La Ex-Conjetura de Serre: Teorema de Quillen-Suslin

(Serre's Ex-Conjeture: Quillen-Suslin Theorem)

Rubén López Ruiz

Trabajo de Fin de Grado

para acceder al

Grado en Matemáticas

Facultad de Ciencias

Universidad de Cantabria

Director: Luis Miguel Pardo Vasallo

Septiembre - 2021

Agradecimientos

Me gustaría agradecer en primer lugar a mi director de TFG, Luis Miguel, toda la ayuda y esfuerzo prestado en la realización de este trabajo. Gracias también por darme un nuevo enfoque de las Matemáticas e introducirme de lleno en el Álgebra Conmutativa.

En segundo lugar, también aprovecho para agradecer a mis padres y a mi novia su apoyo en los momentos más difíciles de esta carrera. Por último, gracias a mis amigos por estar siempre ahí y ser un pilar dentro y fuera de la Universidad.

Abstract. This work is devoted to explore and present one of J. P. Serre's famous conjectures, proposed in the decade of 1950, and the affirmative answer that D. Quillen and A. A. Suslin gave to this conjecture in 1976. This result states that for finitely generated modules over polynomial rings with coefficients in a principal ideal domain, the conditions of projective and free module are equivalent. Before showing the proof of Serre's ex-conjecture, we will introduce the concept of local properties, whose study constitutes the context of this conjecture, as well as some instrumental theorems that are key in the proof. One of these is the so called Quillen-Suslin Theorem, and constitutes the final piece that led Quillen and Suslin to the solution of Serre's conjecture. The main goal of this work is to give Quillen's proof of Quillen-Suslin Theorem. Finally, we will present an application of Serre's ex-conjeture, in order to show that this abstract result has had a certain trascendence in the posterior development of Mathematics, particularly in Algebraic Geometry.

Resumen. Este trabajo se dedica a explorar y presentar una de las famosas conjeturas de J. P. Serre, planteadas en la década de 1950, y la respuesta afirmativa que D. Quillen y A. A. Suslin dieron a dicha conjetura en 1976. Este resultado afirma que para módulos finitamente generados sobre anillos de polinomios con coeficientes en un dominio de ideales principales, las condiciones de módulo proyectivo y libre son equivalentes. Antes de mostrar la prueba de la ex-conjetura de Serre, vamos a introducir el concepto de propiedades locales, cuyo estudio contextualiza esta conjetura, así como algunos resultados instrumentales que son clave en la demostración. Uno de estos es el llamado Teorema de Quillen-Suslin, el cual constituye la pieza final que llevó a Quillen y a Suslin a resolver la conjetura de Serre. El principal objetivo de este trabajo es dar la prueba de Quillen del Teorema de Quillen-Suslin. Para concluir, presentaremos una aplicación de la ex-conjetura de Serre, con el propósito de mostrar que este abstracto resultado ha tenido una cierta trascendencia en el desarrollo posterior de las Matemáticas, especialmente de la Geometría Algebraica.

Índice

Capítulo 0. Introducción y Resumen de Contenidos de la Memoria. i
0.1. Introducción i
0.1.1. Objetivos de este Trabajo Fin de Grado ii
0.2. Resumen de los contenidos de la Memoria iv
0.2.1. Resumen del Capítulo 1 iv
0.2.2. Resumen del Capítulo 2 vi
0.2.3. Resumen del Capítulo 3 vii
0.2.4. Apéndices Finales ix
0.2.5. Sobre el estilo y la ortografía usados en este TFG ix

Capítulo 1. Módulos Proyectivos y Libres: Trivialidad Local de los Módulos Proyectivos 1
1.1. Introducción 1
1.2. Propiedades Locales. Módulos Finitamente Presentados y Módulos Proyectivos 3
1.3. Libres y Proyectivos sobre anillos locales: Trivialidad Local 14

Capítulo 2. Resultados Instrumentales: Teoremas de Vaserstein y Horrocks. 23
2.1. Introducción 23
2.2. Cálculos matriciales con coordenadas en $R[X]$: equivalencia y el Teorema de Vaserstein. 24
2.3. Extensiones de módulos. Primer Teorema de Quillen. 28
2.4. Teorema de Horrocks. 29

Capítulo 3. El Teorema de Quillen-Suslin y algunas aplicaciones. 35
3.1. Introducción 35
3.1.1. Resumen relativo a la resolución final de la Ex-Conjetura de Serre 35
3.1.2. Una aplicación: trivialidad de anillos módulo sucesiones regulares con respecto a una normalización de Noether 36
3.2. El Teorema de Quillen-Suslin. 37
3.3. Respuestas a las preguntas de Serre. 40
3.4. Aplicación del Teorema de Quillen-Suslin al ejemplo paradigmático de anillo de Cohen-Macaulay 41
3.4.1. Trivialidad global de las intersecciones completas con respecto a una normalización de Noether 43

Apéndice A. Algunos Resultados Básicos de Álgebra Conmutativa 49
A.1. Definiciones básicas 49
A.2. Módulos libres 50
A.3. Módulo de fracciones. Localización 50
A.4. El functor $\mathrm{Hom}_R(M, -)$. 51
A.5. Producto tensorial de módulos 52
A.5.1. Propiedades del producto tensorial 52
A.5.2. Extensión de escalares 53
A.6. Lema de Nakayama 53
A.7. La Topología de Zariski en $\mathrm{Spec}(R)$ 53
A.8. Producto fibrado de módulos 54
A.9. Algunas demostraciones sobre propiedades locales citadas en el texto 55

Apéndice B. Noetherianos: Teorema de Lasker-Noether, Dimensión de Krull y Extensiones Enteras de anillos 59

B.1. Descomposición Primaria: El Teorema de Lasker-Noether 59
B.2. Breve resumen de propiedades de dimensión para intersecciones completas 61
B.3. Resumen, aún más breve, de la Normalización de Noether del cociente por un ideal intersección completa en $K[X_1, ..., X_n]$ 67

Apéndice. Glosario de Términos 71

Apéndice. Glosario de Teoremas y Resultados 73

Apéndice. Glosario de Símbolos y Abreviaturas 75

Apéndice. Bibliografía 77

CAPÍTULO 0

Introducción y Resumen de Contenidos de la Memoria.

Índice

0.1. Introducción **i**
0.1.1. Objetivos de este Trabajo Fin de Grado ii
0.2. Resumen de los contenidos de la Memoria **iv**
0.2.1. Resumen del Capítulo 1 iv
0.2.2. Resumen del Capítulo 2 vi
0.2.3. Resumen del Capítulo 3 vii
0.2.3.1. Resumen relativo a la resolución final de la Ex-Conjetura de Serre vii
0.2.3.2. Una aplicación: trivialidad de anillos módulo sucesiones regulares con respecto a una normalización de Noether viii
0.2.4. Apéndices Finales ix
0.2.5. Sobre el estilo y la ortografía usados en este TFG ix

0.1. Introducción

En la década de los 50 del pasado siglo, Jean-Pierre Serre planteó varias conjeturas que definieron la evolución del Álgebra Conmutativa en la segunda mitad del siglo, y que continúan influyendo en la forma del Álgebra Conmutativa. En este Trabajo Fin de Grado exponemos con sumo detalle la respuesta afirmativa que P. Quillen y A. A. Suslin dieron a una de estas conjeturas. Para explicar mejor el momento histórico en el que se enmarcan las Conjeturas de Serre, resumamos brevemente lo que estaba sucediendo en esa década.

En el primer tercio del pasado siglo, E. Noether asienta la concepción axiomática del Álgebra Conmutativa, lenguaje fundamental en el desarrollo posterior de la Geometría Algebraica, la Teoría Algebraica de Números o la Geometría Diofántica. El pensamiento de E. Noether, muy influenciado por la interpretación axiomática de D. Hilbert y E. Artin, se desarrolla de formas muy diversas. De una parte están sus contribuciones originales que ella misma publica: destaquemos el Teorema de Lasker-Noether o su generalización axiomática del Teorema de la Base de Hilbert, fundamentos de los llamados *anillos noetherianos*. Pero, de forma muy particular, el pensamiento de E. Noether también se asienta y expande a partir de su seminario casi permanente, sus conversaciones de pasillo y su generosidad intelectual. Alrededor de E. Noether se encuentra un elenco de matemáticos con quienes ella comparte su pensamiento, entre los que destacamos a W. Krull, B. L. van der Waerden o G. Hermann. Según cuentan los testigos, Noether está haciendo matemáticas en todo momento y aprovecha cualquier circunstancia para compartir ideas. Su pensamiento se propaga a través de obras esenciales como el texto clásico de W. Krull[1], fundamento del Álgebra Conmutativa. Más radical será la pasión de B. L. van der Waerden, un joven de apenas 27 años quien en sus textos fundamentales[2] y[3] introduce el concepto de "Álgebra Moderna" influenciado por el pensamiento de E. Noether.

E. Noether muere relativamente joven en Suiza, expulsada del sistema por su doble condición de mujer y judía, con el régimen nazi en Alemania. La Segunda Guerra Mundial disgregará este círculo de Noether, no sin que antes se produzca la expansión de esta forma de interpretar

[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 matematischen Wissenschaften **33**, Springer, (1930).

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

el Álgebra Conmutativa. Una de las más intensas fue la escuela japonesa (Akizuki, Azumaya, Nakayama...).

A principios de los años 50, el Álgebra Conmutativa se prepara para varios cambios significativos que resumiremos en unos pocos autores. De una parte, D. G. Northcott publica su texto sobre Teoría de ideales[4], que compila los resultados fundamentales sobre ideales en anillos noetherianos y que influirá textos clásicos de Álgebra Conmutativa como el [**Atiyah-Macdonald, 1969**]. De otra parte, A. Weil[5] introduce por primera vez el concepto de variedad algebraica abstracta (como el pegado de variedades afines) que tanto influirá en el pensamiento de la escuela de A. Grothendieck. Por su parte, C. Chevalley fortalecerá la influencia de la obra de Weil con su obra del año 1951[6].

Simultáneamente con estos avances se introduce en el año 1956 el "Álgebra Homológica" por H. Cartan y S. Eilenberg[7], cuyas ideas circulaban solamente entre los especialistas del ámbito. Mientras algunos autores mantienen el estilo clásico del entorno de Noether (como por ejemplo [**Atiyah-Macdonald, 1969**] o [**Zariski-Samuel, 1958-60**]), el ambiente general se va impregnando del Álgebra Homológica y las preguntas que produce.

Según escribe D. A. Buchsbaum, es el propio E. Artin quien en 1953-54 le pide que le explique el Álgebra Homológica. Buchsbaum le explica los functores Ext y Tor y diversos resultados conocidos como por ejemplo la "prueba homológica" del Teorema de la Base de Hilbert. Durante esos cursos, Artin sugiere que la misma prueba sirve para demostrar que todo anillo local regular tiene dimensión proyectiva finita. Con esta confesión de Buchsbaum podemos entender el ambiente que circula entorno a la nueva Álgebra Homológica.

Dos conjeturas se ven pronto influenciadas por este ambiente. Una de ellas, la "Conjetura de Artin", fue analizada independientemente por J. P. Serre en su trabajo de 1956, probando que los anillos locales regulares tienen dimensión homológica finita. De hecho, el objetivo esencial de esta "Conjetura de Artin-Serre" consiste en entender si las localizaciones de anillos locales regulares son locales regulares y si los anillos locales regulares son dominios de factorización única. El resultado de estas investigaciones es conocido como *Teorema de Auslander-Buchsbaum*[8], aunque M. Nagata[9] ya había probado el resultado para anillos locales regulares de dimensión mayor o igual que 3 en 1958.

La relevancia de este resultado, que no es tema de esta memoria, es que para probar que un cierto tipo de anillos (anillos locales regulares) son dominios de factorización única, se usan técnicas homológicas que no parecen relacionarse con las nociones involucradas. Esto supuso el espaldarazo definitivo del Álgebra Homológica dentro (y al lado) del Álgebra Conmutativa, y supuso una creciente marea de trabajo científico. Una buena expresión del Teorema de Auslander-Buchsbaum es el texto [**Rag *et al*, 1975**].

0.1.1. Objetivos de este Trabajo Fin de Grado.

Debemos insistir en que ninguna de las discusiones anteriores son el objetivo de este Trabajo Fin de Grado. Simplemente las exponemos para contrastar con el resultado que nos ocupa.

Para contextualizar este trabajo necesitamos hablar un poco de *propiedades locales* o del *Principio Local-Global*. Las propiedades locales son naturales en cualquier contexto matemático con una topología. Una propiedad local es aquella que puede establecerse tanto local como globalmente y que satisface que la propiedad es cierta localmente si y solo si es cierta globalmente. Por ejemplo, la propiedad "ser continua" es claramente una propiedad local. Dados dos espacios topológicos (X, τ) e (Y, τ') y una función $f : X \to Y$, f es continua (globalmente)

[4][Northcott, 1953] D. G. Northcott, *Ideal Theory*. Cambridge University Press, (1953).

[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).

[8][Auslander-Buchsbaum, 1959] M. Auslander, D. A. Buchsbaum, *Unique factorization in regular local rings*. Proc. Nat. Academy of Sciences of the USA. **45**, (1959), 733-734.

[9][Nagata, 1958] M. Nagata, *A general theory of algebraic geometry over Dedekind domains II. Separably generated extensions and regular local rings*. Amer. Journal of Mathematics **80**, (1958), 382-420.

si y solo si es continua localmente alrededor de cada punto $x \in X$. En cambio, en el mismo contexto topológico, la propiedad "ser homeomorfo" no es una propiedad local: la esfera unidad S^1 es localmente homeomorfa a la recta real $\mathbb{R}$ alrededor de cada punto $x \in S^1$, pero no es globalmente homeomorfa a $\mathbb{R}$.

En el contexto del Álgebra Conmutativa, el espacio topológico usual es el espectro primo de un anillo ($\mathrm{Spec}(R)$) dotado con la topología de Zariski (ver Apéndice A.7). Una propiedad local clásica es la propiedad de "ser cero" para R-módulos. Así, se prueba elementalmente que si M es un R-módulo, son equivalentes:

i) $M = 0$ como R-módulo,
ii) $M_{\mathfrak{p}} = 0$ como $R_{\mathfrak{p}}$-módulo, $\forall \mathfrak{p} \in \mathrm{Spec}(R)$, y
iii) $M_{\mathfrak{m}} = 0$ como $R_{\mathfrak{m}}$-módulo, $\forall \mathfrak{m} \in \mathrm{MaxSpec}(R)$,

donde $M_{\mathfrak{p}}$ y $M_{\mathfrak{m}}$ son respectivamente las localizaciones de M en el primo $\mathfrak{p} \in \mathrm{Spec}(R)$ o en el maximal $\mathfrak{m} \in \mathrm{MaxSpec}(R)$.

En los años en los que nos enmarcamos el interés por las propiedades locales es crítico y constituye la principal motivación de muchas investigaciones. De hecho, en la referencia de 1956[10], Auslander y Buchsbaum afirman que su principal motivación para el estudio de las preguntas de Artin era responder a la siguiente cuestión:

PROBLEMA 1 (Auslander-Buchsbaum-Serre). *Dado un anillo local regular $(R, \mathfrak{m})$ y un ideal primo $\mathfrak{p} \in \mathrm{Spec}(R)$, ¿es $R_{\mathfrak{p}}$ un anillo local regular?.*

La respuesta fue afirmativa, como ya se ha dicho, y el Teorema de Serre-Auslander-Buchsbaum usa extensivamente técnicas homológicas.

La Conjetura de Serre que afrontamos en esta memoria se enmarca en otra línea de pensamiento. En su trabajo [**Serre, 1960-61**], J. P. Serre se plantea la cuestión de saber si la propiedad *"ser libre"* es una propiedad local. Y, en algún sentido, tiene esperanza de que la respuesta es alcanzable y está ligada al desarrollo del Álgebra Homológica.

Recordemos, para enunciar la Conjetura, que un R-módulo P se dice proyectivo si el functor $\mathrm{Hom}_R(P, -)$ es exacto (ver Apéndice A.4 sobre dicho functor y Capítulo 1 sobre la noción de proyectivo).

CONJETURA 0.1.1 (**Conjetura de Serre** (sobre módulos libres y proyectivos)). Sea K un dominio de ideales principales, $R = K[X_1, ..., X_n]$ un anillo de polinomios con coeficientes en K. Sea M un R-módulo finitamente generado. Son equivalentes:

i) M es proyectivo.
ii) M es libre de rango finito.

Esta Conjetura difiere notablemente de la Conjetura de Artin del contexto histórico en el que se encuentra. En primer lugar, las nociones de proyectivo y libre no coinciden con total generalidad. De otra parte, los dominios de ideales principales son un objeto natural en esta pregunta. Un R-módulo es proyectivo si y solamente si es sumando directo de un R-módulo libre. Como ser libre implica ser proyectivo (ver Teorema 1.2.8) la Conjetura de Serre bien puede establecerse del modo siguiente:

CONJETURA 0.1.2 (**Conjetura de Serre** (versión 2)). Sea K un dominio de ideales principales, $R = K[X_1, ..., X_n]$ un anillo de polinomios con coeficientes en K. ¿Es la condición de ser libre hereditaria para sumandos directos en R-módulos finitamente generados?.

Se conocía, por ejemplo, que si R es un dominio de ideales principales, todo submódulo de un R-módulo libre finitamente generado es libre (ver [**Pardo, 2021**] para una prueba). Obviamente, los sumandos directos de R-módulos libres son isomorfos a submódulos, y por tanto, *sobre dominios de ideales principales los módulos finitamente generados son libres si y solo si son proyectivos.*

[10][Auslander-Buchsbaum, 1956], M. Auslander, D. A. Buchsbaum, *Homological dimensions in noetherian rings.* Proc. Nat. Academy of Sciences of the USA. **42**, (1959).

Pero además, Serre observa que la condición de ser proyectivo es equivalente a ser localmente proyectivo (ver Teorema 1.2.11). Más aún, sobre anillos locales noetherianos $(R, \mathfrak{m})$ un R-módulo finitamente generado es libre si y solo si es proyectivo. Por tanto, la Conjetura de Serre se convierte en una pregunta relativa a propiedades locales:

CONJETURA 0.1.3 (**Conjetura de Serre** (versión 3)). Sea K un dominio de ideales principales, $R = K[X_1, ..., X_n]$ un anillo de polinomios con coeficientes en K. ¿Es la condición de ser libre una propiedad local para R-módulos finitamente generados?. En otras palabras, si M es un R-módulo finitamente generado, ¿son equivalentes las propiedades siguientes?:

i) M es libre de rango finito.
ii) M es proyectivo.
iii) $M_{\mathfrak{p}}$ es un $R_{\mathfrak{p}}$-módulo proyectivo, $\forall \mathfrak{p} \in \mathrm{Spec}(R)$.
iv) $M_{\mathfrak{p}}$ es un $R_{\mathfrak{p}}$-módulo libre, $\forall \mathfrak{p} \in \mathrm{Spec}(R)$.

Hasta la fecha del trabajo esencial [**Serre, 1960-61**] se sabe que se dan las siguientes implicaciones:

$$i) \Longrightarrow ii) \Longleftrightarrow iii) \Longleftrightarrow iv).$$

La cuestión pasa a reducirse a averiguar si $ii) \Longrightarrow i)$ en este contexto. La presunción de Serre es que un uso masivo de términos homológicos puede responder a esta implicación.

La respuesta tardó mucho más tiempo que el Teorema de Serre-Auslander-Buchsbaum y, sobre todo, se resolvió sin usar técnicas del Álgebra Homológica. En algún sentido, el Teorema de Quillen-Suslin viene a decir que no solo con técnicas masivas de Álgebra Homológica se van a obtener respuestas a preguntas del Álgebra Conmutativa, ni siquiera a las formuladas desde la terminología del Álgebra Homológica.

En este Trabajo Fin de Grado pretendemos exponer la respuesta afirmativa que D. Quillen y A. A. Suslin dieron a la Ex-Conjetura de Serre. Esto es, pretendemos dar una demostración detallada del siguiente Teorema:

TEOREMA 0.1.4 ([**Quillen, 1976**], [**Suslin, 1976**]). *La respuesta a la pregunta/conjetura de Serre es afirmativa en cualquiera de las tres versiones anteriores establecidas.*

0.2. Resumen de los contenidos de la Memoria

En esta Sección vamos a exponer cuáles son los contenidos de los diferentes Capítulos de esta Memoria, y que conducen a demostrar el Teorema de Quillen-Suslin. Hemos descrito los contenidos Capítulo a Capítulo, con la intención de que esto ayude al lector a una mejor comprensión de la demostración.

0.2.1. Resumen del Capítulo 1.

En este Capítulo nos ocuparemos de asentar y demostrar las propiedades genéricas de los módulos proyectivos. Nos interesan esencialmente los módulos proyectivos finitamente presentados y/o finitamente generados. También nos interesa la relación entre las nociones de módulo proyectivo y módulo libre, así como las propiedades locales de ambas nociones. Todo el material incluido se orienta a poder resolver la Conjetura de Serre.

Comenzaremos con las propiedades locales (o Principio Local-Global en [**Kunz, 1985**]). Una propiedad verifica el Principio Local-Global si esta se satisface globalmente si y solamente si se satisface localmente. En Álgebra Conmutativa el concepto "local" hace referencia al espectro de un anillo ($\mathrm{Spec}(R)$) dotado con la topología de Zariski (ver Apéndice A.7). Hablaremos de propiedades locales y mostraremos algún ejemplo de estas reservando sus demostraciones para el Apéndice A.9.

Recordaremos la noción de R-módulo libre y, en especial, de R-módulo libre de rango finito. Esta noción aparece para generalizar de modo inmediato la situación con espacios vectoriales sobre un cuerpo. Así, si X e Y son dos R-módulos libres de rangos respectivos r y s, el estudio de sus morfismos de R-módulos $f : X \to Y$ se reduce, como en espacios vectoriales, al cálculo

matricial en $M_{s\times r}(R)$, con las particularidades de tener coordenadas en un anillo. Sin embargo, como es bien conocido, los R-módulos no suelen ser libres: por ejemplo todo grupo abeliano finito es un $\mathbb{Z}$-módulo finitamente generado que no es libre. Así que una primera idea pasa por entender qué otras formas hay de definir módulos libres y conocerlos. Por supuesto, también cabe preguntarse si la propiedad de ser libre es una propiedad local. En este contexto se inserta este Trabajo Fin de Grado.

La primera noción candidata a ser equivalente a módulo libre es la noción de *R-módulo proyectivo*. Un R-módulo se dice proyectivo si es *sumando directo de un R-módulo libre*. En la Proposición 1.2.6 se muestran diversas caracterizaciones de los módulos proyectivos. La razón para intentar estudiar la relación entre módulos libres y proyectivos se remonta a las ideas sobre $\mathbb{Z}$-módulos libres finitamente generados. Todo submódulo de un $\mathbb{Z}$-módulo libre finitamente generado es libre (cf. [**Pardo, 2021**] y sus referencias). En particular, si R es un dominio de ideales principales, todo R-módulo finitamente generado es libre si y solo si es proyectivo. Esto no es cierto si se suprime la hipótesis de finitamente generado. Por eso nos restringimos al caso de módulos finitamente generados.

Por una cuestión estética, siguiendo la estela de [**Kunz, 1985**], nos ocuparemos también de los *módulos finitamente presentados*. Una *presentación finita* de un R-módulo M es una sucesión exacta corta de la forma

$$0 \to K \to R^n \to M \to 0,$$

donde $n \in \mathbb{N}$ y K es un submódulo finitamente generado de R^n. En el caso en que el anillo R sea noetheriano, un R-módulo es finitamente generado si y solo si es finitamente presentados (ver Proposición 1.2.3), con lo que la diferencia entre finitamente generado y finitamente presentado no afecta a nuestro interés en la Conjetura de Serre; en ella se trata el anillo de polinomios $R = K[X_1, ..., X_n]$ con coeficientes en un dominio de ideales principales, que es, por el Teorema de la Base de Hilbert, un anillo noetheriano.

Tras estas consideraciones nos ocuparemos de algunas propiedades en la interacción entre las nociones de "libre" y "proyectivo". Así, en el Teorema 1.2.8 probaremos uno de los resultados clásicos sobre el tema:

$$\text{Libre} \implies \text{Proyectivo} \implies \text{Plano}.$$

Debemos señalar que, aunque se introduce aquí el término "plano", no trataremos más este concepto por no extender excesivamente el contenido de este Trabajo Fin de Grado.

En el Ejemplo 1.2.7 mostramos que hay sumandos directos de R-módulos libres de rango 1 que no son libres. Es decir, un ejemplo elemental de un R-módulo proyectivo que no es libre. De ahí lo excepcional de la Conjetura de Serre.

Seguidamente probaremos que la condición de "ser proyectivo" es una propiedad local. Esto se prueba en el Teorema 1.2.11, el cual reproducimos aquí para ayudar al lector:

Teorema 0.2.1 (**Ser proyectivo es una propiedad local**). *Sea P un R-módulo finitamente presentado. Son equivalentes:*

i) P es un R-módulo proyectivo.
ii) $P_{\mathfrak{p}}$ es un $R_{\mathfrak{p}}$-módulo proyectivo, $\forall \mathfrak{p} \in \operatorname{Spec}(R)$.
iii) $P_{\mathfrak{m}}$ es un $R_{\mathfrak{m}}$-módulo proyectivo, $\forall \mathfrak{m} \in \operatorname{MaxSpec}(R)$.

Dado que ser proyectivo es una propiedad local conviene estudiar qué sucede con ambas nociones en el caso de anillos locales. Este es el propósito de la Sección 1.3.

La primera observación constata que, en el caso finitamente generado sobre un anillo local, ser libre equivale a ser proyectivo. Se trata del Teorema 1.3.3, que reproducimos aquí:

Teorema 0.2.2 (**Libre y proyectivo en el ámbito local**). *Si $(R, \mathfrak{m})$ es un anillo local y M es un R-módulo finitamente generado, son equivalentes:*

i) M es un R-módulo libre de rango finito.
ii) M es un R-módulo proyectivo.

Esto nos lleva a reformular el Principio Local-Global de los módulos proyectivos mediante la propiedad "ser localmente libre". Se prueba en el Teorema 1.3.4, que reproducimos aquí:

TEOREMA 0.2.3 (**Proyectivo es ser localmente libre**). *Sea M un módulo finitamente generado sobre un anillo arbitrario R. Entonces las siguientes propiedades son equivalentes:*

i) M es proyectivo.
ii) M es finitamente presentado y localmente libre.

Dado que el anillo $R = K[X_1, ..., X_n]$ de la Conjetura de Serre es noetheriano, esta puede escribirse del modo siguiente:

CONJETURA 0.2.4 (**Conjetura de Serre** (ser libre es una propiedad local)). Sea K un dominio de ideales principales y $R = K[X_1, ..., X_n]$ un anillo de polinomios con coeficientes en K. Pruébese que para cada R-módulo M finitamente generado son equivalentes:

i) M es libre.
ii) M es localmente libre.

La Sección finaliza con un resultado que inspiró a Quillen en su tratamiento de la Conjetura de Serre, conocido como "Trivialidad Local de los Módulos Proyectivos", y que reproducimos aquí para ayudar al lector:

TEOREMA 0.2.5 (**Trivialidad Local de los Módulos Proyectivos**). *Sea P un R-módulo proyectivo finitamente generado. Supongamos que para $\mathfrak{p} \in \mathrm{Spec}(R)$, el $R_{\mathfrak{p}}$-módulo libre $P_{\mathfrak{p}}$ tiene rango r. Entonces existe un $f \in R \setminus \mathfrak{p}$ tal que P_f es un R_f-módulo libre de rango r.*

0.2.2. Resumen del Capítulo 2.

Este Capítulo está dedicado a probar algunos resultados instrumentales que serán esenciales en la prueba del Teorema de Quillen-Suslin.

La primera observación que debemos hacer es que la extensión de escalares (ver Apéndice A.5) preserva la condición de ser módulo libre. En otras palabras, como el producto tensorial conmuta con la suma directa de R-módulos, si $R \subseteq B$ es una extensión de anillos y F es un R-módulo libre, entonces $B \otimes_R F$ es un B-módulo libre. Además, si F es de rango finito,

$$\mathrm{rank}_B(B \otimes_R F) = \mathrm{rank}_R(F).$$

Ahora si P es un R-módulo proyectivo, entonces es sumando directo de un R-módulo libre. Supongamos $F = P \oplus Q$, donde F es un R-módulo libre. De nuevo, como el producto tensorial conmuta con la suma directa, tendremos un isomorfismo de R-módulos

$$R[X] \otimes_R F \cong (R[X] \otimes_R P) \oplus (R[X] \otimes_R Q).$$

Por tanto, también la condición de ser proyectivo se preserva mediante la extensión de escalares $R \subseteq R[X]$. Escribiremos $M[X] = R[X] \otimes_R M$ para expresar el módulo obtenido por extensión de escalares. El argumento esencial del Teorema de Quillen-Suslin se sustenta en este juego de "subir" y "bajar" entre R-módulos y $R[X]$-módulos, usando que $R[X]$ es un R-módulo libre, y por tanto plano.

El otro aspecto esencial es el Álgebra Lineal con matrices tanto sobre R como $R[X]$. Nos interesa esencialmente la relación de equivalencia entre matrices con coordenadas en un anillo B. Dos matrices A_1 y A_2 en $M_{r\times s}(B)$ se dicen equivalentes si existen matrices regulares $P \in GL(r, B)$, $Q \in GL(s, B)$ tales que

$$A_1 = P \cdot A_2 \cdot Q.$$

En la Sección 2.2 los anillos que consideramos son esencialmente R y $R[X]$. Si $A(X) \in M_{r\times s}(R[X])$ es una matriz con coordenadas en $R[X]$, podemos especializar la variable X en $0 \in R$ y obtener la matriz $A(0) \in M_{r\times s}(R)$. La cuestión instrumental que trata el Teorema de Vaerstein es la propiedad "$A(X)$ es equivalente a $A(0)$". Este Teorema establece que se trata de una propiedad local. Reproducimos aquí el resultado para facilitar la lectura del texto:

TEOREMA 0.2.6 (**Teorema de Vaserstein**). *Sea $A(X) \in M_{r\times s}(R[X])$ una matriz con coordenadas en $R[X]$. Son equivalentes:*

- *$A(X)$ es equivalente a $A(0) \in M_{r\times s}(R)$.*
- *La imagen de $A(X)$ en $M_{r\times s}(R_{\mathfrak{m}}[X])$ es equivalente a la imagen de $A(0)$ en $M_{r\times s}(R_{\mathfrak{m}})$ para todo ideal maximal $\mathfrak{m} \in \mathrm{MaxSpec}(R)$.*

Junto al Teorema de Vaserstein hemos introducido una sección instrumental, la Sección 2.3, en la que exponemos el llamado Primer Teorema de Quillen. En él, Quillen se ocupa de los módulos extendidos, es decir los $R[X]$-módulos $M[X] = R[X] \otimes_R M$. Su caracterización local de la condición de "ser extendido" constituye el Primer Teorema de Quillen. Reproducimos este resultado aquí:

TEOREMA 0.2.7 (**Primer Teorema de Quillen**). *Un $R[X]$-módulo M finitamente presentado es extendido (i.e. de la forma $M = N[X]$) si y solamente es localmente extendido, es decir, si para cada ideal $\mathfrak{m} \in \mathrm{MaxSpec}(R)$, $M_{\mathfrak{m}}$ es un $R_{\mathfrak{m}}[X]$-módulo extendido.*

El resultado final de este Capítulo, el cual constituye la piedra angular del Teorema de Quillen-Suslin, es el Teorema de Horrocks. La Sección final del Capítulo se dedica a su enunciado y demostración. De nuevo, reproducimos aquí el resultado para facilitar la lectura:

TEOREMA 0.2.8 (**Teorema de Horrocks**). *Sea $(R, \mathfrak{m})$ un anillo local, y sea M un $R[X]$-módulo proyectivo finitamente generado. Supongamos que existe un polinomio mónico $f \in R[X]$ tal que M_f es libre como $R[X]_f$-módulo. Entonces, M es libre como $R[X]$-módulo.*

En ambos resultados (Primer Teorema de Quillen y Teorema de Horrocks) la equivalencia de matrices juega un papel fundamental.

0.2.3. Resumen del Capítulo 3.

El tercer y último Capítulo tiene un doble propósito: en primer lugar, vamos a culminar todos los esfuerzos técnicos precedentes para exhibir la resolución de la Ex-Conjetura de Serre; y en segundo lugar, vamos a dar una sencilla aplicación del Teorema de Quillen-Suslin que tuvo gran impacto en el desarrollo de algoritmos eficientes en Geometría Algebraica (a través de la corriente TERA) en la última década del siglo pasado. Presentaremos esos resultados en dos subsecciones separadas de esta introducción.

0.2.3.1. *Resumen relativo a la resolución final de la Ex-Conjetura de Serre.*

En los trabajos [**Quillen, 1976**] y [**Suslin, 1976**], D. Quillen y A. A. Suslin resolvieron simultánea e independientemente la Conjetura de Serre. El enunciado final se muestra y se prueba en la Sección 3.3 y se enuncia del modo siguiente:

TEOREMA 0.2.9. *Sea K un dominio de ideales principales, $R = K[X_1, ..., X_n]$ el anillo de polinomios en varias variables con coeficientes en K. Sea M un R-módulo finitamente generado. Son equivalentes:*

i) M es libre y finitamente presentado.
ii) M es proyectivo.
iii) $M_{\mathfrak{p}}$ es libre como $R_{\mathfrak{p}}$-módulo, $\forall \mathfrak{p} \in \mathrm{Spec}(R)$.
iv) $M_{\mathfrak{m}}$ es libre como $R_{\mathfrak{m}}$-módulo, $\forall \mathfrak{m} \in \mathrm{MaxSpec}(R)$.

Obviamente, y tras lo discutido en los Capítulos 1 y 2, la tarea se reduce a probar que $iv) \Longrightarrow i)$. La prueba es por inducción en n y tiene como ingrediente fundamental un Teorema que se enuncia y demuestra al comienzo de la Sección 3.2.

Ese elemento técnico esencial es también conocido como Teorema de Quillen-Suslin y consiste en probar que el Teorema de Horrocks es válido en el caso de cualquier anillo R. Es decir, la Sección 3.2 se dedica a probar el siguiente enunciado:

TEOREMA 0.2.10 (**Teorema de Quillen-Suslin**). *Sea R un anillo cualquiera y sea M un $R[X]$-módulo proyectivo finitamente generado. Sea $f \in R[X]$ un polinomio mónico tal que M_f es un $R_f[X]$-módulo libre. Entonces M es libre como $R[X]$-módulo.*

Cabe aclarar que la demostración de este resultado que se presenta aquí es la elaborada por Quillen. Esta utiliza resultados técnicos de Capítulos precedentes, como el Primer Teorema de Quillen o el Teorema de Horrocks. Adicionalmente, usa el producto fibrado de módulos de un modo excepcionalmente ingenioso para concluir sus propósitos. Esta demostración es el objetivo esencial del Trabajo Fin de Grado.

0.2.3.2. *Una aplicación: trivialidad de anillos módulo sucesiones regulares con respecto a una normalización de Noether.*
Este Trabajo Fin de Grado podría parecer hasta aquí excesivamente abstracto, aunque el Teorema de Quillen-Suslin sea uno de los momentos mágicos del Álgebra Conmutativa del pasado siglo. Por ello, hemos pretendido incluir una aplicación de este resultado; aunque pueda parecer un resultado poco trascendente. Así, en la Sección 3.4 probaremos el siguiente resultado:

TEOREMA 0.2.11. *Sea K un cuerpo algebraicamente cerrado y sea $\mathfrak{a} = (f_1, ..., f_r) \subseteq K[X_1, ..., X_n]$ un ideal de altura r generado por r elementos. Supongamos que tenemos unas nuevas variables $Y_1, ..., Y_n$ de tal modo que la siguiente es una extensión entera de anillos:*

$$A = K[Y_1, ..., Y_{n-r}] \hookrightarrow B = K[X_1, ..., X_n]/\mathfrak{a}.$$

Entonces B es un A-módulo libre de rango finito.

La familia de polinomios $\{f_1, ..., f_r\}$ que genera el ideal $\mathfrak{a}$ de altura r se suele denominar "sucesión secante". Las variables $\{Y_1, ..., Y_n\}$ que hacen que la extensión sea entera se dice que están "en posición de Noether". Luego el anillo de clases residuales de $K[X_1, ..., X_n]$ módulo un ideal generado por una sucesión secante es un módulo libre sobre una normalización de Noether.

A primera vista es solo un resultado técnico más. Supongamos que nuestra sucesión $\{f_1, ..., f_r\}$ secante satisface una propiedad más: el ideal $\mathfrak{a} = (f_1, ..., f_r)$ que genera es un ideal radical (i.e. $\sqrt{\mathfrak{a}} = \mathfrak{a}$). En ese caso se dice que la sucesión $\{f_1, ..., f_r\}$ es una *sucesión secante reducida* (o que la variedad de sus ceros $V = V_{\mathbb{A}}(\mathfrak{a})$ es una variedad intersección completa en el plano de los ideales). Si disponemos de una sucesión secante reducida y de una normalización de Noether de la forma siguiente:

$$A = K[Y_1, ..., Y_{n-r}] \hookrightarrow B = K[X_1, ..., X_n]/\mathfrak{a}. \tag{0.2.1}$$

Entonces B es un A-módulo libre de rango finito y la desigualdad de Bézout geométrica (en el espacio afín) de [**Heintz, 1983**] implica la siguiente cota para el rango de B:

$$\operatorname{rank}_A(B) \leq \prod_{i=1}^{r} \deg(f_i).$$

Ahora consideremos $F = Q(A)$ el cuerpo de fracciones de A y hagamos extensión de escalares

$$F = F \otimes_A A \hookrightarrow F \otimes_A B.$$

La extensión es algebraica cero-dimensional. En particular, $F \otimes_A B$ es un F-espacio vectorial de dimensión finita. Por ser B un A-módulo libre de rango finito, se tendrá:

$$D = \dim_F(F \otimes_A B) = \operatorname{rank}_A(B) \leq \prod_{i=1}^{r} \deg(f_i).$$

Más aún, los cálculos de eliminación en el anillo residual B se pueden releer como cálculos de eliminación en el espacio vectorial $F \otimes_A B$ de dimensión finita sobre F. En otras palabras, como la base de B como A-módulo libre se extiende a una base de $F \otimes_A B$ como F espacio vectorial, todos los cálculos matriciales relativos a la extensión $A \hookrightarrow B$ pueden hacerse como cálculos matriciales sobre el cuerpo F (es decir, en $M_D(F)$). Además, los elementos esenciales sobre endomorfismos $\varphi : B \to B$ se preservan si lo vemos como endomorfismo de espacios vectoriales $i \otimes \varphi : F \otimes_A B \to F \otimes_A B$.

Esta fue una de las ideas claves del desarrollo de los trabajos del colectivo TERA en la última década del siglo pasado (desde [**Pardo, 1995**] hasta [**GHMP, 1997**] o [**GHMMP, 1998**] y sus referencias). Estos autores desarrollaron el mejor algoritmo (el más eficiente posible) para la resolución simbólica de ecuaciones polinomiales multivariadas y, más tarde, probaron que era

imposible mejorar sus técnicas (salvo alguna mejora en el exponente constante, aspecto en el que han trabajado decenas de autores en cientos de publicaciones posteriores).

Estos aspectos no son tema de este Trabajo Fin de Grado, pero sirven para decir que el pequeño Teorema que se prueba en la Sección 3.4, como consecuencia del Teorema de Quillen-Suslin, no es un resultado sin trascendencia posterior.

0.2.4. Apéndices Finales.

El trabajo presentado se finaliza con 2 Apéndices para simplificar su lectura.

El Apéndice A contiene parte de la terminología básica usada en esta Memoria así como algunos resultados teóricos que o bien son básicos o son usados de manera transversal en las demostraciones exhibidas en la Memoria. Además, el Apéndice A.9 incluye las demostraciones de algunas propiedades locales citadas en el Capítulo 1.

