \downarrow{\scriptstyle Tor_{n-1}^R(N,g)} \\ Tor_n^R(N,M') & \xrightarrow{\partial_n(N;M',K')} & Tor_{n-1}^R(N,K') \end{array}$$

Entonces, combinando los Diagramas (2.4.14) y (2.4.16) se tiene que

$$\partial_n(N;M',K') \circ \varphi(M',N) \circ Tor_n^R(N,f) = \partial_n(N;M',K') \circ Tor_n^R(N,f) \circ \varphi(M,N).$$

En consecuencia, $\varphi(M',N) \circ Tor_n^R(N,f) - Tor_n^R(N,f) \circ \varphi(M,N) \in ker(\partial_n(N,M',K')) = \{0\}$, pues se había visto previamente que $\partial_n(N,M',K')$ era monomorfismo. Por tanto, $Tor_n^R(N,f) \circ \varphi(M,N) = \varphi(M',N) \circ Tor_n^R(N,f)$. Es decir, el diagrama:

$$\begin{array}{ccc} Tor_n^R(M,N) & \xrightarrow{\varphi(M,N)} & Tor_n^R(N,M) \\ \downarrow{\scriptstyle Tor_n^R(f,N)} & & \downarrow{\scriptstyle Tor_n^R(N,f)} \\ Tor_n^R(M',N) & \xrightarrow{\varphi(M',N)} & Tor_n^R(N,M') \end{array}$$

conmuta y, por consiguiente, $\phi(M,N)$ es functorial en M. Se utiliza un argumento análogo para probar la functorialidad en N. □

2.5. Functores Ext

Como se indicó en la Introducción, nos limitamos a exponer las nociones y resultados esenciales (véase Sección B.2 para los detalles). Sean M,N R-módulos y $(\underline{P},\epsilon)$ una resolución proyectiva de M. Como el functor $Hom_R(-,N)$ es contravariante, se puede considerar la sucesión:

$$Hom_R(\underline{P},N) : 0 \longrightarrow Hom_R(P_0,N) \overset{Hom_R(d_1,N)}{\longrightarrow} Hom_R(P_1,N) \overset{Hom_R(d_2,N)}{\longrightarrow} \cdots$$

de acuerdo a las notaciones establecidas en la Sección A.3 del Apéndice A. Notemos que, dado $n \in \mathbb{N}$, $Hom_R(d_{n+1},N) \circ Hom_R(d_n,N) = Hom_R(d_n \circ d_{n+1},N) = Hom_R(0,N) = 0$. Por tanto, $Hom_R(\underline{P},N)$ es un complejo de co-cadena, cuyos módulos de co-homología se denotarán por $H^n(Hom_R(\underline{P},N)) = H^n(M,N;\underline{P})$. Sea ahora $f : M \longrightarrow M'$ un morfismo de R-módulos y (P,ϵ), (P',ϵ') resoluciones proyectivas de M y M' respectivamente. Por la Proposición 2.3.2, existe una aplicación $\{F_n\}_{n\in\mathbb{N}} = F : \underline{P} \longrightarrow \underline{P}'$ de co-cadena sobre f. Ahora bien, podemos considerar la aplicación de co-cadena:

$$\{Hom_R(F_n,N)\}_{n\in\mathbb{N}} = Hom_R(F,N) : Hom_R(\underline{P}',N) \longrightarrow Hom_R(\underline{P},N).$$

Entonces, en virtud de la Proposición 2.2.1, $Hom_R(F,N)$ induce un morfismo de R-módulos en los módulos de co-homología del complejo $Hom_R(\underline{P},N)$:

$$H^n(f,N;\underline{P}',\underline{P}) : H^n(Hom_R(\underline{P}',N)) \longrightarrow H^n(Hom_R(\underline{P},N)).$$

Definición 36 (**Functores Ext**). *Sea N un R-módulo y $n \in \mathbb{N}$. Se define el functor contravariante $Ext_R^n(-,N)$, de la categoría de R-módulos en sí misma, de la manera siguiente:*

i) A cada R-módulo M le asigna en R-módulo $Ext_R^n(M,N) := H^n(Hom_R(M,\underline{P}))$, donde $\underline{P}$ es una resolución proyectiva de M;

ii) a cada morfismo $f : M \longrightarrow M'$ de R-módulos le asigna el morfismo:

$$Ext_R^n(f,N) := H^n(f,N;\underline{P}',\underline{P}) : Ext_R^n(M',N) \longrightarrow Ext_R^n(M,N),$$

donde $\underline{P}$ y $\underline{P}'$ son resoluciones proyectivas de M y M' respectivamente.

Dada una sucesión exacta de R-módulos $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$, los morfismos concectores correspondientes se denotarán por:

$$Ext_R^n(M',M'',N) : Ext_R^n(M',N) \longrightarrow Ext_R^{n+1}(M'',N).$$

Definición 37 (**Functores Ext**). *Sea M un R-módulo y $n \in \mathbb{N}$. Se define el functor covariante $Ext_n^R(M,-)$ como sigue:*

i) A cada R-módulo N le asigna el R-módulo $Ext_n^R(M,N)$;

ii) a cada morfismo de R-módulos $f : N \longrightarrow N'$ le asigna el morfismo de R-módulos:

$$Ext_n^R(M,f) := H^n(Hom_R(\underline{P},f)) : Ext_n^R(M,N) \longrightarrow Ext_n^R(M,N'),$$

donde $\underline{P}$ es una resolución proyectiva de M.

Dada una sucesión exacta de R-módulos $0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$, los morfismos conectores correspondientes se denotarán por:

$$Ext_R^n(M,N'',N') : Ext_R^n(M,N'') \longrightarrow Ext_R^{n+1}(M,N').$$

Teorema 2.5.1. *i) Sean N un R-módulo y $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ es una sucesión exacta de R-módulos. Entonces, se tiene las sucesiones exactas:*

$$0 \longrightarrow Ext_R^0(M'',N) \longrightarrow \cdots \longrightarrow Ext_R^{n-1}(M'',N) \xrightarrow{Ext_R^{n-1}(g,N)} Ext_R^n(M,N) \xrightarrow{Ext_R^{n-1}(f,N)}$$
$$\xrightarrow{Ext_R^{n-1}(f,N)} Ext_R^{n-1}(M',N) \xrightarrow{\partial^{n-1}(M',M'';N)} Ext_R^n(M'',N) \longrightarrow \cdots ,$$

$$0 \longrightarrow Ext_R^0(N,M') \longrightarrow \cdots \longrightarrow Ext_R^{n-1}(N,M') \xrightarrow{Ext_R^{n-1}(N,f)} Ext_R^n(N,M) \xrightarrow{Ext_R^{n-1}(N,g)}$$
$$\xrightarrow{Ext_R^{n-1}(N,g)} Ext_R^{n-1}(N,M'') \xrightarrow{\partial^{n-1}(N;M'',M')} Ext_R^n(N,M') \longrightarrow \cdots$$

ii) Si el diagrama:

$$\begin{array}{lccccccccc}
\mathcal{M}: & 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\
& & & \downarrow{f'} & & \downarrow{f} & & \downarrow{f''} & & \\
\mathcal{K}: & 0 & \longrightarrow & K' & \longrightarrow & K & \longrightarrow & K'' & \longrightarrow & 0,
\end{array}$$

cuyas filas son sucesiones exactas de R-módulos, es conmutativo, entonces, los diagramas:

$$\begin{array}{ccc}
Ext_R^{n-1}(M',N) & \xrightarrow{\partial^{n-1}(M'',M';N)} & Ext_R^n(M'',N) \\
{\scriptstyle Ext_R^n(f',N)}\uparrow & & \uparrow{\scriptstyle Ext_R^n(f'',N)} \\
Ext_R^{n-1}(K',N) & \xrightarrow{\partial^{n-1}(K',K'';N)} & Ext_R^n(K'',N)
\end{array}
\qquad
\begin{array}{ccc}
Ext_R^{n-1}(N,M'') & \xrightarrow{\partial^{n-1}(N;M'',M')} & Ext_R^n(M',N) \\
\downarrow{\scriptstyle Ext_R^n(N,f'')} & & \downarrow{\scriptstyle Ext_R^n(N,f')} \\
Ext_R^{n-1}(N,K'') & \xrightarrow{\partial^{n-1}(N;K'',K')} & Ext_R^n(N,K')
\end{array}$$

son conmutativos para todo $n \in \mathbb{N}$, $n \geq 1$.

iii) El functor $Ext_R^n(M,N)$ es lineal en M y N para todo $n \in \mathbb{N}$.

iv) Existe un isomorfismo $Ext_R^0(M,N) \cong Hom_R(M,N)$ que es functorial en M y N.

v) Si P es un R-módulo proyectivo, entonces $Ext_R^n(P,N) = 0$ para todo R-módulo N y todo $n \in \mathbb{N}$ con $n \geq 1$.

2.6. Dimensión Homológica

Dado un R-módulo M y una resolución proyectiva:

$$\mathcal{P} : \cdots \longrightarrow P_n \xrightarrow{d_n} P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \xrightarrow{\epsilon} M \longrightarrow 0$$

de M, se dice que $\mathcal{P}$ es de longitud n si $P_n \neq 0$ y $P_i = 0$ para todo $i > n$.

Definición 38. *Se define la dimensión homológica de M, y se denota por $hd_R(M)$, al menor $n \in \mathbb{N}$ de forma que existe una resolución proyectiva de M de longitud n. Si no existe una resolución proyectiva de M de longitud finita, se define $hd_R(M) := +\infty$. Si $M = 0$ se toma $hd_R(M) = -1$.*

Observación 12. *Una consecuencia inmediata de la Definición 38 precedente es que M es un R-módulo proyectivo si y solamente si $hd_R(M) \leq 0$.*

Proposición 2.6.1. *Sea $(R,\mathfrak{m})$ un anillo local noetheriano y M un R-módulo finitamente generado. Entonces, las siguientes afirmaciones son equivalentes:*

i) M es libre;

ii) M es proyectivo;

iii) $Tor_j^R(M,N) = 0$ para todo R-módulo N y $j \in \mathbb{N}$, $j \geq 1$;

iv) $Tor_1^R(M,k) = 0$ para todo R-módulo, donde $k = R/\mathfrak{m}$ es el cuerpo de restos módulo $\mathfrak{m}$ del anillo local $(R,\mathfrak{m})$.

Demostración. $i) \Rightarrow ii)$ Inmediato; $ii) \Rightarrow iii)$ se sigue del Lema 2.4.4; $iii) \Rightarrow iv)$ es inmediato, pues $iv)$ es un caso particular de $iii)$; $iv) \Rightarrow i)$ Sea M un R-módulo finitamente generado, $\{x_1, \ldots, x_n\}$ un conjunto generador minimal de M y $\varphi : F \longrightarrow M$ el epimorfismo canónico donde F es un R-módulo libre con una base de n elementos. Si escribimos $Q = ker(\varphi)$, entonces se tiene la sucesión exacta:

$$0 \longrightarrow Q \xrightarrow{i} F \xrightarrow{\varphi} M \longrightarrow 0. \tag{2.6.1}$$

En virtud del apartado $i)$ del Teorema 2.4.3, se tiene la sucesión exacta:

$$Tor_R^1(M,k) \longrightarrow Tor_0^R(Q,k) \longrightarrow Tor_0^R(F,k) \longrightarrow Tor_0^R(M,k) \longrightarrow 0.$$

Por hipótesis, $Tor_R^1(M,k) = 0$. Además, los isomorfismos functoriales: $Tor_0^R(Q,k) \cong Q \otimes_R k \cong k \otimes_R Q \cong Q/\mathfrak{m}Q$ (respectivamente para F y M) implican que la sucesión:

$$0 \longrightarrow Q/\mathfrak{m}Q \xrightarrow{\bar{i}} F/\mathfrak{m}F \xrightarrow{\bar{\varphi}} M/\mathfrak{m}M \longrightarrow 0$$

es exacta. Por la Proposición 1.5.2, $\bar{\varphi}$ es isomorfismo de k-espacios vectoriales y $Q/\mathfrak{m}Q = 0$. Además, como $F = R^n$ y R es un anillo noetheriano, por el Corolario A.8.4, F es un R-módulo noetheriano. Como $Q = ker(\varphi) \subseteq F$ es un submódulo de F, Q es finitamente generado. Por el Lema de Nakayama (cf. Proposición A.8.12), $Q = 0$. Por tanto, φ es isomorfismo y M es un R-módulo libre. □

Proposición 2.6.2. *Dado un R-módulo M, las siguientes afirmaciones son equivalentes:*

i) M *es proyectivo;*
ii) $Ext_R^j(M,N) = 0$ *para todo R-módulo N y todo $j \in \mathbb{N}$, $j \geq 1$;*
iii) $Ext_R^1(M,N) = 0$ *para todo R-módulo N.*

Demostración. $i) \Rightarrow ii)$ Se sigue del apartado $v)$ del Teorema 2.5.1; $ii) \Rightarrow iii)$ Inmediato, pues $iii)$ es un caso particular de $ii)$; $iii) \Rightarrow i)$ Consideremos el diagrama:

$$\begin{array}{ccccc} & & M & & \\ & & \downarrow f & & \\ N & \xrightarrow{\varphi} & N'' & \longrightarrow & 0 \end{array} \tag{2.6.2}$$

cuya fila inferior es una sucesión exacta de R-módulos. Definamos $N' := ker(\varphi)$. Entonces, la sucesión $0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$ es exacta. Por el apartado $i)$ del Teorema 2.5.1, se tiene la sucesión exacta:

$$Ext_R^0(M,N) \xrightarrow{Ext_R^0(M,\varphi)} Ext_R^0(M,N'') \xrightarrow{\partial_n(M;N'',N')} Ext_R^1(M,N').$$

Ahora bien por hipótesis, $Ext_R^1(M,N') = 0$. En consecuencia, $Ext_R^0(M,\varphi)$ es epimorfismo. Además, por el apartado $iv)$ del Teorema 2.5.1, se tienen los isomorfismos functoriales $Hom_R(M,N) \cong Ext_R^0(M,N)$, $Hom_R^0(M,N'') \cong Ext_R^0(M,N'')$. En consecuencia, se tiene el diagrama conmutativo:

$$\begin{array}{ccc} Ext_R^0(M,N) & \xrightarrow{Ext_R^0(M,\varphi)} & Ext_R^0(M,N'') \\ \downarrow & & \downarrow \\ Hom_R(M,N) & \xrightarrow{Hom_R(M,\varphi)} & Hom_R(M,N'') \end{array}$$

Por tanto, se sigue que $Hom_R(M,\varphi)$ es epimorfismo de R-módulos y, por consiguiente existe $g : M \longrightarrow N$ tal que $\varphi \circ g = f$. En vista del Diagrama 2.6.2, esto significa que M es proyectivo. □

Proposición 2.6.3. *Dado un R-módulo M y $n \in \mathbb{N}$, las siguientes afirmaciones son equivalentes:*

i) $hd_R(M) \leq n$;
ii) $Ext_R^j(M,N) = 0$ *para todo R-módulo N y todo $j \in \mathbb{N}$, $j \geq n+1$;*
iii) $Ext_R^{n+1}(M,N) = 0$ *para todo R-módulo N;*
iv) si $0 \longrightarrow K_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \longrightarrow M \longrightarrow 0$ *es una sucesión exacta, donde P_j es un R-módulo proyectivo para todo j, $0 \leq j \leq n-1$, entonces K_n es un R-módulo proyectivo.*

DEMOSTRACIÓN. $i) \Rightarrow ii)$ Si $hd_R(M) \leq n$, existe una resolución proyectiva $\cdots \longrightarrow P_n \longrightarrow \cdots \longrightarrow P_0 \longrightarrow M \longrightarrow 0$ de M con $P_n = 0$ para todo $j \geq n+1$. Utilizando esta resolución proyectiva para calcular $Ext^j_R(M,N)$ se tiene $ii)$.
$ii) \Rightarrow iii)$ Inmediato, pues $iii)$ es un caso particular de $ii)$.
$iii) \Rightarrow iv)$ Si $n=0$, se tiene la sucesión exacta $0 \longrightarrow K_0 \longrightarrow M \longrightarrow 0$, lo que implica que $K_0 \cong M$. Además, por hipótesis, se tiene que $Ext^1_R(M,N) = 0$. En virtud de la Proposición 2.6.2 precedente, M es proyectivo y, por tanto, también lo es K_0. Supongamos $n \geq 1$. La sucesión exacta $0 \longrightarrow K_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \longrightarrow M \longrightarrow 0$ induce, para cada j, $0 \leq j \leq n-1$, la sucesión exacta:

$$0 \longrightarrow K_{j+1} \longrightarrow P_j \longrightarrow K_j \longrightarrow 0,$$

donde $K_j = Im(P_j \longrightarrow P_{j-1})$ para cada j, $1 \leq j \leq n-1$ y $K_0 = M$. Por el apartado $i)$ del Teorema 2.5.1, para cada j, $0 \leq j \leq n-1$, se tiene que la sucesión:

$$Ext^{n-j}_R(P_j,N) \longrightarrow Ext^{n-j}_R(K_{j+1},N) \longrightarrow Ext^{n-j+1}_R(K_j,N) \longrightarrow Ext^{n-j+1}_R(P_j,N)$$

es exacta. Pero como P_j es proyectivo y $n-j+1 > n-j \geq 1$, en virtud de la Proposición 2.6.2, se sigue que $Ext^{n-j+1}_R(P_j,N) = Ext^{n-j}_R(P_j,N) = 0$. En consecuencia, se tiene que

$$Ext^{n+1}_R(K_0,N) \cong Ext^n_R(K_1,N) \cong \cdots \cong Ext^1_R(K_n,N).$$

Ahora bien, por hipótesis se tiene que $Ext^{n+1}_R(K_0,N) = 0$, luego $Ext^1_R(K_n,N) = 0$. En virtud de la Proposición 2.6.2, K_n es un R-módulo proyectivo.
$iv) \Rightarrow i)$ Si $n=0$, por hipótesis se tiene que $P_0 \cong M$ con P_0 proyectivo. En consecuencia, M es proyectivo y, por consiguiente $hd_R(M) = 0$. Supongamos $n \geq 1$. En virtud de la demostración de la Proposición 2.3.1, existe una sucesión exacta $0 \longrightarrow K_0 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$ siendo P_0 un R-módulo proyectivo. Por hipótesis, K_0 es proyectivo. Por tanto, se sigue que dicha sucesión exacta es una resolución proyectiva de M y, en consecuencia, $hd_R(M) \leq 1 \leq n$. □

COROLARIO 2.6.4. *Si M es un R-módulo distinto de cero, entonces*

$$hd_R(M) = sup\ \{n \in \mathbb{N} : \exists N \in R - \mathcal{M}od\ |Ext^n_R(M,N) \neq 0\}.$$

DEMOSTRACIÓN. Si la parte de la derecha de la igualdad no es finita, entonces $Ext^j_R(M,N) = H^j(Hom_R(\underline{P},N)) \neq 0$ para todo R-módulo N, $j \in \mathbb{N}$ y resolución proyectiva $(\underline{P},\epsilon)$ de M. En consecuencia, $P_n \neq 0$ para todo $n \in \mathbb{N}$ y por tanto $hd_R(M) = +\infty$. Sea $l = sup\ \{n \in \mathbb{N} : \exists N \in R - \mathcal{M}od\ |Ext^n_R(M,N) = 0\}$, por la Proposición 2.6.3 precedente, $hd_R(M) \leq l$. De otro lado, si $(\underline{P},\epsilon)$ es una resolución proyectiva de M, $P_j = 0$ para todo $j \geq hd_R(M)+1$. En consecuencia, $0 = H^j(Hom_R(\underline{P},N)) = Ext^j_R(M,N)$ para todo $j \geq hd_R(M)+1$. Por tanto, $l \leq hd_R(M)$. □

COROLARIO 2.6.5. *Sea M un R-módulo, entonces si M' es un sumando directo de M, se tiene que $hd_R(M') \leq hd_R(M)$.*

DEMOSTRACIÓN. Es inmediato en vista del Corolario 2.6.4 teniendo en cuenta que, por $iii)$ del Teorema 2.5.1, $Ext^n_R(M',N)$ es un sumando directo de $Ext^n_R(M,N)$ para cada $n \in \mathbb{N}$. □

PROPOSICIÓN 2.6.6. *Sea $0 \longrightarrow M' \longrightarrow P \longrightarrow M'' \longrightarrow 0$ una sucesión exacta de R-módulos donde P es proyectivo. Entonces,*

i) si M'' es proyectivo, entonces también lo es M';
ii) si $hd_R(M'') \geq 1$, $hd_R(M'') = hd_R(M')+1$, donde se admite que ambas partes de la igualdad sean no finitas.

DEMOSTRACIÓN. $i)$ Es una consecuencia inmediata de la Proposición A.4.2.
$ii)$ En virtud del apartado $i)$ del Teorema 2.5.1, se tiene, para cada R-módulo N y $n \in \mathbb{N}$ con $n \geq 1$, la sucesión exacta:

$$Ext^n_R(P,N) \longrightarrow Ext^n_R(M',N) \longrightarrow Ext^{n+1}(M'',N) \longrightarrow Ext^{n+1}_R(P,N).$$

Ahora bien, como P es proyectivo y $n \geq 1$, por la Proposición 2.6.2, $Ext^n_R(P,N) = Ext^{n+1}_R(P,N) = 0$. Entonces, $Ext^n_R(M',N) \cong Ext^{n+1}_R(M'',N)$ y la afirmación $ii)$ se sigue del Corolario 2.6.4. □

PROPOSICIÓN 2.6.7. *Sea $(R,\mathfrak{m})$ un anillo local noetheriano, M un R-módulo finitamente generado, $n \in \mathbb{N}$ y $k = R/\mathfrak{m}$ es el cuerpo de restos módulo $\mathfrak{m}$ del anillo local $(R,\mathfrak{m})$. Entonces, las siguientes afirmaciones son equivalentes:*

i) $hd_R(M) \leq n$;
ii) $Tor_j^R(M,N) = 0$ *para todo R-módulo M y todo $j \in \mathbb{N}$, $j \geq n+1$;*
iii) $Tor_{n+1}^R(M,k) = 0$.

DEMOSTRACIÓN. $i) \Rightarrow ii)$. Por $i)$ existe una resolución proyectiva de M de longitud menor o igual que n. Utilizando dicha resolución para calcular Tor se sigue $ii)$. $ii) \Rightarrow iii)$ trivial, pues $iii)$ es un caso particular de $ii)$. $iii) \Rightarrow i)$ Probémoslo por inducción en n. Si $n = 0$, entonces por hipótesis, $Tor_1^R(M,k) = 0$ y, por la Proposición 2.6.1, M es proyectivo. Por la Observación 12, $hd_R(M) \leq 0$. Supongamos $n \geq 1$. Siguiendo el mismo razonamiento que en la Proposición 2.6.1, podemos considerar una sucesión exacta de R-módulos: $0 \longrightarrow M' \longrightarrow P \longrightarrow M \longrightarrow 0$, donde P es proyectivo. Por el Teorema 2.4.3, se tiene la sucesión exacta:

$$Tor_{n+1}^R(M,k) \longrightarrow Tor_n^R(M',k) \longrightarrow Tor_n^R(P,k).$$

Ahora bien, por hipótesis, $Tor_{n+1}^R(M,k) = 0$. Además, como $n \geq 1$ y P es proyectivo, por la Proposición 2.6.1, $Tor_n^R(P,k) = 0$. Por tanto, $Tor_n^R(M',k) = 0$. Por hipótesis inductiva, $hd_R(M',k) \leq n-1$. En virtud del apartado $ii)$ de la Proposición 2.6.6, $hd_R(M) \leq n$. □

PROPOSICIÓN 2.6.8. *Sea M un R-módulo con $hd_R(M) < +\infty$. Si $a \in R$ no es un divisor de 0 de M ni de R, entonces $hd_{R/(a)}(M/aM) < +\infty$.*

DEMOSTRACIÓN. Probémoslo por inducción en $hd_R(M)$. Supongamos $M \neq 0$, si $hd_R(M) = 0$ entonces, por la Observación 12, M es proyectivo. Por el Corolario A.4.5, $R/(a) \otimes_R M$ es un $R/(a)$-módulo proyectivo. Pero por la Proposición A.6.6, $R/(a) \otimes_R M \cong M/aM$, luego M/aM es un $R/(a)$-módulo proyectivo. De nuevo, por la Observación 12, esto implica $hd_{R/(a)}(M/aM) = 0$. Supongamos $hd_R(M) > 0$. En vista de la demostración de la Proposición 2.3.1, podemos considerar una sucesión exacta de R-módulos: $0 \longrightarrow N \longrightarrow P \longrightarrow M \longrightarrow 0$ donde P es proyectivo. En virtud de la Proposición 2.6.6, $hd_R(N) = hd_R(M) - 1$. Además, por el apartado $i)$ del Teorema 2.4.3 se tiene que la sucesión de R-módulos:

$$Tor_1^R(M,R/(a)) \longrightarrow Tor_0^R(N,R/(a)) \longrightarrow Tor_0^R(P,R/(a)) \longrightarrow Tor_0^R(M,R/(a)) \longrightarrow 0 \tag{2.6.3}$$

es exacta. Ahora bien, como a no es un divisor de 0 de R, la homotecia $a_R : R \longrightarrow R$ por a es monomorfismo. Por tanto, se tiene que la sucesión de R-módulos: $0 \longrightarrow R \xrightarrow{a_R} R \longrightarrow R/(a) \longrightarrow 0$ es exacta. De nuevo, por el Teorema 2.4.3, se tiene la sucesión exacta de R-módulos:

$$Tor_1^R(R/(a),M) \longrightarrow Tor_n^R(R,M) \xrightarrow{Tor_n^R(a_R,M)} Tor_n^R(R,M). \tag{2.6.4}$$

Ahora bien, la afirmación $iv)$ del Teorema 2.4.3 y la Proposición A.6.2 garantizan la existencia de isomorfismos functoriales: $Tor_0^R(R,M) \cong R \otimes_R M \cong M$. En consecuencia, se tiene el diagrama conmutativo:

$$\begin{array}{ccccc}
Tor_0^R(R,M) & \longrightarrow & R \otimes_R M & \longrightarrow & M \\
\downarrow{\scriptstyle Tor_0^R(a_R,M)} & & \downarrow{\scriptstyle a_R \otimes Id_M} & & \downarrow{\scriptstyle a_M} \\
Tor_0^R(R,M) & \longrightarrow & R \otimes_R M & \longrightarrow & M
\end{array}$$

Como a no es divisor de 0 de M, la homotecia $a_M : M \longrightarrow M$ por a en M es monomofismo de R-módulos y, en consecuencia, también lo será $Tor_0^R(a_R,M)$. Por exactitud de la Sucesión (2.6.4), debe ser $Tor_1^R(R/(a),M) = 0$. De nuevo, por la Proposición A.6.2 y el Teorema 2.4.3, $Tor_0^R(R/(a),M) \cong M/aM$ (respectivamente para N y P). Por consiguiente, la Sucesión exacta (2.6.3) es de la forma:

$$0 \longrightarrow N/aN \longrightarrow P/aP \longrightarrow M/aM \longrightarrow 0.$$

Ahora bien, como P es un R-módulo proyectivo, por el Corolario A.4.5, P/aP es un $R/(a)$-módulo proyectivo. Luego por la Proposición 2.6.6, $hd_{R/(a)}(N/aN) = hd_{R/(a)}(M/aM) - 1$. Pero como $hd_R(N) < hd_R(M)$, aplicando hipótesis inductiva se tiene que $hd_{R/(a)}(N/aN) < +\infty$ y, por tanto,

$$hd_{R/(a)}(M/aM) = hd_{R/(a)}(N/aN) + 1 < +\infty.$$

□

2.7. Dimensión Inyectiva y Dimensión Global

Proposición 2.7.1. *Sea R un anillo noetheriano y N un R-módulo. Las siguientes afirmaciones son equivalentes:*

i) *N es inyectivo;*
ii) *$Ext^1_R(M,N)=0$ para todo R-módulo M;*
iii) *$Ext^j_R(M,N)=0$ para todo R-módulo M y todo $j\in\mathbb{N}$, $j\geq 1$;*
iv) *$Ext^1_R(M,N)=0$ para todo R-módulo M finitamente generado;*
v) *$Ext^1_R(\mathfrak{a},N)=0$ para todo ideal $\mathfrak{a}$ de R.*

Demostración. Véase una prueba en la Sección B.2 del Apéndice B. □

Definición 39. *Sea N un R-módulo se define la dimensión inyectiva de N, denotada $inj.dim_R(N)$, de la siguiente manera:*

$$inj.dim_R(N)=sup\,\{n\in\mathbb{N}:\ \exists M\in R-\mathcal{M}od\,|\,Ext^n_R(M,N)\neq 0\}$$

si existe. En caso contrario, se escribe $inj.dim_R(N)=+\infty$. Si $N=0$, entonces se escribe $inj.dim_R(N)=-1$.