En segundo lugar, en el Apéndice B se recogen algunos resultados relativos a anillos y módulos noetherianos, descomposición primaria, dimensión de Krull de anillos y módulos, y extensiones enteras. Se concluye este Apéndice con el Lema de Normalización de Noether. No todos los temas presentes tienen repercusión directa sobre los contenidos del trabajo, pero algunos de ellos son usados y conviene recogerlos de manera formal.

0.2.5. 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[11], juntamente con las reglas de estilo recomendadas por D. E. Knuth y co-autores para la Mathematical Association of America (MAA)[12].

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.).

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

CAPÍTULO 1

Módulos Proyectivos y Libres: Trivialidad Local de los Módulos Proyectivos

Índice

1.1. Introducción **1**
1.2. Propiedades Locales. Módulos Finitamente Presentados y Módulos Proyectivos **3**
1.3. Libres y Proyectivos sobre anillos locales: Trivialidad Local **14**

1.1. Introducción

En este Capítulo nos ocuparemos de asentar y demostrar las propiedades genéricas de los módulos proyectivos. Nos interesan esencialmente los módulos proyectivos finitamente presentados y/o finitamente generados. También nos interesa la relación entre las nociones de módulo proyectivo y módulo libre, así como las propiedades locales de ambas nociones. Todo el material incluido se orienta a poder resolver la Conjetura de Serre.

Comenzaremos con las propiedades locales (o Principio Local-Global en [**Kunz, 1985**]). Una propiedad verifica el Principio Local-Global si esta se satisface globalmente si y solamente si se satisface localmente. En Álgebra Conmutativa el concepto "local" hace referencia al espectro de un anillo (Spec(R)) dotado con la topología de Zariski (ver Apéndice A.7). Hablaremos de propiedades locales y mostraremos algún ejemplo de estas reservando sus demostraciones para el Apéndice A.9.

Recordaremos la noción de R-módulo libre y, en especial, de R-módulo libre de rango finito. Esta noción aparece para generalizar de modo inmediato la situación con espacios vectoriales sobre un cuerpo. Así, si X e Y son dos R-módulos libres de rangos respectivos r y s, el estudio de sus morfismos de R-módulos $f : X \to Y$ se reduce, como en espacios vectoriales, al cálculo matricial en $M_{s\times r}(R)$, con las particularidades de tener coordenadas en un anillo. Sin embargo, como es bien conocido, los R-módulos no suelen ser libres: por ejemplo todo grupo abeliano finito es un $\mathbb{Z}$-módulo finitamente generado que no es libre. Así que una primera idea pasa por entender qué otras formas hay de definir módulos libres y conocerlos. Por supuesto, también cabe preguntarse si la propiedad de ser libre es una propiedad local. En este contexto se inserta este Trabajo Fin de Grado.

La primera noción candidata a ser equivalente a módulo libre es la noción de *R-módulo proyectivo*. Un R-módulo se dice proyectivo si es *sumando directo de un R-módulo libre*. En la Proposición 1.2.6 se muestran diversas caracterizaciones de los módulos proyectivos. La razón para intentar estudiar la relación entre módulos libres y proyectivos se remonta a las ideas sobre $\mathbb{Z}$-módulos libres finitamente generados. Todo submódulo de un $\mathbb{Z}$-módulo libre finitamente generado es libre (cf. [**Pardo, 2021**] y sus referencias). En particular, si R es un dominio de ideales principales, todo R-módulo finitamente generado es libre si y solo si es proyectivo. Esto no es cierto si se suprime la hipótesis de finitamente generado. Por eso nos restringimos al caso de módulos finitamente generados.

Por una cuestión estética, siguiendo la estela de [**Kunz, 1985**], nos ocuparemos también de los *módulos finitamente presentados*. Una *presentación finita* de un R-módulo M es una sucesión exacta corta de la forma

$$0 \to K \to R^n \to M \to 0,$$

donde $n \in \mathbb{N}$ y K es un submódulo finitamente generado de R^n. En el caso en que el anillo R sea noetheriano, un R-módulo es finitamente generado si y solo si es finitamente presentados (ver Proposición 1.2.3), con lo que la diferencia entre finitamente generado y finitamente presentado no afecta a nuestro interés en la Conjetura de Serre; en ella se trata el anillo de polinomios $R = K[X_1, ..., X_n]$ con coeficientes en un dominio de ideales principales, que es, por el Teorema de la Base de Hilbert, un anillo noetheriano.

Tras estas consideraciones nos ocuparemos de algunas propiedades en la interacción entre las nociones de "libre" y "proyectivo". Así, en el Teorema 1.2.8 probaremos uno de los resultados clásicos sobre el tema:

$$\text{Libre} \Longrightarrow \text{Proyectivo} \Longrightarrow \text{Plano}.$$

Debemos señalar que, aunque se introduce aquí el término "plano", no trataremos más este concepto por no extender excesivamente el contenido de este Trabajo Fin de Grado.

En el Ejemplo 1.2.7 mostramos que hay sumandos directos de R-módulos libres de rango 1 que no son libres. Es decir, un ejemplo elemental de un R-módulo proyectivo que no es libre. De ahí lo excepcional de la Conjetura de Serre.

Seguidamente probaremos que la condición de "ser proyectivo" es una propiedad local. Esto se prueba en el Teorema 1.2.11, el cual reproducimos aquí para ayudar al lector:

TEOREMA 1.1.1 (**Ser proyectivo es una propiedad local**). *Sea P un R-módulo finitamente presentado. Son equivalentes:*

i) P es un R-módulo proyectivo.
ii) $P_{\mathfrak{p}}$ es un $R_{\mathfrak{p}}$-módulo proyectivo, $\forall \mathfrak{p} \in \operatorname{Spec}(R)$.
iii) $P_{\mathfrak{m}}$ es un $R_{\mathfrak{m}}$-módulo proyectivo, $\forall \mathfrak{m} \in \operatorname{MaxSpec}(R)$.

Dado que ser proyectivo es una propiedad local conviene estudiar qué sucede con ambas nociones en el caso de anillos locales. Este es el propósito de la Sección 1.3.

La primera observación constata que, en el caso finitamente generado sobre un anillo local, ser libre equivale a ser proyectivo. Se trata del Teorema 1.3.3, que reproducimos aquí:

TEOREMA 1.1.2 (**Libre y proyectivo en el ámbito local**). *Si $(R, \mathfrak{m})$ es un anillo local y M es un R-módulo finitamente generado, son equivalentes:*

i) M es un R-módulo libre de rango finito.
ii) M es un R-módulo proyectivo.

Esto nos lleva a reformular el Principio Local-Global de los módulos proyectivos mediante la propiedad "ser localmente libre". Se prueba en el Teorema 1.3.4, que reproducimos aquí:

TEOREMA 1.1.3 (**Proyectivo es ser localmente libre**). *Sea M un módulo finitamente generado sobre un anillo arbitrario R. Entonces las siguientes propiedades son equivalentes:*

i) M es proyectivo.
ii) M es finitamente presentado y localmente libre.

Dado que el anillo $R = K[X_1, ..., X_n]$ de la Conjetura de Serre es noetheriano, esta puede escribirse del modo siguiente:

CONJETURA 1.1.4 (**Conjetura de Serre** (ser libre es una propiedad local)). Sea K un dominio de ideales principales y $R = K[X_1, ..., X_n]$ un anillo de polinomios con coeficientes en K. Pruébese que para cada R-módulo M finitamente generado son equivalentes:

i) M es libre.
ii) M es localmente libre.

La Sección finaliza con un resultado que inspiró a Quillen en su tratamiento de la Conjetura de Serre, conocido como "Trivialidad Local de los Módulos Proyectivos", y que reproducimos aquí para ayudar al lector:

TEOREMA 1.1.5 (**Trivialidad Local de los Módulos Proyectivos**). *Sea P un R-módulo proyectivo finitamente generado. Supongamos que para $\mathfrak{p} \in \mathrm{Spec}(R)$, el $R_\mathfrak{p}$-módulo libre $P_\mathfrak{p}$ tiene rango r. Entonces existe un $f \in R \setminus \mathfrak{p}$ tal que P_f es un R_f-módulo libre de rango r.*

1.2. Propiedades Locales. Módulos Finitamente Presentados y Módulos Proyectivos

Como ya hemos dicho en la Introducción, la Conjetura de Serre y su solución se enmarcan dentro del estudio de *propiedades locales* (según la terminología de [**Atiyah-Macdonald, 1969**]) o del *Principio Local-Global* (según el gusto de [**Kunz, 1985**]). Una propiedad P sobre un conjunto A se dice que es una propiedad local si la propiedad $P(A)$ se satisface si y solamente si se satisface con respecto a algún espacio topológico asociado. El ejemplo obvio es la condición de continuidad: una aplicación $f : X \to Y$ entre dos espacios topológicos (X, τ), (Y, τ') es continua si y solamente si es continua localmente (alrededor de cada punto). Así, "ser continua" es una propiedad local o, si se prefiere, satisface el Principio Local-Global. Sin salir del contexto topológico podemos encontrar ejemplos de propiedades topológicas que no son locales. Por ejemplo, "ser homeomorfo" no es una propiedad local, ya que toda variedad topológica de dimensión n es localmente homeomorfa a $\mathbb{R}^n$ (esta es, en esencia, la definición de variedad topológica) pero pocas son globalmente homeomorfas a $\mathbb{R}^n$ (el caso trivial). Un ejemplo muy concreto es la variedad topológica $S^1 := \{(x, y) \in \mathbb{R}^2 : \ x^2 + y^2 - 1 = 0\}$. Esta es localmente homeomorfa a $\mathbb{R}$, pero, obviamente, no es homeomorfa globalmente. En suma, la propiedad "ser homeomorfa" no satisface el Principio Local-Global.

En Álgebra Conmutativa, inspirados por propiedades de la Geometría Algebraica, las propiedades locales se estudian con respecto al espacio topológico natural asociado: el espectro primo de un anillo $\mathrm{Spec}(R)$, con la topología de Zariski (ver Apéndice A.7). Supongamos así que estudiamos propiedades de módulos sobre un anillo R fijado de antemano. Para un R-módulo M y un primo $\mathfrak{p} \in \mathrm{Spec}(R)$, el comportamiento "localmente alrededor de $\mathfrak{p}$" de M se analiza como el comportamiento del $R_\mathfrak{p}$-módulo $M_\mathfrak{p}$ (i.e. la localización en $\mathfrak{p}$ del R-módulo M, ver Apéndice A.3). El ejemplo clásico de propiedad local sobre módulos es la propiedad "ser cero" (cf. [**Atiyah-Macdonald, 1969**] para más detalles). Así, dado un R-módulo M son equivalentes:

i) $M = 0$ como R-módulo,
ii) $M_\mathfrak{p} = 0$ como $R_\mathfrak{p}$-módulo, $\forall \mathfrak{p} \in \mathrm{Spec}(R)$, y
iii) $M_\mathfrak{m} = 0$ como $R_\mathfrak{m}$-módulo, $\forall \mathfrak{m} \in \mathrm{MaxSpec}(R)$,

donde $\mathrm{MaxSpec}(R)$ son los ideales maximales de R y $\mathrm{Spec}(R)$ es el espectro primo, ambos con las respectivas topologías de Zariski.

En muchos casos, es relativamente asequible probar que si una propiedad se satisface globalmente, entonces se satisface localmente. La mayor dificultad reside, usualmente, en analizar cuándo una propiedad que se satisface localmente se satisface también globalmente. Comencemos con el ejemplo que encuadra la Conjetura de Serre:

DEFINICIÓN 1 (**Módulo libre**). *Diremos que un R-módulo M es libre si existe un conjunto X tal que M es isomorfo como R-módulo al R-módulo $\bigoplus_X R$ dado por la siguiente identidad:*

$$\bigoplus_X R := \{f : X \to R : \exists Y \text{ finito}, \ Y \subseteq X, \ f(x) = 0, \ \forall x \in X \setminus Y\}.$$

Se dice que M es un R-módulo libre de rango finito si X se puede elegir finito.

Una forma equivalente de introducir los R-módulos libres es la existencia de una base (i.e. un subconjunto $\mathcal{B} \subseteq M$ que es sistema generador de M como R-módulo y familia libre) de tal modo que si $\mathcal{B} \subseteq M$ es una base, entonces $M \cong \bigoplus_\mathcal{B} R$, con la notación precedente.

Puede probarse (cf. [**Pardo, 2021**] por ejemplo) que si M es un R-módulo libre de rango finito entonces todas sus bases tienen el mismo cardinal y a ese cardinal se le denomina *rango de M como R-módulo libre*:

$$\mathrm{rank}_R(M).$$

Nótese que si M es un R-módulo libre de rango finito con $n = \text{rank}_R(M)$, entonces $M \cong R^n$ como R-módulo. El recíproco es obviamente cierto también.

Como la localización es un functor exacto (cf. Proposición A.3.1), es sencillo probar el paso global $\longrightarrow$ local en el caso de R-módulos libres:

PROPOSICIÓN 1.2.1. *Sea M un R-módulo libre, entonces:*

i) $M_\mathfrak{p}$ es un $R_\mathfrak{p}$-módulo libre, $\forall \mathfrak{p} \in \text{Spec}(R)$. Además, si M es de rango finito y $n = \text{rank}_R(M)$, entonces $n = \text{rank}_{R_\mathfrak{p}}(M_\mathfrak{p})$.
ii) $M_\mathfrak{m}$ es un $R_\mathfrak{m}$-módulo libre, $\forall \mathfrak{m} \in \text{MaxSpec}(R)$. Además, si M es de rango finito y $n = \text{rank}_R(M)$, entonces $n = \text{rank}_{R_\mathfrak{m}}(M_\mathfrak{m})$.

La propiedad *ii)* anterior es, obviamente, una consecuencia de la propiedad *i)*. Como concretaremos más adelante, la Ex-Conjetura de Serre trata de describir algunos tipos de anillos para los cuales la propiedad *ii)* anterior implica que "M es un R-módulo libre", al menos para el caso de módulos libres de rango finito. En resumen, la Conjetura de Serre puede escribirse como:

Detectar si, para anillos de polinomios sobre dominios de ideales principales y para módulos finitamente generados, la propiedad "ser libre" es una propiedad local.

Antes de poder avanzar en la comprensión de esta Conjetura, vamos a recordar algunas propiedades locales que serán usadas más adelante en este Trabajo Fin de Grado. Nótese que en el caso de dominios de ideales principales la propiedad "ser libre" es una propiedad que admite el Principio Local-Global para módulos finitamente generados. Es decir, si R es un dominio de ideales principales, los R-módulos finitamente generados son los R-módulos libres de torsión y la propiedad "ser libre" es local (ver [**Pardo, 2021**] para una prueba detallada).

El siguiente resultado muestra propiedades locales de morfismos. Su demostración se propone en el Apéndice A.9.

PROPOSICIÓN 1.2.2. *Sea $f : M \to N$ un morfismo de R-módulos. Con las notaciones del Apéndice A.3, se tiene que:*

i) $Im(f_\mathfrak{p}) \cong Im(f)_\mathfrak{p}$, $\forall \mathfrak{p} \in \text{Spec}(R)$.
ii) $\text{coker}(f_\mathfrak{p}) \cong \text{coker}(f)_\mathfrak{p}$, $\forall \mathfrak{p} \in \text{Spec}(R)$.
iii) Las siguientes propiedades son equivalentes:
  (a) f es epimorfismo de R-módulos.
  (b) $f_\mathfrak{p}$ es epimorfismo de R-módulos, $\forall \mathfrak{p} \in \text{Spec}(R)$.
  (c) $f_\mathfrak{m}$ es epimorfismo de R-módulos, $\forall \mathfrak{m} \in \text{MaxSpec}(R)$.

DEFINICIÓN 2 (**Módulo finitamente presentado**). *Un R-módulo se dice finitamente presentado (o de presentación finita) si existe una sucesión exacta corta de la forma*

$$0 \to K \to F \to M \to 0,$$

donde

i) F es un R-módulo libre de rango finito, y
ii) $K \subseteq F$ es un submódulo finitamente generado.

A la sucesión exacta corta anterior se la denomina presentación finita de M.

Nótese que si un R-módulo admite una presentación finita, entonces es un R-módulo finitamente generado. Si R es un anillo noetheriano (como los $R = K[X_1, ..., X_n]$ que aparecen en la conjetura de Serre), ser finitamente generado equivale a ser finitamente presentado, como se prueba en la siguiente Proposición:

PROPOSICIÓN 1.2.3. *Todos los módulos finitamente generados sobre un anillo R noetheriano admiten una presentación finita.*

DEMOSTRACIÓN. Sea M un R-módulo finitamente generado con R anillo noetheriano. Entonces, existe un epimorfismo $\phi : R^n \longrightarrow M$ para algún $n \geq 1$. Además, tenemos que $\ker(\phi)$

es un ideal de R^n, y como R es noetheriano, R^n también lo es y $\ker(\phi)$ es un ideal finitamente generado. Por tanto, $K = \ker(\phi)$ es un R-módulo finitamente generado y

$$0 \to K \to R^n \xrightarrow{\phi} M \to 0$$

es una presentación finita de M. □

Si $\{v_1, ..., v_m\}$ es un sistema de generadores de K y escribimos una matriz A donde cada fila es v_i, tenemos que M está unívocamente determinado por A (salvo isomorfismo), $M \cong R^n/\langle v_1, ..., v_m\rangle$. En otras palabras, M es isomorfo al co-núcleo de la aplicación lineal $R^m \to R^n$ definida por A.

La siguiente Proposición muestra el comportamiento con respecto a la localización de la condición "ser finitamente presentado". La demostración se recoge en el Apéndice A.9.

PROPOSICIÓN 1.2.4. *Sean M, N dos R-módulos y $S \subset R$ multiplicativamente cerrado. El morfismo de R-módulos*

$$\begin{aligned} \mathrm{Hom}_R(M, N) &\to \mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N) \\ \alpha &\mapsto S^{-1}\alpha \end{aligned}$$

induce un morfismo de $S^{-1}R$-módulos

$$\begin{aligned} h : S^{-1}\,\mathrm{Hom}_R(M, N) &\to \mathrm{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N) \\ \frac{\alpha}{s} &\mapsto \mu_s^{-1} \circ S^{-1}\alpha, \end{aligned}$$

donde $\mu_s^{-1}(\frac{n}{s'}) = \frac{n}{s \cdot s'}$. En esta situación, tenemos que:

i) Si M es finitamente generado, h es inyectivo.
ii) Si M es finitamente presentado, h es isomorfismo.

La segunda noción esencial en este Trabajo Fin de Grado es la noción de R-módulo proyectivo, que podemos definir del modo siguiente:

DEFINICIÓN 3 (**Módulo Proyectivo**). *Un R-módulo M se denomina proyectivo si el functor covariante $\mathrm{Hom}_R(M, -)$ es exacto.*

El lector interesado en detalles sobre el bifunctor $\mathrm{Hom}_R(-,-)$ puede acudir al Apéndice A.4, o a las referencias básicas [**Atiyah-Macdonald, 1969**], [**Kunz, 1985**] o [**Pardo, 2021**] y las referencias que allí se citan. A continuación vamos a mostrar caracterizaciones equivalentes del hecho de ser proyectivo.

DEFINICIÓN 4 (**Sucesión exacta corta escindida**). *Se dice que una sucesión exacta corta de R-módulos*

$$0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \to 0 \tag{1.2.1}$$

es escindida si existe un isomorfismo $\phi : N \to M \oplus P$, de tal forma que $\phi \circ \alpha = i$ y $p \circ \phi = \beta$, donde $i : M \to M \oplus P$ es la inclusión canónica, y $p : M \oplus P \to P$ es la proyección canónica. Gráficamente, la sucesión (1.2.1) es escindida si existe un isomorfismo $\phi : N \to M \oplus P$ tal que el siguiente diagrama es conmutativo:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{\alpha} & N & \xrightarrow{\beta} & P & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle Id} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle Id} & & \\ 0 & \longrightarrow & M & \xrightarrow{i} & M \oplus P & \xrightarrow{p} & P & \longrightarrow & 0. \end{array}$$

EJEMPLO 1.2.5. *Si P es un R-módulo libre en (1.2.1), la sucesión es escindida. En efecto, sea $\mathcal{B} = \{p_i\}_{i \in I}$ una base de P como R-módulo libre. Definimos un morfismo de R-módulos $\gamma : P \to N$ del modo siguiente: para cada $i \in I$, escogemos un elemento $q_i \in N$ tal que $\beta(q_i) = p_i$ (se puede escoger porque β es sobreyectivo). Así, definimos*

$$\gamma(p_i) = q_i.$$

Claramente dado $p = \sum_{i\in I} r_i p_i$, *con* $r_i \in R$,

$$\beta(\gamma(p)) = \beta(\sum_{i\in I} r_i\gamma(p_i)) = \sum_{i\in I} r_i\beta(\gamma(p_i)) = \sum_{i\in I} r_i p_i = p = Id(p).$$

PROPOSICIÓN 1.2.6. *Sea* R *un anillo,* P *un* R*-módulo. Las siguientes afirmaciones son equivalentes:*

i) El R*-módulo* P *es proyectivo.*
ii) P *satisface la* LIFTING PROPERTY *siguiente:*
Sea $f : N \to M$ *un epimorfismo de* R*-módulos. Para todo morfismo de* R*-módulos* $g : P \to M$ *existe un morfismo* $h : P \to N$ *tal que* $f \circ h = g$.
iii) Dada una sucesión exacta corta de R*-módulos*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} P \to 0,$$

existe $h : P \to M$ *tal que* $g \circ h = Id_P$.
iv) Toda sucesión exacta corta de la forma

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} P \to 0$$

es escindida.
v) P *es un sumando directo de un* R*-módulo libre. Es decir, existe un* R*-módulo* Q *tal que* $F = P \oplus Q$ *es libre.*

DEMOSTRACIÓN. *i)* $\iff$ *ii)* Sabemos que el functor $\mathrm{Hom}_R(P, -)$ siempre es exacto a izquierda (Proposición A.4). Es decir, dada

$$0 \to N' \xrightarrow{g} N \xrightarrow{f} M \to 0$$

una sucesión exacta de R-módulos, la siguiente sucesión es exacta:

$$0 \to \mathrm{Hom}_R(P, N') \xrightarrow{\mathrm{Hom}_R(P,g)} \mathrm{Hom}_R(P, N) \xrightarrow{\mathrm{Hom}_R(P,f)} \mathrm{Hom}_R(P, M).$$

Para que $\mathrm{Hom}_R(P, -)$ sea exacto falta ver que dado $f : N \to M$ epimorfismo, entonces $\mathrm{Hom}_R(P, f) : \mathrm{Hom}_R(P, N) \to \mathrm{Hom}_R(P, M)$ es sobreyectivo, es decir, dado $g \in \mathrm{Hom}_R(P, M)$, existe $h \in \mathrm{Hom}_R(P, N)$ tal que $f \circ h = g$.
Pero esto es exactamente la lifting property tal y como está enunciada en *ii)*.

ii) $\implies$ *iii)* Dada la sucesión exacta corta

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} P \to 0,$$

consideramos el diagrama

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle Id_P} & & \\ M & \xrightarrow{g} & P & \longrightarrow & 0. \end{array}$$

Por ii) existe un morfismo $h : P \to M$ tal que $g \circ h = Id_P$.

iii) $\implies$ *iv)* Consideramos la sucesión exacta corta

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} P \to 0.$$

Aplicando *iii)*, existe $h : P \to M$ tal que $g \circ h = Id_P$. Entonces podemos construir el morfismo

$$\begin{aligned} \varphi : M &\to P \oplus M' \\ x &\mapsto (g(x), x - h(g(x))), \end{aligned}$$

que es isomorfismo de R-módulos. La aplicación φ está bien definida: dado $x \in M$, tenemos que

$$g(x - h(g(x))) = g(x) - g(h(g(x))) \overset{g\circ h = Id_P}{=} g(x) - g(x) = 0$$

y $x - h(g(x)) \in M' = \ker(g)$.

Claramente, φ es morfismo de R-módulos. Veamos que es isomorfismo.
- φ inyectivo: dado $x \in \ker(\varphi)$, tenemos que $(g(x), x - h(g(x))) = (0,0)$, lo cual implica que $g(x) = 0$, $0 = h(g(x)) = x$ y por tanto $x = 0$.
- φ sobreyectivo: sea $(p,k) \in P \oplus M'$. Si tomamos $x := h(p) + k \in F$, tenemos que

$$g(x) = g(h(p)) + g(k) = p$$

$$x - h(g(x)) = h(p) + k - h(p) = k.$$

Y con ello $\varphi(x) = (p,k)$.

Finalmente, es claro que, dado $m \in M'$,

$$\varphi(f(m)) = (g(f(m)), f(m) - h(g(f(m)))) = (0, f(m) - h(0)) = (0, f(m)) = i(m)$$

y además, dado $x \in M$,

$$p(\varphi(x)) = p(g(x), x - h(g(x))) = g(x).$$

iv) $\Longrightarrow$ *v)* Escogemos una sucesión exacta corta

$$0 \to K \to F \to P \to 0.$$

con F un R-módulo libre. Entonces, como la sucesión es escindida por hipótesis, $F \cong P \oplus K$ y P es un sumando directo de F.

v) $\Longrightarrow$ *ii)* Supongamos que existe un R-módulo Q tal que $P \oplus Q \cong F$ donde F es un R-módulo libre. Consideramos el diagrama

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle g} & & \\ N & \xrightarrow{f} & M & \longrightarrow & 0. \end{array}$$

Añadiendo Q como sumando directo,

$$\begin{array}{ccccc} & & P \oplus Q \cong F & & \\ & & \downarrow{\scriptstyle g \oplus Id_Q} & & \\ N \oplus Q & \xrightarrow{f \oplus Id_Q} & M \oplus Q & \longrightarrow & 0. \end{array}$$

Veamos ahora que los módulos libres satisfacen la lifting property. Tomamos el diagrama

$$\begin{array}{ccccc} & & F & & \\ & & \downarrow{\scriptstyle \tilde{g}} & & \\ \tilde{N} & \xrightarrow{\tilde{f}} & \tilde{M} & \longrightarrow & 0. \end{array}$$

Sea $\beta = \{e_i : i \in I\} \subseteq F$ una base de F. Entonces existe $\{m_i : i \in I\} \subseteq M$ tales que $\tilde{g}(e_i) = m_i, \forall i \in I$. Y como $\tilde{f}$ es sobreyectiva, existe $\{n_i : i \in I\} \subseteq N$ tales que $\tilde{f}(n_i) = m_i, \forall i \in I$. Ahora como F es libre, existe un único morfismo de R-módulos $\tilde{h} : F \to N$ que lleva e_i en n_i $\forall i \in I$. Y este morfismo $\tilde{h}$ verifica que $\tilde{f} \circ \tilde{h} = \tilde{g}$.

Volviendo a la demostración, como $P \subseteq F$ salvo isomorfismo, podemos tomar

$$h := \tilde{h}|_P : P \to N.$$

Claramente $f \circ h = g$. □

Ejemplo 1.2.7. *En el Ejemplo 1.2.5 anterior vimos que si P es un R-módulo libre, toda sucesión exacta corta de la forma*

$$0 \to N \to M \to P \to 0$$

es escindida. Por la Proposición precedente esto significa que todo módulo libre es proyectivo. El recíproco no es cierto en general. Un sencillo ejemplo es el siguiente: sea K un cuerpo y

consideremos el anillo $R = K \oplus K$. Dotamos a K de una estructura de R-módulo dada por la operación siguiente:

$$\cdot_R : R \times K \to K$$
$$((a,b),c) \mapsto (a,b) \cdot_R c = ac$$

Entonces, K es un R-módulo proyectivo, ya que R es libre como R-módulo y K es sumando directo de R. Pero K no es isomorfo a una suma directa de copias de $R = K \oplus K$, por lo que no puede ser libre como R-módulo.

Una noción que extiende a la de R-módulo proyectivo es la de R-módulo plano.

DEFINICIÓN 5 (**Módulo Plano**). *Un R-módulo M se dice plano si el functor $M \otimes_R -$ es exacto.*

TEOREMA 1.2.8. *Sea M un R-módulo. Entonces:*

$$M \text{ es libre} \implies M \text{ es proyectivo} \implies M \text{ es plano.}$$

Antes de dar la prueba del Teorema necesitamos un par de lemas previos.

Consideremos dos familias de R-módulos indicadas por el mismo conjunto de índices $\{M_i : i \in I\}, \{N_i : i \in I\}$. Consideremos también una familia de morfismos entre estos R-módulos $\{\varphi_i \in \mathrm{Hom}(M_i, N_i) : i \in I\}$. Entonces, existe un único morfismo de R-módulos entre las sumas directas

$$\psi = \bigoplus_{i\in I} \varphi_i : \bigoplus_{i\in I} M_i \to \bigoplus_{i\in I} N_i,$$

de tal modo que si $\lambda_i : M_i \to \bigoplus_{i\in I} M_i$ es la inclusión canónica, se tiene que

$$\psi \circ \lambda_i = \varphi_i, \quad \forall i \in I$$

LEMA 1.2.9. *Con las notaciones anteriores son equivalentes:*

i) Cada morfismo φ_i es inyectivo $\forall i \in I$.
ii) El morfismo suma directa $\psi = \bigoplus_{i\in I} \varphi_i$ es monomorfismo.

DEMOSTRACIÓN. Veamos ambas implicaciones por separado:

ii) $\implies$ *i)* Supongamos que ψ es inyectivo. Sabemos que λ_i es inyectivo. Por tanto, también será inyectiva la composición $\varphi_i = \psi \circ \lambda_i$.

i) $\implies$ *ii)* Supongamos ahora que los morfismos φ_i son todos inyectivos. Sea $m \in \ker(\psi)$ un elemento en el núcleo de ψ. Identificando cada M_i con el correspondiente submódulo de $\bigoplus_{i\in I} M_i$, existe $J \subseteq I$ finito, y para cada $j \in J$ existe $m_j \in M_j$ tales que

$$m = \sum_{j\in J} \lambda_j(m_j).$$

Por tanto, tendremos que

$$0 = \psi(m) = \sum_{j\in J} \psi(\lambda_j(m_j)) = \sum_{j\in J} \varphi_j(m_j).$$

Ahora, $\varphi_j(m_j) \in N_j \ \forall j \in J$, y por definición de la suma directa de R-módulos se tiene

$$0 = \sum_{j\in J} \varphi_j(m_j) = \sum_{j\in J} \varphi_j(m_j) + \sum_{i\in I\setminus J} 0 \implies \varphi_j(m_j) = 0, \ \forall j \in J.$$

Pero como φ_i es inyectiva para cada $i \in I$ concluimos que $m_j = 0 \ \forall j \in J$ y, por tanto, $m = \sum_{j\in J} \lambda_j(m_j) = 0$, lo que prueba la inyectividad de ψ. □

LEMA 1.2.10. *Sea $\{M_i : i \in I\}$ una familia de R-módulos. Son equivalentes:*

i) M_i es un R-módulo plano, $\forall i \in I$.
ii) $\bigoplus_{i\in I} M_i$ es un R-módulo plano.

Demostración. Primero recordemos que el producto tensorial es exacto a derecha siempre, por lo que basta estudiar el comportamiento con respecto a monomorfismos. Consideremos un monomorfismo de R-módulos $f : N' \to N$.

Ahora recordemos que el producto tensorial "conmuta" con la suma directa. Esto significa que tenemos el siguiente diagrama conmutativo donde ρ, τ son isomorfismos

$$\begin{array}{ccc} \bigoplus_{i\in I}(M_i \otimes_R N') & \xrightarrow{\oplus_{i\in I}(Id_i\otimes f)} & \bigoplus_{i\in I}(M_i \otimes_R N) \\ \downarrow \rho & & \downarrow \tau \\ (\bigoplus_{i\in I} M_i) \otimes_R N' & \xrightarrow{Id_0\otimes f} & (\bigoplus_{i\in I} M_i) \otimes_R N \end{array},$$

y donde $Id_i : M_i \to M_i$ es la identidad entre cada sumando, e $Id_0 : \bigoplus_{i\in I} M_i \to \bigoplus_{i\in I} M_i$ es la identidad entre las sumas directas. Observamos así que $Id_0 = \bigoplus_{i\in I} Id_i$.

Usando ahora el Lema precedente concluimos que $Id_0 \otimes f$ es un monomorfismo si y solamente si $Id_i \otimes f$ es un monomorfismo para cada $i \in I$. Por tanto, como esto es válido para cualquier monomorfismo $f : N' \to N$, si $\bigoplus_{i\in I} M_i$ es plano podemos concluir que M_i es plano para cada $i \in I$.

Recíprocamente, si M_i es plano para todo $i \in I$, entonces todo monomorfismo $f : N' \to N$ satisface que $Id_i \otimes f : M_i \otimes N' \to M_i \otimes N$ es monomorfismo para cada $i \in I$. Por el Lema precedente,

$$Id_0 \otimes f = (\bigoplus_{i\in I} Id_i) \otimes f \cong \bigoplus_{i\in I}(Id_i \otimes f)$$

será un monomorfismo, lo que prueba la platitud de $\bigoplus_{i\in I} M_i$, q.e.d. □

Con esto ya podemos dar la prueba del Teorema 1.2.8.

Demostración. (Teorema 1.2.8) En primer lugar, es evidente que si M es libre entonces es proyectivo, ya que los módulos proyectivos son los sumandos directos de los módulos libres ($M = M \oplus \{0\}$).

Veamos ahora que los módulos libres son planos. Para ello, observemos que el anillo R como R-módulo es plano. Esto es por el isomorfismo natural $R \otimes N \cong N$. Sea ahora M un R-módulo libre. Entonces, $M \cong \bigoplus_X R$. Usando el Lema precedente, como R es plano, entonces M debe ser un R-módulo plano.

Veamos finalmente que todo módulo proyectivo es plano. Por la Proposición 1.2.6, todo módulo proyectivo es sumando de un R-módulo libre. Es decir, si P es un R-módulo proyectivo existe un R-módulo libre F y un R-módulo Q tales que $F \cong P \oplus Q$. Como F es libre, entonces es plano, y por el Lema precedente sus sumandos directos también son planos. Así concluimos que P es plano, q.e.d. □

Teorema 1.2.11 (**Ser proyectivo es una propiedad local**). *Ser proyectivo es una propiedad local para módulos finitamente presentados. Es decir, sea P un R-módulo finitamente presentado. Son equivalentes:*

i) P es un R-módulo proyectivo.
ii) $P_\mathfrak{p}$ es un $R_\mathfrak{p}$-módulo proyectivo, $\forall \mathfrak{p} \in \mathrm{Spec}(R)$.
iii) $P_\mathfrak{m}$ es un $R_\mathfrak{m}$-módulo proyectivo, $\forall \mathfrak{m} \in \mathrm{MaxSpec}(R)$.

Demostración. Veamos en primer lugar que $i) \implies ii)$.

Como P es finitamente presentado, tomemos una sucesión exacta corta de la forma

$$0 \to K \to R^n \to P \to 0,$$

para algún $n \in \mathbb{N}$, siendo K un submódulo finitamente generado de R^n. Como P es proyectivo, esta sucesión es escindida, y por tanto tendremos que

$$R^n \cong P \oplus K.$$

Como la localización es un functor exacto, para cada $\mathfrak{p} \in \mathrm{Spec}(R)$ tendremos que

$$(R_{\mathfrak{p}})^n \cong (R^n)_{\mathfrak{p}} \cong P_{\mathfrak{p}} \oplus K_{\mathfrak{p}}.$$

Por tanto, $P_{\mathfrak{p}}$ es un sumando directo de un $R_{\mathfrak{p}}$-módulo libre y, por la Proposición 1.2.6, concluimos que $P_{\mathfrak{p}}$ es un $R_{\mathfrak{p}}$-módulo proyectivo.

Obviamente, *ii)* $\Longrightarrow$ *iii)*, ya que *iii)* es un caso particular de *ii)*.

Para probar *iii)* $\Longrightarrow$ *i)*, consideremos una sucesión exacta cualquiera de la forma siguiente:

$$0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \to 0 \tag{1.2.2}$$

Para cada ideal maximal $\mathfrak{m} \in \mathrm{MaxSpec}(R)$ tenemos la sucesión exacta corta obtenida por localización:

$$0 \to M_{\mathfrak{m}} \xrightarrow{\alpha_{\mathfrak{m}}} N_{\mathfrak{m}} \xrightarrow{\beta_{\mathfrak{m}}} P_{\mathfrak{m}} \to 0 \tag{1.2.3}$$

Como $P_{\mathfrak{m}}$ es proyectivo para cada $\mathfrak{m} \in \mathrm{MaxSpec}(R)$, la sucesión (1.2.3) es escindida $\forall \mathfrak{m} \in \mathrm{MaxSpec}(R)$. Veamos que entonces la sucesión original (1.2.2) es también escindida. En primer lugar, por la Proposición 1.2.2, el morfismo de R-módulos $\mathrm{Hom}_R(P, N) \to \mathrm{Hom}_R(P, P)$ es sobreyectivo si y solo si para todo $\mathfrak{m} \in \mathrm{MaxSpec}(R)$ el morfismo

$$\mathrm{Hom}_R(P, N)_{\mathfrak{m}} \to \mathrm{Hom}_R(P, P)_{\mathfrak{m}}$$

es sobreyectivo. Ahora como P es finitamente presentado, por la Proposición 1.2.4 este morfismo se identifica con

$$\mathrm{Hom}_{R_{\mathfrak{m}}}(P_{\mathfrak{m}}, N_{\mathfrak{m}}) \to \mathrm{Hom}_{R_{\mathfrak{m}}}(P_{\mathfrak{m}}, P_{\mathfrak{m}}).$$

Por tanto la sucesión (1.2.3) es escindida si y solo si este morfismo es sobreyectivo $\forall \mathfrak{m} \in \mathrm{MaxSpec}(R)$. □

COROLARIO 1.2.12. *Sea M un R-módulo finitamente presentado, $U \subset M$ un submódulo finitamente generado. Entonces M/U también es finitamente presentado, y además U es un sumando directo de M si y solo si $U_{\mathfrak{m}}$ es un sumando directo de $M_{\mathfrak{m}}$ para todo $\mathfrak{m} \in \mathrm{MaxSpec}(R)$.*

DEMOSTRACIÓN. Por hipótesis existe una sucesión $0 \to K \xrightarrow{\alpha} R^n \xrightarrow{\beta} M \to 0$ con K finitamente generado. Sea $\beta' : R^n \to M/U$ la composición de β con el homomorfismo canónico $M \to M/U$. Entonces como U y K son finitamente generados, $\ker(\beta') = \beta^{-1}(U)$ es finitamente generado. Por tanto, M/U es finitamente presentado.

Por otra parte, la segunda afirmación del Corolario se obtiene directamente del Teorema 1.2.11. □

PROPOSICIÓN 1.2.13. *Sean $f, g \in R$ con $D(f) \cup D(g) := \{\mathfrak{p} \in \mathrm{Spec}(R) : f \notin \mathfrak{p} \text{ ó } g \notin \mathfrak{p}\} = \mathrm{Spec}(R)$. Sea M un R-módulo tal que M_f es finitamente presentado como R_f-módulo y M_g es finitamente presentado como R_g-módulo. Entonces M es finitamente presentado como R-módulo.*

DEMOSTRACIÓN. En primer lugar, la hipótesis del enunciado $D(f) \cup D(g) = \mathrm{Spec}(R)$ es equivalente a decir que $1 \in (f, g) \subseteq R$ (o bien que $(f, g) = R$). Ahora, por la Proposición 1.2.4 sabemos que existe una sucesión exacta de R-módulos

$$0 \to K \to F \xrightarrow{\alpha} M,$$

con F un R-módulo libre de rango finito tal que la sucesión inducida

$$0 \to K_f \to F_f \xrightarrow{\alpha_f} M_f \to 0$$

es exacta y K_f es finitamente generado como R_f-módulo. Sea $0 \to K' \to F' \xrightarrow{\alpha'} M'$ la sucesión correspondiente construida para M_g. Entonces tenemos una sucesión exacta

$$0 \to U \to F \oplus F' \xrightarrow{(\alpha, -\alpha')} M \to 0,$$

donde

$$(\alpha, -\alpha') : F \oplus F' \to M$$
$$(x, y) \mapsto \alpha(x) - \alpha'(y)$$

y $U = \ker(\alpha, -\alpha')$. El morfismo $(\alpha, -\alpha')$ es sobreyectivo, puesto que si tomamos $m \in M$, sabemos que existe un $x_m \in F$ tal que $\alpha(x_m) = m$ (por ser α sobreyectivo). Con ello, $(\alpha, -\alpha')(x_m, 0) = \alpha(x_m) - \alpha(0) = m$.

Ahora solo faltaría ver que U es finitamente generado. En primer lugar, F y F' son R-módulos libres, luego cualquier localización suya sigue siendo libre. Con ello, F_f y F'_f son R_f módulos libres, y por tanto proyectivos. Además, por la exactitud del functor localización, los morfismos α_f y α'_f son sobreyectivos. Por tanto, tenemos el diagrama conmutativo siguiente:

$$\begin{array}{ccccc} & & F'_f & & \\ & \swarrow^{\varphi} & \downarrow{\scriptstyle \alpha'_f} & & \\ F_f & \xrightarrow[\alpha_f]{} & M & \longrightarrow & 0. \end{array}$$

Es decir, $\alpha_f \circ \varphi = \alpha'_f$. Consideremos entonces el siguiente diagrama conmutativo con filas y columnas exactas

$$\begin{array}{ccccccccc} & & 0 & & 0 & & & & \\ & & \downarrow & & \downarrow & & & & \\ & & G & = & G & & & & \\ & & \downarrow & & \downarrow & & & & \\ 0 & \longrightarrow & U_f & \longrightarrow & F_f \oplus F'_f & \longrightarrow & M_f & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \beta'} & & \downarrow{\scriptstyle \beta} & & \| & & \\ 0 & \longrightarrow & K_f & \longrightarrow & F_f & \longrightarrow & M_f & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & & & \\ & & 0 & & 0 & & & & \end{array}$$

donde β viene dada por $\beta(x, y) = x - \varphi(y)$, β' es el morfismo inducido por β y $G = \ker(\beta) = \ker(\beta')$. La columna del medio es escindida, puesto que F_f es libre como R_f-módulo. Con ello, tenemos que $F_f \oplus F'_f \cong G \oplus F_f$. Así, tomando la proyección $\pi : F_f \oplus F'_f \to G$, tenemos que G es la imagen por un epimorfismo de un R_f-módulo libre de rango finito (finitamente generado), luego G es finitamente generado como R_f-módulo. Como K_f es finitamente generado, U_f también lo es.

De forma análoga se prueba que U_g es finitamente generado como R_g-módulo. Por tanto, tenemos que U es un R-módulo finitamente generado. En efecto, supongamos que $x_1, ..., x_m \in U$ son elementos cuyas imágenes en U_f generan el R_f-módulo U_f, y que $y_1, ..., y_n \in U$ son elementos cuyas imágenes en U_g generan el R_g-módulo U_g, y sea $U' := \langle x_1, ..., x_m, y_1, ..., y_n \rangle$. Entonces $U_{\mathfrak{m}} = U'_{\mathfrak{m}}$ para todo $\mathfrak{m} \in \operatorname{MaxSpec}(R)$, ya que $\mathfrak{m} \in D(f)$ o $\mathfrak{m} \in D(g)$. En conclusión, $U = U'$ y U es finitamente generado. □

PROPOSICIÓN 1.2.14. *Dadas dos sucesiones exactas de R-módulos*

$$0 \to K_j \xrightarrow{\beta_j} F_j \xrightarrow{\alpha_j} M_j \to 0 \qquad (j = 1, 2),$$

donde F_1, F_2 son libres, tenemos que:

i) Si existe un isomorfismo $i : M_1 \to M_2$, entonces también existe un automorfismo $\alpha : F_1 \oplus F_2 \to F_1 \oplus F_2$ tal que el diagrama

$$\begin{array}{ccc} F_1 \oplus F_2 & \xrightarrow{(\alpha_1, 0)} & M_1 \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle i} \\ F_1 \oplus F_2 & \xrightarrow{(0, \alpha_2)} & M_2 \end{array} \tag{1.2.4}$$

es conmutativo. Además tenemos que $\alpha(K_1 \oplus F_2) = F_1 \oplus K_2$ *si identificamos* K_j *con* $\beta_j(K_j) \subset F_j$ $(j = 1, 2)$.

ii) Si existe un automorfismo $\alpha : F_1 \oplus F_2 \to F_1 \oplus F_2$ *con* $\alpha(K_1 \oplus F_2) = F_1 \oplus K_2$*, entonces existe un isomorfismo* $i : M_1 \to M_2$ *tal que el diagrama (1.2.4) es conmutativo.*

DEMOSTRACIÓN. *i)* Como F_1, F_2 son libres, dado un isomorfismo $i : M_1 \to M_2$ podemos encontrar morfismos de R-módulos $\gamma_1 : F_1 \to F_2$ y $\gamma_2 : F_2 \to F_1$ tales que los diagramas

$$\begin{array}{ccc} F_1 & \xrightarrow{\alpha_1} & M_1 \\ \downarrow{\scriptstyle \gamma_1} & & \downarrow{\scriptstyle i} \\ F_2 & \xrightarrow{\alpha_2} & M_2 \end{array} \qquad\qquad \begin{array}{ccc} F_1 & \xrightarrow{\alpha_1} & M_1 \\ {\scriptstyle \gamma_2}\uparrow & & \downarrow{\scriptstyle i} \\ F_2 & \xrightarrow{\alpha_2} & M_2 \end{array}$$

son conmutativos. Para $(x, y) \in F_1 \oplus F_2$ definimos

$$\alpha'(x, y) := (x, y - \gamma_1(x)),$$
$$\alpha''(x, y) := (x - \gamma_2(y), y).$$

Obviamente $\alpha', \alpha'' \in Aut(F_1 \oplus F_2) := \{\varphi : F_1 \oplus F_2 \to F_1 \oplus F_2\}$. Veamos que $\alpha = (\alpha')^{-1} \circ \alpha''$ es el automorfismo que buscamos.

Sabemos que

$$(i\alpha_1, \alpha_2)(\alpha''(x, y)) = i\alpha_1(x) - i\alpha_1\gamma_2(y) + \alpha_2(y) = (i \circ (\alpha_1, 0))(x, y)$$
$$(i\alpha_1, \alpha_2)(\alpha'(x, y)) = i\alpha_1(x) + \alpha_2(y) - \alpha_2\gamma_1(x) = (0, \alpha_2)(x, y).$$

Con ello, como $\alpha'' = \alpha' \circ \alpha$, resulta que $(0, \alpha_2) \circ \alpha = i \circ (\alpha_1, 0)$. Ahora como $\ker(\alpha_1, 0) = K_1 \oplus F_2$, $\ker(0, \alpha_2) = F_1 \oplus K_2$, tenemos directamente de lo anterior que $\alpha(K_1 \oplus F_2) = F_1 \oplus K_2$.

ii) Supongamos que existe $\alpha \in Aut(F_1 \oplus F_2)$ con $\alpha(K_1 \oplus F_2) = F_1 \oplus K_2$. En primer lugar, tenemos la sucesión exacta corta

$$0 \to K_1 \oplus F_2 \xrightarrow{\lambda_1} F_1 \oplus F_2 \xrightarrow{(\alpha_1, 0)} M_1 \oplus F_2 \to 0.$$

Observemos que $Im(\alpha_1, 0) = M_1 \oplus \{0\} \cong M_1$. Así que podemos considerar la sucesión exacta corta

$$0 \to K_1 \oplus F_2 \xrightarrow{\lambda_1} F_1 \oplus F_2 \xrightarrow{\tilde{\alpha_1}} M_1 \to 0$$

($\tilde{\alpha_1}$ es una interpretación de α_1). De igual modo, tenemos la sucesión exacta corta

$$0 \to F_1 \oplus K_2 \xrightarrow{\lambda_2} F_1 \oplus F_2 \xrightarrow{\tilde{\alpha_2}} M_2 \to 0.$$

Ahora consideramos la restricción del isomorfismo α a $K_1 \oplus F_2$

$$\alpha| : K_1 \oplus F_2 \to \alpha(K_1 \oplus F_2) = F_2 \oplus K_2,$$

que es un isomorfismo entre $K_1 \oplus F_2$ y $F_1 \oplus K_2$. De esta forma, tenemos el siguiente diagrama conmutativo donde las filas son exactas

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K_1 \oplus F_2 & \xrightarrow{\lambda_1} & F_1 \oplus F_2 & \xrightarrow{\tilde{\alpha_1}} & M_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha|} & & \downarrow{\scriptstyle \alpha} & & & & \\ 0 & \longrightarrow & F_1 \oplus K_2 & \xrightarrow{\lambda_2} & F_1 \oplus F_2 & \xrightarrow{\tilde{\alpha_2}} & M_2 & \longrightarrow & 0. \end{array}$$

Ahora vamos a definir el isomorfismo $i : M_1 \to M_2$. Sea $m_1 \in M_1$, existe $(x_1, y_1) \in F_1 \oplus F_2$ tal que $\tilde{\alpha_1}(x_1, y_1) = m_1$. Consideramos también $m_2 = \tilde{\alpha_2}(\alpha(x_1, y_1))$, y definimos $i(m_1) = m_2$. Es decir,

$$\begin{array}{ccc} (x_1, y_1) & \xmapsto{\tilde{\alpha_1}} & m_1 \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle i} \\ (x_2, y_2) := \alpha(x_1, y_1) & \xmapsto{\tilde{\alpha_2}} & m_2 \end{array}$$

Veamos que i está bien definida. Dados $(x_1, y_1), (x_1', y_1') \in F_1 \oplus F_2$ tales que $\tilde{\alpha_1}(x_1, y_1) = \tilde{\alpha_1}(x_1', y_1') = m_1$, entonces

$$(x_1', y_1') - (x_1, y_1) = (x_1' - x_1, y_1' - x_1') \in \ker(\tilde{\alpha_1})$$

y por tanto $x_1' - x_1 \in K_1$. Además,

$$\alpha|((x_1', y_1') - (x_1, y_1)) \in \ker(\tilde{\alpha_2}).$$

Pero esto significa que

$$\alpha(x_1', y_1') - \alpha(x_1, y_1) = \alpha|((x_1', y_1') - (x_1, y_1)) \in \ker(\tilde{\alpha_2}).$$

Es decir, que $\tilde{\alpha_2}(\alpha(x_1', y_1') - \alpha(x_1, y_1)) = 0$ y

$$\tilde{\alpha_2}(\alpha(x_1', y_1')) = m_2' = m_2 = \tilde{\alpha_2}(\alpha(x_1, y_1)).$$

Por tanto, i está bien definida. Además es obvio que es morfismo de módulos. Luego tenemos el diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K_1 \oplus F_2 & \xrightarrow{\lambda_1} & F_1 \oplus F_2 & \xrightarrow{\tilde{\alpha_1}} & M_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha|} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle i} & & \\ 0 & \longrightarrow & F_1 \oplus K_2 & \xrightarrow{\lambda_2} & F_1 \oplus F_2 & \xrightarrow{\tilde{\alpha_2}} & M_2 & \longrightarrow & 0. \end{array}$$

Del mismo modo, podíamos haber construido $j : M_2 \to M_1$ con el diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & F_1 \oplus K_2 & \xrightarrow{\lambda_2} & F_1 \oplus F_2 & \xrightarrow{\tilde{\alpha_2}} & M_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle (\alpha|)^{-1}} & & \downarrow{\scriptstyle \alpha^{-1}} & & \downarrow{\scriptstyle j} & & \\ 0 & \longrightarrow & K_1 \oplus F_2 & \xrightarrow{\lambda_1} & F_1 \oplus F_2 & \xrightarrow{\tilde{\alpha_1}} & M_1 & \longrightarrow & 0. \end{array}$$

Por último, veamos que

$$j \circ i = Id_{M_1} \qquad i \circ j = Id_{M_2}.$$

Sea $m_1 \in M_1$. Tomamos $(x_1, y_1) \in F_1 \oplus F_2$ con $\tilde{\alpha_1}(x_1, y_1) = m_1$. Entonces, $i(m_1) = \tilde{\alpha_2}(\alpha(x_1, y_1)) := m_2$. Ahora veamos cuanto vale $j(m_2)$. Sabemos que existe $(x_2, y_2) \in F_1 \oplus F_2$ con $\tilde{\alpha_2}(x_2, y_2) = m_2$. En particular podemos coger $(x_2, y_2) = \alpha(x_1, y_1)$. En este caso,

$$j(m_2) = \tilde{\alpha_1}(\alpha^{-1}(x_2, y_2)) = \tilde{\alpha_1}(\alpha^{-1}(\alpha(x_1, y_1))) = m_1.$$

Por tanto, $j(i(m_1)) = m_1$. De forma análoga tenemos que $i \circ j = Id_{M_2}$, y por tanto i es isomorfismo. □

Corolario 1.2.15. *Sean*

$$F_j' \xrightarrow{\beta_j} F_j \xrightarrow{\alpha_j} M_j \to 0 \qquad (j = 1, 2)$$

dos sucesiones exactas con F_j, F_j' R-módulos libres. Entonces $M_1 \cong M_2$ si y solo si existe un automorfismo $\alpha : F_1 \oplus F_2 \to F_1 \oplus F_2$ y un automorfismo $\beta : F_1' \oplus F_2 \oplus F_1 \oplus F_2' \to F_1' \oplus F_2 \oplus F_1 \oplus F_2'$ tal que el diagrama

$$\begin{array}{ccc} F_1' \oplus F_2 \oplus F_1 \oplus F_2' & \xrightarrow{(\beta_1 \oplus Id_{F_2}, 0)} & F_1 \oplus F_2 \\ \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \alpha} \\ F_1' \oplus F_2 \oplus F_1 \oplus F_2' & \xrightarrow{(0, Id_{F_1} \oplus \beta_2)} & F_1 \oplus F_2 \end{array} \tag{1.2.5}$$

es conmutativo.

Demostración. Veamos las dos implicaciones:

$\Longleftarrow$) Supongamos que el diagrama (1.2.5) es conmutativo. Por un lado, tenemos que

$Im(\beta_1 \oplus Id_{F_2}, 0) = \{(x, y) \in F_1 \oplus F_2 : \exists (z, t) \in F_1' \oplus F_2$ tal que $(x, y) = (\beta_1(z), t)\} = Im(\beta_1) \oplus F_2$.

Pero por la exactitud de las sucesiones, $Im(\beta_1) = \ker(\alpha_1) = K_1$. Del mismo modo,

$$Im(0, Id_{F_1} \oplus \beta_2 = F_1 \oplus Im(\beta_2) = F_1 \oplus K_2.$$

Además, por la conmutatividad del diagrama, $\alpha|_{K_1 \oplus F_2}(K_1 \oplus F_2) = F_1 \oplus K_2$. Finalmente, aplicando el apartado *ii)* de la Proposición 1.2.14, tenemos que $M_1 \cong M_2$.

$\Longrightarrow$) Consideramos $f : M_1 \to M_2$ un isomorfismo de R-módulos, y tenemos el diagrama siguiente

$$\begin{array}{ccccccc} F_1' & \xrightarrow{\beta_1} & F_1 & \xrightarrow{\alpha_1} & M_1 & \longrightarrow & 0 \\ & & & & \downarrow f & & \\ F_2' & \xrightarrow{\beta_2} & F_2 & \xrightarrow{\alpha_2} & M_2 & \longrightarrow & 0. \end{array}$$

De nuevo, definimos $K_1 = \ker(\alpha_1) = Im(\beta_1)$, $K_2 = \ker(\alpha_2) = Im(\beta_2)$, y tenemos el diagrama siguiente con filas exactas

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K_1 & \xrightarrow{\lambda_1} & F_1 & \xrightarrow{\alpha_1} & M_1 & \longrightarrow & 0 \\ & & & & & & \downarrow f & & \\ 0 & \longrightarrow & K_2 & \xrightarrow{\lambda_2} & F_2 & \xrightarrow{\alpha_2} & M_2 & \longrightarrow & 0. \end{array}$$

Ahora aplicando la Proposición 1.2.14 *i)* existe un automorfismo $\alpha : F_1 \oplus F_2 \to F_1 \oplus F_2$ con $\alpha(K_1 \oplus F_2) = F_1 \oplus K_2$, de forma que el siguiente diagrama es conmutativo y sus filas son exactas

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K_1 \oplus F_2 & \xrightarrow{\lambda_1} & F_1 \oplus F_2 & \xrightarrow{(\alpha_1, 0)} & M_1 & \longrightarrow & 0 \\ & & \downarrow \alpha| & & \downarrow \alpha & & \downarrow f & & \\ 0 & \longrightarrow & F_1 \oplus K_2 & \xrightarrow{\lambda_2} & F_1 \oplus F_2 & \xrightarrow{(0, \alpha_2)} & M_2 & \longrightarrow & 0. \end{array}$$

Ahora recordemos que $K_1 \oplus F_2 = Im(\beta_1 \oplus Id_{F_2})$ y $F_1 \oplus K_2 = Im(Id_{F_1} \oplus \beta_2)$. Además, $\alpha|$ es isomorfismo, y $\beta_1 \oplus Id_{F_2}, Id_{F_1} \oplus \beta_2$ son sobreyectivas, luego tenemos el diagrama conmutativo siguiente con filas exactas

$$\begin{array}{ccccccc} F_1' \oplus F_2 & \xrightarrow{\beta_1 \oplus Id_{F_2}} & K_1 \oplus F_2 & \longrightarrow & 0 \\ & & \downarrow \alpha| & & \\ F_1 \oplus F_2' & \xrightarrow{Id_{F_1} \oplus \beta_2} & F_1 \oplus K_2 & \longrightarrow & 0. \end{array}$$

Finalmente, aplicando de nuevo la Proposición 1.2.14 *i)* tenemos el resultado buscado. □

1.3. Libres y Proyectivos sobre anillos locales: Trivialidad Local

El objetivo de esta Sección es explorar la relación que existe entre módulos libres y proyectivos sobre anillos locales. Concluiremos la Sección con un resultado fundamental para la idea de Quillen sobre cómo resolver la Conjetura de Serre: la Trivialidad Local de los módulos proyectivos (Teorema 1.3.5). Observamos también que los conceptos de libre y proyectivo son coincidentes en el ámbito local (ver Teoremas 1.3.3 y 1.3.4).

LEMA 1.3.1. *Sea $(R, \mathfrak{m})$ un anillo local y M un R-módulo finitamente presentado. Entonces,*

i) M es un R-módulo finitamente generado y $\mu(M) < +\infty$.

ii) Si $\mu(M) = n$, entonces existe un módulo libre F de rango n y un submódulo $K \subseteq F$ finitamente generado tal que la siguiente es una sucesión exacta corta:

$$0 \to K \xrightarrow{i} F \xrightarrow{f} M \to 0,$$

donde i es la inclusión.

Demostración. *i)* Por definición de R-módulo finitamente presentado, M es la imagen por un epimorfismo de un R-módulo libre de rango finito. Es decir, tenemos $f : R^n \to M$ epimorfismo de R-módulos con $n \in \mathbb{N}$. Entonces si $\{e_i\}_{i=1,...,n}$ es la base canónica de R^n y $m_i := f(e_i)$, $i = 1, ..., n$, tenemos que $\{m_i\}_{i=1,...,n}$ es un sistema de generadores de $M = f(R^n)$.

ii) En primer lugar, recordemos que como consecuencia del Lema de Nakayama, si escribimos $k(\mathfrak{m}) = R/\mathfrak{m}$,

$$\mu(M) = dim_{k(\mathfrak{m})}(M/\mathfrak{m}M),$$

donde $M/\mathfrak{m}M$ es visto como $k(\mathfrak{m})$-espacio vectorial (Corolario A.6.2). Seguidamente, como M es finitamente presentado, tendremos una sucesión exacta corta de R-módulos:

$$0 \to K_0 \xrightarrow{\lambda} F_0 \xrightarrow{\pi} M \to 0,$$

con F_0 libre de rango finito y K_0 submódulo de F_0 finitamente generado.

Supongamos que $n = \mu(M) < +\infty$. Tendremos un epimorfismo de R-módulos $f : F = R^n \to M$. Sea $K = \ker(f)$. Entonces tendremos la siguiente sucesión exacta corta de R-módulos:

$$0 \to K \xrightarrow{i} R^n \xrightarrow{f} M \to 0,$$

donde i es la inclusión. Como F_0 es libre, es entonces proyectivo y tenemos el diagrama siguiente:

$$\begin{array}{ccccc} & & F_0 & & \\ & & \downarrow{\scriptstyle \pi} & & \\ R^n & \xrightarrow{f} & M & \longrightarrow & 0. \end{array}$$

Por tanto, existirá $\epsilon : F_0 \to R^n$ tal que el diagrama siguiente es conmutativo

$$\begin{array}{ccccc} & & F_0 & & \\ & \swarrow^{\epsilon} & \downarrow{\scriptstyle \pi} & & \\ R^n & \xrightarrow{f} & M & \longrightarrow & 0. \end{array}$$

Podemos reescribir este diagrama como

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K_0 & \xrightarrow{\lambda} & F_0 & \xrightarrow{\pi} & M & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle \epsilon} & & \updownarrow{\scriptstyle Id_M} & & \\ 0 & \longrightarrow & K & \xrightarrow{i} & R^n & \xrightarrow{f} & M & \longrightarrow & 0, \end{array}$$

donde las filas son sucesiones exactas cortas y el diagrama conmuta ($\pi = f \circ \epsilon$).

Consideremos ahora $x \in K_0$. Por ser exacta la fila superior tenemos que $x \overset{\lambda}{\longmapsto} \lambda(x) \overset{\pi}{\longmapsto} 0$. De otro lado, añadiendo la segunda fila tenemos que

$$\begin{array}{ccccc} x & \overset{\lambda}{\longmapsto} & \lambda(x) & \overset{\pi}{\longmapsto} & 0 \\ & & \downarrow{\scriptstyle \epsilon} & & \updownarrow{\scriptstyle Id_M} \\ & & \epsilon(\lambda(x)) & \overset{f}{\longmapsto} & 0 \end{array}$$

es decir, $f(\epsilon(\lambda(x))) = \pi(\lambda(x)) = 0$. Por tanto, $\epsilon(\lambda(x)) = 0$ y $i(K) = \ker(f)$. En conclusión, tenemos un morfismo de R-módulos $\epsilon \circ \lambda : K_0 \to K$. Hemos encontrado así un diagrama conmutativo con filas exactas

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K_0 & \xrightarrow{\lambda} & F_0 & \xrightarrow{\pi} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \epsilon\circ\lambda} & & \downarrow{\scriptstyle \epsilon} & & \uparrow{\scriptstyle Id_M} & & \\ 0 & \longrightarrow & K & \xrightarrow{i} & R^n & \xrightarrow{f} & M & \longrightarrow & 0. \end{array}$$

En la siguiente etapa procederemos a tensorizar con $R/\mathfrak{m}$. Las propiedades del functor covariante $R/\mathfrak{m} \otimes_R -$ (Apéndice A.5) nos dan el siguiente diagrama conmutativo cuyas filas son exactas:

$$\begin{array}{ccccccc} R/\mathfrak{m} \otimes_R K_0 & \xrightarrow{Id\otimes\lambda} & F_0/\mathfrak{m}F_0 & \xrightarrow{Id\otimes\pi} & M/\mathfrak{m}M & \longrightarrow & 0 \\ \downarrow{\scriptstyle Id\otimes(\epsilon\circ\lambda)} & & \downarrow{\scriptstyle Id\otimes\epsilon} & & \downarrow{\scriptstyle Id} & & \\ R/\mathfrak{m} \otimes_R K & \xrightarrow{Id\otimes i} & R^n/\mathfrak{m}R^n & \xrightarrow{Id\otimes f} & M/\mathfrak{m}M & \longrightarrow & 0. \end{array}$$

Nótese que hemos omitido las condiciones de ser monomorfismo. Ahora bien, $\mu(M) = n$, luego $M/\mathfrak{m}M$ es un $k(\mathfrak{m})$-espacio vectorial de dimensión n. Por su parte, $R^n/\mathfrak{m}R^n = (k(\mathfrak{m}))^n$ también es un $k(\mathfrak{m})$-espacio vectorial de dimensión n. Finalmente, $Id \otimes f$ es un epimorfismo entre dos $k(\mathfrak{m})$-espacios vectoriales de dimensión n, luego es un isomorfismo de espacios vectoriales.

A continuación, probaremos la siguiente

Afirmación. *$\epsilon : F_0 \to R$ es un epimorfismo de R-módulos.*

Demostración de la Afirmación. Por el diagrama anterior tenemos que $Id \otimes \pi$ es epimorfismo y acabamos de ver que $Id \otimes f$ es isomorfismo. Por tanto, como los cuadrados del diagrama conmutan, $Id \otimes \epsilon$ ha de ser epimorfismo de espacios vectoriales. Recordemos la forma de $Id \otimes \epsilon$

$$\begin{aligned} Id \otimes \epsilon : F_0/\mathfrak{m}F_0 &\to R^n/\mathfrak{m}R^n \\ z + \mathfrak{m}F_0 &\mapsto \epsilon(z) + \mathfrak{m}R^n \end{aligned}$$

Se trata de un epimorfismo de R-módulos. En particular, se concluye que $R^n \subseteq \epsilon(F_0) + \mathfrak{m}R^n$. Pues si $x \in R^n$, existe $z \in F_0$ tal que $x - \epsilon(z) \in \mathfrak{m}R^n$. Aplicando el Lema de Nakayama, como $(R, \mathfrak{m})$ es anillo local y R^n finitamente generado, concluimos que $R^n = \epsilon(F_0)$ y la afirmación queda demostrada.

Ahora a partir de la suprayectividad de ϵ es sencillo probar que $\epsilon \circ \lambda$ es epimorfismo de R-módulos. Sea $x \in K = \ker(f)$. Entonces existe $y \in F_0$ tal que $\epsilon(y) = x$. Y como el diagrama original era conmutativo, tenemos que $\pi(y) = f(\epsilon(y)) = 0$. Es decir, tenemos el siguiente dibujo

$$\begin{array}{ccccc} & & y & \xmapsto{\pi} & 0 \\ & & \downarrow{\scriptstyle \epsilon} & & \uparrow{\scriptstyle Id} \\ x & \xmapsto{i} & x & \xmapsto{f} & 0 \end{array}$$

En conclusión, $y \in \ker(\pi) = Im(\lambda)$, luego existirá $z \in K_0$ tal que $\lambda(z) = y$. Es decir, siguiendo el diagrama tiene la forma siguiente:

$$\begin{array}{ccccc} z & \xmapsto{\lambda} & y & \xmapsto{\pi} & 0 \\ & & \downarrow{\scriptstyle \epsilon} & & \uparrow{\scriptstyle Id} \\ x & \xmapsto{i} & x & \xmapsto{f} & 0 \end{array}$$

Luego $\epsilon \circ \lambda(z) = x$ y hemos probado que $\epsilon \circ \lambda$ es epimorfismo. Pero por ser M finitamente presentado, K_0 era un submódulo finitamente generado de F_0, y por tanto $K = (\epsilon \circ \lambda)(K_0)$ será también un R-módulo finitamente generado. □

Proposición 1.3.2. *Sea $(R, \mathfrak{m})$ un anillo local y M un R-módulo finitamente presentado. Entonces las afirmaciones siguientes son equivalentes:*

i) M es libre.

ii) Existe una sucesión exacta corta de R-módulos

$$0 \to K \xrightarrow{f} P \xrightarrow{g} M \to 0$$

donde P es proyectivo y, tensorizando por $R/\mathfrak{m}$, la siguiente es una sucesión exacta corta de $k(\mathfrak{m})$-espacios vectoriales

$$0 \to K/\mathfrak{m}K \xrightarrow{Id\otimes f} P/\mathfrak{m}P \xrightarrow{Id\otimes g} M/\mathfrak{m}M \to 0$$

donde las notaciones son las mismas que en el Lema precedente.

Demostración. $i) \Longrightarrow ii)$ Basta considerar la siguiente sucesión exacta corta

$$0 \to 0 \xrightarrow{i} M \xrightarrow{Id_M} M \to 0.$$

Como M es libre, entonces es proyectivo. Además, como $R/\mathfrak{m} \otimes_R -$ es exacto a derecha y $R/\mathfrak{m} \otimes_R 0 = 0$, tenemos la exactitud.

$ii) \Longrightarrow i)$ Nótese que por ser $R/\mathfrak{m} \otimes_R -$ exacto a derecha, la condición $ii)$ es equivalente a decir que $Id \otimes f : K/\mathfrak{m}K \to P/\mathfrak{m}P$ es un monomorfismo de R-módulos.

Seguidamente, obsérvese que en la demostración del Lema precedente hemos usado solamente que F_0 era un R-módulo proyectivo. Supongamos que $\mu(M) = n$ y, usando el Lema precedente, tendremos una sucesión exacta corta

$$0 \to K_0 \xrightarrow{i} F_0 = R^n \xrightarrow{\pi} M \to 0,$$

donde K_0 es un R-módulo finitamente generado e $i : K_0 \to F_0$ es la inclusión canónica. Repitiendo el argumento del Lema precedente, usando el hecho de que P es un R-módulo proyectivo, tendremos $\epsilon : P \to F_0$ un morfismo de R-módulos que hace que el siguiente diagrama sea conmutativo:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & K & \xrightarrow{f} & P & \xrightarrow{g} & M & \longrightarrow & 0 \\
 & & & & \downarrow{\scriptstyle \epsilon} & & \updownarrow{\scriptstyle Id_M} & & \\
0 & \longrightarrow & K_0 & \xrightarrow{i} & R^n & \xrightarrow{\pi} & M & \longrightarrow & 0.
\end{array}$$

Además, igual que en el Lema precedente, tendremos que ϵ es un epimorfismo de R-módulos y tendremos un morfismo $\epsilon \circ f : K \to K_0$ que será también epimorfismo. Tenemos así un diagrama conmutativo de la forma siguiente:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & K_1 & & K_2 & & & & \\
 & & \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle i_2} & & & & \\
0 & \longrightarrow & K & \xrightarrow{f} & P & \xrightarrow{g} & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \epsilon\circ f} & & \downarrow{\scriptstyle \epsilon} & & \updownarrow{\scriptstyle Id_M} & & \\
0 & \longrightarrow & K_0 & \xrightarrow{i} & R^n & \xrightarrow{\pi} & M & \longrightarrow & 0, \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

donde $K_1 = \ker(\epsilon \circ f)$, $K_2 = \ker(\epsilon)$ e i_1, i_2 son las inclusiones canónicas.

Veamos ahora que $f|_{K_1} : K_1 \to K_2$ define un isomorfismo de R-módulos. En primer lugar, observemos que $f(K_1) \subseteq K_2$. Para ello, sea $x \in K_1$. Entonces, $\epsilon(f(x)) = 0$ con lo que $f(x) \in \ker(\epsilon) = K_2$. Claramente por tanto, $f|_{K_1}$ es un morfismo de R-módulos, porque f lo es y la restricción de un morfismo a un submódulo sigue siendo morfismo. Veamos que $f|_{K_1}$ es epimorfismo. Sea $x \in K_2$. Entonces, $\epsilon(x) = 0$, con lo que $\pi(\epsilon(x)) = 0$. Por la conmutatividad del diagrama anterior, tendremos que $i_2(x) = x \in P$ y $g(x) = (\pi \circ \epsilon)(x) = 0$.

Luego $x \in \ker(g) = Im(f)$, y por tanto existe $y \in K$ tal que $x = f(y)$. Es decir, el diagrama con elementos sería el siguiente:

$$\begin{array}{ccccc} & & x & & \\ & & \downarrow{\scriptstyle i_2} & & \\ y & \xmapsto{f} & x & \xmapsto{g} & 0 \\ \downarrow{\scriptstyle \epsilon\circ f} & & \downarrow{\scriptstyle \epsilon} & & \\ (\epsilon\circ f)(y) & & 0 & \xmapsto{\pi} & 0. \end{array}$$

Entonces, $(\epsilon \circ f)(y) = \epsilon(f(y)) = \epsilon(x) = 0$, luego $y \in \ker(\epsilon \circ f) = K_1$. Por tanto, $x = f(y)$ con $y \in K_1$ y tenemos la suprayectividad de $f|_{K_1}$. En elementos, el diagrama será

$$\begin{array}{ccccc} y & \xmapsto{f|_{K_1}} & x & & \\ \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle i_2} & & \\ y & \xmapsto{f} & x & \xmapsto{g} & 0 \\ \downarrow{\scriptstyle \epsilon\circ f} & & \downarrow{\scriptstyle \epsilon} & & \\ \epsilon\circ f(y) & \xmapsto{i} & 0 & \xmapsto{\pi} & 0. \end{array}$$

De otro lado, f ya era monomorfismo de R-módulos, con lo que la restricción $f|_{K_1}$ también lo será. En conclusión, $f|_{K_1} : K_1 \to K_2$ es un isomorfismo de R-módulos. Esto nos genera el siguiente diagrama conmutativo:

$$\begin{array}{ccccccccc} & & 0 & & 0 & & & & \\ & & \downarrow & & \downarrow & & & & \\ & & K_1 & \xleftarrow{f|_{K_1}} & K_2 & & & & \\ & & \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle i_2} & & & & \\ 0 & \longrightarrow & K & \xrightarrow{f} & P & \xrightarrow{g} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \epsilon\circ f} & & \downarrow{\scriptstyle \epsilon} & & \updownarrow{\scriptstyle Id_M} & & \\ 0 & \longrightarrow & K_0 & \xrightarrow{i} & R^n & \xrightarrow{\pi} & M & \longrightarrow & 0. \\ & & \downarrow & & \downarrow & & & & \\ & & 0 & & 0 & & & & \end{array} \tag{1.3.1}$$

Ahora procedemos a tensorizar con $R/\mathfrak{m}$. El functor $R/\mathfrak{m} \otimes_R -$ es exacto a derecha y sabemos que una de las filas permanece exacta por la hipótesis ii). Tenemos entonces el siguiente diagrama conmutativo:

$$\begin{array}{ccccccccc} & & K_1/\mathfrak{m}K_1 & \xleftarrow{Id\otimes f|_{K_1}} & K_2/\mathfrak{m}K_2 & & & & \\ & & \downarrow{\scriptstyle Id\otimes i_1} & & \downarrow{\scriptstyle Id\otimes i_2} & & & & \\ 0 & \longrightarrow & K/\mathfrak{m}K & \xrightarrow{Id\otimes f} & P/\mathfrak{m}P & \xrightarrow{Id\otimes g} & M/\mathfrak{m}M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle Id\otimes(\epsilon\circ f)} & & \downarrow{\scriptstyle Id\otimes\epsilon} & & \updownarrow{\scriptstyle Id\otimes Id_M} & & \\ & & K_0/\mathfrak{m}K_0 & \xrightarrow{Id\otimes i} & R^n/\mathfrak{m}R^n & \xrightarrow{Id\otimes\pi} & M/\mathfrak{m}M & \longrightarrow & 0. \\ & & \downarrow & & \downarrow & & & & \\ & & 0 & & 0 & & & & \end{array} \tag{1.3.2}$$

Ahora volviendo al diagrama (1.3.1), como R^n es un R-módulo libre (y por tanto proyectivo), la sucesión corta vertical que termina en R^n es escindida y por tanto, seguirá siendo exacta al

tensorizar con $R/\mathfrak{m}$. Esto es porque el producto tensorial conmuta con la suma directa, por lo que si tenemos la sucesión exacta

$$0 \to K_2 \xrightarrow{i_2} P = K_2 \oplus R^n \xrightarrow{\epsilon} R^n \to 0,$$

tensorizando con $R/\mathfrak{m}$, la siguiente sucesión también será exacta:

$$0 \to R/\mathfrak{m} \otimes_R K_2 \xrightarrow{Id\otimes i_2} R/\mathfrak{m} \otimes_R (K_2 \oplus R^n) \xrightarrow{Id\otimes\epsilon} R/\mathfrak{m} \otimes_R R^n \to 0.$$

En suma, el diagrama (1.3.2) puede completarse de forma siguiente:

$$\begin{array}{ccccccccc}
 & & & & 0 & & & & \\
 & & & & \downarrow & & & & \\
 & & & & K_1/\mathfrak{m}K_1 & \xrightarrow{Id\otimes f|_{K_1}} & K_2/\mathfrak{m}K_2 & & \\
 & & & & \downarrow{\scriptstyle Id\otimes i_1} & & \downarrow{\scriptstyle Id\otimes i_2} & & \\
0 & \longrightarrow & K/\mathfrak{m}K & \xrightarrow{Id\otimes f} & P/\mathfrak{m}P & \xrightarrow{Id\otimes g} & M/\mathfrak{m}M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle Id\otimes(\epsilon\circ f)} & & \downarrow{\scriptstyle Id\otimes\epsilon} & & \downarrow{\scriptstyle Id\otimes Id_M} & & \\
 & & K_0/\mathfrak{m}K_0 & \xrightarrow{Id\otimes i} & R^n/\mathfrak{m}R^n & \xrightarrow{Id\otimes\pi} & M/\mathfrak{m}M & \longrightarrow & 0. \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

Nótese además que, como $\mu(M) = n$, tendremos que

$$n = dim_{k(\mathfrak{m})}(M/\mathfrak{m}M) = dim_{k(\mathfrak{m})}(R^n/\mathfrak{m}R^n) = dim_{k(\mathfrak{m})}((R/\mathfrak{m})^n).$$

Como $Id \otimes \pi$ es un epimorfismo entre dos espacios vectoriales de la misma dimensión, entonces $Id \otimes \pi$ es un isomorfismo de R-módulos y $\ker(Id \otimes \pi) = \{0\}$.

Si probamos que $Id \otimes i$ es un monomorfismo, habremos concluido que $K_0/\mathfrak{m}K_0 = \{0\}$. Consideramos $x + \mathfrak{m}K_0 \in K_0/\mathfrak{m}K_0$ tal que $(Id \otimes i)(x + \mathfrak{m}K_0) = 0 + \mathfrak{m}R^n$. Como $Id \otimes (\epsilon \circ f)$ es suprayectiva, existirá $y+\mathfrak{m}K \in K/\mathfrak{m}K$ tal que $(Id\otimes(\epsilon\circ f))(y+\mathfrak{m}K) = x+\mathfrak{m}K_0$. Pero entonces

$$(Id \otimes \epsilon) \circ (Id \otimes f)(y + \mathfrak{m}K) = (Id \otimes i) \circ (Id \otimes (\epsilon \circ f))(y + \mathfrak{m}K) = (Id \otimes i)(x + \mathfrak{m}K_0) = 0 + \mathfrak{m}R^n.$$

Es decir, los elementos siguen el siguiente diagrama:

$$\begin{array}{ccc}
y + \mathfrak{m}K & \xmapsto{Id\otimes f} & (Id \otimes f)(y + \mathfrak{m}K) \\
\downarrow{\scriptstyle Id\otimes(\epsilon\circ f)} & & \downarrow{\scriptstyle Id\otimes\epsilon} \\
x + \mathfrak{m}K_0 & \xmapsto{Id\otimes i} & 0 + \mathfrak{m}R^n
\end{array}$$

Escribimos $z + \mathfrak{m}P := (Id \otimes f)(y + \mathfrak{m}K)$ y tendremos que $(Id \otimes \epsilon)(z + \mathfrak{m}P) = 0 + \mathfrak{m}R^n$. Luego $z + \mathfrak{m}P \in \ker(Id \otimes \epsilon) = K_2/\mathfrak{m}K_2$.

$$\begin{array}{ccc}
 & & z + \mathfrak{m}K_2 \\
 & & \downarrow{\scriptstyle Id\otimes i_2} \\
y + \mathfrak{m}K & \xmapsto{Id\otimes f} & z + \mathfrak{m}P \\
\downarrow{\scriptstyle Id\otimes(\epsilon\circ f)} & & \downarrow{\scriptstyle Id\otimes\epsilon} \\
x + \mathfrak{m}K_0 & \xmapsto{Id\otimes i} & 0 + \mathfrak{m}R^n
\end{array}$$

Ahora recordemos que $f|_{K_1}$ era un isomorfismo y esta condición se conserva al tensorizar, con lo que $Id \otimes f|_{K_1}$ sigue siendo un isomorfismo. Por tanto, existirá $y' + \mathfrak{m}K$ tal que $(Id \otimes f|_{K_1})(y' + \mathfrak{m}K) = z + \mathfrak{m}P$. Tenemos así el siguiente diagrama:

$$\begin{array}{ccccc} & & y'+\mathfrak{m}K_1 & \xrightarrow{Id\otimes f|_{K_1}} & z+\mathfrak{m}K_2 \\ & \swarrow^{Id\otimes i_1} & & & \downarrow{\scriptstyle Id\otimes i_2} \\ y''+\mathfrak{m}K & & y+\mathfrak{m}K & \xrightarrow{Id\otimes f} & z+\mathfrak{m}P \\ & & \downarrow{\scriptstyle Id\otimes(\epsilon\circ f)} & & \downarrow{\scriptstyle Id\otimes\epsilon} \\ & & x+\mathfrak{m}K_0 & \xrightarrow{Id\otimes i} & 0+\mathfrak{m}R^n \end{array}$$

Pero por la conmutatividad de los diagramas tendremos que

$(Id\otimes f)(y''+\mathfrak{m}K) = (Id\otimes f)\circ(Id\otimes i_1)(y'+\mathfrak{m}K_1) = (Id\otimes i_2)\circ(Id\otimes f|_{K_1})(y'+\mathfrak{m}K_1) = z+\mathfrak{m}P.$

Por tanto, $(Id\otimes f)(y''+\mathfrak{m}K) = (Id\otimes f)(y+\mathfrak{m}K)$, y recordando la hipótesis de que $Id\otimes f$ es monomorfismo, tenemos que $y+\mathfrak{m}K = y''+\mathfrak{m}K = (Id\otimes i_1)(y'+\mathfrak{m}K_1)$ con $y'\in K_1$. Pero entonces,

$$x+\mathfrak{m}K_0 = (Id\otimes(\epsilon\circ f))(y+\mathfrak{m}K) = (Id\otimes(\epsilon\circ f))\circ((Id\otimes i_1)(y'+\mathfrak{m}K_1)) = 0+\mathfrak{m}K_0.$$

En conclusión, para cada $x+\mathfrak{m}K_0\in K_0/\mathfrak{m}K_0$, si $(Id\otimes i)(x+\mathfrak{m}K_0) = 0+\mathfrak{m}R^n$, necesariamente $x+\mathfrak{m}K_0 = 0+\mathfrak{m}K_0$. Con ello $Id\otimes i$ es un monomorfismo de R-módulos.