Proposición 2.7.2. *Para todo R-módulo N se verifica la siguiente propiedad:*

$$inj.dim_R(N)=sup\,\{n\in\mathbb{N}:\ \exists M\in R-\mathcal{M}od,\ M\,f.g.\ |\ Ext^n_R(M,N)\neq 0\}.$$

Demostración. En vista de la Definición 39, bastará probar la siguiente afirmación: *Sea N un R-módulo e $i\in\mathbb{N}$. Entonces, si $Ext^i_R(M,N)=0$ para todo R-módulo M finitamente generado, $Ext^i_R(M,N)=0$ para todo R-módulo M.* Probémoslo por inducción en i. Si $i=0$, se tiene que $N\cong Hom_R(R,N)\cong Ext^0_R(R,N)=0$ porque R es finitamente generado como R-módulo. Luego $Ext^0_R(M,N)=0$ para todo R-módulo M. Para $i=1$ el resultado se sigue de la equivalencia *ii)* $\Leftrightarrow$ *iv)* de la Proposición 2.7.1 precedente. Supongamos $i\geq 2$. Por la Proposición A.5.2, N es isomorfo a un submódulo de un R-módulo inyectivo Q. Por tanto, existe una sucesión exacta de R-módulos: $0\longrightarrow N\longrightarrow Q\longrightarrow Q/N\longrightarrow 0$, donde Q es inyectivo. Por el Teorema 2.5.1, se tiene la sucesión exacta:

$$Ext^{i-1}_R(M,Q)\longrightarrow Ext^{i-1}_R(M,Q/N)\longrightarrow Ext^i_R(M,N)\longrightarrow Ext^i_R(M,Q). \tag{2.7.1}$$

Ahora bien, como Q es inyectivo e $i\geq 2$, en vista de la Proposición 2.7.1, $Ext^{i-1}_R(M,Q)=Ext^i_R(M,Q)=0$. Además, como, por hipótesis, se tiene que $Ext^i_R(M,N)=0$ para todo R-módulo M finitamente generado y por exactitud de la Sucesión (2.7.1), $Ext^{i-1}_R(M,Q/N)\cong Ext^i_R(M,N)$, se sigue que $Ext^{i-1}_R(M,Q/N)=0$ para todo R-módulo M finitamente generado. Por hipótesis inductiva, $Ext^{i-1}_R(M,Q/N)=0$ para todo R-módulo M. En virtud del isomorfismo $Ext^{i-1}_R(M,Q/N)\cong Ext^i_R(M,N)$, $Ext^i_R(M,N)=0$ para todo R-módulo M. □

Definición 40. *Se define la dimensión global de un anillo R como sigue:*

$$gl.dim(R)=\ sup\{hd_R(M):\ M\in R-\mathcal{M}od\}.$$

Proposición 2.7.3. *Para cada anillo R,*

$$gl.dim(R)=sup\,\{inj.dim_R(N):\ N\in R-\mathcal{M}od\}.$$

Demostración. Por el Corolario 2.6.4,

$$\begin{aligned}gl.dim(R)&=sup_M\{hd_R(M)\}\\&=sup_M\{\,sup\{n\in\mathbb{N}:\exists N\in R-\mathcal{M}od\,|\,Ext^n_R(M,N)\neq 0\}\}\\&=sup\,\{n\in\mathbb{N}:\exists M,N\in R-\mathcal{M}od\,|\,Ext^n_R(M,N)\neq 0\}\\&=sup_N\{\,sup\,\{n\in\mathbb{N}:\exists M\in R-\mathcal{M}od\,|\,Ext^n_R(M,N)\neq 0\}\}=sup_N(inj.dim_R(N)).\end{aligned}$$

□

Proposición 2.7.4. *Para cada anillo R,*

$$gl.dim(R)=sup\,\{hd_R(M):\ M\in R-\mathcal{M}od,\ M\,f.g.\}.$$

DEMOSTRACIÓN.

$$\begin{aligned} gl.dim(R) &= sup_N\{inj.dim_R(N)\} \\ &= sup_N\{\, sup\,\{n \in \mathbb{N} : \exists M \in R-\mathcal{M}od,\ M\, f.g. \,|\, Ext^n_R(M,N) \neq 0\}\} \\ &= sup_{M f.g.}\{\, sup\{n \in \mathbb{N} : \exists N \in R-\mathcal{M}od \,|\, Ext^n_R(M,N) \neq 0\}\} \\ &= sup_{M f.g.}\{hd_R(M)\}, \end{aligned}$$

donde la primera igualdad se sigue de la Proposición 2.7.3 precedente; la segunda igualdad, de la Proposición 2.7.2; y la última, del Corolario 2.6.4. □

PROPOSICIÓN 2.7.5. *Sea* $(R, \mathfrak{m})$ *un anillo local noetheriano y* $k = R/\mathfrak{m}$ *su cuerpo de restos módulo* $\mathfrak{m}$*. Entonces, para cada* $n \in \mathbb{N}$*, las siguientes afirmaciones son equivalentes:*

i) $gl.dim(R) \leq n$;
ii) $Tor^R_j(M,N) = 0$ *para cada par de* R*-módulos* M, N *y para todo* $j \in \mathbb{N}$, $j \geq n+1$;
iii) $Tor^R_{n+1}(k,k) = 0$.

DEMOSTRACIÓN. *i)* ⇒ *ii)* $gl.dim(R) \leq n$ implica que $hd_R(M) \leq n$ para todo R-módulo M. Por tanto, *ii)* se sigue de la implicación *i)* ⇒ *ii)* de la Proposición 2.6.7. *ii)* ⇒ *iii)* Inmediato, pues *iii)* es un caso particular de *ii)*. *iii)* ⇒ *i)* Como R es un anillo noetheriano, $k = R/\mathfrak{m}$ es un anillo noetheriano y k es finitamente generado como R-módulo (cf. Corolario A.8.3). Por la Proposición 2.6.7, $Tor^R_{n+1}(k,k) = 0$ implica $Tor^R_j(k,M) = 0$ para todo R-módulo M y todo $j \in \mathbb{N}$ con $j \geq n+1$. Pero por la Proposición 2.4.5, $Tor^R_j(k,M) \cong Tor^R_j(M,k)$ para cada $j \in \mathbb{N}$. Por tanto, $Tor^R_{n+1}(M,k) = 0$. De nuevo, por la Proposición 2.6.7, se tiene que, si M es finitamente generado, $hd_R(M) \leq n$. Por tanto, $sup_{M f.g.}\{hd_R(M)\} \leq n$. En virtud de la Proposición 2.7.4, $gl.dim(R) \leq n$. □

COROLARIO 2.7.6. *Si* $(R, \mathfrak{m})$ *es un anillo local noetheriano y* $k = R/\mathfrak{m}$ *es su cuerpo de restos módulo* $\mathfrak{m}$*, se tiene que* $gl.dim(R) = hd_R(k)$.

DEMOSTRACIÓN. De un lado, es claro que $hd_R(k) \leq sup_M\{hd_R(M)\} = gl.dim(R)$. En consecuncia, si $hd_R(k) = +\infty$, debe ser $gl.dim(R) = +\infty$. Si $hd_R(k) < +\infty$, sea $l = hd_R(k)$. Como ya se había visto anteriormente, k es un R-módulo finitamente generado, luego tomando $n = l$ y $M = k$ en la Proposición 2.6.7, se sigue que $Tor^R_l(k,k) = 0$. Ahora, por la Proposición 2.7.5, esto significa que $gl.dim(R) \leq l = hd_R(k)$. □

2.8. Resolución de la Ex-conjetura de Serre sobre Anillos Locales Regulares

En esta sección $R = (R, \mathfrak{m})$ será un anillo local noetheriano de maximal $\mathfrak{m}$ y se denotará por $k = R/\mathfrak{m}$ a su cuerpo de restos módulo $\mathfrak{m}$.

LEMA 2.8.1. *Si* $(R, \mathfrak{m})$ *es un anillo local noetheriano y* $a \in \mathfrak{m} \setminus \mathfrak{m}^2$*, entonces la sucesión exacta:*

$$0 \longrightarrow aR/a\mathfrak{m} \xrightarrow{\phi} \mathfrak{m}/a\mathfrak{m} \xrightarrow{\varphi} \mathfrak{m}/aR \longrightarrow 0, \tag{2.8.1}$$

donde ϕ *y* φ *son la inclusión y proyección canónica respectivamente, se escinde.*

DEMOSTRACIÓN. Sea d la dimensión del $k-$espacio vectorial $\mathfrak{m}/\mathfrak{m}^2$. Como $a \notin \mathfrak{m}^2$, por la Proposición 1.5.2, existen $a_1 \ldots, a_{d-1}$ tales que $\{a, a_1, \ldots, a_{d-1}\}$ es un conjunto generador minimal de $\mathfrak{m}$. Sea $\mathfrak{a}$ el ideal de R generado por $\{a_1, \ldots, a_{d-1}\}$ y sea $b \in R$ verificando $ba \in \mathfrak{a}$. Entonces, $ab = \sum_{i=0}^{d-1} r_i a_i$ con $r_i \in R$ para todo i. Si b fuese unidad, se tendría que $a = \sum_{i=0}^{d-1} b^{-1} r_i a_i$ y, en consecuencia, $a \in \mathfrak{a} =< \{a_1, \ldots, a_{d-1}\} >$, contradiciendo la minimalidad de $\{a, a_1, \ldots, a_{d-1}\}$ como conjunto generador de $\mathfrak{m}$. Se sigue que b no es una unidad de R y, por ende, $b \in \mathfrak{m}$. En consecuencia, $\mathfrak{a} \cap aR \subseteq \mathfrak{a} \cap a\mathfrak{m}$. Como, en general, se cumple que $\mathfrak{a} \cap a\mathfrak{m} \subseteq \mathfrak{a} \cap aR$, se sigue que $\mathfrak{a} \cap a\mathfrak{m} = \mathfrak{a} \cap aR$. Ahora bien, por el Segundo Teorema de Isomorfía se tiene que:

$$(\mathfrak{a} + a\mathfrak{m})/a\mathfrak{m} \cong \mathfrak{a}/\mathfrak{a} \cap a\mathfrak{m} = \mathfrak{a}/\mathfrak{a} \cap aR \cong (\mathfrak{a} + aR)/aR = \mathfrak{m}/aR.$$

En consecuencia, $\varphi|_{\mathfrak{a}+a\mathfrak{m}} : (\mathfrak{a} + a\mathfrak{m})/a\mathfrak{m} \longrightarrow \mathfrak{m}/aR$ es isomorfismo y la Sucesión (2.8.1) se escinde. □

COROLARIO 2.8.2. *Sea* $(R, \mathfrak{m})$ *un anillo local noetheriano con* $gl.dim(R) < +\infty$*. Si* $a \in \mathfrak{m} \setminus \mathfrak{m}^2$ *no es divisor de cero de* R*, entonces* $gl.dim(R/aR) < +\infty$.

Demostración. Por el Tercer Teorema de Isomorfía, se tiene que ${}^{R/aR}/_{\mathfrak{m}/aR} \cong R/\mathfrak{m} = k$. Por tanto, se tiene la sucesión exacta: $0 \longrightarrow \mathfrak{m}/aR \longrightarrow R/aR \longrightarrow k \longrightarrow 0$. Por el Corolario 2.7.6, $gl.dim(R/aR) = hd_{R/aR}(k/aR)$, pero como $a \in \mathfrak{m}$, $k/aR = k$. En consecuencia, $gl.dim(R/aR) = hd_{R/aR}(k)$. En vista de la afirmación *ii*) de la Proposición 2.6.6, $hd_{R/aR}(k) < +\infty$ si y solamente si $hd_{R/aR}(\mathfrak{m}/aR) < +\infty$. Ahora bien, como $hd_R(\mathfrak{m}) \leq gl.dim(R) < +\infty$, por la Proposición 2.6.8, $hd_{R/aR}(\mathfrak{m}/a\mathfrak{m}) < +\infty$. Además, virtud del Lema 2.8.1 precedente, $\mathfrak{m}/a\mathfrak{m} \cong \mathfrak{m}/aR \oplus aR/a\mathfrak{m}$. Es decir, $\mathfrak{m}/aR$ es un sumando directo de $\mathfrak{m}/a\mathfrak{m}$. Luego por el Corolario 2.6.5, $hd_{R/aR}(\mathfrak{m}/aR) \leq hd_{R/aR}(\mathfrak{m}/a\mathfrak{m}) < +\infty$. □

Lema 2.8.3. *Sea M un $(R, \mathfrak{m})$ un anillo local noetheriano y $a \in \mathfrak{m}$ un elemento de R que no es divisor de cero de M. Entonces, $hd_R(M/aM) = hd_R(M) + 1$, donde ambos lados de la igualdad pueden ser no finitos.*

Demostración. Como a no es divisor de cero de M, la homotecia $a_M : M \longrightarrow M$ por a es monomorfismo de R-módulos y se tiene la sucesión exacta:

$$0 \longrightarrow M \xrightarrow{a_M} M \xrightarrow{\pi} M/aM \longrightarrow 0,$$

donde π es la proyección natural. Por el Teorema 2.4.3, se tiene, para cada $n \in \mathbb{N}$, la sucesión exacta de R-módulos:

$$Tor_{n+1}^R(M, k) \longrightarrow Tor_{n+1}^R(M/aM, k) \longrightarrow Tor_n^R(M, k) \xrightarrow{Tor_n^R(a_M, k)} Tor_n^R(M, k).$$

Ahora bien, por la linealidad de Tor (ver *iii*) en el Teorema 2.4.3),

$$Tor_n^R(a_M, k) = aTor_n^R(Id_M, k) = a(Tor_n^R(Id_M, k) \circ Tor_n^R(M, Id_k)) = Tor_n^R(Id_M, k) \circ Tor_n^R(M, a_k),$$

donde $a_k : k \longrightarrow k$ es la homotecia por a en k. Notemos que, como $k = R/\mathfrak{m}$ y $a \in \mathfrak{m}$, a_k es el morfismo nulo. Por tanto, $Tor_n^R(M, a_k) = 0$ y, por ende, $Tor_n^R(a_M, k) = 0$. En consecuencia, para cada $n \in \mathbb{N}$, se tiene la sucesión exacta:

$$Tor_{n+1}^R(M, k) \longrightarrow Tor_{n+1}^R(M/aM, k) \longrightarrow Tor_n^R(M, k) \longrightarrow 0. \tag{2.8.2}$$

Por un lado, si $hd_R(M) = +\infty$, en virtud de la Proposición 2.6.7, $Tor_j^R(M, k) \neq 0$ para todo $j \in \mathbb{N}$. Por exactitud de la Sucesión (2.8.2), $Tor_n^R(M/aM, k) \neq 0$ para todo $j \in \mathbb{N}$ y se sigue que $hd_R(M) = hd_R(M/aM) = +\infty$. De otro lado, sea $n = hd_R(M)$, entonces, por la Proposición 2.6.7, $Tor_n^R(M, k) \neq 0$ y $Tor_j^R(M, k) = 0$ para todo $j \geq n + 1$. Por exactitud de la Sucesión (2.8.2), $Tor_{n+1}^R(M/aM, k) \cong Tor_n^R(M, k) \neq 0$ y $Tor_j^R(M/aM, k) = 0$ para todo $j \geq n + 2$. De nuevo, por la Proposición 2.6.7,$Tor_{n+1}^R(M/aM, k) \neq 0$ implica que $hd_R(M/aM) > n$ y $Tor_{n+2}^R(M/aM, k) = 0$ implica que $hd_R(M/aM) \leq n + 1$. Por tanto, debe ser $hd_R(M/aM) = n + 1 = hd_R(M) + 1$. □

Lema 2.8.4. *Sea $(R, \mathfrak{m})$ un anillo local noetheriano tal que $\mathfrak{m} \neq \mathfrak{m}^2$ y tal que todo elemento de $\mathfrak{m} \setminus \mathfrak{m}^2$ es divisor de cero de R. Entonces, todo R-módulo M de dimensión homológica finita es un R-módulo libre.*

Demostración. Como R es un anillo noetheriano, por el Teorema A.10.3 y la Proposición A.10.5, el conjunto de ideales primos asociados a M (ver Definición 62) $Ass_R(M) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ es un conjunto finito, y se verifica:

$$\mathfrak{m} \setminus \mathfrak{m}^2 \subseteq \bigcup_{i=1}^{s} \mathfrak{p}_i.$$

Por consiguiente, $\mathfrak{m} \subseteq \mathfrak{p}_1 \cup \mathfrak{p}_2 \cup \cdots \cup \mathfrak{p}_s \cup \mathfrak{m}^2$. Como $\mathfrak{m} \neq \mathfrak{m}^2$, aplicando el Lema A.2.2 de manera recursiva, se concluye que $\mathfrak{m} \subseteq \mathfrak{p}_i$ para algún i, $1 \leq i \leq s$. Pero como $(R, \mathfrak{m})$ es un anillo local, debe ser $\mathfrak{m} = \mathfrak{p}_i$. Por tanto, $\mathfrak{m} \in Ass_R(M)$. En vista de la Observación 17, existe un monomorfismo de R-módulos: $k = R/\mathfrak{m} \hookrightarrow R$. Sea ahora M un R-módulo con $hd_R(M) = n < +\infty$. Si $n = -1$, $M = 0$ y no hay nada que probar. Supongamos $n \geq 0$. Entonces, como $k \hookrightarrow R$ es monomorfismo, se tiene una sucesión exacta de R-módulos $0 \longrightarrow k \longrightarrow R \longrightarrow R/k$. Por el Teorema 2.4.3, se sigue que la sucesión de R-módulos:

$$Tor_{n+1}^R(M, R/k) \longrightarrow Tor_n^R(M, k) \longrightarrow Tor_n^R(M, R). \tag{2.8.3}$$

es exacta. Además, en virtud de la Proposición 2.6.7, debe ser $Tor_n^R(M, k) \neq 0$ y $Tor_{n+1}^R(M, R/k) = 0$. Por exactitud de la Sucesión (2.8.3), $Tor_n^R(M, R) \neq 0$. Como R es un R-módulo libre, por el

Lema 2.4.4, $Tor_n^R(R, M) = 0$ para todo $n \geq 1$. Luego debe ser $hd_R(M) = n = 0$. En vista de la Observación 12, M es un R-módulo proyectivo. Por la Proposición 2.6.1, M es un R-módulo libre. □

Teorema 2.8.5 (**Serre-Auslander-Buchsbaum**). *Sea $(R, \mathfrak{m})$ un anillo local noetheriano. Entonces, R es local regular si y solamente si tiene dimensión global finita, en cuyo caso $gl.dim(R) = dim_{Kr}(R)$.*

Demostración. Supongamos que R es regular. Entonces, por la Proposición 1.5.7, $\mathfrak{m}$ está generado por una sucesión regular $a_1, \ldots, a_r$ en R. Como a_1 no es divisor de 0 de R, por el Lema 2.8.3:

$$hd_R(R/a_1R) = hd_R(R) + 1 = 1,$$

pues $hd_R(R) = 0$ por ser R un R-módulo libre. Ahora, $(R/aR, \mathfrak{m}/aR)$ es un anillo local noetheriano y, como $a_1, \ldots, a_r$ es una sucesión regular, a_2 no es divisor de 0 de R/a_1R. De nuevo, por el Lema 2.8.3:

$$hd_R(R/(a_1, a_2)R) = hd_R(R/a_1R) + 1 = 2.$$

Aplicando repetidamente el Lema 2.8.3, se concluye que:

$$hd_R(k) = hd_R(R/\mathfrak{m}) = hd_R(R/(a_1, \ldots, a_r)R) = hd_R(R/(a_1, \ldots, a_{r-1})R) + 1 = r - 1 + 1 = r.$$

Pero por el Corolario 2.7.6, $r = hd_R(k) = gl.dim(R) < +\infty$. Más aún, como $(R, \mathfrak{m})$ es un anillo local noetheriano, por el Corolario 1.4.14, $dim_{Kr}(R) = ht(\mathfrak{m})$ y, como $\mathfrak{m} = (a_1, \ldots, a_r)$, en particular $\mathfrak{m}$ es minimal sobre $(a_1, \ldots, a_r)$. Por el Teorema del Ideal Principal de Krull (ver Teorema 1.4.16), $ht(\mathfrak{m}) = r$. Por tanto, se tiene que:

$$gl.dim(R) = r = ht(\mathfrak{m}) = dim_{Kr}(R).$$

Supongamos ahora que $gl.dim(R) < +\infty$. En virtud de la Proposición 1.5.7, para ver que R es regular bastará con probar que $\mathfrak{m}$ está generado por una sucesión regular en R. Probémoslo por inducción en la dimensión del k-espacio vectorial $\mathfrak{m}/\mathfrak{m}^2$. Si $r = dim_k(\mathfrak{m}/\mathfrak{m}^2) = 0$, entonces $\mathfrak{m} = \mathfrak{m}^2$. Además, como R es un anillo noetheriano, $\mathfrak{m}$ es finitamente generado. Por el Lema de Nakayama (ver Proposición A.8.12), $\mathfrak{m} = 0$ y $\mathfrak{m}$ está generado por la sucesión regular nula. Supongamos $r > 0$. Como $hd_R(k) \leq gl.dim(R) < +\infty$, si cada elemento de $\mathfrak{m} \setminus \mathfrak{m}^2$ es un divisor de cero de R, por el Lema 2.8.4, se tiene que $k = R/\mathfrak{m}$ es un R-módulo libre. Por tanto, debe ser $\mathfrak{m} = 0$, lo que contradice la hipótesis $r > 0$. En consecuencia, debe existir un elemento $a \in \mathfrak{m} \setminus \mathfrak{m}^2$ que no es divisor de cero de R. Definiendo $\bar{R} := R/aR$, $\bar{\mathfrak{m}} := \mathfrak{m}/aR$, se sigue que $(\bar{R}, \bar{\mathfrak{m}})$ es un anillo local noetheriano cuyo cuerpo de restos módulo $\bar{\mathfrak{m}}$ es $\bar{R}/\bar{\mathfrak{m}} = (R/aR)/(\mathfrak{m}/aR) \cong k$. Sin pérdida de generalidad, podemos suponer que la clase de a módulo $\mathfrak{m}^2$ forma parte de una base para el k-espacio vectorial $\mathfrak{m}/\mathfrak{m}^2$. En virtud la Proposición 1.5.2, que $\mathfrak{m}$ admite un conjunto generador minimal que contiene a a de cardinal r. Por tanto, $\bar{\mathfrak{m}}$ admite un conjunto generador minimal de cardinal $r - 1$ y, aplicando la Proposición 1.5.2 de nuevo, se tiene que la dimensión del k-espacio vectorial $\bar{\mathfrak{m}}/\bar{\mathfrak{m}}^2$ es $r - 1$. Además, como a no es divisor de cero de R, por el Corolario 2.8.2, $gl.dim(\bar{R}) < +\infty$. Por hipótesis inductiva, $\bar{\mathfrak{m}}$ está generado por una sucesión regular $\bar{a}_1, \ldots, \bar{a}_{r-1}$ en $\bar{R}$, donde para cada i, $1 \leq i \leq r - 1$, $\bar{a}_i$ es a clase de $a_i \in \mathfrak{m}$ módulo aR. Como a no es divisor de cero de R, se tiene que $a, a_1, \ldots, a_{r-1}$ es una sucesión regular en R que genera $\mathfrak{m}$. □

Teorema 2.8.6 (**Serre**). *Sea R un anillo local regular y sea $\mathfrak{p} \in Spec(R)$ un ideal primo de R. Entonces, $R_\mathfrak{p}$ es un anillo local regular.*

Demostración. En virtud del Teorema 2.8.5, $gl.dim(R) < +\infty$. Por tanto, para probar este resultado, bastará comprobar que se cumple $gl.dim(R_\mathfrak{p}) \leq gl.dim(R)$ para cada $\mathfrak{p} \in Spec(R)$. Sea $\mathfrak{p} \in Spec(R)$. Como $hd_R(R/\mathfrak{p}) \leq gl.dim(R) < +\infty$, podemos tomar una resolución libre

$$0 \longrightarrow F_n \longrightarrow F_{n-1} \longrightarrow \cdots \longrightarrow F_0 \longrightarrow R/\mathfrak{p} \longrightarrow 0$$

de $R/\mathfrak{p}$, donde $n \leq gl.dim(R)$. Como, por la Proposición A.2.7, el functor $(-)_\mathfrak{p}$ es exacto, se tiene la sucesión exacta:

$$0 \longrightarrow (F_n)_\mathfrak{p} \longrightarrow (F_{n-1})_\mathfrak{p} \longrightarrow \cdots \longrightarrow (F_0)_\mathfrak{p} \longrightarrow (R/\mathfrak{p})_\mathfrak{p} \longrightarrow 0.$$

Ahora bien, para cada i, $0 \leq i \leq n$, se sigue que, en virtud de la Proposición A.6.2 y el Corolario A.6.4,

$$F_n \otimes_R R_\mathfrak{p} \cong R_\mathfrak{p} \otimes_R F_n \cong (F_n)_\mathfrak{p}.$$

Además, por la Proposición A.6.6,

$$R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \cong (R/\mathfrak{p}) \otimes_R R_\mathfrak{p} \cong (R/\mathfrak{p})_\mathfrak{p}.$$

Por tanto, la sucesión:

$$0 \longrightarrow F_n \otimes_R R_\mathfrak{p} \longrightarrow \cdots \longrightarrow F_0 \otimes_R R_\mathfrak{p} \longrightarrow R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \longrightarrow 0 \tag{2.8.4}$$

es exacta. Notemos que, como F_i es un R-módulo libre para cada i, $0 \leq i \leq n$, $F_i = \bigoplus_{X_i} R$ para algún conjunto X_i. Por la Proposición A.6.2,

$$F_i \otimes_R R_\mathfrak{p} = (\bigoplus_{X_i} R) \otimes_R R_\mathfrak{p} \cong \bigoplus_{X_i} (R \otimes_R R_\mathfrak{p}) \cong \bigoplus_{X_i} R_\mathfrak{p}.$$

Por tanto, $F_i \otimes_R R_\mathfrak{p}$ es un $R_\mathfrak{p}$-módulo libre para cada i, $0 \leq i \leq n$. Por tanto, la Sucesión (2.8.4) es una resolución libre del $R_\mathfrak{p}$-módulo $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ y $hd_{R_\mathfrak{p}}(R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}) \leq n$. Como R es un anillo noetheriano, por la Proposición A.8.1, $(R_\mathfrak{p}, \mathfrak{p}R_\mathfrak{p})$ es un anillo local noetheriano y, en virtud del Corolario 2.7.6,

$$gl.dim(R_\mathfrak{p}) = hd_{R_\mathfrak{p}}(R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}) \leq n < +\infty.$$

□

2.9. Factorización Única en Anillos Locales Regulares

Sean R un anillo noetheriano, $\mathfrak{p} \in Spec(R)$ un ideal primo de R y P un R-módulo proyectivo finitamente generado. Entonces, el $R_\mathfrak{p}$-módulo $P_\mathfrak{p}$ es libre (cf. Teorema A.4.7). Al ser finitamente generado (cf. Proposición A.8.1 y Corolario A.8.5), es de rango finito y tenemos una aplicación $rank_P : Spec(R) \longrightarrow \mathbb{N}$ dada por $rank_P(\mathfrak{p}) = rank_{R_\mathfrak{p}}(P_\mathfrak{p})$. Notemos que si P es un R-módulo libre finitamente generado, $rank_R(P) = rank_P(\mathfrak{p})$, $\forall \mathfrak{p} \in Spec(R)$ (cf. Proposición A.4.1).

Proposición 2.9.1. *Si $0 \longrightarrow P' \longrightarrow P \longrightarrow P'' \longrightarrow 0$ es una sucesión exacta de R-módulos proyectivos finitamente generados, $rank_R(P) = rank_R(P') + rank_R(P'')$, $\forall \mathfrak{p} \in Spec(R)$.*

Demostración. Como la localización es un functor exacto, la siguiente es una sucesión exacta para cada $\mathfrak{p} \in Spec(R)$: $0 \longrightarrow P'_\mathfrak{p} \longrightarrow P_\mathfrak{p} \longrightarrow P''_\mathfrak{p} \longrightarrow 0$. Como todos son proyectivos, la sucesión precedente se escinde, i.e. $P_\mathfrak{p} = P'_\mathfrak{p} \oplus P''_\mathfrak{p}$ y se da la igualdad de rangos enunciada. □

Proposición 2.9.2. *Sea R un anillo noetheriano y $\mathfrak{a} \in Spec(R)$ un ideal no nulo de R que es proyectivo como R-módulo. Entonces, $rank_\mathfrak{a}(\mathfrak{p}) = 1$, $\forall \mathfrak{p} \in Spec(R)$, $\mathfrak{a} \subseteq \mathfrak{p}$.*

Demostración. En un anillo cualquiera R, un ideal $\mathfrak{a} \subseteq R$ es un R-módulo libre si y solamente si es un ideal principal y $rank_\mathfrak{a}(\mathfrak{p}) = 1$ (ver [**Pardo, 21**] Problema 155). Por tanto, $\mathfrak{a}_\mathfrak{p}$ es un $R_\mathfrak{p}$-módulo libre $\forall \mathfrak{p} \in Spec(R)$, $\mathfrak{p} \supseteq \mathfrak{a}$ implica $rank_\mathfrak{a}(\mathfrak{p}) = 1$. □

En lo que sigue, cuando hagamos referencia a una resolución libre finita, entenderemos que cada R-módulo libre de la familia $\{P_i : i \in \mathbb{N}\}$ es finitamente generado (ver Definición 31).