Hemos visto que $Im(Id\otimes i) = \{0\}$ y que sin embargo, $Id\otimes i$ es monomorfismo. Luego necesariamente $K_0/\mathfrak{m}K_0 = \{0\}$.

Recordando ahora el uso que hemos hecho del Lema precedente, K_0 era un R-módulo finitamente generado y, por el Lema de Nakayama, $K_0/\mathfrak{m}K_0 = \{0\}$ implica que $K_0 = \{0\}$. Finalmente, recordemos que K_0 es el núcleo del epimorfismo π de la sucesión exacta corta

$$0\to K_0 = 0 \xrightarrow{i} R^n \xrightarrow{\pi} M\to 0.$$

Luego π es isomorfismo de R-módulos, $M\cong R^n$ y M es un R-módulo libre de rango finito. □

A continuación se enuncian dos resultados inmediatos de aplicación de la Proposición anterior.

TEOREMA 1.3.3 (**Libre y Proyectivo en el ámbito local**). *Un R-módulo finitamente generado sobre un anillo local es proyectivo si y solo si es libre.*

DEMOSTRACIÓN. Si M es proyectivo, entonces el resultado se obtiene al tomar $P = M$ y $K = 0$ en la sucesión exacta de la Proposición 1.3.2*ii*). □

Nótese que se tiene la siguiente caracterización local de los módulos proyectivos:

TEOREMA 1.3.4 (**Proyectivo es ser localmente libre**). *Sea M un módulo finitamente generado sobre un anillo arbitrario R. Entonces las siguientes propiedades son equivalentes:*

i) M es proyectivo.
ii) M es finitamente presentado y localmente libre.

DEMOSTRACIÓN. *i)* $\Longrightarrow$ *ii)* Si M es proyectivo entonces existe M' con $M\oplus M'$ libre y de rango finito (por ser M finitamente generado). Por tanto, tenemos la sucesión exacta corta

$$0\to M'\to F = M\oplus M'\to M\to 0,$$

donde F es un R-módulo libre de rango finito y $M'\subseteq F$ es finitamente generado. Luego M es finitamente presentado.

La condición de localmente libre se obtiene del Teorema 1.3.3 anterior y de que $R_{\mathfrak{m}}$ es anillo local.

ii) $\Longrightarrow$ *i)* Supongamos que existe una sucesión exacta

$$0\longrightarrow K\longrightarrow F\longrightarrow M\longrightarrow 0,$$

con F un R-módulo libre de rango finito y $K\subset F$ submódulo finitamente generado. Si M es localmente libre, la sucesión anterior es localmente escindida $\forall\mathfrak{m}\in \mathrm{MaxSpec}(R)$. Con ello,

también es escindida globalmente (cf. Teorema 1.2.11). Por tanto, $F \cong M \oplus K$, M es un sumando directo de F y con ello es proyectivo. □

En otras palabras, para módulos finitamente presentados ser proyectivo equivale a ser localmente libre.

TEOREMA 1.3.5 (**Trivialidad Local de los Módulos Proyectivos**). *Sea P un R-módulo proyectivo finitamente generado. Supongamos que para $\mathfrak{p} \in \mathrm{Spec}(R)$, el $R_\mathfrak{p}$-módulo libre $P_\mathfrak{p}$ tiene rango r. Entonces existe un $f \in R \setminus \mathfrak{p}$ tal que P_f es un R_f-módulo libre de rango r.*

DEMOSTRACIÓN. Sea $\{w_1, ..., w_r\}$ una sistema minimal de generadores de $P_\mathfrak{p}$ como $R_\mathfrak{p}$-módulo. Podemos tomar cada uno de estos w_i como imágenes de elementos w_i^* de P, multiplicando todos por un denominador común. De esta forma, tenemos un nuevo sistema minimal de generadores de $P_\mathfrak{p}$ como $R_\mathfrak{p}$-módulo, $\{w_1^*, ..., w_r^*\}$. Consideramos ahora la sucesión exacta

$$0 \to K \to R^r \xrightarrow{\alpha} P \to C \to 0,$$

donde α lleva los elementos de la base canónica e_i en w_i^* $(i = 1, ..., r)$, y $K := \ker(\alpha)$, $C := \mathrm{coker}(\alpha) := P/Im(\alpha)$.

Por ser $\{w_1^*, ..., w_r^*\}$ un sistema de generadores de $P_\mathfrak{p}$ como $R_\mathfrak{p}$-módulo, tenemos que $C_\mathfrak{p} = \{0\}$. Y como C es finitamente generado, existe un $f \in R \setminus \mathfrak{p}$ tal que $C_f = \{0\}$. En efecto, sea $\{c_1, ..., c_l\}$ un sistema minimal de generadores de C. Entonces existen $f_1, ..., f_l \in R \setminus \mathfrak{p}$ tales que $c_i f_i = 0$, $(i = 1, ..., l)$. Tomando $f = f_1 f_2 ... f_l \in R \setminus \mathfrak{p}$ tenemos que $C_f = 0$. Ahora la sucesión exacta corta

$$0 \to K_f \to R_f^r \to P_f \to 0$$

es escindida puesto que P_f es un R_f-módulo proyectivo. Por tanto, existe un isomorfismo $\phi : R_f^r \to K_f \oplus P_f$, y como R_f y P_f son finitamente generados, entonces K_f también es finitamente generado. Ahora como $K_\mathfrak{p} = \{0\}$, existe un $g \in R \setminus \mathfrak{p}$ con $K_{fg} = \{0\}$. Con ello, tenemos la sucesión exacta de R_{fg}-módulos

$$0 \to R_{fg}^r \to P_{fg} \to 0,$$

y por tanto, P_{fg} es un R_{fg}-módulo libre de rango r. □

CAPÍTULO 2

Resultados Instrumentales: Teoremas de Vaserstein y Horrocks.

Índice

2.1. Introducción **23**
2.2. Cálculos matriciales con coordenadas en $R[X]$: equivalencia y el Teorema de Vaserstein. **24**
2.3. Extensiones de módulos. Primer Teorema de Quillen. **28**
2.4. Teorema de Horrocks. **29**

2.1. Introducción

Este Capítulo está dedicado a probar algunos resultados instrumentales que serán esenciales en la prueba del Teorema de Quillen-Suslin.

La primera observación que debemos hacer es que la extensión de escalares (ver Apéndice A.5) preserva la condición de ser módulo libre. En otras palabras, como el producto tensorial conmuta con la suma directa de R-módulos, si $R \subseteq B$ es una extensión de anillos y F es un R-módulo libre, entonces $B \otimes_R F$ es un B-módulo libre. Además, si F es de rango finito,

$$\mathrm{rank}_B(B \otimes_R F) = \mathrm{rank}_R(F).$$

Ahora si P es un R-módulo proyectivo, entonces es sumando directo de un R-módulo libre. Supongamos $F = P \oplus Q$, donde F es un R-módulo libre. De nuevo, como el producto tensorial conmuta con la suma directa, tendremos un isomorfismo de R-módulos

$$R[X] \otimes_R F \cong (R[X] \otimes_R P) \oplus (R[X] \otimes_R Q).$$

Por tanto, también la condición de ser proyectivo se preserva mediante la extensión de escalares $R \subseteq R[X]$. Escribiremos $M[X] = R[X] \otimes_R M$ para expresar el módulo obtenido por extensión de escalares. El argumento esencial del Teorema de Quillen-Suslin se sustenta en este juego de "subir" y "bajar" entre R-módulos y $R[X]$-módulos, usando que $R[X]$ es un R-módulo libre, y por tanto plano.

El otro aspecto esencial es el Álgebra Lineal con matrices tanto sobre R como $R[X]$. Nos interesa esencialmente la relación de equivalencia entre matrices con coordenadas en un anillo B. Dos matrices A_1 y A_2 en $M_{r\times s}(B)$ se dicen equivalentes si existen matrices regulares $P \in GL(r, B)$, $Q \in GL(s, B)$ tales que

$$A_1 = P \cdot A_2 \cdot Q.$$

En la Sección 2.2 los anillos que consideramos son esencialmente R y $R[X]$. Si $A(X) \in M_{r\times s}(R[X])$ es una matriz con coordenadas en $R[X]$, podemos especializar la variable X en $0 \in R$ y obtener la matriz $A(0) \in M_{r\times s}(R)$. La cuestión instrumental que trata el Teorema de Vaerstein es la propiedad "$A(X)$ es equivalente a $A(0)$". Este Teorema establece que se trata de una propiedad local. Reproducimos aquí el resultado para facilitar la lectura del texto:

Teorema 2.1.1 (**Teorema de Vaserstein**). *Sea $A(X) \in M_{r\times s}(R[X])$ una matriz con coordenadas en $R[X]$. Son equivalentes:*

- *$A(X)$ es equivalente a $A(0) \in M_{r\times s}(R)$.*

- *La imagen de $A(X)$ en $M_{r\times s}(R_{\mathfrak{m}}[X])$ es equivalente a la imagen de $A(0)$ en $M_{r\times s}(R_{\mathfrak{m}})$ para todo ideal maximal $\mathfrak{m} \in \mathrm{MaxSpec}(R)$.*

Junto al Teorema de Vaserstein hemos introducido una sección instrumental, la Sección 2.3, en la que exponemos el llamado Primer Teorema de Quillen. En él, Quillen se ocupa de los módulos extendidos, es decir los $R[X]$-módulos $M[X] = R[X] \otimes_R M$. Su caracterización local de la condición de "ser extendido" constituye el Primer Teorema de Quillen. Reproducimos este resultado aquí:

TEOREMA 2.1.2 (**Primer Teorema de Quillen**). *Un $R[X]$-módulo M finitamente presentado es extendido (i.e. de la forma $M = N[X]$) si y solamente es localmente extendido, es decir, si para cada ideal $\mathfrak{m} \in \mathrm{MaxSpec}(R)$, $M_{\mathfrak{m}}$ es un $R_{\mathfrak{m}}[X]$-módulo extendido.*

El resultado final de este Capítulo, el cual constituye la piedra angular del Teorema de Quillen-Suslin, es el Teorema de Horrocks. La Sección final del Capítulo se dedica a su enunciado y demostración. De nuevo, reproducimos aquí el resultado para facilitar la lectura:

TEOREMA 2.1.3 (**Teorema de Horrocks**). *Sea $(R, \mathfrak{m})$ un anillo local, y sea M un $R[X]$-módulo proyectivo finitamente generado. Supongamos que existe un polinomio mónico $f \in R[X]$ tal que M_f es libre como $R[X]_f$-módulo. Entonces, M es libre como $R[X]$-módulo.*

En ambos resultados (Primer Teorema de Quillen y Teorema de Horrocks) la equivalencia de matrices juega un papel fundamental.

2.2. Cálculos matriciales con coordenadas en $R[X]$: equivalencia y el Teorema de Vaserstein.

En lo que sigue denotamos:
- $M_{r\times s}(R)$ el R-módulo formado por todas las matrices de tamaño $r \times s$ con coeficientes en R.
- $GL(r, R)$ el grupo de matrices invertibles de tamaño $r \times r$ con coeficientes en R, es decir el grupo de matrices $r \times r$ tal que su determinante es una unidad de R.

Todo homomorfismo de anillos $R \to S$ induce de forma natural un morfismo $M_{r\times s}(R) \to M_{r\times s}(S)$ y un homomorfismo de grupos $GL(r, R) \to GL(r, S)$.

DEFINICIÓN 6 (**Matrices equivalentes**). *Se dice que dos matrices $A_1, A_2 \in M_{r\times s}(R)$ son equivalentes ($A_1 \sim A_2$) si existe una matriz $A \in GL(r, R)$ y una matriz $B \in GL(s, R)$ tal que*

$$A_1 = A \cdot A_2 \cdot B$$

Consideremos ahora dos sucesiones exactas

$$R^{n'_j} \xrightarrow{\beta_j} R^{n_j} \xrightarrow{\alpha_j} M_j \to 0 \quad (n_j, n'_j \in \mathbb{N}) \quad (j = 1, 2).$$

Respecto de la base canónica β_1 viene dada por una matriz B_1 de tamaño $n'_1 \times n_1$, y de la misma forma β_2 viene dada por una matriz B_2 de tamaño $n'_2 \times n_2$.

Retomamos ahora la construcción del Corolario 1.2.15. Con ello, las matrices correspondientes a las aplicaciones $(\beta_1 \oplus Id_{F_2}, 0)$ y $(0, Id_{F_1} \oplus \beta_2)$ (es decir, a las filas del diagrama (1.2.5)) son de la forma

$$\left(\begin{array}{c|c} B_1 & 0 \\ \hline 0 & I_{n_2} \\ \hline \multicolumn{2}{c}{0} \end{array}\right)_{r\times s} \quad \text{y} \quad \left(\begin{array}{c|c} \multicolumn{2}{c}{0} \\ \hline I_{n_1} & 0 \\ \hline 0 & B_2 \end{array}\right)_{r\times s}, \tag{2.2.1}$$

con $r = n_1 + n_2 + n'_1 + n'_2$, $s = n_1 + n_2$ e I_n denota la matriz identidad $n \times n$.

El Corolario 1.2.15 afirma que los módulos M_1 y M_2 son isomorfos si y solo si estas dos matrices son equivalentes. En otras palabras, B_1 y B_2 presentan el mismo R-módulo (salvo isomorfismo) si y solo si las matrices (2.2.1) son equivalentes.

Ahora pasaremos a considerar matrices con coeficientes en $R[X]$. Dada $A \in M_{r\times s}(R[X])$ y dado un anillo T que extiende a $R[X]$, escribiremos $A(X)$ en lugar de A, y dado $f \in T$, denotamos

por $A(f)$ la imagen de A en $M_{r\times s}(T)$ inducida por la sustitución $X \mapsto f$. Además, denotaremos por $A(0)$ a la matriz obtenida al sustituir $X \mapsto 0 \in R$, de modo que $A(0) \in M_{r\times s}(R)$.

Definición 7 (**Matrices localmente equivalentes**). *Se dice que $A_1, A_2 \in M_{r\times s}(R[X])$ son localmente equivalentes para $\mathfrak{m} \in \mathrm{MaxSpec}(R)$ si las imágenes de A_1, A_2 en $M_{r\times s}(R_{\mathfrak{m}}[X])$ son equivalentes.*

El Teorema de Vaserstein demuestra que la equivalencia de matrices sobre $R[X]$ es una propiedad local. Para esta demostración necesitamos primero el siguiente Lema técnico.

Lema 2.2.1. *Sean*

$$A_1 \in M_{r\times s}(R[X]) \qquad A_2 \in M_{s\times t}(R[X]) \qquad A_3 \in M_{r\times t}(R[X]),$$

y sea $S \subset R$ multiplicativamente cerrado. Sea $\overline{A_i}$ $(i = 1, 2, 3)$ la matriz correspondiente a A_i inducida por el homomorfismo canónico $R[X] \to S^{-1}R[X]$.

Supongamos que $\overline{A_1} \cdot \overline{A_2} = \overline{A_3}$ y que $A_1(0) \cdot A_2(0) = A_3(0)$. Entonces existe un $s \in S$ tal que $A_1(sX) \cdot A_2(sX) = A_3(sX)$.

Demostración. Consideremos la matriz $A := A_1 \cdot A_2 - A_3$. Como $A_1(0) \cdot A_2(0) = A_3(0)$, todos los coeficientes de A son divisibles por X. Además, bajo el homomorfismo canónico

$$M_{r\times t}(R[X]) \to M_{r\times t}(S^{-1}R[X]),$$

A se corresponde con la matriz 0. Por tanto, existe un $s \in S$ tal que $sa_{ij} = 0$, $\forall i, j$. Pero en tal caso

$$A_1(sX) \cdot A_2(sX) - A_3(sX) = 0.$$

□

Teorema 2.2.2 (**Teorema de Vaserstein**). *$A \in M_{r\times s}(R[X])$ es equivalente a $A(0)$ si y solo si A es localmente equivalente a $A(0)$ para todo $\mathfrak{m} \in \mathrm{MaxSpec}(R)$.*

Demostración. Veamos las dos implicaciones por separado:

$\Longrightarrow$) Esta implicación es evidente, puesto que si existen $C(X) \in GL(r, R[X])$ y $D(X) \in GL(s, R[X])$ tales que en $R[X]$ se da la igualdad

$$A(0) = C(X)A(X)D(X),$$

entonces esta igualdad se da también en cualquier anillo que contenga a $R[X]$. Como $R \subseteq R_{\mathfrak{m}}$ para todo $\mathfrak{m} \in \mathrm{MaxSpec}(R)$, tenemos el resultado buscado.

$\Longleftarrow$) Consideremos el conjunto

$$I = \{a \in R : \forall f, g \in R[X], f - g \in aR[X] \Longrightarrow A(f) \sim A(g)\}.$$

La demostración pasa por ver, en primer lugar, que I es un ideal de R, y en segundo lugar, que $I = R$ (o equivalentemente $1 \in I$). De este modo, tomando $f = X, g = 0$ tenemos que $X - 0 = X \in R[X]$ y por tanto $A(X) \sim A(0)$.

Veamos en primer lugar que I es ideal de R. Sean $a_1, a_2 \in I$, y $f, g \in R[X]$ tales que $f - g = (r_1a_1 + r_2a_2)\varphi$, con $r_1, r_2 \in R, \varphi \in R[X]$. Entonces $(f - r_1a_1\varphi) - g \in a_2R[X]$, luego

$$A(g) \sim A(f - r_1a_1\varphi).$$

Pero además, $(f - r_1a_1\varphi) - f \in a_1R[X]$, luego

$$A(g) \sim A(f - r_1a_1\varphi) \sim A(f).$$

y con ello $r_1a_1 + r_2a_2 \in I$.

Ahora veamos que $I = R$. Para ello, vamos a ver que, $\forall \mathfrak{m} \in \mathrm{MaxSpec}(R)$, si $A(X) \sim A(0)$ en $R_{\mathfrak{m}}[X]$ (lo cual tenemos por hipótesis), entonces $I \not\subseteq \mathfrak{m}$. De esta forma, como consecuencia del Axioma de Zorn concluimos que necesariamente I es un ideal impropio.

Sea $\mathfrak{m} \in \text{MaxSpec}(R)$. Sabemos por hipótesis que existen $C(X) \in GL(r, R_{\mathfrak{m}}[X]), D(X) \in GL(s, R_{\mathfrak{m}}[X])$ tales que

$$A(X) = C(X)A(0)D(X).$$

Nótese que $A(0) \in M_{r\times s}(R)$ carece de variables. Ahora consideramos el anillo $R_{\mathfrak{m}}[X, Y] \supseteq R_{\mathfrak{m}}[X]$ y reemplazamos X por $X + Y$ en la identidad anterior. Con ello,

$$A(X + Y) = C(X + Y)A(0)D(X + Y). \tag{2.2.2}$$

Como $C(X)$ y $D(X)$ son matrices inversibles sobre $R_{\mathfrak{m}}[X]$, tendremos que

$$A(0) = C^{-1}(X)A(X)D^{-1}(X),$$

y sustituyendo en la expresión (2.2.2),

$$A(X + Y) = C(X + Y)C^{-1}(X)A(X)D^{-1}(X)D(X + Y)$$

Ahora llamamos

$$C^*(X + Y) := C(X + Y)C^{-1}(X) \in M_{r\times r}(R_{\mathfrak{m}}[X, Y]),$$
$$D^*(X + Y) := D^{-1}(X)D(X + Y) \in M_{s\times s}(R_{\mathfrak{m}}[X, Y]).$$

Tomando $C^*(X + Y)$, sabemos que sus coordenadas son polinomios de $R_{\mathfrak{m}}[X, Y]$, es decir, $C^*(X + Y) = (p_{ij}(X, Y))$. De hecho, cada $p_{ij}(X, Y)$ se puede escribir como

$$p_{ij}(X, Y) = \sum_{k=0}^{m_{ij}} a_{ij}^{(k)}(X)Y^k,$$

donde $a_{ij}^{(k)}(X) \in R_{\mathfrak{m}}[X]$. Sea $m = \max\{m_{ij}\}$, y reagrupando coeficientes podemos escribir

$$C^*(X + Y) = C_0(X) + C_1(X)Y + ... + C_m(X)Y^m,$$

con $C_i(X) \in M_{r\times r}(R_{\mathfrak{m}}[X])$, $(i = 1, ..., m)$, y C_0 es la matriz identidad (porque $C^*(X + 0) = C_0(X) = C(X)C^{-1}(X) = Id_r$).

Cada una de estas matrices $C_j(X)$ es una matriz cuyas coordenadas son polinomios en $R_{\mathfrak{m}}[X]$, $C_j(X) = (q_{tl}^{(j)}(X))$, y por tanto, los coeficientes de estos polinomios poseen denominadores en $R \setminus \mathfrak{m}$. Multiplicando todos los denominadores de los coeficientes de $q_{tl}^{(j)}(X)$ podemos obtener un elemento $d_{tl}^{(j)} \in R \setminus \mathfrak{m}$ tal que $d_{tl}^{(j)} \cdot q_{tl}^{(j)}(X) \in R[X]$. Esto se puede hacer porque $R \setminus \mathfrak{m}$ es un sistema multiplicativamente cerrado, con lo que el producto de un número finito de elementos de $R \setminus \mathfrak{m}$ sigue estando en $R \setminus \mathfrak{m}$. Definimos ahora para cada j

$$d_j = \prod_{1\leq t,l\leq r} d_{tl}^{(j)} \in R \setminus \mathfrak{m}.$$

Observemos que $d_jC_j(X) \in M_{r\times r}(R[X])$. Finalmente, definimos

$$a' = \prod_{j=1}^{m} d_j \in R \setminus \mathfrak{m}$$

y consideramos la matriz

$$C^*(X + a'Y) = C_0(X) + C_1(X)a'Y + ... + C_m(X)(a')^mY^m.$$

Ahora observemos que para cada $j = 1, ..., m$, $d_j|a'$, luego $C_j(X)a'$ es una matriz con coordenadas en $R[X]$, y con ello

$$C_j(X)(a')^j = C_j(X)d_j\frac{a'}{d_j}(a')^{j-1} \in M_{r\times r}(R[X]).$$

Además, $C_0(X) \in M_{r\times r}(R[X, Y])$ por ser la matriz identidad. En suma,

$$C^*(X + a'Y) \in M_{r\times r}(R[X, Y]).$$

Del mismo modo, podemos construir $b' \in R \setminus \mathfrak{m}$ tal que $D^*(X + b'Y)$ sea una matriz con coordenadas en $R[X, Y]$. Más aún, el elemento $d' = a'b'$ verifica que

$$C^*(X + d'Y) \in M_{r\times r}(R[X, Y]),$$
$$D^*(X + d'Y) \in M_{s\times s}(R[X, Y]),$$

y además $d' \in R \setminus \mathfrak{m}$ por ser $R \setminus \mathfrak{m}$ multiplicativamente cerrado.

Como $C(X)$ y $D(X)$ son inversibles en $R_{\mathfrak{m}}[X]$, también lo serán $C^*(X+Y)$ y $D^*(X+Y)$. Por tanto, tenemos que las inversas verifican

$$C^{*-1}(X + Y) \in M_{r\times r}(R_{\mathfrak{m}}[X, Y]),$$
$$D^{*-1}(X + Y) \in M_{s\times s}(R_{\mathfrak{m}}[X, Y]).$$

Podemos repetir el argumento desarrollado antes para C^* y D^* con estas matrices y hallamos $e' \in R \setminus \mathfrak{m}$ tal que

$$C^{*-1}(X + e'Y) \in M_{r\times r}(R[X, Y]),$$
$$D^{*-1}(X + e'Y) \in M_{s\times s}(R[X, Y]).$$

Finalmente, eligiendo $p' = d'e' \in R \setminus \mathfrak{m}$ tendremos que

$$C^*(X + p'Y) \in M_{r\times r}(R[X, Y]),$$
$$D^*(X + p'Y) \in M_{s\times s}(R[X, Y]),$$
$$C^{*-1}(X + p'Y) \in M_{r\times r}(R[X, Y]),$$
$$D^{*-1}(X + p'Y) \in M_{s\times s}(R[X, Y]).$$

Ahora consideramos el anillo $R' = R[X]$, el sistema multiplicativamente cerrado $S = R \setminus \mathfrak{m}$ en R' y las matrices

$$\overline{A_1}(Y) := C(X + p'Y)C^{-1}(X) \in M_{r\times r}(S^{-1}R'[Y]),$$
$$\overline{A_2}(Y) := C(X)C^{-1}(X + p'Y) \in M_{r\times r}(S^{-1}R'[Y]).$$

Observemos que $\overline{A_1}(Y)\overline{A_2}(Y) = Id_r$ y $A_1(0)A_2(0) = Id_r$. Entonces por el Lema 2.2.1 existe $\lambda_1 \in S$ tal que

$$A_1(\lambda_1 Y)A_2(\lambda_1 Y) = Id_r.$$

En particular, la matriz

$$\Gamma_0(X, Y) = A_1(\lambda_1 Y) = C^*(X + p'\lambda_1 Y) \in GL(r, R[X, Y])$$

es una matriz inversible cuya inversa tiene coordenadas en $R[X, Y] = R'[Y]$.

Del mismo modo, podemos proceder con las matrices D^* y D^{*-1} y encontrar $\lambda_2 \in S$ tal que

$$\Delta_0(X, Y) = D^*(X + p'\lambda_2 Y) \in GL(s, R[X, Y]).$$

Eligiendo $\lambda = \lambda_1\lambda_2 \in S$, tenemos que

$$\Gamma(X, Y) = C^*(X + p'\lambda Y) \in GL(r, R[X, Y]),$$
$$\Delta(X, Y) = D^*(X + p'\lambda Y) \in GL(s, R[X, Y]).$$

y además $\Gamma(X, 0) = Id_r$, $\Delta(X, 0) = Id_s$. Llamaremos $t' := p'\lambda$.

De esta forma, sobre $R_{\mathfrak{m}}[X, Y]$ tenemos la identidad

$$A(X + t'Y) = C(X + t'Y)C^{-1}(X)A(X)D^{-1}(X)D(X + t'Y),$$

y sobre $R[X]$

$$A(X) = \Gamma(X, 0)A(X)\Delta(X, 0).$$

Por tanto, aplicando de nuevo el Lema 2.2.1, existe un $t'' \in R \setminus \mathfrak{m}$ tal que si $t := t't''$,

$$A(X + tY) = \Gamma(X, t''Y)A(X)\Delta(X, t''Y)$$

sobre $R[X, Y]$. Ahora si tenemos $f, g, \varphi \in R[X]$ tales que $f - g = t\varphi$, entonces

$$A(f) = \Gamma(g, t''\varphi)A(g)\Delta(g, t''\varphi),$$

y con ello $A(f) \sim A(g)$ y $t \in I$. Así hemos probado que $\forall \mathfrak{m} \in \mathrm{MaxSpec}(R)$ existe un $t \in I$ tal que $t \notin \mathfrak{m}$, q.e.d. □

2.3. Extensiones de módulos. Primer Teorema de Quillen.

Definición 8 (**Extensión de escalares**). *Sea $f : R \to T$ un morfismo de anillos y sea N un R-módulo. Entonces podemos definir una estructura de T-módulo sobre $T \otimes_R N$ del modo siguiente:*

$$\cdot_T : T \times (T \otimes_R N) \longrightarrow (T \otimes_R N)$$
$$(\lambda, \sum_{i\in I} x_i \otimes_R n_i) \longmapsto \sum_{i\in I} (\lambda x_i) \otimes_R n_i$$

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 a partir de N por extensión de escalares a partir de $f : R \to T$.

En particular, si consideramos el morfismo de anillos $i : R \to R[X]$ y un R-módulo N, podemos construir el $R[X]$-módulo $N[X] := R[X] \otimes_R N$ por extensión de escalares, mediante la operación siguiente: si $f = r_0 + r_1X + ... + r_tX^t \in R[X], g = n_0 + n_1X + ... + n_sX^s \in N[X]$ (supongamos $t \geq s$), entonces

$$f \cdot_{R[X]} g = r_0n_0 + (r_1n_0 + r_0n_1)X + ... + (\sum_{i+j=t} r_in_j)X^t.$$

Esto nos lleva a la siguiente

Definición 9 (**Módulo extendido y localmente extendido**). *Un $R[X]$-módulo M se dice que es extendido (de R) si existe un R-módulo N tal que $M \cong N[X]$ como $R[X]$-módulos, donde $N[X] = R[X] \otimes_R N$ es la extensión por escalares de N.*

M se dice que es localmente extendido para un ideal maximal $\mathfrak{m} \subseteq R$ si el $R_\mathfrak{m}[X]$-módulo $M_\mathfrak{m}$ es extendido de $R_\mathfrak{m}$.

El Principio Local-Global se mantiene para módulos extendidos. Esta propiedad se enuncia en el Primer Teorema de Quillen, y es clave en la demostración del Teorema de Quillen-Suslin.

Teorema 2.3.1 (**Primer Teorema de Quillen**). *Un $R[X]$-módulo finitamente presentado es extendido si y solo si es localmente extendido para todo $\mathfrak{m} \in \mathrm{MaxSpec}(R)$.*

Demostración. Por hipótesis existe una sucesión exacta de $R[X]$-módulos

$$R[X]^m \xrightarrow{\beta_1} R[X]^n \xrightarrow{\alpha_1} M \to 0. \tag{2.3.1}$$

Tensorizando por $R[X]/(X)$ tenemos la sucesión exacta

$$R^m \xrightarrow{\overline{\beta_1}} R^n \xrightarrow{\overline{\alpha_1}} M/XM \to 0. \tag{2.3.2}$$

Ahora llamamos $B \in M_{m\times n}(R[X])$ a la matriz de β_1 en la base canónica. Entonces, $B(0)$ es la matriz de $\overline{\beta_1}$ en la base canónica.

Ahora a partir de (2.3.1) obtenemos por extensión de escalares la sucesión exacta

$$R^m[X] \xrightarrow{\overline{\beta_1}[X]} R^n[X] \xrightarrow{\overline{\alpha_1}[X]} N[X] := (M/XM)[X] \to 0. \tag{2.3.3}$$

Aquí, el morfismo $\overline{\beta_1}[X] : R^m[X] \to R^n[X]$ actúa como sigue:

$$(\overline{\beta_1}[X])(a_0 + a_1X + ... + a_dX^d) = \overline{\beta_1}(a_0) + \overline{\beta_1}(a_1)X + ... + \overline{\beta_1}(a_d)X^d.$$

Por tanto, podemos identificar la sucesión (2.3.3) con una sucesión exacta

$$R[X]^m \xrightarrow{\beta_2} R[X]^n \xrightarrow{\alpha_2} N[X] \to 0, \tag{2.3.4}$$

a través de los isomorfismos $i_1 : R^m[X] \to R[X]^m, i_2 : R^n[X] \to R[X]^n$

$$i_1 : R^m[X] \longrightarrow R[X]^m$$

$$\begin{pmatrix} a_{00} \\ \vdots \\ a_{0m} \end{pmatrix} + \begin{pmatrix} a_{10} \\ \vdots \\ a_{1m} \end{pmatrix} X + ... + \begin{pmatrix} a_{d0} \\ \vdots \\ a_{dm} \end{pmatrix} X^d \longmapsto \begin{pmatrix} a_{00} + a_{10}X + ... + a_{d0}X^d \\ \vdots \\ a_{0m} + a_{1m}X + ... + a_{dm}X^d \end{pmatrix}$$

(análogo para i_2). De esta forma, β_2 viene descrito por la matriz $B(0)$.

Ahora, por el Corolario 1.2.15, $M \cong N[X]$ si y solo si las matrices $(2n) \times 2(n+m)$

$$A := \left(\begin{array}{c|c} B & 0 \\ \hline 0 & I_n \\ \hline \multicolumn{2}{c}{0} \end{array}\right) \quad \text{y} \quad \left(\begin{array}{c|c} \multicolumn{2}{c}{0} \\ \hline I_n & 0 \\ \hline 0 & B(0) \end{array}\right)$$

son equivalentes. La segunda matriz es equivalente a $A(0)$, ya que se obtiene por permutación de filas y columnas de $A(0)$. Por tanto, por el Teorema de Vaserstein, $M \cong N[X]$ si y solo si A es localmente equivalente a $A(0)$ para todo $\mathfrak{m} \in \text{MaxSpec}(R)$.

Ahora, dado $\mathfrak{m} \in \text{MaxSpec}(R)$, el functor localización en $\mathfrak{m}$ es exacto y $R_{\mathfrak{m}}[X] \cong R[X]_{\mathfrak{m}}$, luego tenemos las sucesiones exactas siguientes

$$R_{\mathfrak{m}}[X]^m \xrightarrow{\tilde{\beta_1}} R_{\mathfrak{m}}[X]^n \xrightarrow{\tilde{\alpha_1}} M_{\mathfrak{m}} \to 0,$$

$$R_{\mathfrak{m}}[X]^m \xrightarrow{\tilde{\beta_2}} R_{\mathfrak{m}}[X]^n \xrightarrow{\tilde{\alpha_2}} N_{\mathfrak{m}}[X] \to 0.$$

De nuevo, por el Corolario 1.2.15 tenemos que $M_{\mathfrak{m}} \cong N_{\mathfrak{m}}[X]$ si y solo si A es localmente equivalente a $A(0)$ en $\mathfrak{m}$. Como la equivalencia de matrices es una propiedad local (Teorema 2.2.2), esto nos permite concluir que M es extendido si y solo si es localmente extendido para todo ideal maximal $\mathfrak{m} \subseteq R$. □

2.4. Teorema de Horrocks.

TEOREMA 2.4.1 ([Horrocks, 1964]). *Sea $(R, \mathfrak{m})$ un anillo local, y sea M un $R[X]$-módulo proyectivo finitamente generado. Supongamos que existe un polinomio mónico $f \in R[X]$ tal que M_f es libre como $R[X]_f$-módulo. Entonces, M es libre como $R[X]$-módulo.*

DEMOSTRACIÓN. En primer lugar, tomamos una base de M_f formada por elementos de M. Veamos que dicha base existe. Como M es un $R[X]$-módulo finitamente generado, entonces M_f es un $R[X]_f$-módulo libre de rango finito. Ahora dada una base de cardinal finito de M_f como $R[X]_f$-módulo libre

$$\tilde{\mathcal{B}} = \{n_i = \frac{m_i}{f^{s_i}} : m_i \in M, s_i \in \mathbb{N}, 1 \leq i \leq r\},$$

tenemos que la familia $\mathcal{B} = \{m_i : m_i \in M, 1 \leq i \leq r\} \subseteq M$ también es una base de M_f como $R[X]_f$-módulo libre. En efecto:

i) $M_f = R[X]_f\langle\mathcal{B}\rangle$: Sea $a \in M_f$. Entonces

$$a = \sum_{k=1}^{t} \frac{g_k}{f^{c_k}} n_k = \sum_{k=1}^{t} \frac{g_k}{f^{c_k}} \frac{m_k}{f^{s_k}} = \sum_{k=1}^{t} \frac{g_k}{f^{c_k+s_k}} m_k \in R[X]_f\langle\mathcal{B}\rangle$$

donde la primera igualdad se da por ser $\tilde{\mathcal{B}}$ base de M_f.

ii) $\mathcal{B}$ es linealmente independiente: Sea $\{m_1, ..., m_t\} \subseteq \mathcal{B}$ y $\{\frac{g_1}{f^{c_1}}, ..., \frac{g_t}{f^{c_t}}\} \subseteq R[X]_f$ tales que $\sum_{k=1}^{t} \frac{g_k}{f^{c_k}} m_k = 0$. Entonces

$$\sum_{k=1}^{t} \frac{f^{s_k}}{f^{s_k}} \frac{g_k}{f^{c_k}} m_k = \sum_{k=1}^{t} f^{s_k} \frac{g_k}{f^{c_k}} n_k = 0$$

Y por ser $\tilde{\mathcal{B}}$ base de M_f tenemos que $\frac{f^{s_k}g_k}{f^{c_k}} = 0$ para $1 \leq k \leq t$, y como $f \neq 0$ ha de ser $\frac{g_k}{f^{c_k}} = 0$, $1 \leq k \leq t$.

Denotamos por $F = \langle \mathcal{B} \rangle \subseteq M$, y sea $P := M/F$. Por una parte, $P_f \cong M_f/F_f$, ya que si tomamos el morfismo

$$\begin{aligned} \phi : M_f &\to P_f \\ \frac{m}{f^s} &\mapsto \frac{m+F}{f^s} \end{aligned}$$

tenemos que ϕ es sobreyectivo y $\ker(\phi) = \{\frac{m}{f^s} : \frac{m+F}{f^s} = 0 + F\} = F_f$. Aplicando el Primer Teorema de Isomorfía obtenemos el resultado. Esto, junto con el hecho de que $M_f = F_f$, nos da que $P_f = 0$, y $f^n P = 0$ para algún $n \in \mathbb{N}$. Con ello tenemos que

$$P \cong (M/F)/f^n(M/F) \cong M/(F + f^n M) \cong (M/f^n M)/((F + f^n M)/f^n M).$$

El primer "$\cong$" viene de que $f^n P := f^n(M/F) = 0$. Para el segundo, tenemos que $f^n(M/F)$ es un submódulo de M/F, por lo que es de la forma N/F con N submódulo de M y $F \subseteq N$. Precisamente, $N = f^n M + F$, con lo que $(M/F)/f^n(M/F) \cong M/F/(f^n M + F)/F \cong M/f^n M + F$. El tercero es consecuencia del Segundo Teorema de Isomorfía ($f^n M \subseteq (F + f^n M) \subseteq M$).

Aquí, como M es un módulo proyectivo finitamente generado sobre $R[X]$, por la Proposición A.5.3, $M/f^n M$ es un módulo proyectivo finitamente generado sobre $S := R[X]/(f^n)$. Como f es mónico, f^n también es mónico, y siguiendo el Ejemplo A.2.3 tenemos que el anillo residual $S = R[X]/(f^n)$ es un R-módulo libre de rango finito (igual a $t = n \cdot \deg(f)$).