Lema 2.9.3. *Sea P un R-módulo proyectivo que admite una resolución libre finita. Entonces, existe F un R-módulo libre finitamente generado de manera que $P \oplus F$ es un R-módulo libre finitamente generado.*

Demostración. Sea $0 \longrightarrow F_n \longrightarrow \cdots \longrightarrow F_0 \longrightarrow P \longrightarrow 0$ una resolución libre finita de P. Probemos el lema por inducción en n. Si $n = 0$, $P \cong F_0$ y se tiene trivialmente el resultado. Supongamos $n > 0$ y $K = ker(F_0 \longrightarrow P)$. Entonces, como P es proyectivo, la sucesión exacta corta: $0 \longrightarrow K \longrightarrow F_0 \longrightarrow P \longrightarrow 0$ se escinde y $F_0 \cong P \oplus K$. Por tanto, K es un R-módulo proyectivo. Más aún, se tiene que $0 \longrightarrow F_n \longrightarrow \cdots \longrightarrow F_1 \longrightarrow K \longrightarrow 0$ es una resolución libre finita de K. Por hipótesis inductiva, existe G un R-módulo libre finitamente generado de forma que $F = K \oplus G$ es un R-módulo libre finitamente generado. Pero como F_0 y G son R-módulos libres finitamente generados también lo será:

$$F_0 \oplus G \cong (P \oplus K) \oplus G \cong P \oplus (K \oplus G) = P \oplus F.$$

□

LEMA 2.9.4. *Sean R un anillo noetheriano y P un R-módulo verificando: $P \oplus R^n \cong R^{n+1}$ para algún $n \in \mathbb{N}$. Entonces, $P \cong R$.*

DEMOSTRACIÓN. Véase una prueba en la Sección A.7 del Apéndice A. □

COROLARIO 2.9.5. *Sea R un anillo noetheriano y $\mathfrak{a}$ un ideal no nulo de R que es proyectivo como R-módulo y que admite una resolución libre finita. Entonces, $\mathfrak{a} \cong R$.*

DEMOSTRACIÓN. Es consecuencia inmediata de combinar las Proposiciones 2.9.1 y 2.9.2 con el Lema 2.9.4. □

LEMA 2.9.6. *Sea R un dominio noetheriano. Entonces, R es dominio de factorización única si y solamente si cada ideal primo de altura 1 es principal.*

El lector puede encontrar una demostración en [**Pardo, 21**].

TEOREMA 2.9.7 (**Auslander-Buchsbaum**). *Todo anillo local regular $(R, \mathfrak{m})$ es dominio de factorización única.*

DEMOSTRACIÓN. Sea $(R, \mathfrak{m})$ un anillo local regular de cuerpo residual $k := R/\mathfrak{m}$ y de dimensión r. Probemos el teorema por inducción en r. Si $r = 0$, el ideal cero es maximal y, por tanto, R es cuerpo. Supongamos $r \geq 1$. Como R es local regular, en virtud del Corolario 1.5.4, R es dominio de integridad y, en vista del Lema 2.9.6, bastará ver que todo ideal de R de altura 1 es principal. Sea $\mathfrak{p} \in Spec(R)$ un ideal primo de R de altura 1. Notemos que, como $r \geq 1$, $\mathfrak{m} \neq 0$. Por el Lema de Nakayama (ver Proposición A.8.12) debe ser $\mathfrak{m} \neq \mathfrak{m}^2$. Sea $a \in \mathfrak{m} \setminus \mathfrak{m}^2$, entonces la clase de a módulo $\mathfrak{m}^2$ pertenece a una base del k-espacio vectorial $\mathfrak{m}/\mathfrak{m}^2$ y, por la Proposición 1.5.2, a pertenece a un conjunto generador minimal de $\mathfrak{m}$. Es decir, a es parte de un sistema regular de parámetros de $\mathfrak{m}$. Por el Corolario 1.5.6, aR es un ideal primo de R, i.e. a es un elemento primo de R. Consideremos el conjunto multiplicativamente cerrado $S = \{1, a, a^2 \dots\}$ y el anillo $T = S^{-1}R$. Si $a \in \mathfrak{p}$, $aR \subseteq \mathfrak{p}$ es un ideal primo contenido en $\mathfrak{p}$. Como $\mathfrak{p}$ es de altura 1 debe ser $aR = \mathfrak{p}$ y se tiene que $\mathfrak{p}$ es principal. Por tanto, podemos suponer que $a \notin \mathfrak{p}$. Por primalidad de $\mathfrak{p}$, debe verificarse: $a^n \notin \mathfrak{p}$ para cualquier $n \in \mathbb{N}$, $n \geq 1$. Por tanto, $S \cap \mathfrak{p} = \emptyset$. Como existe una correspondencia entre ideales primos de R con intersección vacía con S e ideales de $S^{-1}R = T$, $\mathfrak{p}T = S^{-1}\mathfrak{p}$ es un ideal primo de T. Más aún, como dicha correspondencia preserva la inclusión y $\mathfrak{p}$ es un ideal primo de R de altura 1, $\mathfrak{p}T$ es un ideal primo de T de altura 1 (ver Proposición A.2.4). Si a pertenece a todo ideal primo de R, en particular pertenece a todo ideal primo de altura 1. Siguiendo el mismo argumento que para el ideal $\mathfrak{p}$, se sigue que todo ideal primo de R de altura 1 es principal y, por tanto, R es DFU (cf. Lema 2.9.6). Sea $\mathfrak{q}$ un ideal primo de R que no contiene a a.

AFIRMACIÓN. $T_{\mathfrak{q}T} = R_{\mathfrak{q}}$.

DEMOSTRACIÓN. De un lado, sea $\frac{r}{s} \in R_{\mathfrak{q}}$, entonces $r \in R$ y $s \notin \mathfrak{q}$. Por consiguiente, $\frac{r}{s} = \frac{r/1}{s/1}$, donde $r/1 \in S^{-1}R = T$ y $s/1 \notin \mathfrak{q}T$. Entonces, $r/s \in T_{\mathfrak{q}T}$. De otro lado, sea $\frac{r/a^n}{s/a^m} = \frac{ra^{n-m}}{s} \in T_{\mathfrak{q}T}$, donde $m, n \in \mathbb{N}$. Por una parte, si $n \geq m$, $ra^{n-m} \in R$. Por otra parte, si $n < m$, como $a^{m-n} \notin \mathfrak{q}$; $s \notin \mathfrak{q}$ y $\mathfrak{q}$ es un ideal primo de R, $sa^{m-n} \notin \mathfrak{q}$. En conclusión, $\frac{r/a^n}{s/a^m} \in R_{\mathfrak{q}}$. □

Notemos que como R es un anillo local regular, en vista de la demostración del Teorema 2.8.6, $R_{\mathfrak{m}}$ es un anillo local regular de dimensión menor o igual que r. Además, como $a \notin \mathfrak{q}$, $\mathfrak{q} \subsetneq \mathfrak{m}$. En virtud de la Proposición 1.4.12:

$$dim_{Kr}(R_{\mathfrak{q}}) = ht(\mathfrak{q}) < ht(\mathfrak{m}) = dim_{Kr}(R_{\mathfrak{m}}) \leq r.$$

En virtud de la Afirmación precedente, $T_{\mathfrak{q}T}$ es un anillo local regular de dimensión estrictamente menor que r. Por hipótesis de inducción, $T_{\mathfrak{q}T}$ es dominio de factorización única. Ahora bien, si $\mathfrak{p} \nsubseteq \mathfrak{q}$, existe $x \in \mathfrak{p}$ con $x \notin \mathfrak{q}$. Por tanto, $x/1 \in \mathfrak{p}R_{\mathfrak{q}}$ es una unidad de $R_{\mathfrak{q}}$. Por consiguiente, $\mathfrak{p}T_{\mathfrak{q}T} = \mathfrak{p}R_{\mathfrak{q}} = R_{\mathfrak{q}} = T_{\mathfrak{q}T}$ es un $T_{\mathfrak{q}T}$-módulo libre. De otro lado, si $\mathfrak{p} \subseteq \mathfrak{q}$, $\mathfrak{p} \cap (R \setminus \mathfrak{q}) = \emptyset$. Por tanto, en virtud de la correspondencia que preserva el orden de la Proposición A.2.4, $\mathfrak{p}R_{\mathfrak{q}} = \mathfrak{p}T_{\mathfrak{q}T}$ es un ideal primo de $R_{\mathfrak{q}} = T_{\mathfrak{q}T}$ de altura 1. Por el Lema 2.9.6, $\mathfrak{p}T_{\mathfrak{q}T}$ es un ideal principal. Como $T_{\mathfrak{q}T}$ es dominio de integridad, el elemento que genera el ideal $\mathfrak{p}T_{\mathfrak{p}T}$ no es un divisor de cero. Por consiguiente, $\mathfrak{p}T_{\mathfrak{q}T} = (\mathfrak{p}T)_{\mathfrak{q}T}$ es un $T_{\mathfrak{q}T}$-módulo libre. Pero todo ideal primo de T es de la forma

$\mathfrak{q}T$ para algún ideal $\mathfrak{q}$ de R (cf. Proposición A.2.4). Por tanto, en virtud del Teorema A.4.7, el ideal $\mathfrak{p}T$ es proyectivo como T-módulo. Ahora bien, como R es noetheriano, $\mathfrak{p}$ es finitamente generado como R-módulo, por la demostración de la Proposición 2.3.1, se puede construir una sucesión exacta de la forma:

$$\mathcal{P}: \quad 0 \longrightarrow K_r \longrightarrow P_{r-1} \longrightarrow \cdots \longrightarrow P_0 \longrightarrow \mathfrak{p} \longrightarrow 0,$$

donde P_i es un R-módulo proyectivo finitamente generado para todo i, $1 \leq i \leq r-1$ y K_r es un R-módulo finitamente generado. Como R es regular de dimensión r, por el Teorema 2.8.5, se sigue que:

$$hd_R(\mathfrak{p}) \leq gl.dim(R) = r < +\infty.$$

Por la equivalencia $i) \Leftrightarrow iv)$ de la Proposición 2.6.3, $P_r := K_r$ es un R-módulo proyectivo. Ahora bien, como P_i es un R-módulo finitamente generado para cada i, $1 \leq i \leq r$, por la Proposición 2.6.1, $\{P_i\}_{i=1}^r$ es una familia de R-módulos libres finitamente generados, i.e. $\mathcal{P}$ es una resolución libre finita de $\mathfrak{p}$ como R-módulo. Como $\mathcal{P}$ es una sucesión exacta, por la Proposición A.2.7, también lo será la sucesión:

$$0 \longrightarrow S^{-1}P_r \longrightarrow \cdots \longrightarrow S^{-1}P_0 \longrightarrow S^{-1}\mathfrak{p} = \mathfrak{p}T \longrightarrow 0. \tag{2.9.1}$$

Más aún, como P_i es un R-módulo libre finitamente generado para cada $i, 1 \leq 1 \leq r$, en virtud del Corolario A.6.4, se tiene que:

$$S^{-1}P_i \cong S^{-1}R \otimes_R P_i = T \otimes_R P_i \cong T \otimes_R R^{n_i} \cong (T \otimes_R R)^{n_i} = T^{n_i},$$

con $n_i \in \mathbb{N}$ y donde las últimas dos igualdades se tienen por la Proposición A.6.2. Por consiguiente, $S^{-1}P_i$ es un T-módulo libre finitamente generado para todo i, $1 \leq i \leq r$, i.e. la Sucesión (2.9.1) es una resolución libre finita de $\mathfrak{p}T$ como T-módulo. Como $\mathfrak{p}T$ es proyectivo como T-módulo, en virtud del Corolario 2.9.5, $\mathfrak{p}T \cong T$. En particular, $\mathfrak{p}T$ es un ideal principal. Sea $p \in \mathfrak{p}$ tal que $pT = \mathfrak{p}T$. Si $a^i \mid p$ para todo $i \in \mathbb{N}$ y $\mathfrak{a} := aR$ es el ideal de R generado por a, entonces $p \in a^iR = (aR)^i = \mathfrak{a}^i$ para todo $i \in \mathbb{N}$. Como $(R, \mathfrak{m})$ es un anillo local noetheriano, $\mathfrak{a} \subseteq \mathfrak{m} = \mathfrak{R}$ es un ideal contenido en el radical de Jacobson de R; y R es finitamente generado como R-módulo, por el Teorema de la Intersección de Krull (cf. Teorema 1.3.4), se tiene que:

$$p \in \bigcap_{i \in \mathbb{N}} \mathfrak{a}^i = (0).$$

En consecuencia, $p = 0$ y $\mathfrak{p}T = (0)$. Pero como R es dominio de integridad, (0) es un ideal primo de R. Por la correspondencia biyectiva que preserva el orden dada en la Proposición A.2.4, debe ser $\mathfrak{p} = (0)$ y, por tanto, $\mathfrak{p}$ es un ideal principal. De otro lado, sea $n \in \mathbb{N}$ tal que $a^n \mid p$, $a^{n+1} \nmid p$. Entonces, $p = a^nq$ para algún q en R verificando $a \nmid q$. Como $a^n \notin \mathfrak{p}$ y $\mathfrak{p}$ es un ideal primo, debe ser $q \in \mathfrak{p}$. Entonces, $\mathfrak{p}T = pT \subseteq qT \subseteq \mathfrak{p}T$. Sustituyendo p por q podemos suponer, sin pérdida de generalidad, que $a \nmid p$.

Afirmación. $pT \cap R = pR$.

Demostración. De un lado, como $R \subseteq T$ mediante el morfismo natural $R \longrightarrow S^{-1}R = T$, $pR \subseteq pT$. Además, $pR \subseteq R$. Por tanto, $pR \subseteq pT \cap R$. De otro lado, un elemento de $pT \cap R$ será de la forma cp/a^m con $c \in R$ y $m \in \mathbb{N}$ verificando $a^m \mid cp$. Entonces, $a \mid cp$. Como $a \nmid p$ y a es primo, $a \mid c$. Sea $c_1 = c/a$. Se tiene que $a^{m-1} \mid c_1p$, siguiendo el mismo razonamiento, se llega a que $a \mid c_1$, i.e. $a^2 \mid c$. Repitiendo este proceso $m-2$ veces se concluye que $a^m \mid c$. En consecuencia, $cp/a^m = p(c/a^m) \in pT$. $\square$

Finalmente, por la Proposición A.2.4, $\mathfrak{p} = i_R^{-1}(\mathfrak{p}T) = \mathfrak{p}T \cap R = pT \cap R = pR$. Por tanto, $\mathfrak{p}$ es un ideal principal. $\square$

APÉNDICE A

Algunos Resultados Clásicos de Álgebra Conmutativa

En este Apéndice vamos a recopilar algunos resultados clásicos de Álgebra Conmutativa, esencialmente a la manera de los seguidores de E. Noether y E. Artin. Aprovecharemos también para dar pruebas detalladas que no caben en el cuerpo del TFG y que creemos, ayudan a comprender las secciones 1.2 y 1.3 del Capítulo 1.
Las demostraciones no incluidas pueden encontrarse en cualquiera de las referencias básicas de este TFG: [**Pardo, 21**], [**Raghavan et al., 1975**] y [**Atiyah, 1969**].

A.1. Sucesiones Exactas y Sucesiones Exactas Cortas

Definición 41 (**Sucesiones exactas de R-módulos**). *Las sucesiones exactas de R-módulos son complejos de cadena de R-módulos*

$$C: \underline{M} \qquad \xrightarrow{d_{n+1}} M_n \xrightarrow{d_n} M_{n-1} \xrightarrow{d_{n-1}} M_{n-2} \xrightarrow{d_{n-2}} \dots$$

que verfican:

$$Im(d_{n+1}) = ker(d_n), \ \forall n \in \mathbb{Z}.$$

Se llaman sucesiones exactas cortas a las sucesiones exactas de la forma:

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

Proposición A.1.1. *Una sucesión de R-módulos*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

es exacta si y solamente si f es un monomorfismo de R-módulos, g es un epimorfismo de R-módulos y $ker(g) = Im(f)$.

Demostración. Es inmediata teniendo en cuenta que la condición de que f sea monomorfismo es equivalente a la condición de exactitud de la sucesión en M' y que la condición de que g sea epimorfismo es equivalente a la condición de exactitud de la sucesión en M''. $\square$

Observación 13. *Toda sucesión exacta de R-módulos ... $\xrightarrow{f_{n+1}} M_n \xrightarrow{f_n} M_{n-1} \xrightarrow{f_{n-1}}$ ... puede descomponerse en sucesiones exactas cortas de R-módulos*

$$\begin{tikzcd}
 & & \vdots \arrow[d, "f_{n+1}"] & & \\
0 \arrow[r] & M'_n \arrow[r] & M_n \arrow[r] \arrow[d, "f_n"] & M''_n \arrow[r] & 0 \\
0 \arrow[r] & M'_{n-1} \arrow[r] & M_{n-1} \arrow[r] \arrow[d, "f_{n-1}"] & M''_{n-1} \arrow[r] & 0 \\
 & & \vdots & &
\end{tikzcd}$$

definiendo $M'_i = Im(f_{n+1})$ y $M''_i = ker(f_n)$.

Proposición A.1.2. *Sea $\{0 \longrightarrow M'_i \xrightarrow{f_i} M_i \xrightarrow{g_i} M''_i \longrightarrow 0\}_{i \in I}$ una familia de sucesiones de R-módulos. Entonces,*

$$0 \longrightarrow M'_i \xrightarrow{f_i} M_i \xrightarrow{g_i} M''_i \longrightarrow 0$$

es una sucesión exacta para cada $i \in I$ si y solamente si la sucesión:

$$0 \longrightarrow \bigoplus_{i\in I} M_i' \xrightarrow{\bigoplus_{i\in I} f_i} \bigoplus_{i\in I} M_i \xrightarrow{\bigoplus_{i\in I} g_i} \bigoplus_{i\in I} M_i'' \longrightarrow 0$$

es exacta. Donde para definir el morfismo de R-módulos $\bigoplus_{i\in I} f_i : \bigoplus_{i\in I} M_i' \longrightarrow \bigoplus_{i\in I} M_i$, dado $i \in I$ y $m' \in M_i'$, se define $(\bigoplus_{i\in I} f_i)(m_i') := f_i(m_i')$, y se extiende por linealidad a $\bigoplus_{i\in I} M_i'$. El morfismo de R-módulos $\bigoplus_{i\in I} g_i$ se define de manera análoga.

Lema A.1.3 (**Snake Lemma**). *Consideremos un diagrama de R-módulos y morfismos como el siguiente, en el que las filas son sucesiones exactas cortas:*

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

Entonces, exite un morfismo de R-módulos: $d : ker(f'') \longrightarrow Coker(f')$ tal que la siguiente sucesión es exacta:

$$0 \longrightarrow ker(f') \longrightarrow ker(f) \longrightarrow ker(f'') \xrightarrow{d} Coker(f') \longrightarrow Coker(f) \longrightarrow Coker(f'') \longrightarrow 0,$$

donde los demás morfismos son inducidos por las filas horizontales del diagrama inicial.

Una prueba puede encontrarse en [**Pardo, 21**].

A.2. Anillos de Fracciones y Localización

La construcción de anillos de fracciones es una generalización natural de la construcción del cuerpo de fracciones de un dominio de integridad, en la que dado un conjunto S que verifica ciertas propiedades, se construye un anillo en el que los elementos de S son unidades.

Definición 42. *Sea R un anillo. Un subconjunto S de R se dice multiplicativamente cerrado si $1 \in S$ y S es cerrado para el producto.*

Dado un anillo R y $S \subset R$ multiplicativamente cerrado, se puede definir una relación de equivalencia $\equiv$ en $R \times S$ de manera que $(a, s) \equiv (b, t)$ si $(at - bs)u = 0$ para algún u en S.
El conjunto de clases de equivalencia se denota $S^{-1}R$ y se le dota de estructura de anillo con las siguientes operaciones (que son independientes de la clase elegida):

$$(a, s) + (b, t) = (at + bs, st);$$
$$(a, s)(b, t) = (ab, ts).$$

El anillo $S^{-1}R$ se denomina anillo de fracciones de R con respecto a S.
Existe un morfismo natural entre R y $S^{-1}R$ dado por $i_R : R \longrightarrow S^{-1}R$ con $i_R(a) = (a, 1) = (a/1)$ para cada $a \in R$ que verifica que si $s \in S$, entonces $i_R(s)$ es una unidad en $S^{-1}R$. De hecho, dicho morfismo es universal con respecto a esta propiedad.

Definición 43. *Con las notaciones precedentes se consideran las siguientes nociones:*

i) Sea $\mathfrak{a}$ es un ideal de R, entonces se define el ideal extendido de $\mathfrak{a}$ y se denota $\mathfrak{a}^e$ al ideal de $S^{-1}R$ generado por $f(\mathfrak{a})$.
ii) Sea $\mathfrak{b}$ un ideal de $S^{-1}R$, se define el ideal contraído de de $\mathfrak{b}$ y se denota $\mathfrak{b}^c$ al ideal $f^{-1}(\mathfrak{b})$ de R.

Lema A.2.1. *Sea $\mathfrak{a}$ un ideal propio de un anillo R y $\mathfrak{p}_1, \ldots, \mathfrak{p}_s \in Spec(R)$ un conjunto finito de ideales primos. Si $\mathfrak{a} \subseteq \bigcup_{i=1}^{s} \mathfrak{p}_i$, entonces existe j con $0 \le j \le s$ tal que $\mathfrak{a} \subseteq \mathfrak{p}_j$.*

Lema A.2.2. *Sean $\mathfrak{a}$, $\mathfrak{b}_0$, $\mathfrak{b}_1, \ldots, \mathfrak{b}_n$ ideales de un anillo R, donde $\mathfrak{b}_0$ es un ideal primo. Entonces, existe un subconjunto propio $J \subsetneq \{0, 1, \ldots, n\}$ tal que $\mathfrak{a} \subseteq \bigcup_{j\in J} \mathfrak{b}_j$.*

Proposición A.2.3. *Con las notaciones precedentes, todo ideal de $S^{-1}R$ es ideal extendido de algún ideal de R. Más aún, existe una correspondencia biyectiva que conserva el orden entre los ideales contraídos de R y los ideales de $S^{-1}R$*

Hay, además, una relación estrecha entre los ideales de un anillo R y los ideales de $S^{-1}R$ localizado de R en $\mathfrak{p}$ con $\mathfrak{p} \in Spec(R)$:

PROPOSICIÓN A.2.4. *Sea R un anillo y S un subconjunto de R multiplicativamente cerrado, entonces:*

$$\begin{array}{cccc} \varphi : & \{\mathfrak{p} \in Spec(R) : S \cap \mathfrak{p} = \emptyset\} & \longrightarrow & \{\mathfrak{p}S^{-1}R = S^{-1}\mathfrak{p} \in Spec(S^{-1}R)\} \\ & \mathfrak{p} & \longmapsto & \mathfrak{p}S^{-1}R \\ & i_R^{-1}(\mathscr{P}) & \longleftarrow & \mathscr{P} \end{array}$$

es una biyección que preserva la inclusión entre los ideales primos de R con $S \cap \mathfrak{p} = \emptyset$ y los ideales primos de $S^{-1}R$, donde $i_R : R \longrightarrow S^{-1}R$ es el morfismo natural descrito anteriormente.

Dado un anillo R y $\mathfrak{p}$ un ideal primo de R, un conjunto multiplicativamente cerrado de especial interés será $S = R \setminus \mathfrak{p}$. En este caso, $S^{-1}R$ se escribe $R_\mathfrak{p}$. Además, $R_\mathfrak{p}$ es un anillo que tiene a $\mathfrak{m} = \{a/s : a \in \mathfrak{p}\}$ como único maximal. Un anillo que verifica esta propiedad se dice anillo local. En particular, $R_\mathfrak{p}$ se denomina el localizado de R en $\mathfrak{p}$.
De manera análoga a partir de un R-módulo M se puede construir su módulo de fracciones $S^{-1}M$, que tiene estructura de $S^{-1}R$-módulo. Cuando $S = \mathfrak{p}$ con $\mathfrak{p} \in Spec(R)$ se denota por $M_\mathfrak{p}$ y se denomina el localizado de M en $\mathfrak{p}$.
De la misma forma, aplicando La Proposición A.2.4 a $S = R \setminus \mathfrak{p}$ se tiene el siguiente resultado sobre anillos localizados:

COROLARIO A.2.5. *Sea R un anillo y $\mathfrak{p}$ un ideal primo de R. Los ideales primos de $R_\mathfrak{p}$ están en correspondencia biyectiva con los ideales primos de R contenidos en $\mathfrak{p}$. Además, dicha biyección preserva el orden.*

Al proceso por el cual se pasa de M a $M_\mathfrak{p}$ se denomina localización en $\mathfrak{p}$. Es una herramienta especialmente útil en la rama de Geometría Algebraica, donde se analiza el comportamiento de anillos de funciones alrededor de un punto p: permite considerar exclusivamente una colección de ellas que son no nulas en dicho punto y estudiar cómo se comportan en un entorno obviando información no local. Esto nos permite definir la conocidas como propiedades locales en módulos.
La localización define, además, un functor covariante S^{-1} de la categoría de R-módulos a la categoría de $S^{-1}R$-módulos que asigna a cada morfismo de R-módulos $f : M \longrightarrow N$ un morfismo de $S^{-1}R$-módulos $S^{-1}f : S^{-1}M \longrightarrow S^{-1}N$ con $(S^{-1}f)(a/t) = f(a)/t$ para cada $a/t \in S^{-1}M$. Este functor será de gran utilidad a la hora de probar dichas propiedades locales.

PROPOSICIÓN A.2.6. *Sea M un R-módulo. Ser cero es una propiedad local. Es decir, son equivalentes:*

i) $M = 0$.
ii) $M_\mathfrak{p} = 0$ *para todo* $\mathfrak{p} \in Spec(R)$.
iii) $M_\mathfrak{m} = 0$ *para todo* $\mathfrak{m} \in MaxSpec(R)$.

Además, se tiene esta propiedad, que afirma la exactitud del functor localización y establece una relación entre los soportes de módulos (Ver Definición 62 en la Sección A.10 del Apéndice A) que forman parte de una sucesión exacta corta:

PROPOSICIÓN A.2.7. *Dada una sucesión exacta corta de R-módulos*

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

se tiene que

$$\mathbf{0} \longrightarrow S^{-1}M' \longrightarrow S^{-1}M \longrightarrow S^{-1}M'' \longrightarrow \mathbf{0}$$

es también una sucesión exacta corta. En particular, la localización en $\mathfrak{p}$ es un functor exacto. Esto implica que $M_\mathfrak{p} = 0$ si y solamente si $M'_\mathfrak{p} = 0$ y $M''_\mathfrak{p} = 0$ o equivalentemente:

$$Supp(M) = Supp(M') \cup Supp(M'')$$

.

A.3. El Bi-functor $Hom_R(-,-)$.

Dado un anillo R, a partir del R-módulo $Hom_R(M,N)$, donde M y N son R-módulos, se pueden definir dos functores de la categoría de R-módulos en sí misma, uno covariante y otro contravariante.
El functor covariante $Hom_R(M,-)$ asigna a cada R-módulo N el R-módulo $Hom_R(M,N)$ y a cada morfismo de R-módulos $f : N \longrightarrow N'$ el morfismo

$$\begin{array}{rccl} Hom_R(M,f): & Hom_R(M,N) & \longrightarrow & Hom_R(M,N') \\ & g & \longmapsto & Hom_R(M,f)(g) := f \circ g. \end{array}$$

El functor contravariante $Hom_R(-,N)$ asigna a cada R-módulo M el R-módulo $Hom_R(M,N)$ y a cada morfismo de R-módulos $f : M \longrightarrow M'$ el morfismo

$$\begin{array}{rccl} Hom_R(f,N): & Hom_R(M',N) & \longrightarrow & Hom_R(M,N) \\ & g & \longmapsto & Hom_R(f,N)(g) := g \circ f. \end{array}$$

A la combinación de ambos functores se le denomina bi-functor. $Hom_R(-,-)$.

PROPOSICIÓN A.3.1. *Sea R un anillo y M un R-módulo. Entonces, $Hom_R(M,-)$ y $Hom_R(-,M)$ son functores exactos a izquierda. Esto es, si $0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0$ es una sucesión exacta de R-módulos. Entonces, se tienen las sucesiones exactas:*

$$0 \longrightarrow Hom_R(M,N') \overset{Hom_R(M,f)}{\longrightarrow} Hom_R(M,N) \overset{Hom_R(M,g)}{\longrightarrow} Hom_R(M,N'')$$

y

$$0 \longrightarrow Hom_R(N'',M) \overset{Hom_R(g,M)}{\longrightarrow} Hom_R(N,M) \overset{Hom_R(f,M)}{\longrightarrow} Hom_R(N',M)$$

A.4. Módulos Libres y Proyectivos: Propiedades Esenciales

DEFINICIÓN 44 (**Módulo Libre**). *Un R-módulo M se dice libre si existe un conjunto X de tal modo que M es isomorfo al R-módulo siguiente:*

$$\bigoplus_X R := \{f : X \longrightarrow R : f \text{ es aplicación y } \exists Y \subseteq X \text{ finito con } f(x) = 0, \ \forall x \in X \setminus Y\}$$

Si podemos elegir X de cardinal finito diremos que M es un R-módulo libre de rango finito.