Ahora veamos que $M/f^n M$ es también un R-módulo proyectivo finitamente generado. Sabemos que $M/f^n M$ es un S-módulo proyectivo, por lo que existe un S-módulo libre, $\bigoplus_X S$ y un S-módulo Q tal que

$$(M/f^n M) \oplus Q \cong \bigoplus_T S.$$

Este isomorfismo de S-módulos también será un ismorfismo de R-módulos porque $R \subseteq S$. Además, como S es un R-módulo libre de rango finito, tenemos el isomorfismo de R-módulos

$$\bigoplus_T S \cong \bigoplus_T (R^t) \cong \bigoplus_{T \times \{1,\dots,t\}} R.$$

En particular, $M/f^n M$ es un sumando directo de un R-módulo libre y por tanto es un R-módulo proyectivo. Además, es finitamente generado porque M es un $R[X]$-módulo finitamente generado: si $\{m_1, ..., m_s\}$ generan M como $R[X]$-módulo, entonces $\{m_1 + f^n M, ..., m_s + f^n M\}$ generan $M/f^n M$.

Por el Corolario 1.3.3, como $(R, \mathfrak{m})$ es anillo local, $M/f^n M$ es un R-módulo libre. Finalmente, por el Lema A.2.2 $M/f^n M$ es libre de rango finito. Hemos probado así que $M/f^n M$ es un R-módulo libre de rango finito.

Por otra parte, $(F + f^n M)/f^n M$ es también finitamente generado como R-módulo. Veámoslo. Primero tomamos la base $\mathcal{B} = \{m_1, ..., m_r\}$ de F como $R[X]$-módulo. Ahora multiplicamos por potencias de X

$$\mathcal{B}' = \{X^k m_i : 0 \leq k \leq \deg_X(f^n) - 1, 1 \leq i \leq r\}.$$

$\mathcal{B}'$ es sistema generador de $F + f^n M/f^n M$ como R-módulo. Dado $h \in F + f^n M$, se expresa como

$$h = \sum_{i=1}^{r} h_i(X) m_i + g,$$

donde $g \in f^n M, h_i(X) \in R[X], (i = 1, ..., r)$. Como f es mónico, f^n también lo es, y podemos dividir cada $h_i(X)$ por f^n. Es decir

$$h_i(X) = q_i(X) f^n + r_i(X) \qquad (i = 1, ..., r),$$

tal que $\deg_X(r_i(X)) \leq \deg_X(f^n) - 1, \forall i \in \{1, ..., r\}$. Así, podemos reescribir la combinación anterior

$$h = \sum_{i=1}^{r} h_i(X)m_i + g = \sum_{i=1}^{r} r_i(X)m_i + \sum_{i=1}^{r} q_i(X)f^n m_i + g.$$

Ahora bien, $g_1 := \sum_{i=1}^{r} q_i(X)f^n m_i + g \in f^n M$ y además

$$h - g_1 = \sum_{i=1}^{r} r_i(X)m_i.$$

Pero cada $r_i(X)$ es un polinomio de grado acotado por $\deg_X(f^n) - 1$, por lo que podemos suponer

$$r_i(X) = \sum_{k=0}^{\deg(f^n)-1} a_{ik}X^k, \quad a_{ik} \in R \qquad (i = 1, ..., r),$$

con lo que

$$h - g_1 = \sum_{i=1}^{r} \sum_{k=0}^{\deg(f^n)-1} a_{ik}X^k m_i.$$

Por tanto, $h + f^n M$ es combinación lineal de elementos de $\mathcal{B}'$ con coeficientes en R:

$$h + f^n M = (\sum_{i=1}^{r} \sum_{k=0}^{\deg(f^n)-1} a_{ik}X^k m_i) + f^n M,$$

por lo que $F + f^n M/f^n M$ es un R-módulo finitamente generado.

Así, tenemos la sucesión exacta corta siguiente:

$$0 \to F + f^n M/f^n M \to M/f^n M \to P \to 0,$$

donde $M/f^n M$ es un R-módulo libre y $F + f^n M/f^n M$ es un R-módulo finitamente generado. Por tanto, P es un R-módulo proyectivo finitamente presentado.

Si $\overline{f}$ es la imagen de f en $(R/\mathfrak{m})[X]$, entonces $(F/\mathfrak{m}F)_{\overline{f}} = (M/\mathfrak{m}M)_{\overline{f}}$, y con ello el morfismo canónico $F/\mathfrak{m}F \longrightarrow M/\mathfrak{m}M$ es inyectivo. Ahora como M es proyectivo como R-módulo (porque $R[X]$ es un R-módulo libre), podemos aplicar la Proposición 1.3.2 a la sucesión exacta

$$0 \to F \to M \to P \to 0.$$

Con ello obtenemos que P es libre como R-módulo y $M \cong P \oplus F$ como R-módulos.

A continuación, vamos a construir una familia de generadores de M del modo siguiente: primero, elijamos una base de $P = M/F$ como R-módulo libre formada por elementos de M módulo F:

$$\mathcal{B}_1 = \{m_1 + F, ..., m_s + F\} = \{p_1, ..., p_s\},$$

donde $m_1, ..., m_s \in M$. Por otra parte, como F es un $R[X]$-módulo libre por construcción, posee una base $\mathcal{B}$ construida anteriormente, que ahora designamos como

$$\mathcal{B} = \{p_{s+1}, ..., p_t\},$$

donde $t - s = \text{rank}_{R[X]_f}(M_f)$.

Observemos ahora que como $M \cong P \oplus F$ como R-módulos, la familia

$$\mathcal{B}_2 = \mathcal{B}_1 + \mathcal{B} = \{p_1, ..., p_t\}$$

genera los elementos de M en el sentido siguiente: para cada $m \in M$, existen $\lambda_1, ..., \lambda_s \in R$ y $\mu_{s+1}, ..., \mu_t \in R[X]$ tales que

$$m = \sum_{i=1}^{s} \lambda_i p_i + \sum_{j=s+1}^{t} \mu_j p_j.$$

Para probar esto, observemos que el elemento $m+F \in M/F = P$ es una combinación lineal de los elementos de la base de P. Es decir, existirán $\lambda_1, ..., \lambda_s \in R$ tales que

$$h = m - \sum_{i=1}^{s} \lambda_1 p_i \in F.$$

A su vez, si $h \in F$, tendrá una combinación lineal única en la base F como $R[X]$-módulo libre. Es decir, existirán $\mu_{s+1}, ..., \mu_t \in R[X]$ tales que

$$h = \sum_{j=s+1}^{t} \mu_j p_j.$$

Notemos que si $s = 0$, $M = F$ y es libre como $R[X]$-modulo. Luego supongamos que $s > 0$. Para $k = 1, ..., s$, el elemento $-Xp_k$ pertenece a M por ser este un $R[X]$-módulo. Por tanto, tenemos ecuaciones de la forma

$$-Xp_k = \sum_{i=1}^{s} \alpha_{ki} p_i + \sum_{j=s+1}^{t} b_{kj} p_j \quad (\alpha_{ki} \in R, b_{kj} \in R[X]). \tag{2.4.1}$$

Ahora si tenemos una ecuación de la forma $\sum_{i=1}^{s} a_i p_i + \sum_{j=s+1}^{t} b_j p_j = 0$, $(a_i, b_j \in R[X])$, con la ayuda de las ecuaciones anteriores podemos reducirla a una ecuación de la forma

$$\sum_{i=1}^{s} \alpha_i p_i + \sum_{j=s+1}^{t} \tilde{b}_j p_j = 0 \quad (\alpha_i \in R, \tilde{b}_j \in R[X]).$$

Con esto, como $M \cong P \oplus F$, las representaciones de los elementos de M son únicas, y así tenemos que $\alpha_i = \tilde{b}_j = 0$, $(i = 1, ..., s; j = s+1, ..., t)$.

Las ecuaciones (2.4.1) pueden escribirse en forma matricial del modo siguiente:

$$(A + XId_s | B) \cdot \begin{pmatrix} p_1 \\ \vdots \\ p_s \\ p_{s+1} \\ \vdots \\ p_t \end{pmatrix} = 0,$$

donde $A = (\alpha_{ki}) \in M_{s\times s}(R), B = (b_{kj}) \in M_{s\times(t-s)}(R[X])$.

B es por tanto una matriz cuyos coeficientes son polinomios de $R[X]$. Es decir, B es de la forma

$$B = B_0 + B_1 X + ... + B_m X^m,$$

con $B_i \in M_{s\times(t-s)}(R), i = 0, ..., m$. Ahora podemos efectuar la división con resto de B entre el polinomio $A + XId_s$. Obtenemos que

$$B = B^* + (A + XId_s)\tilde{B},$$

con $B^*, \tilde{B} \in M_{s\times(t-s)}(R[X])$, y además $\deg_X(B^*) < \deg_X(A + XId_s) = 1$, o equivalentemente, $B^* \in M_{s\times(t-s)}(R)$.

Con este resultado podemos escribir las ecuaciones (2.4.1) como

$$(A + XId_s) \cdot \left[\begin{pmatrix} p_1 \\ \vdots \\ p_s \end{pmatrix} + \tilde{B} \begin{pmatrix} p_{s+1} \\ \vdots \\ p_t \end{pmatrix} \right] + B^* \begin{pmatrix} p_{s+1} \\ \vdots \\ p_t \end{pmatrix} = 0.$$

Observemos ahora que dados $h_1, ..., h_s \in F$, si consideramos los elementos $q_i = p_i + h_i \in M$, $(i = 1, ..., s)$, entonces el conjunto

$$\{q_1 + F, ..., q_s + F\} \subseteq M/F = P$$

es también una base de P como R-módulo libre. Si definimos

$$\begin{pmatrix} h_1 \\ \vdots \\ h_s \end{pmatrix} = \tilde{B} \begin{pmatrix} p_{s+1} \\ \vdots \\ p_t \end{pmatrix},$$

tenemos un vector de elementos de F que es $R[X]$-módulo libre. Así, la matriz $(A + XId_s|B)$ tal que

$$(A + XId_s|B) \cdot \begin{pmatrix} p_1 \\ \vdots \\ p_s \\ p_{s+1} \\ \vdots \\ p_t \end{pmatrix} = 0,$$

se puede construir suponiendo que la matriz B tiene coeficientes solamente en R. A partir de aquí supondremos que este es el caso, es decir $B = (\beta_{kj}) \in M_{s\times(t-s)}(R)$.

Ahora vamos a probar la siguiente

Afirmación. *El ideal J de $R[X]$ generado por los menores de tamaño $s \times s$ de $(A + XId_s|B)$ coincide con $R[X]$.*

Demostración de la Afirmación. Consideramos $\mathfrak{m} \in \mathrm{MaxSpec}(R[X])$. Por el Teorema 1.3.4, $M_{\mathfrak{m}}$ es libre como $R[X]_{\mathfrak{m}}$-módulo, por ser M proyectivo y finitamente generado. Además, como $M_f = F_f$ como $R[X]$-módulos, se tiene que $(M_{\mathfrak{m}})_f = (F_{\mathfrak{m}})_f$ como $R[X]_{\mathfrak{m}}$-módulos. Como consecuencia,

$$\mathrm{rank}_{R[X]}(M_{\mathfrak{m}}) = \mathrm{rank}_{R[X]}(F_{\mathfrak{m}}) = t - s.$$

Por otra parte, consideramos la sucesión exacta

$$0 \to K \to R[X]^t_{\mathfrak{m}} \to M_{\mathfrak{m}} \to 0,$$

donde K es el submódulo de $R[X]^t_{\mathfrak{m}}$ generado por las filas de la matriz $(A + XId_s|B)$. Esta es escindida por ser $M_{\mathfrak{m}}$ libre. Por tanto, $R[X]^t_{\mathfrak{m}} \cong M_{\mathfrak{m}} \oplus K$ y encontramos que K es un $R[X]_{\mathfrak{m}}$-módulo libre de rango s. Entonces, como las filas de $(A + XId_s|B)$ se pueden extender hasta una base de $R[X]^t_{\mathfrak{m}}$, al menos uno de los menores $s \times s$ ha de ser una unidad en $R[X]_{\mathfrak{m}}$. Por tanto, tenemos que $J_{\mathfrak{m}} = R[X]_{\mathfrak{m}}$ y como la igualdad de ideales es una propiedad local concluimos que $J = R[X]$.

La afirmación anterior nos lleva a que

$$R[X] = R[X] \cdot g + R[X] \cdot I,$$

donde $g := det(A + XId_s)$ e $I = (\{\beta_{kj}\})$ es el ideal de R generado por los coeficientes de B. Esto es porque claramente el ideal suma $(g) + I$ contiene a $J = R[X]$. Observemos que g es un polinomio mónico, porque A es una matriz con coeficientes solamente en R. Por tanto, el anillo $T := R[X]/(g)$ es libre como R-módulo. Haciendo el cociente por (g), tenemos que

$$T = T \cdot g + T \cdot I.$$

Pero $T \cdot g = R[X]/(g) \cdot g = 0$, luego $T = T \cdot I$. Por tanto, necesariamente $I = R$. Finalmente, como $(R, \mathfrak{m})$ es local y $\mathfrak{m} = R \setminus R^* \subsetneq I = (\{\beta_{kj}\})$, tenemos que al menos un coeficiente de B es una unidad de R.

Como consecuencia de lo anterior, podemos hacer operaciones elementales en filas y columnas hasta llevar la matriz $(A + XId_s|B)$ a una matriz de la forma

$$\left(\begin{array}{c|c} & 0 \\ A' + XId_{s-1}|B' & \vdots \\ & 0 \\ \hline 0 \ \ldots \ 0 & 1 \end{array}\right)$$

donde A' y B' son matrices con coeficientes en R, e Id_{s-1} es la matriz identidad.

Observemos que en el apartado anterior solo hemos modificado la matriz con operaciones elementales en filas y columnas. Por ello, podemos aplicar de nuevo el mismo argumento que antes a $(A'+XId_{s-1}|B')$. Repitiendo el proceso s veces, podemos llevar la matriz inicial $(A+XId_s|B)$ a una matriz de la forma

$$(0|Id_s)$$

donde Id_s es la matriz identidad. Pero esto significa precisamente que M es un $R[X]$-módulo libre de rango $t-s$, q.e.d. □

CAPÍTULO 3

El Teorema de Quillen-Suslin y algunas aplicaciones.

Índice

3.1. Introducción **35**
3.1.1. Resumen relativo a la resolución final de la Ex-Conjetura de Serre 35
3.1.2. Una aplicación: trivialidad de anillos módulo sucesiones regulares con respecto a una normalización de Noether 36
3.2. El Teorema de Quillen-Suslin. **37**
3.3. Respuestas a las preguntas de Serre. **40**
3.4. Aplicación del Teorema de Quillen-Suslin al ejemplo paradigmático de anillo de Cohen-Macaulay **41**
3.4.1. Trivialidad global de las intersecciones completas con respecto a una normalización de Noether 43

3.1. Introducción

El tercer y último Capítulo tiene un doble propósito: en primer lugar, vamos a culminar todos los esfuerzos técnicos precedentes para exhibir la resolución de la Ex-Conjetura de Serre; y en segundo lugar, vamos a dar una sencilla aplicación del Teorema de Quillen-Suslin que tuvo gran impacto en el desarrollo de algoritmos eficientes en Geometría Algebraica (a través de la corriente TERA) en la última década del siglo pasado. Presentaremos esos resultados en dos subsecciones separadas de esta introducción.

3.1.1. Resumen relativo a la resolución final de la Ex-Conjetura de Serre.

En los trabajos [**Quillen, 1976**] y [**Suslin, 1976**], D. Quillen y A. A. Suslin resolvieron simultánea e independientemente la Conjetura de Serre. El enunciado final se muestra y se prueba en la Sección 3.3 y se enuncia del modo siguiente:

TEOREMA 3.1.1. *Sea K un dominio de ideales principales, $R = K[X_1, ..., X_n]$ el anillo de polinomios en varias variables con coeficientes en K. Sea M un R-módulo finitamente generado. Son equivalentes:*

i) M es libre y finitamente presentado.
ii) M es proyectivo.
iii) $M_{\mathfrak{p}}$ es libre como $R_{\mathfrak{p}}$-módulo, $\forall \mathfrak{p} \in \mathrm{Spec}(R)$.
iv) $M_{\mathfrak{m}}$ es libre como $R_{\mathfrak{m}}$-módulo, $\forall \mathfrak{m} \in \mathrm{MaxSpec}(R)$.

Obviamente, y tras lo discutido en los Capítulos 1 y 2, la tarea se reduce a probar que $iv) \Longrightarrow i)$. La prueba es por inducción en n y tiene como ingrediente fundamental un Teorema que se enuncia y demuestra al comienzo de la Sección 3.2. Ese elemento técnico esencial es también conocido como Teorema de Quillen-Suslin y consiste en probar que el Teorema de Horrocks es válido en el caso de cualquier anillo R. Es decir, la Sección 3.2 se dedica a probar el siguiente enunciado:

TEOREMA 3.1.2 (**Teorema de Quillen-Suslin**). *Sea R un anillo cualquiera y sea M un $R[X]$-módulo proyectivo finitamente generado. Sea $f \in R[X]$ un polinomio mónico tal que M_f es un $R_f[X]$-módulo libre. Entonces M es libre como $R[X]$-módulo.*

Cabe aclarar que la demostración de este resultado que se presenta aquí es la elaborada por Quillen. Esta utiliza resultados técnicos de Capítulos precedentes, como el Primer Teorema

de Quillen o el Teorema de Horrocks. Adicionalmente, usa el producto fibrado de módulos de un modo excepcionalmente ingenioso para concluir sus propósitos. Esta demostración es el objetivo esencial del Trabajo Fin de Grado.

3.1.2. Una aplicación: trivialidad de anillos módulo sucesiones regulares con respecto a una normalización de Noether.

Este Trabajo Fin de Grado podría parecer hasta aquí excesivamente abstracto, aunque el Teorema de Quillen-Suslin sea uno de los momentos mágicos del Álgebra Conmutativa del pasado siglo. Por ello, hemos pretendido incluir una aplicación de este resultado; aunque pueda parecer un resultado poco trascendente. Así, en la Sección 3.4 probaremos el siguiente resultado:

TEOREMA 3.1.3. *Sea K un cuerpo algebraicamente cerrado y sea $\mathfrak{a} = (f_1, ..., f_r) \subseteq K[X_1, ..., X_n]$ un ideal de altura r generado por r elementos. Supongamos que tenemos unas nuevas variables $Y_1, ..., Y_n$ de tal modo que la siguiente es una extensión entera de anillos:*

$$A = K[Y_1, ..., Y_{n-r}] \hookrightarrow B = K[X_1, ..., X_n]/\mathfrak{a}.$$

Entonces B es un A-módulo libre de rango finito.

La familia de polinomios $\{f_1, ..., f_r\}$ que genera el ideal $\mathfrak{a}$ de altura r se suele denominar "sucesión secante". Las variables $\{Y_1, ..., Y_n\}$ que hacen que la extensión sea entera se dice que están "en posición de Noether". Luego el anillo de clases residuales de $K[X_1, ..., X_n]$ módulo un ideal generado por una sucesión secante es un módulo libre sobre una normalización de Noether.

A primera vista es solo un resultado técnico más. Supongamos que nuestra sucesión $\{f_1, ..., f_r\}$ secante satisface una propiedad más: el ideal $\mathfrak{a} = (f_1, ..., f_r)$ que genera es un ideal radical (i.e. $\sqrt{\mathfrak{a}} = \mathfrak{a}$). En ese caso se dice que la sucesión $\{f_1, ..., f_r\}$ es una *sucesión secante reducida* (o que la variedad de sus ceros $V = V_{\mathbb{A}}(\mathfrak{a})$ es una variedad intersección completa en el plano de los ideales). Si disponemos de una sucesión secante reducida y de una normalización de Noether de la forma siguiente:

$$A = K[Y_1, ..., Y_{n-r}] \hookrightarrow B = K[X_1, ..., X_n]/\mathfrak{a}. \tag{3.1.1}$$

Entonces B es un A-módulo libre de rango finito y la desigualdad de Bézout geométrica (en el espacio afín) de [**Heintz, 1983**] implica la siguiente cota para el rango de B:

$$\operatorname{rank}_A(B) \leq \prod_{i=1}^{r} \deg(f_i).$$

Ahora consideremos $F = Q(A)$ el cuerpo de fracciones de A y hagamos extensión de escalares

$$F = F \otimes_A A \hookrightarrow F \otimes_A B.$$

La extensión es algebraica cero-dimensional. En particular, $F \otimes_A B$ es un F-espacio vectorial de dimensión finita. Por ser B un A-módulo libre de rango finito, se tendrá:

$$D = \dim_F(F \otimes_A B) = \operatorname{rank}_A(B) \leq \prod_{i=1}^{r} \deg(f_i).$$

Más aún, los cálculos de eliminación en el anillo residual B se pueden releer como cálculos de eliminación en el espacio vectorial $F \otimes_A B$ de dimensión finita sobre F. En otras palabras, como la base de B como A-módulo libre se extiende a una base de $F \otimes_A B$ como F espacio vectorial, todos los cálculos matriciales relativos a la extensión $A \hookrightarrow B$ pueden hacerse como cálculos matriciales sobre el cuerpo F (es decir, en $M_D(F)$). Además, los elementos esenciales sobre endomorfismos $\varphi : B \to B$ se preservan si lo vemos como endomorfismo de espacios vectoriales $i \otimes \varphi : F \otimes_A B \to F \otimes_A B$.

Esta fue una de las ideas claves del desarrollo de los trabajos del colectivo TERA en la última década del siglo pasado (desde [**Pardo, 1995**] hasta [**GHMP, 1997**] o [**GHMMP, 1998**] y sus referencias). Estos autores desarrollaron el mejor algoritmo (el más eficiente posible) para la resolución simbólica de ecuaciones polinomiales multivariadas y, más tarde, probaron que era

imposible mejorar sus técnicas (salvo alguna mejora en el exponente constante, aspecto en el que han trabajado decenas de autores en cientos de publicaciones posteriores).

Estos aspectos no son tema de este Trabajo Fin de Grado, pero sirven para decir que el pequeño Teorema que se prueba en la Sección 3.4, como consecuencia del Teorema de Quillen-Suslin, no es un resultado sin trascendencia posterior.

3.2. El Teorema de Quillen-Suslin.

Como ya se ha indicado en la Introducción, el elemento técnico fundamental del Teorema de Quillen-Suslin consiste en "pasar de local a global" el Teorema de Horrocks (Teorema 2.4.1). En ello juegan un papel esencial varios de los resultados técnicos expuestos en capítulos anteriores, especialmente en el Capítulo 2.

TEOREMA 3.2.1 (**Teorema de Quillen-Suslin**). *Sea M un $R[X]$-módulo proyectivo finitamente generado, y sea $f \in R[X]$ un polinomio mónico tal que M_f es un $R_f[X]$-módulo libre. Entonces M es libre como $R[X]$-módulo.*

DEMOSTRACIÓN. La prueba del Teorema la vamos a dividir en tres partes, de forma que la demostración se reduce a probar tres afirmaciones. La primera de ellas es la siguiente:

AFIRMACIÓN. *Con las hipótesis del enunciado, M es un $R[X]$-módulo extendido.*

DEMOSTRACIÓN DE LA AFIRMACIÓN. Como M_f es un $R[X]_f$-módulo libre, para cualquier ideal maximal $\mathfrak{m} \in \mathrm{MaxSpec}(R)$, localizando y recordando que la localización es un functor exacto (es decir, conmuta con la suma directa), concluiremos que

$$(M_f)_{\mathfrak{m}} \cong (M_{\mathfrak{m}})_f$$

son isomorfos como $R_{\mathfrak{m}}[X]_f$-módulos. Por tanto, ambos son $R_{\mathfrak{m}}[X]_f$-módulos libres. Con ello, por el Teorema de Horrocks el módulo $M_{\mathfrak{m}}$ es un $R_{\mathfrak{m}}[X]$-módulo libre. Ahora sabemos que todo $R_{\mathfrak{m}}[X]$-módulo libre es un $R_{\mathfrak{m}}[X]$-módulo extendido, por la siguiente cadena de isomorfismos

$$M_{\mathfrak{m}} \cong \bigoplus_T (R_{\mathfrak{m}}[X]) \cong R_{\mathfrak{m}}[X] \otimes_{R_{\mathfrak{m}}} (\bigoplus_T R_{\mathfrak{m}}).$$

Con esto hemos probado que M es un $R[X]$-módulo localmente extendido. Por el Primer Teorema de Quillen concluimos que M es un $R[X]$-módulo extendido.

La afirmación anterior prueba que existe un R-módulo N tal que $M = N[X]$, es decir, se tienen los isomorfismos de $R[X]$-módulos siguientes:

$$M \cong N[X] \cong R[X] \otimes_R N.$$

Si probamos que $N = M/(X-1)M$ es un R-módulo libre habremos probado que M es libre como $R[X]$-módulo, ya que $R[X] \otimes_R -$ es un functor que conmuta con la suma directa y $R[X]$ es libre como R-módulo.

Para ello, vamos a construir una cierta extensión de M. Comenzamos considerando la localización del anillo $R[X]$ en la variable X, $R[X]_X$. Consideramos también una cierta variable X^{-1}, el anillo de polinomios $R[X^{-1}]$ y tomemos la siguiente identificación (isomorfismo de R-álgebras):

$$\begin{aligned} i : R[X]_X &\to R[X^{-1}]_{X^{-1}} \\ \frac{1}{X} &\mapsto X^{-1}. \end{aligned}$$

Con esta identificación podemos interpretar ambos anillos como el anillo de polinomios de Laurent en una variable

$$R[X, X^{-1}] = \{ \sum_{i=-k}^{m} a_k X^k : k, m \in \mathbb{N},\ a_k \in R \},$$

$$R[X, X^{-1}] \cong R[X]_X \cong R[X^{-1}]_{X^{-1}}.$$

Ahora vamos a sumergir los espectros primos $\mathrm{Spec}(R[X])$ y $\mathrm{Spec}(R[X^{-1}])$ dentro del espectro primo de $R[X, X^{-1}]$ como abiertos en la topología de Zariski (de hecho, como dos abiertos distinguidos):

$$\mathrm{Spec}(R[X]) \cong D(X) = \{\mathfrak{p} \in \mathrm{Spec}(R[X, X^{-1}]) : X \notin \mathfrak{p}\}$$
$$\mathrm{Spec}(R[X^{-1}]) \cong D(X^{-1}) = \{\mathfrak{p} \in \mathrm{Spec}(R[X, X^{-1}]) : X^{-1} \notin \mathfrak{p}\}$$

El espectro de $R[X, X^{-1}]$ suele llamarse recta proyectiva sobre $R[X]$.

Sea ahora $f \in R[X]$ el polinomio mónico del enunciado. Podemos suponer que f tiene la forma siguiente:

$$f = X^n + a_1 X^{n-1} + ... + a_n.$$

Definamos el polinomio $g \in R[X^{-1}]$ dado mediante

$$g = 1 + a_1 X^{-1} + ... + a_n (X^{-1})^n.$$

Como $g = X^{-n} f$ en $R[X, X^{-1}]$ y como X^{-n} es una unidad en $R[X, X^{-1}]$, tenemos que $R[X, X^{-1}]_f \cong R[X, X^{-1}]_g$ como anillos. Además, $(M_X)_f \cong (M_X)_g$ es un $R[X, X^{-1}]_g$-módulo libre, por ser M_f un $R[X]_f$-módulo libre.

Denotemos por $A = R[X^{-1}]$ y consideremos

$$M_1 = M_X \text{ como } R[X, X^{-1}]\text{-módulo,}$$
$$M_2 = (M_X)_g \text{ como } A_g\text{-módulo.}$$

Nótese que con la identificación anterior, $A_{X^{-1}} \cong R[X, X^{-1}]$ y M_1 puede ser visto como $A_{X^{-1}}$-módulo. Además, $M_1 = M_X$ es un $A_{X^{-1}}$-módulo proyectivo y finitamente generado (la condición de proyectivo se preserva por localización), y por tanto tenemos que M_1 es finitamente presentado y localmente libre (cf. Teorema 1.3.4).

De otro lado, hemos visto ya que $M_2 = (M_X)_g$ es un $R[X, X^{-1}]_g$ módulo libre de rango finito. Sea $\mathcal{B} = \{v_1, ..., v_m\}$ una base de $(M_X)_g$ y consideremos el módulo libre sobre A_g generado por dicha base, es decir,

$$M_2 = \bigoplus_{\mathcal{B}} A_g.$$

Ahora, con la identificación

$$A_{X^{-1}g} \cong (A_g)_{X^{-1}} \cong (A_{X^{-1}})_g \cong R[X, X^{-1}]_g,$$

podemos localizar M_2 por X^{-1}, o lo que es lo mismo, hacer extensión de escalares para obtener

$$(M_2)_{X^{-1}} = R[X, X^{-1}] \otimes_{A_g} A_g \cong \bigoplus_{\mathcal{B}} R[X, X^{-1}]_g \cong (M_X)_g = (M_1)_g,$$

donde los isomorfismos son como $R[X, X^{-1}]_g$-módulos.

Denotemos por $\alpha : (M_1)_g \to (M_2)_{X^{-1}}$ ese isomorfismo. Siguiendo la construcción del Apéndice A.8, consideremos el $A_{X^{-1}g}$-módulo

$$N := (M_2)_{X^{-1}} = (M_X)_g,$$

y sean

$$\alpha_1 := \alpha \circ i_1 : M_1 \to N,$$
$$\alpha_2 := i_2 : M_2 \to N,$$

donde i_1 e i_2 son las inclusiones canónicas

$$i_1 : M_1 \to (M_1)_g,$$
$$i_2 : M_2 \to (M_2)_{X^{-1}}.$$

Por la Proposición A.8.1, existe el producto fibrado sobre N

$$P := M_1 \prod_N M_2,$$

con respecto a α_1, α_2. Además, por la Proposición A.8.3 ese producto fibrado induce isomorfismos:

$\theta_1 : P_{X^{-1}} \to M_1$, isomorfismo de $A_{X^{-1}}$-módulos, (es decir, de $R[X, X^{-1}]$-módulos)
$\theta_2 : P_g \to M_2$, isomorfismo de A_g-módulos (es decir, de $R[X^{-1}]_g$-módulos).

AFIRMACIÓN. *El producto fibrado P definido mediante la construcción precedente satisface las siguientes propiedades:*

i) $P_{X^{-1}}$ es un $A_{X^{-1}}$-módulo finitamente presentado.
ii) P_g es un A_g-módulo finitamente presentado.
iii) P es finitamente presentado como $R[X^{-1}]$-módulo.

DEMOSTRACIÓN DE LA AFIRMACIÓN. Antes que nada, observemos que el espectro primo de $R[X^{-1}]$ se descompone del modo siguiente:

$$\operatorname{Spec}(R[X^{-1}]) = D_1(X^{-1}) \cup D_1(g), \tag{3.2.1}$$

donde

$$D_1(X^{-1}) = \{\mathfrak{q} \in \operatorname{Spec}(R[X^{-1}]) : X^{-1} \notin \mathfrak{q}\},$$
$$D_1(g) = \{\mathfrak{q} \in \operatorname{Spec}(R[X^{-1}]) : g \notin \mathfrak{q}\}.$$

La razón es porque el ideal suma (X^{-1}, g) en $R[X^{-1}]$ es el ideal trivial. Como f era mónico, tenemos que

$$g - \sum_{i=1}^{n} a_i (X^{-1})^i = 1 \in (X^{-1}, g).$$

Por tanto, no hay ningún ideal primo que contenga simultáneamente a X^{-1} y g, dándose así la igualdad (3.2.1).

i) Ya hemos visto, por el isomorfismo θ_1, que $P_{X^{-1}}$ es isomorfo a $M_1 = M_X$, el cual también hemos visto que era finitamente presentado.

ii) Por el isomorfismo θ_2, $P_g \cong M_2 = \bigoplus_{\mathcal{B}} A_g$ como A_g-módulos. Como los módulos libres de rango finito son finitamente presentados (por la sucesión exacta corta $0 \to 0 \to A_g^m \to A_g^m \to 0$), concluimos que P_g es un A_g-módulo finitamente presentado.

iii) Finalmente, con el punto *i*) y *ii*), y el hecho de que $\operatorname{Spec}(R[X^{-1}]) = D_1(X^{-1}) \cup D_1(g)$, estamos en condiciones de aplicar la Proposición 1.2.13. Con ello, concluimos que P es finitamente presentado como $R[X^{-1}]$-módulo.

Finalmente, podemos concluir la última afirmación que completa la prueba.

AFIRMACIÓN. *M es un $R[X]$-módulo libre.*

DEMOSTRACIÓN DE LA AFIRMACIÓN. Sea $\mathfrak{m} \in \operatorname{MaxSpec}(R)$. Consideremos el módulo

$$(P_{\mathfrak{m}})_{X^{-1}} \cong (M_{\mathfrak{m}})_X,$$

donde el isomorfismo se considera entre $R_{\mathfrak{m}}[X, X^{-1}]$-módulos. Por la afirmación precedente, $P_{X^{-1}}$ es isomorfo a M_X, luego ambas localizaciones siguen siendo isomorfas como $R_{\mathfrak{m}}[X, X^{-1}]$-módulos.

De otro lado, en la demostración de la Afirmación 1 vimos que para cada $\mathfrak{m} \in \operatorname{MaxSpec}(R)$, $M_{\mathfrak{m}}$ es libre como $R_{\mathfrak{m}}[X]$-módulo. Por tanto, como la localización es exacta, $(M_{\mathfrak{m}})_X$ es un $R_{\mathfrak{m}}[X]_X$-módulo libre de rango finito. Con ello, $(P_{\mathfrak{m}})_{X^{-1}}$ es un $R_{\mathfrak{m}}[X, X^{-1}]$-módulo libre de rango finito.

Ahora observemos que X^{-1} es un polinomio mónico en el anillo $R[X^{-1}]$. Por el Teorema de Horrocks, concluimos que $P_{\mathfrak{m}}$ es un $R_{\mathfrak{m}}[X]$-módulo libre de rango finito.

Además, hemos visto en la Afirmación 2 que P es finitamente presentado y localmente libre como $R[X^{-1}]$-módulo. Por el Primer Teorema de Quillen concluimos que P es un $R[X^{-1}]$-módulo extendido. Es decir, existe un R-módulo N' tal que

$$P \cong N'[X^{-1}] = R[X^{-1}] \otimes_R N'.$$

Se puede observar también que

$$N' \cong P/X^{-1}P \cong P/(X^{-1} - 1)P. \tag{3.2.2}$$

De otro lado, P_g es un $R[X^{-1}]_g$-módulo libre y se tiene:

$$g + (X^{-1}) = 1 + (X^{-1})$$

en $R[X^{-1}]$. Por tanto, g es unidad en $R[X^{-1}]/(X^{-1})$ y se tendrá

$$P_g/X^{-1}P_g = (P/X^{-1}P)_g \cong P/X^{-1}P,$$

que es un R-módulo libre de rango finito. Por (3.2.2), $P/(X^{-1}-1)P$ también es un R-módulo libre de rango finito.

Finalmente, observemos que

$$M/(X-1)M \cong M_X/(X-1)M_X \cong P_{X^{-1}}/(X^{-1}-1)P_{X^{-1}}.$$

Por tanto, son isomorfos como R-módulos

$$M/(X-1)M \cong P/(X-1)P.$$

Retomando la Afirmación 1, $M = N[X]$ era un $R[X]$-módulo extendido y

$$N \cong M/(X-1)M \cong P/(X-1)P$$

es un R-módulo libre. Es decir, existe $m \in \mathbb{N}$ tal que $N \cong R^m$ como R-módulos. Tensorizando con $R[X]$ tenemos

$$M = N[X] = R[X] \otimes_R R^m \cong (R[X])^m,$$

lo que permite concluir que M es un $R[X]$-módulo libre de rango finito, q.e.d. □

3.3. Respuestas a las preguntas de Serre.

Con todo lo expuesto anteriormente, estamos en condiciones de probar la Conjetura de Serre, que ahora pasa a ser Teorema.

TEOREMA 3.3.1 (**Ex-Conjetura de Serre**). *Si K es un dominio de ideales principales, todo $K[X_1, ..., X_n]$-módulo proyectivo finitamente generado es libre.*

DEMOSTRACIÓN. La demostración se realiza por inducción sobre n. Para $n = 0$ la afirmación es correcta. Dado M un K-módulo proyectivo finitamente generado, M es libre, ya que todos los submódulos de un módulo libre de rango finito sobre un dominio de ideales principales son libres.

Ahora sea $n > 0$ y supongamos que la afirmación ha sido probada para $K[X_1, ..., X_{n-1}]$. Sea M un módulo proyectivo finitamente generado sobre $K[X_1, ..., X_n]$, y consideremos S el sistema multiplicativamente cerrado formado por todos los polinomios mónicos de $K[X_1]$. Entonces $S^{-1}M$ es un módulo proyectivo sobre $S^{-1}K[X_1, ..., X_n] = S^{-1}K[X_1][X_2, ..., X_n]$.

Veamos ahora que $S^{-1}K[X_1]$ es un anillo de ideales principales. Sea $R := S^{-1}K[X_1]$. Como $K[X_1]$ es un dominio de factorización única, sabemos que R también lo es. Dado ahora $\mathfrak{p} \in \mathrm{Spec}(R)$ con $\mathfrak{p} \cap K = (0)$, $R_{\mathfrak{p}}$ es un anillo de fracciones en $Q(K)[X_1]$, donde $Q(K)$ denota el cuerpo de fracciones de K. Con ello, $\mathrm{ht}(\mathfrak{p}) \leq 1$ y $\mathfrak{p}$ es un ideal principal. De otro lado, si $\mathfrak{p} \cap K = (p)$ con $p \in K$ un elemento primo, entonces $R/pR := K/(p)(X_1)$ es un cuerpo, y por tanto $\mathfrak{p} = pR$. Así, cada $\mathfrak{p} \in \mathrm{Spec}(R)$, $\mathfrak{p} \neq (0)$, está generado por un elemento primo π de R. Consideremos ahora $a_1, a_2 \in R \setminus \{0\}$, y sea c el máximo común divisor de a_1, a_2. Si $\mathfrak{p} = (\pi)$ es un ideal primo de R y π aparece en la factorización de a_1 elevado a la potencia ν_i $(i = 1, 2)$, entonces aparece en la factorización de c elevado a la potencia $\min\{\nu_1, \nu_2\}$. Por tanto,

$$(a_1, a_2)R_{\mathfrak{p}} = cR_{\mathfrak{p}}, \quad \forall \mathfrak{p} \in \mathrm{Spec}(R),$$

de lo cual concluimos que $(a_1, a_2) = (c)$ y R es un anillo de ideales principales.

Así, $S^{-1}M$ es un $S^{-1}K[X_1, ..., X_n]$-módulo libre por hipótesis de inducción. Finalmente, para aplicar el Teorema de Quillen-Suslin tenemos que ver que existe un polinomio $f \in S$ tal que M_f es un $K[X_1, ..., X_n]_f$-módulo libre. Esto lo haremos a continuación, de forma análoga a la demostración del Teorema 1.3.5.

En primer lugar, sea $\{m_i\}_{i\in I}$ una base de $S^{-1}M$. Podemos tomar cada uno de estos m_i como la imagen de elementos m_i^* de M, multiplicando todos por un denominador común. Así, tenemos una nueva base de $S^{-1}M$, $\{m_i^*\}_{i\in I}$. Consideremos ahora la sucesión exacta corta

$$0 \to U \to \bigoplus_I K[X_1, ..., X_n] \xrightarrow{\alpha} M \to C \to 0,$$

donde α lleva los elementos de la base canónica e_i en m_i^*, $(i \in I)$, y $U := \ker(\alpha)$, $C := \operatorname{coker}(\alpha) = M/Im(\alpha)$. Notemos que, como $\{m_i^*\}_{i\in I}$ generan $S^{-1}M$, tenemos que $S^{-1}C = S^{-1}U = \{0\}$. Ahora, como C es finitamente generado (por serlo M), sabemos que existe $g_1 \in S$ tal que

$$C_{g_1} = \{0\}.$$

Ahora la sucesión exacta corta

$$0 \to U_{g_1} \to \bigoplus_I K[X_1, ..., X_n]_{g_1} \xrightarrow{\alpha} M_{g_1} \to 0$$

es escindida ya que M_{g_1} es proyectivo como $K[X_1, ..., X_n]_{g_1}$-módulo. Por tanto,

$$\bigoplus_I K[X_1, ..., X_n]_{g_1} \cong U_{g_1} \oplus M_{g_1},$$

y como M_{g_1} y $\bigoplus_I K[X_1, ..., X_n]_{g_1}$ son finitamente generados, U_{g_1} también lo es. De igual forma que antes, como $S^{-1}U = \{0\}$, existirá $g_2 \in S$ con $U_{g_1g_2} = \{0\}$. Llamando $f := g_1g_2 \in S$, la siguiente es una sucesión exacta

$$0 \to \bigoplus_I K[X_1, ..., X_n]_f \to M_f \to 0,$$

y por tanto M_f es un $K[X_1, ..., X_n]_f$-módulo libre. Con ello, podemos aplicar el Teorema de Quillen-Suslin, concluyendo que M es un $K[X_1, ..., X_n]$-módulo libre. □

3.4. Aplicación del Teorema de Quillen-Suslin al ejemplo paradigmático de anillo de Cohen-Macaulay

En esta Sección vamos a demostrar el Teorema 3.1.3 que hemos enunciado en la Introducción del Capítulo. Como explicábamos allí, se trata de un resultado de gran impacto en el desarrollo de algoritmos de complejidad intrínseca del contexto TERA-Kronecker. El resultado establece que los anillos de Cohen-Macaulay paradigmáticos son módulos libres de rango finito sobre cualquier normalización de Noether. El resultado, consecuencia del Teorema de Quillen-Suslin, aparece enunciado en [**RS, 1991**] o en [**GHS, 1993**].

Gracias al Lema de Normalización de Noether (Teorema B.3.7), podemos obtener el siguiente Corolario:

Corolario 3.4.1. *Sea K un cuerpo algebraicamente cerrado, $\mathfrak{a} \subseteq K[X_1, ..., X_n]$ un ideal de altura r generado por r elementos. Entonces, existe una matriz regular $P \in GL(n, K)$ que define un cambio lineal de variables en $\mathbb{A}^n(K)$*

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} = P \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix},$$

de tal modo que la siguiente es una extensión entera de anillos:

$$A^{(P)} := K[Y_1, ..., Y_{n-r}] \to B = K[X_1, ..., X_n]/\mathfrak{a},$$

y B es un $A^{(P)}$-módulo libre de rango finito.

En otras palabras, si $\mathfrak{a}$ es un ideal de altura r generado por r elementos en $K[X_1, ..., X_n]$, el anillo cociente $B = K[X_1, ..., X_n]/\mathfrak{a}$ es un módulo libre de rango finito sobre un anillo de polinomios en $n - r$ variables sobre el cuerpo K, y dichas variables son combinaciones lineales de las variables $X_1, ..., X_n$.

Por otra parte, podemos usar la Desigualdad de Bézout en el espacio afín $\mathbb{A}^n(K)$ (ver [**Heintz, 1983**] o [**Fdez, 2021**]) para dar cotas cuantitativas sobre el rango del módulo libre B. Supongamos

que $\mathfrak{a} = (f_1, ..., f_r)$ es un ideal de $K[X_1, ..., X_n]$ de altura r generado por r elementos. Supongamos además que $\mathfrak{a}$ es un ideal radical y sea $P \in GL(n, K)$ una matriz regular que genera un cambio lineal de coordenadas en $\mathbb{A}^n(K)$ que pone las variables en posición de Noether con respecto al ideal $\mathfrak{a}$, esto es, como en el Corolario, se tiene

$$A = K[Y_1, ..., Y_{n-r}] \to B = K[X_1, ..., X_n]/\mathfrak{a}.$$

Entonces B es un A-módulo libre de rango finito y

$$\operatorname{rank}_A(B) \leq \prod_{i=1}^{r} \deg(f_i).$$

Un desarrollo más detallado de esta afirmación extendería en exceso este trabajo, por lo que nos limitamos a citarla por su valor cuantitativo.

En el Apéndice B hemos recopilado un buen número de propiedades básicas y nociones relativas a anillos noetherianos, extensiones enteras y otras propiedades fundamentales del Álgebra Conmutativa. El siguiente enunciado resume las propiedades que consideramos más destacadas en los anillos tipo involucrados en el Teorema 3.1.3, que se enuncia en la Introducción.

TEOREMA 3.4.2. *Sea K un cuerpo algebraicamente cerrado, $\mathfrak{a} = (f_1, ..., f_r)$ un ideal de $K[X_1, ..., X_n]$ de altura r generado por r elementos. Se tiene:*

i) Todos los ideales primos asociados al ideal $\mathfrak{a}$ son elementos minimales del conjunto

$$\{\mathfrak{q} \in \operatorname{Spec}(K[X_1, ..., X_n]) : \mathfrak{q} \supseteq \mathfrak{a}\}.$$

ii) Los ideales minimales (y por tanto, los asociados) sobre $\mathfrak{a}$ tienen todos altura r y co-altura $n - r$.

iii) Existe una matriz regular $P \in GL(n, K)$ que define un cambio de coordenadas en $\mathbb{A}^n(K)$

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} = P \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$$

y que pone las variables $\{Y_1, ..., Y_n\}$ en posición de Noether con respecto al ideal $\mathfrak{a}$. Esto es, se tiene una extensión entera de anillos

$$A = K[Y_1, ..., Y_{n-r}] \hookrightarrow B = K[X_1, ..., X_n]/\mathfrak{a}.$$

En particular, B es un A-módulo finitamente generado y por tanto, una A-álgebra finita.

iv) Dada una descomposición primaria irredundante de $\mathfrak{a}$

$$\mathfrak{a} = \bigcap_{i=1}^{m} \mathfrak{q}_i,$$

donde cada $\mathfrak{q}_i$ es $\mathfrak{p}_i$-primario y $\operatorname{Ass}(K[X_1, ..., X_n]/\mathfrak{a}) = \{\mathfrak{p}_1, ..., \mathfrak{p}_m\}$. Entonces, $\operatorname{ht}(\mathfrak{q}_i) = \operatorname{ht}(\mathfrak{p}_i) = r$ y $\operatorname{coht}(\mathfrak{q}_i) = \operatorname{coht}(\mathfrak{p}_i) = n - r$ para cada $i = 1, ..., m$. Además, las siguientes son extensiones enteras de anillos

$$K[Y_1, ..., Y_{n-r}] \hookrightarrow K[X_1, ..., X_n]/\mathfrak{p}_i$$

para cada $i = 1, ..., m$.

v) Los elementos no nulos de $K[Y_1, ..., Y_{n-r}]$ no son divisores de cero de $K[X_1, ..., X_n]/\mathfrak{a}$.

vi) Para cada ideal primo $\mathfrak{q} \in \operatorname{Spec}(K[X_1, ..., X_n]/\mathfrak{a})$ se tiene que

$$\operatorname{coht}(\mathfrak{q}^c) = \operatorname{coht}(\mathfrak{q}),$$

donde $\mathfrak{q}^c = \mathfrak{q} \cap K[Y_1, ..., Y_{n-r}]$.

3.4.1. Trivialidad global de las intersecciones completas con respecto a una normalización de Noether.

El objetivo de esta subsección consiste en demostrar el Teorema objetivo de la Sección, y que reproducimos de nuevo:

TEOREMA 3.4.3. *Sea K un cuerpo algebraicamente cerrado, $\mathfrak{a} = (f_1, ..., f_r)$ un ideal de $K[X_1, ..., X_n]$ de altura r generado por r elementos. Sea $P \in GL(n, K)$ una matriz regular que define un cambio lineal de variables en $\mathbb{A}^n(K)$:*

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} = P \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}.$$

Supongamos que las nuevas variables están en posición de Noether con respecto al ideal $\mathfrak{a}$, esto es, supongamos que la siguiente es una extensión entera de anillos:

$$A = K[Y_1, ..., Y_{n-r}] \hookrightarrow B = K[X_1, ..., X_n]/\mathfrak{a}.$$

Entonces, B es un A-módulo libre de rango finito.

DEMOSTRACIÓN. Antes de nada, observemos que el cambio de variables definido por la matriz regular P define un isomorfismo de K-álgebras como el siguiente:

$$\begin{aligned} \varphi : K[X_1, ..., X_n] &\to K[Y_1, ..., Y_n] \\ f &\mapsto f \circ P^{-1}. \end{aligned}$$

Este isomorfismo permite identificar el ideal $\mathfrak{a}$ con su imagen $\mathfrak{b} = \varphi(\mathfrak{a}) = (\varphi(f_1), ..., \varphi(f_r))$ que será también un ideal de altura r generado por r elementos. Asimismo, φ permite un isomorfismo entre los respectivos anillos residuales:

$$B = K[X_1, ..., X_n]/\mathfrak{a} \cong B' = K[Y_1, ..., Y_n]/\mathfrak{b}.$$

Finalmente a través de φ tenemos también una extensión entera de anillos de la forma

$$A = K[Y_1, ..., Y_{n-r}] \hookrightarrow B' = K[Y_1, ..., Y_n]/\mathfrak{b}.$$

Claramente B' es un A-módulo libre de rango finito si y solamente si B es un A-módulo libre de rango finito. En otras palabras, y sin pérdida de generalidad, podemos suponer que la matriz P es la identidad Id_n y que tenemos una extensión entera de anillos

$$A = K[X_1, ..., X_{n-r}] \hookrightarrow B = K[X_1, ..., X_n]/\mathfrak{a},$$

donde $\mathfrak{a} = (f_1, ..., f_r)$.

Seguidamente veremos que B es un A-módulo finitamente generado. Es un argumento clásico en el contexto de extensiones enteras de A-álgebras finitamente generadas. Lo incluimos por hacer la demostración lo más autocontenida posible. Como B es una extensión entera de A, para cada $j = n - r + 1, ..., n$, existirá un polinomio mónico $p_j(T) \in A[T]$ de grado D_j tal que

$$p_j(X_j) \in \mathfrak{a}.$$

Es decir, tenemos los polinomios $p_j(T)$, $(j = n - r + 1, ..., n)$, tales que

$$p_j(X_j) \in A[X_j] = K[X_1, ..., X_{n-r}, X_j] \subseteq K[X_1, ..., X_n].$$

Podemos considerar el ideal $\mathfrak{b} = (p_{n-r+1}, ..., p_n) \subseteq \mathfrak{a} \subseteq K[X_1, ..., X_n]$ generado por ellos. Consideremos también el cociente por $\mathfrak{b}$

$$B_1 = K[X_1, ..., X_n]/\mathfrak{b} = A[X_{n-r+1}, ..., X_n]/\mathfrak{b}.$$

Ahora observemos que el siguiente conjunto es un sistema generador de B_1 como A-módulo:

$$\mathcal{M} = \{ \prod_{j=n-r+1}^{n} X_j^{\mu_j} + \mathfrak{b} : \ 0 \leq \mu_j \leq D_j - 1 \}.$$

Esta afirmación se prueba elementalmente por inducción sobre r. Para ello, recordemos que es posible la división euclídea con resto cuando el divisor es un polinomio mónico.

Así, en el caso $r = 1$, sea $f \in K[X_1, ..., X_n]$. Dividamos con resto f por p_n, notando que $A = K[X_1, ..., X_{n-1}]$. Entonces, existen $q, r \in A[X_n]$ con $\deg_{X_n}(r) \leq \deg_{X_n}(p_n) = D_n - 1$, tales que

$$f = q \cdot p_n + r.$$

Como $p_n \in \mathfrak{b}$ y el grado de r con respecto a la variable X_n es menor o igual a $D_n - 1$, podemos suponer

$$r = \sum_{k=0}^{D_n-1} a_k(X_1, ..., X_{n-1}) \cdot X_n^k,$$

y habremos probado que

$$f - r = f - \sum_{k=0}^{D_n-1} a_k(X_1, ..., X_{n-1}) \cdot X_n^k \in \mathfrak{b},$$

o lo que es lo mismo, $\mathcal{M}$ generan $B_1 = K[X_1, ..., X_n]/\mathfrak{b}$ como A-módulo (en el caso $r = 1$).

Inductivamente, para $r \geq 2$ repetiremos el procedimiento. Así, dado $f \in K[X_1, ..., X_n]$ dividimos f por $p_n \in \mathfrak{b}$ y tendremos $q, r \in K[X_1, ..., X_{n-r}][X_n]$ tales que

$$\begin{aligned} &- \quad f = q \cdot p_n + r, \\ &- \quad \deg_{X_n}(r) \leq D_n - 1, \\ &- \quad r = \sum_{k=0}^{D_n-1} a_k(X_1, ..., X_{n-1}) \cdot X_n^k. \end{aligned} \tag{3.4.1}$$

Ahora consideramos el anillo $R_{n-1} = K[X_1, ..., X_{n-1}]$, el ideal $\mathfrak{b}_{n-1} = (p_{n-r+1}, ..., p_{n-1}) \subseteq R_{n-1}$ y seguimos teniendo una extensión entera de anillos

$$A = K[X_1, ..., X_{n-r}] \hookrightarrow B_{n-1} = R_{n-1}/\mathfrak{b}_{n-1}.$$

Nótese que seguimos teniendo una extensión entera de anillos porque para cada $j = n - r + 1, ..., n - 1$, la ecuación $p_j(X_j) \in \mathfrak{b}_{n-1}$ es una ecuación de dependencia entera de $X_j + \mathfrak{b}_{n-1}$ (es mónico con respecto a X_j) en $\mathfrak{b}_{n-1}$, que es una A-álgebra generada por $\{X_{n-r+1} + \mathfrak{b}_{n-1}, ..., X_{n-1} + \mathfrak{b}_{n-1}\}$.

Podemos aplicar la hipótesis inductiva y tendremos que la siguiente familia genera B_{n-1} como A-módulo:

$$\mathcal{M}_{n-1} = \{ \prod_{j=n-r+1}^{n-1} X_j^{\mu_j} : \ 0 \leq \mu_j \leq D_j - 1, \ n - r + 1 \leq j \leq n - 1\}.$$

Retomamos las identidades descritas en (3.4.1) y los coeficientes del polinomio r, $\{a_0, ..., a_{D_n-1}\} \subseteq K[X_1, ..., X_{n-1}]$. Por hipótesis inductiva, para cada $k = 0, ..., D_n - 1$, existirán $\alpha_{\underline{\mu}}^{(k)} \in A$, con $\underline{\mu} = (\mu_{n-r+1}, ..., \mu_{n-1})$, $0 \leq \mu_i \leq D_i - 1$, tales que

$$a_k - \sum_{\underline{\mu}} \alpha_{\underline{\mu}}^{(k)} \cdot \prod_{j=n-r+1}^{n-1} X_j^{\mu_j} \in \mathfrak{b}_{n-1} \subseteq \mathfrak{b}.$$

En conclusión, r es una combinación lineal con coeficientes en A de monomios en $\mathcal{M}$. Para concluir, retomemos (3.4.1) y observemos que $p_n \in \mathfrak{b}$ con lo que

$$f - r = q \cdot p_n \in \mathfrak{b},$$

y tendremos probado que $f + \mathfrak{b}$ es una combinación lineal con coeficientes en A de elementos de $\mathcal{M}$. Como $\mathcal{M}$ es un conjunto finito, entonces B_1 es un A-módulo finitamente generado.

Hemos probado que $B_1 = K[X_1, ..., X_n]/\mathfrak{b}$ es un A-módulo finitamente generado. Recordemos que el ideal $\mathfrak{b}$ satisface $\mathfrak{b} \subseteq \mathfrak{a} = (f_1, ..., f_r)$ y con ello tenemos la siguiente proyección canónica proveniente del Segundo Teorema de Isomorfía:

$$\pi : B_1 = K[X_1, ..., X_n]/\mathfrak{b} \to B_1/(\mathfrak{a}/\mathfrak{b}) \cong K[X_1, ..., X_n]/\mathfrak{a} = B.$$

Como π es epimorfismo de anillos también es epimorfismo de A-módulos. Entonces, B es la imagen por un epimorfismo de A-módulos de un A-módulo finitamente generado. Concluimos así que B es un A-módulo finitamente generado.

Volvamos al objetivo de nuestro Teorema. Se trata de ver que B es un A-módulo libre y, como es finitamente generado, de rango finito. Haremos la prueba por inducción en $n-r$, usando fuertemente el Teorema de Quillen-Suslin (Teorema 3.2.1). En este sentido, para probar que B es un A-módulo libre de rango finito, bastará ver que es un A-módulo proyectivo. Pero, como la condición de ser proyectivo es una propiedad local (Teorema 1.2.11) bastará con probar que es localmente proyectivo. Es decir, basta con que probemos que para todo $\mathfrak{m} \in \mathrm{MaxSpec}(A)$, $B_{\mathfrak{m}}$ es un $A_{\mathfrak{m}}$-módulo proyectivo. Finalmente, como $(A_{\mathfrak{m}}, \mathfrak{m}A_{\mathfrak{m}})$ es un anillo local y $B_{\mathfrak{m}}$ es un $A_{\mathfrak{m}}$-módulo finitamente generado, $B_{\mathfrak{m}}$ es un $A_{\mathfrak{m}}$-módulo proyectivo si y solo si $B_{\mathfrak{m}}$ es un $A_{\mathfrak{m}}$-módulo libre de rango finito (cf. Corolario 1.3.3). En conclusión, para probar que B es un A-módulo libre de rango finito, bastará con probar la siguiente afirmación:

Afirmación. *Para cada ideal maximal $\mathfrak{m} \in \mathrm{MaxSpec}(A)$, el $A_{\mathfrak{m}}$-módulo $B_{\mathfrak{m}}$ es libre y de rango finito.*

Demostración de la Afirmación. Como ya hemos dicho, la haremos por inducción en $n-r$. En el caso $n-r=0$, tenemos $A = B = K[X_1, ..., X_n]$. Claramente, B es un A-módulo libre de rango 1 y para cada $\mathfrak{m} \in \mathrm{MaxSpec}(A)$, $B_{\mathfrak{m}}$ es un $A_{\mathfrak{m}}$-módulo libre de rango 1, con lo que la afirmación queda verificada trivialmente.

Para el caso $n - r \geq 1$, recordemos en primer lugar que por el Nullstellensatz de Hilbert-Kronecker (ver [**Pardo, 2021**] para una sencilla demostración), como K es algebraicamente cerrado el espectro maximal de A tiene la forma siguiente:

$$\mathrm{MaxSpec}(A) = \{\mathfrak{m}_a = (X_1 - a_1, ..., X_{n-r} - a_{n-r}) : a = (a_1, ..., a_{n-r}) \in K^{n-r}\}.$$

Para simplificar las notaciones, hagamos la prueba para $\mathfrak{m} = \mathfrak{m}_0$ y los mismos argumentos (con los cambios oportunos de notación) serán aplicables a cualquier otro ideal maximal $\mathfrak{m}_a \in \mathrm{MaxSpec}(A)$. Consideramos la variable $X_{n-r} \in A$, el ideal $\mathfrak{a}_1 = (f_1, ..., f_r, X_{n-r})$. Vamos a probar la siguiente igualdad:

$$\mathfrak{a}_1^c = \mathfrak{a}_1 \cap A = (X_{n-r}).$$

Para probarlo, observemos primero que el contenido $\supseteq$ es obvio. Veamos entonces el otro contenido. Sea $\mathfrak{q}_1$ un ideal primo minimal sobre $\mathfrak{a}_1$. Por el Teorema del Ideal Principal de Krull, sabemos que

$$\mathrm{ht}(\mathfrak{q}_1) \leq r + 1.$$

De otro lado, sabemos que $\mathfrak{a} = (f_1, ..., f_r)$ tiene altura r. Por el Teorema de la Pureza de Macaulay sabemos que todos los primos minimales sobre $\mathfrak{a}$ tienen altura r. Como $\mathfrak{a} \subseteq \mathfrak{a}_1 \subseteq \mathfrak{q}_1$, puede suceder que $\mathfrak{q}_1$ sea minimal sobre $\mathfrak{a}$ o que exista $\mathfrak{p} \in \mathrm{Spec}(K[X_1, ..., X_n])$ tal que $\mathfrak{p}$ es minimal sobre $\mathfrak{a}$ y $\mathfrak{p} \subseteq \mathfrak{q}_1$. De cualquier modo, siempre existe $\mathfrak{p}$ minimal sobre $\mathfrak{a}$ tal que $\mathfrak{p} \subseteq \mathfrak{q}_1$. En particular, tendremos

$$r = \mathrm{ht}(\mathfrak{p}) \leq \mathrm{ht}(\mathfrak{q}) \leq r + 1.$$

Pasando a las co-alturas, tenemos

$$n - r = n - \mathrm{ht}(\mathfrak{p}) = \mathrm{coht}(\mathfrak{p}) \geq \mathrm{coht}(\mathfrak{q}_1) \geq n - r - 1.$$

Considerando el ideal $\mathfrak{q} = \mathfrak{q}_1/\mathfrak{a} \in \mathrm{Spec}(K[X_1, ..., X_n]/\mathfrak{a})$, tenemos la extensión entera de anillos

$$A = K[X_1, ..., X_{n-r}] \hookrightarrow B = K[X_1, ..., X_n]/\mathfrak{a}.$$

Sea $\mathfrak{q}^c = \mathfrak{q} \cap A$ el ideal contracción. Por el Teorema del Ascenso sabemos que se preservan las co-alturas, así que

$$n - r - 1 \leq \mathrm{coht}(\mathfrak{q}^c) = \mathrm{coht}(\mathfrak{q}) = \mathrm{coht}(\mathfrak{q}_1) \leq n - r.$$

Adicionalmente, como $\mathfrak{q}_1 \supseteq \mathfrak{a}_1$, tendremos que

$$\mathfrak{q} = \mathfrak{q}_1/\mathfrak{a} = (X_{n-r} + \mathfrak{a}) \text{ en } B$$

y la contracción satisface

$$\mathfrak{q}^c = (\mathfrak{q}_1/\mathfrak{a}_1)^c \supseteq (X_{n-r}) \text{ en } A.$$

Ahora bien, (X_{n-r}) es un ideal primo en A, X_{n-r} no es divisor de cero en A (porque A es dominio) y por tanto, la altura de (X_{n-r}) es 1 por el Teorema del Ideal Principal de Krull. En particular, su co-altura es $n-r-1$ y tendremos que $(X_{n-r}) \subseteq \mathfrak{q}^c$, luego

$$\operatorname{coht}(\mathfrak{q}^c) \leq \operatorname{coht}((X_{n-r})) = n-r-1.$$

Por tanto, la co-altura de $\mathfrak{q}^c$ es necesariamente $n-r-1$. Su altura será 1 y se tiene la inclusión $(X_{n-r}) \subseteq \mathfrak{q}^c$ de dos ideales primos de la misma altura. Por tanto,

$$\mathfrak{q}^c = (X_{n-r}).$$

Ahora bien, $\mathfrak{a}_1/\mathfrak{a}$ es un ideal tal que

$$(X_{n-r}+\mathfrak{a}) \subseteq \mathfrak{a}_1/\mathfrak{a} \subseteq \mathfrak{q}_1/\mathfrak{a} = \mathfrak{q}.$$

Luego $(\mathfrak{a}_1/\mathfrak{a})^c \subseteq (X_{n-r})$. Pero esto implica que

$$(\mathfrak{a}_1/\mathfrak{a})^c = (X_{n-r}).$$

Como la extensión $A \hookrightarrow B$ es entera, también lo será

$$K[X_1,...,X_{n-r-1}] = K[X_1,...,X_{n-r}]/(X_{n-r}) = K[X_1,...,X_{n-r}]/(\mathfrak{a}_1/\mathfrak{a})^c \hookrightarrow B/(\mathfrak{a}_1/\mathfrak{a}).$$

Por el Segundo Teorema de Isomorfía tendremos la extensión entera de anillos

$$K[X_1,...,X_{n-r-1}] \hookrightarrow (K[X_1,...,X_n]/\mathfrak{a})/(\mathfrak{a}_1/\mathfrak{a}) = K[X_1,...,X_n]/\mathfrak{a}_1.$$

En particular, $\mathfrak{a}_1$ es un ideal generado por $r+1$ elementos de co-altura $n-r-1$. Por el Teorema del Ideal Principal de Krull todos los ideales primos minimales sobre $\mathfrak{a}_1$ tienen altura $\leq r+1$ y, por tanto, co-altura $\geq n-r-1$. Ahora como la dimensión del anillo $K[X_1,...,X_n]/\mathfrak{a}_1$ es $n-r-1$, todos los ideales primos minimales sobre $\mathfrak{a}_1$ tienen co-altura acotada por $n-r-1$. En suma, si $\mathfrak{q}$ es un ideal minimal sobre $\mathfrak{a}_1$, tenemos que $\operatorname{coht}(\mathfrak{q}) = n-r-1$ y $\operatorname{ht}(\mathfrak{q}) = r+1$.

Resumiendo, $\mathfrak{a}_1 = (f_1,...,f_r,X_{n-r})$ es un ideal de $K[X_1,...,X_n]$ tal que sus primos minimales tienen altura $r+1$. En particular, $\mathfrak{a}_1$ tiene altura $r+1$ y está generado por $r+1$ elementos. Además, tenemos la extensión entera de anillos

$$A_1 = K[X_1,...,X_{n-r-1}] \hookrightarrow B_1 = K[X_1,...,X_n]/\mathfrak{a}_1.$$

Aplicando la hipótesis inductiva, todas las localizaciones de B_1 por un maximal $\mathfrak{m} \in \operatorname{MaxSpec}(A_1)$ hacen que $(B_1)_{\mathfrak{m}}$ sea un $(A_1)_{\mathfrak{m}}$-módulo libre. Por tanto, B_1 es un A_1-módulo proyectivo y por el Teorema de Quillen-Suslin, B_1 es un A_1-módulo libre de rango finito. Veamos que $B_{\mathfrak{m}}$ es un $A_{\mathfrak{m}}$-módulo libre y habremos terminado.

Para empezar, nótese que el elemento X_{n-r} no es divisor de cero en B. Por el Teorema de Lasker-Noether, los divisores de cero de B como anillo son las clases (módulo $\mathfrak{a}$) de los elementos de B que están en algún ideal primo asociado a $\mathfrak{a}$. Por el Teorema de la Pureza de Macaulay, los primos asociados al ideal $\mathfrak{a}$ son los primos minimales sobre $\mathfrak{a}$ y todos tienen altura r. Hemos visto antes que todos los primos minimales sobre $\mathfrak{a}_1 = \mathfrak{a} + (X_{n-r})$ tienen altura $r+1$. Por tanto, X_{n-r} no puede estar en nigún primo minimal sobre $\mathfrak{a}$.

Consideremos ahora la proyección canónica

$$\begin{aligned} \pi_1 : B &\to B_1 \\ f+\mathfrak{a} &\mapsto f+\mathfrak{a}_1. \end{aligned}$$

Nótese que $A_1 = A/(X_{n-r})$ y que la restricción de π_1 a A tiene la forma siguiente:

$$\begin{aligned} \pi_1|_A : A &\to A_1 \\ g &\mapsto g+(X_{n-r}). \end{aligned}$$

Podemos elegir ahora una familia $\{e_1,...,e_m\}$ de elementos de B tales que $\{\pi_1(e_1),...,\pi_1(e_m)\}$ es una base de B_1 como A_1-módulo libre. Como el producto tensorial conmuta con la suma directa (ver Apéndice A.5), tenemos que la familia

$$\{\pi_1(e_1)+\mathfrak{m}_1B_1,...,\pi_1(e_m)+\mathfrak{m}_1B_1\}$$

es una base de $B_1/\mathfrak{m}_1B_1$ como $A_1/\mathfrak{m}_1$-espacio vectorial (donde $\mathfrak{m}_1 = \mathfrak{m}/(X_{n-r})$).

Observemos ahora unas pocas propiedades (algunas de las cuales son propiedades naturales del producto tensorial).

i) En primer lugar,
$$K = A/\mathfrak{m} = A_1/\mathfrak{m}_1.$$

ii) Se tiene

$$B_1/\mathfrak{m}_1 B_1 = (K[X_1, ..., X_n]/\mathfrak{a}_1)/(\mathfrak{a}_1+(X_1, ..., X_{n-r-1})/\mathfrak{a}_1) \cong K[X_1, ..., X_n]/(\mathfrak{a}_1+(X_1, ..., X_{n-r-1})).$$

iii) Como $\mathfrak{a} + (X_1, ..., X_{n-r}) = \mathfrak{a}_1 + (X_1, ..., X_{n-r-1})$ (porque $\mathfrak{a}_1 = \mathfrak{a} + (X_{n-r})$), tenemos también
$$B/\mathfrak{m}B \cong K[X_1, ..., X_n]/(\mathfrak{a}_1 + (X_1, ..., X_{n-r-1})) \cong B_1/\mathfrak{m}_1 B_1.$$

Por tanto, $B/\mathfrak{m}B$ es isomorfo a $B_1/\mathfrak{m}_1 B_1$ como K-espacio vectorial y el isomorfismo viene dado del modo siguiente:

$$\begin{aligned} \psi : B/\mathfrak{m}B &\to B_1/\mathfrak{m}_1 B_1 \\ h + \mathfrak{m}B &\mapsto \pi_1(h) + \mathfrak{m}_1 B_1. \end{aligned}$$

En particular, como $\{\pi_1(e_1) + \mathfrak{m}_1 B_1, ..., \pi_1(e_m) + \mathfrak{m}_1 B_1\}$ son una base de $B_1/\mathfrak{m}_1 B_1$ como K-espacio vectorial, el siguiente conjunto es una base de $B/\mathfrak{m}B$ como K-espacio vectorial:

$$\{e_1 + \mathfrak{m}B, ..., e_m + \mathfrak{m}B\}.$$

Consideremos ahora el anillo local $(A_\mathfrak{m}, \mathfrak{m}A_\mathfrak{m})$ y el $A_\mathfrak{m}$-módulo finitamente generado $B_\mathfrak{m}$. Observemos que

$$A_\mathfrak{m}/\mathfrak{m}A_\mathfrak{m} \cong A/\mathfrak{m} \cong K.$$

También tenemos el isomorfismo natural

$$B_\mathfrak{m}/(\mathfrak{m}A_\mathfrak{m})B_\mathfrak{m} \cong B_\mathfrak{m}/\mathfrak{m}B_\mathfrak{m} \cong (B/\mathfrak{m}B)_\mathfrak{m} \cong B/\mathfrak{m}B,$$

siendo el último un isomorfismo como K-espacios vectoriales. Por tanto, como $B \subseteq B_\mathfrak{m}$, la familia $\{e_1 + \mathfrak{m}B, ..., e_m + \mathfrak{m}B\}$ también es una base de $B_\mathfrak{m}/\mathfrak{m}B_\mathfrak{m}$ como K-espacio vectorial.

Estamos así en las condiciones del Lema de Nakayama con el anillo local $(A_\mathfrak{m}, \mathfrak{m}A_\mathfrak{m})$ y el $A_\mathfrak{m}$-módulo finitamente generado $B_\mathfrak{m}$. Entonces, por el Corolario que se deduce del Lema de Nakayama (ver Corolario A.6.2), el conjunto $\{e_1, ..., e_m\}$ es un sistema generador de cardinal minimal de $B_\mathfrak{m}$ como $A_\mathfrak{m}$-módulo.

Veamos finalmente que $\{e_1, ..., e_m\}$ es una familia libre y habremos concluido que es una base de $B_\mathfrak{m}$ como $A_\mathfrak{m}$-módulo libre, lo que termina la prueba de la afirmación. Para ello, consideremos una combinación lineal de elementos de $\{e_1, ..., e_m\}$ con coeficientes en $A_\mathfrak{m}$ igual a 0 en $B_\mathfrak{m}$. Es decir, sea

$$a_1 e_1 + ... + a_m e_m = 0, \text{ con } a_1, ..., a_m \in A_\mathfrak{m} \text{ no todos nulos.}$$

Multiplicando por denominadores de los a_i si fuera necesario, podemos suponer, sin pérdida de generalidad, que tenemos una combinación lineal de la forma

$$a_1 e_1 + ...a_m e_m = 0, \tag{3.4.2}$$

donde $a_1, ..., a_m \in A$ (no todos nulos) y la igualdad se verifica en B. Ahora, como $A = K[X_1, ..., X_{n-r}]$ es un dominio de factorización única, podemos extraer la máxima potencia de X_{n-r} que divide a todos los coeficientes $a_1, ..., a_m$. Esto es, existe $l \in \mathbb{N}$ y existen $a'_1, ..., a'_m \in A$ tales que

$$a_1 = X_{n-r}^l a'_1, ..., a_m = X_{n-r}^l a'_m,$$

y existe j tal que $X_{n-r} \nmid a'_j$. Sin pérdida de generalidad podemos suponer que $X_{n-r} \nmid a'_1$. Esto es posible porque no todos los $a_1, ..., a_m$ son nulos. Así, podemos reescribir (3.4.2) sacando factor común X_{n-r}^l:

$$X_{n-r}^l(a'_1 e_1 + ... + a'_m e_m) = 0.$$

Como X_{n-r} no es divisor de cero en B, esta igualdad implica que

$$a'_1 e_1 + ... + a'_m e_m = 0, \tag{3.4.3}$$

donde la igualdad se satisface en B. Tomemos la proyección $\pi_1 : B \to B_1$ y tendremos que (3.4.3) se transforma en la siguiente igualdad en B_1:

$$\pi_1(a'_1)\pi_1(e_1) + ... + \pi_1(a'_m)\pi_1(e_m) = 0.$$

Pero $\{\pi_1(e_1), ..., \pi_1(e_m)\}$ era una base de B_1 como A_1-módulo libre y $\pi_1(a'_1), ..., \pi_1(a'_m) \in A_1$, por lo que tenemos las siguientes igualdades en A_1:

$$\pi_1(a'_1) = 0, ..., \pi_1(a'_m) = 0.$$

Ahora bien $a'_1 \in A$, $\pi_1(a'_1) = \pi_1|_A(a'_1) = a'_1 + (X_{n-r}) \in A_1$. Luego $\pi_1(a'_1) = 0$ equivale a decir que $a'_1 + (X_{n-r}) = 0 + (X_{n-r})$ en A_1. O equivalentemente, que $X_{n-r}|a'_1$ en $K[X_1, ..., X_n]$. Pero esto no es posible por nuestra construcción de a'_1. Llegamos así a una contradicción, con lo que de la igualdad (3.4.2) se deduce que $a_1 = ... = a_m = 0$ y la familia $\{e_1, ..., e_m\} \subseteq B \subseteq B_{\mathfrak{m}}$ es una base de $B_{\mathfrak{m}}$ como $A_{\mathfrak{m}}$-módulo libre. □

APÉNDICE A

Algunos Resultados Básicos de Álgebra Conmutativa

Índice

A.1. Definiciones básicas **49**
A.2. Módulos libres **50**
A.3. Módulo de fracciones. Localización **50**
A.4. El functor $\mathrm{Hom}_R(M,-)$. **51**
A.5. Producto tensorial de módulos **52**
A.5.1. Propiedades del producto tensorial 52
A.5.2. Extensión de escalares 53
A.6. Lema de Nakayama **53**
A.7. La Topología de Zariski en $\mathrm{Spec}(R)$ **53**
A.8. Producto fibrado de módulos **54**
A.9. Algunas demostraciones sobre propiedades locales citadas en el texto **55**

Las demostraciones de los resultados enunciados en este Apéndice pueden encontrarse en [**Pardo, 2021**].

A.1. Definiciones básicas

Definición 10 (**Anillo local**). *Sea $R \neq \{0\}$ un anillo. Se dice que R es un anillo local si $\mathrm{MaxSpec}(R)$ consta únicamente de un elemento $\mathfrak{m}$. Lo denotaremos como $(R,\mathfrak{m})$.*

Definición 11 (**Sucesión exacta**). *Una sucesión de R-módulos y homomorfismos de R-módulos*

$$\ldots \to M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to \ldots$$

se dice que es exacta en M_i si $Im(f_i) = Ker(f_{i+1})$. Se dice que la sucesión es exacta si lo es para cada M_i.

Se llaman sucesiones exactas cortas a las sucesiones exactas de la forma:

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0,$$

donde 0 es el R-módulo nulo.

Definición 12 (**Functor exacto**). *Sea R un anillo. Un functor F de la categoría de R-módulos en sí misma se denomina exacto si transforma sucesiones exactas cortas*

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

en sucesiones exactas cortas

$$0 \to F(M') \xrightarrow{F(f)} F(M) \xrightarrow{F(g)} F(M'') \to 0.$$

Definición 13 (**Número mínimo de generadores**). *Sea M un R-módulo finitamente generado. Llamaremos número mínimo de generadores de M a la cantidad*

$$\mu(M) := \min\{n \in \mathbb{N} : \exists\{a_1,\ldots,a_n\} \in M, M = R\langle\{a_1,\ldots,a_n\}\rangle\}.$$

DEFINICIÓN 14. *Dado M un R-módulo finitamente generado, definimos la aplicación*

$$\begin{aligned}\mu_{\_}(M) : \operatorname{Spec}(R) &\to \mathbb{R}_+ \\ \mathfrak{p} &\mapsto \mu_{\mathfrak{p}}(M) = \mu(M_{\mathfrak{p}})\end{aligned}$$

En el caso de que además M sea proyectivo, dado $\mathfrak{p} \in \operatorname{Spec}(R)$, llamamos a $\mu_{\mathfrak{p}}(M)$ el rango de M en $\mathfrak{p}$.

A.2. Módulos libres

DEFINICIÓN 15 (**Módulo libre**). *Diremos que un R-módulo M es libre si existe un conjunto X tal que M es isomorfo como R-módulo al R-módulo $\bigoplus_X R$ dado por la siguiente identidad:*

$$\bigoplus_X R := \{f : X \to R : \exists Y \text{ finito}, \ Y \subseteq X, \ f(x) = 0, \ \forall x \in X \setminus Y\}.$$

Se dice que M es un R-módulo libre de rango finito si X se puede elegir finito.

DEFINICIÓN 16 (**Base de un R-módulo**). *Se llama base de un R-módulo M a todo subconjunto $\mathcal{B} \subseteq M$ que verifica las siguientes dos propiedades:*

i) El conjunto $\mathcal{B}$ es sistema generador de M, es decir, $M = R\langle\mathcal{B}\rangle$.
ii) Los elementos de $\mathcal{B}$ son una familia libre sobre R, es decir, para cualquier conjunto J finito, para cualquier lista de elementos $\{v_j \in \mathcal{B} : j \in J\} \subseteq \mathcal{B}$ y para cualesquiera $\{a_j \in R : j \in J\}$, se tiene que si

$$\sum_{j \in J} a_j v_j = 0$$

entonces $a_j = 0$ para todo $j \in J$.

PROPOSICIÓN A.2.1. *Un R-módulo es libre si y solo si posee alguna base.*

LEMA A.2.2. *En un R-módulo libre M de rango finito los sistemas generadores minimales y las bases coinciden.*

A continuación se muestra un ejemplo de módulo libre importante especialmente en el Teorema de Horrocks (Teorema 2.4.1).

EJEMPLO A.2.3. *Sea R un anillo y $g \in R[X]_{mon}$ un polinomio mónico con coeficientes en R. Entonces $R[X]/(g)$ es un R-módulo libre. La razón esencial es que la división euclídea por polinomios mónicos está garantizada. Es decir, si $g \in R[X]_{mon}$ y $f \in R[X]$, entonces existen $q, r \in R[X]$ tales que $f = qg + r$ y $\deg_X(r) \leq \deg_X(g) - 1$. Con esta propiedad garantizamos que*

$$\mathcal{B} = \{1 + (g), ..., X^{d-1} + (g)\}$$

es un sistema generador de $R[X]/(g)$, donde $d = \deg_X(g)$. Además, como g es mónico, los polinomios q, r son únicos, por lo que $\mathcal{B}$ será también una familia libre.

PROPOSICIÓN A.2.4. *Sea $A \subset B$ una extensión de anillos. Supongamos que B es un A-módulo libre de rango finito, y sea M un B-módulo libre de rango finito. Entonces M es un A-módulo libre de rando finito.*

A.3. Módulo de fracciones. Localización

DEFINICIÓN 17 (**Sistema multiplicativamente cerrado**). *Sea R un anillo. Un subconjunto $S \subseteq R$ se dice sistema multiplicativamente cerrado si verifica:*

i) $1 \in S$, $0 \notin S$, y
ii) $\forall x, y \in S, xy \in S$.