Si M es un R-módulo libre de rango finito, entonces todas sus bases tienen el mismo cardinal. A ese cardinal se le denomina rango de M como R-módulo libre y se denota por $rank_R(M)$. Una prueba de esta afirmación puede encontrarse en [**Pardo, 21**].

PROPOSICIÓN A.4.1. *Sea M un R-módulo libre. Entonces,*

i) $M_\mathfrak{p}$ es un $R_\mathfrak{p}-$módulo libre para todo $p \in Spec(R)$. Además, si M es de rango finito y $n = rank_R(M)$, entonces $n = rank_{R_\mathfrak{p}}(M_\mathfrak{p})$;
ii) $M_\mathfrak{m}$ es un $R_\mathfrak{m}-$módulo libre para todo $\mathfrak{m} \in MaxSpec(R)$. Además, si M es de rango finito y $n = rank_R(M)$, entonces $n = rank_{R_\mathfrak{m}}(M_\mathfrak{m})$.

DEFINICIÓN 45 (**Módulo Proyectivo**). *Un R-módulo P se dice proyectivo si el functor covariante $Hom_R(P,-)$ es exacto.*

PROPOSICIÓN A.4.2. *Sea P un R-módulo. Las siguientes afirmaciones son equivalentes:*

i) P es un R-módulo proyectivo;
ii) el R-módulo P satisface la siguiente propiedad: dado un epimorfismo de R-módulos cualquiera $g : N \longrightarrow M$ y dado cualquier morfismo de R-módulos $f : P \longrightarrow M$, existe un morfismo de R-módulos $h : P \longrightarrow N$ tal que $g \circ h = f$. Esto es, dado un diagrama

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

donde la sucesión horizontal es exacta, existe $h : P \longrightarrow N$ tal que el siguiente diagrama es conmutativo:

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

iii) *toda sucesión exacta corta de la forma:*

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

se escinde. Es decir, existe un isomorfismo $\psi : M \longrightarrow M' \oplus M''$ que, además, hace conmutativo el siguiente diagrama cuyas filas son sucesiones exactas cortas:

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "f"] \arrow[d, "Id_{M'}"] & M \arrow[r, "g"] \arrow[d, "\psi"] & M'' \arrow[r] \arrow[d, "Id_{M''}"] & 0 \\
0 \arrow[r] & M' \arrow[r, "i'"] & M' \oplus M'' \arrow[r, "\pi''"] & M'' \arrow[r] & 0,
\end{tikzcd}$$

donde $i' : M' \longrightarrow M' \oplus M''$ y $\pi'' : M' \oplus M'' \longrightarrow M''$ son la inclusión y proyección canónica respectivamente.

iv) *el R-módulo P es un sumando directo de un R-módulo libre. Es decir, existe un R-módulo Q tal que $F = P \oplus Q$ es un R-módulo libre.*

COROLARIO A.4.3. *Todo R-módulo libre es proyectivo; toda suma directa de R-módulos proyectivo es un R-módulo proyectivo; todo sumando directo de un R-módulo proyectivo es un R-módulo proyectivo.*

PROPOSICIÓN A.4.4. *Sea*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

una sucesión exacta de R-módulos. Si P es un R-módulo proyectivo, la sucesión de R-módulos:

$$0 \longrightarrow P \otimes_R M' \xrightarrow{Id_P \otimes f} P \otimes_R M \xrightarrow{Id_P \otimes g} P \otimes_R M'' \longrightarrow 0,$$

es exacta.

COROLARIO A.4.5. *Si P es un R-módulo proyectivo y $f : R \longrightarrow S$ es un morfismo de anillos, entonces $S \otimes_R P$ es un S-módulo proyectivo.*

DEFINICIÓN 46 (**Módulo Plano**). *Un R-módulo N se dice plano si el functor $(- \otimes_R N)$ es exacto.*

TEOREMA A.4.6. *Sea M un R-módulo. Entonces,*

$$M \text{ es libre} \Longrightarrow M \text{ es proyectivo} \Longrightarrow M \text{ es plano.}$$

TEOREMA A.4.7. *Sea R un anillo noetheriano y M un R-módulo finitamente generado. Son equivalentes:*

i) *M es un R-módulo proyectivo.*

ii) *$M_{\mathfrak{p}}$ es un $R_{\mathfrak{p}}$-módulo libre para cada $\mathfrak{p} \in Spec(R)$.*

A.5. Módulos Inyectivos: Propiedades Básicas

DEFINICIÓN 47. *Un R-módulo I se dice inyectivo si el functor contravariante $Hom_R(-, I)$ es un functor exacto.*

OBSERVACIÓN 14. *Notemos que, en virtud de la Proposición A.3.1, $Hom_R(-, I)$ es un functor exacto a izquierda para cualquier R-módulo I. Por tanto, $Hom_R(-, I)$ será exacto si y solamente si dada una sucesión exacta de R-módulos*

$$0 \longrightarrow N' \xrightarrow{\ i\ } N \xrightarrow{\ \pi\ } N'' \longrightarrow 0,$$

se tiene que, en la sucesión de R-módulos:

$$0 \longrightarrow Hom_R(N'', I) \xrightarrow{Hom_R(\pi, I)} Hom_R(N, I) \xrightarrow{Hom_R(i, I)} Hom_R(N', I),$$

el morfismo $Hom_R(i, I)$ es suprayectivo.

De manera análoga a la propiedad de levantamiento para módulos proyectivos, la condición de ser inyectivo puede expresarse del modo siguiente:
Un R-módulo I es inyectivo si y solamente si dado cualquier monomorfismo $i : N' \longrightarrow N$ y

dado cualquier morfismo $f : N' \longrightarrow I$, existe un morfismo $h : N \longrightarrow I$ tal que el siguiente diagrama conmuta:

$$\begin{tikzcd} 0 \arrow[r] & N' \arrow[r, "i"] \arrow[d, "f"] & N \arrow[dl, dotted, "\exists h"] \\ & I & \end{tikzcd}$$

El siguiente resultado clásico de R. Baer simplifica la caracterización de los R-módulos inyectivos (ver una prueba en [**Pardo, 21**], por ejemplo).

TEOREMA A.5.1 (**Criterio de Baer**). *Un R-módulo es inyectivo si y solamente si para cada ideal $\mathfrak{a}$ de R y cada morfismo $f : \mathfrak{a} \longrightarrow N$, existe una extensión $g : R \longrightarrow N$ verificando que $g|_{\mathfrak{a}} = f$.*

PROPOSICIÓN A.5.2. *Todo R-módulo es isomorfo a un submódulo de un R-módulo inyectivo.*

A.6. Producto Tensorial de R-módulos

PROPOSICIÓN A.6.1. *Sean M, N dos R-módulos. Existe un par (T, Φ) con T R-módulo, $\Phi : M \times N \longrightarrow T$ bilineal que verifica la siguiente propiedad: para todo $R-$módulo T' y toda aplicación $f : M \times N \longrightarrow P$ bilineal existe un único morfismo de R-módulos $\varphi : T \longrightarrow P$ que hace el diagrama*

$$\begin{tikzcd} M \times N \arrow[d, "\Phi"'] \arrow[dr, "f"] & \\ T \arrow[r, "\varphi"'] & P \end{tikzcd}$$

conmutativo. Además, T es único salvo isomorfismo.

DEFINICIÓN 48. *Dados M, N dos R-módulos, el par (T, Φ) que verifica A.6.1 se denomina producto tensorial de M y N. Se denota por $(M \otimes_R N, \Phi)$, aunque de manera habitual la aplicación Φ se omite. Las imágenes de los elementos $(m, n) \in M \times N$ se escriben $\Phi(m, n) = m \otimes n$.*

De esta manera se establece una correspondencia biyectiva entre aplicaciones bilineales $M \times N \longrightarrow P$ y morfismos de R-módulos $T \longrightarrow P$.
La demostración de la existencia del par (Φ, T) en la Proposición A.6.1 se hace construyendo el cociente del R-módulo libre $T_0 = \bigoplus_{M \times N} R$ por el submódulo N generado por el conjunto $\{\lambda_1(m_1+m_2)*\lambda_2(n_1+n_2) - \lambda_1\lambda_2(m_1*n_1) - \lambda_1\lambda_2(m_1*n_2) - \lambda_1\lambda_2(m_2*n_1) - \lambda_1\lambda_2(m_2*n_2)\}$. Por tanto, se tiene que cada elemento $(m, n) \in M \times N$ determina unívocamente un elemento de la base de T_0. Como la proyección canónica $\pi : T_0 \longrightarrow T$ es morfismo suprayectivo, $\{\Phi(m, n) : (m, n) \in M \times N\}$ es un conjunto generador de T. Sin embargo, no todos los elementos en T son de la forma $\Phi(m, n)$ para algún $(m, n) \in M \times N$.

A.6.1. Propiedades del Producto Tensorial.

PROPOSICIÓN A.6.2. *Sea $\{M_i\}_{i \in I}$ una familia de R-módulos. Dados M,N y P R-módulos, el producto tensorial verifica las siguientes propiedades:*

i) *Conmuta con la suma directa: $(\bigoplus_I M_i) \otimes_R N \cong \bigoplus_I (M_i \otimes_R N)$.*
ii) *Es conmutativo: $M \otimes_R N \cong N \otimes_R M$. Más aún, el isomorfismo $M \otimes_R N \cong N \otimes_R M$ es functorial en M y N.*
iii) *Es asociativo: $(M \otimes_R N) \otimes_R P \cong M \otimes_R (N \otimes_R P)$.*
iv) *Posee "elemento neutro": $(R \otimes_R M) \cong M$.*

OBSERVACIÓN 15. *Un caso más general de la propiedad iii) en la Proposición A.6.2 se da si M es un R-módulo, P es un S-módulo y N es un $R-S$-bimódulo (es decir, N tiene estructura de R-módulo y S-módulo). En este caso, $M \otimes_R N$ y $N \otimes_S P$ son $R-S$-bimódulos y $(M \otimes_R N) \otimes_S P \cong M \otimes_R (N \otimes_S P)$*

OBSERVACIÓN 16. *La propiedad enunciada en la Proposición A.6.1 admite una versión más general para aplicaciones multilineales dando lugar al conocido como producto multi-tensorial y se relaciona con el producto tensorial de la siguiente forma:*

$$M_1 \otimes_R M_2 \otimes_R ... \otimes_R M_n \cong (...(M_1 \otimes_R M_2) \otimes_R ...M_{n-1}) \otimes_R M_n.$$

De esta manera se elimina cualquier tipo de ambigüedad.

PROPOSICIÓN A.6.3. *Sean M, y N R-módulos. Entonces, se tiene:*

$$S^{-1}M \otimes_{S^{-1}R} S^{-1}N \cong S^{-1}(M \otimes_R N).$$

En particular, si $\mathfrak{p} \in spec(R)$,

$$M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} N_{\mathfrak{p}} \cong (M \otimes_R N)_{R_{\mathfrak{p}}}.$$

COROLARIO A.6.4. *Sean M, y N R-módulos. Entonces,*

$$S^{-1}M \cong S^{-1}R \otimes_R M.$$

En particular, si $\mathfrak{p} \in spec(R)$,

$$M_{\mathfrak{p}} \cong R_{\mathfrak{p}} \otimes_R M.$$

PROPOSICIÓN A.6.5. *Sea N un R-módulo, entonces el functor $- \otimes_R N$ es un functor exacto a derecha. Es decir, dada una sucesión exacta de R-módulos: $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$, la sucesión:*

$$0 \longrightarrow M' \otimes_R N \longrightarrow M \otimes_R N \longrightarrow M'' \otimes_R N \longrightarrow 0$$

es exacta.

A.6.2. Extensión de Escalares.

DEFINICIÓN 49. *Sea $f : R \longrightarrow T$ un morfismo de anillos y sea N un R-módulo. Entonces, podemos definir una estructura de T-módulo sobre $T \otimes_R N$ de la manera siguiente:*

$$\begin{array}{rccc} \cdot_T : & T \times (T \otimes_R N) & \longrightarrow & T \otimes_R N \\ & (\lambda, \sum_{i \in I} x_i \otimes n_i & \longmapsto & (\sum_{i \in I} (\lambda x_i) \otimes n_i \end{array}$$

para cada conjunto finito I con $x_i \in T$, $n_i \in N$. Se dice que $T \otimes_R N$ es el módulo obtenido por extensión de escalares a partir de $f : R \longrightarrow T$.

Como consecuencia de esta construcción se tiene el siguiente resultado:

PROPOSICIÓN A.6.6. *Sea M un R-módulo y $\mathfrak{a}$ un ideal de R. Entonces, la extensión de escalares de M a través de la proyección canónica $\pi : R \longrightarrow R/\mathfrak{a}$ satisface:*

$$R/\mathfrak{a} \otimes_R M \cong M/\mathfrak{a}M.$$

A.7. Producto Exterior

DEFINICIÓN 50. *Sean M, N R-módulos; $p \geq 1$ un entero y $\otimes^p M$ el producto tensorial de M consigo mismo p veces. Se dice que un morfismo $f : \otimes^p M \longrightarrow N$ es alterno si para cada $x_1, ..., x_p \in M$, $f(x_1 \otimes_R ... \otimes_R x_n) = 0$ siempre que $x_i = x_j$ para algún i, j con $i \neq j$, $1 \leq i, j \leq p$.*

PROPOSICIÓN A.7.1. *Sea M un R-módulo y $p \geq 1$ un entero. Existe un par (E_p, ψ) donde E_p es un R-módulo y $\psi : \otimes^p M \longrightarrow E_p$ es un morfismo alterno que verifica la siguiente propiedad: para todo R-módulo N y morfismo alterno $f : \otimes^p M \longrightarrow N$ existe un único morfismo $\tilde{f} : E_p \longrightarrow N$ que hace el diagrama*

$$\begin{tikzcd} \otimes^p M \arrow[d, "\psi"'] \arrow[dr, "f"] & \\ E_p \arrow[r, "\tilde{f}"'] & N \end{tikzcd}$$

conmutativo. Además, E_p es único salvo isomorfismo.

DEFINICIÓN 51. *Dado un R-módulo M el par (E_p, ψ) que verifica A.7.1 se denomina p-ésima potencia exterior. Se denota por $(\wedge^p M, \psi)$, aunque de manera habitual la aplicación ψ se omite. Las imágenes de los elementos $x_1 \otimes_R ... \otimes_R x_p \in \otimes^p M$ se escriben $\psi(x_1 \otimes_R ... \otimes_R x_p) = x_1 \wedge ... \wedge x_p$.*

Para demostrar la existencia del producto exterior se utiliza un argumento análogo al enunciado para el producto tensorial de R-módulos. Se considera el conjunto T_0 generado por los elementos de la forma $x_1 \otimes_R ... \otimes_R x_p$ y se toma su cociente por el submódulo N que está generado el subconjunto $\{m_1 \otimes_R ... \otimes_R m_i \otimes_R ... \otimes_R m_j \otimes_R ... \otimes_R m_p : x_i = x_j\}_{1 \leq i < j \leq p}$ Por tanto, ${T_0}/{N}$ está generado por $\{x_1 \wedge ... \wedge x_p$ tal que $x_i \in M\}$. Sin embargo, al igual que en el producto tensorial,

no todos los elementos en $\wedge^p M$ son de esta forma.
Se toma $\bigwedge^0 M = R$ para que el producto exterior esté definido para todo $p \in \mathbb{N}$. Además, notemos que $\bigwedge^1 M = M$ para cualquier R-módulo M.
Las bilinealidad (o multilinealidad) del producto (multi-)tensorial es heredada por el producto exterior, que además cuenta con un añadido: desarrollando el elemento $(m_1+m_2)\wedge(m_1+m_2)\wedge m_3\wedge...\wedge m_p = 0$ se ve que $m_1\wedge m_2\wedge...\wedge m_p = -(m_2\wedge m_1\wedge...\wedge m_p)$. De hecho, más en general, para cualquier permutación $\sigma \in \mathscr{S}_n$, $m_1 \wedge m_2 \wedge ... \wedge m_p = sgn(\sigma)(m_{\sigma(1)} \wedge m_{\sigma(2)} \wedge ... \wedge m_{\sigma(p)})$. El producto exterior es, entonces, anticonmutativo.

PROPOSICIÓN A.7.2. *Sean M, N R-módulos, $f : R \longrightarrow S$ un morfismo de anillos. Se tiene que*

i) El producto exterior conmuta con el producto tensorial: $\wedge^p(S \otimes_R M) = S \otimes_R \wedge^p M$.
ii) $\bigwedge^p(M \oplus N) \cong \bigoplus_{0\le i\le p}(\bigwedge^i M \otimes_R \bigwedge^{p-i} N)$.
iii) Si M es libre de rango finito con base $\{e_1, ..., e_n\}$, $\wedge^p M$ es libre de rango $\binom{n}{p}$ y el conjunto $\{e_{i_1} \wedge ... \wedge e_{i_p}, 1 \le i_1 < ... < i_p \le n\}$ es una base. En particular, $\wedge^n M \cong R$. Además, $\bigwedge^i M = 0$ para todo $i \in \mathbb{N}$ con $i > n$.

LEMA A.7.3. *Sean R un anillo noetheriano y P un R-módulo verificando: $P \oplus R^n \cong R^{n+1}$ para algún $n \in \mathbb{N}$. Entonces, $P \cong R$.*

DEMOSTRACIÓN. Como $P \oplus R^n \cong R^{n+1}$ es un R-módulo libre, P es un R-módulo proyectivo. En vista de la Proposición 2.9.1 y la Proposición A.4.1,

$$rank_R(P) = rank_{R_\mathfrak{p}}((R^{n+1})_\mathfrak{p}) - rank_{R_\mathfrak{p}}((R^n)_\mathfrak{p}) = rank_R(R^{n+1}) - rank_R(R^n) = 1,\ \forall \mathfrak{p} \in Spec(R).$$

Por tanto, $P_\mathfrak{p}$ es un $R_\mathfrak{p}$-módulo libre de rango 1 para todo $\mathfrak{p} \in Spec(R)$. En consecuencia, para cada $\mathfrak{p} \in Spec(R)$ e $i \in \mathbb{N}$ con $i > 1$, se tiene que:

$$(\bigwedge^i P)_\mathfrak{p} \cong R_\mathfrak{p} \otimes_R (\bigwedge^i P) \cong \bigwedge^i (R_\mathfrak{p} \otimes_R P) \cong \bigwedge^i P_\mathfrak{p} = 0,$$

donde la primera y tercera igualdad se siguen del Corolario A.6.4; y la segunda y cuarta igualdad se tienen por i) y iii) de la Proposición A.7.1 respectivamente. Ahora bien, por la Proposición A.10.10, la aplicación $\bigwedge^i P \longrightarrow \prod_\mathfrak{p}(\bigwedge^i P)_\mathfrak{p}$ es inyectiva. Luego debe ser $\bigwedge^i P = 0$ para todo $i \in \mathbb{N}, i > 1$. Entonces:

$$R \cong \bigwedge^{n+1} R^{n+1} \cong \bigwedge^{n+1}(P \oplus R^n) \cong \bigoplus_{0\le i\le n+1}(\bigwedge^i P \otimes_R \bigwedge^{n+1-i} R^n) \cong \bigwedge^1 P \otimes_R \bigwedge^n R^n \cong P \otimes_R R \cong P,$$

donde la tercera igualdad se tiene por ii) de la Proposición A.7.1 y la cuarta se sigue de que, para $i = 0$, $\bigwedge^{n+1} R^n = 0$ (cf. iii) de la Proposición A.7.1); de otro lado, para $i > 1$ se había visto que $\bigwedge^i P = 0$. □

A.8. Anillos y módulos Noetherianos. Lema de Nakayama

DEFINICIÓN 52. *Un R-módulo M se dice noetheriano si satisface cualquiera de las siguientes condiciones equivalentes:*

i) Cada submódulo de M es finitamente generado.
ii) Cada cadena ascendente numerable de submódulos $N_0 \subset ... \subset N_m \subset ...$ se estabiliza. Esto es, existe $n \in \mathbb{N}$ tal que $M_n = M_m$ para todo $m \ge n$ (c.c.a.).
iii) Todo conjunto no vacío de submódulos de M posee elemento maximal para la inclusión.

DEFINICIÓN 53. *Un anillo R se dice noetheriano si es noetheriano como R-módulo.*

Una propiedad que se deriva como consecuencia directa de la Proposición A.2.3 es la siguiente:

PROPOSICIÓN A.8.1. *Sea R un anillo noetheriano y $\mathfrak{p}$ un ideal primo de R, entonces $R_\mathfrak{p}$ es un anillo local noetheriano.*

Los módulos noetherianos se relacionan con las sucesiones exactas cortas de la siguiente manera:

PROPOSICIÓN A.8.2. *Sea $\mathbf{0} \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow \mathbf{0}$ una sucesión exacta corta de R-módulos, entonces M es noetheriano si y solamente si M' y M'' son noetherianos.*

COROLARIO A.8.3. *Sea M es un R-módulo y N un submódulo de M. Entonces M es noetheriano si y solamente si N y M/N son noetherianos. En particular, si R es un anillo noetheriano y $\mathfrak{a}$ es un ideal propio de R entonces $R/\mathfrak{a}$ es noetheriano.*

COROLARIO A.8.4. *Si $\{M_i\}_{1\leq i\leq n}$ es una familia de R-módulos noetherianos, $\bigoplus_{i=i}^{n} M_i$ es noetheriano.*

COROLARIO A.8.5. *Si R es un anillo noetheriano y M es un R-módulo finitamente generado, M es noetheriano.*

TEOREMA A.8.6 (**Hilbert Basissatz**). *Si R un anillo noetheriano, $R[X_1, ..., X_n]$ es un anillo noetheriano.*

COROLARIO A.8.7. *Si R es un anillo noetheriano, toda R-álgebra finitamente generada es noetheriana. Es decir, para cada $n \in \mathbb{N}$ y cada ideal $\mathfrak{a} \subseteq R[X_1, \ldots, X_n]$, si R es noetheriano también lo es la R-álgebra cociente $R[X_1, ..., X_n]/\mathfrak{a}$.*

DEFINICIÓN 54. *Sea R un anillo y $\mathfrak{a}$ un ideal de R. Se define el radical de $\mathfrak{a}$ y se denota $\sqrt{\mathfrak{a}}$ al ideal*

$$\sqrt{\mathfrak{a}} := \{a \in R :\ \exists n \in N,\ a^n \in \mathfrak{a}\}$$

En particular, si $\mathfrak{a} = (0)$, $\sqrt{\mathfrak{a}}$ se denomina nilradical de R y se denota $\mathfrak{n}(R)$.

DEFINICIÓN 55. *Sea R un anillo. El radical de Jacobson $\mathfrak{R}$ de R es la intersección de todos los ideales maximales de R.*

PROPOSICIÓN A.8.8. *Si R es un anillo noetheriano, cada ideal contiene una potencia de su radical.*

Aplicando la Proposición A.8.8 al ideal (0) se tiene:

COROLARIO A.8.9. *Si R es un anillo noetheriano el nilradical es nilpotente.*

PROPOSICIÓN A.8.10. *Sea M un R-módulo finitamente generado, $\mathfrak{a}$ un ideal de R y $\Phi \in Hom_R(M, M)$ un endomorfismo de M tal que $\Phi(M) \subseteq \mathfrak{a}M$. Entonces, Φ es la raíz de un polinomio mónico con coeficientes en $\mathfrak{a}$.*

COROLARIO A.8.11. *Sea M un R-módulo finitamente generado e $\mathfrak{a}$ un ideal de R que verficica $\mathfrak{a}M = M$. Entonces, existe $x \in 1 + \mathfrak{a}$ tal que $xM = 0$.*

PROPOSICIÓN A.8.12. *Sean M un R-módulo de generación finita y $\mathfrak{a}$ un ideal contenido en el radical de Jacobson $\mathfrak{R}$ de R. Si $\mathfrak{a}M = M$ entonces $M = 0$.*

COROLARIO A.8.13. *Sean M es un R-módulo de generación finita, N un submódulo de M y $\mathfrak{a} \in \mathfrak{R}$. Si $\mathfrak{a}M = M + N$, entonces $M = N$.*

LEMA A.8.14. *Si R es un anillo local y M, N son R-módulos finitamente generados distintos de cero, entonces $M \otimes_R N \neq 0$.*

PROPOSICIÓN A.8.15. *Si M y N son R-módulos finitamente generados, entonces*

$$Supp(M \otimes_R N) = Supp(M) \cap Supp(N).$$

A.9. Anillos y módulos Artinianos. Teorema de Jordan-Hölder

DEFINICIÓN 56. *Un R-módulo se dice artiniano si verifica cualquiera de las siguientes condiciones equivalentes:*

i) Toda cadena descendente numerable de submódulos $M_0 \subset M_1 \subset ... \subset M_m \subset ...$ se estabiliza. Esto es, existe $n \in \mathbb{N}$ tal que $M_n = M_m$ para todo $m \geq n$ (c.c.d.).
ii) Todo conjunto no vacío de M posee elemento minimal para la inclusión.

DEFINICIÓN 57. *Un anillo R se dice artiniano si lo es como R-módulo.*

PROPOSICIÓN A.9.1. *Sea $\mathbf{0} \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow \mathbf{0}$ una sucesión exacta corta de R-módulos, entonces M es artiniano si y solamente si M' y M'' son artinianos.*

COROLARIO A.9.2. *Si R un anillo artiniano y M un R-módulo finitamente generado, entonces M es artiniano.*

Corolario A.9.3. *Sea R un anillo tal que el ideal (0) se puede escribir como producto de ideales maximales $\mathfrak{m}_1 ... \mathfrak{m}_r$ (no necesariamente distintos). Entonces R es artiniano si y solamente si R es noetheriano*

Proposición A.9.4. *Sea R un anillo artiniano, entonces*

i) Cada ideal primo de R es maximal.
ii) El radical de Jacobson de R es un conjunto finito.
iii) El radical de Jacobson de R (que en virtud de i) coincide con la intersección de todos los ideales primos de R) es un ideal nilpotente.

Definición 58. *Se consideran las siguientes nociones:*

i) Un R-módulo M se dice simple si sus únicos submódulos son (0) y M.
ii) Una cadena estricta finita de submódulos de M es una cadena de submódulos $(0) \subsetneq M_1 \subsetneq ... \subsetneq M_n$. Se dice que esta cadena es de longitud n.
iii) Una serie de composición en un R-módulo es una cadena estricta finita $0 \subsetneq M_1 \subsetneq ... \subsetneq M_n = M$ tal que M_{i+1}/M_i para $1 \leq i \leq n$ son módulos simples. En este caso se dirá que esta serie tiene longitud n.
iv) La longitud de un R-módulo es el mínimo de las longitudes de sus series de composición, si posee alguna. En caso contrario se dice que M es de longitud infinita. Se denota por $\ell_R(M)$.

Proposición A.9.5. *Si M es un R-módulo artiniano y noetheriano, entonces posee una serie de composición (i.e. es de longitud finita).*

Teorema A.9.6 (**Jordan-Hölder**). *Si M es un R-módulo de longitud finita, entonces:*

i) Todas las series de composición de M tienen la misma longitud $\ell_R(M)$.
ii) Si $N \subsetneq M$, entonces $\ell_R(N) < \ell_R(M)$.
iii) Toda cadena finita estricta tiene longitud menor que $\ell_R(M)$.
iv) Un R-módulo M es de longitud finita si y solamente si M es noetheriano y artiniano.

Corolario A.9.7. *Si M es un R-módulo de longitud finita y N es un submódulo de M, entonces N es de longitud finita.*

Proposición A.9.8. *Sea $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow$ una sucesión exacta corta de R-módulos. Son equivalentes*

i) M' y M'' son de longitud finita.
ii) M es de longitud finita.

Además, si todos ellos son de longitud finita, $\ell_R(M') - \ell_R(M) + \ell_R(M'') = 0$.

Descomponiendo una sucesión exacta en sucesiones exactas cortas y aplicando repetidamente la Proposición anterior se tiene el siguiente corolario para sucesiones exactas de R-módulos de longitud finita:

Corolario A.9.9. *Sea $0 \longrightarrow M_0 \longrightarrow M_1 \longrightarrow \cdots \longrightarrow M_d \longrightarrow 0$ una sucesión exacta de R-módulos de longitud finita, entonces $\sum_{n=0}^{d}(-1)^n \ell_R(M_n) = 0$.*

Proposición A.9.10. *Si V es un k-espacio vectorial, las siguientes condiciones son equivalentes:*

i) V es de longitud finita (como k-módulo).
ii) V es de dimensión finita (como k-espacio vectorial).
iii) Condición de Cadena Ascendente (c.c.a.).
iv) Condición de Cadena Descendente (c.c.d.).

Además, si estas condiciones se dan, longitud=dimensión.

A.10. Descomposición Primaria. Teorema de Lasker-Noether. Teorema de Akizuki

Definición 59. *Sea M un R-módulo, N un submódulo de M y $a \in R$.*

i) El morfismo de R-módulos $a_M : M \longrightarrow M$ con $a_M(x) = ax$ se denomina homotecia por a.

ii) Se dice que N es un submódulo primario de M si $N \neq M$ y para cada $a \in R$, $a_{M/N}$ es inyectiva o nilpotente (i.e. existe $n \in \mathbb{N}$ tal que $a_{M/N} \circ \overset{n)}{\cdots} \circ a_{M/N}$ es la aplicación nula.

iii) Un ideal $\mathfrak{a}$ de R se dice primario si lo es como submódulo.

PROPOSICIÓN A.10.1. *Sea M un R-módulo y N un submódulo primario en M. El conjunto $\mathfrak{p} = \{a \in R : \ a_{M/N}$ no es inyectiva$\}$ es un ideal primo de R*

DEFINICIÓN 60. *Sea M un R-módulo y N un submódulo de M.*

i) El ideal $\mathfrak{p}$ descrito en A.10.1 se denomina ideal primo perteneciente a N en M. Y se dice que N es $\mathfrak{p}$-primario.

ii) Una descomposición de la forma $N = N_1 \cap \cdots \cap N_r$ donde $\{N_i\}_{1\leq i\leq r}$ es una familia de submódulos primarios en M se denomina descomposición primaria de N. Esta descomposición se dice irredundante si N no puede expresarse como intersección de un subconjunto propio de $\{N_i\}_{1\leq i\leq r}$ y $\mathfrak{p}_i \neq \mathfrak{p}_j$ si $i \neq j$ para todo $1 \leq i, j \leq r$ donde $\mathfrak{p}_i$ es el ideal primo perteneciente a N_i.

DEFINICIÓN 61. *Sea M un R-módulo. Un submódulo N de M se dice irreducible si $N \neq M$ y N no se puede escribir como $N = N_1 \cap N_2$ con $N_1, N_2 \subsetneq N$.*

TEOREMA A.10.2 (**Lasker-Noether**). *Todo submódulo propio de un R-módulo noetheriano posee una descomposición primaria irredundante.*

La demostración de este Teorema se realiza viendo que para un R-módulo M se tiene que:

- Si M es noetheriano, todo submódulo propio de M se puede escribir como intersección finita de submódulos irreducibles y cada submódulo irreducible es primario.
- La intersección de una familia finita de submódulos $\mathfrak{p}$-primarios de M es un submódulo $\mathfrak{p}$-primario.

DEFINICIÓN 62. *Sea M un R-módulo:*

i) Dado un subconjunto $S \subseteq M$ se define $Ann_R(S) := \{a \in R : \ as = 0 \ \forall s \in S\}$.

ii) Un ideal primo $\mathfrak{p}$ de R se dice asociado a M si existe $x \in M$ tal que $\mathfrak{p} = Ann_R(x)$.

iii) El conjunto de todos los ideales primos asociados a M se escribe $Ass_R(M)$.

iv) Dado un R-módulo M, se define el soporte de M y se denota $Supp(M)$ como el conjunto de localizados de M distintos de cero. Esto es,

$$Supp(M) = \{\mathfrak{p} \in R : \ M_{\mathfrak{p}} \neq 0\}.$$

OBSERVACIÓN 17. *Dado un R-módulo M, una caracterización útil de $Ass_R(M)$ también utilizada como forma alternativa para definir este conjunto es la siguiente:*
Si $\mathfrak{p}$ es un ideal primo de R, entonces $\mathfrak{p} \in Ass_R(M)$ si y solamente si $R/\mathfrak{p} \longrightarrow M$ es un morfismo inyectivo de R-módulos.

El siguiente Teorema es conocido como Primer Teorema de Unicidad y tendrá relevancia en la prueba de propiedades que establecen relaciones entre el soporte y el conjunto de primos asociados de un R-módulo.

TEOREMA A.10.3 (**Primer Teorema de Unicidad**). *Sea R un anillo noetheriano, M un R-módulo finitamente generado, $(0) = N_1 \cap \cdots \cap N_r$ una descomposición primaria irredundante de (0) y N_i submódulos $\mathfrak{p}_i$-primarios con $1 \leq i \leq r$. Entonces, $Ass_R(M) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$. En particular, $Ass(M)$ es finito y $Ass(M) = 0$ si y solamente si $M = 0$.*

COROLARIO A.10.4. *Sea R un anillo noetheriano, M un R-módulo y N un submódulo de N finitamente generado con descomposición primaria irredundante $N = N_1 \cap \cdots \cap N_r$. Entonces, $Ass_R(M/N) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ donde $\mathfrak{p}_i$ es el ideal primo perteneciente a N_i con $1 \leq i \leq r$. En particular, el conjunto $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ no depende de la descomposición.*

El Primer Teorema de Unicidad nos da, además, una manera alternativa de expresar el conjunto de divisores de cero de un R-módulo finitamente generado cuando R es noetheriano:

PROPOSICIÓN A.10.5. *Sea R un anillo noetheriano y M un R-módulo finitamente generado. Entonces, el conjunto de divisores de cero de M se puede expresar como*

$$\bigcup_{\mathfrak{p}\in Ass_R(M)} \mathfrak{p}.$$

Una caracterización muy usada del nilradical de un anillo y que se utilizará frecuentemente en lo que sigue es:

Proposición A.10.6. *Sea R un anillo, entonces*

$$\mathfrak{n}(R) = \bigcap_{\mathfrak{p}\in Spec(R)} \mathfrak{p}.$$

Notemos que para un anillo R y un ideal $\mathfrak{a} \subset R$ se tiene que $\sqrt{\mathfrak{a}} = \mathfrak{n}(R/\mathfrak{a})$. Por otra parte, los ideales primos de $R/\mathfrak{a}$ se pueden identificar con ideales primos de R que contienen a $\mathfrak{a}$. Aplicanco la Proposición anterior al anillo $R/\mathfrak{a}$ se tiene:

Corolario A.10.7. *Sea R un anillo y $\mathfrak{a}$ un ideal de R, entonces*

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p}\in Spec(R),\, \mathfrak{p}\supset\mathfrak{a}} \mathfrak{p}.$$

Además, el Teorema A.10.3 proporciona una forma distinta de expresar el radical del anulador de un R-módulo M en términos del conjunto de sus ideales primos asociados:

Corolario A.10.8. *Sea R un anillo noetheriano M y un R-módulo finitamente generado entonces*

$$\sqrt{Ann_R(M)} = \bigcap_{\mathfrak{p}\in Ass_R(M)} \mathfrak{p}.$$

Ahora, observando que $Ann_R(R) = (0)$ y $\sqrt{0} = \mathfrak{n}(R)$, en virtud del Corolario A.10.8 se deduce el siguiente resultado:

Corolario A.10.9. *Si R es un anillo noetheriano entonces,*

$$n(R) = \bigcap_{\mathfrak{p}\in Ass_R(R)} \mathfrak{p}.$$

Proposición A.10.10. *Sea M un R-módulo. Entonces el morfismo de R-módulos $M \longrightarrow \prod_{\mathfrak{p}\in Spec(R)} M_{\mathfrak{p}}$ inducido por los morfismos canónicos $M \longrightarrow M_{\mathfrak{p}}$ es inyectivo.*

Proposición A.10.11. *Sea R un anillo noetheriano y M un R-módulo finitamente generado. Para cada ideal $\mathfrak{p} \in Spec(R)$ las siguientes afirmaciones son equivalentes:*

i) $\mathfrak{p} \in Supp(M)$.
ii) *Existe* $\mathfrak{p}' \in Ass_R(M)$ *tal que* $\mathfrak{p} \supset \mathfrak{p}'$.
iii) $\mathfrak{p} \supset Ann_R(M)$.

Corolario A.10.12. *Si R es un anillo noetheriano y M es un R-módulo finitamente generado se tiene que $Ass_R(M) \subset Supp(M)$. Además, los primos minimales de $Ass_R(M)$ y $Supp(M)$ coinciden.*

El Primer Teorema de Unicidad (cf. Teorema A.10.3) sirve también como herramienta para probar los siguientes resultados:

Proposición A.10.13. *Sea R un anillo noetheriano y M un R-módulo finitamente generado, entonces M es de longitud finita si y solamente si cada $\mathfrak{p} \in Supp(M)$ es un ideal maximal.*

Teorema A.10.14 (**Akizuki**). *Un anillo R es artiniano si y solamente si R es noetheriano y todo ideal primo $\mathfrak{p}$ de R es maximal.*

Corolario A.10.15. *Todo anillo artiniano es noetheriano.*

Corolario A.10.16. *Si R es un anillo artiniano y M es un R-módulo finitamente generado, entonces R es de longitud finita (como R-módulo) y M es de longitud finita.*

A.11. El Lema de Artin-Rees

Definición 63. *Sean (R, Σ) y (M, Σ') anillo y R-módulo filtrado respectivamente. Dado un ideal $\mathfrak{a} \in R$ se dice que una filtración Σ' es compatible con $\mathfrak{a}$ si $\mathfrak{a}M^n \subseteq M^{n+1}$ para todo $n \in \mathbb{N}$. Se dice que la filtración Σ' es $\mathfrak{a}$-estable si existe $n_0 \in \mathbb{N}$ tal que $\mathfrak{a}M^m = M^{m+1}$ para todo $m \geq n_0$.*

Observación 18. *Sea R es un anillo, $\mathfrak{a} \subset R$ un ideal, M un R-módulo y N un submódulo de M. Entonces,*

i) Si una filtración Σ' sobre M es compatible con $\mathfrak{a}$ se tiene, en virtud de la Observación 1, que la filtración Σ'' inducida en N por Σ' es también compatible con $\mathfrak{a}$.

ii) La filtración $\mathfrak{a}$-ádica sobre M es un claro ejemplo de filtración $\mathfrak{a}$-estable.

Dados un anillo R y un ideal $\mathfrak{a} \subset R$, se puede definir el conjunto $\overline{R} := R \oplus \mathfrak{a} \oplus \mathfrak{a}^2 \oplus \ldots$ al que se puede dotar de estructura de anillo graduado mediante las operaciones que inducen la suma y el producto de R. Dados $a, b \in \overline{R}$, existen conjuntos finitos $I, J \subseteq \mathbb{N}$ y conjuntos finitos de elementos homogéneos $\{a_i \in \mathfrak{a}^i : i \in I\}$, $\{b_j \in \mathfrak{a}^j : j \in J\}$ tales que:

$$a = \sum_{i \in I} a_i, \;\; b = \sum_{j \in J} b_j.$$

Ahora, consideramos el conjunto $I \cup J$. Añadiendo $a_k = 0$ para $k \in I \cup J \setminus I$ y $b_k = 0$ para $k \in I \cup J \setminus J$, dado que $I \cup J$ es finito, podemos definir la suma de a y b mediante la siguiente identidad:

$$a + b := \sum_{k \in I \cup J} (a_k + b_k),$$

Dado que $\overline{R}$ es suma directa de subgrupos $\{\mathfrak{a}^i : i \in \mathbb{N}\}$, esta definición es única y $a_k + b_k \in \mathfrak{a}^k$ es claramente un elemento homogéneo de grado k en $\overline{R}$. De modo similar, usando las mismas presentaciones de a y b podemos definir el producto:

$$a \cdot b := \sum_{i \in I, j \in J} a_i \cdot b_j.$$

De nuevo, la naturaleza de $\overline{R}$ como suma directa de sus subgrupos nos garantiza la buena definición del producto, donde el producto natural $\mathfrak{a}^n \times \mathfrak{a}^m \longrightarrow \mathfrak{a}^{m+n}$, nos indica que $a_i \cdot b_j$ es un elemento homogéneo de grado $i + j$ de $\overline{R}$.
De manera similar, consideremos un anillo R un ideal $\mathfrak{a} \subseteq R$ y un R-módulo M. Como en la definición, consideremos el anillo $\overline{R} = R \oplus \mathfrak{a} \oplus \cdots$ y el grupo abeliano $\overline{M} := M \oplus \mathfrak{a}M \oplus \mathfrak{a}^2 M \cdots$ Sobre M podemos, de manera natural, inducir una estructura de $\overline{R}$-módulo, mediante la siguiente operación:

$$(\sum_{i \in I} a_i) \cdot (\sum_{j \in J} m_j) := \sum_{i,j} a_i \cdot m_j, \qquad a_i \in \mathfrak{a}^i, \; m_j \in \mathfrak{a}^i M,$$

siendo los argumentos elementales los esperados.

Lema A.11.1. *Sea $\mathfrak{a}$ un ideal de R, M un R-módulo con una filtración $\Sigma' = \{M_0 \supseteq M_1 \supseteq ...\}$ compatible con $\mathfrak{a}$. Entonces, $\overline{M}$ es finitamente generado como $\overline{R}$-módulo si y solamente sí Σ' es $\mathfrak{a}$-estable.*

Demostración. Por una parte, si $\overline{M}$ es finitamente generado, existen $\{t_1, ..., t_r\}$ que lo generan, con $t_i = \sum_{j=1}^{k_i} t_{i,j}$, donde $t_{i,j} \in M_{j_i}$. Para cada i con $1 \leq i \leq r$ se define $n_i = max_j\{j_i\}$ y $n = max_{1 \leq i \leq r}\{n_i\}$. Entonces, $t_i \in M_0 \oplus ... \oplus M_n$ para todo i con $0 \leq 1 \leq r$ y, en consecuencia, $M_0 \oplus ... \oplus M_n$ genera a $\overline{M}$ como $\overline{R}$-módulo. Veamos que $\mathfrak{a}M_m = M_{m+1}$ para todo $m \geq n$. Por una parte, se tiene que, como Σ' es compatible con $\mathfrak{a}$, $\mathfrak{a}M_m \subseteq M_{m+1}$. Sea, ahora, $x \in M_{m+1} \subset \overline{M}$ un elemento homogéneo de grado $m+1$. Entonces, x se puede expresar como una combinación lineal del sistema generador ya fijado. Es decir, existe un subconjunto $\{x_1, \ldots, x_t\} \subseteq \{t_{i,j} : \; 1 \leq i \leq r, \; 1 \leq j \leq k_i\}$ y existen $\{a_1, \ldots, a_t\} \subseteq \overline{R}$ de tal modo que:

- $x_i \in M_{d_i}$ es un elemento homogéneo de grado $d_i \leq n$
- $a_i \in \mathfrak{a}^{m+1-d_i}$, es un elemento homogéneo de grado $m + 1 - d_i$
- $x = \sum_{i=1}^t a_i.x_i$.

Ahora, en virtud de la definición del producto de ideales, cada a_i puede verse como $a_i = \sum_j b_{i,j} c_{i,j}$ con $b_{i,j} \in \mathfrak{a}$ y $c_{i,j} \in \mathfrak{a}^{m-d_i}$. Entonces, $x = \sum_{i,j} b_{i,j}(c_{i,j} x_i)$ con $c_{i,j} x_i \in \mathfrak{a}^{m-d_i} M_{d_i} \subseteq M_m$ y por tanto se tiene $\mathfrak{a}M_m = M_{m+1}$.
Recíprocamente, supongamos que la filtración Σ' es $\mathfrak{a}$-estable. Entonces existe $n \in \mathbb{N}$ con $\mathfrak{a}M_m = M_{m+1}$ para todo $m \geq n$. Aplicando esta relación de manera recursiva se observa que para cualquier $m \in \mathbb{N}$, $m \geq n$ se tiene que $M_m = \mathfrak{a}^{m-n} M_n$. Como $\mathfrak{a}^{m-n} \subseteq R$, M_n genera M_m

como R-módulo para todo $m \geq n$. En consecuencia, $M_0 \oplus ... \oplus M_n$ genera $\overline{M}$ como R-módulo y por tanto, también como $\overline{R}$-módulo. Considérese ahora el R-módulo $M_0 \oplus ... \oplus M_n$. Sea i con $0 \leq i \leq n$. Como $M = M_0$ es noetheriano y $M_i \subseteq M$ es un submódulo de M, se tiene que M_i es finitamente generado como R-módulo. Es decir, existe un conjunto $F_i \subseteq M_i$ finito de manera que $M_i = R < F_i >$. Sea $x \in M_0 \oplus \ldots M_n$. Entonces $x = \sum_{i=0}^{n} x_i$ donde $x_i \in M_i$ es un elemento homogéneo de grado i. Como M_i está generado por F_i como submódulo, existen conjuntos finitos $\{f_{i,k}\}_{k\in K}$, $\{r_{i,k}\}_{k\in K}$ donde $K \subseteq \mathbb{N}$ es un conjunto finito tal que $x_i = \sum_{k\in K}(r_{i,k}) \cdot (f_{i,k})$. Por consiguiente, se tiene

$$x = \sum_{i=0}^{n} x_i = \sum_{0\leq i\leq n,\ k\in K} (r_{i,k}) \cdot (f_{i,k}).$$

En consecuencia se tiene que $M_0 \oplus \cdots \oplus M_n$ está generado como R-módulo por $F := \bigcup_{i\in I} F_i$, que es un conjunto finito por se unión finita de conjuntos finitos. Por tanto, $M_0 \oplus \cdots \oplus M_n = R < F >$ y $M_0 \oplus \cdots \oplus M_n$ es finitamente generado como R-módulo. Como R puede verse como un submódulo de $\overline{R}$ mediante la inclusión canónica $R \hookrightarrow \overline{R} = R \oplus \mathfrak{a} \oplus \mathfrak{a}^2 \ldots$, se tiene que $M_0 \oplus \cdots \oplus M_n = \overline{R} < F >$. Pero como $\overline{M}$ estaba generado por $M_0 \oplus \cdots \oplus M_n$ como $\overline{R}$-módulo, se tiene que $\overline{M} = \overline{R} < F >$ es finitamente generado como $\overline{R}$-módulo. □

Seguidamente enunciamos un resultado técnico de gran utilidad, encontrado, al menos por E. Artin y D. Rees.

Teorema A.11.2 (**Lema de Artin-Rees**). *Sea R un anillo noetheriano, $\mathfrak{a}$ un ideal de R, M un R-módulo finitamente generado y N un submódulo de M. Entonces, dada una filtración $\mathfrak{a}$-estable Σ' sobre M, la filtración $\Sigma'' = \{N \cap M_n : n \in \mathbb{N}\}$ inducida sobre N es $\mathfrak{a}$-estable.*

Demostración. Supongamos que $\Sigma' = \{M = M_0 \supseteq M_1 \supseteq ...\}$ es una filtración $\mathfrak{a}$-estable sobre M y sea $\Sigma'' = \{N = M_0 \cap N \supseteq M_1 \cap N \supseteq \ldots\}$ la filtración inducida por Σ sobre N. Consideremos los graduados:

- $\overline{R} = R \oplus \mathfrak{a} \oplus \mathfrak{a}^2 \oplus \ldots$
- $\overline{M} = M \oplus M_1 \oplus \mathbb{M}_2 \oplus \ldots$
- $\overline{N} = N \oplus (M_1 \cap N) \oplus (M_2 \cap N) \oplus \ldots$

Observamos que, como Σ' es una filtración $\mathfrak{a}$-compatible en M, entonces la filtración Σ'' en $\mathfrak{a}$-compatible en N. Es decir, dado que $\mathfrak{a}M_m \subseteq M_{m+1}$, tenemos que

$$\mathfrak{a}(N \cap M_m) \subseteq \mathfrak{a}N \cap \mathfrak{a}M_m \subseteq N \cap (\mathfrak{a}M_m) \subseteq N \cap M_{m+1},$$

donde hemos usado que $\mathfrak{a}N \subseteq N$ por ser N un submódulo de M. Por tanto, al ser Σ'' una filtración $\mathfrak{a}$-estable sobre M, se tiene que $\overline{N}$ es un $\overline{R}$-módulo con las operaciones descritas anteriormente.

De otro lado, tenemos las inclusiones canónicas entre las componentes homogéneas de $\overline{N}$ y $\overline{M}$. Es decir, los monomorfismos:

$$i_n : N \cap M_m \hookrightarrow M_m,$$

donde $i_0 : N \hookrightarrow M$ es la inclusión natural. Estos monomorfismos inducen un monomorfismo graduado entre las respectivas sumas directas

$$i := \bigoplus_{n\in\mathbb{N}} i_n : \overline{N} = \bigoplus_{n\in\mathbb{N}}(N \cap M_n) \hookrightarrow \overline{M} = \bigoplus_{n\in\mathbb{N}} M_n.$$

Como i es momomorfismo de $\overline{R}$-módulos, podemos identificar $\overline{N}$ con un submódulo de $\overline{M}$.

Observemos ahora que $\overline{R} = R \oplus \mathfrak{a} \oplus \mathfrak{a}^2 \oplus \ldots$ es un R-álgebra generada por los elementos de $\mathfrak{a}$, es decir, por los elementos homogéneos de grado 1. Si R es anillo noetheriano, $\mathfrak{a}$ es un ideal finitamente generado y, por tanto, un R-módulo finitamente generado. Estamos así en las hipótesis del apartado *ii*) de la Proposición 1.2.3: $\overline{R}$ es un anillo graduado y una R-álgebra generada por un número finito de elementos homogéneos de grado 1. En particular, existe $t \in \mathbb{N}$ y un ideal $\mathfrak{b}$ en $R[X_1, \ldots X_t]$ tales que

$$\overline{R} \cong R[X_1, \ldots, X_t]/\mathfrak{b}.$$

Luego $\overline{R}$ es un anillo noetheriano. Por el Lema 1.3.1 precedente, como $\overline{R}$ es noetheriano y la filtración Σ es $\mathfrak{a}$-estable, entonces $\overline{M}$ es un $\overline{R}$-módulo finitamente generado. Por el Corolario A.8.5, $\overline{M}$ es un $\overline{R}$-módulo noetheriano. Por tanto, todos los submódulos de $\overline{M}$ son finitamente generados y, en particular, $\overline{N}$ es un $\overline{R}$-módulo finitamnete generado. Aplicando de nuevo el Lema 1.3.1, inducimos que la filtración Σ'' es $\mathfrak{a}$-estable en N. $\square$

COROLARIO A.11.3. *Sean R un anillo noetheriano, $\mathfrak{a}$ ideal de R, M un R-módulo finitamente generado y N un submódulo de M. Entonces existe $n \in \mathbb{N}$ tal que $\mathfrak{a}(\mathfrak{a}^m M \cap N) = \mathfrak{a}^{m+1} M \cap N$ para todo $m \geq n$.*

DEMOSTRACIÓN. Consideremos las filtraciones $\mathfrak{a}$-ádicas en R y M: $\Sigma_{\mathfrak{a}}(R)$ y $\Sigma_{\mathfrak{a}}(M)$. Como $\Sigma_{\mathfrak{a}}(M)$ es $\mathfrak{a}$-estable, por el Teorema 1.3.2 precedente, la filtración $\{M \cap N \supseteq M_1 \cap N \supseteq ...\}$ es $\mathfrak{a}$-estable en N. Es decir, existe $n \in \mathbb{N}$ tal que $\mathfrak{a}(\mathfrak{a}^m \cap N) = \mathfrak{a}^{m+1} M \cap N$ para todo $m \geq n$. $\square$

A continuación presentamos un enunciado del clásico Teorema de la Intersección de Krull de W. Krull que, entre otras cosas, establece que la topología $\mathfrak{a}$-ádica es metrizable en el caso de los módulos finitamente geenrados sobre anillos noetherianos.

TEOREMA A.11.4 (**Teorema de la Intersección de Krull**). *Sean R un anillo noetheriano, $\mathfrak{a}$ un ideal de R y M un R-módulo finitamente generado. Entonces,*

i) Si $N := \bigcap_{n \in \mathbb{N}} \mathfrak{a}^n M$, $\mathfrak{a}N = N$.

ii) Si $\mathfrak{a}$ está contenido en el radical de Jacobson de R,

$$\bigcap_{n \in \mathbb{N}} \mathfrak{a}^n M = (0)$$

y la topología definida por la filtración $\mathfrak{a}$-ádica sobre M es Hausdorff y metrizable.

iii) Si R es dominio noetheriano, para cada ideal propio $\mathfrak{a}$ de R se tiene:

$$\bigcap_{n \in \mathbb{N}} \mathfrak{a}^n = (0)$$

y la topología $\mathfrak{a}$-ádica sobre R es Hausdorff y metrizable.

DEMOSTRACIÓN. i) Aplicando el Corolario 1.3.3 al submódulo de M dado mediante

$$N := \bigcap_{n \in \mathbb{N}} \mathfrak{a}^n M,$$

existirá $n_0 \in \mathbb{N}$ tal que para cada $m \in \mathbb{N}$, $m \geq n_0$, $\mathfrak{a}(\mathfrak{a}^m M \cap N)) = \mathfrak{a}^{m+1} M \cap N$. Dado que $\mathfrak{a}N \subseteq N$, probemos el otro contenido. Supongamos que $x \in N$. Por tanto, $x \in \mathfrak{a}^n M$ para cada $n \in \mathbb{N}$. En particular, $x \in \mathfrak{a}^{n_0+1} \cap N = \mathfrak{a}(\mathfrak{a}^{n_0} M \cap N)$. Como $\mathfrak{a}^{n_0} M \cap N \subseteq N$, concluimos que $x \in \mathfrak{a}(\mathfrak{a}^{n_0} M \cap N) \subseteq \mathfrak{a}N$ y habremos probado el otro contenido.

ii) Como R es noetheriano y M es un R-módulo finitamente generado, M es un R-módulo noetheriano (cf. Corolario A.8.5). Como N es submódulo de M, entonces N es un R-módulo finitamente generado. Por el Lema de Nakayama (cf. Corolario A.8.13), si $\mathfrak{a}$ es un ideal contenido en el radical de Jacobson, entonces $\mathfrak{a}N = N$ implica $N = 0$. Así, ii) es una consecuencia inmediata de lo probado en i). El resto de las afirmaciones se siguen de la Proposición 1.2.12.

iii) Sea $\mathfrak{b} := \bigcap_{n \in \mathbb{N}} \mathfrak{a}^n$ ideal de R. Por la afirmación i) precedente, tenemos que $\mathfrak{a}\mathfrak{b} = \mathfrak{b}$. Entonces, por el Corolario A.8.11 concluimos que existe $x \in 1 + \mathfrak{b}$ tal que $x\mathfrak{b} = 0$. Escribimos $x = 1 + y$, con $y \in \mathfrak{b}$. Necesariamente, $y \neq 0$ porque, en otro caso, tendríamos $(1 + y).1 = (1 + 0)1 = 1 = 0$, que no se da en anillos conmutativos con unidad. De otro lado, $1 + y \neq 0$, pues si $1 + y = 0$, entonces $1 \in \mathfrak{b} \subseteq \mathfrak{a}$ y estaríamos en contradicción con la hipótesis de que $\mathfrak{a} \nsubseteq R$ es un ideal propio. Ahora, si $\mathfrak{b} \neq (0)$, existirá $z \in \mathfrak{b} \setminus \{0\}$ y se ha de verificar $(1+y)z = 0$. Pero hemos visto que $1+y \neq 0$ y hemos supuesto $z \neq 0$, por lo tanto concluiríamos que R tiene divisores de cero no nulos, lo que contradice la hipótesis de que R es dominio de integridad. En conclusión, no puede existir un elemento no nulo $z \in \mathfrak{b} \setminus \{0\}$ y, en consecuencia, se tiene que $\mathfrak{b} = (0)$. El resto de las afirmaciones se siguen de la Proposición 1.2.12. $\square$

COROLARIO A.11.5. *Sea R es un anillo noetheriano y $\mathfrak{a}$ es un ideal de R contenido en el radical de Jacobson. Entonces, si el anillo graduado $G_{\mathfrak{a}}(R)$ asociado a la filtración $\mathfrak{a}$-ádica sobre R es dominio, también lo es R.*

DEMOSTRACIÓN. Sean $x, y \in R$, $x, y \neq 0$. Veamos que $xy \neq 0$. Por el apartado *ii)* del Teorema precedente 1.3.4, $\bigcap_{n\in\mathbb{N}} \mathfrak{a}^n = (0)$. Por tanto, existen $m, n \in \mathbb{N}$ con $x \in \mathfrak{a}^m$, $x \notin \mathfrak{a}^{m+1}$; $y \in \mathfrak{a}^n$, $y \notin \mathfrak{a}^{n+1}$. Ahora, sean $\overline{x}$, $\overline{y}$ las clases de x e y módulo $\mathfrak{a}^m/\mathfrak{a}^{m+1}$ y $\mathfrak{a}^n/\mathfrak{a}^{n+1}$ respectivamente. Como $G_{\mathfrak{a}}(R)$ es dominio, $\overline{x}\,\overline{y} = \overline{xy} \neq 0$, lo que implica que $xy \neq 0$. $\square$

APÉNDICE B

Resultados Técnicos de Álgebra Homológica

B.1. Elementos del Álgebra Homológica

DEFINICIÓN 64. *Sea R un anillo y $\mathcal{M} := \{M_n : n \in \mathbb{Z}\}$ una familia numerable de R-módulos.*

i) Un complejo de cadena con soporte $\mathcal{M}$ es un par $\{\mathcal{M}, \mathcal{D}\}$ donde $\mathcal{D} = \{d_n : n \in Z\}$ es una familia numerable de morfismos $d_n \in Hom_R(M_n, M_{n-1})$ de tal modo que $d_{n-1} \circ d_n = 0$.

ii) Un complejo de co-cadena con soporte $\mathcal{M}$ es un par $(\mathcal{M}, \mathcal{C})$ donde $\mathcal{C} = \{c^n : n \in \mathbb{Z}\}$ es una familia numerable de morfismos $c^n \in Hom_R(M_n, M_{n+1})$ de tal forma que $c^{n+1} \circ c_n = 0$

Los complejos de cadena y co-cadena se representan usualmente mediante:

(B.1.1) C. cadena $\underline{M}$ $\quad \ldots \xrightarrow{d_{n+1}} M_n \xrightarrow{d_n} M_{n-1} \xrightarrow{d_{n-1}} M_{n-2} \xrightarrow{d_{n-2}} \ldots$

(B.1.2) C. co-cadena $\overline{M}$ $\quad \ldots \xrightarrow{c^{n-1}} M^n \xrightarrow{c_n} M^{n+1} \xrightarrow{c^{n+1}} M^{n+2} \xrightarrow{c^{n+2}} \ldots$

A priori no parece que haya gran diferencia entre las nociones salvo los índices ascendentes o descendentes de las relaciones. Sin embargo, tendrán roles diferentes en cuanto sigue. Una forma de ver cómo surgen los complejos de co-cadena pasa por dualizar los complejos de cadena. Así, supongamos dado un complejo de cadena como el descrito en (B.1.1). Podemos dualizar mediante el functor contravariante $Hom_R(-, R)$ (cf. Sección A.3 del Apéndice A). Así, definimos los R-módulos N^n como los duales de los R-módulos M_n (i.e. $N^n := Hom_(M_n, R))$ y los morfismos c^{n-1} como $Hom_R(d_n, R) : N^{n-1} \longrightarrow N^n$. Claramente, por el carácter functorial de $Hom_R(-, R)$ tenemos un complejo de co-cadena en (B.1.2).

i) Dado un complejo de cadena como (B.1.1), al índice del R-módulo M_n se le llama *grado*. Los elementos de $ker(d_n)$ denominan *ciclos de grado n*, mientras que a los elementos de $Im(d_{n+1})$ se les denomina *bordes de grado n* del complejo. El *n-ésimo módulo de homología* se define como el R-módulo cociente:

$$H_n(\underline{M}) = {}^{ker(d_n)}/_{Im(d_{n+1})}.$$

ii) Igualmente, para un complejo de co-cadena como (B.1.2), los elementos de $ker(c^n)$ se denominan *co-ciclos de grado n*; los elementos de $= Im(c^{n-1})$ se denominan *co-bordes de grado n* y al R-módulo cociente siguiente se le denomina *n-ésimo módulo de co-homología*:

$$H^n(\overline{M} = {}^{ker(c^n)}/_{Im(c^{n-1})}.$$

Un complejo de cadena (respectivamente co-cadena) de R-módulos $\underline{M}$ (resp. $\overline{M}$) es una sucesión exacta de R-módulos si y solamente si todos sus módulos de homología (resp. co-homología) son nulos.