DEFINICIÓN 18 (**Módulo de fracciones**). *Sea R un anillo, M un R-módulo y sea S un sistema multiplicativo de R. Llamamos módulo de fracciones (o módulo cociente) de M con denominador S al conjunto $S^{-1}M = (M \times S)/\sim$, donde $\sim$ es la relación de equivalencia en S dada por*

$$(m,s) \sim (n,t) \Longleftrightarrow \exists u \in S \text{ con } u(mt-ns) = 0.$$

Denotamos a las clases de equivalencia en $S^{-1}M$ como $[m,s] = \frac{m}{s}$. Las operaciones

$$+_{S^{-1}M}: \quad \frac{m}{s} +_{S^{-1}M} \frac{n}{t} = \frac{mt+ns}{st}$$

$$\cdot_{S^{-1}M}: \quad \frac{m}{s} \cdot_{S^{-1}M} \frac{n}{t} = \frac{mn}{st}$$

definen en $S^{-1}M$ una estructura de R-módulo. Llamamos morfismo de localización al morfismo de R-módulos $i : M \longrightarrow S^{-1}M$ dado por $i(m) = \frac{m}{1}$.

En el caso de que S sea un ideal de R generado por un elemento $a \in R$, es decir, $S = \{1, a, a^2, ...\}$, denotamos $S^{-1}M \equiv M_a$.

DEFINICIÓN 19 (**Localización de un R-módulo**). *Sea R un anillo, $\mathfrak{p} \in \mathrm{Spec}(R)$ un ideal primo de R y M un R-módulo. Sea $S = R \setminus \mathfrak{p}$. El módulo de fracciones $S^{-1}M$ se denota también por $M_{\mathfrak{p}}$, y se llama localización de M por el ideal primo $\mathfrak{p}$.*

La definición anterior es buena debido a que el conjunto $S = R \setminus \mathfrak{p}$ es multiplicativamente cerrado. Esto es consecuencia de que si tomamos $\mathfrak{p}$ un ideal propio de R, las condiciones

i) $\mathfrak{p}$ es un ideal primo, y
ii) $R \setminus \mathfrak{p}$ es multiplicativamente cerrado

son exactamente la misma.

A partir de la idea de localización se puede definir un functor (que llamaremos functor localización) de la categoría de R-módulos en la categoría de $S^{-1}R$-módulos. Dado un subconjunto $S \subset R$ multiplicativamente cerrado y un morfismo de R-módulos $f : M' \to M$, definimos

$$S^{-1}f : S^{-1}M' \to S^{-1}M$$
$$\frac{m}{s} \mapsto \frac{f(m)}{s}$$

Este functor verifica una serie de propiedades que se recogen en la siguiente Proposición.

PROPOSICIÓN A.3.1. *El functor localización, S^{-1}, de la categoría de R-módulos en la de $S^{-1}R$-módulos es covariante y exacto. Es decir, verifica las siguientes propiedades:*

i) Dados $f \in \mathrm{Hom}(M_1, M_2)$, $g \in \mathrm{Hom}(M_2, M_3)$, y M un R-módulo, entonces

$$S^{-1}(g \circ f) = S^{-1}g \circ S^{-1}f,$$
$$S^{-1}Id_M = ID_{S^{-1}M}.$$

ii) Transforma sucesiones exactas en sucesiones exactas (cf. a la Definición 12).
iii) Si N y P son submódulos de un R-módulo M, entonces:
- $S^{-1}(N+P) = (S^{-1}N) + (S^{-1}P)$.
- $S^{-1}(N \cap P) = (S^{-1}N) \cap (S^{-1}P)$.
- $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$.

A.4. El functor $\mathrm{Hom}_R(M,-)$.

DEFINICIÓN 20 (**Functor $\mathrm{Hom}_R(M,-)$**). *Sea R un anillo (fijo) y M un R-módulo. Se define el functor $\mathrm{Hom}_R(M,-)$ de la categoría de R-módulos en sí misma del modo siguiente:*

- *A cada R-módulo N le asocia el R-módulo $\mathrm{Hom}_R(M,N)$.*

- *A cada morfismo $f \in \mathrm{Hom}_R(N, N')$ entre dos R-módulos le asocia el homomorfismo*

$$\begin{aligned} \mathrm{Hom}_R(M, f) : \mathrm{Hom}_R(M, N) &\to \mathrm{Hom}_R(M, N') \\ g &\mapsto f \circ g \end{aligned}$$

PROPOSICIÓN A.4.1. *El functor $\mathrm{Hom}_R(M, -)$ es covariante. Es decir, dados N, N', N'' R-módulos, $f \in \mathrm{Hom}_R(N, N'), g \in \mathrm{Hom}_R(N', N'')$, y dado $h \in \mathrm{Hom}_R(M, N)$, entonces*

i) $\mathrm{Hom}_R(M, g \circ f)(h) = (\mathrm{Hom}_R(M, g) \circ \mathrm{Hom}_R(M, f))(h)$
ii) $\mathrm{Hom}_R(M, Id_N)(h) = Id_{\mathrm{Hom}_R(M,N)}(h)$

PROPOSICIÓN A.4.2. *El functor $\mathrm{Hom}_R(M, -)$ es exacto a izquierda. Es decir, dada una sucesión exacta corta de R-módulos*

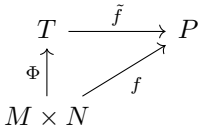
$$0 \to N' \xrightarrow{f} N \xrightarrow{g} N'' \to 0$$

la siguiente es una sucesión exacta de R-módulos:

$$0 \to \mathrm{Hom}_R(M, N') \xrightarrow{\mathrm{Hom}_R(M,f)} \mathrm{Hom}_R(M, N) \xrightarrow{\mathrm{Hom}_R(M,g)} \mathrm{Hom}_R(M, N'')$$

A.5. Producto tensorial de módulos

DEFINICIÓN 21 (**Producto tensorial**). *Sean M y N dos R-módulos. Entonces existe un par (T, Φ) formado por un R-módulo T y una aplicación bilineal $\Phi : M \times N \to T$ tal que se verifica la siguiente propiedad: para todo R-módulo P y para toda aplicación bilineal $f : M \times N \to P$, existe un único morfismo de R-módulos $\tilde{f} \in \mathrm{Hom}(T, P)$ tal que el siguiente diagrama es conmutativo*



Además, el par (T, Φ) es único salvo isomorfismo y lo llamamos producto tensorial de M y N. Se denota como $T := M \otimes_R N$ y a la aplicación Φ como $\Phi(x, y) = x \otimes_R y$.

A.5.1. Propiedades del producto tensorial.

PROPOSICIÓN A.5.1. *El producto tensorial conmuta con la suma directa. Es decir, dada una familia $\{M_i : i \in I\}$ de R-módulos y dado N un R-módulo se tiene que*

$$(\bigoplus_{i \in I} M_i) \otimes N \cong \bigoplus_{i \in I} (M_i \otimes N)$$

En particular, si M y N son R-módulos libres entonces $M \otimes N$ también es libre como R-módulo. En el caso de dos R-módulos finitamente generados

$$\mathrm{rank}(M \otimes N) = \mathrm{rank}(M) \cdot \mathrm{rank}(N)$$

El producto tensorial define un functor que tiene la siguiente propiedad de exactitud:

PROPOSICIÓN A.5.2. *Dado un R-módulo M, el functor $M \otimes_R -$ es un functor exacto a derecha. Es decir, dada una sucesión exacta corta de R-módulos*

$$0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0$$

la siguiente es una sucesión exacta

$$M \otimes_R N' \longrightarrow M \otimes_R N \longrightarrow M \otimes_R N'' \longrightarrow 0$$

PROPOSICIÓN A.5.3. *Sea $f : A \to B$ un morfismo de anillos, P un A-módulo proyectivo, entonces $B \otimes_A P$ es un B-módulo proyectivo.*

A.5.2. Extensión de escalares.

DEFINICIÓN 22 (**Extensión de escalares**). *Sea $f : R \to T$ un morfismo de anillos y sea N un R-módulo. Entonces podemos definir una estructura de T-módulo sobre $T \otimes_R N$ del modo siguiente:*

$$\cdot_T : T \times (T \otimes_R N) \longrightarrow (T \otimes_R N)$$
$$(\lambda, \sum_{i\in I} x_i \otimes_R n_i) \longmapsto \sum_{i\in I} (\lambda x_i) \otimes_R n_i$$

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 a partir de N por extensión de escalares a partir de $f : R \to T$.

Como consecuencia de esta construcción tenemos el siguiente

COROLARIO A.5.4. *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 $\pi : R \to R/\mathfrak{a}$ satisface:*

$$R/\mathfrak{a} \otimes_R M \cong M/\mathfrak{a}M$$

donde el isomorfismo es como $R/\mathfrak{a}$-módulos.

A.6. Lema de Nakayama

LEMA A.6.1 (**Lema de Nakayama**). *Sea R un anillo e I un ideal contenido en el radical de Jacobson de R, es decir*

$$I \subseteq Jac(R) = \bigcap_{\mathfrak{m}\in \mathrm{MaxSpec}(R)} \mathfrak{m}.$$

Sea M un R-módulo arbitrario, y $N \subset M$ un submódulo tal que M/N es finitamente generado. Entonces

$$M = N + IM \implies M = N$$

COROLARIO A.6.2. *Sea $(R, \mathfrak{m})$ un anillo local, M un R-módulo finitamente generado y $k(\mathfrak{m}) = R/\mathfrak{m}$ el cuerpo residual. Sea $M/\mathfrak{m}M = R/\mathfrak{m} \otimes_R M$ el R-módulo cociente.*

Definamos la estructura de $k(\mathfrak{m})$-espacio vectorial siguiente sobre $M/\mathfrak{m}M$:

$$\cdot_{k(\mathfrak{m})} : k(\mathfrak{m}) \times M/\mathfrak{m}M \to M/\mathfrak{m}M$$
$$(\lambda + \mathfrak{m}, m + \mathfrak{m}M) \mapsto \lambda m + \mathfrak{m}M$$

Entonces se verifica

$$\mu(M) = dim_{k(\mathfrak{m})}(M/\mathfrak{m}M)$$

Además, $m_1, ..., m_t \in M$ forman un sistema generador minimal de M si y solo si las clases $\overline{m_1}, ..., \overline{m_t} \in M/\mathfrak{m}M$ forman una base.

A.7. La Topología de Zariski en Spec(R)

Sea R un anillo y $\mathfrak{a} \subseteq R$ un ideal de R. Se define

$$V(\mathfrak{a}) := \{\mathfrak{p} \in \mathrm{Spec}(R) : \mathfrak{a} \subseteq \mathfrak{p}\}.$$

Otra forma de entender estos objetos es la siguiente: dado $f \in R$ denotamos por $f(\mathfrak{p}) := f + \mathfrak{p} \in R/\mathfrak{p}$ para cada $\mathfrak{p} \in \mathrm{Spec}(R)$. Entonces,

$$V(\mathfrak{a}) = \{\mathfrak{p} \in \mathrm{Spec}(R) : f(\mathfrak{p}) = 0, \forall f \in \mathfrak{a}\}$$

Algunas propiedades elementales de estos conjuntos son las siguientes:

i) $V(R) = \emptyset$, $V((0)) = \mathrm{Spec}(R)$.
ii) Dado un conjunto de ideales de R, $\{\mathfrak{a}_i : i \in I\}$,

$$V(\sum_{i\in I} \mathfrak{a}_i) = \bigcap_{i\in I} V(\mathfrak{a}_i)$$

iii) Dados dos idales de R, $\mathfrak{a}, \mathfrak{b}$,

$$V(\mathfrak{a} \cdot \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$$

A la vista de estas propiedades, podemos afirmar que existe una única topología en $\mathrm{Spec}(R)$ para la que los cerrados son

$$\{V(\mathfrak{a}) : \mathfrak{a} \subseteq R \text{ es ideal.}\}$$

Esta topología se denomina Topología de Zariski en $\mathrm{Spec}(R)$.

Los abiertos de esta topología son obviamente los complementarios de los cerrados. Pero hay unos abiertos especiales que constituyen una base: los abiertos distinguidos. Dado $f \in R$, llamamos abierto distinguido definido por f al conjunto

$$D(f) := \{\mathfrak{p} \in \mathrm{Spec}(R) : f(\mathfrak{p}) \neq 0\} = \{\mathfrak{p} \in \mathrm{Spec}(R) : f \notin \mathfrak{p}\}$$

Es claro que todo abierto de la topología es unión (posiblemente infinita) de abiertos distinguidos.

$$V(\mathfrak{a})^c = \bigcup_{f \in \mathfrak{a}} D(f)$$

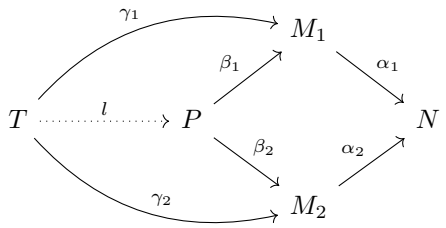
donde $(\cdot)^c$ indica complementario.

A.8. Producto fibrado de módulos

Esta sección del Apéndice A se dedica a resumir el concepto de producto fibrado de R-módulos, así como sus propiedades fundamentales. Esta construcción es esencial en la demostración del Teorema de Quillen-Suslin (Teorema 3.2.1). Las demostraciones de esta Sección se pueden encontrar en [**Kunz, 1985**].

En lo que sigue sea R un anillo y $\alpha_i : N \to M_i$, $(i = 1, 2)$, dos morfismos de R-módulos.

Definición 23 (**Producto Fibrado**). *Un producto fibrado de M_1 y M_2 sobre N (con respecto a α_1 y α_2) es una terna (P, β_1, β_2), donde P es un R-módulo, $\beta_i : M_i \to P$, $(i = 1, 2)$, son dos morfismos de R-módulos que verifican $\alpha_1 \circ \beta_1 = \alpha_2 \circ \beta_2$, y se verifica la siguiente propiedad universal: para cada otra terna (T, γ_1, γ_2) existe un único morfismo de R-módulos $l : T \to P$ tal que $\gamma_i = \beta_i \circ l$, $(i = 1, 2)$.*



El producto fibrado de M_1 y M_2 sobre N se denota como $P := M_1 \prod_N M_2$.

Proposición A.8.1. *Un producto fibrado de M_1 y M_2 sobre N siempre existe.*

Algunas propiedades elementales del producto fibrado son las siguientes:

Proposición A.8.2.

i) $\ker(\beta_1) \cap \ker(\beta_2) = 0$.

ii) *β_1 induce un isomorfismo* $\ker(\beta_2) \cong \ker(\alpha_1)$, *y β_2 induce un isomorfismo* $\ker(\beta_1) \cong \ker(\alpha_2)$. *En particular,*

$$\beta_2 \text{ (resp. } \beta_1\text{) es inyectiva} \iff \alpha_1 \text{ (resp. } \alpha_2\text{) es inyectiva.}$$

iii) *α_2 induce un morfismo inyectivo* $\mathrm{coker}(\beta_2) \to \mathrm{coker}(\alpha_1)$, *y α_1 induce un morfismo inyectivo* $\mathrm{coker}(\beta_1) \to \mathrm{coker}(\alpha_2)$. *En particular,*

$$\alpha_1 \text{ (resp. } \alpha_2\text{) es sobreyectiva} \implies \beta_2 \text{ (resp. } \beta_1\text{) es sobreyectiva.}$$

iv) Si $S \subset R$ es un sistema multiplicativamente cerrado, entonces $(S^{-1}(M_1 \prod_N M_2), S^{-1}\beta_1, S^{-1}\beta_2)$ es un producto fibrado de $S^{-1}M_1$ y $S^{-1}M_2$ sobre $S^{-1}N$, es decir,

$$S^{-1}(M_1 \prod_N M_2) = S^{-1}M_1 \prod_{S^{-1}N} S^{-1}M_2.$$

El producto fibrado se puede utilizar por ejemplo para "pegar" módulos sobre subconjuntos abiertos de Spec(R) (con la topología de Zariski en Spec(R)). Dados $f, g \in R$ sea M_1 un R_f-módulo y M_2 un R_g-módulo, y supongamos que existe un isomorfismo de R_{fg}-módulos

$$\alpha : (M_1)_g \to (M_2)_f.$$

(Aquí consideramos $(M_1)_g$ y $(M_2)_f$ como R_{fg}-módulos a través del morfismo canónico $(R_f)_g \cong R_{fg} \cong (R_g)_f$).

Sea ahora $N := (M_2)_f$, y sean α_1 la composición del morfismo canónico $\mu_g : M_1 \to (M_1)_g$ con α, y $\alpha_2 = \mu_f : M_2 \to (M_2)_f$ el morfismo canónico.

$$\begin{array}{ccc} M_1 & \xrightarrow{\mu_g} & (M_1)_g \\ & & \downarrow \alpha \\ M_2 & \xrightarrow{\mu_f} & (M_2)_f \end{array}$$

PROPOSICIÓN A.8.3. *Con las notaciones anteriores, si $P := M_1 \prod_{(M_2)_f} M_2$ es el producto fibrado con respecto a α_1 y α_2, entonces los morfismos canónicos*

$$\beta_i : P \to M_i \qquad (i = 1, 2)$$

inducen:

- *un isomorfismo de R_f-módulos $(\beta_1)_f : P_f \to M_1$, y*
- *un isomorfismo de R_g-módulos $(\beta_2)_g : P_g \to M_2$.*

En este caso decimos que *P se forma al pegar M_1 y M_2 sobre $D(fg)$ con respecto a α.*

A.9. Algunas demostraciones sobre propiedades locales citadas en el texto

En esta Sección final se incluyen las pruebas de algunas propiedades locales citadas en el cuerpo de este Trabajo Fin de Grado.

PROPOSICIÓN A.9.1. *Sea $f : M \to N$ un morfismo de R-módulos. Con las notaciones del Apéndice A.3, se tiene que:*

i) $Im(f_\mathfrak{p}) \cong Im(f)_\mathfrak{p}$, $\forall \mathfrak{p} \in \mathrm{Spec}(R)$.
ii) $\mathrm{coker}(f_\mathfrak{p}) \cong \mathrm{coker}(f)_\mathfrak{p}$, $\forall \mathfrak{p} \in \mathrm{Spec}(R)$.
iii) Las siguientes propiedades son equivalentes:
  (a) f es epimorfismo de R-módulos.
  (b) $f_\mathfrak{p}$ es epimorfismo de R-módulos, $\forall \mathfrak{p} \in \mathrm{Spec}(R)$.
  (c) $f_\mathfrak{m}$ es epimorfismo de R-módulos, $\forall \mathfrak{m} \in \mathrm{MaxSpec}(R)$.

DEMOSTRACIÓN. *i)* Es fácil ver la igualdad siguiente:

$$Im(f_\mathfrak{p}) = \{f_\mathfrak{p}(\frac{m}{s}) : \frac{m}{s} \in M_\mathfrak{p}\} = \{\frac{f(m)}{s} : m \in M, s \in R \setminus \mathfrak{p}\} = Im(f)_\mathfrak{p}.$$

ii) Sea $\mathfrak{p} \in \mathrm{Spec}(R)$, y consideremos la siguiente sucesión exacta

$$M \xrightarrow{f} N \xrightarrow{\pi} \mathrm{coker}(f) \to 0,$$

donde π es la proyección canónica sobre el co-núcleo. Localizando por $S = R \setminus \mathfrak{p}$, la siguiente sucesión también será exacta (cf. Proposición A.3.1)

$$M_\mathfrak{p} \xrightarrow{f_\mathfrak{p}} N \xrightarrow{\pi} \mathrm{coker}(f)_\mathfrak{p} \to 0.$$

En particular, usando i), tenemos

$$\operatorname{coker}(f_{\mathfrak{p}}) \cong N_{\mathfrak{p}}/Im(f_{\mathfrak{p}}) \cong N_{\mathfrak{p}}/Im(f)_{\mathfrak{p}} \cong \operatorname{coker}(f)_{\mathfrak{p}}.$$

iii) Por la exactitud del functor localización, tendremos que si f es epimorfismo, entonces $\operatorname{coker}(f) = 0$, luego $\operatorname{coker}(F_{\mathfrak{p}}) \cong \operatorname{coker}(f)_{\mathfrak{p}} = 0$. Por tanto, $f_{\mathfrak{p}}$ es epimorfismo y queda probado $(a) \Longrightarrow (b)$.

$(b) \Longrightarrow (c)$ es evidente porque $\operatorname{MaxSpec}(R) \subseteq \operatorname{Spec}(R)$.

Finalmente, para $(c) \Longrightarrow (a)$ usaremos también la propiedad *ii*). Si $f_{\mathfrak{m}}$ es epimorfismo $\forall \mathfrak{m} \in \operatorname{MaxSpec}(R)$, entonces

$$\operatorname{coker}(f_{\mathfrak{m}}) = 0, \forall \mathfrak{m} \in \operatorname{MaxSpec}(R).$$

Y por *ii*) tenemos que

$$\operatorname{coker}(f)_{\mathfrak{m}} \cong \operatorname{coker}(f_{\mathfrak{m}}) = 0, \forall \mathfrak{m} \in \operatorname{MaxSpec}(R).$$

Ahora como la propiedad de ser cero es una propiedad local, concluimos que el R-módulo $\operatorname{coker}(f) = 0$. Es decir, $Im(f) = N$ y f es epimorfismo. □

Proposición A.9.2. *Sean M, N dos R-módulos y $S \subset R$ multiplicativamente cerrado. El morfismo de R-módulos*

$$\begin{aligned} \operatorname{Hom}_R(M,N) &\to \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N) \\ \alpha &\mapsto S^{-1}\alpha \end{aligned}$$

induce un morfismo de $S^{-1}R$-módulos

$$\begin{aligned} h : S^{-1}\operatorname{Hom}_R(M,N) &\to \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N) \\ \frac{\alpha}{s} &\mapsto \mu_s^{-1} \circ S^{-1}\alpha, \end{aligned}$$

donde $\mu_s^{-1}(\frac{n}{s'}) = \frac{n}{s \cdot s'}$. En esta situación, tenemos que:

i) Si M es finitamente generado, h es inyectivo.
ii) Si M es finitamente presentado, h es isomorfismo.

Demostración. Sea $\{m_1, ..., m_t\}$ un sistema de generadores de M y

$$0 \to K \to R^t \xrightarrow{\epsilon} M \to 0$$

la presentación correspondiente.

i) Para $\alpha \in \operatorname{Hom}_R(M,N)$, $s \in S$, sea $\frac{\alpha}{s} \in \ker(h)$. Entonces $\frac{\alpha(m_i)}{s} = 0$, $(i = 1, ..., t)$ y existe un $s' \in S$ con $s'\alpha(m_i) = 0$, $(i = 1, ..., t)$. Con ello, $s'\alpha = 0$ y $\frac{\alpha}{s} = 0$. En conclusión, $\ker(h) = 0$ y h es inyectivo.

ii) Sea M finitamente presentado. Podemos asumir entonces que K es finitamente generado, y bastaría con probar que h es sobreyectivo.

Sean $i_M : M \to S^{-1}M$ e $i_N : N \to S^{-1}N$ los homomorfismos canónicos. Si $l \in \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$, entonces existe $s \in S$ tal que $n_i' := s \cdot l(\frac{m_i}{1}) \in i_N(N)$, $(i = 1, ..., t)$. Sea $n_i' = \frac{n_i}{1}$ con $n_i \in N$ y $\beta : R^t \to N$ la aplicación lineal dada por $\beta(e_i) = n_i$, $(i = 1, ..., t)$.

Tenemos que ver ahora que existe un $s' \in S$ con $(s'\beta)(K) = 0$. En tal caso, β induce un homomorfismo $\alpha : M \to N$ con $\alpha(m_i) = s'n_i$, $(i = 1, ..., t)$ y por tanto $l = \mu_{s's}^{-1} \circ S^{-1}\alpha$.

De acuerdo a la construcción de β, el diagrama

$$\begin{array}{ccccc} R^t & & \xrightarrow{\qquad\beta\qquad} & & N \\ \downarrow{\scriptstyle \epsilon} & & & & \downarrow{\scriptstyle i_N} \\ M & \xrightarrow{i_M} & S^{-1}M & \xrightarrow{s \cdot l} & S^{-1}N \end{array}$$

es conmutativo. Por tanto, $i_N(\beta(K)) = 0$. Como K es finitamente generado, de lo anterior sigue que existe un $s' \in S$ con $s' \cdot \beta(K) = 0$, como queríamos demostrar.

□

APÉNDICE B

Noetherianos: Teorema de Lasker-Noether, Dimensión de Krull y Extensiones Enteras de anillos

Índice

B.1. Descomposición Primaria: El Teorema de Lasker-Noether **59**
B.2. Breve resumen de propiedades de dimensión para intersecciones completas **61**
B.3. Resumen, aún más breve, de la Normalización de Noether del cociente por un ideal intersección completa en $K[X_1, ..., X_n]$ **67**

En este Apéndice recogemos algunos resultados clásicos, más o menos conocidos, relativos a anillos y módulos noetherianos, descomposición primaria, dimensión de Krull de anillos y módulos, y extensiones enteras. Concluiremos con el Lema de Normalización de Noether. No todos los temas incluidos tienen repercusión directa sobre los contenidos de este Trabajo Fin de Grado; pero algunos de ellos son usados y conviene recogerlos de manera formal. Las referencias para todos estos enunciados son cualquier texto elemental y básico de Álgebra Conmutativa, como [**Atiyah-Macdonald, 1969**], [**Kunz, 1985**] o [**Pardo, 2021**] y las referencias allí señaladas.

Recordemos que un anillo R es noetheriano si todos sus ideales son finitamente generados. Por el Teorema de la Base de Hilbert, todo anillo de polinomios $R[X_1, ..., X_n]$ con coeficientes en un anillo noetheriano es también noetheriano. Como los dominios de ideales principales son noetherianos, los anillos de la forma $K[X_1, ..., X_n]$, donde K es un dominio de ideales principales, son anillos noetherianos.

De modo similar, un R-módulo se dice noetheriano si todos sus submódulos son finitamente generados. Si R es un anillo noetheriano, un R-módulo M es noetheriano si y solamente si es finitamente generado (lo que, en el contexto noetheriano, significa ser finitamente presentado).

Localizaciones, cocientes, sumas finitas y productos finitos de módulos noetherianos siguen siendo noetherianos.

B.1. Descomposición Primaria: El Teorema de Lasker-Noether

Por su aplicación en la Sección 3.4, recordamos aquí el Teorema de Lasker-Noether. Una demostración del mismo puede seguirse en cualquier texto clásico de Intorducción al Álgebra Conmutativa, como el [**Atiyah-Macdonald, 1969**] o el [**Kunz, 1985**].

Definición 24 (**Anillo noetheriano**). *Un anillo R se dice noetheriano si todo ideal es finitamente generado.*

Ejemplo B.1.1.

i) Los cuerpos y los dominios de ideales principales son obviamente anillos noetherianos.
ii) Un Teorema clásdico de D. Hilbert (conocido como el Basissatz), demostrado en [**Hilbert, 1890**]*, afirma que si R es un anillo noetheriano, el anillo $R[X_1, ..., X_n]$ es también noetheriano.*
iii) Si un anillo R es noetheriano, los cocientes $R/\mathfrak{a}$ y las localizaciones $S^{-1}R$ son también anillos noetherianos.

La idea de Lasker y Noether consiste en probar una especie de factorización en anillos noetherianos cualesquiera, extendiendo al lenguaje de ideales la idea de factorización en primos; aunque se pierde un tanto la unicidad. La idea clave es la de *ideal primario*.

DEFINICIÓN 25 (**Ideal primario**). *Sea R un anillo, $\mathfrak{q}$ un ideal propio de R y $a \in R$ un elemento. Consideremos el endomorfismo de R-módulos definido por la homotecia siguiente:*

$$\begin{aligned} \eta_{a,R/\mathfrak{q}} : R/\mathfrak{q} &\to R/\mathfrak{q} \\ b + \mathfrak{q} &\mapsto a - b + \mathfrak{q}. \end{aligned}$$

Decimos que $\mathfrak{q}$ es un ideal primario si para todo $a \in R$, la homotecia $\eta_{a,R/\mathfrak{q}}$ es o bien un monomorfismo de R-módulos o es nilpotente (es decir, o existe $n \in \mathbb{N}$ tal que $(\eta_{a,R/\mathfrak{q}})^n$ es el morfismo nulo).

EJEMPLO B.1.2.

i) Los ideales primos y maximales son ideales primarios.
ii) Si R es un dominio de ideales principales, los ideales primarios son de la forma (p^n), con $n \in \mathbb{N}$ y $p \in R$ un elemento primo.

PROPOSICIÓN B.1.3. *Si $\mathfrak{q} \subset R$ es un ideal primario, entonces su radical es un ideal primo. Es decir, se tiene que*

$$\sqrt{\mathfrak{q}} = \{a \in R : \eta_{a,R/\mathfrak{q}} \text{ no es biyectivo}\} = \{a \in R : \exists n \in \mathbb{N},\ a^n \in \mathfrak{q}\} \in \operatorname{Spec}(R).$$

Si $\mathfrak{q}$ es un ideal primario y $\mathfrak{p} = \sqrt{\mathfrak{q}}$ es su radical, diremos que $\mathfrak{q}$ es un ideal $\mathfrak{p}$-primario.

PROPOSICIÓN B.1.4. *Dada una familia de ideales primarios $\mathfrak{q}_1, ..., \mathfrak{q}_m \subseteq R$ tales que todos son $\mathfrak{p}$-primarios, entonces su intersección*

$$\mathfrak{q} = \bigcap_{i=1}^{r} \mathfrak{q}_i,$$

también es un ideal $\mathfrak{p}$-primario.

DEFINICIÓN 26. *Sea $\mathfrak{a}$ un ideal en un anillo R. Llamaremos descomposición primaria de $\mathfrak{a}$ a toda presentación de $\mathfrak{a}$ como intersección de primarios*

$$\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{q}_i,$$

donde cada $\mathfrak{q}_i \subseteq R$ es un ideal $\mathfrak{p}_i$ primario. Una descomposición primaria de un ideal $\mathfrak{a}$ se dice reducida (o irredundante) si $\mathfrak{p}_i \neq \mathfrak{p}_j$ para cada $i \neq j$.

TEOREMA B.1.5 (**Lasker-Noether**). *Sea $\mathfrak{a}$ un ideal en un anillo noetheriano R. Entonces, $\mathfrak{a}$ posee una descomposición primaria irredundante.*

El Teorema de Lasker-Noether se puede complementar con una cierta unicidad.

DEFINICIÓN 27. *Sea R un anillo y $\mathfrak{a}$ un ideal de R. Un ideal primo $\mathfrak{p} \in \operatorname{Spec}(R)$ se dice asociado al ideal $\mathfrak{a}$ si existe $x \in R$, $x + \mathfrak{a} \neq 0$, tal que*

$$\mathfrak{p} = \operatorname{Ann}_R(x + \mathfrak{a}) = \{a \in R : ax \in \mathfrak{a}\}.$$

Denotamos por $\operatorname{Ass}(R/\mathfrak{a})$ al conjunto de los primos asociados al ideal $\mathfrak{a}$.

TEOREMA B.1.6 (**Unicidad de Lasker-Noether**). *Sea R un anillo noetheriano, $\mathfrak{a} \subseteq R$ un ideal propio y sea dada una descomposición primaria irredundante del ideal $\mathfrak{a}$ de la forma*

$$\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{q}_i,$$

donde cada ideal $\mathfrak{q}_i$ es $\mathfrak{p}_i$-primario, entonces

$$\operatorname{Ass}(R/\mathfrak{a}) = \{\mathfrak{p}_1, ..., \mathfrak{p}_r\}.$$

De hecho, los ideales asociados $\operatorname{Ass}(R/\mathfrak{a})$ contienen a los ideales primos minimales entre aquellos que contienen al ideal $\mathfrak{a}$. Los primos asociados que no son minimales se llaman primos inmersos sobre $\mathfrak{a}$.

Una de las propiedades que determinan los primos asociados es la siguiente.

COROLARIO B.1.7. *Sea $\mathfrak{a} \subseteq R$ un ideal en un anillo noetheriano, y sea*

$$\mathfrak{a} = \bigcap_{i=1}^{m} \mathfrak{q}_i$$

una descomposición primaria irredundante de $\mathfrak{a}$, donde cada $\mathfrak{q}_i$ es un ideal $\mathfrak{p}_i$-primario. Consideremos también el conjunto de los divisores de cero módulo $\mathfrak{a}$:

$$\mathrm{Div}(\mathfrak{a}) = \{\mathfrak{a} \in R : a + \mathfrak{a} \text{ es un divisor de cero en } R/\mathfrak{a}\}.$$

Entonces,

$$\mathrm{Div}(\mathfrak{a}) = \bigcup_{i=1}^{m} \mathfrak{p}_i.$$

Así, si un elemento $x \in R$ no pertenece a ningún ideal primo asociado a un ideal $\mathfrak{a}$, entonces $x + \mathfrak{a} \in R/\mathfrak{a}$ no es divisor de cero.

Obviamente, el radical de un ideal se obtiene mediante los ideales primos asociados, aunque puede haber redundancias. Esto es, si

$$\mathfrak{a} = \bigcap_{i=1}^{m} \mathfrak{q}_i$$

es una descomposición primaria irredundante de $\mathfrak{a}$, donde cada $\mathfrak{q}_i$ es un ideal $\mathfrak{p}_i$-primario, se tiene

$$\sqrt{\mathfrak{a}} = \bigcap_{i=1}^{m} \mathfrak{q}_i = \bigcap_{\mathfrak{p} \in \mathrm{Ass}(R/\mathfrak{a})} \mathfrak{p}.$$

B.2. Breve resumen de propiedades de dimensión para intersecciones completas

En [**Kronecker, 1882**], L. Kronecker introduce la pregunta de cuántas ecuaciones polinomiales son necesarias para describir implícitamente una variedad algebraica afín o proyectiva. Él mismo responde con un método, conocido como el método de Kronecker, que prueba que toda variedad algebraica V en el espacio afín n-dimensional $\mathbb{A}^n(K)$ sobre un cuerpo algebraicamente cerrado se puede expresar mediante $n+1$ ecuaciones polinomiales.

En primer lugar fijemos un poco las notaciones. Dado K un cuerpo algebraicamente cerrado, sea $\mathbb{A}^n(K) = K^n$ el espacio afín de dimensión n sobre K. Sea $K[X_1, ..., X_n]$ el anillo de polinomios en n variables con coeficientes en K. Dado un polinomio $f \in K[X_1, ..., X_n]$ definimos la variedad algebraica de sus ceros $V_{\mathbb{A}}(f) \subseteq \mathbb{A}^n(K)$ mediante:

$$V_{\mathbb{A}}(f) := \{x \in \mathbb{A}^n(K) : f(x) = 0\}.$$

Dada una familia $\mathcal{F} \subseteq K[X_1, ..., X_n]$ de polinomios, $\mathcal{F}$ no necesariamente finita, denotamos por $V_{\mathbb{A}}(\mathcal{F})$ a la variedad algebraica formada por todos los ceros comunes a todos los polinomios de $\mathcal{F}$:

$$V_{\mathbb{A}}(\mathcal{F}) := \{x \in \mathbb{A}^n(K) : f(x) = 0, \forall f \in \mathcal{F}\}.$$

Es fácil observar que si $\mathfrak{a} = (\mathcal{F})$ es el ideal de $K[X_1, ..., X_n]$ generado por $\mathcal{F}$ se tiene que $V_{\mathbb{A}}(\mathfrak{a}) = V_{\mathbb{A}}(\mathcal{F})$. Por eso se definen la *variedades algebraicas afines* como cualquier elemento del conjunto

$$\{V_{\mathbb{A}}(\mathfrak{a}) : \mathfrak{a} \subseteq K[X_1, ..., X_n] \text{ es un ideal}\}.$$

Se observa también que existe una única topología en $\mathbb{A}^n(K)$ en la que el conjunto de sus cerrados es, precisamente, $\{V_{\mathbb{A}}(\mathfrak{a}) : \mathfrak{a} \subseteq K[X_1, ..., X_n] \text{ es un ideal}\}$. Esta topología se denomina topología de Zariski en $\mathbb{A}^n(K)$ (cf., por ejemplo, [**Pardo, 2021**]).

El Teorema de la Base de Hilbert (cf. [**Hilbert, 1890**]) prueba que todo ideal de $K[X_1, ..., X_n]$ es un ideal finitamente generado. Por tanto, si $V \subseteq \mathbb{A}^n(K)$ es una variedad algebraica, y $\mathfrak{a} = (f_1, ..., f_s) \subseteq K[X_1, ..., X_n]$ es un ideal tal que $V = V_{\mathbb{A}}(\mathfrak{a})$, tenemos entonces las igualdades

$$V = V_{\mathbb{A}}(\mathfrak{a}) = V_{\mathbb{A}}(f_1, ..., f_s) = \bigcap_{i=1}^{s} V_{\mathbb{A}}(f_i).$$

En particular, todo cerrado en la topología de Zariski de $\mathbb{A}^n(K)$ es intersección finita de cerrados de la forma $V_{\mathbb{A}}(f)$ con $f \in K[X_1, ..., X_n]$. A los cerrados de la forma $V_{\mathbb{A}}(f)$ los denominaremos *hipersuperficies*. La pregunta de Kronecker se traduce entonces del modo siguiente:

Dado un cerrado Zariski, $V \subseteq \mathbb{A}^n(K)$, ¿cuántas hipersuperficies se necesitan intersecar para obtener V?

La respuesta de Kronecker fue $n + 1$.

TEOREMA B.2.1 ([**Kronecker, 1882**]). *Dado un cerrado $V \subseteq \mathbb{A}^n(K)$ para la topología de Zariski, existen $n + 1$ polinomios $f_1, ..., f_{n+1} \in K[X_1, ..., X_n]$ tales que*

$$V = V_{\mathbb{A}}(f_1) \cap ... \cap V_{\mathbb{A}}(f_{n+1}).$$

Pero esta respuesta es insuficiente. Si hablásemos de variedades afines lineales tendríamos una relación entre el número mínimo de ecuaciones necesarias para describir la variedad y su dimensión:

TEOREMA B.2.2. *Sea $L \subseteq \mathbb{A}^n(K)$ una variedad afín lineal de dimensión r. Entonces, existen $l_1, ..., l_{n-r} \in K[X_1, ..., X_n]$ polinomios de grado 1 tales que*

$$L = V_{\mathbb{A}}(l_1) \cap ... \cap V_{\mathbb{A}}(l_{n-r}).$$

Para tratar de interpretar este elemental resultado de Álgebra Lineal, necesitamos interpretar la noción de "dimensión". En este sentido, es W. Krull (en [**Krull, 1935**]) quien nos apunta una noción de dimensión.

DEFINICIÓN 28. *Un cerrado $V \subseteq \mathbb{A}^n(K)$ para la topología de Zariski se llama reducible si existen dos cerrados $W_1, W_2 \subseteq \mathbb{A}^n(K)$ en la topología de Zariski tales que:*

- $V = W_1 \cap W_2$.
- $W_i \subsetneq V$, $i = 1, 2$.

Los cerrados irreducibles juegan un papel similar al que juegan las componentes conexas en topología. De hecho, todo cerrado $V \subseteq \mathbb{A}^n(K)$ en la topología de Zariski admite una descomposición única como unión finita de cerrados irreducibles gracias al Teorema de la Base de Hilbert (mediante la interpretación de E. Noether).

TEOREMA B.2.3. *Para todo cerrado $V \subseteq \mathbb{A}^n(K)$ en la topología de Zariski, existen $V_1, ..., V_s \subseteq \mathbb{A}^n(K)$ cerrados irreducibles tales que*

$$V = V_1 \cup ... \cup V_s. \tag{B.2.1}$$

Además, las descomposiciones minimales de tipo (B.2.1) son únicas (salvo permutación). A los elementos en $\{V_1, ..., V_s\}$ para una descomposición minimal de V se los denomina componentes irreducibles de V.