DEFINICIÓN 65. *Sean $\underline{M}, \underline{N}$ dos complejos de cadena de R-módulos, un morfismo de complejos de R-módulos o aplicación de cadena $f : \underline{M} \longrightarrow \underline{N}$ es una familia de morfismos de R-módulos $\{f_n : M_n \longrightarrow N_n\}_{n\in\mathbb{Z}}$ de forma que $f_{n-1} \circ d_n = d'_n \circ f_n$ para cada $n \in \mathbb{Z}$. Es decir, de forma que los siguiente diagramas conmuten para todo $n \in \mathbb{Z}$:*

(B.1.3)
$$\begin{array}{ccc} M_n & \xrightarrow{f_n} & N_n \\ \downarrow{\scriptstyle d_n} & & \downarrow{\scriptstyle d'_n} \\ M_{n-1} & \xrightarrow{f_{n-1}} & N_{n-1} \end{array}$$

Proposición B.1.1. *Sean $\underline{M}$ y $\underline{N}$ dos complejos de cadena de R-módulos y $f : \underline{M} \longrightarrow \underline{N}$ una aplicación de cadena. Entonces, para cada $n \in \mathbb{N}$, $f_n : M_n \longrightarrow N_n$ induce un morfismo de R-módulos:*

$$\begin{array}{cccc} H_n(f): & H_n(\underline{M}) & \longrightarrow & H_n(\underline{N}) \\ & x + Im(d_{n+1}) & \mapsto & f_n(x) + Im(d'_{n+1}). \end{array}$$

Demostración. Veamos que $H_n(f)$ está bien definido. Por una parte, si $x \in f(ker(d_n))$, existe $x' \in ker(d_n)$ tal que $f(x') = x$. Como f es una aplicación de cadena, el Diagrama (B.1.3) es conmutativo y se tiene que $d'_n(x) = (d'_n \circ f_n)(x') = (f_{n-1} \circ d_n)(x') = f_{n-1}(d_n(x')) = f_{n-1}(0) = 0$. En consecuencia, $f(ker(d_n)) \subseteq ker(d'_n)$. Por otra parte, si $x \in f_n(Im(d_{n+1}))$, existe $x' \in Im(d_{n+1})$ tal que $f(x') = x$. Además, $x' = d_{n+1}(y)$ para algún $y \in M_{n+1}$. Como f es una aplicación de cadena, $d'_{n+1}(f_{n+1}(y)) = (d'_{n+1} \circ f_{n+1})(y) = (f_n \circ d_{n+1})(y) = f_n(x') = x$. En consecuencia, $x \in Im(d'_{n+1})$. Finalmente, las propiedades de linealidad de $H_n(f)$ se derivan de las del morfismo f_n. □

Definición 66. *Sean $\overline{M}$, $\overline{N}$ dos complejos de co-cadena. Una aplicación de co-cadena $f : \overline{M} \longrightarrow \overline{N}$ es una una familia de morfismos de R-módulos $\{f^n : M^n \longrightarrow N^n\}_{n\in\mathbb{Z}}$ tales que los diagramas siguientes conmuten para todo $n \in \mathbb{Z}$:*

$$\begin{array}{ccc} M^n & \xrightarrow{f^n} & N^n \\ \big\downarrow{\scriptstyle c^n} & & \big\downarrow{\scriptstyle c'^n} \\ M^{n+1} & \xrightarrow{f^{n+1}} & N^{n+1} \end{array}$$

Observación 19. *Los módulos de homología y co-homología tienen un caracter functorial sobre los morfismos de cadena y co-cadena. Es claro que $H_n(Id_{M_n}) = Id_{H_n}$ (resp. $H^n(Id) = Id_{H^n}$) y dados $f : \underline{M} \longrightarrow \underline{N}$, $g : \underline{N} \longrightarrow \underline{P}$ dos morfismos de cadena, $H_n(g \circ f) = H_n(g) \circ H_n(f)$ y similarmente pasa con los morfismos de co-cadena.*

Definición 67 (**Functor exacto**). *Sea F es un functor de la categoría de R-módulos en sí misma.*

i) Si F es covariante, se dice exacto a izquierda (resp. a derecha) si para cada s.e.c. $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$, la siguiente es una sucesión exacta:

$$0 \longrightarrow F(M') \longrightarrow F(M) \longrightarrow F(M'').$$

(Resp. si la sucesión $F(M') \longrightarrow F(M) \longrightarrow F(M'') \longrightarrow 0$ es exacta).

ii) Si F es contravariante, se dice que F es exacto a izquierda (resp. a derecha) si para cada s.e.c. $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$, la siguiente es una sucesión exacta:

$$0 \longrightarrow F(M'') \longrightarrow F(M) \longrightarrow F(M').$$

(Resp. si la sucesión $F(M'') \longrightarrow F(M) \longrightarrow F(M') \longrightarrow 0$ es exacta).

Un functor se dice exacto si es exacto a izquierda y a derecha.

Definición 68. *Sean $\underline{M}$, $\underline{N}$, $\underline{P}$ complejos de cadena de R-módulos y $f : \underline{M} \longrightarrow \underline{N}$, $g : \underline{N} \longrightarrow \underline{P}$ aplicaciones de cadena. Se dice que la sucesión de complejos de cadena*

$$0 \longrightarrow \underline{M} \xrightarrow{f} \underline{N} \xrightarrow{g} \underline{P} \longrightarrow 0$$

es exacta si, para cada $n \in \mathbb{Z}$, las siguientes son sucesiones exactas de R-módulos:

$$0 \longrightarrow M_n \xrightarrow{f_n} N_n \xrightarrow{g_n} P_n \longrightarrow 0$$

Proposición B.1.2. *Sea $0 \longrightarrow \underline{M} \xrightarrow{f} \underline{N} \xrightarrow{g} \underline{P} \longrightarrow 0$ una sucesión exacta de complejos de cadena de R-módulos. Entonces, existe un morfismo de R-módulos*

$$\partial_n : H_n(\underline{P}) \longrightarrow H_{n-1}(\underline{M}).$$

A esta familia de morfismos de R-modulos $\{\partial_n\}_{n\in\mathbb{Z}}$ se la denomina morfismos conectores.

Demostración. Como f y g son aplicaciones de cadena, se tiene el siguiente diagrama conmutativo:

(B.1.4)
$$\begin{tikzcd}
 & & N_{n+1} \arrow[r, "g_{n+1}"] \arrow[d, "d'_{n+1}"] & P_{n+1} \arrow[r] \arrow[d, "d''_{n+1}"] & 0 \\
0 \arrow[r] & M_n \arrow[r, "f_n"] \arrow[d, "d_n"] & N_n \arrow[r, "g_n"] \arrow[d, "d'_n"] & P_n \arrow[r] \arrow[d, "d''_n"] & 0 \\
0 \arrow[r] & M_{n-1} \arrow[r, "f_{n-1}"] \arrow[d, "d_{n-1}"] & N_{n-1} \arrow[r, "g_{n-1}"] \arrow[d, "d'_{n-1}"] & P_{n-1} \arrow[r] & 0 \\
0 \arrow[r] & M_{n-2} \arrow[r, "f_{n-2}"] & N_{n-2}. & &
\end{tikzcd}$$

Sea $\bar{z} \in H_n(\underline{P})$, $\bar{z} = z + Im(d''_{n+1})$ con $z \in ker(d''_n)$. Como la sucesión

(B.1.5)
$$0 \longrightarrow M_n \longrightarrow N_n \longrightarrow P_n \longrightarrow 0$$

es exacta, g_n es un epimorfismo de R-módulos y existe $y \in N_n$ con $g_n(y) = z$. Sea $y' = d'_n(y)$. Entonces, $g_{n-1}(y') = (g_{n-1} \circ d'_n)(y) = (d''_n \circ g_n)(y) = d''_n(z) = 0$. Por consiguiente, $y' \in ker(g_{n-1})$. Como la sucesión

(B.1.6)
$$0 \longrightarrow M_{n-1} \longrightarrow N_{n-1} \longrightarrow P_{n-1} \longrightarrow 0$$

es exacta, $ker(g_{n-1}) = Im(f_{n-1})$ y por tanto, existe $x \in M_{n-1}$ tal que $y' = f_{n-1}(x)$. Ahora, $(d'_{n-1} \circ f_{n-1})(x) = d'_{n-1}(y') = (d'_{n-1} \circ d'_n)(y) = 0$. En consecuencia, $f_{n-2}(d_{n-1}(x)) = (f_{n-2} \circ d_{n-1})(x) = (d'_{n-1} \circ f_{n-1})(x) = 0$ y $d_{n-1}(x) \in ker(f_{n-2})$. Como

(B.1.7)
$$0 \longrightarrow M_{n-2} \longrightarrow N_{n-2} \longrightarrow P_{n-2} \longrightarrow 0$$

es una sucesión exacta, f_{n-2} es un monomorfismo de R-módulos y se tiene que $d_{n-1}(x) = 0$, concluyendo así que $x \in ker(d_{n-1})$. Definimos así el morfismo de R-módulos

$$\begin{array}{rccc} \partial_n : & H_n(\underline{P}) & \longrightarrow & H_{n-1}(\underline{M}) \\ & \bar{z} & \mapsto & \partial_n(\bar{z}) := \bar{x}, \end{array}$$

donde $\bar{x} = x + Im(d_n)$. Veamos que ∂_n está bien definido comprobando que $\bar{x}$ no depende de la elección de z ni de y. Por una parte, con las notaciones precedentes, sea $z \in ker(d''_n)$; $y_1, y_2 \in N_n$ tales que $g_n(y_1) = g_n(y_2) = z$; $y'_1 = d'_n(y_1)$, $y'_2 = d'_n(y_2)$; $\bar{x_1} = x_1 + Im(d_n)$ y $\bar{x_2} = x_2 + Im(d_n)$ tales que $f_{n_1}(x_1) = y'_1$ y $f_{n-1}(x_2) = y'_2$. Se tiene que $g_n(y_1) - g_n(y_2) = g_n(y_1 - y_2) = 0$ e $y_1 - y_2 \in ker(g_n)$. Como la Sucesión (B.1.5) es exacta, $y_1 - y_2 \in ker(g_n) = Im(f_n)$ y existe $x' \in M_n$ tal que $f_n(x') = y_1 - y_2$. Además, $(d'_n \circ f_n)(x') = (f_{n-1} \circ d_n)(x') = y'_1 - y'_2$. Pero $f_{n-1}(x_1 - x_2) = y'_1 - y'_2$. Como la Sucesión (B.1.6) es exacta, f_{n-1} es monomorfismo de R-módulos y debe ser $d_n(x') = x_1 - x_2$. En consecuencia $x_1 - x_2 \in Im(d_n)$ y $\bar{x_1} = x_1 + Im(d_n) = x_2 + Im(d_n) = \bar{x_2}$. En conclusión, $\bar{x}$ no depende de la elección de y. Por otra parte, para verificar que $\bar{x}$ no depende de la elección de z bastará comprobar que si $z \in Im(d''_{n+1})$, entonces $x \in Im(d_n)$. Si $z \in Im(d''_{n+1})$ entonces existe $z' \in P_{n+1}$ tal que $d''_{n+1}(z') = z$. Además, como la sucesión

(B.1.8)
$$0 \longrightarrow M_{n+1} \longrightarrow N_{n+1} \longrightarrow P_{n+1} \longrightarrow 0$$

es exacta, g_{n+1} es epimorfismo de R-módulos y existe $y'' \in P_{n+1}$ de modo que $g_{n+1}(y'') = z'$. Además, se tiene que $(d''_{n+1} \circ g_{n+1})(y'') = (g_n \circ d'_{n+1})(y'')$. Como ya se ha visto que $\bar{x}$ no depende de la elección de y, se puede tomar $y = d'_{n+1}(y'')$ sin pérdida de generalidad. Entonces se tiene que $y' = d'_n(y) = (d'_n \circ d'_{n+1})(y'') = 0$. Como f_{n-1} es monomorfismo de R-módulos debe ser $x = 0 \in Im(d_n)$.
Las propiedades de linealidad de ∂_n se derivan de las propiedades de linealidad de los morfismos del Diagrama (B.1.4). □

Algunos autores prueban la siguiente Proposición mediante el "Snake Lemma". Hemos preferido usar la Proposición de [**Raghavan et al., 1975**].

Proposición B.1.3. *Sea* $0 \longrightarrow \underline{M} \xrightarrow{f} \underline{N} \xrightarrow{g} \underline{P} \longrightarrow 0$ *una sucesión exacta de complejos de cadena de R-módulos. Entonces, la sucesión de R-módulos*

$$\cdots \longrightarrow H_n(\underline{M}) \xrightarrow{H_n(f)} H_n(\underline{N}) \xrightarrow{H_n(g)} H_n(\underline{P}) \xrightarrow{\partial_n} H_{n-1}(\underline{M}) \xrightarrow{H_{n-1}(f)} H_{n-1}(\underline{N})$$

es exacta.

Demostración. *i*) Veamos que es exacta en $H_n(\underline{P})$. Por una parte, sea $\bar{z} = z+Im(d''_{n+1} \in Im(H_n(g))$, entonces existe $\bar{y} \in H_n(\underline{N})$ tal que $H_n(g)(\bar{y}) = \bar{z}$; $\bar{y} = y + Im(d'_{n+1})$ e $y \in ker(d'_n)$. Entonces $y' = d'_n(y) = 0$. Como la Sucesión (B.1.6) es exacta, f_{n-1} es monomorfismo de R-módulos y, por construcción (ver la demostración de la Proposición 2.2.2), $\partial_n(\bar{z}) = \bar{x}$, donde $\bar{x} = x + Im(d_n)$ con $x = 0$. Por consiguiente, $\bar{x} = 0$ e $Im(H_n(g)) \subseteq ker(\partial_n)$. Por otra parte, si $\bar{z} = z + Im(d''_{n+1}) \in ker(\partial_n)$ entonces $\partial(\bar{z}) = \bar{x} = x + Im(d_n)$ con $x \in Im(d_n)$. Por tanto, existe $x' \in M_n$ tal que $d_n(x') = x$. Definimos $y'' := y - f_n(x')$, donde y es un elemento de Y_n tal que $g_n(y) = z$ (ver demostración de la Proposición 2.2.2). Como el diagrama

$$\text{(B.1.9)} \qquad \begin{tikzcd} M_n \arrow[r, "f_n"] \arrow[d, "d_n"] & N_n \arrow[d, "d'_n"] \\ M_{n-1} \arrow[r, "f_{n-1}"] & N_{n-1} \end{tikzcd}$$

es conmutativo, $d'_n(f_n(x')) = f_{n-1}(d_n(x')) = y'$. Por consiguiente, $d'_n(y'') = d'_n(y - f_n(x')) = d'_n(y) - d'_n(f_n(x')) = y' - y' = 0$ e $y'' \in ker(d'_n)$. Por tanto, $y'' + Im(d'_{n+1}) \in H_n(\underline{N})$. Además, $g_n(y'') = g_n(y - f_n(x')) = g_n(y) - (g_n \circ f_n)(x')$. Como la Sucesión (B.1.5) es exacta, $f_n \circ g_n = 0$ y se tiene que $g_n(y'') = z$. En consecuencia, $\bar{z} = H_n(g)(\bar{y''})$ donde $\bar{y''} = y'' + Im(d'_{n+1})$ y se tiene que $ker(\partial_n) \subseteq Im(H_n(g))$.

ii) Probemos la exactitud en $H_{n-1}(\underline{M})$. Supongamos que $\bar{x} = x + Im(d_n) \in Im(\partial_n)$. Entonces $\bar{x} = \partial_n(\bar{z})$ para algún $\bar{z} = z+Im(d''_{n+1}) \in H_n(\underline{P})$. Supongamos $z = g(y)$ e $y' = d'_n(y)$ de acuerdo a las notaciones en la Proposición 2.2.2. Entonces, $H_{n-1}(f)(\bar{x}) = f_{n-1}(x) + Im(d'_n)$. Pero $f_{n-1}(x) = y' = d'_n(y) \in Im(d'_n)$. Por tanto, $f_{n-1}(x) \in Im(d'_n)$, $H_{n-1}(f)(x) = 0$ e $Im(\partial_n) \subseteq ker(H_{n-1}(f))$. De otro lado, si $\bar{x} = x + Im(d_n) \in ker(H_{n-1}(f))$, entonces $H_{n-1}(f)(\bar{x}) = f_{n-1}(x) + Im(d'_n) = 0$, es decir, $f_{n-1}(x) \in Im(d'_n)$. Sea $y \in N_n$ tal que $d'_n(y) = f_{n-1}(x)$; $z = g_n(y)$ y $\bar{z} = z + Im(d''_{n+1})$. Como el diagrama

$$\begin{tikzcd} N_n \arrow[r, "g_n"] \arrow[d, "d'_n"] & P_{n+1} \arrow[d, "d''_n"] \\ N_{n-1} \arrow[r, "g_{n-1}"] & P_{n-1} \end{tikzcd}$$

es conmutativo, se tiene que $d''_n(z) = (d''_n \circ g_n)(y) = (g_{n-1} \circ d'_n)(y) = (g_{n-1} \circ f_{n-1})(x)$. Además, como la Sucesión (B.1.6) es exacta se tiene que $g_{n-1} \circ f_{n-1} = 0$. En consecuencia, $z \in ker(d''_n)$ y $\bar{z} \in H_n(\underline{P})$. Más aún, por construcción (ver Proposición 2.2.2), se tiene que $\partial_n(\bar{z}) = \bar{x}$ y, por consiguiente, $\bar{x} \in Im(\partial_n)$. Se concluye de esta forma que $ker(H_{n-1}(f)) \subseteq Im(\partial_n)$.

iii) Veamos la exactitud en $H_n(\underline{N})$. Sea $\bar{y} = y + Im(d'_{n+1}) \in H_n(\underline{N})$ con $\bar{y} \in Im(H_n(f))$. Entonces, $\bar{y} = H_n(f)(\bar{x})$ para algún $\bar{x} = x + Im(d_{n+1}) \in H_n(\underline{M})$. Entonces, $y = f(x)$ para algún $x \in ker(d_n)$. Entonces, $H_n(g)(\bar{y}) = (H_n(g) \circ H_n(f))(\bar{x}) = (g_n \circ f_n)(x) + Im(d''_{n+1})$. Pero como la Sucesión (B.1.5) es exacta, $g_n \circ f_n = 0$ y $H_n(g)(\bar{y}) = 0$. Se conluye así que $Im(H_n(f)) \subseteq ker(H_n(g))$. Finalmente, supongamos $\bar{y} = y + Im(d'_{n+1}) \in H_n(\underline{N})$, $\bar{y} \in ker(H_n(g))$. Entonces, $H_n(g)(\bar{y}) = g(y) + Im(d''_{n+1}) = 0$. Es decir, $g(y) \in Im(d''_{n+1})$. Sea $z'' \in Z_{n+1}$ tal que $d''_{n+1}(z'') = g(y)$. Como la Sucesión (B.1.8) es exacta, g_{n+1} es epimorfismo de R-módulos. Sea $y'' \in N_{n+1}$ tal que $g_{n+1}(y'') = z''$. Como el diagrama

$$\begin{tikzcd} N_{n+1} \arrow[r, "g_{n+1}"] \arrow[d, "d'_{n+1}"] & P_n \arrow[d, "d''_{n+1}"] \\ N_n \arrow[r, "g_n"] & P_n \end{tikzcd}$$

es conmutativo, $g_n(y) = (d''_{n+1} \circ g_{n+1})(y') = (g_n \circ d'_{n+1})(y'') = g_n(d'_{n+1}(y''))$. Entonces, $g_n(y - d'_{n+1}(y'')) = g_n(y) - g_n(y) = 0$ e $y - d'_{n+1}(y'') \in ker(g_n)$. Como la Sucesión (B.1.5) es exacta, $ker(g_n) = Im(f_n)$ y, en consecuencia, existe $x \in X_n$ con $f_n(x) = y - d'_{n+1}(y'')$. Ahora bien, se tiene que $d'_n(f_n(x)) = d'_n(y - d'_{n+1}(y'')) = d'_n(y) - (d'_n \circ d'_{n+1})(y'')$. Pero $d'_n \circ d'_{n+1} = 0$ y $d'_n(y) = 0$ porque $\bar{y} = y + Im(d'_{n+1}) \in H_n(\underline{N}) = {}^{ker(d'_n)}/_{Im(d'_{n+1})}$. Luego $f_n(x) \in ker(d'_n)$. Notemos que, como el Diagrama (B.1.9) es conmutativo, $f_{n-1}(d_n(x)) = d'_n(f_n(x)) = 0$. Como la Sucesión (B.1.5) es exacta, f_{n-1} es monomorfismo de R-módulos y debe ser $d_n(x) = 0$, con lo que se tiene que $x \in ker(d_n)$. Definimos $\bar{x} := x + Im(d_{n+1}) \in H_n(\underline{M})$. Se tiene que $f_n(x)+Im(d'_{n+1}) = y+Im(d'_{n+1})$ porque $f_n(x)-y = y-d'_{n+1}(y'')-y = -d'_{n+1}(y'') \in Im(d'_{n+1})$. Por tanto, se concluye que $\bar{y} = H_n(f)(\bar{x})$ y $ker(H_n(g)) \subseteq Im(H_n(f))$. ☐

Proposición B.1.4. *Sean $\underline{M}$, $\underline{N}$ y $\underline{P}$ complejos de cadena de R-módulos; sea*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \underline{M} & \xrightarrow{f} & \underline{N} & \xrightarrow{g} & \underline{P} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\ 0 & \longrightarrow & \underline{M}' & \xrightarrow{f'} & \underline{N}' & \xrightarrow{g'} & \underline{P}' & \longrightarrow & 0 \end{array} \tag{B.1.10}$$

un diagrama conmutativo cuyas filas son sucesiones exactas. Entonces, el diagrama

$$\begin{array}{ccccccccccccc} \dots & \longrightarrow & H_n(\underline{M}) & \xrightarrow{H_n(f)} & H_n(\underline{N}) & \xrightarrow{H_n(g)} & H_n(\underline{P}) & \xrightarrow{\partial_n} & H_{n-1}(\underline{M}) & \xrightarrow{H_{n-1}(f)} & H_{n-1}(\underline{N}) & \longrightarrow & \dots \\ & & \downarrow{\scriptstyle H_n(\alpha)} & & \downarrow{\scriptstyle H_n(\beta)} & & \downarrow{\scriptstyle H_n(\gamma)} & & \downarrow{\scriptstyle H_{n-1}(\alpha)} & & \downarrow{\scriptstyle H_{n-1}(\beta)} & & \\ \dots & \longrightarrow & H_n(\underline{M}') & \xrightarrow{H_n(f')} & H_n(\underline{N}') & \xrightarrow{H_n(g')} & H_n(\underline{P}') & \xrightarrow{\partial'_n} & H_{n-1}(\underline{M}') & \xrightarrow{H_{n-1}(f')} & H_{n-1}(\underline{N}') & \longrightarrow & \dots \end{array}$$

es conmutativo.

Demostración. Para probar esta Proposición bastará ver que para cada $n \in \mathbb{Z}$ se tiene:
i) $H_n(\beta) \circ H_n(f) = H_n(f') \circ H_n(\alpha)$.
ii) $H_n(\gamma) \circ H_n(g) = H_n(g') \circ H_n(\beta)$.
iii) $H_{n-1}(f) \circ \partial_n = \partial'_n \circ H_{n-1}(f')$.
i) y *ii)* Por una parte, en virtud de la Proposición 2.2.1 se tiene que si

$$\bar{x} = x + Im(d_{n+1}) \in H_n(\underline{M}), \qquad \bar{y} = y + Im(d'_{n+1}) \in H_n(\underline{N}),$$

entonces

$$(H_n(\beta) \circ H_n(f))(\bar{x}) = (\beta_n \circ f_n)(x) + Im(c'_n), \qquad (H_n(\gamma) \circ H_n(g))(\bar{y}) = (\gamma_n \circ g_n)(y) + Im(c''_n).$$

Como el Diagrama (B.1.10) es conmutativo, se sigue que los diagramas:

$$\begin{array}{ccc} M_n & \xrightarrow{f_n} & N_n \\ \downarrow{\scriptstyle\alpha_n} & & \downarrow{\scriptstyle\beta_n} \\ M'_n & \xrightarrow{f'_n} & N'_n \end{array} \qquad\qquad \begin{array}{ccc} N_n & \xrightarrow{g_n} & P_n \\ \downarrow{\scriptstyle\beta_n} & & \downarrow{\scriptstyle\gamma_n} \\ N'_n & \xrightarrow{g'_n} & P'_n \end{array}$$

son conmutativos. Por tanto,

$$(H_n(\beta) \circ H_n(f))(\bar{x}) = (\beta_n \circ f_n)(x) + Im(c'_n) = (f'_n \circ \alpha_n)(x) + Im(c'_n) = (H_n(f') \circ H_n(\alpha))(\bar{x})$$

y

$$H_n(\gamma) \circ H_n(g)(\bar{y}) = (\gamma_n \circ g_n)(y) + Im(c''_n) = (g'_n \circ \beta_n)(y) + Im(c''_n) = H_n(g') \circ H_n(\beta)(\bar{y}).$$

iii) Sea $\bar{z} = z + Im(d''_{n+1}) \in H_n(\underline{P})$. En virtud de la Proposición 2.2.2 y con las notaciones utilizadas en ella, podemos tomar $y \in N_n$ tal que $g_n(y) = z$ y $\partial_n(\bar{z}) = \bar{x} = x + Im(d_n)$. Además, se tiene que $H_n(\gamma)(\bar{z}) = \gamma_n(z) + Im(c''_{n+1}) = (\gamma_n \circ g_n)(y) + Im(c''_{n+1})$. Y, por lo visto en *ii)*, $\gamma_n(z) = (\gamma_n \circ g_n)(y) = (g'_n \circ \beta_n)(y)$. Entonces, por una parte, $H_{n-1}(f) \circ \partial_n(\bar{z}) = \alpha_{n-1}(x) + Im(c_n)$. Además, por construcción, se verifica que $f_{n-1}(x) = d'_n(y)$. Por otra parte, evaluemos la función $\partial'_n : H_n(\underline{P}') \longrightarrow H_{n-1}(\underline{M}')$ en $\gamma_n(z) + Im(c''_{n+1})$ tomando $\beta_n(y) \in Y'_n$ tal que $g'_n(\beta_n(y)) = \gamma_n(z)$ y siguiendo el procedimiento de la Proposición 2.2.2. Sea $\bar{x}' = x' + Im(c_n)$ tal que $\partial'_n(\gamma(z)+Im(c''_{n+1})) = \bar{x}'$. Por construcción, se tiene que $f'_{n-1}(x') = c'_n(\beta_n(y))$. Además, los diagramas

$$\begin{array}{ccc} N_n & \xrightarrow{\beta_n} & N'_n \\ \downarrow{\scriptstyle d'_n} & & \downarrow{\scriptstyle c'_n} \\ N_{n-1} & \xrightarrow{\beta_{n-1}} & N'_{n-1} \end{array} \qquad\qquad \begin{array}{ccc} M_{n-1} & \xrightarrow{f_{n-1}} & N_{n-1} \\ \downarrow{\scriptstyle\alpha_{n-1}} & & \downarrow{\scriptstyle\beta_{n-1}} \\ M'_{n-1} & \xrightarrow{f'_{n-1}} & N'_{n-1} \end{array}$$

conmutan. El primero porque $\beta : \underline{N} \longrightarrow \underline{N}'$ es un morfismo de complejos de R-módulos, y el segundo porque el Diagrama B.1.10 es conmutativo. Por consiguiente,

$$c'_n(\beta_n(y)) = \beta_{n-1}(d'_n(y)) = \beta_{n-1}(f_{n-1}(x)) = f'_{n-1}(\alpha_{n-1}(x)).$$

En suma, se tiene que $f'_{n-1}(x') = f'_{n-1}(\alpha_{n-1}(x))$. Como las filas del Diagrama B.1.10 son sucesiones exactas, f_{n-1} es monomorfismo de R-módulos, $x' = \alpha_{n-1}(x)$. Por tanto,

$$(H_{n-1}(\alpha)\circ\partial_n)(\bar{z}) = \alpha_{n-1}(x)+Im(c_n) = x'+Im(c_n) = \partial'_n(\gamma_n(z)+Im(c''_{n+1}) = (\partial'_n\circ H_n(\gamma))(\bar{z}).$$

□

DEFINICIÓN 69. *Sean $\underline{M}$, $\underline{N}$ complejos de cadena de R-módulos. Sean $f, g : \underline{M} \longrightarrow \underline{N}$ dos morfismos de cadena. Una homotopía entre f y g es una familia de morfismos de R-módulos $\{h_n : M_n \longrightarrow N_{n+1}\}_{n\in\mathbb{Z}}$ que verifican la siguiente propiedad:*

$$(h_{n-1}\circ d_n)(x) + (d'_{n+1}\circ h_n)(x) = f_n(x) - g_n(x) \quad \forall x \in M_n,\ \forall n \in \mathbb{Z}. \tag{B.1.11}$$

Cuando existe una homotopía entre f y g se dice que f y g son homótopos.