A partir de los cerrados irreducibles, Krull introduce una noción de dimensión que generaliza el concepto "punto $\subsetneq$ recta $\subsetneq$ plano":

DEFINICIÓN 29 (**Dimensión de Krull**). *Una cadena de longitud s de cerrados irreducibles en $\mathbb{A}^n(K)$ es una cadena*

$$\emptyset \neq V_0 \subsetneq V_1 \subsetneq ... \subsetneq V_s,$$

donde cada $V_i \subseteq \mathbb{A}^n(K)$ es un cerrado irreducible. La dimensión de un cerrado $W \subseteq \mathbb{A}^n(K)$ (llamada dimensión de Krull) es el máximo de las longitudes de cadenas de cerrados irreducibles contenidas en W. Es decir, el máximo de los $s \in \mathbb{N}$ tales que existen $V_0, ..., V_s \subseteq W$ cerrados irreducibles tales que

$$\emptyset \neq V_0 \subsetneq V_1 \subsetneq ... \subsetneq V_s \subseteq W.$$

Es fácil ver que la dimensión de los conjuntos finitos de puntos es 0. Con un poco de ayuda del Nullstellensatz de Hilbert no es difícil ver que la dimensión de Krull de $\mathbb{A}^n(K)$ es n.

En el caso de hipersuperficies, el Teorema del Ideal Principal de Krull nos permite concluir que la dimensión de una hipersuperficie $V_{\mathbb{A}}(f) \subseteq \mathbb{A}^n(K)$, donde $f \notin K$, es

$$\dim(V_{\mathbb{A}}(f)) = n - 1.$$

Aparentemente, al aumentar el número de hipersuperficies que describen un cerrado de la topología de Zariski la dimensión debería caer en 1 a cada ecuación añadida. Esto no es así por razones obvias, como en los siguientes ejemplos.

Ejemplo B.2.4.

- *Tomemos $f_1 = X_1$, $f_2 = X_1 + 1$. Se tiene que $V_{\mathbb{A}}(f_1) \subseteq \mathbb{A}^3(K)$ tiene dimensión 2; pero $V_{\mathbb{A}}(f_1, f_2) = \emptyset$ tiene dimensión -1 (como dimensión de Krull del vacío).*
- *Tomemos $f_1 = X_1 \cdot X_2$, $f_2 = X_1$. Se tiene que $V_{\mathbb{A}}(f_1) \subseteq \mathbb{A}^3(K)$ tiene dimensión 2 (es la noción de un par de hiperplanos), mientras que $V_{\mathbb{A}}(f_1, f_2) = V_{\mathbb{A}}(X_1)$ es un hiperplano y no una curva de dimensión 1.*

Así que hay que tener cuidado con las interacciones (en general no lineales) entre las ecuaciones polinomiales. Ahí acude la noción de ideal.

Consideremos $W \subseteq \mathbb{A}^n(K)$ un subconjunto y definamos el ideal $I(W) \subseteq K[X_1, ..., X_2]$ dado mediante la siguiente igualdad:

$$I(W) := \{f \in K[X_1, ..., X_n] : f(x) = 0,\ \forall x \in W\}.$$

Resumamos algunas propiedades sencillas de demostrar:

Proposición B.2.5. *Con las notaciones anteriores:*

i) Dado $W \subseteq \mathbb{A}^n(K)$ un subconjunto cualquiera,

$$V_{\mathbb{A}}(I(W)) = \overline{W}^Z,$$

donde $\overline{W}^Z$ es la clausura de W en la topología de Zariski de $\mathbb{A}^n(K)$. En particular, si $W \subseteq \mathbb{A}^n(K)$ es cerrado para la topología de Zariski,

$$V_{\mathbb{A}}(I(W)) = W.$$

ii) Sea $V \subseteq \mathbb{A}^n(K)$ un cerrado para la topología de Zariski de $\mathbb{A}^n(K)$. Son equivalentes:
(a) V es irreducible.
(b) $I(V) \in \mathrm{Spec}(K[X_1, ..., X_n])$ es un ideal primo.

iii) Si $V = \{a\} \subseteq \mathbb{A}^n(K)$ es un punto de $\mathbb{A}^n(K)$, entonces $I(V)$ es un ideal maximal en $K[X_1, ..., X_n]$. De hecho, es el núcleo del morfismo de anillos

$$\begin{aligned} \varphi_a : K[X_1, ..., X_n] &\to K \\ f &\mapsto f(a). \end{aligned}$$

Al ideal $I(\{a\})$ lo denotaremos mediante $\mathfrak{m}_a$ y está generado por n elementos de $K[X_1, ..., X_n]$:

$$\mathfrak{m}_a = (X_1 - a_1, ..., X_n - a_n),$$

donde $a = (a_1, ..., a_n)$.

Una forma más delicada de identificar variedades algebraicas e ideales es el famoso Teorema de los Ceros de Hilbert (Nullstellensatz). En la forma de Rabinowitsch, el enunciado toma la forma siguiente:

Teorema B.2.6. *Sea $\mathfrak{a} \subseteq K[X_1, ..., X_n]$ un ideal. Se tiene que*

$$I(V_{\mathbb{A}}(\mathfrak{a})) = \sqrt{\mathfrak{a}} := \{f \in K[X_1, ..., X_n] : \exists m \in \mathbb{N},\ f^m \in \mathfrak{a}\}.$$

Además, los ideales maximales en $K[X_1, ..., X_n]$ son dados por:

$$\mathrm{MaxSpec}(K[X_1, ..., X_n]) = \{\mathfrak{m}_a : a \in \mathbb{A}^n(K)\}.$$

No vamos a discutir los detalles de estas ideas en este trabajo, en el cual las usaremos instrumentalmente, pero recordemos que $\sqrt{\mathfrak{a}}$ se denomina el radical del ideal $\mathfrak{a}$ y satisface

$$\sqrt{\mathfrak{a}} = \bigcap \{\mathfrak{p} \in \operatorname{Spec}(K[X_1, ..., X_n]) : \mathfrak{p} \supseteq \mathfrak{a}\}.$$

Este juego entre ideales y cerrados en la topología de Zariski condujo a W. Krull a introducir la dimensión en anillos:

Definición 30. *Sea R un anillo.*

i) Una cadena de longitud s de ideales primos de R es una cadena

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq ... \subsetneq \mathfrak{p}_s,$$

donde cada $\mathfrak{p}_i \in \operatorname{Spec}(R)$.

ii) Se denomina altura de un ideal primo al máximo de las longitudes de cadenas de primos contenidas en él. Se denota mediante $\operatorname{ht}(\mathfrak{p})$.

iii) Se denomina co-altura de un ideal primo al máximo de las longitudes de cadenas de primos por encima de él. Se denota mediante $\operatorname{coht}(\mathfrak{p})$ *y es el máximo de los $s \in \mathbb{N}$ tales que existen $\mathfrak{p}_0, ..., \mathfrak{p}_s \in \operatorname{Spec}(R)$ verificando*

$$\mathfrak{p} \subseteq \mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_s.$$

iv) La dimensión (de Krull) de un anillo R es el máximo de las alturas o co-alturas de sus ideales primos. Es decir,

$$\dim(R) := \max\{\operatorname{ht}(\mathfrak{p}) : \mathfrak{p} \in \operatorname{Spec}(R)\} = \max\{\operatorname{coht}(\mathfrak{p}) : \mathfrak{p} \in \operatorname{Spec}(R)\}.$$

La dimensión de Krull de un anillo no siempre es finita, ni siquiera cuando el anillo es noetheriano. Un famoso teorema de P. Samuel, conocido como el Teorema de la Dimensión Local, prueba que si $(R, \mathfrak{m})$ es local y noetheriano, entonces

$$\dim(R) = \operatorname{ht}(\mathfrak{m}) < \infty.$$

El Teorema de la Dimensión Local es más completo (ver [**Pardo, 2021**]) pero obviamos sus propiedades.

Sí se puede probar, gracias a Krull, que la dimensión de $K[X_1, ..., X_n]$ satisface:

$$n = \dim(\mathbb{A}^n(K)) = \dim(K[X_1, ..., X_n]).$$

Más aún, si $\mathfrak{a}$ es un ideal de $K[X_1, ..., X_n]$ se tiene que las dimensiones en la topología de Zariski (geometría) y la dimensión de los anillos coinciden en el sentido siguiente:

$$\dim(V_{\mathbb{A}}(\mathfrak{a})) = \dim(K[X_1, ..., X_n]/\mathfrak{a}).$$

Este sería un primer paso para hacer interactuar el número de ecuaciones (i.e. los generadores minimales de $\mathfrak{a}$) y la dimensión geométrica. Pero el camino no es tan trivial. Aquí intervienen Krull y Macaulay (ver [**Macaulay, 1916**]) con dos teoremas famosos como son los siguientes.

Dado un ideal (no necesariamente primo) $\mathfrak{a} \subseteq K[X_1, ..., X_n]$, llamamos co-altura de un ideal a la dimensión del anillo cociente $K[X_1, ..., X_n]/\mathfrak{a}$:

$$\operatorname{coht}(\mathfrak{a}) = \dim(K[X_1, ..., X_n]/\mathfrak{a}).$$

Y llamamos altura del ideal $\mathfrak{a}$ al mínimo de las alturas de los primos que contienen al ideal $\mathfrak{a}$:

$$\operatorname{ht}(\mathfrak{a}) = \min\{\operatorname{ht}(\mathfrak{p}) : \mathfrak{p} \in \operatorname{Spec}(K[X_1, ..., X_n]),\ \mathfrak{p} \supseteq \mathfrak{a}\}.$$

No resulta fácil encajar las alturas y co-alturas de cualquier ideal por culpa de las componentes inmersas; pero Krull y Macaulay nos dieron alguna pista.

Definición 31 (**Sucesión regular**). *Sea R un anillo y $f_1, ..., f_r \in R$. Diremos que forman una sucesión regular si satisfacen:*

i) f_1 no es divisor de cero de R y para $1 \leq i \leq r-1$, f_{i+1} no es divisor de cero de $R/(f_1, ..., f_i)$.

ii) El ideal $\mathfrak{a} = (f_1, ..., f_r)$ es un ideal propio de R.

El primer resultado, que se sigue de la estructura de bases de trascendencia, muestra que altura y co-altura "casan" bien en el caso de ideales primos de $K[X_1, ..., X_n]$ (una prueba puede verse en [**Pardo, 2021**] o [**Kunz, 1985**]).

TEOREMA B.2.7 (**Catenaridad de** $K[X_1, ..., X_n]$). *Si* $\mathfrak{p} \subseteq K[X_1, ..., X_n]$ *es un ideal primo, entonces*

$$\mathrm{ht}(\mathfrak{p}) + \mathrm{coht}(\mathfrak{p}) = n.$$

Seguidamente, las dos contribuciones de Krull y Macaulay se resumen del modo siguiente:

TEOREMA B.2.8 (**de la Pureza de Macaulay**). *Sean* $f_1, ..., f_r \in K[X_1, ..., X_n]$ *tales que el ideal que generan* $\mathfrak{a} = (f_1, ..., f_r)$ *tiene altura* r*. Entonces, todos los ideales primos asociados de* $\mathfrak{a}$ *tienen altura* r*.*

TEOREMA B.2.9 (**del Ideal Principal de Krull**). *Sean* $f_1, ..., f_r \in K[X_1, ..., X_n]$*, sea* $\mathfrak{a} = (f_1, ..., f_r)$ *el ideal que generan y supongamos que* $\mathfrak{a} \neq (1)$*. Entonces, todo ideal primo minimal* $\mathfrak{p}$ *entre los primos que contienen a* $\mathfrak{a}$ *satisfacen*

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

Más aún, si $f_1, ..., f_r$ *forman una sucesión regular de polinomios, se tiene que todo ideal primo* $\mathfrak{p} \in \mathrm{Spec}(K[X_1, ..., X_n])$ *tal que* $\mathfrak{p} \supseteq \mathfrak{a}$ *satisface*

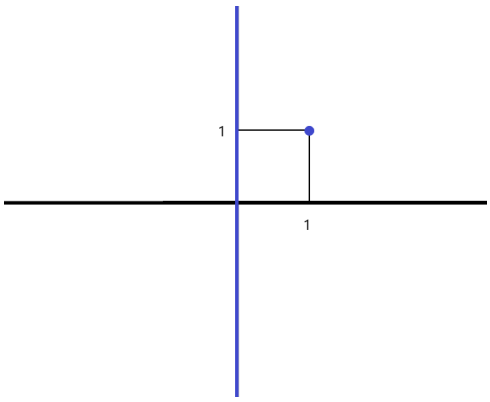
$$\mathrm{ht}(\mathfrak{p}) = r.$$

En particular, concluimos los siguientes hechos de estos dos resultados históricos:

i) Si $\mathfrak{a} = (f_1, ..., f_r)$ es un ideal generado por una sucesión regular, entonces $\mathrm{ht}(\mathfrak{a}) = r$ y $\mathrm{coht}(\mathfrak{a}) = n - r$. Y por tanto,
$$\mathrm{ht}(\mathfrak{a}) + \mathrm{coht}(\mathfrak{a}) = n.$$

ii) Sea $\mathfrak{a} = (f_1, ..., f_r)$ un ideal de altura r y $V = V_{\mathbb{A}}(\mathfrak{a})$ la variedad de sus ceros. Entonces, si $V = W_1 \cup ... \cup W_s$ es la descomposición de V en componentes irreducibles, se tiene que
$$n - r = \dim(V_{\mathbb{A}}(\mathfrak{a})) = \dim(V) = \dim(W_i), \quad 1 \leq i \leq s.$$
Esto significa la "pureza" del lado geométrico: todas las componentes irreducibles tienen la misma dimensión.

Obsérvese que, por ejemplo, el cerrado Zariski $V = V_{\mathfrak{a}}(X_1) \cup V_{\mathfrak{a}}(X_1 - 1, X_2 - 1)$ no puede ser dado por un ideal $\mathfrak{a}$ generado por un único elemento: se trata de la unión de una recta con un punto exterior, y tiene dos componentes irreducibles (una recta de dimensión 1 y un punto de dimensión 0).



En todo caso, conviene instrumentalizar mejor esta interacción entre dimensión y número de ecuaciones. En este sentido surge la idea de intersección completa.

DEFINICIÓN 32 (**Intersección completa**). *Con las notaciones precedentes:*

i) Un cerrado $V \subseteq \mathbb{A}^n(K)$ *para la topología de Zariski de dimensión* d *se dice intersección completa conjuntista si existen* $f_1, ..., f_{n-d} \in K[X_1, ..., X_n]$ *tales que*
$$V = V_{\mathbb{A}}(f_1, ..., f_{n-d}).$$

ii) Un cerrado $V \subseteq \mathbb{A}^n(K)$ *para la topología de Zariski de dimensión* d *se dice intersección completa idealísticamente si existen* $f_1, ..., f_{n-d} \in K[X_1, ..., X_n]$ *tales que*
$$I(V) = (f_1, ..., f_{n-d}).$$

Para más detalles sobre estas nociones véase [**Kunz, 1985**].

Tenemos así fijadas algunas de las nociones usadas en el principal Teorema que se pretende probar en esta Sección de aplicaciones del Teorema de Quillen-Suslin. Nos estamos ocupando de un anillo cociente de la forma

$$K[X_1, ..., X_n]/\mathfrak{a},$$

donde $\mathfrak{a} = (f_1, ..., f_r)$ es un ideal de altura r generado por r elementos. Este anillo satisface las siguientes propiedades que resumen lo descrito hasta ahora:

i) Como $\mathfrak{a}$ es un ideal de altura r generado por r elementos, por el Teorema de la Pureza de Macaulay, los ideales primos asociados a $\mathfrak{a}$ son todos minimales y de altura r. Es decir, siguiendo las notaciones del Teorema de Lasker-Noether (ver Apéndice B.1) tenemos que $\mathfrak{a}$ admite una descomposición primaria irredundante de la forma

$$\mathfrak{a} = \bigcap_{i=1}^{m} \mathfrak{q}_i, \tag{B.2.2}$$

donde cada $\mathfrak{q}_i$ es un ideal $\mathfrak{p}_i$-primario. Los primos asociados al ideal $\mathfrak{a}$ son $\{\mathfrak{p}_1, ..., \mathfrak{p}_m\}$. Los divisores de cero del cociente $K[X_1, ..., X_n]/\mathfrak{a}$ son los elementos del conjunto

$$\mathrm{Div}(\mathfrak{a}) = \{f \in \mathfrak{a} : f \in \bigcup_{i=1}^{m} \mathfrak{p}_i\}.$$

Además, el Teorema de Macaulay implica que todos esos primos asociados son minimales entre los primos que contienen al ideal $\mathfrak{a}$. Es decir, se satisface:
- $\forall \mathfrak{p} \in \mathrm{Spec}(R)$, si $\mathfrak{p} \supseteq \mathfrak{a} \Longrightarrow \exists i$ tal que $\mathfrak{p} \supseteq \mathfrak{p}_i$.
- $\forall \mathfrak{p} \in \mathrm{Spec}(R)$ con $\mathfrak{p} \supseteq \mathfrak{a}$, si $\mathfrak{p}_i \supseteq \mathfrak{p}$ para algún i, entonces $\mathfrak{p}_i = \mathfrak{p}$.

Finalmente, todos tienen la misma altura, es decir

$$\mathrm{ht}(\mathfrak{p}_i) = \mathrm{ht}(\mathfrak{q}_i) = \mathrm{ht}(\mathfrak{a}) = r, \quad \forall i \in \{1, ..., m\}.$$

ii) Por la catenaridad de $K[X_1, ..., X_n]$, si $\{\mathfrak{p}_1, ..., \mathfrak{p}_m\}$ son los ideales primos asociados a nuestro ideal $\mathfrak{a}$ de la descomposición (B.2.2) anterior, entonces

$$\mathrm{coht}(\mathfrak{p}_i) = \mathrm{coht}(\mathfrak{q}_i) = \mathrm{coht}(\mathfrak{a}) = n - r, \quad \forall i \in \{1, ..., m\}.$$

Además, los siguientes son los ideales primos minimales del anillo cociente:

$$\{\mathfrak{p}_1/\mathfrak{a}, ..., \mathfrak{p}_m/\mathfrak{a}\} \subseteq \mathrm{Spec}(K[X_1, ..., X_n]/\mathfrak{a}).$$

(Recordemos que el espectro primo del anillo cociente viene dado por $\mathrm{Spec}(R/\mathfrak{b}) = \{\mathfrak{p}/\mathfrak{b} : \mathfrak{p} \in \mathrm{Spec}(R)\}$).

iii) La co-altura se mantiene por paso al cociente por definición. Por tanto, en el anillo cociente $K[X_1, ..., X_n]/\mathfrak{a}$ se tiene que

$$\mathrm{coht}(\mathfrak{p}_i/\mathfrak{a}) = \mathrm{coht}(\mathfrak{p}_i) = n - r,$$

para cada $i \in \{1, ..., m\}$. Por tanto, como la dimensión de Krull de un anillo es el máximo de las co-alturas de sus ideales primos, tenemos que

$$\dim(R) = \max\{\mathrm{coht}(\mathfrak{p}) : \mathfrak{p} \in \mathrm{Spec}(R)\}.$$

Entonces, la dimensión de Krull de un anillo es el máximo de las co-alturas de sus ideales primos minimales

$$\dim(R) = \max\{\mathrm{coht}(\mathfrak{p}) : \mathfrak{p} \in \mathrm{Spec}(R),\ \mathfrak{p} \text{ minimal}\}.$$

Concluimos así que la dimensión de Krull de nuestro anillo cociente satisface

$$\dim(K[X_1, ..., X_n]/\mathfrak{a}) = \max_{1 \leq i \leq m} \{\mathrm{coht}(\mathfrak{p}_i/\mathfrak{a})\} = n - r.$$

B.3. Resumen, aún más breve, de la Normalización de Noether del cociente por un ideal intersección completa en $K[X_1, ..., X_n]$

El otro elemento que aparece en el enunciado que pretendemos estudiar en esta Sección es el concepto de "variables en posición de Noether" con respecto a un ideal. Vamos a hacer un resumen aún más breve de este concepto. Las demostraciones pueden verse en cualquier texto básico de Álgebra Conmutativa, como [**Atiyah-Macdonald, 1969**], [**Kunz, 1985**] o [**Pardo, 2021**].

DEFINICIÓN 33. *Sea $A \subseteq B$ una extensión de anillos y sea $\alpha \in B$ un elemento. Diremos que α es entero sobre A si existe un polinomio mónico*

$$p(T) = T^D + a_{D-1}T^{D-1} + ... + a_0 \in A[T]$$

de tal modo que $p(\alpha) = 0$.

Se puede probar que la suma y el producto de elementos enteros es entero. Así, sea $A \subseteq B$ un anillo, sean $\{\alpha_1, ..., \alpha_n\} \subseteq B$ una familia finita de elementos. Denotamos por $A[\alpha_1, ..., \alpha_n]$ al menor subanillo de B que contiene a A y al conjunto $\{\alpha_1, ..., \alpha_n\}$. A los anillos de la forma $A[\alpha_1, ..., \alpha_n]$ se les denomina *A-álgebras finitamente generadas*. Se tiene entonces la siguiente

PROPOSICIÓN B.3.1. *Sea A un anillo, $A[\alpha_1, ..., \alpha_n]$ una A-álgebra finitamente generada. Son equivalentes:*

i) Los elementos de $\{\alpha_1, ..., \alpha_n\}$ son enteros sobre A.
ii) Todos los elementos del anillo $A[\alpha_1, ..., \alpha_n]$ son enteros sobre A.

DEFINICIÓN 34 (**Extensión entera**). *Una extensión de anllos $A \subseteq B$ se dice que es una extensión entera si todos los elementos de B son enteros sobre A.*

Si $A \subseteq B$ y $B = A[\alpha_1, ..., \alpha_n]$ es una A-álgebra finitamente generada, entonces $A \subseteq B$ es una extensión entera de anillos si y solo si B es un A-módulo finitamente generado. Se puede decir, en este caso, que B es una *A-álgebra finita*.

Las extensiones enteras de anillos son una generalización de las extensiones algebraicas de cuerpos. En otras palabras, si F y K son dos cuerpos tales que $F \subseteq K$ es una extensión algebraica de cuerpos, entonces es una extensión entera de anillos.

Algunas de las propiedades esenciales de las extensiones enteras de anillos se expresan mediante la operación de contracción de ideales. Recuérdese que si $A \subseteq B$ es una extensión de anillos y $\mathfrak{b} \subseteq B$ es un ideal, llamamos ideal contracción de $\mathfrak{b}$ en A al ideal de A

$$\mathfrak{b}^c = \mathfrak{b} \cap A = \{x \in A : x \in \mathfrak{b}\} \subseteq A.$$

La siguiente Proposición resume algunas de las propiedades más elementales de la contracción en relación con extensiones enteras.

PROPOSICIÓN B.3.2. *Sea $A \subseteq B$ una extensión entera de anillos. Entonces:*

i) Si $\mathfrak{b} \subseteq B$ es un ideal de B, la siguiente es una extensión entera de anillos:

$$A/\mathfrak{b}^c \hookrightarrow B/\mathfrak{b}.$$

ii) Si $S \subseteq A$ es un conjunto multiplicativamente cerrado, $S^{-1}B$ es un anillo entero sobre $S^{-1}A$.
iii) La contracción define una aplicación continua suprayectiva entre los respectivos espectros primos de los anillos. Es decir, la siguiente aplicación es suprayectiva y continua:

$$c : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$$
$$\mathfrak{q} \mapsto \mathfrak{q}^c,$$

donde hemos considerado las topologías de Zariski en $\mathrm{Spec}(A)$ y $\mathrm{Spec}(B)$.
iv) No existe inclusión propia entre los ideales primos que se contraen en el mismo ideal primo. Es decir, dados $\mathfrak{q}_1, \mathfrak{q}_2 \in \mathrm{Spec}(B)$ dos ideales primos tales que $\mathfrak{q}_1^c = \mathfrak{q}_2^c \in \mathrm{Spec}(A)$, entonces

$$\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \Longrightarrow \mathfrak{q}_1 = \mathfrak{q}_2.$$

v) La contracción define también una operación continua y sobreyectiva entre los respectivos espectros maximales. Es decir, la siguiente aplicación está bien definida y es continua y sobreyectiva:

$$c : \mathrm{MaxSpec}(B) \to \mathrm{MaxSpec}(A)$$
$$\mathfrak{m} \mapsto \mathfrak{m}^c,$$

donde consideramos las respectivas topologías de Zariski.

No solo los primos y maximales se transforman bien en extensiones enteras, sino también las cadenas finitas. Son los llamados Teoremas del Ascenso y del Descenso debidos a Krull, Cohen y Serdenberg (quienes los probaron de manera independiente en distintas épocas).

TEOREMA B.3.3 (**del Ascenso o Going-Up**). *Sea $A \subseteq B$ una extensión entera de anillos. Sean $n, m \in \mathbb{N}$ dos números naturales con $m \geq n$. Supongamos que existen:*

i) Una cadena de ideales primos de A con m elementos

$$\mathfrak{p}_1 \subseteq ... \subseteq \mathfrak{p}_m.$$

ii) Una cadena de ideales primos en B con n elementos

$$\mathfrak{q}_1 \subseteq ... \subseteq \mathfrak{q}_n,$$

de tal modo que $\mathfrak{q}_i^c = \mathfrak{p}_i$, $i = 1, ..., n$.

Entonces, existen $\mathfrak{q}_{n+1} \subseteq ... \subseteq \mathfrak{q}_m$ ideales primos de B tales que

$$\mathfrak{q}_j^c = \mathfrak{p}_j, \quad j = n+1, ..., m.$$

Un Corolario inmediato del Teorema del Ascenso es el siguiente:

COROLARIO B.3.4. *Sea $A \subseteq B$ una extensión entera de anillos. Sea $\mathfrak{q} \in \mathrm{Spec}(B)$ un ideal primo de B. Entonces,*

$$\mathrm{coht}(\mathfrak{q}^c) = \mathrm{coht}(\mathfrak{q}).$$

En particular, las dimensiones de Krull de A y B coinciden, esto es,

$$\dim(A) = \dim(B) = \max\{\mathrm{coht}(\mathfrak{q}) : \mathfrak{q} \in \mathrm{Spec}(B)\}.$$

En otras palabras, las extensiones enteras de anillos preservan la dimensión de Krull, y la co-altura de los ideales primos se conserva por contracción.

En lo que respecta a las alturas, existe un resultado similar que aquí enunciaremos en el caso en que A sea un dominio de factorización única, aunque sigue siendo cierto cuando A es un dominio normal (íntegramente cerrado en su cuerpo de fracciones).

TEOREMA B.3.5 (**del Descenso o Going-Down**). *Sean A y B dos dominios de integridad. Supongamos que $A \subseteq B$ es una extensión entera de anillos y que A es dominio de factorización única. Sean $m, n \in \mathbb{N}$ dos números naturales con $m \geq n$. Supongamos que existen*

i) Una cadena de ideales primos de A con m elementos

$$\mathfrak{p}_1 \subseteq ... \subseteq \mathfrak{p}_m.$$

ii) Una cadena de ideales primos en B con $m - n$ elementos

$$\mathfrak{q}_{n+1} \subseteq ... \subseteq \mathfrak{q}_m,$$

de tal modo que $\mathfrak{q}_i^c = \mathfrak{p}_i$, $i = n+1, ..., m$.

Entonces existen ideales primos $\mathfrak{q}_1 \subseteq ... \subseteq \mathfrak{q}_n$ en B de tal modo que tenemos una cadena de ideales primos en B de longitud n

$$\mathfrak{q}_1 \subseteq \mathfrak{q}_n \subseteq \mathfrak{q}_{n+1} \subseteq ... \subseteq \mathfrak{q}_m,$$

verificando $\mathfrak{q}_i^c = \mathfrak{p}_i$, $i = 1, ..., m$.

El Corolario evidente es que se preservan las alturas.

COROLARIO B.3.6. *Sea $A \subseteq B$ una extensión entera de dominios de integridad. Supongamos que A es dominio de factorización única. Sea $\mathfrak{q} \in \mathrm{Spec}(B)$ un ideal primo de B. Entonces*

$$\mathrm{ht}(\mathfrak{q}^c) = \mathrm{ht}(\mathfrak{q}).$$

La última noción requerida es la noción de Normalización de Noether de un ideal en un anillo de polinomios (debida a [**Noether, 1921**], [**Noether, 1927**]). Lo haremos en el caso de cuerpos algebraicamente cerrados porque es el caso que nos interesa para nuestra aplicación.

Nótese que si K es un cuerpo algebraicamente cerrado, por el Nullstellensatz de Hilbert, los maximales del anillo $K[X_1, ..., X_n]$ están en biyección con los puntos del espacio afín $\mathbb{A}^n(K) := K^n$. Es decir,

$$\mathrm{MaxSpec}(K[X_1, ..., X_n]) = \{\mathfrak{m}_a : a \in \mathbb{A}^n(K)\},$$

donde $\mathfrak{m}_a = (X_1 - a_1, ..., X_n - a_n)$ cuando $a = (a_1, ..., a_n)$. Por el Teorema del Ideal Principal de Krull se concluye que

$$\mathrm{ht}(\mathfrak{m}_a) = n, \quad \forall a \in \mathbb{A}^n(K).$$

Por tanto, la dimensión de Krull de $K[X_1, ..., X_n]$ es n.

La idea de Normalización de Noether consiste en ver las K-álgebras finitamente generadas como algo "cercano" a un anillo de polinomios estándar. Es decir, se da el siguiente Teorema:

TEOREMA B.3.7 (**Lema de Normalización de Noether**). *Sea K un cuerpo algebraicamente cerrado y sea $\mathfrak{a} \subseteq K[X_1, ..., X_n]$ un ideal. Entonces, existe una matriz regular $P \in GL(n, K)$ que define un cambio lineal de coordenadas en $\mathbb{A}^n(K)$ del modo siguiente:*

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} = P \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix},$$

de tal modo que la siguiente es una extensión entera de anillos para algún $r \in \{1, ..., n\}$:

$$K[Y_1, ..., Y_r] \hookrightarrow K[X_1, ..., X_n]/\mathfrak{a}. \tag{B.3.1}$$

Nótese que si la extensión (B.3.1) es entera, el número natural r está determinado de manera única por la identidad siguiente:

$$\begin{aligned} r &= \dim(K[Y_1, ..., Y_r]) = \dim(K[X_1, ..., X_n]/\mathfrak{a}) \\ &= \mathrm{coht}(\mathfrak{a}) = \max\{\mathrm{coht}(\mathfrak{p}) : \mathfrak{p} \in \mathrm{Spec}(K[X_1, ..., X_n],\ \mathfrak{p} \supseteq \mathfrak{a}\}. \end{aligned}$$

Se puede decir que *las variables $\{Y_1, ..., Y_n\}$ están en posición de Noether con respecto al ideal $\mathfrak{a}$.*

Supongamos ahora que $\mathfrak{a} \in K[X_1, ..., X_n]$ es un ideal, $P \in GL(n, K)$ un cambio lineal de coordenadas en $\mathbb{A}^n(K)$ tal que, como en el Teorema, tengamos una extensión entera de anillos

$$K[Y_1, ..., Y_r] \hookrightarrow K[X_1, ..., X_n]/\mathfrak{a}. \tag{B.3.2}$$

Consideremos una descomposición primaria irredundante del ideal $\mathfrak{a}$

$$\mathfrak{a} = \bigcap_{i=1}^{m} \mathfrak{q}_i,$$

donde cada $\mathfrak{q}_i$ es $\mathfrak{p}_i$-primario, $i = 1, ..., m$. Supongamos que el ideal $\mathfrak{a}$ es *equidimensional*, es decir, que todos sus primos asociados tienen la misma co-altura

$$\mathrm{coht}(\mathfrak{p}_i) = \mathrm{coht}(\mathfrak{q}_i) = \dim(K[X_1, ..., X_n]/\mathfrak{a}).$$

Entonces, todos los primos asociados son minimales y sus contracciones satisfacen

$$\mathrm{coht}(\mathfrak{p}_i^c) = \mathrm{coht}(\mathfrak{p}_i) = \dim(K[X_1, ..., X_n]/\mathfrak{a}) = \dim(K[Y_1, ..., Y_r]) = r.$$

Pero si los maximales de $K[Y_1, ..., Y_r]$ tienen todos altura r (recordemos que hemos supuesto que K es algebraicamente cerrado), entonces el único ideal primo de $K[Y_1, ..., Y_r]$ de co-altura r es el ideal 0. Hemos concluido así que, bajo nuestras hipótesis,

$$\mathfrak{p}_i = (0) \text{ para cada } i = 1, ..., m.$$

Más aún, tenemos que las siguientes también son extensiones enteras de anillos:

$$K[Y_1, ..., Y_r]/\mathfrak{p}_i^c = K[Y_1, ..., Y_r] \hookrightarrow K[X_1, ..., X_n]/\mathfrak{p}_i,$$

para cada $i = 1, ..., m$. Además, como los divisores de cero del anillo $K[X_1, ..., X_n]/\mathfrak{a}$ son dados por

$$\mathrm{Div}(\mathfrak{a}) = \{f + \mathfrak{a} : f \in \bigcup_{i=1}^{m} \mathfrak{p}_i\},$$

concluimos que ningún elemento no nulo $p \in K[Y_1, ..., Y_r]/\{0\}$ es divisor de cero módulo $\mathfrak{a}$. La razón es que $p \notin \bigcup_{i=1}^{m} \mathfrak{p}_i$ y por tanto $p + \mathfrak{a} \notin \mathrm{Div}(\mathfrak{a})$.

Esta situación es especialmente cierta en el caso en que $\mathfrak{a} = (f_1, ..., f_{n-r})$ es un ideal de altura $n - r$ generado por $n - r$ elementos, como consecuencia del Teorema de la Pureza de Macaulay.

Por último, como $K[X_1, ..., X_n]/\mathfrak{a}$ es una K-álgebra finitamente generada, entonces también es una $K[Y_1, ..., Y_r]$-álgebra finitamente generada. Y como la extensión (B.3.2) es entera, tendremos que $K[X_1, ..., X_n]/\mathfrak{a}$ es un $K[Y_1, ..., Y_r]$-módulo finitamente generado y una $K[Y_1, ..., Y_r]$-álgebra finita.

Glosario de Términos

A-álgebra finitamente generada, 67

altura, 64
anillo local, 49
anillo noetheriano, 59

co-altura, 64

descomposición primaria, 60
dimensión de Krull, 62

extensión de escalares, 28
extensión entera, 67

functor exacto, 49

ideal asociado, 60
ideal primario, 60
intersección completa, 66

localización, 51

matrices equivalentes, 24
matrices localmente equivalentes, 25
módulo de fracciones, 51
módulo extendido, 28
módulo finitamente presentado, 4
módulo libre, 3
módulo plano, 8
módulo proyectivo, 5

presentación finita, 4
producto fibrado, 54
producto tensorial, 52

sistema multiplicativamente cerrado, 50
sucesión exacta, 49
sucesión exacta corta escindida, 5

Glosario de Teoremas y Resultados

Catenaridad de $K[X_1, ..., X_n]$, 65

Ex-Conjetura de Serre, 40

Lema de Nakayama, 53
Lema de Normalización de Noether, 69

Primer Teorema de Quillen, 28

Teorema de Horrocks, 29
Teorema de la Pureza de Macaulay, 65
Teorema de Lasker-Noether, 60
Teorema de Quillen-Suslin, 37
Teorema de Vaserstein, 25
Teorema del Ascenso (Going-Up), 68
Teorema del Descenso (Going-Down), 68
Teorema del Ideal Principal de Krull, 65
Trivialidad Local de los Módulos Proyectivos, 21

Glosario de Símbolos y Abreviaturas

$D(f)$, 10
$GL(r, R)$, 24
$Jac(R)$, 53
$M \otimes_R N$, 52
$M_{\mathfrak{p}}$, 51
M_a, 51
$M_{r\times s}(R)$, 24
$S^{-1}M$, 51
$\mathrm{Ass}(R/\mathfrak{a})$, 60
$\mathrm{Div}(\mathfrak{a})$, 61
$\mathrm{Hom}_R(M, -)$, 52
$\mathrm{MaxSpec}(R)$, 49
$\mathrm{Spec}(R)$, 51
$\mathrm{coht}(\mathfrak{p})$, 64
$\dim(W)$, 62
$\mathrm{ht}(\mathfrak{p})$, 64
$\mu(M)$, 49
$(R, \mathfrak{m})$, 49

Bibliografía

[Adkins-Weintraub, 1992] W.A. Adkins, S.H. Weintraub, *Algebra: an approach via module theory*. Springer-Verlag (1992), 120.

[Atiyah-Macdonald, 1969] M. F. Atiyah, I. G. Macdonald, *Introduction to Conmutative Algebra*, Addison-Wesley Publishing Co, (1969).

[Fdez, 2021] T. Fernández Ruiz, *La Desigualdad de Bézout Geométrica de J. Heintz: deconstrucción, una prueba autocontenida*. Trabajo Fin de Grado, Grado en Matemáticas, Facultad de Ciencias, Universidad de Cantabria, (2021).

[GHMMP, 1998] M. Giusti, J. Heintz, J. E. Morais, J. Morgenstern, L. M. Pardo, *Straight-line programs in geometric elimination theory*, Journal of Pure and Applied Algebra **124**, (1998), 101-146.

[GHMP, 1997] M. Giusti, J. Heintz, J. E. Morais, L. M. Pardo, *Le rôle des structures de données dans les problèmes d'élimination (The relevance of data structures for elimination problems, in French)*, Comptes Rendues Acad. Sci. Paris, Sér. I **325**, (1997), 1223-1228.

[GHS, 1993] M. Giusti, J. Heintz, J. Sabia, *On the efficiency of effective Nullstellensätze*. Computational Complexity **3**, (1993), 56-95.

[Heintz, 1983] J. Heintz, *Definability and First Quantifier Elimination over Algebraically Closed Fields*, Theoretical Computational Science **24**, (1983), 239-277.

[Hilbert, 1890] D. Hilbert, *Über die Theorie der algebraischen Formen*, Math. Annalen **46**, (1890), 473-530.

[Horrocks, 1964] G. Horrocks, *Projective Modules over an Extension of a Local Ring*. Proc. London Math. Soc. **14** (1964), 714-718.

[Kronecker, 1882] L. Kronecker, *Grundzüge Einer Arithmetischen Theorie Der Algebraischen Grössen*, J. für Reine und Augen. Matematik **92**, (1882), 1-122.

[Krull, 1935] W. Krull, *Idealtheorie*, Springer, (1935).

[Kunz, 1985] E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*. Birkhäuser (1985), 63-122.

[Macaulay, 1916] F. S. Macaulay, *The Algebraic Theory of Modular Systems*. Cambridge Tracts in Mathematics and Mathematical Physics, Cambridge University Press, (1916).

[Noether, 1921] E. Noether, *Idealtheorie in Ringbereichen*, Math. Annalen **83**, (1921), 24-66.

[Noether, 1927] E. Noether, *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern*, Math. Annalen **96**, (1927), 26-61.

[Pardo, 1995] L. M. Pardo, *How lower and upper complexity bounds meet in elimination theory*, Lecture Notes in Computer Science **948**, G. Cohen, M. Giusti & T. Mora, eds., Springer Verlag, (1995), 33-69.

[Pardo, 2021] L. M. Pardo, *Notas para un Curso Básico de Álgebra Conmutativa*. Universidad de Cantabria (2021).

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

[Rag *et al*, 1975] S. Raghavan, B. Singh, R. Sridharan, *Homological Methods in Commutative Algebra*, Tata Institute for Fund. Res., Oxford University Press, (1975).

[RS, 1991] F. Rossi, W. Spangher, *Some Effective Methods in the Openness of Loci for Cohen-Macaulay and Gorenstein Properties*. En "Effective Methods in Algebraic Geometry", T.Mora, C.Traverso, Progress in Mathematics **94**, Birkhäuser Verlay, (1991), 441-455.

[Serre, 1955] J.P. Serre, *Faisceaux algébriques cohérents*. Annals of Mathematics, Second Series, **61** (1955), 197–278.

[Serre, 1960-61] J. P. Serre *Sur les modules projectifs*, En "Séminaire Dubreil", (1960-61).

[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.

[Zariski-Samuel, 1958-60] O. Zariski, P. Samuel, *Conmutative Algebra*, Van Nostrand; vol. I (1958), vol. II (1960).