La homotopía define una relación de equivalencia $\sim$ en el conjunto de morfismos de cadena de $\underline{M}$ en $\underline{N}$, donde dos morfismos de cadena $f, g : \underline{M} \longrightarrow \underline{N}$ están relacionados si existe una homotopía entre ellos, es decir, si son homótopos. Para ver que $f \sim f$ basta tomar $h_n = d_n$. Ahora, si $f \sim g$, entonces existen $\{h_n\}_{n\in\mathbb{Z}}$ verificando la Igualdad (B.1.11). Por tanto, se tiene que

$$-(h_{n-1}\circ d_n)(x) - (d'_{n+1}\circ h_n)(x) = g_n(x) - f_n(x) \quad \forall x \in M_n,\ \forall n \in \mathbb{Z}.$$

Como d_n, d'_n y h_n son morfismos de R-módulos, se sigue que

$$(-h_{n-1}\circ d_n)(x) + (d'_{n+1}\circ -h_n)(x) = g_n(x) - f_n(x) \quad \forall x \in M_n,\ \forall n \in \mathbb{Z}.$$

Por tanto se tiene que $\{h'_n\}_{n\in\mathbb{Z}}$ donde $h'_n = -h_n$ es una homotopía entre g y f, concluyendo que $g \sim f$. Finalmente, sean $f^1, f^2, f^3 : \underline{M} \longrightarrow \underline{N}$ verificando $f^1 \sim f^2$ y $f^2 \sim f^3$ con homotopías $\{h^1_n\}_{n\in\mathbb{Z}}$ y $\{h^2_n\}_{n\in\mathbb{Z}}$ respectivamente. Tomando $h_n = h^1_n + h^2_n$ se tiene que

$$\begin{gathered}(h_{n-1}\circ d_n)(x) + (d'_{n+1}\circ h_n)(x) = (h^1_{n-1}\circ d_n)(x) + (h^2_{n-1}\circ d_n)(x)\\ +(d'_{n+1}\circ h^1_n)(x) + (d'_{n+1}\circ h^2_n)(x) = f^1_n(x) - f^2_n(x) + f^2_n(x) - f^3_n(x) = f^1_n(x) - f^3_n(x)\end{gathered}$$

para cada $x \in M_n$ y cada $n \in \mathbb{Z}$. Por tanto, $\{h_n\}_{n\in\mathbb{Z}}$ es una homotopía entre f^1_n y f^3_n. Concluimos así que $f^1_n \sim f^3_n$.

PROPOSICIÓN B.1.5. *Sean $\underline{M}$, $\underline{N}$ complejos de cadena de R-módulos; $f, g : \underline{M} \longrightarrow \underline{N}$ morfismos de cadena homótopos. Entonces, $H_n(f) = H_n(g)$ para todo $n \in \mathbb{Z}$.*

DEMOSTRACIÓN. Sean $n \in \mathbb{Z}$, $\bar{x} = x + Im(d_{n+1}) \in H_n(\underline{M})$. Entonces, $H_n(f)(\bar{x}) = f_n(x)+Im(d'_{n+1}) = g_n(x)+Im(d'_{n+1}) = H_n(g)(\bar{x})$ si y solamente si $f_n(x)-g_n(x) \in Im(d'_{n+1})$. Pero como f y g son homótopos, existe un morfismo de R-módulos $h_n : M_n \longrightarrow N_{n+1}$ tal que $f_n(x) - g_n(x) = (h_{n-1}\circ d_n)(x) + (d'_{n+1}\circ h_n)(x)$. Además, como $\bar{x} \in H_n(\underline{M})$, $x \in ker(d_n)$. En consecuencia, $(h_{n-1}\circ d_n)(x) = h_{n-1}(0) = 0$. Por tanto, $f_n(x) - g_n(x) = d'_{n+1}(h_n(x)) \in Im(d'_{n+1})$. □

B.2. Existencia y Propiedades Esenciales de los Functores Ext

Sean M,N R-módulos y $(\underline{P}, \epsilon)$ una resolución proyectiva de M. Como el functor $Hom_R(-, N)$ es contravariante, se puede considerar la sucesión:

$$Hom_R(\underline{P}, N) : 0 \longrightarrow Hom_R(P_0, N) \overset{Hom_R(d_1,N)}{\longrightarrow} Hom_R(P_1, N) \overset{Hom_R(d_2,N)}{\longrightarrow} \cdots$$

de acuerdo a las notaciones establecidas en la Sección A.3 del Apéndice A. Notemos que, dado $n \in \mathbb{N}$, $Hom_R(d_{n+1}, N)\circ Hom_R(d_n, N) = Hom_R(d_n\circ d_{n+1}, N) = Hom_R(0, N) = 0$. Por tanto, $Hom_R(\underline{P}, N)$ es un complejo de co-cadena, cuyos módulos de co-homología se denotarán por $H^n(Hom_R(\underline{P}, N)) = H^n(M, N; \underline{P})$. Sea ahora $f : M \longrightarrow M'$ un morfismo de R-módulos y (P, ϵ), (P', ϵ') resoluciones proyectivas de M y M' respectivamente. Por la Proposición 2.3.2, existe una aplicación $\{F_n\}_{n\in\mathbb{N}} = F : \underline{P} \longrightarrow \underline{P}'$ de cadena sobre f. Además, se tiene que:

$$Hom_R(d'_{n+1}, N)\circ Hom_R(F_n, N) = Hom_R(F_n\circ d'_{n+1}, N) = Hom_R(F_{n+1}, N)\circ Hom_R(d_{n+1}, N).$$

En consecuencia, el diagrama:

$$\begin{tikzcd}
Hom_R(P_{n+1},N) & Hom_R(P'_{n+1},N) \arrow[l, "Hom_R(F_{n+1},N)"'] \\
Hom_R(P_n,N) \arrow[u, "Hom_R(d_{n+1},N)"'] & Hom_R(P'_n,N) \arrow[l, "Hom_R(F_n,N)"'] \arrow[u, "Hom_R(d'_{n+1},N)"']
\end{tikzcd}$$

conmuta para todo $n \in \mathbb{N}$ y $\{Hom_R(F_n,N)\}_{n\in\mathbb{N}} := Hom_R(F,N) : Hom_R(\underline{P}',N) \longrightarrow Hom_R(\underline{P},N)$ es una aplicación de co-cadena. En virtud de la Proposición 2.2.1, $Hom_R(F,N)$ induce un morfismo de R-módulos:

$$H^n(f,N;\underline{P}',\underline{P}) := H^n(Hom_R(F,N)) : H^n(M,N;\underline{P}') \longrightarrow H^n(M,N;\underline{P}).$$

Veamos que dicho morfismo está bien definido al no depender de la elección de F. Si F y G son aplicaciones de cadena sobre f, entonces por la Proposición 2.3.2, F y G son aplicaciones homótopas, i.e. existe una homotopía $h = \{h_n : P_n \longrightarrow P'_{n+1}\}$. Entonces, se tiene:

$$\begin{aligned}
&Hom_R(d_n,N) \circ Hom_R(h_{n-1},N) + Hom_R(h_n,N) \circ Hom_R(d'_{n+1},N) \\
= {}& Hom_R(h_{n-1} \circ d_n,N) + Hom_R(d'_{n+1} \circ h_n,N) = Hom_R(h_{n-1} \circ d_n + d'_{n+1} \circ h_n,N) \\
&= Hom_R(F_n - G_n,N) = Hom_R(F_n,N) - Hom_R(G_n,N).
\end{aligned}$$

En consecuencia, $\{Hom_R(h_n,N) : Hom_R(P'_{n+1},N) \longrightarrow Hom_R(P_n,N)\}$ es una homotopía entre $Hom_R(F,N)$ y $Hom_R(G,N)$. En virtud de la Proposición 2.2.5, ambas inducen el mismo morfismo $H^n(f,N;\underline{P}',\underline{P})$. Dadas una sucesión exacta de R-módulos y

$$\mathcal{P} :\ 0 \longrightarrow \underline{P}' \longrightarrow \underline{P} \longrightarrow \underline{P}'' \longrightarrow 0$$

una resolución proyectiva de dicha sucesión, se tiene que la sucesión de complejos de co-cadena:

$$Hom_R(\mathcal{P},N) :\ 0 \longrightarrow Hom_R(\underline{P}'',N) \longrightarrow Hom_R(\underline{P},N) \longrightarrow Hom_R(\underline{P}',N) \longrightarrow 0$$

es exacta (ver la demostración del apartado *ii*) del Lema B.2.1). Denotaremos por:

$$\partial^n(N,\mathcal{P}) : H^n(M',N;\underline{P}'') \longrightarrow H^{n+1}(M'',N;\underline{P}').$$

a los morfismos conectores asociados a $Hom_R(\mathcal{P},N)$ de la Proposición 2.2.2.

LEMA B.2.1. *i) Sean $f : M \longrightarrow M'$, $g : M' \longrightarrow M''$ morfismos de R-módulos; y sean $\underline{P}$, $\underline{P}'$ y $\underline{P}''$ resoluciones proyectivas de M, M' y M'' respectivamente. Entonces, para cada $n \in \mathbb{N}$ se tiene:*

$$H^n(g \circ f,N;\underline{P}'',\underline{P}) = H^n(f,N;\underline{P}',\underline{P}) \circ H^n(g,N;\underline{P}'',\underline{P}').$$

Más aún, $H^n(1_M,N;\underline{P},\underline{P}) = Id_{H^n(M,N;\underline{P})}$.
ii) Si $\mathcal{P} : 0 \longrightarrow \underline{P}' \xrightarrow{\varphi} \underline{P} \xrightarrow{\pi} \underline{P}'' \longrightarrow 0$ es una resolución proyectiva de una sucesión exacta de R-módulos $0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{j} M'' \longrightarrow 0$, entonces la siguiente sucesión de R-módulos es exacta:

$$\begin{aligned}
0 \longrightarrow H^0(M',N;\underline{P}') \longrightarrow \cdots \longrightarrow H^n(M',N;\underline{P}') &\xrightarrow{\partial^n(N,\mathcal{P})} H^{n+1}(M'',N;\underline{P}'') \\
\xrightarrow{H^{n+1}(i,N;\underline{P}'',\underline{P})} H^{n+1}(M,N;\underline{P}) &\xrightarrow{H^{n+1}(j,N;\underline{P},\underline{P}')} H^{n+1}(M',N;\underline{P}') \longrightarrow \cdots
\end{aligned}$$

iii) Dado un diagrama conmutativo, cuyas filas son sucesiones exactas:

$$\begin{tikzcd}
\mathcal{M} : & 0 \arrow[r] & M' \arrow[r] \arrow[d, "f'"] & M \arrow[r] \arrow[d, "f"] & M'' \arrow[r] \arrow[d, "f''"] & 0 \\
\mathcal{L} : & 0 \arrow[r] & L' \arrow[r] & L \arrow[r] & L'' \arrow[r] & 0,
\end{tikzcd}$$

y dado el diagrama conmutativo de resoluciones proyectivas siguiente:

$$\begin{tikzcd}
\mathcal{P} : & 0 \arrow[r] & \underline{P}' \arrow[r, "\varphi^1"] \arrow[d, "F'"] & \underline{P} \arrow[r, "\pi^1"] \arrow[d, "F"] & \underline{P}'' \arrow[r] \arrow[d, "F''"] & 0 \\
\mathcal{Q} : & 0 \arrow[r] & \underline{Q}' \arrow[r, "\varphi^1"] & \underline{Q} \arrow[r, "\pi^2"] & \underline{Q}'' \arrow[r] & 0,
\end{tikzcd} \tag{B.2.1}$$

donde $\mathcal{P}$ y $\mathcal{Q}$ son resoluciones proyectivas de $\mathcal{M}$ y $\mathcal{L}$ respectivamente; y F, F' y F'' son aplicaciones de cadena sobre f, f' y f'' respectivamente. Entonces, el siguiente diagrama es conmutativo para cada $n \in \mathbb{N}$:

$$\begin{tikzcd} H^{n+1}(M'', N; \underline{P}'') & H^{n+1}(L'', N; \underline{Q}'') \arrow[l, "H^n(f'', N; \underline{P}'', \underline{Q}'')"'] \\ H^n(M', N; \underline{P}') \arrow[u, "\partial^n(N,\mathcal{P})"] & H^n(L', N; \underline{Q}'). \arrow[l, "H^{n+1}(f', N; \underline{P}', \underline{Q}')"'] \arrow[u, "\partial^n(N,\mathcal{Q})"'] \end{tikzcd} \tag{B.2.2}$$

Demostración. i) Sean F y G aplicaciones de cadena sobre f y g respectivamente. Entonces de igual forma que en el Lema 2.4.1, se sigue que $G \circ F$ es una aplicación de cadena sobre $g \circ f$ y se tiene que:

$$\begin{aligned} H^n(g \circ f, N; \underline{P}'', \underline{P}) &= H^n(Hom_R(G \circ F, N)) = H^n(Hom_R(F, N) \circ Hom_R(G, N)) \\ &= H^n(Hom_R(F, N)) \circ H^n(Hom_R(G, N)) = H^n(f, N; \underline{P}', \underline{P}) \circ H^n(g, N; \underline{P}'', \underline{P}'). \end{aligned}$$

Más aún, al igual que en el Lema 2.4.1, $Id_{\underline{P}}$ es una aplicación de cadena sobre Id_M y, en consecuencia,

$$H^n(Id_M, N; \underline{P}, \underline{P}) = H^n(Hom_R(Id_{\underline{P}}, N)) = Id_{H^n(Hom_R(\underline{P}, N))} = Id_{H^n(M,N;\underline{P})}.$$

ii) Como $\mathcal{P}$ es una sucesión exacta, la sucesión siguiente es exacta para cada $n \in \mathbb{N}$:

$$\mathcal{P}_n : 0 \longrightarrow P'_n \xrightarrow{\varphi_n} P_n \xrightarrow{\pi_n} P''_n \longrightarrow 0.$$

Fijado $n \in \mathbb{N}$, como en virtud de la Proposición A.3.1, el functor $Hom_R(-, N)$ es exacto a izquierda, se tiene que la sucesión:

$$0 \longrightarrow Hom_R(P''_n, N) \xrightarrow{Hom_R(\pi_n, N)} Hom_R(P_n, N) \xrightarrow{Hom_R(\varphi_n, N)} Hom_R(P'_n, N).$$

es exacta. Ahora bien, como P''_n es proyectivo, la Sucesión $\mathcal{P}_n$ se escinde. Es decir, existe $h : P_n \longrightarrow P'_n$ tal que $h \circ \varphi_n = Id_{P'_n}$. Entonces dada $g \in Hom_R(P'_n, N)$ podemos considerar $g \circ h \in Hom_R(P_n, N)$ y se tiene que:

$$Hom_R(\varphi_n, N)(g \circ h) = g \circ h \circ \varphi_n = g \circ Id_{P'_n} = g.$$

En consecuencia, $Hom_R(\varphi_n, N)$ es suprayectivo y se tiene la siguiente sucesión exacta para cada $n \in \mathbb{N}$:

$$0 \longrightarrow Hom_R(P''_n, N) \xrightarrow{Hom_R(\pi_n, N)} Hom_R(P_n, N) \xrightarrow{Hom_R(\varphi_n, N)} Hom_R(P'_n, N) \longrightarrow 0.$$

Es decir, se tiene la sucesión exacta de complejos de co-cadena:

$$0 \longrightarrow Hom_R(\underline{P}'', N) \xrightarrow{Hom_R(\pi, N)} Hom_R(\underline{P}, N) \xrightarrow{Hom_R(\varphi, N)} Hom_R(\underline{P}', N) \longrightarrow 0$$

Razonando de la misma manera que en el Lema 2.4.1, por la Proposición 2.2.3, se tiene la siguiente sucesión exacta:

$$\begin{aligned} &0 \longrightarrow H^0(Hom_R(\underline{P}', N)) \longrightarrow \cdots \longrightarrow H^n(Hom_R(\underline{P}', N)) \xrightarrow{\partial^n(N,\mathcal{P})} H^{n+1}(Hom_R(\underline{P}'', N)) \\ &\xrightarrow{H^{n+1}(Hom_R(\pi, N)} H^{n+1}(M, N; \underline{P}) \xrightarrow{H^{n+1}(Hom_R(\varphi, N))} H^{n+1}(M', N; \underline{P}') \longrightarrow \cdots \end{aligned}$$

Pero como $\mathcal{P}$ es una resolución proyectiva de $0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{j} M'' \longrightarrow 0$, φ y π son aplicaciones de cadena sobre i y j respectivamente. Por tanto, $Hom_R(\varphi, N) = H^n(i, N; \underline{P}, \underline{P}')$ y $Hom_R(\pi, N) = H^n(j, N; \underline{P}'', \underline{P})$, con lo que se tiene ii).
iii) Siguiendo el mismo argumento que en el apartado ii) precedente, se tienen las sucesiones exactas de complejos de co-cadena:

$$\begin{aligned} 0 \longrightarrow Hom_R(\underline{P}'', N) \longrightarrow Hom_R(\underline{P}, N) \longrightarrow Hom_R(\underline{P}', N) \longrightarrow 0, \\ 0 \longrightarrow Hom_R(\underline{Q}'', N) \longrightarrow Hom_R(\underline{Q}, N) \longrightarrow Hom_R(\underline{Q}', N) \longrightarrow 0. \end{aligned}$$

Además, como el Diagrama (B.2.1) es conmutativo, también lo será el diagrama:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Hom_R(\underline{P}'', N) & \xrightarrow{Hom_R(\pi^1, N)} & Hom_R(\underline{P}, N) & \xrightarrow{Hom_R(\varphi^1, N)} & Hom_R(\underline{P}', N) & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle Hom_R(F'', N)} & & \uparrow{\scriptstyle Hom_R(F, N)} & & \uparrow{\scriptstyle Hom_R(F', N)} & & \\ 0 & \longrightarrow & Hom_R(\underline{Q}'', N) & \xrightarrow{Hom_R(\pi^2, N)} & Hom_R(\underline{Q}, N) & \xrightarrow{Hom_R(\varphi^2, N)} & Hom_R(\underline{Q}', N) & \longrightarrow & 0 \end{array}$$

Por la Proposición 2.2.4, se tiene el diagrama conmutativo:

$$\begin{array}{ccc} H^{n+1}(Hom_R(\underline{P}'', N)) & \xleftarrow{H^n(Hom_R(F'', N))} & H^{n+1}(Hom_R(\underline{Q}'', N)) \\ \uparrow{\scriptstyle \partial^n(N, \mathcal{P})} & & \uparrow{\scriptstyle \partial^n(N, \mathcal{Q})} \\ H^n(Hom_R(\underline{P}', N)) & \xleftarrow{H^n(Hom_R(F', N))} & H^n(Hom_R(\underline{Q}', N)). \end{array}$$

□

Proposición B.2.2. *Sea M un R-módulo y sean $\underline{P}, \underline{Q}$ dos resoluciones proyectivas de M. Entonces,*

$$H^n(Id_M, N; \underline{P}, \underline{Q}) : H^n(M, N; \underline{P}) \longrightarrow H^n(M, N; \underline{Q})$$

es un isomorfismo de R-módulos, para cada $n \in \mathbb{N}$. Además, si $f : M \longrightarrow M'$ es un morfismo de R-módulos y $\underline{P}'$, $\underline{Q}'$ son resoluciones proyectivas de M', entonces el diagrama:

$$\text{(B.2.3)} \qquad \begin{array}{ccc} H^n(M, N; \underline{P}) & \xrightarrow{H^n(Id_M, N; \underline{P}, \underline{Q})} & H^n(M, N; \underline{Q}) \\ \uparrow{\scriptstyle H^n(f, N; \underline{P}', \underline{P})} & & \uparrow{\scriptstyle H^n(f, N; \underline{Q}', \underline{Q})} \\ H^n(M', N\underline{P}') & \xrightarrow{H^n(Id_{M'}, N; \underline{P}', \underline{Q}')} & H^n(M', N; \underline{Q}') \end{array}$$

es conmutativo para todo $n \in \mathbb{N}$. Más aún, si $\mathcal{M} : 0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ es una sucesión exacta de R-módulos y

$$\mathcal{P} : \ 0 \longrightarrow \underline{P}' \longrightarrow \underline{P} \longrightarrow \underline{P}'' \longrightarrow 0, \quad \mathcal{Q} : \ 0 \longrightarrow \underline{Q}' \longrightarrow \underline{Q} \longrightarrow \underline{Q}'' \longrightarrow 0$$

son resoluciones proyectivas de $\mathcal{M}$, entonces el diagrama siguiente conmuta para todo $n \in \mathbb{N}$:

$$\text{(B.2.4)} \qquad \begin{array}{ccc} H^{n+1}(M'', N; \underline{P}'') & \xrightarrow{H_n(Id_{M''}, N; \underline{P}'', \underline{Q}'')} & H^{n+1}(M'', N; \underline{Q}'') \\ \uparrow{\scriptstyle \partial^n(N, \mathcal{P})} & & \uparrow{\scriptstyle \partial^n(N, \mathcal{Q})} \\ H^n(M', N; \underline{P}') & \xrightarrow{H_n(Id_{M'}, N; \underline{P}', \underline{Q}')} & H^n(M', N; \underline{Q}'). \end{array}$$

Demostración. Tomando $M = M' = M''$; $f = g = Id_M$; $\underline{P} = \underline{P}''$; $\underline{P}' = \underline{Q}$ en el apartado $i)$ del Lema B.2.1 precedente, se tiene que:

$$H^n(Id_M, N; \underline{Q}, \underline{P}) \circ H^n(Id_M, N; \underline{P}, \underline{Q}) = H^n(Id_M, N; \underline{P}, \underline{P}) = Id_{H^n(M, N; \underline{P})}.$$

De la misma manera,

$$H^n(Id_M, N; \underline{P}, \underline{Q}) \circ H^n(Id_M, N; \underline{Q}, \underline{P}) = H^n(Id_M, N; \underline{Q}, \underline{Q}) = Id_{H^n(M, N; \underline{Q})}.$$

En consecuencia, $H^n(Id_M, N; \underline{P}, \underline{Q})$ y $H^n(Id_M, N; \underline{Q}, \underline{P})$ son isomorfismos de R-módulos.
Ahora, si $f : M \longrightarrow M'$ es un morfismo de R-módulos, de nuevo, aplicando el apartado $i)$ del Lema B.2.1 a la composición de f con las aplicaciones identidad correspondientes a izquierda y derecha, se tiene:

$$\begin{aligned} H^n(f, N; \underline{Q}', \underline{Q}) \circ H^n(Id_{M'}, N; \underline{P}', \underline{Q}') &= H^n(Id_{M'} \circ f, N; \underline{P}', \underline{Q}) = H^n(f, N; \underline{P}', \underline{Q}) \\ &= H^n(f \circ Id_M, N; \underline{P}, \underline{Q}') = H^n(Id_M, N; \underline{P}, \underline{Q}) \circ H^n(f, N; \underline{P}', \underline{P}), \end{aligned}$$

de donde se sigue la conmutatividad del Diagrama (B.2.3).
$iii)$ Finalmente, consideremos el diagrama conmutativo:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle Id_{M'}} & & \downarrow{\scriptstyle Id_M} & & \downarrow{\scriptstyle Id_{M''}} & & \\ 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0, \end{array}$$

cuyas filas son la sucesión exacta $\mathcal{M}$. Entonces, estamos en las condiciones de la Proposición 2.3.4. Por tanto, existen aplicaciones de cadena $F : \underline{P} \longrightarrow \underline{Q}$; $F' : \underline{P'} \longrightarrow \underline{Q'}$; $F'' : \underline{P''} \longrightarrow \underline{Q''}$ sobre f, f' y f'' respectivamente de forma que el diagrama:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \underline{P'} & \longrightarrow & \underline{P} & \longrightarrow & \underline{P''} & \longrightarrow & 0 \\
 & & \big\downarrow{\scriptstyle F'} & & \big\downarrow{\scriptstyle F} & & \big\downarrow{\scriptstyle F''} & & \\
0 & \longrightarrow & \underline{Q'} & \longrightarrow & \underline{Q} & \longrightarrow & \underline{Q''} & \longrightarrow & 0
\end{array}
\tag{B.2.5}
$$

conmute. Notemos que se trata de un caso particular del enunciado *iii*) del Lema B.2.1 precedente, donde se han tomado $L = M$, $L' = M'$, $L'' = M''$; $f = Id_M$, $f' = Id_{M'}$, $f'' = Id_{M''}$. Por tanto, se sigue que el Diagrama (B.2.4) es conmutativo. □

DEFINICIÓN 70 (**Functores Ext**). *Sea N un R-módulo y $n \in \mathbb{N}$. Se define el functor contravariante $Ext^n_R(-, N)$, de la categoría de R-módulos en sí misma, de la manera siguiente:*

i) A cada R-módulo M le asigna en R-módulo $Ext^n_R(M, N) := H^n(Hom_R(M, \underline{P}))$, donde $\underline{P}$ es una resolución proyectiva de M;

ii) a cada morfismo $f : M \longrightarrow M'$ de R-módulos le asigna el morfismo:

$$Ext^n_R(f, N) := H^n(f, N; \underline{P}, \underline{P'}) : Ext^n_R(M', N) \longrightarrow Ext^n_R(M, N),$$

donde $\underline{P}$ y $\underline{P'}$ son resoluciones proyectivas de M y M' respectivamente.

Del Lema B.2.1 se sigue que $Ext^n_R(-, N)$ es un functor contravariante. Ahora bien, si $\underline{P}$ y $\underline{Q}$ son resoluciones proyectivas de un R-módulo M, se sigue de la Proposición B.2.2 precedente que $H^n(M, N; \underline{P}) \cong H^n(M, N; \underline{Q})$. Por tanto, los R-módulos $\{Ext^n_R(M, N)\}_{n\in\mathbb{N}}$ son independientes de la resolución proyectiva $\underline{P}$ de M elegida (salvo isomorfismo). Además, si $f : M \longrightarrow M'$ es un morfismo de R-módulos y $\underline{P'}$,$\underline{Q'}$ son resoluciones proyectivas de M', se tiene, de nuevo, por la Proposición B.2.2:

$$H^n(f, N; \underline{Q'}, \underline{Q}) \circ H^n(Id_{M'}, N; \underline{P'}, \underline{Q'}) = H^n(Id_M, N; \underline{P}, \underline{Q}) \circ H^n(f, N; \underline{P'}, \underline{P}).$$

Es decir,

$$H^n(f, N; \underline{Q'}, \underline{Q}) = H^n(Id_M, N; \underline{P}, \underline{Q}) \circ H^n(f, N; \underline{P'}, \underline{P}) \circ H^n(Id_{M'}, N; \underline{Q'}, \underline{P'}),$$

donde $H^n(Id_M, N; \underline{P}, \underline{Q})$ y $H^n(Id_{M'}, N; \underline{Q'}, \underline{P'})$ son isomorfismos. En consecuencia, el morfismo $H^n(f, N; \underline{P}, \underline{P'}) = Ext^n_R(f, N)$ es independiente de las resoluciones $\underline{P}$, $\underline{P'}$ elegidas (salvo composición con isomorfismos). Más aún, dado un R-módulo N y una sucesión exacta de R-módulos $\mathcal{M} : 0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$, el Diagrama (B.2.4) de la Proposición B.2.2 garantiza que los morfismos conectores:

$$\partial^n(N, \mathcal{P}) : H^n(M', N; \underline{P'}) \longrightarrow H^{n+1}(M'', N; \underline{P''})$$

no dependen de la resolución $0 \longrightarrow \underline{P'} \longrightarrow \underline{P} \longrightarrow \underline{P''} \longrightarrow 0$ de $\mathcal{M}$ elegida (salvo composición con isomorfismos). Por tanto, se denotarán por:

$$\partial^n(M', M''; N) : Ext^n_R(M', N) \longrightarrow Ext^{n+1}(M'', N) \qquad n \in \mathbb{N}.$$

Supongamos ahora que $\underline{P}$ es una resolución proyectiva de M y $f : N \longrightarrow N'$ es un morfismo de R-módulos. Entonces, f induce una aplicación de cadena:

$$\{Hom_R(P_n, f)\}_{n\in\mathbb{N}} = Hom_R(\underline{P}, f) : Hom_R(\underline{P}, N) \longrightarrow Hom_R(\underline{P}, N'),$$

donde:

$$
\begin{array}{rccc}
Hom_R(P_n, f) : & Hom_R(P_n, N) & \longrightarrow & Hom_R(P_n, N') \\
 & g & \mapsto & f \circ g
\end{array}
$$

Ahora, en virtud de la Proposición 2.2.1, $Hom_R(\underline{P}, f)$ induce un morfismo de R-módulos:

$$H^n(Hom_R(\underline{P}, f)) : H^n(Hom_R(\underline{P}, N)) \longrightarrow H^n(Hom_R(\underline{P}, N')).$$

Ahora bien, se tiene que $H^n(Hom_R(\underline{P}, N)) = H^n(M, N; \underline{P}) = Ext^n_R(M, N)$ y $H^n(Hom_R(\underline{P}, N')) = H^n(M, N'; \underline{P}) = Ext^n_R(M, N')$. En vista de estas consideraciones, podemos dar la siguiente definición:

DEFINICIÓN 71 (**Functores Ext**). *Sea M un R-módulo y $n \in \mathbb{N}$. Se define el functor covariante $Ext^R_n(M, -)$ como sigue:*

i) A cada R-módulo N le asigna el R-módulo $Ext_n^R(M,N)$*;*

ii) a cada morfismo de R-módulos $f : N \longrightarrow N'$ *le asigna el morfismo de R-módulos:*

$$Ext_n^R(M,f) := H^n(Hom_R(\underline{P},f)) : Ext_n^R(M,N) \longrightarrow Ext_n^R(M,N'),$$

donde $\underline{P}$ *es una resolución proyectiva de* M*.*

Es fácil comprobar que $Ext_R^n(M,-)$ es un functor covariante. Ahora bien, si $f : N \longrightarrow N'$ es un morfismo de R-módulos y $\underline{P}$, $\underline{Q}$ son resoluciones proyectivas de M y $n \in \mathbb{N}$, consideremos el diagrama:

$$\text{(B.2.6)} \qquad \begin{array}{ccc} H^n(M,N;\underline{P}) & \xrightarrow{H^n(Hom_R(\underline{P},f))} & H^n(M,N';\underline{P}) \\ {\scriptstyle H^n(Id_M,N;\underline{Q},\underline{P})}\uparrow & & \uparrow{\scriptstyle H_n(Id_M,N';\underline{Q},\underline{P})} \\ H^n(M,N;\underline{Q}) & \xrightarrow{H^n(Hom_R(\underline{Q},f))} & H^n(M,N';\underline{Q}) \end{array}$$

Notemos que $H^n(Id_M,N;\underline{Q},\underline{P}) = H^n(Hom_R(F,N))$ y $H^n(Id_M,N';\underline{Q},\underline{P}) = H^n(Hom_R(F,N'))$ para cualquier $F : \underline{P} \longrightarrow \underline{Q}$ aplicación de cadena sobre Id_M. Pero, para cada $g \in Hom_R(Q_n,N)$ se verifica:

$$\begin{aligned}(Hom_R(P_n,f)\circ Hom_R(F_n,N))(g) &= Hom_R(P_n,f)(Hom_R(F_n,N)(g)) = Hom_R(P_n,f(g\circ F_n)) \\ &= f\circ g\circ F_n = (Hom_R(Q_n,f)(g))\circ F_n = (Hom_R(F_n,N')\circ Hom_R(Q_n,f))(g).\end{aligned}$$

Entonces, se sigue que:

$$H^n(Hom_R(\underline{P},f))\circ H^n(Hom_R(F,N)) = H^n(F,N')\circ H^n(\underline{Q},N),$$

de donde se sigue la conmutatividad del Diagrama (B.2.6). Además, por la Proposicion 2.4.2, se tiene que $H_n(Id_M,N;\underline{Q},\underline{P})$ y $H_n(Id_M,N';\underline{P},\underline{Q})$ son isomorfismos. Por consiguiente, $H^n(Hom_R(\underline{P},f)) = Ext_R^n(M,f)$ es independiente de la resolución proyectiva $\underline{P}$ de M elegida (salvo composición con isomorfismos).

Consideremos ahora un R-módulo M, una resolución proyectiva $(\underline{P},\epsilon)$ de M y una sucesión exacta de R-módulos:

$$0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0.$$

Como P_n es un R-módulo proyectivo, $Hom_R(P_n,-)$ es un functor exacto para todo $n \in \mathbb{N}$, i.e.

$$0 \longrightarrow Hom_R(P_n,N') \longrightarrow Hom_R(P_n,N) \longrightarrow Hom_R(P_n,N'') \longrightarrow 0$$

es una sucesión exacta de R-módulos para todo $n \in \mathbb{N}$. Por tanto la sucesión de complejos de cadena:

$$\mathcal{P}: \qquad 0 \longrightarrow Hom_R(\underline{P},N') \longrightarrow Hom_R(\underline{P},N) \longrightarrow Hom_R(\underline{P},N'') \longrightarrow 0$$

es exacta y, en virtud de la Proposición 2.2.2, existen morfismos conectores:

$$\partial^n : Ext_R^n(M,N'') = H^n(Hom_R(\underline{P},N'')) \longrightarrow H^{n+1}(Hom_R(\underline{P},N')) = Ext_R^{n+1}(M,N'), \quad n \in \mathbb{N}.$$

Veamos ahora que estos morfismos conectores no dependen de la resolución proyectiva $(\underline{P},\epsilon)$ de M elegida (salvo composición con isomorfismos). Sean $(\underline{P},\epsilon_P)$ y $(\underline{Q},\epsilon_Q)$ dos resoluciones proyectivas de M y $0 \longrightarrow N' \xrightarrow{i} N \xrightarrow{j} N'' \longrightarrow 0$ una sucesión exacta de R-módulos. Por la Proposición 2.3.2, existe $F : \underline{P} \longrightarrow \underline{Q}$ una aplicación de cadena sobre Id_M. En consecuencia, se tiene el siguiente diagrama conmutativo cuyas filas son sucesiones exactas:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Hom_R(\underline{P},N') & \xrightarrow{Hom_R(\underline{P},i)} & Hom_R(\underline{P},N) & \xrightarrow{Hom_R(\underline{P},j)} & Hom_R(\underline{P},N'') & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle Hom_R(F,N')} & & \uparrow{\scriptstyle Hom_R(F,N)} & & \uparrow{\scriptstyle Hom_R(F,N'')} & & \\ 0 & \longrightarrow & Hom_R(\underline{Q},N') & \xrightarrow{Hom_R(\underline{Q},i)} & Hom_R(\underline{Q},N) & \xrightarrow{Hom_R(\underline{Q},j)} & Hom_R(\underline{Q},N'') & \longrightarrow & 0 \end{array}$$

Por la Proposición 2.2.4, se sigue que el siguiente diagrama es conmutativo para todo $n \in \mathbb{N}$:

$$\begin{array}{ccc} H^{n+1}(Hom_R(\underline{P},N')) & \xleftarrow{H^{n+1}(Hom_R(F,N'))} & H^{n+1}(Hom_R(\underline{Q},N')) \\ \uparrow{\scriptstyle \partial^n} & & \uparrow{\scriptstyle \partial^n} \\ H^n(Hom_R(\underline{P},N'')) & \xleftarrow{H^n(Hom_R(F,N''))} & H^n(Hom_R(\underline{Q},N'')), \end{array}$$

donde $H^{n+1}(Hom_R(F, N')) = H^{n+1}(Id_M, N'; \underline{Q}, \underline{P})$ y $H^n(Hom_R(F, N'')) = H_n(Id_M, N''; \underline{Q}, \underline{P})$ son isomorfismos (cf. Proposición B.2.2). Por tanto, estos morfismos conectores se denotarán por:

$$\partial^n(M; N'', N') : Ext_R^n(M, N'') \longrightarrow Ext_R^{n+1}(M, N').$$

Teorema B.2.3. *i) Sean N un R-módulo y $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ es una sucesión exacta de R-módulos. Entonces, las sucesiones:*

$$0 \longrightarrow Ext_R^0(M'', N) \longrightarrow \cdots \longrightarrow Ext_R^{n-1}(M'', N) \xrightarrow{Ext_R^{n-1}(g,N)} Ext_R^n(M, N) \xrightarrow{Ext_R^{n-1}(f,N)}$$
$$\xrightarrow{Ext_R^{n-1}(f,N)} Ext_R^{n-1}(M', N) \xrightarrow{\partial^{n-1}(M', M''; N)} Ext_R^n(M'', N) \longrightarrow \cdots$$

$$0 \longrightarrow Ext_R^0(N, M') \longrightarrow \cdots \longrightarrow Ext_R^{n-1}(N, M') \xrightarrow{Ext_R^{n-1}(N,f)} Ext_R^n(N, M) \xrightarrow{Ext_R^{n-1}(N,g)}$$
$$\xrightarrow{Ext_R^{n-1}(N,g)} Ext_R^{n-1}(N, M'') \xrightarrow{\partial^{n-1}(N; M'', M')} Ext_R^n(N, M') \longrightarrow \cdots$$

son exactas.

ii) Si el diagrama:

(B.2.7)
$$\begin{array}{cccccccccc}
\mathcal{M}: & 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\
& & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\
\mathcal{K}: & 0 & \longrightarrow & K' & \longrightarrow & K & \longrightarrow & K'' & \longrightarrow & 0,
\end{array}$$

cuyas filas son sucesiones exactas de R-módulos, es conmutativo, entonces, los diagramas:

$$\begin{array}{ccc}
Ext_R^{n-1}(M', N) & \xrightarrow{\partial^{n-1}(M'', M'; N)} & Ext_R^n(M'', N) \\
\uparrow{\scriptstyle Ext_R^n(f', N)} & & \uparrow{\scriptstyle Ext_R^n(f'', N)} \\
Ext_R^{n-1}(K', N) & \xrightarrow{\partial^{n-1}(K', K''; N)} & Ext_R^n(K'', N)
\end{array}
\qquad
\begin{array}{ccc}
Ext_R^{n-1}(N, M'') & \xrightarrow{\partial^{n-1}(N; M'', M')} & Ext_R^n(M', N) \\
\downarrow{\scriptstyle Ext_R^n(N, f'')} & & \downarrow{\scriptstyle Ext_R^n(N, f')} \\
Ext_R^{n-1}(N, K'') & \xrightarrow{\partial^{n-1}(N; K'', K')} & Ext_R^n(N, K')
\end{array}$$

son conmutativos para todo $n \in \mathbb{N}$, $n \geq 1$.

iii) El functor $Ext_R^n(M, N)$ es lineal en M y N para todo $n \in \mathbb{N}$.

iv) Existe un isomorfismo $Ext_R^0(M, N) \cong Hom_R(M, N)$ que es functorial en M y N.

v) Si P es un R-módulo proyectivo, entonces $Ext_R^n(P, N) = 0$ para todo R-módulo N y todo $n \in \mathbb{N}$ con $n \geq 1$.

Demostración. *i)* La primera de las sucesiones es exactamente la sucesión del apartado *ii)* del Lema B.2.1, que es exacta. Para comprobar la exactitud de la segunda se aplica la Proposición 2.2.3 a la sucesión exacta de complejos de co-cadena:

$$0 \longrightarrow Hom_R(\underline{Q}, M') \longrightarrow Hom_R(\underline{Q}, M) \longrightarrow Hom_R(\underline{Q}, M'') \longrightarrow 0,$$

donde $\underline{Q}$ es una resolución proyectiva cualquiera de N.

ii) Por una parte, tomemos resoluciones proyectivas $0 \longrightarrow \underline{P}' \longrightarrow \underline{P} \longrightarrow \underline{P}'' \longrightarrow 0$ y $0 \longrightarrow \underline{Q}' \longrightarrow \underline{Q} \longrightarrow \underline{Q}'' \longrightarrow 0$ de $\mathcal{M}$ y $\mathcal{K}$ respectivamente. Por la Proposición 2.3.2, se tiene que existen aplicaciones de cadena $F' : \underline{P}' \longrightarrow \underline{Q}'$ y $F'' : \underline{P}'' \longrightarrow \underline{Q}''$ sobre f' y f'' respectivamente. Ahora, en virtud de la Proposición 2.3.4, existe una aplicación de cadena $F : \underline{P} \longrightarrow \underline{Q}$ sobre f que hace el Diagrama (B.2.1) conmute. Ahora estamos en las condiciones del apartado *iii)* del Lema B.2.1. En consecuencia, el Diagrama (B.2.2), que es precisamente el primer diagrama del apartado *ii)*, conmuta. De otro lado, si $\underline{P}$ es una resolución proyectiva cualquiera de N, como el Diagrama (B.2.7) es conmutativo, también lo será el diagrama:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & Hom_R(\underline{P}, M') & \longrightarrow & Hom_R(\underline{P}, M) & \longrightarrow & Hom_R(\underline{P}, M'') & \longrightarrow & 0 \\
& & \downarrow{\scriptstyle Hom_R(\underline{P}, f')} & & \downarrow{\scriptstyle Hom_R(\underline{P}, f)} & & \downarrow{\scriptstyle Hom_R(\underline{P}, f'')} & & \\
0 & \longrightarrow & Hom_R(\underline{P}, K') & \longrightarrow & Hom_R(\underline{P}, K) & \longrightarrow & Hom_R(\underline{P}, K'') & \longrightarrow & 0
\end{array}$$

Aplicando la Proposición 2.2.4 al diagrama anterior, se sigue que el diagrama:

$$\begin{array}{ccc} H^{n-1}(Hom_R(\underline{P}, M'')) & \xrightarrow{\partial^{n-1}} & H^n(Hom_R(\underline{P}, M')) \\ {\scriptstyle H^{n-1}(Hom_R(\underline{P},f''))}\downarrow & & \downarrow{\scriptstyle H^n(Hom_R(\underline{P},f'))} \\ H^{n-1}(Hom_R(\underline{P}, K'')) & \xrightarrow{\partial'^{n-1}} & H^n(Hom_R(\underline{P}, K')) \end{array}$$

donde ∂^{n-1} y ∂'^{n-1} son los morfismos conectores correspondientes, es conmutativo. Es decir, el segundo diagrama del apartado *ii*) es conmutativo. *iii*) De un lado, sean $k, l : N \longrightarrow N'$ morfismos de R-módulos; $a, b \in R$; $\underline{P}$ una resolución proyectiva de un R-módulo M. Entonces, para cada $n \in \mathbb{N}$, se tiene que:

$$\begin{aligned} aExt^n_R(M, k) + bExt^n_R(M, l) &= aH^n(Hom_R(\underline{P}, k)) + bH^n(Hom_R(\underline{P}, l)) \\ = H^n(Hom_R(\underline{P}, ak)) + H^n(Hom_R(\underline{P}, bl)) &= H^n(Hom_R(\underline{P}, ak + bl)) = Ext^n_R(M, ak + bl). \end{aligned}$$

En consecuencia, se tiene la linealidad en N. De otro lado, sea N un R-módulo; $f, g : M \longrightarrow M'$ morfismos de R-módulos; $a, b \in R$; $(\underline{P}, \epsilon)$ y $(\underline{P}', \epsilon')$ resoluciones proyectivas de M y M' respectivamente; y $n \in \mathbb{N}$. Por la Proposición 2.3.2, existen aplicaciones de cadena $F, G : \underline{P} \longrightarrow \underline{P}'$ sobre f y g respectivamente. Entonces,

$$(af + bg) \circ \epsilon = a(f \circ \epsilon) + b(g \circ \epsilon) = a(\epsilon' \circ F_0) + b(\epsilon' \circ G_0) = \epsilon' \circ (aF_0 + bG_0).$$

Por tanto, $aF + bG$ es una aplicación de cadena sobre $af + bg$. En consecuencia,

$$\begin{aligned} Ext^n_R(af + bg, N) &= H^n(af + bg, N; \underline{P}', \underline{P}) = H^n(Hom_R(aF + bG, N)) \\ = H^n(Hom_R(aF, N) + Hom_R(bG, N)) &= H^n(aHom_R(F, N)) + H^n(bHom_R(G, N)) \\ = aH^n(Hom_R(F, N)) + bH^n(Hom_R(G, N)) &= aExt^n_R(f, N) + bExt^n_R(g, N), \end{aligned}$$

donde las igualdades se siguen de la linealidad del morfismo inducido por una aplicación de cadena (ver Proposición 2.2.1). Por tanto, $Ext^n_R(M, N)$ es lineal en M. *iv*) Sean N y M dos R-módulos, y sea $(\underline{P}, \epsilon)$ una resolución proyectiva de M. Entonces, como la sucesión $P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} M \longrightarrow 0$ es exacta y, como el functor $Hom_R(-, N)$ es exacto a izquierda, se sigue que la sucesión de R-módulos:

$$0 \longrightarrow Hom_R(M, N) \xrightarrow{Hom_R(\epsilon, N)} Hom_R(P_0, N) \xrightarrow{Hom_R(d_1, N)} Hom_R(P_1, N) \tag{B.2.8}$$

es exacta. En particular, $Hom_R(\epsilon, N)$ es monomorfismo de R-módulos y, por el Primer Teorema de Isomorfía, $Hom_R(M, N) \cong Im(Hom_R(\epsilon, N))$. Por exactitud de la Sucesión (B.2.8): $Ext^0_R(M, N) = ker(Hom_R(d_1, N)) = Im(Hom_R(\epsilon, N)) \cong Hom_R(M, N)$. Dicho isomorfismo se denotará por:

$$\begin{array}{rccl} \psi(M, N) : & Hom_R(M, N) & \longrightarrow & Ext^0_R(M, N) \\ & g & \mapsto & g \circ \epsilon = Hom_R(\epsilon, N)(g) \in Im(Hom_R(\epsilon, N)), \end{array}$$

para cada $g \in Hom_R(M, N)$. Veamos que $\psi(M, N)$ es functorial en M y N. Sea $f : M \longrightarrow M'$ un morfismo de R-módulos y sean $(\underline{P}, \epsilon)$, $(\underline{P}', \epsilon')$ resoluciones proyectivas de M y M' respectivamente. En virtud de la Proposición 2.3.2, podemos suponer que existe una aplicación de cadena $F : \underline{P} \longrightarrow \underline{P}'$ sobre f. Consideremos el siguiente diagrama:

$$\begin{array}{ccc} Ext^0_R(M, N) & \xleftarrow{\psi(M,N)} & Hom_R(M, N) \\ {\scriptstyle Ext^0_R(f,N)}\uparrow & & \uparrow{\scriptstyle Hom_R(f,N)} \\ Ext^0_R(M', N) & \xleftarrow{\psi(M',N)} & Hom_R(M', N) \end{array} \tag{B.2.9}$$

Utilizando F para evaluar $Ext^n_R(f, N)$, se tiene que:

$$\begin{aligned} (Ext^0_R(f, N) \circ \psi(M', N))(g) &= H^0(Hom_R(F, N)) \circ \psi(M', N)(g) = g \circ \epsilon' \circ F_0 \\ &= g \circ f \circ \epsilon = (\psi(M, N) \circ Hom_R(f, M))(g), \end{aligned}$$

de donde se sigue la conmutatividad del Diagrama (B.2.9). Esto prueba que $\psi(M, N)$ es functorial en M. De otro lado, si $g : N \longrightarrow N'$ es un morfismo de R-módulos y $\underline{P}$ es una resolución proyectiva de M, podemos considerar el diagrama:

$$
\begin{array}{ccc}
Ext^0_R(M,N) & \xleftarrow{\psi(M,N)} & Hom_R(M,N) \\
{\scriptstyle Ext^0_R(M,g)}\big\downarrow & & \big\downarrow{\scriptstyle Hom_R(M,g)} \\
Ext^0_R(M,N') & \xleftarrow{\psi(M,N')} & Hom_R(M,N')
\end{array}
\tag{B.2.10}
$$

Se tiene que:

$$
\begin{aligned}
(Ext^0_R(M,g)\circ\psi(M,N))(h) &= H^0(Hom_R(\underline{P},g))\circ(h\circ\epsilon) = g\circ h\circ\epsilon \\
&= (g\circ h)\circ\epsilon = (\psi(M,N')\circ Hom_R(M,g))(h),
\end{aligned}
$$

de donde se sigue la conmutatividad del Diagrama (B.2.10). Esto prueba que $\psi(M,N)$ es functorial en N. v) Si P es un R-módulo proyectivo, $0\longrightarrow P\xrightarrow{Id_P}P\longrightarrow 0$ es una resolución proyectiva de P. Utilizándola para calcular $Ext^n_R(M,N)$ se tiene que, como $P_n=0$ para todo $n\in N$ con $n\geq 1$, $H^n(Hom_R(\underline{P},N)) = Ext^R_n(M,N)=0$ para todo R-módulo N y todo $n\in\mathbb{N}$ con $n\geq 1$. □

Proposición B.2.4. *Sea R un anillo noetheriano y N un R-módulo. Las siguientes afirmaciones son equivalentes:*

i) N es inyectivo;
ii) $Ext^1_R(M,N)=0$ para todo R-módulo M;
iii) $Ext^j_R(M,N)=0$ para todo R-módulo M y todo $j\in\mathbb{N}$, $j\geq 1$;
iv) $Ext^1_R(M,N)=0$ para todo R-módulo M finitamente generado;
v) $Ext^1_R(\mathfrak{a},N)=0$ para todo ideal $\mathfrak{a}$ de R.

Demostración. $i)\Rightarrow ii)$ Sea M un R-módulo cualquiera. En virtud de la demostración de la Proposición 2.3.1, podemos considerar una sucesión exacta de R-módulos: $0\longrightarrow Q\xrightarrow{i} P\longrightarrow M\longrightarrow 0$, donde P es proyectivo. Por el apartado i) del Teorema 2.5.1, se tiene la sucesión exacta de R-módulos:

$$
Ext^0_R(P,N)\xrightarrow{Ext^0_R(i,N)} Ext^0_R(Q,N)\longrightarrow Ext^1_R(M,N)\longrightarrow Ext^1_R(P,N). \tag{B.2.11}
$$

Ahora bien, como P es proyectivo, en virtud de la Proposición 2.6.2, $Ext^1_R(P,N)=0$. Además, por el apartado iv) del Teorema 2.5.1, existen isomorfismos functoriales $Hom_R(P,N)\cong Ext^0_R(P,N)$ y $Hom_R(Q,N)\cong Ext^0_R(Q,N)$. Es decir, se tiene el diagrama conmutativo:

$$
\begin{array}{ccc}
Ext^0_R(P,N) & \xrightarrow{Ext^0_R(i,N)} & Ext^0_R(Q,N) \\
\big\downarrow & & \big\downarrow \\
Hom_R(P,N) & \xrightarrow{Hom_R(i,N)} & Hom_R(Q,N)
\end{array}
$$

Como N es inyectivo, en vista de la Observación 14, $Hom_R(i,N)$ es epimorfismo y, en consecuencia, también lo será $Ext^0_R(i,N)$. Por exactitud de la Sucesión (B.2.11), debe ser $Ext^1_R(M,N)=0$. $ii)\Rightarrow iii)$ Probémoslo por inducción. Si $n=1$ el resultado es cierto por hipótesis. Supongamos $n\geq 2$. Dado un R-módulo M consideramos una sucesión exacta de R-módulos: $0\longrightarrow Q\xrightarrow{i}P\longrightarrow M\longrightarrow 0$, donde P es proyectivo. En virtud de la afirmación i) del Teorema 2.5.1, se tiene la sucesión exacta: $Ext^{n-1}_R(Q,N)\longrightarrow Ext^n_R(M,N)\longrightarrow Ext^n_R(P,N)$. Ahora bien, $Ext^{n-1}(Q,N)=0$ por hipótesis inductiva y como P es proyectivo, por la Proposición 2.6.2, $Ext^n_R(P,N)=0$. Luego por exactitud debe ser $Ext^n_R(M,N)=0$. $iii)\Rightarrow iv)$ Inmediato, pues iv) es un caso particular de iii). $iv)\Rightarrow v)$ Inmediato, pues como R es un anillo noetheriano, todo ideal de R es finitamente generado como R-módulo. $v\Rightarrow i)$ Para cada ideal $\mathfrak{a}$ de R se tiene la sucesión exacta de R-módulos: $0\longrightarrow\mathfrak{a}\xrightarrow{i}R\xrightarrow{\pi}R/\mathfrak{a}\longrightarrow 0$. De nuevo, por el Teorema 2.5.1, se tiene la sucesión exacta: $Ext^0_R(R,N)\xrightarrow{Ext^0_R(i,N)}Ext^0_R(\mathfrak{a},N)\longrightarrow Ext^1_R(R/\mathfrak{a},N)$. Los isomorfismos functoriales $Ext^0_R(R,N)\cong Hom_R(R,N)$ y $Ext^0_R(\mathfrak{a},N)\cong Hom_R(\mathfrak{a},N)$ garantizan la exactitud de la sucesión: $Hom_R(R,N)\xrightarrow{Hom_R(i,N)}Hom_R(\mathfrak{a},N)\longrightarrow Ext^1_R(R/\mathfrak{a},N)$. Ahora bien, por hipótesis se tiene que $Ext^1_R(R/\mathfrak{a},N)=0$. Por tanto, $Hom_R(i,N)$ es epimorfismo. Es decir, dado $f\in Hom_R(\mathfrak{a},N)$, existe $g\in Hom_R(R,N)$ tal que $g\circ i=f$. En virtud del Teorema de Baer (cf. Teorema A.5.1), N es inyectivo. □

Bibliografía

[Atiyah, 1969] M.F. Atiyah, I.G. Macdonald *Introduction to Conmutative Algebra*, Addison-Wesley Publishing Company, Inc., Massachusetts, 1969.

[Auslander-Buchsbaum, 1957] M. Auslander, D.A. Buchsbaum, *Homological dimension in local rings.*Trans. of the Amer. Math. Soc. **85** (1957), 390–405.

[Auslander-Buchsbaum, 1959] M. Auslander, D.A. Buchsbaum, *Unique factorization in regular local rings.* Proc. of the Nat. Acad. of Sci. of the USA **45** (1959), 733–734.

[Cohen, 1949] I.S. Cohen, *On the structure and ideal theory of complete local rings.* Trans. Amer. Math. Soc, **59** (1946), 54-106.

[Gordon-Jobson, 1973] R. Gordon and J. C. Robson, *Krull dimension, Memoirs Amer. Math. Soc No. 133* American Mathematical Society, Province, Rhode Island, 1973, 69-75.

[Hartshorne,1997] R. Hartshorne, *Algebraic Geometry* University of California, Berkeley, California, 1997

[Hatcher, 2002] Allen Hatcher *Algebraic Topology*, Cambridge University Press, 2002, 147-148.

[Nagata, 1958] M. Nagata, *A general theory of algebraic geometry over Dedekind domains. II. Separably generated extensions and regular local rings.* American J. of Math. **80** (1958), 382–420.

[Nagata, 1962] M. Nagata *Local Rings*, John Wiley and Sons, Inc. Kyoto, 1962, p. 203.

[Pardo, 21] L. M. Pardo, *"Algunas Notas para un curso de Álgebra Conmutativa"*. Manuscrito, UC, 2021.

[Raghavan et al., 1975] , S. Raghavan, R. Balwant Singh, R. Sridharan *Homological methods in Conmutative Algebra*, Tata Institute of Fundamental Research, Bombay, 1975.

[López, 21] , R. López Ruiz *La Ex-Conjetura de Serre: Teorema de Quillen-Suslin* Trabajo Fin de Grado, UC, Santander, 2021.

[Serre, 1955] J. P. Serre, *Sur la dimension homologique des anneaux et des modules noetheriens.* Proc. Intern. Symp. Alg. Number Theory, Tokyo, 1955, 175-190.

[Shafarevich, 2007] I.R. Shafarevich, *Basic Algebraic Geometry. Varieties in Projective Space. Third edition*, Steklov Mathematical Institute of the Russian Academy of Sciences Moscow, Russia, 2007.

[Weibel, 1994] Charles A. Weibel *An introduction to homological algebra*, Cambridge University Press, Cambridge, 1994.

[Zarinski-Samuel, 1958-60] O. Zariski, P. Samuel, *Conmutative Algebra*, Van Nostrand; vol. I (1958), vol. II (1960).